Hyper-connectivity: Intricacies of national and international cyber securities.

Maurice Dawson

Submitted in partial fulfillment of the award of Doctor of Philosophy by Prior Output at London Metropolitan University

PART II

August 2017

1. Dawson, M., Burton, S. L., Bessette, D., & Wright, J. (2018). Massive Open Online Courses and Integrating Open Source Technology and Open Access Literature Into Technology-Based Degrees. In M. Khosrow-Pour, D.B.A. (Ed.), *Encyclopedia of Information Science and Technology,* Fourth Edition (pp. 7898-7911). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2255-3.ch687
2. Dawson, M., & Cárdenas-Haro, J. A. (2017). Tails Linux Operating System: Remaining Anonymous with the Assistance of an Incognito System in Times of High Surveillance. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)*, 1(1), 47-55.
3. Dawson, M. (2017). Cyber Security Policies for Hyperconnectivity and Internet of Things: A Process for Managing Connectivity. In *Information Technology-New Generations* (pp. 911-914). Springer, Cham.
4. Dawson, M., Lieble, M., & Adeboje, A. (2017). Open Source Intelligence: Performing Data Mining and Link Analysis to Track Terrorist Activities. In *Information Technology-New Generations* (pp. 159-163). Springer, Cham.
5. Dawson, M. (2016). Exploring Secure Computing for the Internet of Things, Internet of Everything, Web of Things, and Hyperconnectivity. In M. Dawson, M. Eltayeb, & M. Omar (Eds.) *Security Solutions for Hyperconnectivity and the Internet of Things* (pp. 1-12). Hershey, PA: Information Science Reference. doi:10.4018/978-1-5225-0741-3.ch001
6. Davis, L., Dawson, M., & Omar, M. (2016). Systems Engineering Concepts with Aid of Virtual Worlds and Open Source Software: Using Technology to Develop

Learning Objects and Simulation Environments. In F. Neto, R. de Souza, & A. Gomes (Eds.)*Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning* (pp. 483-509). Hershey, PA: Information Science Reference. doi:10.4018/978-1-5225-0125-1.ch020

7. Dawson, M., Omar, M., Abramson, J., Leonard, B., & Bessette, D. (2016). Battlefield Cyberspace: Exploitation of Hyperconnectivity and Internet of Things. In M. Dawson, D. Kisku, P. Gupta, J. Sing, & W. Li (Eds.) *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 204-235). Hershey, PA: Information Science Reference. doi:10.4018/978-1-5225-0703-1.ch010
8. Dawson, M., & Adeboje, W. (2016). Islamic Extremists in Africa: Security Spotlight on Kenya and Nigeria. In M. Dawson, D. Kisku, P. Gupta, J. Sing, & W. Li (Eds.) *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 93-103). Hershey, PA: Information Science Reference. doi:10.4018/978-1-5225-0703-1.ch005
9. Dawson, M., Eltayeb, M., & Omar, M. (2016). Security Solutions for Hyperconnectivity and the Internet of Things (pp. 1-347). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0741-3
10. Dawson, M., DeWalt, B., & Cleveland, S. (2016). The Case for UBUNTU Linux Operating System Performance and Usability for Use in Higher Education in a Virtualized Environment.
11. Dawson, M., & Omar, M. (2015). *New Threats and Countermeasures in Digital*

Crime and Cyber Terrorism (pp. 1-368). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8345-7

12. Dawson, M. (2015). A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism. In M. Dawson, & M. Omar (Eds.) *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 1-7). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8345-7.ch001
13. Dawson, M., Wright, J., & Omar, M. (2015). Mobile Devices: The Case for Cyber Security Hardened Systems. In M. Dawson, & M. Omar (Eds.) *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 8-29). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8345-7.ch002
14. Leonard, B., & Dawson, M. (2015). Legal Issues: Security and Privacy with Mobile Devices. In M. Dawson, & M. Omar (Eds.) *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 95-104). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8345-7.ch006
15. Dawson, M., Leonard, B., & Rahim, E. (2015). Advances in Technology Project Management: Review of Open Source Software Integration. In M. Wadhwa, & A. Harper (Eds.) *Technology, Innovation, and Enterprise Transformation* (pp. 313-324). Hershey, PA: Business Science Reference. doi:10.4018/978-1-4666-6473-9.ch016
16. Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the Methods

behind Cyber Terrorism. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1539-1549). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-5888-2.ch147

17. Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). The Future of National and International Security on the Internet. In A. Kayem, & C. Meinel (Eds.) *Information Security in Diverse Computing Environments* (pp. 149-178). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-6158-5.ch009

18. Dawson, M., Al Saeed, I., Wright, J., & Onyegbula, F. (2014). Open Source Software to Enhance the STEM Learning Environment. In V. Wang (Ed.), *Handbook of Research on Education and Technology in a Changing Society* (pp. 569-580). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-6046-5.ch042

19. Dawson Jr, M. E., Crespo, M., & Brewster, S. (2013). DoD cyber technology policies to secure automated information systems. *International Journal of Business Continuity and Risk Management*, *4*(1), 1-22.

20. Dawson, M. E., & Al Saeed, I. (2012). Use of Open Source Software and Virtualization in Academia to Enhance Higher Education Everywhere.*Cutting-edge Technologies in Higher Education*, *6*, 283-313.

21. Dawson, M., & Rahim, E. (2011). Transitional leadership in the defence and aerospace industry: a critical analysis for recruiting and developing talent.*International Journal of Project Organisation and Management*, *3*(2),

164-183.

22. Dawson, M., Burrell, D. N., Rahim, E., & Brewster, S. (2010). Integrating Software Assurance into the Software Development Life Cycle (SDLC).*Journal of Information Systems Technology and Planning*, *3*(6), 49-53.

23. Dawson, M., Burrell, D. N., Rahim, E., & Brewster, S. (2010). Examining the role of the chief information security officer (ciso) & security plan. *Journal of Information Systems Technology & Planning*, 3(6), 1-5.

24. Cardenas-Haro, J. A., & Dawson, M. (2017). Tails Linux Operating System: The Amnesiac Incognito System in Times of High Surveillance, Its Security Flaws, Limitations, and Strengths in the Fight for Democracy. In M. Dawson, M. Eltayeb, & M. Omar (Eds.), *Security Solutions for Hyperconnectivity and the Internet of Things* (pp. 260-271). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0741-3.ch010

25. Eltayeb, M., & Dawson, M. (2016). Understanding user's acceptance of personal cloud computing: Using the Technology Acceptance Model. *Information technology: New generations*, 448, 3-12.

26. Omar, M., & Dawson, M. (2013, April). Research in Progress-Defending Android Smartphones from Malware Attacks. In *Advanced Computing and Communication Technologies (ACCT), 2013 Third International Conference on* (pp. 288-292). IEEE.

Encyclopedia of Information Science and Technology, Fourth Edition

Mehdi Khosrow-Pour
Information Resources Management Association, USA

IGI Global
DISSEMINATOR OF KNOWLEDGE

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Khosrow-Pour, Mehdi, 1951- editor.
Title: Encyclopedia of information science and technology / Mehdi Khosrow-Pour, editor.
Description: Fourth edition. | Hershey, PA : Information Science Reference, [2018] | Includes bibliographical references and index.
Identifiers: LCCN 2017000834| ISBN 9781522522553 (set : hardcover) | ISBN 9781522522560 (ebook)
Subjects: LCSH: Information science--Encyclopedias. | Information technology--Encyclopedias.
Classification: LCC Z1006 .E566 2018 | DDC 020.3--dc23 LC record available at https://lccn.loc.gov/2017000834

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Massive Open Online Courses and Integrating Open Source Technology and Open Access Literature Into Technology-Based Degrees

Maurice Dawson
University of Missouri – St. Louis, USA

Sharon Burton
Grand Canyon University, USA

Dustin Bessette
National Graduate School of Quality Management, USA

Jorja Wright
University of Charleston, USA

INTRODUCTION

The purpose of this chapter is to (1) understand MOOCS, massive online open courses, and differentiate MOOCS from other like learning and training methodologies, (2) comprehend the manner in that MOOCS can be utilized, as well as the (3) lasting impacts of MOOCS on learning whether in academics or the corporate environment. MOOCs are aimed at large scale participation in online education (Bud, Smith, & Reisman, 2015). This chapter will identify for educators, administrators, and practitioners the staggering awareness of the outcomes of this learning modality. MOOCs are continuing to change the way individuals receive education and learn. One idea of MOOCs is that learners may learn through collective education using what is believed to be a form of experimentation wrapped in andragogy, adult learning, andragogy. Education through Knowles' adult learning, offers the notion of learners gaining knowledge and understanding through (a) self-directedness, (b) need to know, (c) use of experience in learning, (d) readiness to learn, (e) orientation to learning, and (f) internal motivation (Knowles, 1979; Taylor & Kroth, 2009). Another view is that MOOCs could be the answer to the economic concerns faced by institutions of higher learning, the push to increase learner enrollment, and the drive to enhance graduation completion rates (Ng'ambi & Bozalek, 2015). Administrators, educators, and practitioners are faced with the increased popularity of MOOCs. The popularities of MOOCs include the positives as well as the concerns: their impersonal nature, numerous students enrolled into an individual section of a MOOC course, instructors serving as facilitators, as well as there being no instructors assigned to courses. MOOCs, post-date open courseware which was on the increase in 1990s and the sharing of courseware online. Specifically, open courseware stems from face-to-face instructions wherein instructors share aspects of their courses on the Internet which may be reading lists, assignments, recorded videos, audio lectures, or syllabi. One of the understood top aspects regarding MOOCs is that these courses fulfil knowledge gaps for learners. MOOCs propose for the learners the alternative of completing quality courses without a financial obligation. Some MOOCs

DOI: 10.4018/978-1-5225-2255-3.ch687

courses, like Cousera, offer certificates. With this said MOOCS offer inexpensive avenues to add certificates to learners' resumes and therefore ways to drive personal accomplishments. MOOCs have maintained a large following of users. They draw attention and remain the element learners need to study and become educated outside of the traditional classroom.

This chapter will delve into key significant areas. First, the researchers will gain understanding regarding the development of a method in which Open Source Software (OSS), open source technologies, and open access literature can be incorporated to strengthen the MOOC environment. Second, readers will garner comprehension of how to strengthen the MOOC environment and therefore increase retention in addition to increasing enrollment in higher education. Third, the lasting impacts of MOOCs will be described, mainly as the impacts relate to STEM, Science, Technology, Engineering, and Mathematics and how such programs are entering the online space. Through this chapter, educators and administrators will grasp an increased interpretation of the technologies that have influenced learning and development. Administrators and Practitioners will learn meaningful solutions about open technology solutions so that as-is and to-be MOOCs can be improved with minimal cost. Further readers, researchers, administrators, and practitioners will learn how to infuse MOOCs learning and training initiatives to ensure best outcomes in the academic and e business world.

BACKGROUND

MOOCs is another form of distance education and learning community; the term originated in 2008 by David Cornier and senior research fellow Bryan Alexander (Martin, 2010). At that time, MOOCs described a course entitled *Connectivism and Connective Knowledge* (Pence, 2012). According to Caulfield, Collier, and Halawa (2013), MOOCs stem from the category of online connected learning communities. MOOCs are representative of Siemens' and Downes' connectivist learning theory, which provides that learning occur through connections within networks (Pence, 2012). The model uses a network with nodes and associations to explain learning (Siemens, 2013). The name MOOC was derived because (a.) MOOCs are collaborative with the appearance of experimentation, (b.) the courses move along numerous paths, and (c.) MOOCs necessitate participation in "Massively Multiplayer Online Game (MMOG)" (Pence, 2012, p. 27).

MOOCs, a recent innovation in the distance education field, were labeled as disruptive innovation (Christensen, 1997). According to Flynn (2013), MOOCs describe the varied kinds of changes in an evolving business education environment. The concept bracing MOOCs began in the 1960s; however, this approach to distance education re-ignites because of the digital education age (Flynn, 2013). As posited by Ta'eed (2012), Khan Academy was the first to house the free lectures. The Bill Gates Foundation and Google supported Khan Academy, a non-profit, with substantial backing in 2006. Today Khan Academy has over 3000 short video lectures, which were stated to have over 160 million hits (Severns, 2014; Ta'eed, 2012).

Understanding MOOCs and their relevance is important as MOOCs meaningfully progressed online distance education in past years (Rodriguez, 2012). Standing as an online distance educational model, MOOCs, are supported by colleges and universities; therefore, the need exist for faculty to understand and augment their knowledge regarding MOOCs' past, current and future trends. MOOCS have several prescribed frameworks: cognitive-behaviorist, connectivist social and constructivist (Rodriguez, 2012), connectivism (Pence, 2012), constructivist, connectivist experiential, and social structure, (Koutropoulos et al., 2012). The postulations of these researchers are that MOOCs were formed by technologies

and reside beneath the online distance education environment.

FACULTY DEVELOPMENT IN MOOCs

Through the lens of MOOCs, readers, practitioners, and academicians can postulate the reasons MOOCs emerged on the distance education platform. As educators continue to concentration on the online distance education environment, comprehending MOOCs is yet another lane in learning for meditation and conjecture. Faculty development with MOOCs has the potential to facilitate networking and permit instructors to converse and discuss concepts and experiences. Professors interested in MOOCs can add value to their repertoire of knowledge by engaging in MOOC mentoring, coaching, and job shadowing programs. Mentorships are associations encompassing a seasoned faculty member who guides faculty with minimal experience or faculty with no experience (Tareef, 2013). Coaching, as given by Rahim and Burrell (2013), is "having an ability to help an employee who has raw talent develop into a star performer". Job shadowing involves investigating the actions of a professional systematically, and then including the desired actions into one's work procedures (Leonard, Barton, & Barton, 2013).

Professional development within institutions of higher education remains a significant variable driving excellence of education learners' academic experiences (Marshall, 2012; Mosley, 2007). Every institution of higher education should establish if, how, and when MOOCs will hold an academic space in their educational lineup. Faculty should comprehend the evolution of MOOCs into and around their institutions. According to Demirci (2014), the syllabus of MOOCs is very similar to other syllabus. Further learning activities are developed to accommodate large audiences. The lessons and activities can be organized as asynchronous and with flexibility (Demirci, 2014). Faculty should look to faculty development programs, mentorships, and coaching to gain additional information regarding MOOCS and their impact.

HOW ARE MOOCS BEING SUPPORTED

Elite institutions of higher education are supporting MOOCs. According to Thrift (2013), an obsession exists with MOOCs because (a) institutions of higher learning are enticed by the promise of profit in educational environments, (b) middle-class aggravation over tuition costs is fueled, (c) economic downturn is propelling countries to seek better priced education that is valued, and (d) MOOCs seem to provide a more efficient mode of education. Pence (2012), provided, the thought remains that partaking in MOOCs may gather meaningful stature. Another advantage of MOOCs provided by Pence (2012) is that MOOCs can produce analytics about education. Analytics can support a drive for operational sustainability. Data regarding MOOCs is found primarily through blog posts (Yong, 2014).

OFFERING MOOCS

Led by Sebastian Thrun, in 2011 Stanford University offered a MOOC. Thrun's postulation was that eventually participants would graduate with degrees with MOOCs on the transcripts (Krause, 2014). Stanford's MOOC enrollment was over "160,000 students from 190 different countries" (Flynn, 2013, p. 152). According to Krause (2014), 28,000 completed the courses. The MOOC project expanded. Thrun left Stanford to start Udacity, a for-profit company (Flynn, 2013, Krause, 2014). The goal was to make education a democracy by providing it to learners at no cost (Flynn, 2013). Udacity offers STEM courses, Science, Technology, Engineering, and Math.

Motivated by Thrun, Andrew Ng, and Daphne Koller, two other Stanford faculty members co-founded Cousera, a for profit company (Krause, 2014). Coursera functioned akin to an educational cooperative between Stanford University, University of Pennsylvania, University of Michigan, and Princeton University (Flynn, 2013). According to Krasue, Coursera and Stanford, now partners with "33 high caliber universities" (Decker, 2014, p. 7). Coursera courses start frequently and are available in a wide range of topics.

Articulated by Flynn, (2013), $30 million each in institutional backing, funding of grants, and resources was donated by MIT and Harvard to launch edX, a MOOC. This not-for-profit initiative started with 32 charter members (PR, N, 2014). Harvard is the oldest institution of higher learning in the United States, established in 1636. Harvard's support of MOOCs is significant. Kolowich (2013a), states that Harvard is very careful with its MOOCs partnerships. Since its beginning, edX has continuously progressed and offers courses on an array of subjects. MIT offers MOOC curricula (Kolowich (2013b).

Initially opposed to MOOCs, universities like Duke University decided against the MOOCs revolution. Disclosed by Kolowich (2013c), the faculty voted the measure down after Duke's provost, Peter Lange, signed a contract with 2U, a MOOCs group. The Chronicles of Higher Education article provided that the faculty's vote superseded the contract signed by Lange. Now Duke is a part of the MOOCs revolution and advertises MOOCs on its online website. Another institution that initially rejected MOOCs was Amherst College, a liberal arts institution. April 2013, Amherst College's faculty rejected Harvard's edX invitation to become a part of the elite association of higher education institutions providing MOOCs (Kolowich, 2013a). During this time, the academe world had mixed views about the MOOCs form of distance education. Today, when viewing Amherst's web site, MOOCs are now advertised.

MOOCS CRITIQUED

Many elite colleges and universities have supported MOOCs. Some people see MOOCs as innovative and the future of education. Other people understand MOOCs to be all that is wrong with education. What is known is that MOOCs are receiving critiques. According to Rees (2014), MOOCs are akin to students going to the library to check out educational materials and then reading and studying the materials. Some believe that MOOCs will destroy today's understanding of higher education (Fox, 2013). Others document that the course completion rate for MOOCs is too low (Guzdial, 2013). Questions are surfacing as to whether MOOCs will devalue instructors in the realm of education. The concern of sustaining revenue and not offering too many MOOCs is just another concern. What is understood about MOOCs is that they are perceived as a business model like other educational delivery models.

The MOOCs model was founded on the idea that institutions of higher of learning are the developing segments in line for the high-capacity, low-perimeter data and information-technology treatment after cost review, sales, and the media, as given by Thrift (2013). MOOCs are accessible and accommodate large numbers of learners. MOOCS support lifelong learning. In essence, MOOCs characterizes emerging technology whose educational impact has yet to be fully understood. As shown through Amherst's and Duke's later embracing of MOOCs, this form of online distance education will continue to undertake in the practices of higher education.

MOOCs IMPLEMENTATION AND CHANGE

The MOOCS phenomenon has driven an ever-increasing conversation regarding online courses whether in higher education, or business. These developments must be explored from an institutional policy standpoint, focusing on an examina-

tion of the different approaches to MOOCs and e-learning. MOOCS implementation represents change. This change points to (1) curriculum and course design and redesign, (2) a sound e-learning policy as a medium for curriculum development; (3) an emphasis on technology usage; (4) specific policies around licensing; (5) how MOOCs support student advancement; and (6) overall educational enhancement that drives student success.

The change to incorporate MOOCS requires a paradigm shift, a new approach to thinking about online educational processes and technologies. In order for MOOCs to be administered successfully, a top down approach is needed (Burton, 2016). Because people in like organizations will exhibit like behaviors, there must be a change leader to drive communication up and down the communication chain. This leader has to know the key organizational factors: understanding the vision of the implementation, ensuring accountability of key roles for the MOOCs implementation, ensuring the appropriate stakeholders' involvement, determining what skills need to be developed (e.g., developer, staff, students, employees, etc.), ensuring the appropriate metrics, policies and actions, as well as determining how to reinforce behaviors. Initiating the change will require an understanding of the MOOCs implementation range and scope of the project. All leaders and project participants must understand all difficulties and intricacies involved with MOOCs development, and implementations. Timeframe be known for the development and implementation. Most of all, to make the implementation work, all involved must buy-in to the idea.

MOOCs are a disruptive form of education. However; due technology driving learning to the anytime and anyplace environment, the conversation about MOOCs has change. The new conversation need to be about how this form of education will progress leaning institutions and organization toward business process improvement. MOOCs can be implemented as change to support the learning institutions and organizations broader strategic objectives.

OPEN ACCESS LITERATURE

Open access is digital, online, free of charge for everyone with an internet connection, free of most copyright and licensing restrictions (Suber, 2004). Technology has opened many doors and opportunities for the current needs for many academicians, researchers, and practitioners based on the need to have open access availability for literature. The possibility of restricting literature in the future will come at a cost that will be indefinitely become a nuisance for businesses and schools to utilize. MOOC programs of today already are facing the possibility of creating online learning environments that only enhance and filtrate open access literature and learning. Open access has even made it possible for a vast majority of scholars to share theories, research and information such that it can be primarily used in an online database of journals for future reference and research.

Proponents of open access publishing sometimes argue their case on the fairness of providing everyone with access to scholarly material, and by so doing, creating a scientific/academic level-playing field (Nicolas, Huntington, & Jamali, 2007). Open access publishing has become a well known publishing and research style that many scholars, faculty, and practitioners are beginning to position themselves around based on the possibility of other scholars referencing and citing their research and work. This is the ultimate goal of open access literature. With better availability and access to vital research, data can be disseminated to more outside sources to create a better understanding of global research. Therefore, the literature of today needs to be adaptable and accessible for communities and scholars of tomorrow. Creating a validation for open access literature is a primary need for many societies to have based on the utilization of tools in the virtual and traditional classrooms. The tools and styles used are practices of students in virtual learning environments (Bessette & Burton, 2013). The learning environments of the MOOCs are ideally using and utilizing online open access literature and references such that it is readily

available to more people today than ever before. Libraries with traditional literature are becoming outdated as technology for academic advancement is taking place.

The age of the electronic journal has also brought another problem to the library (Chang, 2006). Traditional libraries of today are being more advanced to replace the current physical copy of journals and textbooks and utilizing technology to the max. This adaptation is creating a faster advancement and movement for the retrieval process of literature. More scholars, students, researchers, and practitioners are requiring access 24/7. The increase of the electronic journal and the open access journal are beginning to develop a keen sense of adaption for research to be published and researched at any time in any place. The need for high speed internet access has also become part of the availability and usefulness for online open access literature.

Scholars, faculty, researchers, and practitioners need to coordinate and publish exclusively in all types of scholarly journals. These journals also need to be read and referenced accordingly in order to successfully develop keen communication between scholars of different disciplines. Without scholastic publishing and referencing of open access work, scholarly research will be under-utilized and problems will persist. Costs of subscriptions for scholastic journals will increase, creating a crisis that is also known as serials crisis. To prevent the "Serials Crisis" situation from becoming worse, research organizations and libraries are starting to support open access publishing (Chang, 2006). Every academic discipline needs to currently outweigh the cost for using and utilizing open access literature based that all research needs to have an open accessible and ideal use based on the needs of scholars for the future.

The utilization of MOOCS into the open access literature will deviate cognitive learning and skill development for students. It is then possible to assume that students will accelerate their learning capabilities to such a level that is currently unmeasured. The need for the open accessibility and developmental change is in the hands of academicians today. MOOC classes will invite,

Figure 1. Screenshot of Directory of Open Access Journals

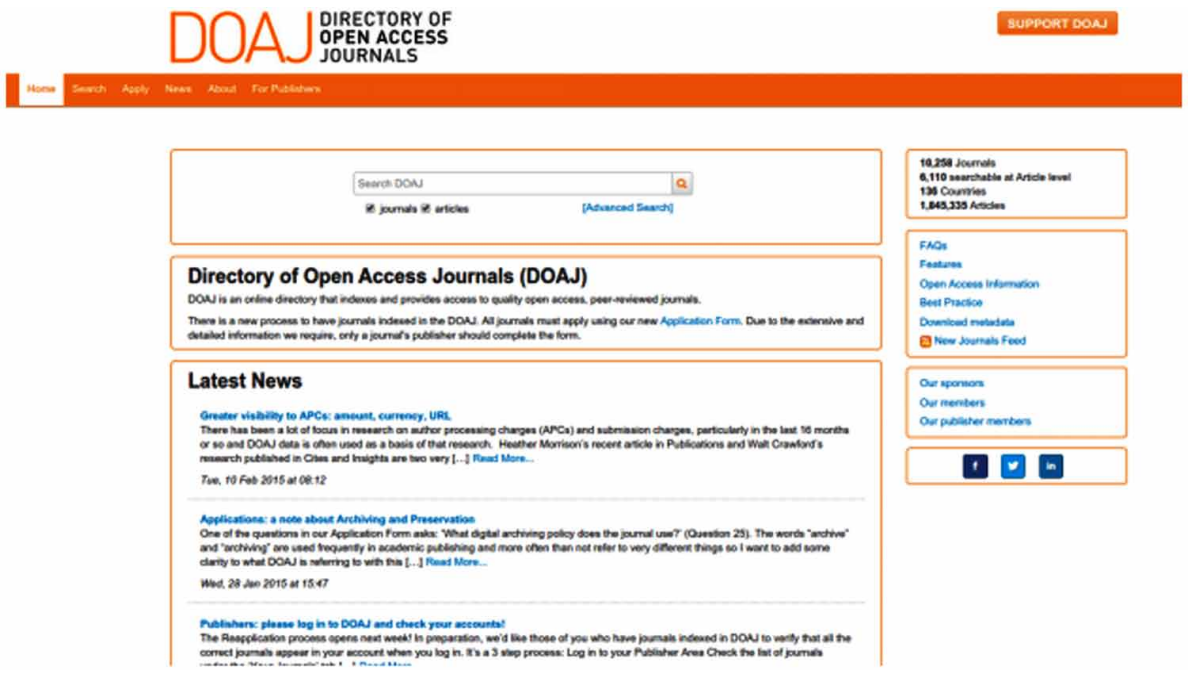


Table 1. Linux distributions and uses

Linux Distributions	Description and Potential Use	Package
Ubuntu	One of the most popular Linux OS developed to be a complete OS that can be an easily replacement for other comparable OSs.	Debian-based
Edubuntu	OS targeted for grades k-12. Contained in OS are tons of software applications that is useful to those who are education majors.	Debian-based
Damn Small Linux	This OS is designed to as a small OS to be utilized on older hardware. This OS is great for institutions that have old computers and want to revitalize them for use. OS is also great for VMs as DSL requires a low amount of memory.	Knoppix-based
BackTrack	OS based on Ubuntu for digital forensics and penetration testing. Great tool for students majoring in technology fields. As cyber security is becoming a hot topic around the world this tool provides students the ability to learn from over thirty software applications that aid in penetration testing and more.	Debian-based
Fedora	This OS is supported by the Fedora Project and sponsored by Red Hat. This OS provides a great resource for learning Red Hat Enterprise Language (RHEL). As there are thousands of jobs requiring expertise specifically with Red Hat this OS is a great tool to prepare students for employment in IT. Fedora has over six Fedora Spins such as Design-suite, Scientific-KDE, Robotics, Electronic-lab, Games, and more.	RPM-based
Kali	An advanced forensics and penetration testing distribution that is the successor of BackTrack.	Debian-based
Elementary	OS is based on Ubuntu and showcases the Pantheon desktop. This OS is focused on usability, and design aesthetics. The desktop environment has been compared to Mac OS. This desktop origins from being an Ubuntu desktop theme.	Debian-based
CentOS	This OS derived entirely from RHEL. The source code is developed from Red Hat which allows a student to learn RHEL with a small number of differences. CentOS can be used for teaching IT students on how to setup, administer, and secure a server.	RPM-based
Ubuntu Studio	This OS is derived from Ubuntu. This OS is developed specifically for multimedia production such as audio, video, and graphics. Departments for multimedia could use this OS for multimedia instruction and the development of projects. As many of the tools for multimedia production are expensive this alleviates large license costs for institutions.	Debian-based
Lubuntu	OS is based on Ubuntu and uses the LXDE desktop environment. It replaces Ubuntu's Unity shell and GNOME desktop.	Debian-based

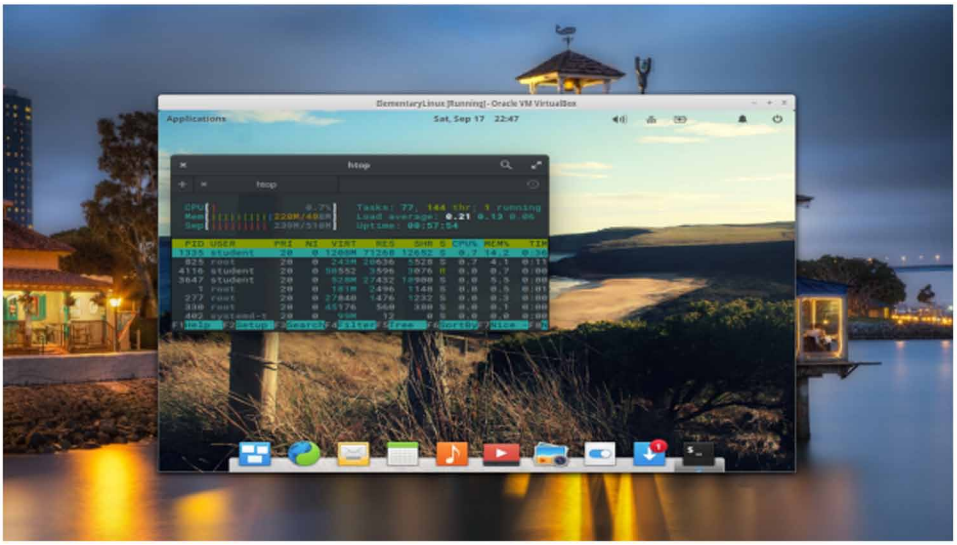
enhance, and protect the vital means of academic learning through learning techniques as part of program changes and alterations. Open access literature is needed for MOOC system improvements as well as academic and career changes nationwide. In the figure below is a screenshot of the Directory of Open Access Journals (DOAJ) which is of one of the most popular sites for open access refereed works.

STEM NEEDS FOR MOOCS

As STEM is continues to play a critical role in America, Linux could provide the ability an affordable large scale deployment. Even more important is the environment where individuals can practice skillsets and techniques learned from the classroom. Thus, Linux provides the ability for students to perform low level code analysis. In developing the class environments with cost in consideration Linux allows for this to be done with removing costly barriers with the exception of hardware. The barriers are proprietary software licenses, and software that operates on a particular

V

Figure 2. Elementary Linux in a VM



hardware configuration. The associated software licensing allows for applications to be used freely in MOOCs for enhancing the overall experience.

The addition of Virtual Machines (VM) in MOOCs enhance the overall courseroom experience. VMs can be loaded to the MOOC site which mimic the instructor's teaching environment for a particular course [See Figure 2]. The course tools such as programming environments, networking tools, offensive security applications, and more can already included in the VM. Additionally, this environment can be exported to an ISO image file so that as this file format will work with multiple hypervisors.

SOFTWARE LICENSING

When considering software licensing it is essential to understand the license agreements for the applications that are used within the MOOC (Dawson, Leonard, & Rahim, 2015). This will allow for the use or redistribution of software. The use of OSS can greatly enhance the STEM environment (Dawson, Al Saeed, Wright, & Onyegbula, 2014).

GNU GPL v3

After a review of the terms and conditions provided by this license it appears to be more comprehensive in its requirements for use of the licensed software. It contains several more terms and appears to contain many more prohibitions that the previous version of the license terms contained. It contains the requirement to include appropriate notices for distribution of the code. It also contains specific prohibitions regarding restriction on the subsequent use of the code, including modified versions, by downstream users (Kumar, 2006).

GNU GPL v2

After review of the terms and conditions of this license, this version's license does not appear to have as many requirements and certainly is not as long as the newest version of this software's license appears to be. While considerably shorter than the subsequent version's license, this license does still maintain and include the requirement that appropriate notices accompany the distribution of the code (Kumar, 2006).

LGPLv3

After review of the terms and conditions of this license, this version's license does not appear to have as many requirements as either of the licenses under the GNUGPLv3 or v2, but it does maintain several requirements for compliance. Of note, is this license includes an exception to the GNUGPL license, namely that the work produced under this license may be reproduced without compliance with Section 3 of the GNUGPL, which relates to Protecting Users' Legal Rights from Anti-Circumvention Law.

LGPL v2

After review of the terms and conditions of this license, this version's license appears to somewhat longer than the terms and conditions of the subsequent version's license, but it appears to be closer to the GNUGPLv2's license terms than the LGPLv3's terms and conditions, and noticeably does not include the exception to the GNUGPL license as is contained in the subsequent version of this license.

LLGPL

After review of the Lisp Lesser General Public License (LLGPL), this version's license is like the LGPL but with a prequel. This prequel defines the effect in terms more typically used in Lisp programs. This license is grounded in the C programming language as the license specifically calls out functions not present in other languages that are not traditionally compiled (Greenbaum, 2013).

Apache 2.0

The previous Apache licenses were based on the GPL v2 however the Apache License v2 permits code that is covers to be subsumed into closed source projects (Rosen, 2015). It also explicitly grants patent right where necessary to modify, operate, and distribute the software.

MIT License

The MT license provides permission, free of charge, to any individual obtain a copy of the software and associated documentation. Additionally, it (Rosen, 2015). Also provided without limitation is the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the software (Rosen, 2015).

Creative Commons

After review of the terms and conditions of this license, it appears that this license is very similar to that of Modified BSD. It is interesting of note that the license begins by indicating that the company is not a law firm. Additionally, this license appears to include a waiver of copyrights and related rights, and a fall-back in the event that the waiver is invalidated, which appears to be based upon the purpose of promoting the overall ideal of free culture. In addition this license includes a limitation to make sure that neither patent or trademark rights are being waived by this license.

Artistic License 2.0

After review of the terms and conditions of this license, this license appears to be very similar to that at issue in the Jacobsen case discussed above. Moreover, it appears that this license makes clear that the copyright holder intends to retain some creative control over the copyrighted work overall, while still trying to ensure that the copyrighted material remains as open and available to others as possible under the circumstances.

Modified BSD

After review of the terms and conditions of this license, these terms and conditions appear to be the shortest list of terms and conditions of all of

Figure 3. System Engineering Virtual Test

the licenses reviewed in this paper. Additionally this license appears to allow reproduction and modification of the copyrighted material provided certain conditions are met, which if subject to legal challenge, a court might construe as being subject to only protection as a contract, at best, and a bare license at worst. Moreover, based upon the legal authorities cited in this paper, it may be unclear whether this license may provide sufficient copyright protection.

Clear BSD License

After review of the terms and conditions of this license, this license appears to be very similar to the Modified BSD License, in that it is very short, and appears to allow reproduction only if certain conditions are met. This license does make clear that no patent rights are granted by this license.

VIRTUAL WORLDS

Virtual worlds can provide a platform to teach the labs in an environment that is dynamic and takes advantage of ubiquitous learning (Davis, Dawson, & Omar, 2016; Dawson & Al Saeed, 2012). Access to a MOOC could occur in a manner that a student performs an engineering lab design in the virtual world environment. This would allow the individuals to have a low fidelity lab in which the activities provided in the MOOC can be done in an environment that allows for synchronous or asynchronous participation. The MOOC environment could be enhanced with the use of virtual environments with the use of virtual laboratories, virtual museums, augmented reality, collaborative e-learning, Neto, de Souza, & Gomes, 2016).

CONCLUSION

Despite the fact that many innovations in the field of educational technology have existed throughout the decades, undoubtedly the most conspicuous public conversations in mainstream media are pointed to the phenomenon, massive open online courses (MOOCs). Pappano (2012), in her New York Times November 2012 article branded the year 2012 as the "Year of the MOOCs". This labeling help to propel MOOCs into being a significant educational technological catchphrase.

Conceptually, MOOCs appeared to be the utmost in learning in the online space; however, glitches appeared. These glitches include but are not limited to underwhelming involvement, lower than expected completion rates, and imbalanced content significance according to Marrapodi, Shimkus, and Onisk (2016). Notwithstanding the rising accessibility, attraction, and probability of MOOCs, their economic justification and their academic value required more exploration, and particularly the technological aspects.

FUTURE RESEARCH DIRECTIONS

More research is needed regarding MOOCs and quality of development, MOOCS and STEM needs, as software licensing. The data shows that the instructional quality of MOOCs varies. With this said instructional principals must be revisited to determine a best practice. Data needs to define the top principles of learning for MOOCS, and the specific types of learning environments. Some data exist about MOOCs in STEM education; however, more is needed. A key point of focus will be having the appropriate mix of academic information to learning exercises (e.g., videos, assignments, and activities). The key point is to make learning stick. Finally, when determining the type of MOOC course to develop, the development team must have a better understanding of the type of licenses required for MOOCs. It is important to know that key obstacle in terms of licenses are proprietary software licenses, as well as software that operates on a distinct hardware configuration. The associated software licensing permits the applications to be used freely in MOOCs for enhancing the overall experience

MOOCS encompass a host of different types of courses. These types of courses allow for global delivery. Delivery approached will continue to vary; however, will need to be studied and concentrated as to the needs of different student populations. Technology is important; thus, due to ubiquitous technological advancement, software licensing will have to be consistently reviewed. MOOCs can prove useful as a new phenomenon of course delivery for students, faculty, and administrators to use. To effectively do this one must maximize the technical use OSS, open source technologies, and open access literature while minimizing the overall associated license costs. The use of virtual words with MOOCs would provide students an environment that allows student to be fully immersed in required technology labs (Calongne, 2008).

REFERENCES

Bessette, D., & Burton, S. (2013). The Involvement of Professional and Managerial Practices and principles for Online Learners in Virtual Programs. In R. McBride & M. Searson (Eds.), *Proceedings of Society for Information Technology & Teacher Education International Conference 2013* (pp. 3040-3045). Chesapeake, VA: AACE.

Burd, E., Smith, S., & Reisman, S. (2015). Exploring Business Models for MOOCs in Higher Education. *Innovative Higher Education*, *40*(1), 37–49. doi:10.1007/s10755-014-9297-0

Burton, S. L. (2016). *Transitioning to I can from I can't*. Raleigh, NC: Lulu Publications.

Calongne, C. M. (2008). Educational Frontiers: Learning in a Virtual World. *EDUCAUSE Review*, *43*(5), 36.

Caulfield, M., Collier, A., & Halawa, S. (2013). Rethinking online community in MOOCS used for blended learning. *Educause Review Online*. Retrieved from http://www.educause.edu/ero/article/rethinking-online-community-moocs-used-blended-learning

Chang, C. C. (2006). Business models for open access journals publishing. *Online Information Review*, *30*(6), 699–713. doi:10.1108/14684520610716171

Christensen, C. (1997). *The innovator's dilemma*. Boston, MA: Harvard Business School.

Davis, L., Dawson, M., & Omar, M. (2016). Systems Engineering Concepts with Aid of Virtual Worlds and Open Source Software: Using Technology to Develop Learning Objects and Simulation Environments. In F. Neto, R. de Souza, & A. Gomes (Eds.), *Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning* (pp. 483–509). Hershey, PA: Information Science Reference; doi:10.4018/978-1-5225-0125-1.ch020

Dawson, M., Al Saeed, I., Wright, J., & Onyegbula, F. (2014). Open Source Software to Enhance the STEM Learning Environment. In V. Wang (Ed.), *Handbook of Research on Education and Technology in a Changing Society* (pp. 569–580). Hershey, PA: Information Science Reference; doi:10.4018/978-1-4666-6046-5.ch042

Dawson, M., Leonard, B., & Rahim, E. (2015). Advances in Technology Project Management: Review of Open Source Software Integration. In M. Wadhwa & A. Harper (Eds.), *Technology, Innovation, and Enterprise Transformation* (pp. 313–324). Hershey, PA: Business Science Reference; doi:10.4018/978-1-4666-6473-9.ch016

Dawson, M. E., & Al Saeed, I. (2012). Use of Open Source Software and Virtualization in Academia to Enhance Higher Education Everywhere. *Cutting-edge Technologies in Higher Education*, *6*, 283–313. doi:10.1108/S2044-9968(2012)000006C013

Decker, G. L. (2014). MOOCology 1.0. In S. D. Krause & C. Lowe (Eds.), Invasion of the MOOCs: The promise and perils of Massive Open Online Courses (pp. 122-129). Anderson, SC: Parlor Press.

Demirci, N. (2014). What is Massive Open Online Courses (MOOCs) and What is promising us for learning?: A Review-evaluative Article about MOOCs. (English). *Necatibey Faculty Of Education Electronic Journal Of Science & Mathematics Education*, *8*(1), 231–256. doi:10.12973/nefmed.2014.8.1.a10

Flynn, J. T. (2013). MOOCS: Disruptive Innovation and the Future of Higher Education. *Christian Education Journal*, *10*(1), 149–162. doi:10.1145/2240236.2240246

Fox, A. (2013). From MOOCs to SPOCs. *Communications of the ACM*, *56*(12), 38–40. doi:10.1145/2535918

Greenbaum, E. (2013). Lisping Copyleft: A Close Reading of the Lisp LGPL. *International Free and Open Source Software Law Review*, *5*(1), 15–30. doi:10.5033/ifosslr.v5i1.75

Guzdial, M., & Adams, J. C. (2014). MOOCs need more work; So do CS Graduates. *Communications of the ACM*, *57*(1), 18–19. doi:10.1145/2555813

Harnad, S., & Brody, T. (2004). Comparing the Impact of Open Access (OA) vs. Non-OA Articles in the Same Journals. *D-Lib Magazine*, *10*(6).

Knowles, M. (1979). Malcom Knowles on...'How I coped with fads in training'. *Training and Development Journal*, *33*(9), 36. PMID:10240407

Kolowich, S. (2013a). Why some colleges are saying no to MOOC deals, at least for now. *The Chronicles of Higher Education.* Retrieved from http://chronicle.com.proxy.cecybrary.com/article/Why-Some-Colleges-Are-Saying/138863

Kolowich, S. (2013b). *MIT will offer MOOC curricula, noy just single course,on edX*. Retrieved from http://chronicle.com/blogs/wiredcampus/mit-will-offer-mooc-curricula-not-just-single-courses-on-edx/46715

Kolowich, S. (2013c). Duke U.'s undergraduate faculty derails plan for online courses for credit. *The Chronicles of Higher Education*. Retrieved from http://chronicle.com.proxy.cecybrary.com/article/Duke-Us-Undergraduate/138895

Koutropoulos, A., Gallagher, M., Abajian, S. C., de Waard, I., Hogue, R., Keskin, N., & Rodriguez, C. (2012). Emotive vocabulary in MOOCs: Context & participant retention. *European Journal of Open, Distance*. *E-learning*, *1*. Retrieved from http://www.eric.ed.gov/PDFS/EJ979609.pdf

Krause, S. D. (2014). MOOC Assigned. In S. D. Krause & C. Lowe (Eds.), Invasion of the MOOCs: The promise and perils of Massive OPen Online Courses (pp. 122-129). Anderson, SC: Parlor Press.

Kumar, S. (2006). Enforcing the Gnu GPL. *U. Ill. JL Tech. & Pol'y*, 1.

Leonard, D., Barton, G., & Barton, M. (2013). Make yourself an expert. *Harvard Business Review*, *91*(4), 127–132. PMID:23593772

Marrapodi, J., Shimkus, D., & Onisk, M. (2016, September). Do's and don'ts for MOOCS and SPOOCS. *Training (New York, N.Y.)*, *53*(5), 20–27.

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research? a review of qualitative interviews in is research. *Journal of Computer Information Systems*, *54*(1), 11–22. doi:10.1080/08874417.2013.11645667

Martin, F. G. (2012). Education wills massive open online courses change how we teach? *Communications of the ACM*, *55*(8), 26–28. doi:10.1145/2240236.2240246

McAuley, A., Stewart, B., Siemens, G., & Cormier, D. (2010). *The MOOC model for digital practice*. Academic Press.

Mosley, A. L. (2007). *An evaluation study of a training program to prepare community college faculty for online teaching* (Doctoral Dissertation). Retrieved from ProQuest Dissertations and Theses database (PQDT). (UMI Number: 3262899)

Neto, F. M., de Souza, R., & Gomes, A. S. (2016). *Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning*. Hershey, PA: IGI Global; doi:10.4018/978-1-5225-0125-1

Ngambi, D., & Bozalek, V. (2015). Editorial: Massive open online courses (MOOCs): Disrupting teaching and learning practices in higher education. *British Journal of Educational Technology*, *46*(3), 451–454. doi:10.1111/bjet.12281

Nicholas, D., Huntington, P., & Jamali, H. R. (2007). Open access in context: A user study. *The Journal of Documentation*, *63*(6), 853–878. doi:10.1108/00220410710836394

Pappano, L. (2012, November 2). The year of the MOOC. *The New York Times.* Retrieved from http://www.nytimes.com/2012/11/04/education/edlife/massive-open-online-courses-are-multiplying-at-a-rapid-pace.html

Pence, H. E. (2012). When will college truly leave the building: If MOOCs are the answer, what is the question? *Journal of Educational Technology Systems*, *41*(1), 25–33. doi:10.2190/ET.41.1.c

Perens, B. (1999). *The open source definition. Open Sources: Voices from the Open Source Revolution*. Academic Press.

Rahim, E., & Burrell, D. N. (2013). *The value of an MBA in a post-recession world*. Colorado Technical University. Retrieved from http://www.coloradotech.edu/resources/blogs/december-2013/the-value-of-an-mba-in-a-post-recession-world?form=degreetype

Rees, J. (2014). The MOOC racket. *Future Tense*. Retrieved fromhttp://www.slate.com/articles/technology/future_tense/2013/07/moocs_could_be_disastrous_for_students_and_professors.html

Rodriguez, C. (2012). MOOCs and the AI-Stanford like courses: Two successful and distinct course formats for massive open online courses. *European Journal of Open, Distance And E-Learning*. Retrieved from http://www.eric.ed.gov/PDFS/EJ982976.pdf

Rosen, L. (2005). *Open source licensing* (Vol. 692). Prentice Hall.

Severns, M. (2014). *Math teacher's parody prompts project to critique Khan's Academy lessons*. Retrieved from http://www.slate.com/blogs/future_tense/2012/06/26/khan_academy_mystery_science_theater_300_parody_by_math_teachers_video_.html

Siemens, G. (2013). *2013 in MOOC s- Which event best defined the quest to solve education?* Retrieved from https://allmoocs.wordpress.com/tag/george-siemens/

Suber, P. (2004). *What is open access? An overview.* ALPSP-SSP Meeting, Washington, DC.

Ta'eed, C. (2012, September 15). Will the Internet replace traditional education? *The Next Web*. Retrieved from http://thenextweb.com/insider/2012/09/15/will-internet-replace-traditional-education

Tareef, A. (2013). The relationship between mentoring and career development of higher education faculty members. *College Student Journal*, *47*(4), 703–710.

Taylor, B., & Kroth, M. (2009). Andragogy's transition into the future: Meta-analysis of andragogy and its search for a measurable instrument. *Journal of Adult Education*, *38*, 1–11.

Thrift, N. (2013). To MOOC or not to MOOC. *The Chronicles of Higher Education*. Retrieved from http://chronicle.com.proxy.cecybrary.com/blogs/worldwise/to-mooc-or-not-to-mooc/31721

Yong, C. (2014). Investigating MOOCs through blog mining. *International Review of Research in Open and Distance Learning*, *15*(2), 85–106.

KEY TERMS AND DEFINITIONS

GNU Public License: A widely used free software license that is managed under the GNU Not Linux Project (Stallman, 1991).

Linux: An open source version of the UNIX OS (Perens, 1999).

MOOC: An online course with the option of free and open registration, publicly shared curriculum, and open ended outcomes (McAuley, Stewart, Siemens, & Cormier, 2010).

Open Source Software: Software that allows the original source code to be free available which may be freely redistributed or modified (Perens, 1999).

Software License: Legal instrument for governing the use or redistribution of software (Dawson, Leonard, & Rahim, 2015).

International Journal of Hyperconnectivity and the Internet of Things
Volume 1 • Issue 1 • January-June 2017

Tails Linux Operating System:
Remaining Anonymous with the Assistance of an Incognito System in Times of High Surveillance

Maurice Dawson, University of Missouri-St. Louis, St. Louis, MO, USA
Jose Antonio Cárdenas-Haro, California State University, Bakersfield, CA, USA

ABSTRACT

After the information released by Edward Snowden, the world realized about the security risks of high surveillance from governments to citizens or among governments, and how it can affect the freedom, democracy, and peace. And organizations such as WikiLeaks has shown just how much data is collected to include the poor security controls in place to protect that information. Research has been carried out for the creation of the necessary tools for the countermeasures to all these surveillance. One of the most potent tools is the Tails system as a complement of The Onion Router (TOR). Even though there are limitations and flaws, the progress has been significant, and we are moving in the right direction. As more individuals and organizations fall under a watchful eye on their Internet activities then maintaining anonymity it not only essential for getting out information but one's safety.

KEYWORDS

Anonymity, Cyber Security, Intelligence, Linux, Tails Linux Operating Systems, TOR

INTRODUCTION

The erosion of privacy in the Web has created a movement from the free software advocates, in the search and development of free and proper tools for everybody. The TOR project is the core of this movement, followed by other many tools which are part of The Amnesic Incognito Live System (Tails). In this document is analyzed the importance of Tails and all its tools in the fight for privacy, freedom, and democracy.

THE BIRTH OF PUBLIC TOR

TOR project was set by the government and developed by the Defense Advanced Research Projects Agency (DARPA) as a security measure to avoid national and international surveillance of the classified government operations (Fagoyinbo & Babatunde, 2013). The Onion Routing principle is the use of several layers of encryption to conceal a user's location and ensure private and anonymous

DOI: 10.4018/IJHIoT.2017010104

communications. Every router in this network only knows the address of the previous router and the address of the following one (Reed, Sylverson & Goldschlag, 1998).

Later the TOR project was released as a free software, and the development continues with funding from diverse sources (Tor: Sponsors, 2010); and these give more confidence to the public about its independence and reliability. So the use of this secure network soon became very popular in all the world propitiating its grow in many users and routers as well. The development of this project is continuous and dynamic; we are now in the second generation of TOR (Dingledine, Mathewson & Syverson, 2011).

This network was made available as a protection of the individuals' privacy (which is a constitutional right in most countries), and to promote and maintain the freedom of confidential communications through the Internet among the public, avoiding or, at least, making very hard the monitoring of them. TOR is an excellent tool not only for the hide of political activists but also for domestic violence survivors to escape abusers (Russell, 2014), or just for regular users to bypass censorship (Gurnow, 2014).

The National Security Agency (NSA) has said that TOR is "the King of high secure, low latency Internet anonymity" (The Guardian, 2013). The TOR project received an award for projects of social benefit from the FSF (Free Software Foundation) in 2010, acknowledging it not only for the privacy and anonymity that it provides, but also for the freedom of access and expression on the Internet granted to millions of people, which has proved to be pivotal in dissident movements around the world (FSF, 2010). The Business Week magazine has described it as one of the most effective means to defeat surveillance around the world (Lawrence, 2014).

HOW IT WORKS

The more people using TOR network, the better. It is easier for a person to be anonymous among many others, it is harder to keep track of someone in a busy unknown and highly tangled network that is frequently changing and mixing up the connections randomly (Edman, Sivrikaya & Yener, 2007). As an analogy, we can say that a chameleon to camouflage effectively needs leaves, branches and trees, the more, the better for the blend. In defeating surveillance, we need to take care of several aspects. Who we talk to and when is just as important as what we said, and to secure these we also need encryption and randomness in the routing as well. The messages from the different anonymous users are shuffled and then sent to the next randomly selected router, shuffled again and so forth until the final destination is reached. So as an observer it is very hard to know which data were coming into the TOR network corresponds to which data coming out of it.

All the data is encrypted, including the origin and destination IP addresses, every time before it is sent to the next relay of the anonymous circuit. Since the TOR is a dynamic network that is constantly evolving, the path that our packets take to change all the time making things harder for the observer (Dingledine, Serjantov & Syverson, 2006). The users can set up a browser, a relay, a hidden service or all of them. Also "bridge relays" can be used to circumvent any blocking to the TOR network.

THE NECESSITY OF ANONYMITY AND CYBER SECURITY

We all need privacy for many diverse reasons, and is not only about the individuals, but also the private companies and even the governmental entities in the world need some anonymity at different levels. Journalists who want to protect their sources, or the law enforcement agencies that require communication with their infiltrated personnel in criminal groups protecting their identity, or the human rights activists in oppressive regimes, or the private companies in avoiding the disclosure of their technological developments for economic reasons, or the governments saving a lot of information for national security.

Surveillance and Espionage have always being an issue; several countermeasures have been developed according to the times, but now is harder than ever. The cell phones can easily be converted into tracking devices and recordings of the phone calls, web pages visited, Internet search history and interactions in social media can create a detailed profile of anyone. The persons can be affected negatively by all these. They could suffer work discrimination because of their political views, or even their physical integrity could be in danger for those who are living in tyrannic regimes, like the recent case of Niloy Neel a Bangladeshi blogger killed in Dhaka (BBC, 2015). The governments are always looking for ways to have more control and capabilities for surveillance; Linus Torvalds, the creator of the Linux Operating System (OS) and still in control of the development of the Linux kernel, revealed that the NSA asked him to put a backdoor in the OS (Greenwald, 2014).

Furthermore, there is the high risk of a democracy degrading into an authoritarian state if its citizens are surveilled to the degree of losing their privacy. The government can face significant economic risks if sensitive information is leaked, as in the case of the tax accounts hacked in the IRS (Weise, 2015). The use of technology is increasing and spreading quickly in most of the devices used by humans, which represents a new security threat if the owners lose the control of them, as in the case of the car hacked when in the middle of the road (Ward, 2015). For all these and more, the governments and the citizens are always looking for ways to avoid the intrusion in their data and systems.

BIRTH OF TAILS OPERATING SYSTEM

The first version of the operating system The Amnesic Incognito Live System (Tails) was released in mid-2009 as a merge of the Incognito and Amnesia Linux distributions. It was created by a team of anonymous hackers which still are in charge of its development, with support and funding from the TOR project and the Freedom of Press Foundation (FPF) (Finances of Tails., 2015), and also from the Debian and Mozilla projects (Tails report, 2014), and other sources that continue founding it. The Tails project is based on the Debian distribution with the security and anonymity as a core philosophy to give privacy to anyone anywhere. Tails were born as a complement of TOR to enhance the anonymization of their users. The Tails Linux distribution became so famous after being known that is the OS used by Edward Snowden, the whistleblower who leaked information about the PRISM project to The Guardian and The Washington Post newspapers (Finley, 2014). The Tails team created this Linux distribution as a countermeasure of erosion of online privacy. The big companies of the Internet, as well as the governments (especially in totalitarian regimes), want to take away our privacy making our lives more transparent every time.

THE STRENGTHS

The Tails OS is an integrated system consisting of several tools aimed to avoid the detection of the identity of their users. It is designed to boot from a removable live media as a Universal Serial Bus (USB) stick or a Digital Video Disk (DVD), and the saving of any file in it is deleted after a reboot for security reasons; of course, we can use the hard drive or another USB memory for the saving of the required data. In the case when we really want to delete any document, videos, pictures or any data file, the Tails is equipped with a tool called “Nautilus Wipe” for securely deleting the data; this is necessary since regular operating systems only remove the file name and link from the file system directory, not even the reformatting or overwriting of the hard drive or memory stick is a guarantee that the deleted or previous information is indeed gone. Tails come with visual camouflage that can be activated to give the look and feel of a Microsoft Windows 8 system, the purpose of this is to avoid attracting unwanted attention when working in public places.

All the traffic is handled through the TOR network, using Media Access Control (MAC) spoofing; all these to avoid leaving any digital footprint. It also gives the option to use Invisible Internet Project (I2P) as an alternative to TOR. The I2P is an anonymous overlay network used as an instrument to

circumvent surveillance and censorship. This Linux distribution includes several state-of-the-art cryptographic tools to encrypt files, emails and instant messaging. It uses LUKS Linux Unified Key Setup (LUKS) which is an encryption tool for hard drives or USB sticks. All the communications with websites are encrypted automatically using Hypertext Transfer Protocol Secure (HTTPS). In the case of documents and emails, are encoded using Open Pretty Good Privacy (OpenPGP). The chatting or instant messaging is done using Off-the-Record (OTRP messaging which is another tool for encryption which also provides deniable authentication that cannot be achieved with PGP systems (Borisov, Goldberg & Brewer, 2004). It includes the "Shamir's Secret Sharing" program which runs an algorithm used in cryptography where the decryption of a message is only possible with some threshold number of participants (Shamir, 1979).

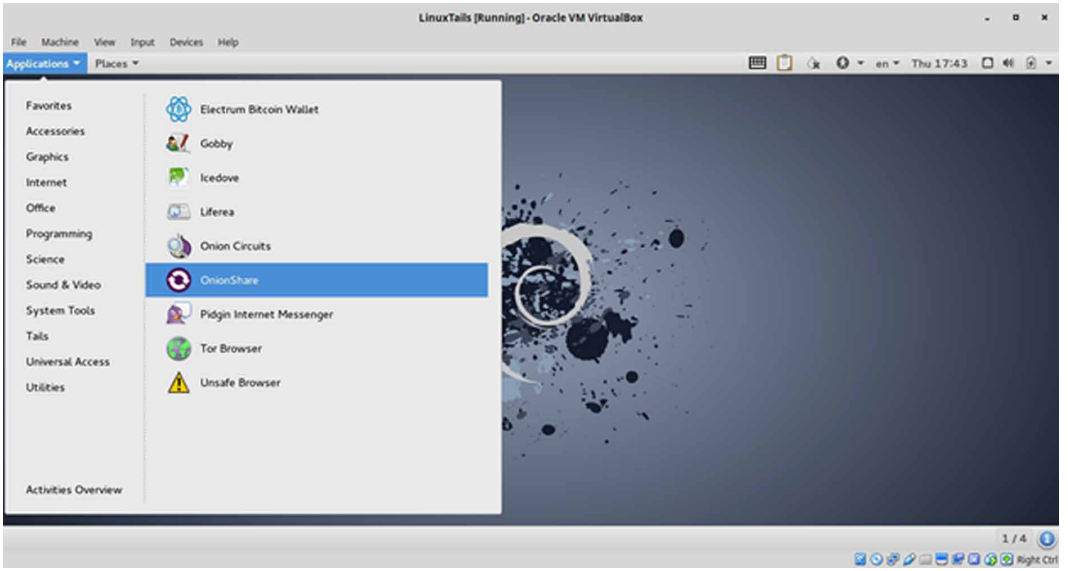
Tails also come with software to create virtual keyboard as a countermeasure against hardware keyloggers, and even with tools to anonymize metadata in files, to calculate checksums. It includes the "AppArmor" system which is a Linux kernel enhancement to confine programs to a limited set of resources. To prevent the "cold boot" attacks and forensics to the Random Access Memory (RAM), it deletes all the memory at the shutdown.

The updates to patch any security hole are available in a prompt manner as an automatic mechanism to upgrade the USB stick or the Secure Digital (SD) card to the most recent version of Tails. The creators of Tails and TOR support and promote the search for flaws in the system as a way to keep it in a continuous improvement state. This incredible operating has been created using only free software, which is a must in these cases since closed private software cannot be trustable. It is not a coincidence that Tails is the preferred operating system by Edward Snowden (Finley, 2014).

APPLICATIONS FOR ANONYMITY

Tails has many software included for networking, encryption, and privacy. This OS can be run as a Virtual Machine (VM), LiveUSB drive, or directly installed on the native machine. There are no associated costs with Tails which is great as this is yet another level of protection ensuring there is no financial footprint associated with the use of this OS. Tails has an application that allows for the creation and management of encryption keys for emails. Figure 1 displays the Tails OS running in a

Figure 1. Tails Desktop in Oracle VirtualBox



virtual environment. The use of encrypted storage devices, key signing, strong password generation, removing identifying metadata in files, and more add to the over security. The removable of the metadata is important because Open Source Intelligence (OSINT) can be done which can provide data such as geolocation, time stamps, and more. Further, text can be used to create a behavioral analysis profile on subjects. A software application such as Maltego can scrap the web for any digital footprint to create a link analyses from tweets, email messages, and more.

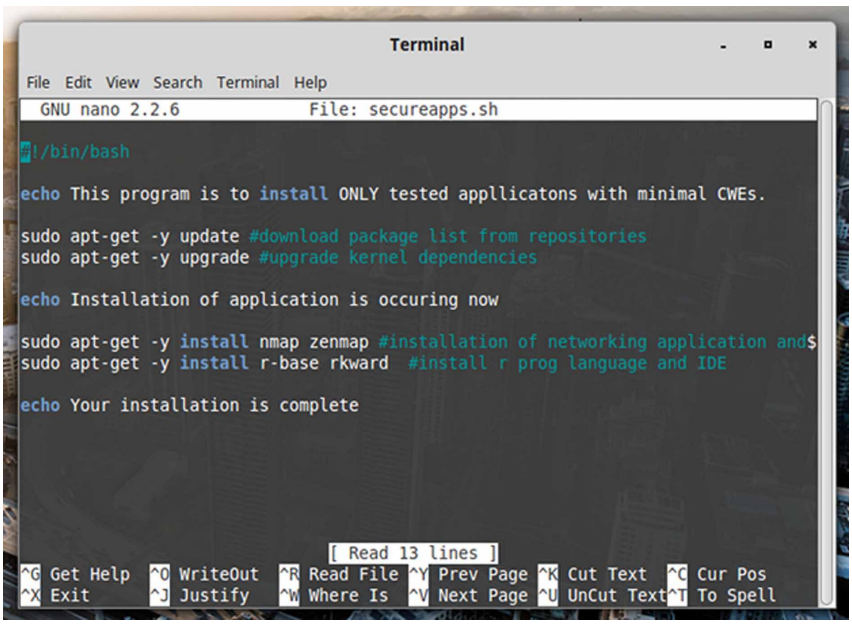
Since this OS is Debian based all software packages available for Debian can be installed in Tails. However, this would be cautioned unless a source code scan in conducted to see what Common Weakness Enumerations (CWEs) are in the system of origin. Once these CWEs have been addressed to an acceptable level, then that particular software application can be installed. Additional packages can break the security of this OS. Thus to do this would require the creation of a secured installation script. In Figure 2, an example is shown that could be written to provide those needing additional application the ability only to run already whitelisted program that does not affect the security posture of Tails.

Bitcoin is a peer to peer electronic cash system that no one controls, and there are not printed currency (Nakamoto, 2008). In Tails included, is Electrum which is a Bitcoin wallet. This application is a lightweight wallet that connects to external user's to query blockchain data. Bitcoin allows the exchange of goods or services with some level of anonymity. In turbulent economies where currency continuously falls this currency could be the method used to ensure organizations are not being financial undermined by nefarious entities (Osterrider, Strika, & Lorenz, 2017).

LIMITATIONS AND FLOWS

As is the case with everything, the Tails system has its limitations. This system is the conjunction of many tools, any flaw in any of its tools becomes a flaw for the Tails system. Furthermore, working effectively under this system requires some technical knowledge, most of the tools in Tails are not precisely user-friendly. It is known that the NSA has been able to crack the computers of some TOR users, but not the core security of the TOR network (Ball, Schneier & Greenwald, 2013); this has to

Figure 2. Sample Installation Script



do more with errors or carelessness from the users. Tails were created as a complement to the TOR browser, as an integrated system for the improvement of the security and anonymity.

TOR encrypts all inside its network and anonymizes the origin of the traffic, but the communications from the TOR network and the final destinations are like the regular transferring of information on the Internet. So, depending on your data, you might need to use some of the tools provided in Tails for further encryption and authentication. Also, we need to change some of our habits, it is not recommended to enable or install browser plugins, neither to open any document downloaded through TOR while online. The Tails does not protect against compromised pieces of hardware, like a key logger unless you use for this specific case a virtual keyboard "Florence" provided in one of its tools. The Basic Input/Output System (BIOS) or firmware attacks are other forms of compromised hardware.

Another important factor that needs close attention is the metadata in our files. Tails does not clear it for us, but it provides the tools necessary for the removal of information that can help to identify us from the metadata, before sending any of the files. In the case of e-mails even if we encrypt the contents, the subject and other headers remain understandable. Another problem in the case of TOR is that it does not protect us from a global adversary, this means an entity monitoring all or most of the nodes in the TOR network, such entity using statistical data may infer the relations between the users and the connections (Dingledine, Mathewson & Syverson. 2004). Another important habit here is the use of a strong password, and the Tails will not create strong passwords for you. It is not straightforward to hide the fact that you are using Tails, and this in some ways is a disadvantage, a flaw in the anonymity. Users have to be ready to update the Tails system every time that there is a patch available.

QUESTIONABLE GOVERNMENTS

Some governments have suppressed the ability to freely communicate and present non-biased news to the public that may not be to the current party holding power. Some countries have been found using FinFisher's FinSpy application which intercepts and records a variety of information (Dawson, 2015). This software application has been found within the hands of over twenty governments that have questionable records on human rights (Pelroth, 2013). The FinSpy software was used in Ethiopia to target political dissidents. In Morocco, there have been reports of the government using the Internet to monitor its citizens. In Tunisia Internet censorship and control has been in place since it was publicly available in 1996 (Wagnner, 2012). These activities have repeated in authoritarian and corrupt governments.

TOOL FOR FREEDOM AND DEMOCRACY

As humans, we have the natural right to privacy and in all the democracies that right is granted in the constitutions. Unapproved or unreasonable searches and seizures go against the human rights. The exchange of information between individuals, corporations or governmental agencies has to be encrypted. It is evident that would be easier for the cops and law enforcement agencies to detect illegal activities if the information were not encrypted, but in the same way it would be easier for the criminals to affect the citizens.

The open source philosophy is a great medium to provide trustable tools to build all the infrastructure that we need to keep the freedom and democracy not only on the Internet but also in our lives. The open source has given birth to the Linux operating system, encryption tools, Wikipedia, Wikileaks, Bitcoin, BitTorrent, social media and many more valuable programs. The General Public License (GPL) is a free software license to guarantee anybody the right and freedom to use, modify and share the programs (Dawson, Leonard, & Rahim, 2015). All these show how humans around the globe can be organized without borders to improve their economies, to build the required products

without the need of the private companies or centralized governments with all the toxic and corrupted control that they represent. In other words, out of the master and slave model, or without "baby sitters".

The mistrust of a central authority is common anywhere, as humans, we have the innate desire for freedom in everything. It is important to clarify that while some media and governments have slandered and libeled the DarkNet, the TOR, and the Tail Linux OS saying that these are evil tools used by criminals; all these are also essential tools used by many people for the good, including dissidents, journalists and law enforcement agencies around the world.

There is always the risk of cyber espionage or mass surveillance done by governments around the globe. In the case of US is with the project PRISM developed by the NSA (Ball, 2013). The UK has the project Tempora (Bump, 2013). In Russia is the SORM project (Paganini, 2014) and China has two significant tools for the control of the Internet, the Golden Shield (or Great Firewall) for censorship and surveillance (Randy, 2009); and the Green Dam for Personal Computer (PC) content control (Watts, 2009; Chen, 2009). There are also companies that sell technology for surveillance even to oppressive regimes (Gilbert, 2015), so we can say that all or, at least, most of the states around the world do some kind surveillance that could go worst as the technology improves and evolves. The monitoring between nations can cause tensions and damage in the diplomatic relations or even the loss of them (Smith, 2014; Menn, 2015; Fitsanakis, 2013).

Furthermore, the surveillance does not come only from the states. The private companies also want your data for economic purposes. They want to know what are you more likely to consume, to buy, and this way you could become the target of some specific advertising. Companies like Microsoft, Apple, Facebook, Yahoo, Google or Amazon among others are collecting their user's data is also for psychological manipulation to make you consume some products that other way you might not buy. They need all the possible information from you to link it with your real life behavior, and these give them some control over you. Your cell phone location, who you share information with, who you talk to, what you buy, etc. The companies usually have arrangements with the government to share this information or they might also be under government surveillance for these data (Branstetter, 2015; Greenwald, MacAskill, Poitras, Ackerman, & Rusche, 2013; Bekker, 2013). The problem is that the more you are surveilled, the less autonomous and free you are. It is not easy to know the level and kind of control that they could exercise over us, but our freewill is indeed affected.

People are saying that they do not care about surveillance because they do not have anything to hide pure ignorance, it is like saying that they do not care about free speech because they do not have anything to say. Thanks to free thinkers and researchers, there are tools, services, protocols and free software available and under continuous development and improvement to avoid surveillance, for an anonymous and private exchange of information; science and technology is fighting back. All these come down to live a free life which is a core human value, and a foundation for any true democracy.

CONCLUSION

As more people express the desire for privacy, the demand will fuel the market as data found publicly can fall prey to those conducting OSINT mining and analysis for bad reasons. By making the surveillance harder we protect ourselves as individuals, and all the others by making it more expensive to monitoring everyone all the time. At the end encryption and chaos is all about mathematics, and in the quest for more privacy, the numbers work in our favor. It is a lot easier the encryption of the data than the decryption of it for intruders. Our universe fundamentally prefers privacy. In order of having a free society, we need to have freedom from analysis about behaviors and communications among us. When considering issues of privacy, cyber terrorism, and digital crime it Tails allows us to navigate freely, safely, and securely (Dawson & Omar, 2015; Dawson, Omar, & Abramson 2015). In our hyperconnected society, it is imperative that anonymity is maintained during certain actions because of misuse and abuse.

REFERENCES

Ball, J. (2013). NSA's Prism surveillance program: how it works and what it can do. *The Guardian*.

Ball, J., Schneier, B., & Greenwald, G. (2013). NSA and GCHQ target Tor network that protects anonymity of web users. *The Guardian*.

BBC. (2015, August 07). Bangladesh blogger Niloy Neel hacked to death in Dhaka. Retrieved from http://www.bbc.com/news/world-asia-33819032

Bekker, S. (2013, June 20). PRISM and Microsoft: What We Know So Far". Redmond Channel Partner.

Borisov, N., Goldberg, I., & Brewer, E. (2004, October). Off-the-record communication, or, why not to use PGP. *Proceedings of the 2004 ACM workshop on Privacy in the electronic society* (pp. 77-84). ACM. doi:10.1145/1029179.1029200

Branstetter, B. (2015, August 16). The NSA is asking your favorite apps how to spy on you better. Business Insider.

Bump, P. (2013, June 21). The UK Tempora Program Captures Vast Amounts of Data – and Shares with NSA. The Atlantic Wire. Retrieved 23 June 2013.

Chen, W. (2009, June 13). Let people decide on Green Dam. China Daily.

Dawson, M. (2015). A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism. In M. Dawson & M. Omar (Eds.), *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 1–7). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8345-7.ch001

Dawson, M., Leonard, B., & Rahim, E. (2015). Advances in Technology Project Management: Review of Open Source Software Integration. In M. Wadhwa & A. Harper (Eds.), *Technology, Innovation, and Enterprise Transformation* (pp. 313–324). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-6473-9.ch016

Dawson, M., & Omar, M. (2015). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*. Hershey, PA: IGI Global; doi:10.4018/978-1-4666-8345-7

Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the Methods behind Cyber Terrorism. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology* (3rd ed., pp. 1539–1549). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-5888-2.ch147

Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The second-generation onion router*. Naval Research Lab Washington DC.

Dingledine, R., Serjantov, A., & Syverson, P. (2006, June). Blending different latency traffic with alpha-mixing. In *Privacy Enhancing Technologies* (pp. 245–257). Springer Berlin Heidelberg. doi:10.1007/11957454_14

Edman, M., Sivrikaya, F., & Yener, B. (2007, May). *A Combinatorial Approach to Measuring Anonymity*. ISI. doi:10.1109/ISI.2007.379497

Fagoyinbo, J. B. (2013). *The Armed Forces: Instrument of Peace, Strength, Development and Prosperity*. AuthorHouse.

Finances of Tails. (2015). Retrieved from https://tails.boum.org/doc/about/finances/index.en.html

Fitsanakis, J. (2013, June 20). Analysis: PRISM Revelations Harm US Political, Financial Interests. IntelNews.

FSF. (2010). *2010 Free Software Awards announced*. Free Software Foundation.

Gilbert, D, (2015). Hacking Team hacked: Spy tools sold to oppressive regimes Sudan, Bahrain and Kazakhstan. *International Business Times magazine*.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillan.

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., & Rushe, D. (2013). Microsoft handed the NSA access to encrypted messages. *The Guardian*.

Gurnow, M., (2014, July). Seated Between Pablo Escobar and Mahatma Gandhi: The Sticky Ethics of Anonymity Networks. *Dissident Voice*.

James, R. (2009). A brief history of Chinese internet censorship. *Time.*

Lawrence, D. (2014). *The inside story of Tor, the best Internet anonymity tool the government ever built*. Bloomberg Businessweek.

Levine, Y. (2014). Almost everyone involved in developing Tor was (or is) funded by the US government.

Menn, J. (2015). Russian Researchers Expose Breakthrough US Spying Program. *Reuters.*

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Osterrieder, J., Strika, M., & Lorenz, J. (2017). Bitcoin and cryptocurrencies—not for the faint-hearted. *International Finance and Banking*, *4*(1), 56. doi:10.5296/ifb.v4i1.10451

Paganini, P. (2014). *New powers for the Russian surveillance system SORM-2*. Security Affairs. Retrieved.

Perloth, N. (2013). Researchers Find 25 Countries Using Surveillance Software. New York Times. Retrieved from https://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software/

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Anonymous connections and onion routing. *IEEE Journal on* Selected Areas in Communications, *16*(4), 482–494.

Russell, B., (May 2014). Domestic violence survivors turn to Tor to escape abusers. *The Verge*.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612–613. doi:10.1145/359168.359176

Smith, A. (2014, August 2). U.S. Spy Scandal Triggers Outrage, Paranoia in Germany. NBC News.

Tails. (2014, June 14). Tails report for May, 2014. Retrieved from https://tails.boum.org/news/report_2014_05/index.en.html

The Guardian. (2013). Tor: 'The king of high-secure, low-latency anonymity.

Tor Project. (n. d.). Tor: Sponsors.

Wagner, B. (2012). Push-button-autocracy in Tunisia: Analysing the role of Internet infrastructure, institutions and international markets in creating a Tunisian censorship regime. *Telecommunications Policy*, *36*(6), 484–492. doi:10.1016/j.telpol.2012.04.007

Ward, M. (2015, August 06). Warning after security experts hack Tesla car. BBC News. Retrieved from http://www.bbc.com/news/technology-33802344

Watts, J. (2009, June). China orders PC makers to install blocking software. *The Guardian.*

Weise, E. (2015). IRS Hacked, 100,000 Tax Accounts Breached. *USA Today*. Retrieved from http://www.usatoday.com/story/tech/2015/05/26/irs-breach-100000-accounts-get-transcript/27980049/

Maurice Dawson is an Assistant Professor of Information Systems at the College of Business Administration at University of Missouri- St. Louis with affiliation to the Cybersecurity and Information Technology Innovation Lab (CITIL). He is currently a Visiting Professor at the Polytechnic University of Puerto Rico, Visiting Professor at the University of Nairobi, and a Senior Research Fellow at the American Leadership & Policy Foundation (ALPF). Additionally, he was a Visiting Assistant Professor (Honorary) at the University of Tennessee in the College of Engineering within the Department of Industrial and Systems Engineering. Dawson has received a Fulbright Specialist Grant to Russia in 2014 to South Ural State University. Dawson served a Visiting Scholar with the University of The Gambia through the International Studies and Programs (ISP) Fellowship awarded from the University of Missouri Systems (UMS) in 2014. Dawson received an appointment as an International Business (IB) Research Associate in the UMSL International Business Institute (IBI). He is currently completing a second PhD at London Metropolitan University in the Intelligent Systems Research Centre (ISRC).

Jose Antonio Cárdenas-Haro received his PhD in Computer Science from the Arizona State University (ASU), his Master's in Computer Science was granted by the Ensenada Center for Scientific Research and Higher Education (CICESE), and he also he holds a BS in Electronic Engineering from the Technological Institute of Los Mochis (ITLM). His research interests include parallel and distributed computing, algorithms, network security, cyber security, bioinformatics and applied mathematics. Cardenas is currently working in the Computer & Electrical Engineering department at California State University, Bakersfield.

Cyber Security Policies for Hyperconnectivity and Internet of Things: A Process for Managing Connectivity

116

Maurice Dawson

Abstract

Hyperconnectivity and Internet of Things are changing the landscape of Information Technology (IT). Architectures are becoming more sophisticated while cyber security is slowing adapting to this shift of Internet-enabled technologies in automotive, industrial, consumer, and networking. This slow adoption of proper security controls, defenses, and aggressive measures is leaving individuals vulnerable. This submission explores how policies can be created that automate the process of device connectivity, and how current frameworks can be used to minimize system risks.

Keywords

Internet of Things • Hyperconnectivity • Complex Systems • Internet of Everything • Connected Devices • Cyber Security Risk Management

116.1 Introduction

For years cyber security has been a concern of the Department of Defense (DoD) allow them to mature their Certification & Accreditation (C&A) process from the Orange Book to the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) [1]. This has included C&A processes such as Department of Defense Information Technology Certification & Accreditation Process (DITSCAP), Department of Defense Information Assurance Certification & Accreditation Process (DIACAP), Common Criteria, Department of Central Intelligence Directives (DCID), and more. Doing this allowed for the ability to understand how to appropriately apply security controls to systems while learning how to manage risk for complex systems. These cyber security policies are applied to stand-alone systems, enterprise networks, tactical systems, and those entities in a system of systems environment. Even when systems are interconnected, there is a requirement of a certificate of net-worthiness and security testing before continued connection [1]. Data classification and Acquisition Category (ACAT) level drive the need for policy compliance. Through all agencies, this created massive processes for policing the higher levels of government still require an annual auditing known as the Federal Information Security Management Act (FISMA). In the public and private sectors, the cyber security policies are not matured in comparison to the DoD. Thus the problem arises as more companies produce that has Internet-enabled technology without proper cyber security.

116.2 Internet of Things

The Internet of Things (IoT) has spawned a need for seemingly normal devices to have the ability to connect with the Internet. Thus a world is created in which smart technologies enable objects with a network to communicate with each other and interface with human effortlessly [2]. This connected world of convenience and technology does not come without its drawbacks, as interconnectivity implies hackability [3–4]. IoT is found in the automotive, consumer, industrial, and general

M. Dawson (✉)
University of Missouri-St. Louis, 1 University Drive, St. Louis, MO 63121, USA
e-mail: Dawsonmau@umsl.edu; http://www.umsl.edu/

S. Latifi (ed.), *Information Technology – New Generations*, Advances in Intelligent Systems and Computing 558, DOI 10.1007/978-3-319-54978-1_116

computing environments. These environments are incredibly diverse with application in traffic monitors to smart energy grids. Looking beyond IoT to Internet of Everything (IoT) there is a potential market that approximately $14.4 trillion and over 99 percent of physical devices are still unconnected [5].

116.3 Managing Risks

Developers of nongovernmental systems should start using policy, guidance, and directives to formulate baselines [1, 6–8]. NIST Speical Publications (SP) could provide an organization the start they need to start addressing these issues. NIST SP is broken into three sub-series to present cyber security, information systems guidelines, recommendations, and reference materials [1]. The SP 800, Computer Security is the primary outlet for publishing cyber security/information systems guidelines, recommendations, and reference materials. The SP 1800, NIST Cyber Security Practice Guides compliments the SP 800 targeting particular cyber challenges in the public and private sectors. The SP 1800 provide practical, user-friendly guides to facilitate the adoption of standard based approaches to security. The SP 500, Computer Systems Technology is a general Information Technology (IT) sub-series used by NIST's Information Technology Laboratory (ITL) [1].

The RMF is a framework created by the RMF to address risk management that public and private sector can use to baseline security controls in products [1] (NIST, 2012). The RMF uses the risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders (EO), policies, standards, or regulations. There are six RMF categorization steps that serves as the basis for this NIST guidance [1]. Step 1: Categorize is categorize which the system is assessed and categorized based on an impact analysis. Step 2: Select is chosen which during this period the systems is given a baseline set of security controls that are to be addressed in the design. Step 3: Implement is applied, and during this stage, the controls selected in Step 2 are deployed within the system to included the associated environment of operation. Step 4: Assess is when the controls implemented are assessed to see if they are working as intended and that the desired outcome meets the security requirements for the system. Step 5: Authorize is to get authority for the system to operate based back an acceptable decision upon the acceptable risk for the system. Step 6: Monitor is to continually assess the security control of the system on an ongoing basis. This can include annual security checks to review compliance. This process can not only be implemented but used as a way to measure compliance with federal standards that end up as a performance measurement in the annual FISMA reports.

RMF provides organizations developing Internet-enabled technologies and those that are connected to begin addressing risks associated with their products. Creating a process that allows for updating application software, and system configurations while undergoing an annual compliance helps create a more security hardened product [9–12]. In Fig. 116.1 a process is described that allows devices to be tested according to current standards.

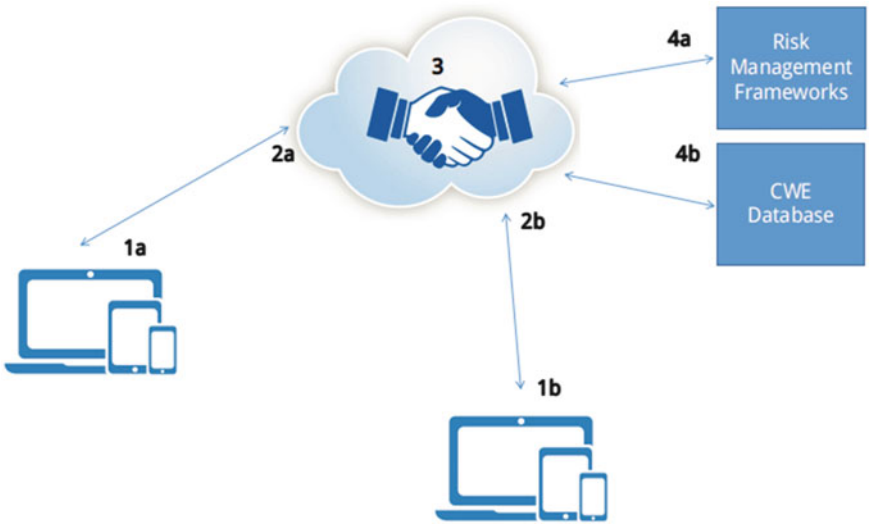


Fig. 116.1 Security testing process for connected devices

116.4 Hyperconnectivity

The term hyperconnectivity was invented by two Canadian social scientists that discuss the social constructs relating to this term [3–4, 13]. However, other found definitions define this as a to connect oneself to difference information and social stream with a deft facility. Thus IoT, big data, and social media blend allowing vast amounts of information to be shared publicly. As the IoT devices lack the essential security to combat advanced cyber attacks these devices become an unsecured gateway into the system.

Many mobile devices allow for the use of applications to integrate cloud-based applications on the instrument. This coupled with the use of default settings, lack of Anti-Virus (AV) software, and other items that do not allow for defense in depth concept. For example, the default settings on a mobile device may have the Global Positioning System (GPS) enabled. This GPS setting is enabled when needed to use for navigation. If this setting is not changed then when an individual takes photos the latitude and longitude coordinates are created in the Exchangeable Image Format (EXIF) data for the file. This could allow for pattern analysis and know the type of device that took the photo. Knowing the kind of device allows the attacker to research vulnerabilities and exploits specifically targeting that platform. With some open source tools, Open Source Intelligence (OSINT) can be performed that provides data such as behavior analysis, text mining, location analysis, and exploitation of connections [14–15].

Policies be implemented that address the system and components of that system. Once dealing with the system then policies need to be created for the connecting system. As organizations seek to implement Bring Your Device (BYOD), there needs to be a system that addresses the security configuration and a script that runs on the instrument each time to check policy compliance before allowing a connection. However, for household devices, this will be much more complex as there is no central organization responsible for cyber security policy. Devices will need to be outfitted with an automated test before allowing paring or connectivity through a software application.

116.5 Testing

Testing is integral to the software and systems lifecycle for development. However, there is guidance from NIST in the SP 800–15, but there is not truly something that addresses developing tests on commercial devices that provide an analysis that looks at risks [16]. So the need for the development of Built-In Test (BIT) like testing applications that allow users to set their level of acceptable risk In Fig. 116.1, shown is a testing process for multiple devices. In Steps 1a and 1b devices that decide to pair connect to the web in Steps 2a and 2b. During Step 3 is where a handshake is done Steps 4a and 4b the appropriate security measures are selected to allow the secure connection. In Step 4a an appropriate risk management framework is chosen with security controls being applied to the device. Step 4b looks at the CWE database, uses the appropriate tests for the devices depending up applications discovered. Once tests have been satisfied Step 3 performs a handshake that allows devices to connect. Devices have the ability to perform checks as necessary as possible to remain securely attached. For this process to occur a software-based application will be on the devices that allow connectivity to the Internet. The risk management framework and CWE database get updated daily to ensure that the device owner understands the appropriate risk before deciding to connect or pair device ultimately.

116.6 Conclusion

Creating a software-based application is a method that could significantly reduce risks in a hyperconnected environment. Using an application that can apply a selected framework while providing the end user their risk level if connecting to another device after reviewing CWE compliance has the potential to reduce the number of vulnerabilities drastically. However, there has to be a minimum accepted risk for personal users, and an acceptable associated risk for those in various industries. Future research will look into this concept further while maturing this process to enable implementation at an organization and personal use level.

References

1. NIST, S (2004). 800–37. Guide for the security certification and accreditation of federal information systems.
2. Ashton, K. (2009). That 'internet of things' thing. *RFiD Journal, 22* (7), 97–114.
3. Dawson, M., Eltayeb, M., & Omar, M. (2016). *Security solutions for hyperconnectivity and the internet of things* (pp. 1–347). IGI Global: Hershey.
4. Dawson, M. (2016). Exploring secure computing for the internet of things, internet of wverything, web of things, and hyperconnectivity. In M. Dawson, M. Eltayeb, & M. Omar (Eds.), *Security solutions for hyperconnectivity and the internet of things* (pp. 1–12). IGI Global: Hershey.
5. Bojanova, I., Hurlburt, G., & Voas, J. (2013). Today, the Internet of Things. Tomorrow, the Internet of Everything. Beyond that, perhaps, the Internet of Anything—a radically super-connected ecosystem where questions about security, trust, and control assume entirely new dimensions. information-development, 04.

6. Commanders, C., Defense, U. S. O., & Defense, A. S. O. (2003). Subject: DoD information system certification and accreditation reciprocity. System.
7. Diem, J. W., Smith, J. S., & Butler, L. A. (2009). United States Army Operational Test Command (USAOTC) Integrated Technologies Evolving to Meet New Challenges-A Study in Cross Command Collaboration. ARMY OPERATIONAL TEST COMMAND FORT HOOD TX.
8. Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3), 81–85.
9. Tohidi, H. (2011). The Role of Risk Management in IT systems of organizations. *Procedia Computer Science, 3*, 881–887.
10. Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied computing and informatics, 9*(2), 107–118.
11. Wood, C. C. (2008). Information security policies made easy, Version 10. Information Shield, Inc.
12. Whitman, M. E., Mattord, H. J. (2011). Principles of information security. Cengage Learning.
13. Fredette, J., Marom, Revital., Steiner, K., Witters, L. (2012). The promise and peril of hyperconnectivity for organizations and societies. The global information technology report, 113–119.
14. Mercado, S. C. (2009). Sailing the sea of OSINT in the information age. Secret Intelligence: A Reader, 78.
15. Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior, 28*(2), 673–682.
16. Scarfone, K. A., Souppaya, M. P., Cody, A., Orebaugh, A. D. (2008). SP 800–115. Technical guide to information security testing and assessment.

Open Source Intelligence: Performing Data Mining and Link Analysis to Track Terrorist Activities

22

Maurice Dawson, Max Lieble, and Adewale Adeboje

Abstract

The increasing rates of terrorism in Africa is a growing concern globally, and the realization of such dreadful circumstances demonstrates the need to disclose who is behind such terrible acts. Terrorists and extremist organizations have been known to use social media, and other forms of Internet-enabled technologies to spread idealism. Analyzing this data could provide valuable information regarding terrorist activity with the use of Open Source Intelligence (OSINT) tools. This study attempts to review the applications and methods that could be used to expose extremist Internet behavior.

Keywords

Social Network Analysis • Twitter • Terrorism • Extremist • Boko Haram • Al Shabaab • Fulani Militants • OSINT

22.1 Introduction

Africa has been plagued with three of the five most dangerous terrorist organizations. Nigeria is home to the world's most dangerous terrorist organization Boko Haram and the Fulani Militants which is the world's fourth deadliest terror group [1–6]. Somali is home to Al-Shabaab which is the world's fifth deadliest terror organization. Analyzing data captured in the Global Terrorism Database (GTD) from the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START) from the year 1970–2015 approximately 40,422 incidents have been reported in the Middle East and North Africa [3–7]. The GTD does not include a separate regional analysis of North Africa. In Sub-Saharan Africa, the number of the incident for the same period is approximately 13,434 [3–7].

Nigeria is Africa's largest economy surpassing South Africa in recent years. However, this country is home to the infamous 419 Scam in which gained international attention due to the number of individuals this scam has taken financial advantage of globally. Somalia is a failed state where terrorist group Al-Shabaab are launching terror attacks in neighboring Kenya and Ethiopia. Both of these countries are strong economies in East Africa. Ethiopia is the home to the African Union (AU) and many other organizations that have a significant presence in Addis Ababa. Kenya is home to one of Africa's best universities, largest military, and growing digital economy.

22.2 Data Collection Using Open Source Intelligence

Open Source Intelligence (OSINT) is unclassified information or data that is publicly available. OSINT is not to be a substitute for other sources of intelligence but rather complement existing methods to collect information such as

M. Dawson (✉) • M. Lieble
University of Missouri-St. Louis, 1 University Drive, St. Louis, MO 63121, USA
e-mail: Dawsonmau@umsl.edu; http://www.umsl.edu/

A. Adeboje
Colorado Technical University, 4435 N. Chestnut St, Colorado Springs, CO 80907, USA
e-mail: Adewale.Adeboje@my.cs.coloradotech.edu

S. Latifi (ed.), *Information Technology – New Generations*, Advances in Intelligent Systems and Computing 558, DOI 10.1007/978-3-319-54978-1_22

Geospatial Intelligence (GEOINT), Signal Intelligence (SIGINT), Human Intelligence (HUMINT), and Measurement Intelligence (MASINT). This data collection method relies on information that is found publicly without the need to request access to it, and it can be used to generate reports [8]. These reports can be behavioral activities, organization operations, political viewpoints, and relationships by simple Twitter retweets, mentions, or Wikipedia that are further analyzed [9, 10]. Technology has made the idea of spying being done by some secret agency has been replaced by analysts who can perform complex analysis with the aid of computer applications in an open society freely sharing data [11].

Data that was captured in this research study was OSINT and analyzed using various software applications. The Metasploit Community Edition (CE), Python, R, RapidMiner, and KNIME were among the applications used in this study. The data was captured through an anonymous account, and further analysis was conducted using the Tor Browser.

22.3 Open Source Software for Intelligence Analysis

Open Source Software (OSS) can enable the search of nefarious activities to be performed on terrorist groups. Since these applications are freely provided, or part of a penetration testing software such as Maltego users have the ability to use these applications. Programs such as Python, R, RapidMiner, KNIME, and others can be utilized for mining data. These applications allow for intelligence to be collected.

Table 22.1 provides details about a small selection of software applications, their description, and potential use. These applications are all open source which allows any individual or organization use them. Many can be loaded onto lightweight Linux distributions which can operate with minimal computing resources to be effective. This will allow for organizations with a limited budget or legacy systems to run these applications as part of their suite of OSINT tools. However, the Internet is a fundamental component to running these applications as many of these tools crawl the net looking for hashtags, emails, select phases and other digital footprints. The idea behind OSINT is that these items are found freely online through forums, Wikipedia pages, blogs, social media, and more. Thus not having the Internet become an immediate barrier in conducting OSINT on a target.

22.4 Links and Transforms

The research was on the Somalia founded terrorist group Al-Shabaab using the application Maltego which is native in Kali Linux. This was conducted transforms the terrorist entity and labeling it as Al-Shabaab. From there a search was carried out on Twitter accounts that either mentioned the entity or contained tweet about the entity. From there we were able to view specific tweets and retweets that included various elements such as specific key phrases that were deemed to support terrorist activity. From there the tweets were accounts, and tweets were further investigated. The OSINT analysis starts with the terrorist entity Al-Shabaab and from there a transform against Twitter affiliations. From there accounts with tweets to this entity, and-and those that mentioned this entity were captured. From there the social account was mapped to the al_shabaab alias. That alias shows a further connection to a few social media accounts such as an active Instagram account, inactive Bitly link management account, and another. The Instagram account has the profile name al_shabaab with three posts, and under seven followers.

The other entities researched were Boko Haram to include infamous leader Abubakar Shekau. This searched allowed the view of accounts that used his name, and potential sympathizer of the Islamist militant group. A few of the OSINT gathered was followers, tweets, geolocation of tweets, and websites that contained specific phrases. Figure 22.1 shows the analysis conducted on Al-Shabaab and Boko Haram. Figure 22.2 displays the transforms done against the entity Boko Haram, and terrorist leader Shekau. This figure shows news organizations, websites, incoming, and outgoing links to multiple entities.

Table 22.1 Data mining and link analysis applications

Software application	Description & potential use	Source
R language	Language used for statistical computing and graphics.	[12]
Maltego Community Education	Program used to determine the relationships and real world links	[13]
RapidMiner	A program used for all steps of the data mining process including results visualization, validation, and optimization.	[14]
R Studio	IDE for R that allows for the use of R.	[15]
KNIME	Used for enterprise reporting, Business Intelligence (BI), data mining, data analysis, and text mining.	[16]
Python	High level, general purpose programming language.	[17]

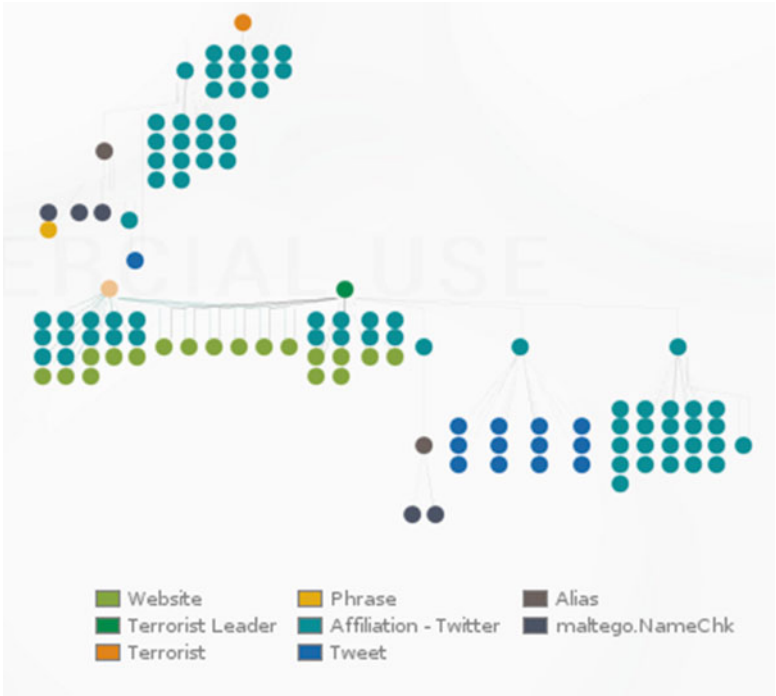


Fig. 22.1 Sub-Saharan African Terrorist Analysis

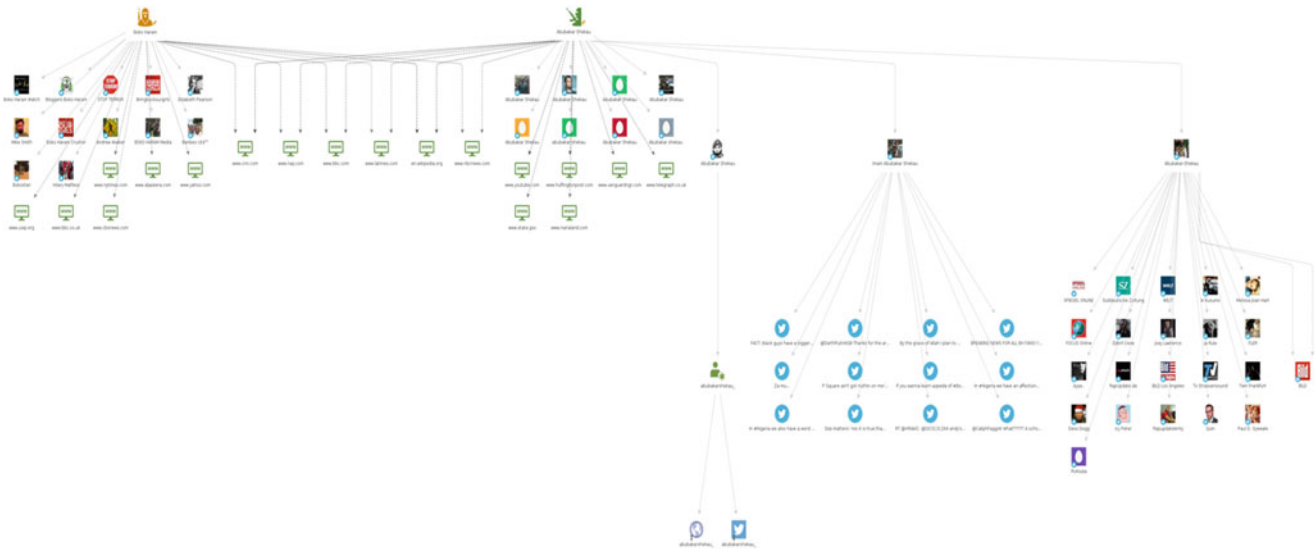


Fig. 22.2 Nigeria–Boko Haram Analysis

22.5 Data Analysis Using R and Python

The R Language is well known for its interactive capabilities as a tool for statistical computing and graphical representation of various statistical procedures. In addition to its analytical capabilities, R is well suited for data mining of all kinds including social network analysis and sentiment analysis. The below image features data collected from Twitter tweets using R. The below information represents details relating to tweets that featured the words "Al-Shabaab," a Somalian militant group. After the relevant tweets were collected, a function that provides all of the usernames of those tweets was utilized as well as a service that provided information about what source was used by those specific users to post those tweets (Fig. 22.3).

Python is a programming language than can be used for various forms of data mining and social media analysis. This tool can be used for sophisticated data analysis as well as simple reports that can be easily understood by a beginning

```
> sapply(tweets, function(x) x$getScreenName())
 [1] "anthonykyal121"  "ferozeahmedboda" "AyahNReza"       "seandw14"        "Joesy642"        "JosamNgoka"      "GeopoliticalJD"  "JohnnieChrome"   "mpendaraha18"
[10] "somali_activist" "alniinawaa4"     "douglaskawuma"   "AbdiAddow1"      "paddymwiine"     "alan_gumisiriza" "LeleiKiplangat"  "ntvuganda"       "john1966olsen"
[19] "PDWilliamsGWU"   "IamRusoke"       "lameck_njeje"    "TerrorFreeSomal" "HambySr"         "younggopp"       "arafrika"
> sapply(tweets, function(x) x$getStatusSource())
 [1] "<a href=\"http://twitter.com/download/android\" rel=\"nofollow\">Twitter for Android</a>"
 [2] "<a href=\"http://twitter.com/download/android\" rel=\"nofollow\">Twitter for Android</a>"
 [3] "<a href=\"http://twitter.com/download/android\" rel=\"nofollow\">Twitter for Android</a>"
 [4] "<a href=\"http://twitter.com\" rel=\"nofollow\">Twitter Web Client</a>"
 [5] "<a href=\"http://twitter.com/download/iphone\" rel=\"nofollow\">Twitter for iPhone</a>"
 [6] "<a href=\"http://twitter.com/download/android\" rel=\"nofollow\">Twitter for Android</a>"
 [7] "<a href=\"http://twitter.com/download/iphone\" rel=\"nofollow\">Twitter for iPhone</a>"
 [8] "<a href=\"http://twitter.com/download/android\" rel=\"nofollow\">Twitter for Android</a>"
 [9] "<a href=\"http://twitter.com/download/iphone\" rel=\"nofollow\">Twitter for iPhone</a>"
[10] "<a href=\"http://twitter.com/download/iphone\" rel=\"nofollow\">Twitter for iPhone</a>"
[11] "<a href=\"http://twitter.com\" rel=\"nofollow\">Twitter Web Client</a>"
[12] "<a href=\"http://twitter.com/download/android\" rel=\"nofollow\">Twitter for Android</a>"
[13] "<a href=\"http://twitter.com/download/iphone\" rel=\"nofollow\">Twitter for iPhone</a>"
[14] "<a href=\"https://mobile.twitter.com\" rel=\"nofollow\">Mobile Web (M2)</a>"
[15] "<a href=\"http://twitter.com/download/android\" rel=\"nofollow\">Twitter for Android</a>"
[16] "<a href=\"http://twitter.com/download/android\" rel=\"nofollow\">Twitter for Android</a>"
[17] "<a href=\"http://snappytv.com\" rel=\"nofollow\">SnappyTV.com</a>"
[18] "<a href=\"http://twitter.com\" rel=\"nofollow\">Twitter Web Client</a>"
[19] "<a href=\"http://twitter.com/#!/download/ipad\" rel=\"nofollow\">Twitter for iPad</a>"
[20] "<a href=\"http://twitter.com/download/android\" rel=\"nofollow\">Twitter for Android</a>"
[21] "<a href=\"http://twitter.com/download/android\" rel=\"nofollow\">Twitter for Android</a>"
[22] "<a href=\"http://twitter.com/download/android\" rel=\"nofollow\">Twitter for Android</a>"
[23] "<a href=\"http://twitter.com\" rel=\"nofollow\">Twitter Web Client</a>"
[24] "<a href=\"http://twitter.com/download/iphone\" rel=\"nofollow\">Twitter for iPhone</a>"
[25] "<a href=\"http://blackberry.com/twitter\" rel=\"nofollow\">Twitter for BlackBerry®</a>"
>
```

Fig. 22.3 Al-Shabaab Tweet Word Search

Fig. 22.4 Python Jihad Word Search Program

File Edit Format Run Options Window Help

```
import tweepy
from tweepy import Stream
from tweepy import OAuthHandler
from tweepy.streaming import StreamListener
ckey = 't0KKZp3EI7CylfmfaTFpe6r1K'
csecret = 'fLXY82VFvHc5NF7CBcSLSjGGhfFiOBDVL7Rqa3zOIu5BrI1UNY'
atoken = '706140478878552064-0kCZWapnnIlXoUcKQ2wxUnjxuwKQVck'
asecret = 'yPqbhl8DWGTBwL6eYh5j0vyuW6RL3tZfAyVqP4njm8CBa'

from tweepy import OAuthHandler
class listener(StreamListener):


        def on_data(self, data):
                print (data)
                return True

def on_error(self, status):
        print (status)


auth = OAuthHandler(ckey, csecret)
auth.set_access_token(atoken, asecret)
twitterStream = Stream(auth, listener())
twitterStream.filter(track=["jihad"])
```

user. The coding for Python is relatively similar to that of R but has it very own, unique forms of capabilities that set itself apart from others. Regarding social media analysis, Python is capable of extracting data from Twitter and other social media platforms. An example of the Twitter streaming function through Python is displayed below (Fig. 22.4).

22.6 Findings

Maltego served as a useful tool for link analysis. The platform allowed for detailed mining of particular forms of data. Graphs can be constructed and serve as a sort of an investigation. Furthermore, this program proved useful for cyber threat analysis of many types and ultimately acts as a tool for OSINT. Figure 22.2 displays at social media analysis through Maltego about the search term of "Boko Haram." The output of this function provided specific Twitter accounts that have held some relation to an entity based on each Twitter accounts name or tweeting patterns. Further analysis was conducted on each of these Twitter accounts by performing a function that generated all of the tweets for each Twitter account. In addition to this, sentiment analysis was conducted on each of these tweets to determine a whether or not the tweets for each of these Twitter users was positive, negative, or neutral. Discovered through the

research were that many of the tweets have different sentiment values, including positive, negative, and neutral.

22.7 Discussion and Recommendation

Given the results of the data analysis in this study, it is recommended that multiple tools be used for data collection with a human in the loop to check the data collected. The applications were able to grab numerous lines of evidence, but the creation of the links had to be validated by an analyst that was able to verify the credibility of the properties for the entity. In the future entities that have a certain number of links could be weighted at a more trusted level and those with lower links require further analysis. The other recommendation is collect all images and the run an extraction on the Exchangeable Image File Format (EXIF) metadata. This metadata can be mapped on a heat map that correlates with the time stamp found in the metadata. The terrorist's organizations found were not linked to each other or other known groups. In the future research could look at the connections to other bodies such as Non-government Organizations (NGOs), universities, political parties, etc. It is also essential that the types of metrics used to do associations of data elements and associated target behaviors and parametric information. This would be used to define new ways to characterize information to associated objects. A statistical assessment of the accuracy by manual inspection of associations would help intelligence analysts gain confidence in new metrics for the data mining and tracking algorithms.

22.8 Conclusion

The study's objective was to collect OSINT data and conduct a link analysis. Several main conclusions emerged from this research study. The results of the data analysis showed that some OSINT data collected were indeed mapped to terrorist organizations however these links were not all negative. A majority of these links were from news agencies or reporters. Required was an inspection of each entity, and the associated properties to validate if transform conducted was useful.

References

1. Dawson, M., Kisku, D. R., Gupta, P., Sing, J. K., & Li, W. (2016). *Developing next-generation cuntermeasures for homeland security threat prevention* (pp. 1–428). IGI Global: Hershey, PA. doi:10.4018/978-1-5225-0703-1.
2. Dawson, M., & Adeboje, W. (2016). Islamic extremists in Africa: Security spotlight on Kenya and Nigeria. In M. Dawson, D. Kisku, P. Gupta, J. Sing, & W. Li (Eds.), *Developing next-generation countermeasures for homeland security threat prevention* (pp. 93–103). Hershey, PA: Information Science Reference. doi:10.4018/978-1-5225-0703-1.ch005
3. National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database [Nigeria]. Retrieved from https://www.start.umd.edu/gtd
4. National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database [Somalia]. Retrieved from https://www.start.umd.edu/gtd
5. National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database [Kenya]. Retrieved from https://www.start.umd.edu/gtd
6. National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database [Ethiopia]. Retrieved from https://www.start.umd.edu/gtd
7. National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database [Syria]. Retrieved from https://www.start.umd.edu/gtd
8. Stalder, F., & Hirsh, J. (2002). Open source intelligence. *First Monday, 7*(6), 1–8.
9. Milne, D., & Witten, I. H. (2013). An open-source toolkit for mining Wikipedia. *Artificial Intelligence, 194*, 222–239.
10. Cleveland, S., Jacson, B. C., & Dawson, M. (2016) Microblogging in higher education: Digital natives, knowledge creation, social engineering, and intelligence analysis of educational tweets (pp. 1–19). E-Learning and Digital Media.
11. Steele, R. D. (2000). *On intelligence: Spies and secrecy in an open world*. Washington, D.C: AFCEA International Press.
12. Ihaka, R., & Gentleman, R. (1996). R: A language for data analysis and graphics. *Journal of Computational and Graphical Statistics, 5*(3), 299–314.
13. Bradbury, D. (2011). In plain view: Open source intelligence. *Computer Fraud & Security, 2011*(4), 5–9.
14. Hofmann, M., & Klinkenberg, R. (Eds.). (2013). *RapidMiner: Data mining use cases and business analytics applications*. Boca Raton: CRC Press.
15. Gandrud, C. (2013). *Reproducible research with R and R studio*. Boca Raton: CRC Press.
16. Berthold, M. R., Cebron, N., Dill, F., Gabriel, T. R., Kötter, T., Meinl, T., Ohl, P., Seib, C., Thiel, K., & Wiswedel, B. (2008). *KNIME: The Konstanz information miner* (pp. 319–326). Berlin Heidelberg: Springer.
17. Lutz, M. (1996). *Programming python* (Vol. 8). Sebastapol: O'Reilly.

Security Solutions for Hyperconnectivity and the Internet of Things

Maurice Dawson
University of Missouri-St. Louis, USA

Mohamed Eltayeb
Colorado Technical University, USA

Marwan Omar
Saint Leo University, USA

A volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

IGI GLOBAL
DISSEMINATOR OF KNOWLEDGE
www.igi-global.com

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Dawson, Maurice, 1982- editor. | Eltayeb, Mohamed, 1978- editor. | Omar, Marwan, 1982- editor.
Title: Security solutions for hyperconnectivity and the Internet of things / Maurice Dawson, Mohamed Eltayeb, and Marwan Omar, editors.
Description: Hershey, PA : Information Science Reference, [2017] | Series: Advances in information security, privacy, and ethics | Includes bibliographical references and index.
Identifiers: LCCN 2016023423| ISBN 9781522507413 (hardcover) | ISBN 9781522507420 (ebook)
Subjects: LCSH: Cyberterrorism--Prevention. | Computer crimes--Prevention. | Internet of things. | Computer security. | Data protection.
Classification: LCC HV6773.15.C97 S43 2017 | DDC 005.8--dc23 LC record available at https://lccn.loc.gov/2016023423

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 1
Exploring Secure Computing for the Internet of Things, Internet of Everything, Web of Things, and Hyperconnectivity

Maurice Dawson
University of Missouri – St. Louis, USA

ABSTRACT

Secure computing is essential as environments continue to become intertwined and hyperconnected. As the Internet of Things (IoT), Web of Things (WoT), and the Internet of Everything (IoE) dominate the landscape of technological platforms, protection these complicated networks is important. The everyday person who wishes to have more devices that allow the ability to be connected needs to be aware of what threats they could be potentially exposing themselves to. Additionally, for the unknowing consumer of everyday products needs to be aware of what it means to have sensors, Radio Frequency IDentification (RFID), Bluetooth, and WiFi enabled products. This submission explores how Availability, Integrity, and Confidentiality (AIC) can be applied to IoT, WoT, and IoE with consideration for the application of these architectures in the defense sector.

DOI: 10.4018/978-1-5225-0741-3.ch001

INTRODUCTION

The next era of computing will be outside of the traditional desktop (Gubbi, Buyya, Marusic, & Palaniwami, 2013). When you consider Bring Your Own Device (BYOD) as a radical step imagine using devices such as a refrigerator that contain an embedded computing device to track the quantity of groceries within. This embedded device would allow access to email, weather, and other devices that allow connectivity through WiFi, or some Application Programming Interface (API) to a web based application. Thus, the data collected would be weather, thermostat cooling patterns, foods purchased, the cost of items per month, average consumption, and more. This massive amount of data that can also be collected means there has to be the large place that this data is stored. At the moment organizations such as Cisco Systems and others are pushing for IoT, and IoT but none has a plan for ensuring Information Assurance (IA) posture is maintained during various modes of operation.

HYPERCONNECTIVITY

Hyperconnectivity is a growing trend that is driving cyber security experts to develop new security architectures for multiple platforms such as mobile devices, laptops, and even wearable displays (Dawson, Omar, Abramson, & Bessette, 2014). The futures of both national and international security rely on complex countermeasures to ensure that a proper security posture is maintained during this state of hyper-connectivity. To protect these systems from the exploitation of vulnerabilities, it is essential to understand current and future threats to include the instructions, laws, policies, mandates, and directives that drive their need to be secured. It is imperative to understand the potential security-related threats with the use of social media, mobile devices, virtual worlds, augmented reality, and mixed reality.

In an article published by Forbes, a contributor describes the concept of hyper-connectivity in six different scenarios (Ranadivé, 2013). These events range from energy to hospitality. In health-care there would be real time monitoring through wrist monitors that the medical staff could monitor to get instantaneous feeds on patients that are real time. They would be able to foresee problems before they occur or receive alerts during various events. Imagine a pregnant woman that is having early complications could be monitored first through a wristband that delivers real-time patient information wirelessly.

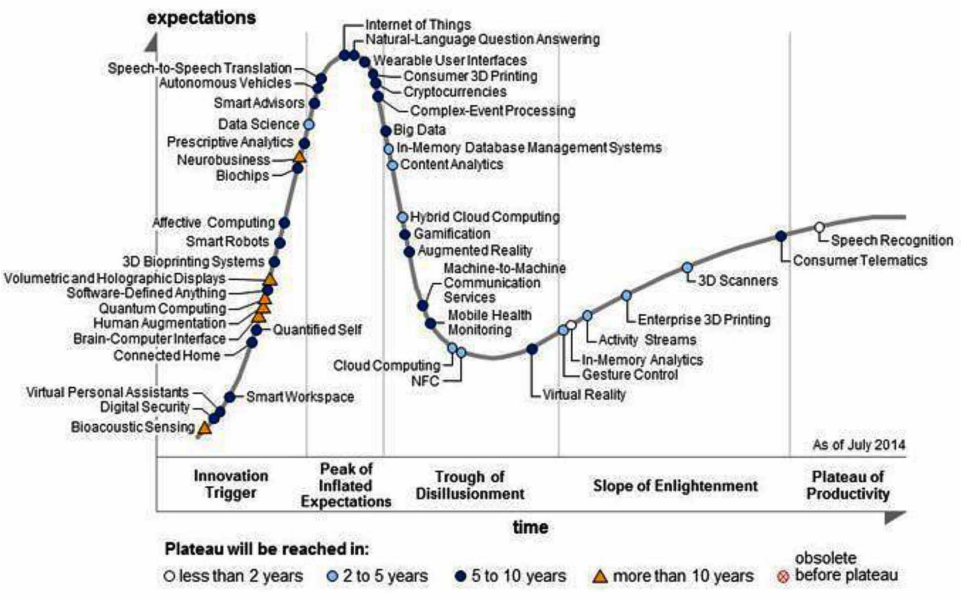
When discussing hyperconnectivity, it is necessary to examine systems of systems concepts. Systems of systems is a collection of systems tied together to create a more complex system (Popper, Bankes, Callaway, & DeLaurentis, 2004). When thinking about the possibilities of hyperconnectivity the Personal Area Network (PAN) is

an excellent example as it allows multiple technologies to be interconnected with soil ware applications. The Google Glass has the potential to all Global Positioning System (GPS), social media, digital terrain overlays, and synchronization with other devices. This increases the complexity of the system as it becomes part of larger systems which multiplies the number of potential vulnerabilities.

INTERNET OF THINGS

IoT is a global infrastructure for information society enabling services by interconnecting physical and virtual things based on existing and evolving interoperable Information Communication Technologies (ICT) (International Telecommunication Union, 2012). Gartner has developed a figure which displays the hype cycle of emerging technologies. This hype circle shows the expectations on the y-axis where on the x-axis time is displayed [See Figure 1]. The time shown is the innovation trigger, the peak of inflated expectations, the trough of disillusionment, slope of enlightenment, and plateau of productivity (Gartner, 2014). What the figure fails to provide is anything associated with security about the technologies identified. The figure simply shows the cycle of emerging technologies with time corresponding to expectations.

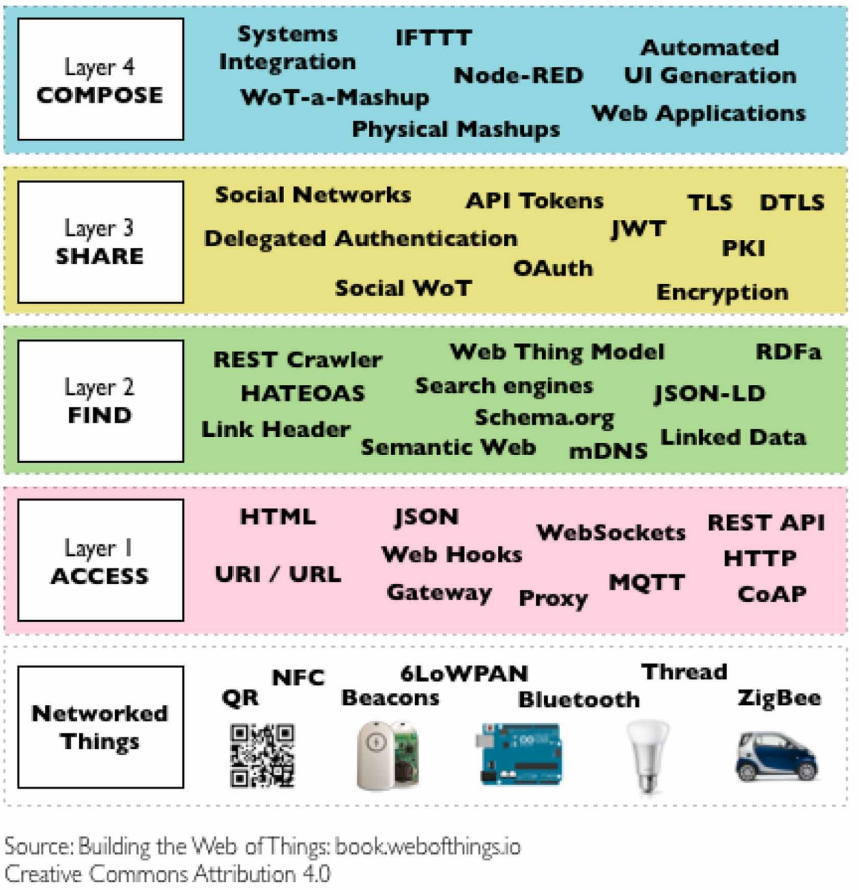
Figure 1. Gartner 2014 hype cycle of emerging technologies
(Source: Gartner Inc.)



WEB OF THINGS

The WoT is a continued vision that describes concepts where everyday objects are fully integrated into the World Wide Web (WWW). This concept focused on embedded computing devices that enable communication with WWW. The devices can ring from refrigerators to mobile devices with integrated with the Web through an API (Guinard & Trifa, 2009). The Social WoT offers opportunities to use social connections and underlying social graphs to share digital artifacts (Guinard, 2011). This would help bridge a gap between social networks and networks of objects transforming communication. Figure 2 displays the WoT architecture and the detailed layers it is comprised of.

Figure 2. Building the web of things



Source: Building the Web of Things: book.webofthings.io
Creative Commons Attribution 4.0

This bridge between social connections and basic things could allow for a plethora of data that can be analyzed unlike before. When looking at the networked things you can see the multiple of different technologies can be enabled in WoT. When looking at Layer 1, you can immediately see items that are a cause of problems. For examples, Hyper Text Markup Language (HTML) and JavaScript Object Notation (JSON) contain known vulnerabilities. In current social networks, geolocation provides individuals exact location. However, anyone that develops an application using this API can tweak items providing, even more, the granularity of its users. Even without modification of Tweets only adding the location will provide details such as neighborhood, city, state, or country. This publication information can be used to start an analysis. In iOS version 6.26+ and Android version 5.55+ precise location can be shared if elected to do so. Also, third party applications or websites may share specific Tweet locations as well.

Various social media accounts provide the ability to associate a particular location. This position over time can provide trends of sites visited with time/date stamps. This can be used to start developing a full analysis on Tweeting trends from particular locations, frequency of location visits, and content analysis through text mining. Exchange Image File Format (EXIF) data is a standard that specifies the formats for images, sounds, and ancillary tags used by digital cameras. The EXIF digital image standard defines the following; the basic structure of digital image data files, labels and JPEG marker segments the conventional uses, and how to define and management format versions (Tešić, 2005). Research has been conducted on how to extract efficiently EXIF data for prosecuting those involved in child pornography (Alvarex, 2004).

In Layer 3, some of these concerns can be appropriately addressed. In this layer controls can be made for the ability to share content. Content can be tagged with a severity and classification to have automatically a security feature added. If the data were Personal Identifiable Information (PII) then the data would have encryption, and access controls that only allow certain individuals to obtain it. That data could be sent wireless over a Bluetooth enabled device or a medical beacon.

INTERNET OF EVERTHING

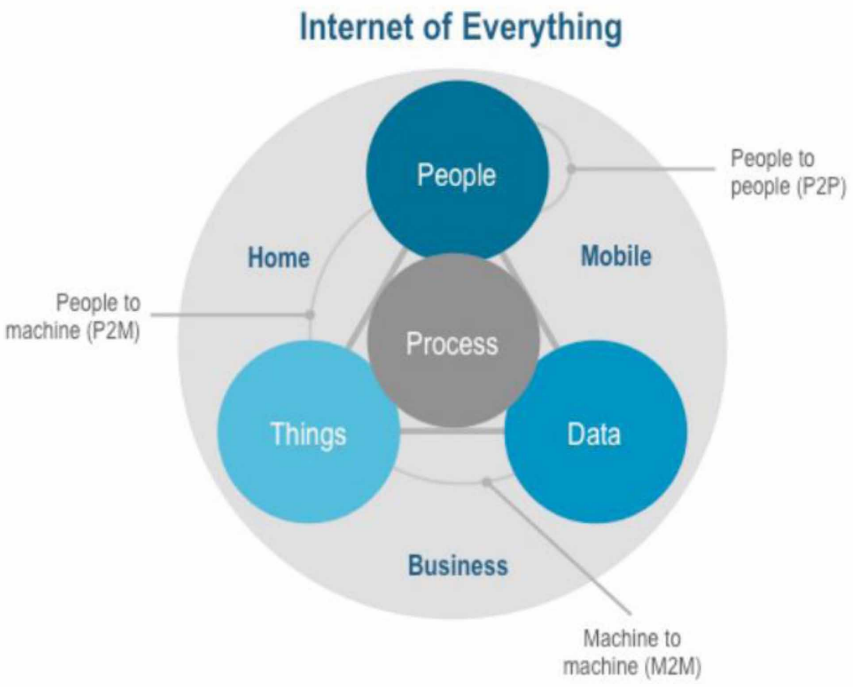
The IoE consists of four grouping with are data, things, people, and process (Bradley, Barbier, & Handler, 2013). IoE leverages data as a means to make more insightful decisions. IoT plays a significant role in the things of IoE as this is the network of physical devices and objects connected to the Internet for decisions making. The IoE connects people in more valuable and relevant ways. The process is the last part which is delivering the correct information to the right entity at the right time.

Researchers at Cisco Systems estimate that over 99 percent of physical devices are still unconnected and that there is a market of $14.4 trillion. This white paper urges business leaders to transform their organizations based on key learnings to be competitive for the future. (Evans, 2012). IoE is comprised of four key things which are people, data, and things built on the process. The model IoE is made up of three types of connections: People to Machine (P2M), Machine to Machine (M2), and People to People (P2P).

BODY HACKING AND ENHANCEMENT

One of the newest trends in staying connected is human enhancement through body hacking (Nortol, 2007). This involves individuals placing RFID chips into their bodies. These RFID components are associated with unique ID numbers that can be used for unlocking doors, logistical tracking, embedded electronics, e-government, and more. The use for e-government would allow interaction between government

Figure 3. The what, where, and how of the Internet of everything
(Source: Cisco IBSG, 2012)



and outside groups through the connected body parts. A health organization could monitor the status of a group through embedded chips or other devices connected to an individual or group.

The issues surrounding body hacking is the lack of security controls associated with making these mods. Early when discussed in this chapter was hyperconnectivity, IoT, and IoE to provide an overview of these various technological concepts. When adding more connectivity to systems the complexity increases thus it becomes more difficult to protect effectively from potential threats. For items such a pacemakers it has already been proven to be hackable (Kirk, 2012; Richardson, n.d.).

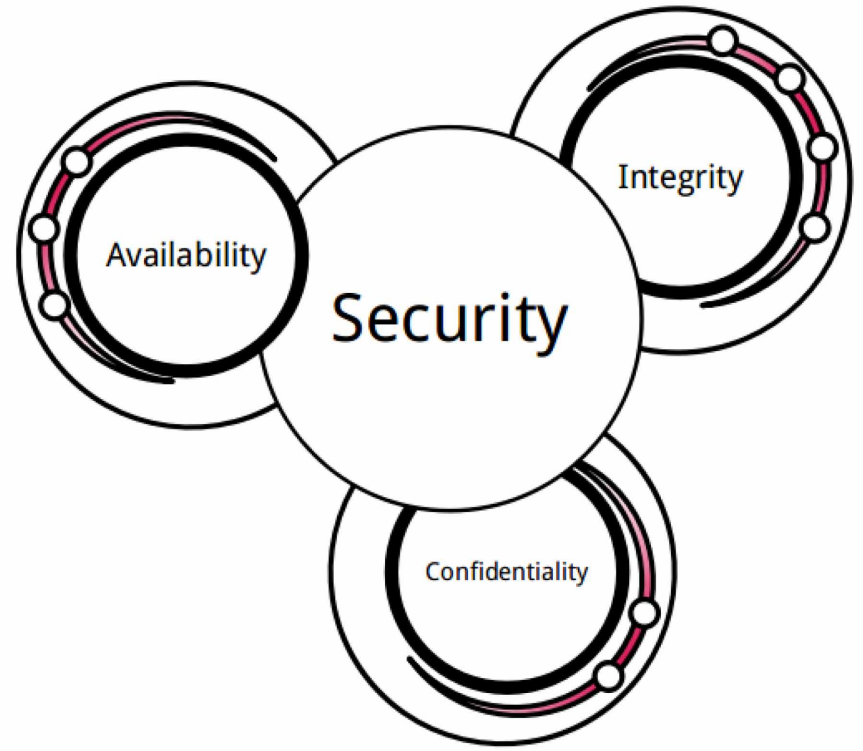
In the report Enhanced Warfighters: Risk, Ethics, and Policy (2013) that is prepared for The Greenwall Foundation discussed is the findings of using technology for soldiers. As other technologies are emerging within the United States (U.S.), a military sector so is robotics, Artificial Intelligence (AI), human enhancement technologies, other cyber capabilities. The issues surrounding human enhancement technologies among other items are the operational, ethical, and legal implications (Mehlman, Lin, P., & Abney, 2013). Regarding risks, those identified are about the technology falling into the wrong hands allowing for reverse engineering. Reverse engineering would allow non-friendlies to develop similar technologies on their own to rival those found on the warfighters.

SECURITY AND PRIVACY

As a new wave of Internet-enabled technologies arrive, it is imperative to understand fully the security and privacy concerns (Thierer, 2015). And understanding these concerns also means understanding how to appropriately apply IA controls to systems. Addressing security objectives appropriately will allow for risks to be mitigated. This means following the principles of security to ensure IA posture is achieved.

With all of these connected devices using proven standards, policies, and guidance can help with the ease of integrating these technologies into everyday life. Currently, there is a lack of guidance for securing IoT, IoE, and WoT as a cohesive unit. However there is appropriate documentation available through the National Institute of Standards and Technology (NIST), Federal Information Processing Systems (FIPS), Department of Defense (DoD), Institute of Electronic and Electrical Engineers (IEEE), International Organization for Standardization (ISO), Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and more. It will be key for the security engineer to understand how to protect these devices individually and then understand the how the devices become more vulnerable when connected. Mobile devices would need to be hardened with appropriate security controls (Dawson, Wright, & Omar, 2016; Omar & Dawson,

Figure 4. AIC triad



2013). Encryption would need to be on devices that have IoT capabilities such as refrigerators, televisions, or smart watches. This would allow the protection of data in transit and at rest. Access controls would need to be placed to ensure that other users of the hyperconnected systems to do not have

With the potential threats of cyber terrorism affecting national and international security the importance of security is elevated to greater heights (Dawson, Omar, & Abramson, 2015). New threats against national infrastructure and digital crime are making researchers consider new methods of handling cyber incidents (Dawson, & Omar, 2015). It is imperative that if the government or commercial sectors want to make use of these new technological Internet and Web-enabled architectures that they are prepared to battle new threats.

Currently, DoD is using limited IoT to be more efficient in combat. New battlefield technology includes helmets that provide a Heads Up Display (HUDs) to provide Global Positioning System (GPS) battle mapping to integrate with other technologies that provide real-time tracking of the battlefield. A potential example includes the ability to control Unmanned Air Vehicles (UAV) through sensors tied to platoon

leaders rather than the use of a Universal Ground Control System (UGCS) or Portable Ground Control System (PGCS). IoT, IoE, and WoT can place the control of tactical devices directly in the hands of those soldiers who are a front line during combat missions. In years to comes body enhancement with RFIDs and other sensors could provide situational awareness data to the soldiers and those that lead them. This data can be analyzed to maximize the effectiveness of troop movement, target location, and other activities deemed key to the mission of the military.

CONCLUSION

Secure computing is essential as technological environments continue to become intertwined and hyperconnected. The policies to properly secure these new environments must also be explored as many of the security controls found within guidance such as the DoD focuses on singular systems and components (Dawson Jr, Crespo, & Brewster, 2013). There needs to be the creation of new controls that review embedded sensors, body modifications, and devices that fully take advantage of Internet-enabled technologies. With the emergence of these technologies, the possibilities are endless however there will be new vulnerabilities unexplored.

REFERENCES

Alvarez, P. (2004). Using extended file information (EXIF) file headers in digital evidence analysis. *International Journal of Digital Evidence*, *2*(3), 1–5.

Bradley, J., Barbier, J., & Handler, D. (2013). *Embracing the Internet of everything to capture your share of $14.4 trillion.* White Paper, Cisco.

Dawson, M., & Omar, M. (2015). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*. Hershey, PA: IGI Global; doi:10.4018/978-1-4666-8345-7.ch001

Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the Methods behind Cyber Terrorism. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology* (3rd ed.; pp. 1539–1549). Hershey, PA: Information Science Reference; doi:10.4018/978-1-4666-5888-2.ch147

Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). The Future of National and International Security on the Internet. In A. Kayem & C. Meinel (Eds.), *Information Security in Diverse Computing Environments* (pp. 149–178). Hershey, PA: Information Science Reference; doi:10.4018/978-1-4666-6158-5.ch009

Dawson, M., Wright, J., & Omar, M. (2016). Mobile Devices: The Case for Cyber Security Hardened Systems. In Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications (pp. 1103-1123). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8751-6.ch047

Dawson, M. E. Jr, Crespo, M., & Brewster, S. (2013). DoD cyber technology policies to secure automated information systems. *International Journal of Business Continuity and Risk Management*, *4*(1), 1–22. doi:10.1504/IJBCRM.2013.053089

Evans, D. (2012). The internet of everything: How more relevant and valuable connections will change the world. *Cisco IBSG*, 1-9.

Gartner. (2014, August 11). *Gartner's 2014 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business*. Retrieved February 28, 2016, from http://www.gartner.com/newsroom/id/2819918

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. doi:10.1016/j.future.2013.01.010

Guinard, D. (2011). *A web of things application architecture-Integrating the real-world into the web.* (Doctoral dissertation). ETH Zurich.

Guinard, D., & Trifa, V. (2009, April). Towards the web of things: Web mashups for embedded devices. In *Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web (MEM 2009), in proceedings of WWW (International World Wide Web Conferences),*(p. 15).

Harris, S., & Meyers, M. (2002). *CISSP*. McGraw-Hill/Osborne.

International Telecommunication Union. (2012a). ITU-T recommendation Y.2060: Series Y: Global information infrastructure, internet protocol aspects and next-generation networks: Frameworks and functional architecture models: Overview of the Internet of Things. Geneva: International Telecommunication Union.

International Telecommunication Union. (2012b). ITU-T recommendation Y.2063: Series Y: Global information infrastructure, internet protocol aspects and next-generation networks: Frameworks and functional architecture models: Framework of the Web of Things. Geneva: International Telecommunication Union.

International Telecommunication Union. (2012c). ITU-T recommendation Y.2069: Series Y: Global information infrastructure, internet protocol aspects and next-generation networks: Frameworks and functional architecture models: Terms and definitions for the Internet of Things. Geneva: International Telecommunication Union.

Kirk, J. (2012). Pacemaker hack can deliver deadly 830-volt jolt. *Computerworld*, 17.

Mehlman, M., Lin, P., & Abney, K. (2013). *Enhanced Warfighters: Risk, Ethics, and Policy.* Case Legal Studies Research Paper, (2013-2).

Norton, Q. (2007). *The Next Humans: Body Hacking and Human Enhancement*. O'Reilly Emerging Technology Conference.

Omar, M., & Dawson, M. (2013, April). Research in Progress-Defending Android Smartphones from Malware Attacks. In *Advanced Computing and Communication Technologies (ACCT), 2013 Third International Conference on* (pp. 288-292). IEEE. doi:10.1109/ACCT.2013.69

Popper, S., Bankes, S., Callaway, R., & DeLaurentis, D. (2004). *System-of-Systems Symposium: Report on a Summer Conversation*. Arlington, VA: Potomac Institute for Policy Studies.

Ranadivé, V. (2013, February 19). *Hyperconnectivity: The Future is Now*. Retrieved March 21, 2016, from http://www.forbes.com/sites/vivekranadive/2013/02/19/hyperconnectivity-the-future-is-now/#401d45d26b9f

Richardson, C. (n.d.). Critical Infrastructure Protection. *Alternative Energy CBRN Defense Critical Infrastructure Protection*, *13*.

Tešić, J. (2005). Metadata practices for consumer photos. *MultiMedia, IEEE*, *12*(3), 86–92. doi:10.1109/MMUL.2005.50

Thierer, A. D. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. *Adam Thierer, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation, 21*.

KEY TERMS AND DEFINITIONS

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (Harris, 2002).

Availability: Timely, reliable access to data and information services for authorized users (Harris, 2002).

Confidentiality: Assurance that information is not disclosed to unauthorized individuals, processes, or devices (Harris, 2002).

Hyperconnectivity: Use of multiple means of communications such as instant messaging, phones, Web 2.0, Web 3.0, and other communication methods.

Integrity: Quality of an IS reflecting the logical correctness and reliability of the OS; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (Harris, 2002).

Internet of Everything: Consists of four grouping with are data, things, people, and process (Bradley, Barbier, & Handler, 2013).

Internet of Things: A global infrastructure for information society enabling services by interconnecting physical and virtual things based on existing and evolving interoperable ICT (International Telecommunication Union, 2012).

Non-Repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (Harris, 2002).

Open Source Intelligence: Intelligence collected from publicly available sources.

Web of Things: Refers to making use of the IoT in order for (physical and virtual) things to be connected and controlled via the world wide web (International Telecommunication Union, 2012).

Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning

Francisco Milton Mendes Neto
Federal Rural University of the Semiarid Region, Brazil

Rafael de Souza
Federal Rural University of the Semiarid Region, Brazil

Alex Sandro Gomes
Federal University of Pernambuco, Brazil

A volume in the Advances in Game-Based Learning (AGBL) Book Series

Information Science REFERENCE
An Imprint of IGI Global

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Mendes Neto, Francisco Milton, 1973- editor. | Castro de Souza, Rafael, 1991- editor. | Gomes, Alex Sandro, editor.
Title: Handbook of research on 3-D virtual environments and hypermedia for ubiquitous learning / Francisco Milton Mendes Neto, Rafael Castro de Souza, and Alex Sandro Gomes, editors.
Description: Hershey, PA : Information Science Reference, 2016. | Includes bibliographical references and index.
Identifiers: LCCN 2015051298| ISBN 9781522501251 (hardcover) | ISBN 9781522501268 (ebook)
Subjects: LCSH: Virtual reality in education. | Virtual reality in education--Research.
Classification: LCC LB1044.87 .H337 2016 | DDC 371.33/468--dc23 LC record available at http://lccn.loc.gov/2015051298

This book is published in the IGI Global book series Advances in Game-Based Learning (AGBL) (ISSN: 2327-1825; eISSN: 2327-1833)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 20
Systems Engineering Concepts with Aid of Virtual Worlds and Open Source Software:
Using Technology to Develop Learning Objects and Simulation Environments

Latina Davis
Morgan State University, USA

Maurice Dawson
University of Missouri – St. Louis, USA

Marwan Omar
Saint Leo University, USA

ABSTRACT

Technology is changing the landscape of learning and teaching in America. The use of virtual worlds enable engineering and technology programs to implement software programs such as Second Life and Open Simulator to enhance what they may currently already have. Additionally, virtual worlds can add a more dynamic environment in the online classroom for multiple platforms such as the Personal Computer (PC), wearables, and mobile devices. The purpose of this chapter is to provide a review of these programs to include how to implement these items into an engineering course. Further detailed in this submission is how to incorporate Institute of Electrical and Electronics Engineers (IEEE) documentation and other engineering guidelines into the projects. Included in this chapter is a detailed layout of a simulated environment as well as various approaches of structuring and organization for classroom activities.

DOI: 10.4018/978-1-5225-0125-1.ch020

SIMULATION

Simulation allows for the imitation of a real world scenario or systems. This can be accomplished using software technology such as virtual worlds. Simulation can come in the form of training, education, video games, modeling, low fidelity prototypes, and usability. Simulation can use learning objects and incorporate other modern day technologies such as Google Glass for increasing teaching effectiveness.

UBIQUITOUS LEARNING

Ubiquitous Learning (U-Learning), supported by the revolutionary and abundant digital resources, is viewed as an effective learning approach for situating students in real-life and relevant learning environments that supports and promotes a variety of learning needs. U-Learning involves applying ubiquitous technologies in the enhancement of education strategies and models. Embedded Internet-based devices that we use in our daily live can present a supportive environment for U-Learning. The rise in Internet availability and accessibility has truly made a significant number of learning resources and options available to today's students at all levels of education. U-Learning has the unique power of providing educational resources in a manner that is flexible, calm, and seamless due to its pervasive and persistent model (Martinez-Maldonado, Clayphan, Muñoz-Cristóbal, Prieto, Rodríguez-Triana, & Kay, 2013); U-Learning aims at removing educational and learning physical barriers by utilizing the advancements in technology The ubiquitous learning has become more than a technology phenomenon and a prominent vision that strives to revolutionize the educational landscape and present technology-driven educational settings, because it thrives on the concept and idea of making a variety of educational and learning assets available to students, creates new and varied learning environments, customized learning and enables the realization of a series of training activities from anywhere, anytime and from any device (Durán, Álvarez & Únzaga, 2014).

Ubiquitous and pervasive learning environments offer students unique possibilities for team work and collaboration both face-to-face and remotely. These environments include an array of modern and innovative technologies at different stages of adoption: interactive whiteboards are already available in many classrooms; interactive tabletops are just starting to be introduced in schools (Kharrufa et al, 2013), and handheld devices are already used by students and teachers in the form of smart-phones or tablets.

U-Learning Space and Design

Many studies in the past have investigated the effectiveness of deploying different learning and teaching styles with different U-Learning environments to determine which strategy produces the best learning outcomes for students with different learning needs. It's important to note that developing a u-Learning space has to take into consideration the outcome of the existing learning theories in terms of best practices, such as a structured relationship between information and learners' understanding in educational settings. This helps to prevent learning isolated from a meaningful context. For example, if a student understands *why* and *how* something happens rather than just being told that it is true, then the information is more relevant and, therefore, is more meaningful to the student. The rationale for this is that *how* is the inclusion of the pedagogical information; and *why* is the inclusion of interactive learning, allowing students to create knowledge from what they perceive (Ogata & Yano, 2012).

Colorado Technical University has successfully deployed an award-winning, revolutionary U-Learning system that is called " Intellipath". Intellipath™ is adaptive learning software that personalizes learning based on a student's pre-determined knowledge state on a particular subject or topic, and creates individual learning nodes, or steps for the student to ensure the student understands each element to a specific unit of work. Intellipath™ allows the instructor and students to work closely together to ensure transfer of learning is taking place. What is unique about this learning technology is that the learning lessons are connected throughout the entire course map. Work on one node influences learning on other nodes in the course map. Learning is a continuum throughout the course, assessment is constant, and by revising nodes students can continually improve their learning.

Ubiquitous Computing

As computers become ubiquitous, they capture our attention and daily activity, which allow them to infiltrate into the background. Ubiquitous computing, however, includes computing devices such as smartphones, tablets, cameras, and other digital gadgets. Integrating ubiquitous computing into ubiquitous learning promotes the interaction between students and their digital gadgets to become connected with the manifold digital embedded devices and/or services (Möller, Haas, & Vakilzadian, 2013). Therefore, in a ubiquitous learning settings or environment, students have the unique ability of exploring the ubiquitous space built and powered by ubiquitous and mobile technology to interact with the various embedded digital devices and/or services. Thus, ubiquitous learning has the potential to create a sustainable and persistent learning and education environment that has barrier free and adapts to varying students learning needs.

Students have the advantage and ability of deciding which learning approaches best fit their learning needs and they are able to customize the environment to best fit their specifying situation (Martinez-Maldonado & Kay, 2013). In the U-Learning space, sharing information and knowledge between learners and mobile devices becomes a reality and contributes to creating a learning environment where learners can access, share, and distribute knowledge anytime and anywhere and therefore we become a more powerful society by connecting people, ideas, and knowledge. With U-Learning, we are able to create and available and accessible learning community utilizing mobile technology that makes learning attainable, traceable, and identifiable (Möller, Haas, & Vakilzadian, 2013).

Learning Objects

Learning objects allow for educational content to be broken down into smaller pieces that can be reused in various learning environments (Boss & Krauss, 2007). Learning objects are grounded in the object oriented paradigm of computer science (Wiley, 2000). These are digital resources uniquely identified and metatagged that can be used to support learning. Provided is a new and innovative method to reuse technologies in the learning environment. Thus learning objects (LSTC, 2000a) leads other candidates for the next generation of instructional design.

The IEEE Learning Technology Standards Committee (LTSC) System Interoperability in Education and Training has a couple actively working on an augmented reality learning experience model. This new standard will include technologies such as wearables (LSTC, 2000b). In virtual worlds these objects can be given a 3 Dimensional (3-D) representation which allows users to interact with these objects. Also behavioral tasks and indicators can be observed with 3-D learning objects (Vincenti, 2010).

SLOODLE

SLOODLE is an open source project which integrates virtual environments with the Moodle Learning Management System (LMS). This application allows to connect to a chat room, present, obtain feedback, management in world assignments with an assignment drop box, give quizzes, track points, identity linking, and more (Kemp, Livingstone, & Bloomfield, 2009). As this software application is integrated with the Moodle LMS it allows for universities to implement new technologies to enhance online education. In technical fields such as systems engineering this will allow for the creation and reuse of design objects.

For example, an engineer professor could search for virtual objects by associated tags. Those tags would bring forward the appropriate virtual object to the instructor. These objects would save hours in design time for a new lab. Additionally, in a software engineering oriented environment this could be useful in teaching the principles of code reuse in an interactive environment.

OPEN SOURCE APPLICATIONS AND TECHNOLOGY EFFECTIVENESS

Open Source Software

Open source software (OSS), as the name suggests, refers to the software that is made available and can be accessed by any user without requiring any fees. Unlike commercial proprietary software, the source code of open source software can be accessed, developed, and improved by any person and without any limitations (Jacobs, Kussmaul, & Sabin, 2011). Open source software started becoming popular and widely used by academia during the last two decades (Rooij, 2009). The reason behind the popularity and importance of using Free Open Source Software (FOSS) is that many educational institutions lack the financial capability to purchase proprietary or closed software that is usually very expensive. Therefore FOSS owes much of its success and credibility to academia where students and faculty alike were the pioneers to participate in developing and improving FOSS. The basic idea behind the development of OSS is that if many people view the same code then we will have a better opportunity to improving that code faster because it's from the community and to the community. Members of the open source community feel some kind of commitment towards continuously improving open source projects.

Open Source Software for Educational Institutions

There is a myriad of free, open source software applications that can be utilized to enhance the learning process for students in the areas of software engineering, project management, database development, and web development. Studies have shown that FOSS is increasing gaining ground and has grown in use at an exponential rate by educational organizations (Rowell. 2008) We will discuss some of the major open source tools that could be easily utilized in a classroom setting and are currently in use by enterprise software developers. Moreover; such tools will serve as an invaluable resource for students who are planning to enter the business enterprise environment and enable them to head start their professional career. OSS can be defined as software that is made available in source code form. This is important as this source code may fall under the General Public License (GPL) which is a widely used free software license that is managed under the GNU Not Linux (GNU) Project (GNU, 2007). Virtualization is impor-

tant as this is an effective method to reproduce system learning environments on the same systems the learner is using reducing the overall hardware footprint and need to for a massive lab. This paper will also cover various software applications that can be integrated into the university system.

Virtualization

In terms of virtualization there are available tools to create a virtual version of a system. In terms of educational resources this provides a method for institutions to train on Virtual Machines (VMs). This allows a university to teach students complex techniques to computer science, engineering, or Information Technology (IT) students such as networking, programming, system administration, and Information Assurance (IA). There are multiple types of virtualization such as hardware, desktop, memory, storage, data, and network.

For institutions that would like the opportunity to provide a cloud like environment tools such as Oracle Virtual Box and Vmware Player provide that ability. However it should be noted that new Linux distributions running that require GNOME 3 will have issues running on older hardware. With older hardware as a constrained there are bare minimal Linux distributions such as Puppy Linux and Damn Small Linux (DSL). VMs provide the ability for a student to experiment with hundreds of Operating Systems (OSs) without installing or uninstalling the base OS. As faculty members, we have used VMware software as well as Oracle virtual box as effective tools to host Linux as well as Windows operating systems; the results have been impressive in that students were able to better grasp the theories and principles presented in class because they had the opportunity to tinker with all the inner workings of those OSs. This approach also helped us save invaluable time and resources that would have otherwise been needed for installing and un-installing all those OSs.

Additionally, this allows for the creation of baseline OS images for classes. For example, an engineering course would have an OS created with all the software, case studies, and etc. preloaded. This baseline OS for software engineering would have development tools, static code analysis tools, debugging tools, case studies, eBooks, links to online course management tool, and etc. This would allow an institution to have image ready for every class to ensure consistency, and that the students have all required tools needed. In the case for a more technical course such as software engineering the students would have a baseline OS image with all the programming software, the Integrated Development Environment (IDE), quality testing tools, and etc. preloaded. In considering virtual environments the image can include the necessary installation software or preloaded software to immediately start work in the U-Learning environment.

Why We Need to Consider Linux Essential in Higher Education

Linux is an Unix like OS that is built on the Linux kernel developed by Linus Torvalds with thousands of software engineers. As of 2012 there are over two hundred active Linux distributions. The majority of the kernel and associated packages are free and OSS. This type of software provides a license which allows users the right to use, copy, study, change, and improve the software as the source code is made available. Providing source code allows developers or engineers to understand the inner workings of development. Imagine being able to study Mac or Windows by viewing all the source code to replicate similar developments. This exercise would be great for a developer to learn low level coding techniques, design, integration, and implementation (Dawson, & Al Saeed, 2013).

In terms of associated cost the majority of Linux distributions are free. However some distributions require a cost for updates or assistance that related to specific needs such as OS modifications for server hosting (Dawson, & Al Saeed, 2013). In software, there is a packet management system that automates the process of installing, configuring, upgrading, and removing software packages from an OS. In the Linux OS builds the most common packet management systems are Debian, Red Hat Package Manager (RPM), Knoppix, and netpkg.

ENHANCING THE STEM ENVIRONMENT

When discussing teaching tools one must consider all the OSS applications that can be used to improve Science, Technology, Engineering, and Mathematics (STEM) fields such as systems engineering (Dawson, Al Saeed, Wright, & Onyegbula, 2015). OSS provides the ability to do many technical items at a low cost and view source code of the software application (Dawson & Al Saeed, 2012). It is essential to take advantage of these tools and applications as many institutions of learning are having budget problems. These items allow for any institution to be competitive in instructions regardless of location. When thinking about U-Learning the virtual environment is key is the marketplace for low fidelity prototyping.

SYSTEMS ENGINEERING GUIDANCE

IEEE provides guidance on software and systems engineering. The INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Process and Activities provides a great baseline for understand the field of systems engineering (Haskins, 2007). Recently INCOSE released an updated version that brings in more relevant items (INCOSE, 2015). Requirements engineering is essential when starting any program (IEEE Computer Society, 1998). Proper derivation and management of requirements add to the success factor in software engineering (Hofmann & Lehner, 2001). The same could be said in systems engineering as software is a subset engineering field.

Software Engineering Standards

Table 1 represents some IEEE software standards that are essential for systems engineering. All of the items below can be applied to a virtual project to limit the virtual environment for development. These software standards can be used as conditions or requirements that must be met while developing the projects.

SYSTEMS ENGINEERING COURSE PROJECT: ATM MACHINE

Detailed in the following pages is the required project for graduate systems engineering course. This project was designed to simulate an ATM while being developed with an engineering methodology. Through the design of this test environment multiple virtual objects were created as a result of this project through object oriented design techniques. The literature that follows provides the detailed design

Table 1. List of IEEE Software Standards

IEEE Standard	Name of Standard	Additional Info & Citation
IEEE Standard Glossary of Software Engineering Terminology	IEEE Standard Glossary of Software Engineering Terminology	A glossary that contains the vocabulary for the software engineering domain (IEEE Standards Coordinating Committee, 1990)
IEEE Std 730-2002	IEEE Standard for Software Quality Assurance Plans	This particular standard specifies the format and content of Software Quality Assurance plans (Lee et al, 2005).
IEEE Std 830-1998	IEEE Recommended Practice for Software Requirements Specifications	This document recommends the content and characteristics of a Software Requirements Specification(IEEE Computer Society, 1998).
IEEE Std 1028-2008	IEEE Standard for Software Reviews	This standard defines five types of software reviews and procedures for their execution. The five review types include management reviews, technical reviews, inspections, walk-throughs and audits (Westfall, 2008).
IEEE Std 1062-1998	IEEE Recommended Practice for Software Acquisition	This document recommends a set of useful practices that can be selected and applied during software acquisition (IEEE Standards Association, 1998).
IEEE Std 1074-2006	IEEE Standard for Developing Software Life Cycle Processes	This standard describes an approach for the definition of software life cycle processes (Hawker, 2009).
IEEE Std 1220-2005 (ISO/IEC 26702)	IEEE Standard for the Application and Management of the Systems Engineering Process	(Doran, 2006) This standard is listed in a literature survey on international standards for systems requirements engineering (Scheider & Berenbach, 2013).
IEEE Std 1233-1998	IEEE Guide for Developing System Requirements Specifications	This standard provides guidance on the development of a System Requirements Specification, covering the identification, organization, presentation, and modification of requirements (Moore, 1998). It also provides guidance on the characteristics and qualities of requirements such as objective or threshold requirements specification.
IEEE Std 1362-1998 (Reaffirmed 2007)	IEEE Guide for Information Technology-- System Definition-- Concept of Operations (ConOps) Document	This document provides guidance on the format and content of a Concept of Operations (ConOps) document, describing characteristics of a proposed system from the users' viewpoint.
IEEE Std 132-1998	IEEE Guide-- Adoption of PMI Standard-- A Guide to the Project Management Body of Knowledge	In the third edition of the PMBOK is recognized as an international standard which is the IEEE Std 132-1998 (Ahlemann et al, 2009).
IEEE Std 1517-1999	IEEE Standard for Information Technology— Software Life Cycle Processes— Reuse Processes	The standard the provide life cycle processes for reuse of software (Moore, 1998).
ISO 9001:2000	Quality Management Systems— Requirements	This standard has been debated upon in relation to the impact of quality management (Martinez-Costa, 2009).
IEEE/EIA 12207- 2008	Systems and Software Engineering - Software Life Cycle Processes	An international standard to establish common framework for software life cycle processes. This is applicable to software products and the acquisition of systems.
IEEE/EIA 12207.1- 1996	Industry Implementation of International Standard ISO/IEC 12207:1995, Standard for Information Technology-- Software Life Cycle Processes--Life Cycle Data	It is essential to know the basic relation between primary parties in the form of something that is binding(Gary, 1999). In this contract specified will be the requirements and the life cycle process model which will be used.
ISO/IEC 90003	Software and Systems Engineering-- Guidelines for the Application of ISO 9001:2000 to Computer Software	This standard provides guidance for organizations in the application of ISO 9001:2000 to the acquisition, supply, development, operation and maintenance of computer software.

of a systems engineering project in a virtual environment with the systems engineering life cycle being used a the applied methodology. Displayed is an example of U-Learning that supports key concepts, contextual factors, and current practices in systems engineering.

High Level Systems Analysis

To begin any analysis of the system, a High Level Systems Analysis (HLSA) must be performed while in conjunction of communication with the users. This is the structure of the system, defining the essential core design features and elements providing the framework for required components and for ones that may follow resulting in future adjustments. A High Level Systems Diagram (HLSD) is constructed from the analysis that provides an engineering view of the users' vision for what the system needs to be and do; including the paths that's are required for the system to function properly. The HLSD is an approach in the methodology of SDLC following behind with a more in depth model of the system a Low Level Systems Diagram (LLSD). From the graphical representation models a problem definition can be created to depict the problem of the system and what steps can be performed to begin the design and implementation of the system to be evaluated to fit requirements of the user.

Before performing any task the Stakeholder and Users of the proposed system, needs to communicate with researchers and developers to understand exactly what the Users wants; a High Level Systems Analysis (HLSA) takes place. From the HLSA a High Level System Diagram (HLSD) highlights graphically the main entities of the systems goals and objectives; also known as the scope. A problem definition will be determined from the analysis and JAD sessions, which then results in the analysis and design phase to implementing the project. Developers can perceive what the desire system ought to look like or function as, also being well aware if the system is complex or not. This gives developers a better way in deciding how to approach a problem. The entities that make up the HLSD shown in Figure 1 in this research paper are human users, an ATM Machine, and a Bank Network. These are what drive this system; there are dependent on each other to properly operate.

Low Level Systems Diagram

Low Level System Diagram (LLSD) shown in Figure 2 gives a more detailed graphical representation of the system. It allows intended users to visually recognize what exactly it takes to run the system including systems entities. The requirements within the LLSD will allow user to select requested account and expect task to be achieved.

Figure 1. High Level Systems Diagram (HLSD)

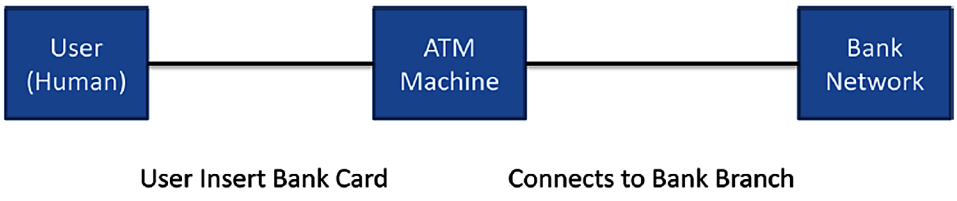
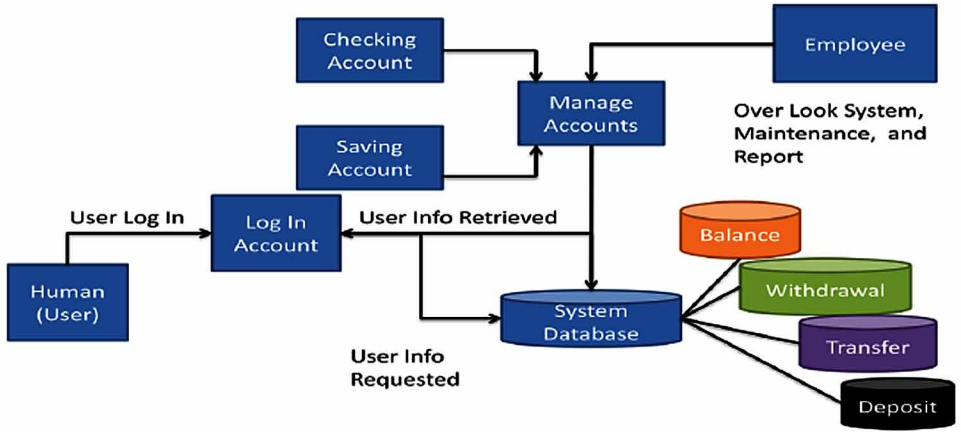


Figure 2. Love Level Systems Diagram (LLSD)



Problem Statement

The problem being addressed can be defined as the ATM machines are not reliable as developers want users to think that they are. Majority of ATM machines charge users to access their own personal accounts. As well as not having access to a 24 hour self cash services; that allows users to access their bank accounts to withdraw, deposit, transfer or check funds within their accounts. Existing ATM machines are not benefiting users at a hundred percent reliability. From the problem definition a scope is formed to focus primarily on the goal of the system.

Scope

The scope of this research can be expressed by the following statement. To analyze, model, implement, and evaluate an ATM machine inside a virtually society. The primary focus is a user accessing their bank branch that they are associated to perform task such as; check balance, deposit, transfer and or withdraw funds at any desired time. Outside of the scope is the interaction between bank network employees and the potential users of the system will not be discussed in depth.

Objectives and Goals

The main objective is to research and clearly understand the requirements of an ATM system, as well as understand the application model requirements for integration with an ATM system simulation. The goal of this research paper is to discuss the planning, analyzing, designing, implementing, testing and evaluating phases of the development of a graphical user interface of an ATM machine model using the software Second Life; virtual world.

Plan the path in which a developer will take to follow for production. Analyze requirements and literature review to understand the entities within the system.

Use OOAD to graphically model users, use cases and scenarios, data and flow diagrams.

Implement the OO model into Second Life by constructing an environment in which the system will possibly be able to operate in. Program objects to function when virtual users wants to perform a task.

Supporting Tools and Resources

The tools used in this research include Enterprise Architect (EA) software which is an advance modeling and design tool formatted in UML; the Interface Design Process Chart to follow a plane in developing a graphical user interface. Scratch building block coding to program objects for functionality as well as Second Life software to design and implement the proposed system in focus.

Microsoft Project 2007 was used to plan out the development of the system. The planner kept a detailed list of task that must be completed as well as providing a calendar to show graphically how far along the developer is on the project as well as keeping aware of deadlines.

Research Project Methodology

Three types of methods were used when developing the GUI for an ATM Machine. The three are known as the Interface Design Process Chart; which is a structured path in planning for development. The Systems Development Life Cycle; which is a process path aiding analysis within a project. As well as Scratch; which is a building block programming system allowing developers to write scripts to objects to perform a function or task.

Interface Design Process Chart

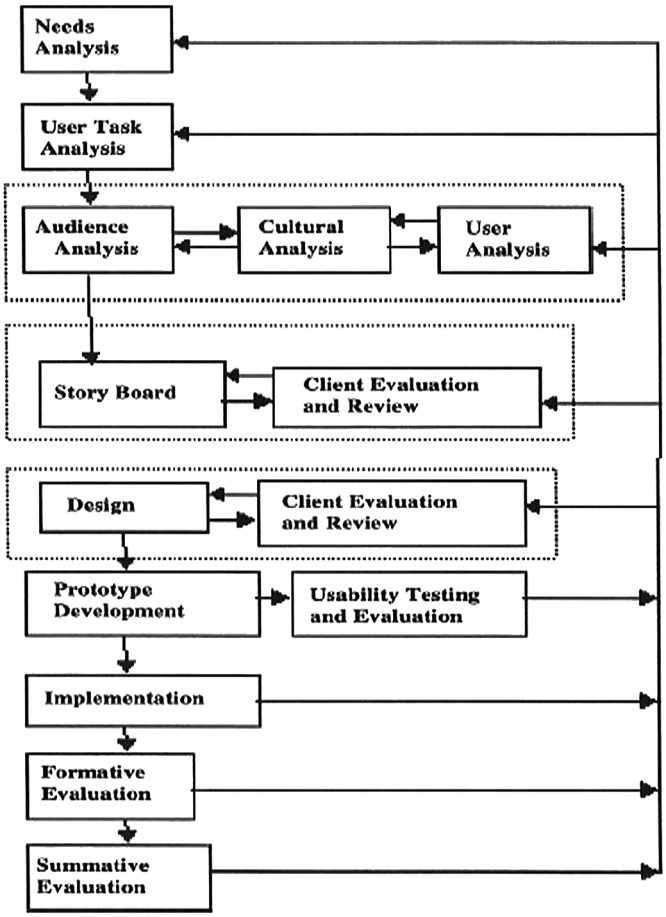
The process path that was used to develop and design the GUI was the Systems Development Life Cycle (SDLC) and Interface Design Process chart shown in Figure 3. The development of the ATM and environment was designed within Second Life which is a part of the design and implementation phases.

The structured path of the development of a successful GUI aids developers. Beginning from the Needs Analysis and continuing to insure users' requirements down to the summarative evaluation shows how each step is repeated for proper development. The path is beneficial because it provided guidance throughout the different planning stages.

Systems Development Life Cycle

The Systems Development Life Cycle (SDLC) consist of steps that will lead a developer to an effective and efficient system; planning, analysis, design, implementation, and maintenance are phases that are required for a successful system shown in Figure 4. The end of one process of a system begins another process. That being said a developer cannot proceed on within a development of a system without completing each process, but a system can repeat a phase if requirements aren't successfully meant by the developer. The first phase is the planning, where an individual identifies the need for a new or enhanced system. Second phase is the analysis where study of the requirements of a system is identified by potential users and current systems. The third phase is the design stage, where the results from the analysts phase is modeled from a logical to a physical design. The fourth phase consist of implementing the system from either documents or models to be coded, tested and or installed into a real life application which the user involvement is an essential to the development of the system in focus. The last phase consists of maintenance where a problem of the developed system has aroused and a better solution has been

Figure 3. Interface design process chart

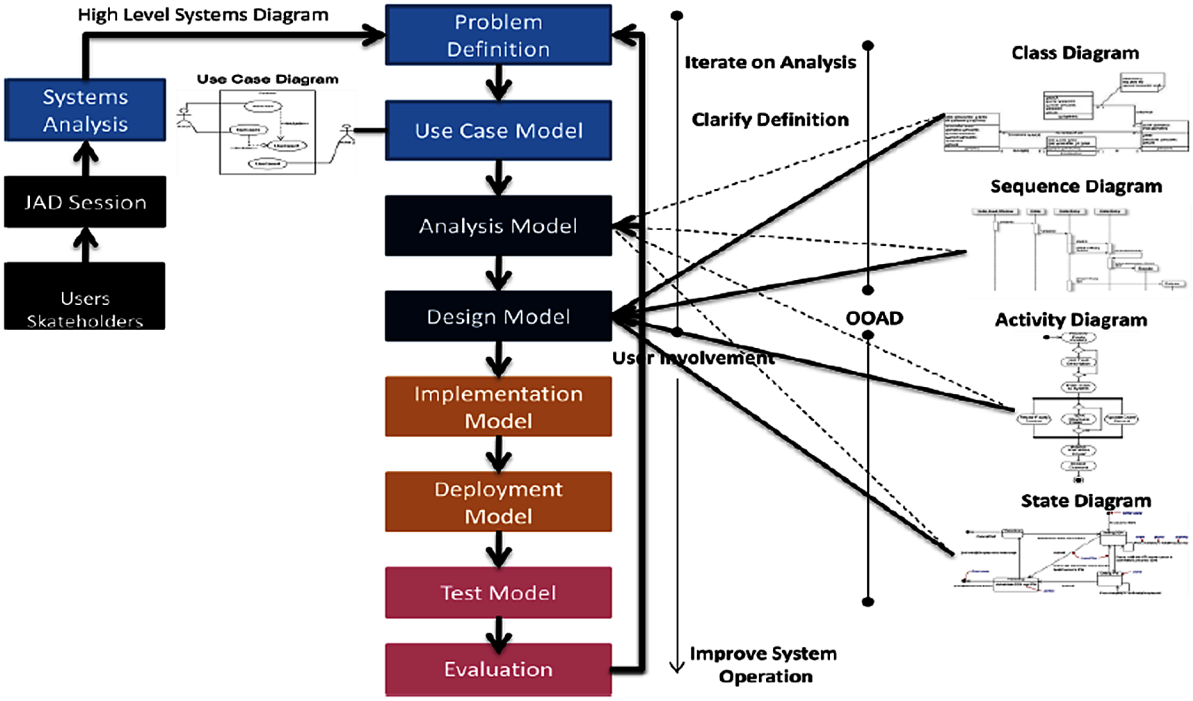


discussed for the system to perform better. This usually occurs after a potential user has tested the system and as mentioned before an error is found.

The diagram that is represented provides the procedures one will pursue in an object oriented (OO) particular approach to solving a problem. It is necessary to follow these procedures when approaching a complex system; beginning with the initial users'; it is necessary to coordinate and communicate with the users of a system to understand the system itself and what the users' want which will take place within a Joint Application Development (JAD) Session where collaboration occurs.

For this particular research, literature review and communication between human users' determined the ATM machine requirements. From the requirements based on the users' needs and resources available, a HLSA was developed resulting in a HLSD to highlight all key components of the system, being able to model a LLSD; which gave a solid focus on what the project goals and objectives were; also known as the projects scope. With a diagram of the system, it was clear to see how complex the system is. A problem definition was determined from the analysis and JAD sessions, which resulted in the analysis and design phase to implementing the project. Within this paper only particular aspects of the OOAD design phase will be addressed.

Figure 4. Systems development life cycle approach



Object Oriented Analysis and Design

Object-Oriented Analysis and Design (OOAD) follows a structure, in which systems can be planned, analyzed, designed, implemented, and tested using models as a graphical representation of the system. A very familiar structure that OOAD follows is known as the System Development Life-Cycle (SDLC) mentioned previously. Object-Oriented Analysis and Design (OOAD) is distributed amongst multiple diagrams in several analysis techniques. Object-Oriented Analysis (OOA) focuses on the techniques on analyzing the requirements for a system. Object-Oriented Design (OOD) focuses on the implementation of the system. "OOA focuses on *what* the system does, OOD on *how* the system does it". Examples of how a system should work are made up of diagrams are used to further enhance the design of a system and the properties within a system. Within the design phase models are constructed from the analysis of the system in focus. Models consist of the Use Case Model as well as their Scenarios. From the Use Case Models, Class diagrams can be constructed as well as Object, Sequence and Activity Diagrams. An OOAD detailed description of the case study of the ATM simulation will be discussed within the Case Study section of this paper.

Use Case and Use Case Scenario

As stated before to have a sufficient outcome of a complex problem the Object-Oriented Analysis and Design approach is considered an efficient approach. Following the Systems Development Life Cycle diagram in Figure 4, the first step in analysis and design would consist of the Use Case Model. In this

project, the goal is to observe the requirements of the ten instruments of a flight deck system. Within the use case modeling, scenarios will be created. The scenarios describe the requirements of this system and their subsystems.

The Use Case Model focuses only on the Actor(s) and requirements of the system. Figure 5 illustrates the use case diagram for the *ATM Machine System.* The ATM machine is composed of seven use cases; that interact to provide the users access to their bank accounts. Use Case scenarios are depicted from the use case requirements, which would allow one to construct a Class Diagram Figure 5 illustrates a close view of a Use Case and its Actors with use case scenarios provided.

Users are represented by Actors because it is an entity that interacts with the system. They are the systems external use because they provide the information that is processed within the system. An Actor can be a person, computer hardware, or device just to name a few for example. The use cases are requirements that must fulfill the environment that it is in. The environment is what surrounds the use cases and separates the users. The particular environment within this project is the ATM Machine system. Built within use cases are scenarios; which are the procedure it takes to fulfill the requirement.

Below are three Case Scenarios from the *ATM Machine* Case Study.

Figure 5. Use case diagram

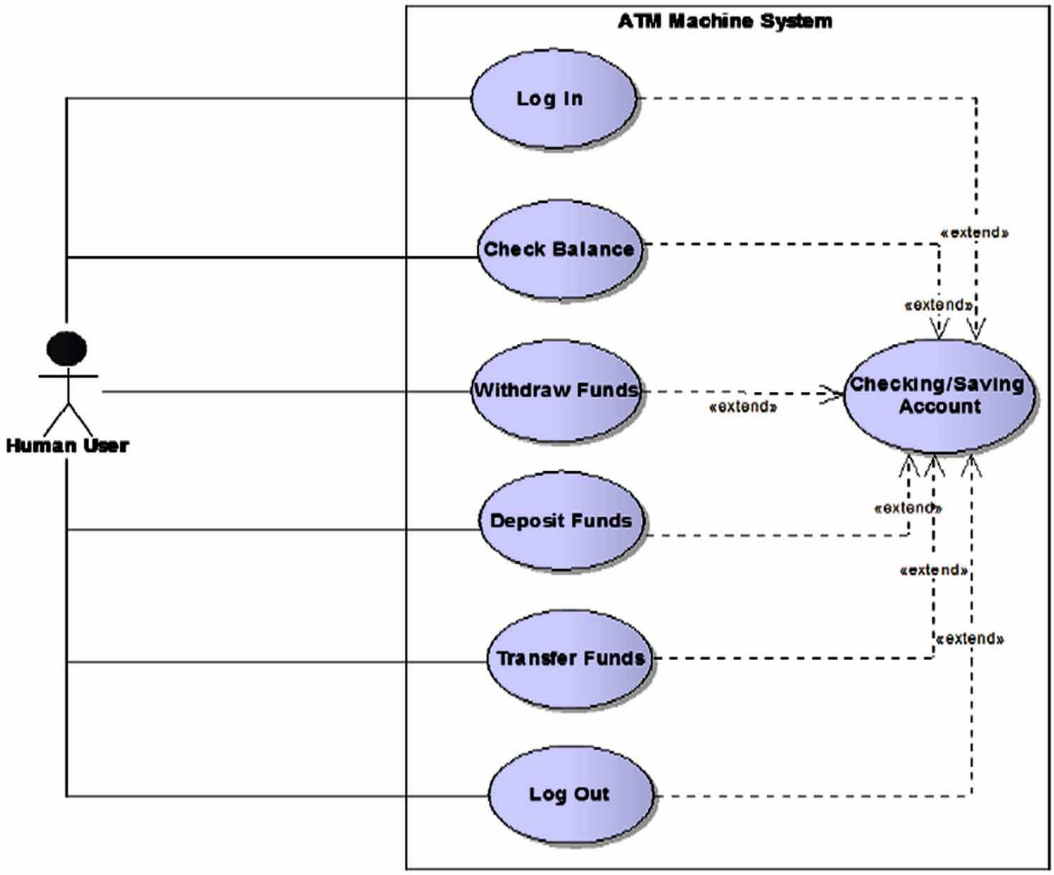
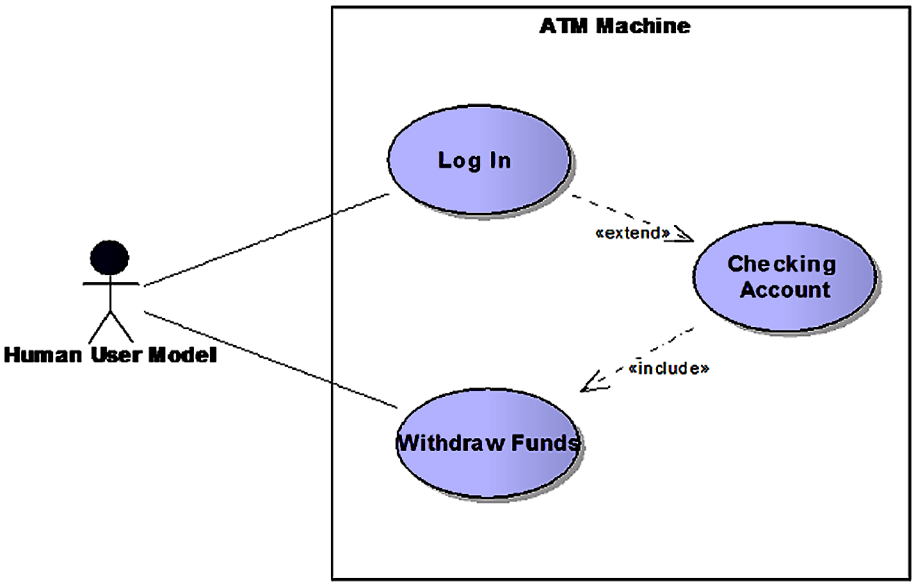


Figure 6. Closer view of "Log In" use case diagram



Login

1. User inserts and remove bank card to be read by ATM Machine.
2. ATM Machine prompts User to enter pin number.
3. User enters pin number.
4. ATM Machine prompts User to either select Checking or Saving Account if correct pin number is entered.
    a. If incorrect pin number is entered the User has 2 more attempts to try to access account before system locks out User and then the User will need to contact their bank branch for further assistance.
5. User selects desired account.
6. ATM Machine prompts User to select a desired task.
7. User either selects: Check Balance, Withdraw Funds, Deposit Funds, or Transfer Funds.
8. ATM Machine sends for request.

Withdraw

1. User selects "Withdraw Funds" task.
2. ATM Machine request selected task.
3. ATM Machine sends message back "Select Amount", only $500 maximum can be withdrawn from the machine.
4. User selects desired amount:
    a. If User has enough funds within their account, the system will process the request.
    b. If User does not have enough funds within their account requested, the system will send a message back "Insufficient Funds" and logs the User out of the system.

5. If request processes, the ATM Machine sends message back "Would You Like A Receipt, Yes or No."
6. If User either selects "Yes",the amount requested and balance of the desired account will be printed on a receipt with desired amount of cash requested.
    a. If User selects "No", ATM Machine request amount of cash desired and sends message to screen " Would You Like Another Transaction, Yes or No."
        i. If User selects "Yes", the system will prompt the User to select another task.
        ii. If User selects "No", the system will ask the User to log out of the system.

Transfer

1. User selects "Transfer Funds" task ATM Machine request selected task.
2. ATM Machine sends message back "Enter Amount Transfer to desired account", No maximum limit can be transfer between accounts.
3. User enters desired amount to transfer, then selects the "Done" option.
4. ATM Machine calculates transfer and sends message back "Would You Like A Receipt, Yes or No."
    a. If User either selects "Yes"; the balance of the desired account will be printed on a receipt.
    b. If User selects "No"; ATM Machine sends message to screen "Would You Like Another Transaction, Yes or No."
        i. If User selects "Yes", the system will prompt the User to select another task.
        ii. If User selects "No", the system will ask the User to log out of the system.

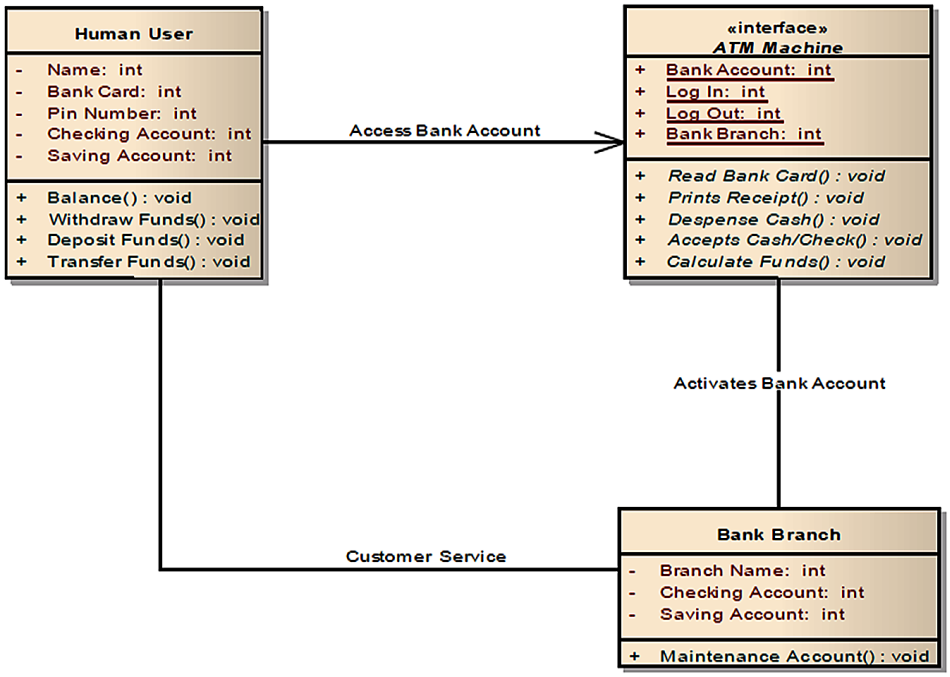
Class Diagram

From the analysis of a use case diagram and its scenario, forms a class diagram. Attributes and operations are expressed which consist of the instruments functions. As well as how the instruments relate and interact with one another. The class diagram gives one a whole visual understanding of how other systems relate to a particular system. A Class is a generic definition for a set of similar objects. It captures and specifies the properties and behaviors that are essential to the system. The Class determines the structure and capabilities of its objects. As stated before, Classes have has attributes and operations.

An attribute are properties or more often things in the real world with name and values. An attribute captures the characteristics of an object. While an operation performs a function in order to provide services to the system also known as a method. Within the model there are indicators that relate to properties and operations. (-) indicate the properties and (+) indicates the operations

Class Diagrams are based off of the analysis of Use Case Diagrams. The *ATM Machine* Use Cases are illustrated in classes with attributes expressed in terms of characteristics and the operations are based on the systems functionality. Figure 7 illustrates the ATM Machine class diagram. This diagram consists of two entities and an interface to work amongst each other within the scope of this research. The ATM Machine is the main instrument in use pertaining to the image. Users must first gain access from the ATM machine before entering their account.

Figure 7. ATM systems class diagram



Object Diagram

Object diagrams originate from class diagrams as well as use case scenarios. The nouns or objects a use case scenario has, represents the potential class diagram for the use cases. Where then an object diagram is constructed with its behaviors and states instead of attributes and operations. An object diagram shows the data of return types for behaviors within a system Objects are self-contained with well defined characteristics. Objects may have many states but cannot act in multiple states at one time. A state would consist of which an object exist in. The states are represented by the values of properties. For example, when a human is in an awake state; they have behaviors such as standing, walking or running. The behavior of an object is related to how an object acts and reacts. Objects behaviors are known as methods and or functions and can be either physical or conceptual.

Physical objects are tangible as well as being visible and touchable for example an automobile. Conceptual objects are intertangible such as a bank account and a time schedule. Within the research project there will be conceptual objects discussed. An Object Diagram represents Class diagrams in depth detail from the use case scenarios. From the use case diagram for the ATM System, there is a use case named "Log In". The use case scenario for the "Log In" is provided in detailed below:

Login

1. User inserts and remove bank card to be read by ATM Machine.
2. ATM Machine prompts User to enter pin number.
3. User enters pin number.

4. ATM Machine prompts User to either select Checking or Saving Account if correct pin number is entered.
    a. If incorrect pin number is entered the User has 2 more attempts to try to access account before system locks out User and then the User will need to contact their bank branch for further assistance.
5. User selects desired account.
6. ATM Machine prompts User to select a desired task.
7. User either selects: Check Balance, Withdraw Funds, Deposit Funds, or Transfer Funds.
8. ATM Machine sends for request.

From the use case scenarios, nouns and or objects can be depicted to construct an Object Diagram. The Class Diagram is a template for objects; the Object diagram can be expressed in Figure 8 with the resulting attributes and operations. These are called behaviors and states.

The object diagram shows the requested access and data return types of the behaviors to detect the ATM and Bank Networks for activation. The ATM system acts as a dependent to access uses accounts and communicate with Bank Networks.

Sequence Diagram

A technique to model various interacting diagrams would consist of a sequence diagram. The sequence shows the passage of time, interaction of objects, and sending messages between the objects. Sequence diagrams are constructed from object diagrams [6].

The sequence diagram shown in Figure 9 illustrates the user activating the ATM system to connect to Bank networks to access accounts. The ATM system connects to Bank Networks and validates users' access code to access their account. The user is now able to select which account they would like to access as well as the desire task in favor.

Figure 8. ATM systems object diagram

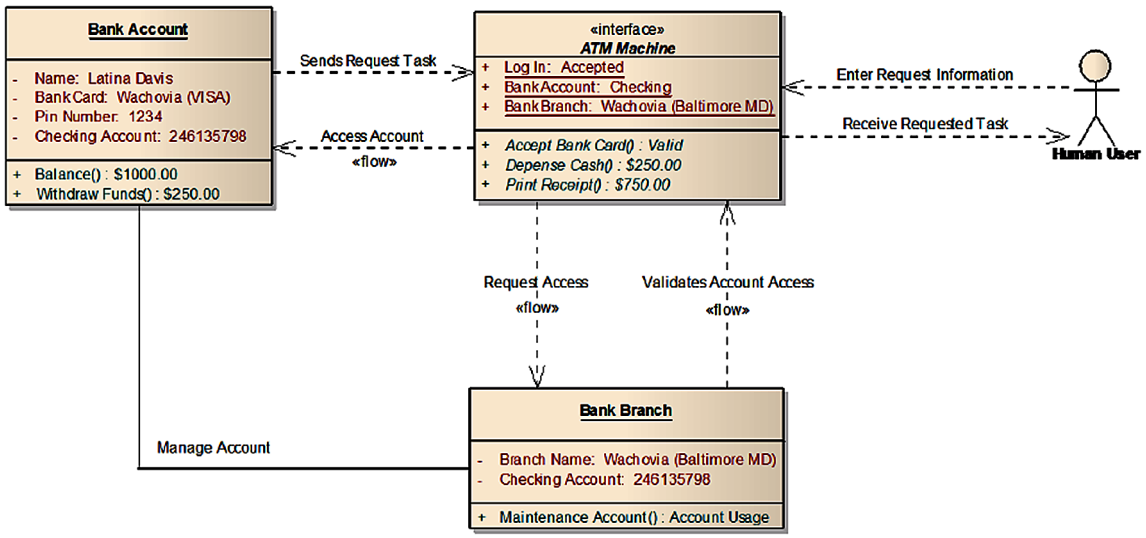
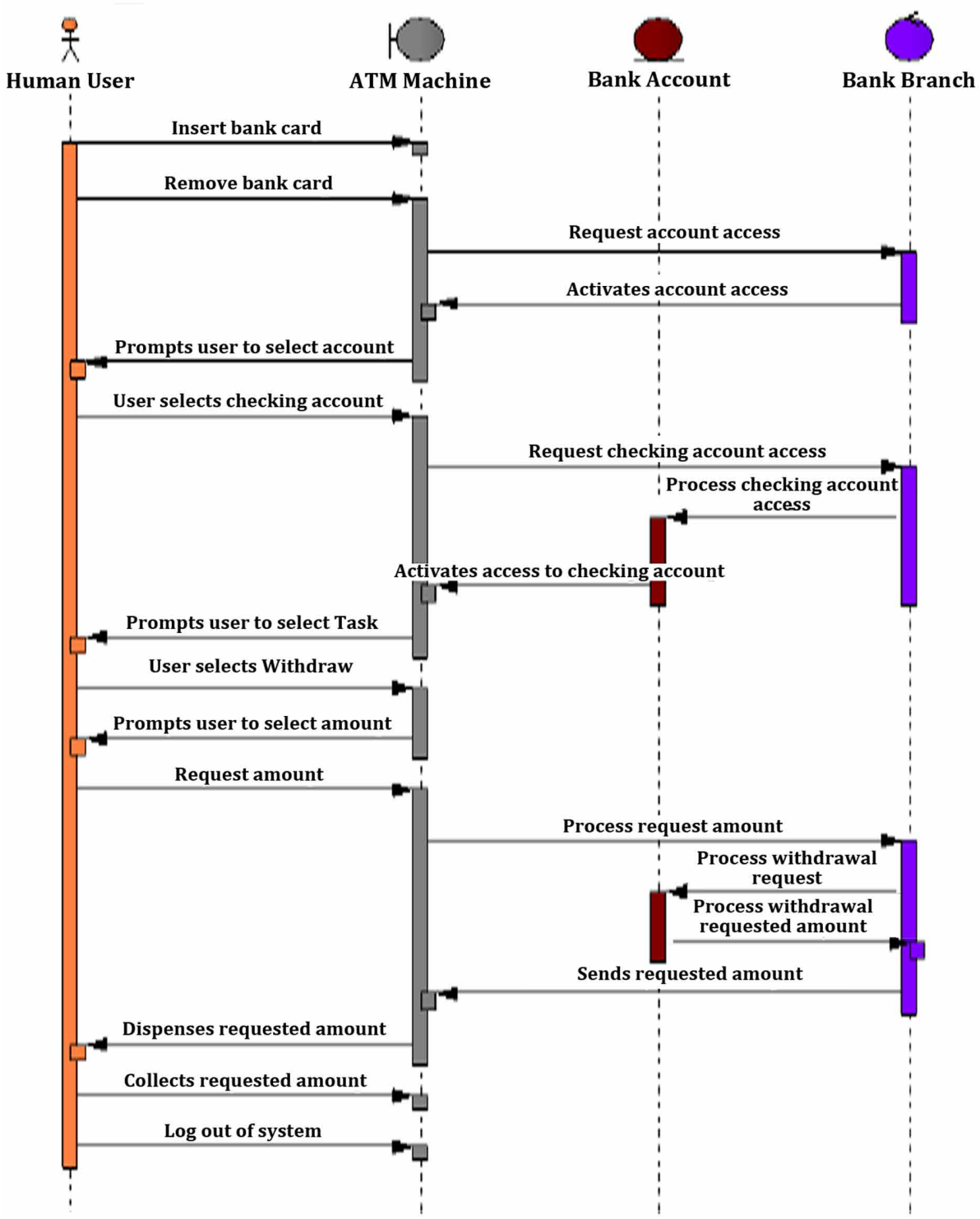


Figure 9. ATM systems sequence diagram



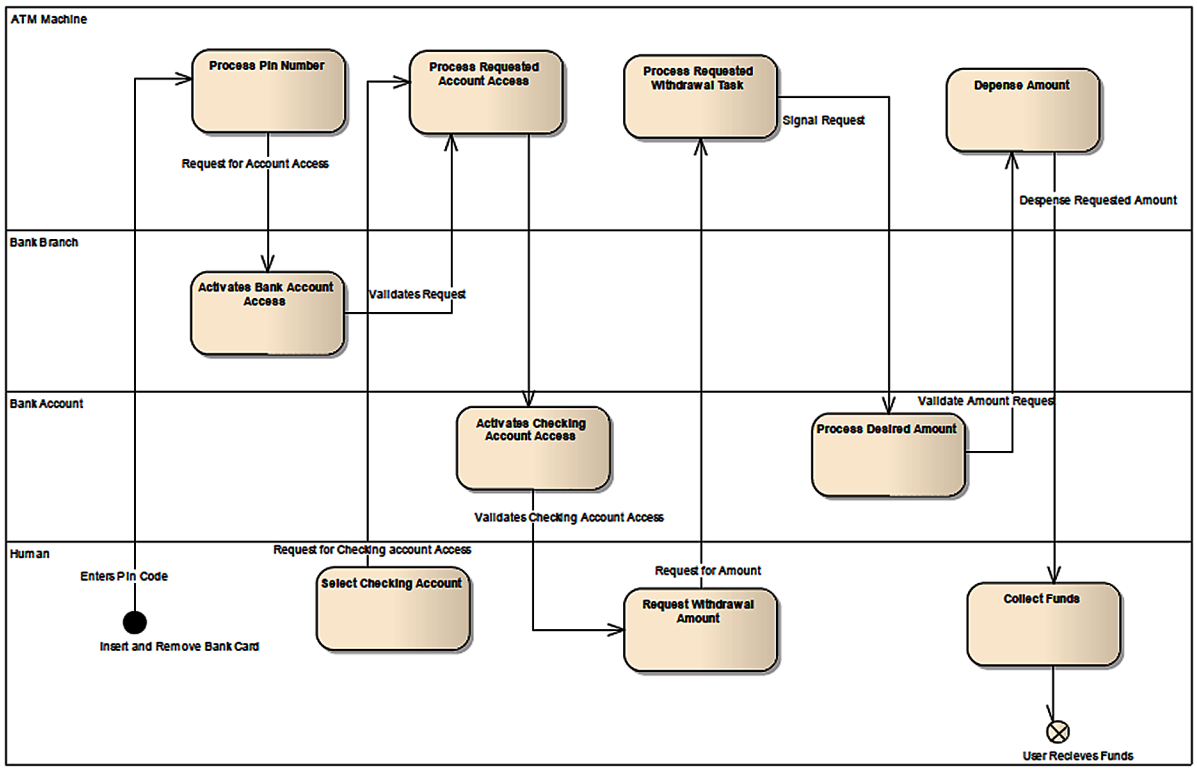
Activity Diagram

To further enhance the design of the *ATM system,* an Activity Diagram was constructed to observe activities within the system of use case "Log In". This is another form of illustrating the behaviors and states of the objects as they interact within the system. Figure 10 illustrates the activity diagram for "Log In".

This particular type of diagram addresses the activities within a use case. The activity blocks are classified as action states. They are used to model a single step throughout the procedure. An activity diagram cannot be decomposed any further. Transitions are represented by an arrow connecting the two action state nodes. A black circle corresponds to the initial start of the process or procedure of the system. The system is complete when there is a circle with an X signifying the process is final. This is another form of illustrating the behavior of the objects as they interact within a system. The Activity Diagram is designed for modeling the performance of actions of a procedure or action within a system.

In the first activity the user inserts their bank card to begin operation, the ATM system send s a signal to the Bank Networks to verify the users; card number. The ATM receives confirmation to allow the user to enter their pin code; if the pin code is valid the ATM system and Bank Network allows the user to have access to their account. The user is now able to select one out of the four options available, one at a time. When the user is done they are able to notice the ATM system that they have completed their transaction and wish to "Log Out" of the system; which is another use case of its own.

Figure 10. ATM system activity diagram



ATM Second Life Model

Second Life is an online virtual world, where people can socialize and connect with other people all over the world. It has been used to teach classes, concerts, and stores to name a few situations. People are able to buy, trade, learn and create their own world. Second Life Market was used to buy objects to write scripts to for the objects within the system will operate; such as furniture, screens, boats, and kiosk to name a few. The software can be used to virtually represent a system or an environment of its proposed operations. In Figure 11 the Second Life environment described can be observed. The furniture, pay phone, plants, ATM Machine objects and building was bought from the Second Life Market and the scratch software was implemented into the scripts of the ATM Machine objects to satisfy the development of the GUI in focus.

The primary purpose to this system is to develop a test plan to implement an analyzed system into a virtual world. The GUI system designed to be the ATM system will be developed within in the Second Life software. The users within Second Life will be able to touch the ATM system and the scripts will show within the chat log. The ATM system will "Welcome" the users and prompt the users to enter their pin number and select if they either would want to access their "Checking or Saving Account". The system will then prompt the users to check their balance, withdraw, deposit or transfer funds within their account. Finally the system will notify the users that they have successfully completed their transaction and are logged out of the system with a notice displaying "Thank You" which completes the process. The use of scripts was used to generate when users "touch" the ATM, the time frame between each statement is 1 second. Total time it should take for users to complete the process within Second Life should be about 8 to 10 seconds long. Recording time started when subjects touched and activated the systems script.

Figure 11. Second Life ATM machine simulation

SECOND LIFE RESULTS

Subject Model 1

The first subject is a female ranging between the ages of 25 – 30. The subject decided out of the two ATM Machines she wanted to explore. The subject decided to interact with the ATM Machine closer to the entrance and exit of the environment; shown in Figure 12.

Subject 1 Results

1. **Time to complete test module:** 8 seconds
2. **Time to select and touch ATM object and run script:** 1 second
3. **Time to Complete Script:** Approximately 1 second per line

Subject Model 2

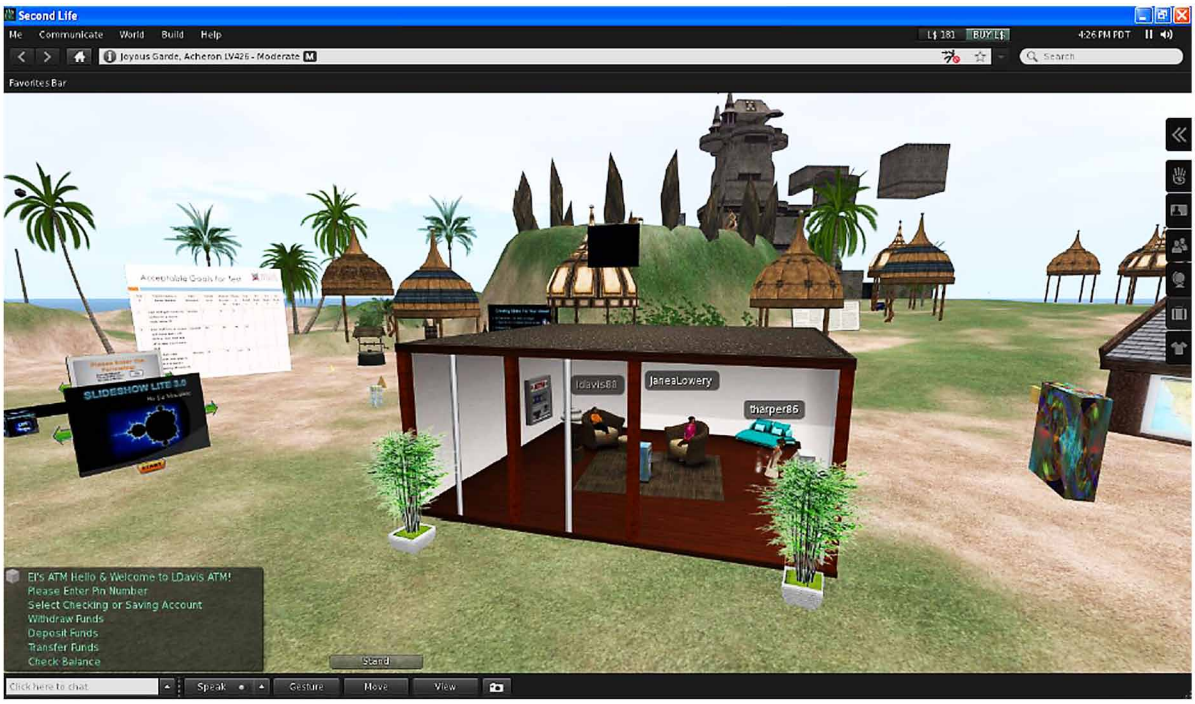
The second subject is a female ranging between the ages of 25 – 30. The subject decided out of the two ATM Machines she wanted to explore. The subject decided to interact with the ATM Machine further from the entrance and exit of the environment; shown in Figure 13.

Subject 2 Results

1. **Time to complete test module:** 12 seconds
2. **Time to select and touch ATM object and run script:** 3 second
3. **Time to Complete Script:** Approximately 1 second per line

Figure 12. Subject 1 module

Figure 13. Subject 2 module



Subject Model 3

The third subject is a male ranging between the ages of 25 – 30. The subject decided out of the two ATM Machines he wanted to explore. The subject decided to interact with the ATM Machine closer to the entrance and exit of the environment; shown in Figure 14.

Subject 3 Results

1. **Time to complete test module:** 10 seconds
2. **Time to select and touch ATM object and run script:** 2 second
3. **Time to Complete Script:** Approximately 1 second per line

Project Conclusion

In conclusion a GUI of an ATM Machine has been produced and integrated with the scratch software to program scripts within the objects of the system. Three types of methodologies were used to plan, analyze, design, implement, test and evaluate the developed system within this paper. Beginning from the initial problem definition and users' requirements a HLSA was proposed resulting into graphically modeling the system with HL and LL systems diagrams. This allowed the developers to capture the main important entities within this project.

Figure 14. Subject 3 module

Once analyzing the problem and system a plan for design was implemented into Enterprise Architect (EA) using the SDLC OOAD methodology. The idea then lead to purchasing objects from the Second Life Market to use as prototypes within the environment of Second Life. Difficulties aroused while using the software Second Life. Difficulties such as programming objects as well as receiving objects from the market; some objects were unable to be modified and required to purchase other objects that would cooperate with the proposed system and environment. The overall experience was interesting in learning to plan a development of a GUI.

Future work will be to present the development process of the research project as well as further enhance knowledge within Second Life to use an effective tool in simulation work.

CONCLUSION

As technology is continuously changing the landscape of learning and teaching in America U-Learning has to be taken seriously. It is essential that learning institutions increase interaction, and productivity to ensure survival which increasing overall participation. The creation of learning objects for virtual worlds will decrease the course and lab development time for professors. Additionally, it will provide instructors the ability to teach interactive concepts of object oriented design and code reuse. The use of virtual learning environments helps enable systems engineering and technology programs integrate with modern technologies such as wearables. As learning occurs more in distance education the use of virtual learning environments needs to be further explored.

REFERENCES

Ahlemann, F., Teuteberg, F., & Vogelsang, K. (2009). Project management standards–Diffusion and application in Germany and Switzerland. *International Journal of Project Management*, *27*(3), 292–303. doi:10.1016/j.ijproman.2008.01.009

Boss, S., & Krauss, J. (2007).Reinventing Project-Based Learning: Your Field Guide to Real-World Projects in the Digital Age. International Society for Technology in Education.

Boulos, M. N. K., Hetherington, L., & Wheeler, S. (2007). Second Life: An overview of the potential of 3-D virtual worlds in medical and health education. *Health Information and Libraries Journal*, *24*(4), 233–245. doi:10.1111/j.1471-1842.2007.00733.x PMID:18005298

Dawson, M., Al Saeed, I., Wright, J., & Omar, M. (2013). Technology Enhanced Learning with Open Source Software for Scientists and Engineers. *INTED2013 Proceedings*, 5583-5589.

Dawson, M., Al Saeed, I., Wright, J., & Onyegbula, F. (2015). Open Source Software to Enhance the STEM Learning Environment. In Open Source Technology: Concepts, Methodologies, Tools, and Applications (pp. 1493-1503). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-7230-7.ch075

Dawson, M. E., & Al Saeed, I. (2012). Use of Open Source Software and Virtualization in Academia to Enhance Higher Education Everywhere. *Cutting-edge Technologies in Higher Education*, *6*, 283–313. doi:10.1108/S2044-9968(2012)000006C013

Doran, T. (2006). IEEE 1220: For practical systems engineering. *Computer*, *39*(5), 92–94.

Durán, E. B., Álvarez, M. M., & Únzaga, S. I. (2014, April). Ontological model-driven architecture for ubiquitous learning applications. In *Proceedings of the 7th Euro American Conference on Telematics and Information Systems* (p. 14). ACM. doi:10.1145/2590651.2590776

Ghezzi, C., Jazayeri, M., & Mandrioli, D. (2002). *Fundamentals of software engineering*. Prentice Hall PTR.

GNU. (2007). *GNU General Public License.* Retrieved April 25, 2012 from http://www.gnu.org/copyleft/gpl.html

Gray, L. (1999). *A Comparison of IEEE/EIA 12207, ISO/IEC 12207, J-STD-016, and MIL-STD-498 for Acquirers and Developers*. Fairfax, VA: Abelia Corporation.

Haskins, C. (Ed.). (2007). *INCOSE Systems Engineering Handbook: A Guide for Sytem Life Cycle Processes and Activities*. INCOSE.

Hawker, J. S. (2009). *A software process engineering course*. Academic Press.

Hofmann, H. F., & Lehner, F. (2001). Requirements engineering as a success factor in software projects. *IEEE Software*, (4), 58-66.

IEEE Computer Society. Software Engineering Standards Committee, & IEEE-SA Standards Board. (1998). IEEE Recommended Practice for Software Requirements Specifications. Institute of Electrical and Electronics Engineers.

IEEE Standards Association. (1998). *IEEE Std 1062–1998 IEEE Recommended Practice for Software Acquisition*. Author.

IEEE Standards Coordinating Committee. (1990). *IEEE Standard Glossary of Software Engineering Terminology (IEEE Std 610.12-1990)*. Los Alamitos, CA: IEEE Computer Society.

INCOSE. (2015). *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. John Wiley & Sons.

Jacobs, S., Kussmaul, C., & Sabin, M. (2011). Free and open source software in computing education. *Proceedings of the 2011 conference on Information technology education*.

Kaghed, N., & Dezaye, A. (2009). Quality Assurance Strategies of Higher Education in Iraq and Kurdistan: A Case Study. *Quality in Higher Education*, *15*(1), 71–77. doi:10.1080/13538320902731286

Kemp, J. W., Livingstone, D., & Bloomfield, P. R. (2009). SLOODLE: Connecting VLE tools with emergent teaching practice in Second Life. *British Journal of Educational Technology*, *40*(3), 551–555. doi:10.1111/j.1467-8535.2009.00938.x

Kharrufa, A., Martinez-Maldonado, R., Kay, J., & Olivier, P. (2013, October). Extending tabletop application design to the classroom. In *Proceedings of the 2013 ACM international conference on Interactive tabletops and surfaces* (pp. 115-124). ACM. doi:10.1145/2512349.2512816

Lee, J. W., Jung, S. H., Park, S. C., Lee, Y. J., & Jang, Y. C. (2005, August). System based SQA and implementation of SPI for successful projects. In *Information Reuse and Integration, Conference, 2005. IRI-2005 IEEE International Conference on* (pp. 494-499). IEEE.

LTSC. (2000a). *Learning technology standards committee website*. Available:http://ltsc.ieee.org/

LTSC. (2000b). *IEEE standards board: Project authorization request (PAR) form.* Available: https://ieee-sa.centraldesktop.com/ltsc/

Martínez-Costa, M., Choi, T. Y., Martínez, J. A., & Martínez-Lorente, A. R. (2009). ISO 9000/1994, ISO 9001/2000 and TQM: The performance debate revisited. *Journal of Operations Management*, *27*(6), 495–511. doi:10.1016/j.jom.2009.04.002

Martinez-Maldonado, R., Dimitriadis, Y., Clayphan, A., Muñoz-Cristóbal, J. A., Prieto, L. P., Rodríguez-Triana, M. J., & Kay, J. (2013, November). Integrating orchestration of ubiquitous and pervasive learning environments. In *Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration* (pp. 189-192). ACM. doi:10.1145/2541016.2541076

Martinez-Maldonado, R., & Kay, J. (2013). Open learner models to support reflection on brainstorming at interactive tabletops. In *Proc. AIED 2013*, (pp. 683-686).

Möller, D. P., Haas, R., & Vakilzadian, H. (2013, July). Ubiquitous learning: teaching modeling and simulation with technology. In *Proceedings of the 2013 Grand Challenges on Modeling and Simulation Conference* (p. 24). Society for Modeling & Simulation International.

Moore, J. W. (1998). *Software engineering standards*. John Wiley & Sons, Inc.

Ogata, H., & Yano, Y. (2012). *Context-aware Support for Computer-Supported Ubiquitous Learning*. Retrieved from http://140.115.126.240/mediawiki/images/e/e9/Context_Awareness.pdf

Pan, G., & Bonk, C. (2007). The emergence of open-source software in north America. *International Review of Research in Open and Distance Learning*, *8*(3).

Perens, B. (1999). The open source definition. In *Open sources: Voices from the open source revolution* (pp. 171–185). Academic Press.

Rooij, S. W. (2009). Adopting open-source software applications in U.S. higher education: A cross-disciplinary review of the literature. *Review of Educational Research*, *79*(2), 682–701. doi:10.3102/0034654308325691

Rowell, L. (2008). Open source software: finding its place in higher education. *eLearn 2008.Global Engineering Education Conference (EDUCON)*. IEEE. doi:10.1145/1361066.1361070

Schneider, F., & Berenbach, B. (2013). A literature survey on international standards for systems requirements engineering. *Procedia Computer Science*, *16*, 796–805. doi:10.1016/j.procs.2013.01.083

Shishko, R., & Aster, R. (1995). NASA systems engineering handbook. *NASA Special Publication*, 6105.

Toth, K. (2006). Experiences with open source software engineering tools. *IEEE Software*, *23*(6), 44–52. doi:10.1109/MS.2006.158

Vincenti, G. (Ed.). (2010). *Teaching through Multi-User Virtual Environments: Applying Dynamic Elements to the Modern Classroom: Applying Dynamic Elements to the Modern Classroom*. IGI Global. doi:10.4018/978-1-61692-822-3

Westfall, L. (2008). *The certified software quality engineer handbook*. ASQ Quality Press.

Wiley, D. A. (2000). Connecting learning objects to instructional design theory: A definition, a metaphor, and a taxonomy. In D. A. Wiley (Ed.), *The Instructional Use of Learning Objects: Online Version*. Retrieved October 3, 2015, from http://reusability.org/read/chapters/wiley.doc

KEY TERMS AND DEFINITIONS

Linux: An open source version of the UNIX OS (Perens, 2009).

Open Source Software: Software that allows the original source code to be free available which may be freely redistributed or modified (Perens, 2009).

Requirements Engineering: Per IEEE this refers to the process of defining, documenting, and maintaining requirements for a program. This can be applied to systems and software engineering (IEEE Computer Society, 1998).

Quality Management: A process that ensures products or systems meet a specific standard (Westfall, 2008).

Second Life: An online virtual world, where people can socialize and connect with other people all over the world (Boulos, Hetherington, & Wheeler, 2007).

Software Engineering: A discipline that focuses on the application of engineering to the design, development, integration, and maintenance of software (Ghezzi et al, 2002).

Systems Engineering: An interdisciplinary field within engineering that is focused on complex systems and managing their associated life cycle. (Shishko & Aster, 1995).

Developing Next-Generation Countermeasures for Homeland Security Threat Prevention

Maurice Dawson
University of Missouri-St. Louis, USA

Dakshina Ranjan Kisku
National Institute of Technology, India

Phalguni Gupta
National Institute of Technical Teachers' Training & Research, India

Jamuna Kanta Sing
Jadavpur University, India

Weifeng Li
Tsinghua University, China

A volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

IGI GLOBAL
DISSEMINATOR OF KNOWLEDGE

www.igi-global.com

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Dawson, Maurice, 1982- editor.
Title: Developing next-generation countermeasures for homeland security threat prevention / Maurice Dawson, Dakshina Ranjan Kisku, Phalguni Gupta, Jamuna Kanta Sing and Weifeng Li, editors.
Description: Hershey, PA : Information Science Reference, [2017] | Includes bibliographical references and index.
Identifiers: LCCN 2016023422| ISBN 9781522507031 (hardcover) | ISBN 9781522507048 (ebook)
Subjects: LCSH: Terrorism--United States--Prevention. | Terrorism--Prevention. | National security--United States. | Internal security--United States.
Classification: LCC HV6432 .D48 2017 | DDC 363.325/170973--dc23 LC record available at https://lccn.loc.gov/2016023422

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 10
Battlefield Cyberspace: Exploitation of Hyperconnectivity and Internet of Things

Maurice Dawson
University of Missouri – St. Louis, USA

Marwan Omar
Saint Leo University, USA

Jonathan Abramson
Post University, USA

Brian Leonard
Alabama A&M University, USA

Dustin Bessette
National Graduate School of Quality Management, USA

ABSTRACT

The threat of cyber terrorism has become a reality with recent attacks such as Stuxtnet, Flame, Sony Pictures, and North Korea's websites. As the Internet of Things (IoT) continues to become more hyperconnected it will be imperative that cyber security experts to develop new security architectures for multiple platforms such as mobile devices, laptops, embedded systems, and even wearable displays. The futures of national and international security rely on complex countermeasures to ensure that a proper security posture is maintained during this state of hyperconnectivity. To protect these systems from exploitation of vulnerabilities it is essential to understand current and future threats to include the laws that drive their need to be secured. Examined within this chapter are the potential security related threats with the use of social media, mobile devices, virtual worlds, augmented reality, and mixed reality.

DOI: 10.4018/978-1-5225-0703-1.ch010

BACKGROUND ON RESEARCH

For years, experts and government officials have warmed of cyber terrorism as a threat to nation security (Cavelty, 2008). These malicious attacks can affect one single person to entire government entities. These attacks can be done with a few lines of code or large complex programs that have the ability to target specific hardware. The authors investigate the attacks on individuals, corporations, and government infrastructures throughout the world. Provided will be specific examples of what a cyber terrorist attack is and why this method of attack is the preferred method of engagement today. The authors will also identify software applications, which track system weaknesses and vulnerabilities. As the United States government has stated, an act of cyber terrorism is an act of war; it is imperative that we explore this new method of terrorism and how it can be mitigated to an acceptable risk.

Information assurance (lA) is defined as the practice of protecting and defending information and information systems by ensuring their availability, integrity, authentication, confidentiality and non repudiation. This definition also encompasses disaster recovery, physical security, cryptography, application security, and business continuity of operations. To survive and be successful, an enterprise must have a disaster recovery strategy and response plan in place to mitigate the effects of natural disasters (e.g., floods, fires, tornadoes, earthquake, etc.), inadvertent actions by trusted insiders, terrorist attacks, vandalism, and criminal activity. In order to lay the groundwork for this review properly, it is essential to detail current processes techniques being utilized by officials within the government to accredit and certify systems to include their TA enabled products (Dawson, Jr., Crespo, & Brewster, 2013).

Cyber security has become a matter of national, international, economic, and societal importance that affects multiple nations (Walker, 2012). Since the 1990s users have exploited vulnerabilities to gain access to networks for malicious purposes. In recent years, the number of attacks on United States networks has continued to grow at an exponential rate. This includes malicious embedded code, exploitation of backdoors, and more. These attacks can be initiated from anywhere in the world from behind a computer with a masked Internet Protocol (IP) address. This type of warfare, cyber warfare, changes the landscape of war itself (Beidleman, 2009). This type of warfare removes the need to have a physically capable military and requires the demand for a force that has a strong technical capacity e.g. computer science skills. The United States (U.S.) and other countries have come to understand that this is an issue and has developed policies to handle this in an effort to mitigate the threats.

ln Estonia and Georgia there were direct attacks on government cyber infrastructure (Beidleman, 2009). The attacks in Estonia rendered the government's infrastructure useless. The government and other associated entities heavily relied upon this e-government infrastructure. These attacks help lead to the development of cyber defense organizations that drive laws and policies within Europe.

LAWS AND POLICIES TO COMBAT TERRORISM

The events of 9/ll not only changed policies with the U.S. but also policies with other countries in how they treat and combat terrorism. The United Nations (U.N.) altered Article 51 of the U.N. charter. This article allows members of the U.N. to take necessary measures to protect themselves against an armed attack to ensure international peace and security.

Israel is a country with some of the most stringent policies towards national and international security. This country requires all citizens to serve in the military to include multiple checkpoints throughout the country. This country has utilized stringent checks in the airport long before 9/11, however, now they have additional measures to ensure the nation's security as they are surrounded by countries that have tried to invade before. Israel has also deployed more Unmanned Air Vehicles (UAVs), and Unmanned Ground Vehicles (UGVs) to patrol the border in the event something occurs.

The United Kingdom (U.K.) has the Prevention of Terrorism Act 2005 and the Counter-Terrorism Act 2008 which was issued by Parliament. The first act was created to detain individuals who were suspected in acts of terrorism. This act was intended to replace the Anti-terrorism, Crime and Security Act 200 I as it was deemed unlawful. These acts seem to mirror the same ones, created in the U.S., to monitor potential terrorists and terrorists. The U.K. also shared their information with the U.S. for coordinating individual that may be of risk.

In the U.S., the methods for national security were enhanced to ensure no threats occur on U.S. soil. These changes include enhanced security in all ports of entry. The signing of the Homeland Security Act of 2002 (HS Act) (Public Law 07-296) created an organization that received funding and lots of resources for monitoring the security posture of this country. Additional changes include enhanced monitoring of citizens and residents within the country to prevent terrorist activities by the mention of key words e.g. bomb, explosive, or Al Qaeda.

The USA PATRIOT was signed into law by President George W. Bush in 2001 after September 11, 200 I (Bullock, Haddow, Coppola, & Yeletaysi, 2009). This act was created in response to the event of 9111 which provided government agencies increased abilities. These increased abilities provided the government rights to search various communications such as email, telephone records, medical records, and more of those who were thoughts of terrorist acts (Bullock, Haddow, Coppola, & Yeletaysi, 2009). This allowed law enforcement to have the upper hand in being proactive to stopping potential acts against U.S. soil. In the 2011 year, President Obama signed an extension on the USA PATRIOT Act. This act has received criticism from the public due to the potential to be misused or abused by those in power. This act has allowed government agencies to impede on constitutional rights.

The Protecting Cyberspace as a National Asset Act of 2010 was an act that also amends Title 11 of the Homeland Security Act of 2002. This act enhanced security and resiliency of the cyber and communication infrastructure within the U.S. This act is important as the President declared that any cyber aggressions would be considered an act of war. This is also important as Estonia's entire digital infrastructure was taken down by hackers who supported the former Soviet rule. This type of attack could be damaging to the infrastructure in the U.S.- causing loss of power for days or more which could result **in** death. In an area, such as the Huntsville Metro, we could have multiple nuclear facility melt downs, loss of lSR capabilities, and communication to the warfighter that we are supporting.

Additional changes from this act include the ability to carry out a research and development program to improve cyber security infrastructure. At the moment all government organizations must comply with the Federal Information Security Management Act (FlSMA) of 2002. This act has shown many holes within the U.S. cyber security infrastructure to include those organizations that are leads. This act provides DHS the ability to carry out the duties described in the Protecting Cyberspace as a National Asset Act of 2010.

Stuxnet Worm

During the fall of 20 l 0 many headlines declared that Stuxnet was the game-changer in terms of cyber warfare (Denning, 2012). This malicious worm was complex and designed to target only a specific system. This worm had the ability to detect location, system type, and more. And this worm only attacked the system if it met specific parameters that were designed in the code. Stuxnet tampered directly with software in a programmable logic controller (PLC) that controlled the centrifuges at Natanz. This tampering ultimately caused a disruption **in** the Iranian nuclear program.

America's Homeland Security Preparing for Cyber Warfare

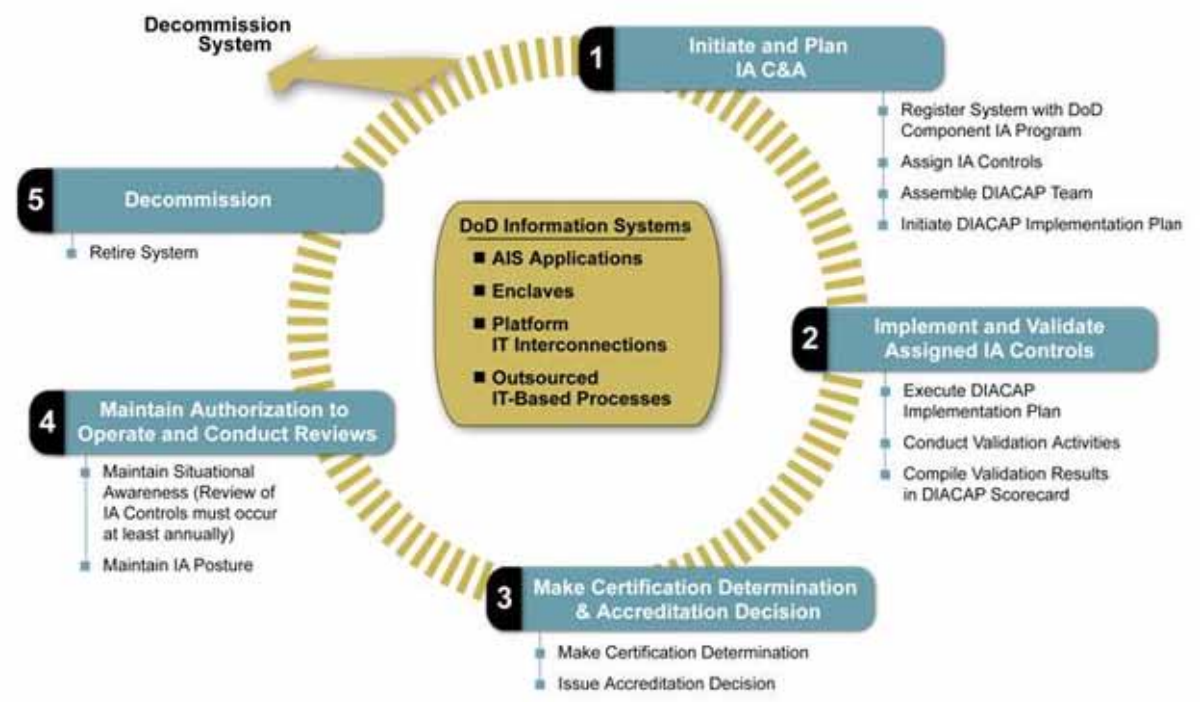
The Department of Homeland Security (DHS) is concerned with cyber attacks on infrastructure such as supervisory control and data acquisition (SCADA) systems. SCADA systems are the systems that autonomously monitor and adjust switching among other processes within critical infrastructures such as nuclear plants, and power grids. DHS is worried about these systems as they are unmanned frequently and remotely accessed. As they are remotely accessed, this could allow anyone to take control of assets to critical infrastructure remotely. There has been increasing mandates and directives to ensure any system deployed meets stringent requirements. As the Stuxnet worm has become a reality, future attacks could be malicious code directly targeting specific locations of critical infrastructure.

Cyber Security Certification and Accreditation Processes to Secure Systems

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is the process that the Department of Defense (DoD) utilizes to ensure that risk management is applied to Automated Information Systems (AIS) to mitigate IA risks and vulnerabilities (Dawson, Jr., Crespo, & Brewster, 2013). DIACAP is the standard process that all services utilize to ensure that all DoD systems maintain IA posture throughout the systems life cycle. DIACAP is the replacement of the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). Figure 1 displays the process which includes five key steps. The first step is to initiate and plan the IA C & A process. The second step is to implement and validate the assigned IA controls. The third step is to make the certification determination and accreditation decision. The fourth step is to maintain authorization to operate and conduct reviews. The final step is to decommission the system.

The Common Criteria (CC), an internationally approved set of security standards, provides a clear and reliable evaluation of security capabilities of Information technology (IT) products (CCEVS, 2008). By providing an independent assessment of a product's ability to meet security standards, the CC gives customers more confidence in the security of products and leads to more informed decisions (CCEVS, 2008). Since the requirements for certification are clearly established, vendors can target very specific security needs while providing users from other countries to purchase IT products with the same level of confidence, since certification is recognized across all complying nations. Evaluating a product with respect to security requires identification of customer's security needs and an assessment of the capabilities of the product. The CC aids customers in both of these processes through two key components: protection profiles and evaluation assurance levels (CCEVS, 2008).

Figure 1. DIACAP Stages
(Department of Defense, 2007)



The CC is the process that replaced the Orange Book. The CC has evaluated assurance levels (EAL) 1 through 7. EAL products 1 through 4 may be used and certified in any of the participating countries. However, EAL 5 through 7 must be certified by the countries national security agency, that is the United States' national agency is the National Security Agency and United Kingdom's national agency is the Communication Electronics Security Group (CESG). By all accounts, the NSA'a Orange Book program, in which the NSA forced vendors through prolonged product testing at Fort Meade, MD was a dismal failure. Also, the government's failure to Orange-Book-tested products, which were often out of date after years of testing, was a blow to the vendors that invested huge sums in the Orange Book Evaluations.

Additionally the National Security Agency (NSA) and DHS sponsors a joint venture known as the National Centers of Academic Excellence in IA Education (CAE/IAE), IA 2-year Education and Training (CAE/2Y) and lA Research (CAE/R) programs. Students that attend institutions with these designations are eligible to apply for scholarships and grants which they repay through government service. These programs were created to address the lack of available talent in lA. Table 1 shows the Committee on National Security Standards (CNSS) that institutions must map to in order to receive the designation as a NSA/IAE.

Since the purpose was to expand the numbers of lA personnel, it is hard to evaluate the program's real success (Bishop & Taylor, 2009). One of the major problems is the lack of resources to all institutions who are NSA/IAE. Even though this program is targeted towards post high school efforts, more reforms are currently taking place in the K-12 educational areas.

Table 1. CNSS training standards

Standard Name	Year	Description
NSTTSSI 4011	1994	Information Systems Security Professionals
CNSSI 4012	2004	Senior Systems Manager
CNSIS 4013	2004	System Administrators in Information Systems Security
CNSSI 4014	2004	Information Systems Security Officer (ISSO)
NSTTSSI 4015	2000	System Certifiers
CNSSI 4016	2005	Risk Analysis

Human Computer Interaction

Future national and international threats that will be directly correlated to the Internet will be many as more devices are added to the Internet the problem of security also multiplies. Richard Clarke mentions that there are currently 12 bill ion device currently connected to the Internet; this figure is supposed to grow to 50 billion in ten years (Clarke, 2012). Our dependence and interdependence with the Internet creates new challenges as the more devices that are put online, the more exposure or vectors we are creating. The number of devices on the Internet is growing exponentially. As more applications for technology and wireless technologies are adopted, we are going to see this grow even further. What comes to mind are the self-driving vehicles that will be coming in a few years. We already have some self-driving cars, but they are not widely adopted yet or available to the public. When this does happen, we are going to see another exponential growth rate and the number of connected devices as each automobile will constitute at least a single IP address if not probably more.

Communication is the on-going and never ending process through which we create our social reality. Never in history has this been truer, as the computing and communication platforms that we have today far exceed anything that has ever been planned or projected. Information technology has radically altered the process in the way people learn and communicate. Weiser notes the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it (Weiser, 1991). An example has been the explosive growth ofSMS texting, email, and social media. As these technologies are weaved into our lives, so are the dangers.

Research Projects

Many of the research projects that have taken place in mixed reality have been in educational domains and military domains. The focus of mixed reality research and education is to expand the capability of students to learn and interact and retain constructed knowledge and for businesses to maximize the knowledge that they have. Interesting new ways of looking at problems and topical areas enhance the learning experience and enhance capabilities, such as the ability to create a physical environment when it does not exist in the real world. Park et al. 2008, studied human behavior in urban environments using human subjects in a virtual environment which demonstrated that virtual reality and mixed reality have the capability to model human behavior and that the products of these research projects are useful and may save time and money. Tn many situations, they provide an environment for simulation and analysis and design that would not be possible in the real world.

Most mixed reality devices, at this point, are ruling on the Internet or another networks in order to communicate with one another, connectivity is very important. Since the devices are entering cyberspace, they are going to be exposed to the same sorts of risks that any device connecting to cyberspace will encounter. Cheok et al. state that mixed reality is "the fusion of augmented and virtual realities". Mixed reality is more than virtual and more than augmented reality, by combining the two we are able to create real time learning environments, research experiments, and knowledge based collaboration areas that are enhanced by the application of mixed reality.

Using games for learning and for entertainment is one of the areas for different types of mixed reality applications. Pellerin et al. 2009 describe a profile management technique for multiplayer ubiquitous games. Multiplayer ubiquitous games use different types of net aware skills me network aware objects and network objects such as an RFTD tag which allows the participant to interact with the physical environment. Hardware and software to support multiplayer ubiquitous game MUG is dependent on planning out the architecture in this specific example and NFC smartcard is used as well as a reader and a HTTP server the NFC smartcard communicates with NFC reader which in turn communicates with the HTTP server. This is done in order to create a mechanism which as the authors state's guarantees a stronger identification scheme than just a login password and might help Fortson common online game cheats". The previous was an example of an approach that's used to handling player profiles and allows interactions and centralized and decentralized ways. This is very similar to the CCN X protocol which is also or which also has a goal of allowing centralized and decentralized interactions are communication.

Virtual Worlds

With the continual rise of virtual world environments, such as OpenSimulator (OpenSim) and Second Life (SL), they have the ability to be used for positive or negative gains in military warfare in the areas of training (Dawson, 2011). OpenSim is an open source multi-user 3D application server designed by taking the advantage and making a reverse-engineering to the published Application Programming Interface functions or (APIs) and specific Linden Lab open source parts of the SL code (Dawson & AI Saeed, 2012). One of the strengths for creating any virtual environment is making it accessible by a variety of users through using various protocols. OpenSim provides a method for virtual world developers to create customized virtual worlds easily extensible through using the technologies that fit with their needs. For example, a terrorist could create a virtual representation of a building by using publicly available drafting plans. This virtual representation would serve as scenario based training for terrorists. Additionally, this would allow for terrorists of different cells or groups to communicate freely. The first step would be for the terrorists to decide their targets. Once targets are decided then they would perform research on the target. This research would be on all related items such as technologies, physical infrastructure, and personnel. In the next steps the individual would capture any online maps or building architectural diagrams that would allow these areas to be rendered with the virtual world. Once the rendering of these areas has been completed a mock up scenario would be prepared. This would allow a test run to occur and later a live run. These steps can be prepared with the use of open source technology at no expense to the terrorist. See Figure 2 which outlines the processes described.

With the possible scenario presented policing the virtual worlds may become a necessity to maintain national security (Parti, 20 I 0). The U.S. Army is currently implementing a program known as Military Open Simulator Enterprise Strategy (MOSES). MOSES runs on OpenSim and is moving towards a Common Access Card (CAC) enabled environment for secure and encrypted communications (Maxwell

Figure 2. Process for building virtual world representations of real world items

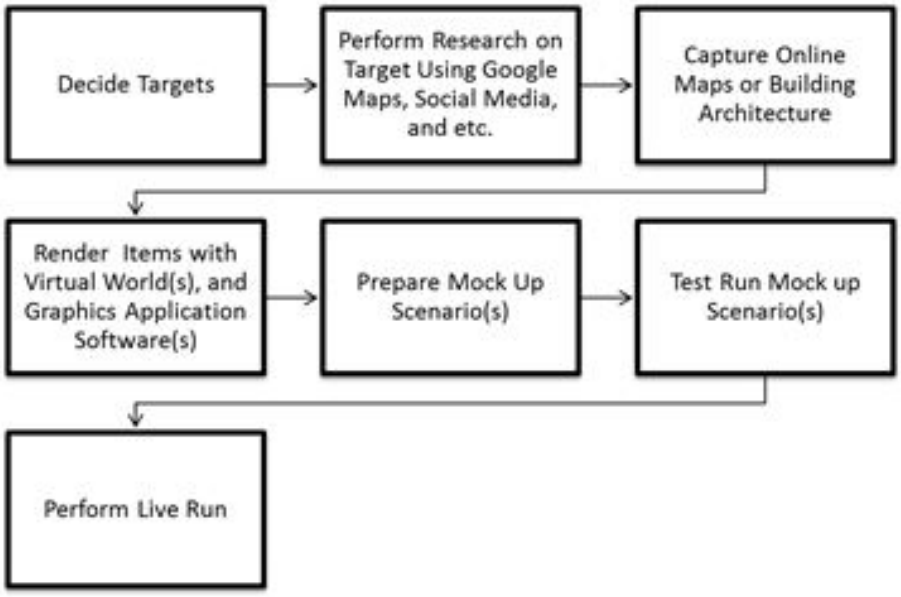


Figure 3. MOSES interaction scenario

& McLennan, 2012). in Figure 3 displayed is an interrogation scenario in MOSES. Additionally the U.S. could follow a model similar to Estonia where kids from the age of seven to nineteen learn how to develop software programs. This would help in deterring threats to include having future developers build security into the software from the beginning.

Open-Source Software for Cyber Security

Researchers, as well as scientists, have long advocated for the use of open source software for improving the nation's security posture. Open source software can be used as an effective tool in order to protect government networks and defend them against cyber criminals. Corporation, government agencies, and educational institutions have been seriously considering incorporating open source security into their systems security because of the many advantages offered by open-source software; those advantages are exemplified by lower cost ownership, customizability (the ability of modifying the code to meet security requirement) and reasonable security. In fact, the US department of Homeland security has already established a $10 million program to fund research efforts aimed at finding open-source software that could be used for security purposes and boost existing cyber defenses (Hsu, 2011). What is encouraging about the future of open source software for security is that the threat landscape is rapidly changing attacks are becoming highly organized as well as sophisticated, and the cost of commercial software security continues to rise; this trend, in turn gives open source software a cutting edge where businesses and governments are enticed to take advantage of the many benefits offered by open source software. Since the US government is looking for ways to cut costs and business organizations are looking at security as a financial burden; it is a matter of time before open-source software becomes mainstream and a competitive security solution.

Back Track Linux

BackTrack is a Linux-based operating system designed for digital forensics and network penetration testing (Myers, 2012). It is named after the search algorithm, "BackTrack" and is considered an essential security component for all security professionals. BackTrack has become a very popular open source security component for all security professionals and hacker because it contains a set of security tools that can perform virtually any security task ranging from attack simulation and vulnerability assessment to web application security and wireless hacking. BackTrack is mainly a penetration testing tool which is used to assess the security of a network, application or system.

BackTrack Linux is a free open-source software that can be downloaded free from http://www.backtrack linux.org. This security software comes bundled with many other tools that could be installed and run separately from BackTrack; those tools include Nmap, Wireshark, and Metasploit, just to name a few. BackTrack was designed with security in mind, which includes an environment that makes security testing an easy and efficient task for security professionals. It is considered a one-stop-shop and a superior security solution for all security requirements because it offers capabilities that can be used for a variety of security activities such as server exploitation, web application security assessment, and social engineering (BackTrack Linux, 2011).

Kali Linux

Kali Linux a Linux distrobution focused on offensive security. Kali Linux has replaced BackTrack Linux and is funded by Offensive Security Ltd. This Debian derived distribution has over 600 preinstalled penetration tools that can run natively on a computer's hard disk, live CD, live USD, or with a Virtual Machine (VM). This distrobution provides penetration tools for social engineering to web penetration testing (Patel, 2013; Muniz, 2013).

Tools and Methods for Monitoring Networks

Monitoring traffic across networks is of great interest to systems administrators due to the fact that this traffic has a tremendous impact on the security of networks and provides them with network situational awareness. The ability to monitor and analyze network traffic in real time can help detect and possibly prevent cyber criminals from breaking into information systems networks. Network monitoring software enables us to understand the state of network and determine the potential existence of malicious or abnormal network behavior. Network monitoring tools can prove valuable in preventing unauthorized access by providing insight into the volume of data traffic that flows over a network, examining and analyzing such data, and ultimately preventing security incidents. Over the years, the open -source security community has developed published open-source tools that are capable of monitoring network traffic and deterring possible attacks. More specifically, open-source software tools are capable of examining most activities within a computer network including malicious activity such as scanning attempts, exploits, network probing, and brute force attacks (Celeda, 2011). Below are some of the most common open-source software tools that are being used for network security monitoring. An example of this is Snort, the open source software developed by Sourcetire and used for intrusion detection and prevention (Snort, 2012). Snort is one of the most widely adopted network monitoring technologies that can be used by network administrators as a defensive technique to report suspicious network traffic activity and alert system administrators about potential cyber-attacks. Snort has gained considerable popularity and attention among other network monitoring tools because it combines the benefits of signature based tools and anomaly detection techniques (Roesch, 1999). Another reason behind Snort popularity and success is that Snort is capable of performing real time traffic analysis and packet logging on TP networks (Tuteja & Shanker, 2012). Furthermore, Snort's strength comes from its intrusion prevention capabilities which is a new feature added to Snort. The intrusion prevention feature allows Snort to take preventive actions, such as dropping or re-directing data packets, against potentially malicious traffic (Salah & Kahtani, 2009).

Nmap ("Network Mapper") is a free open source utility for discovering networks and performing security auditing (Sadasivam, Samudrala, &Yang, 2005). Nmap is a valuable and widely used network scanner that has the ability to scan rapidly and discover hosts and services by sending specially designed packets to the target host analyzes and responds. NMAP is different from other port scanner software applications in that it does not just send packets at some predefined constant rate, instead, nmap takes into account network conditions such as latency fluctuations, network congestion, and the target interference with the scan during the run time (A irdemon, 2011). Nmap has some advanced network discovery capabilities that go beyond basic port scanning and host scanning; N map can identify the type and version of an operating system, what type of firewalls are being used on the network, and what listening services

are rum1ing on the hosts. Nmap runs on major operating system such as Microsoft windows, Linux, and Solaris. NMAP has become one of the most useful network scanning tools that network administrators cannot afford to ignore especially because this tool has proven to be flexible, intuitive interface (the new Zenmap with the graphical user interface), deployable, cross platform and most importantly it is free.

TOOLS AND METHODS FOR NETWORK ATTACKS

Network attacks pose a significant challenge to information systems due to the dramatic impact such attacks have on computer networks. Network attacks could paralyze entire networked systems, disrupt services, and bring down entire networks. Tn the recent years, network attacks have increased exponentially and have evolved rapidly in complexity to evade traditional network defenses (e.g. intrusion detection systems, firewalls...etc). As computer networks grow and evolve to include more applications and services; malicious hackers continue to exploit inevitable vulnerabilities in network based applications. This, in turn, creates a fertile ground for hackers to develop and implement complex attacks and break into critical information assets. Below are a few network attacks illustrating the dangers and consequences of network attacks to include methods to defend against those attacks.

Hackers use a portscan attack, one of the most popular reconnaissance techniques, to break into vulnerable network services and applications. Most of the network services need to use TCP or UPD ports for their connections. Further, a port scan allows hackers to listen via open and available ports by sending a message to each port one at a time and waiting to receive a response. Once the port replies to a message, a hacker would then dig further and attempt to find potential vulnerabilities, flaws, or weaknesses in that port and ultimately launch a port scan attack which can compromise a remote host. The consequences of port scans are numerous and diverse ranging from draining network resources, to congesting network traffic, to actual exploitation of network devices. Cyber criminals utilize a plethora of free, open-source software tools to launch a port scan attack; one of the most popular security tools is Nmap (as explained in the section above). Nmap provides some attractive probing capabilities, such as the ability to determine a host's operating system and to provide a list of potential flaws in a port, all of which could help hackers launch a port scan attack.

Combating a port scan attack requires deploying firewalls at critical locations of a network to filter suspicious or unsolicited traffic. Also, security gateways must be able to raise alerts, and block or shutdown communications from the source of the scan (Check point security, 2004).

A SYN attack which is also known as SYN Flooding targets the TCP/lP stack. lt exploits a weakness in the way that most hosts implement the TCP three-way handshake. When Host Y receives the SYN request from X, it maintains the opened connection in a "listen queue" for at least 75 seconds (Reed, 2003). Many implementations can only keep track of a very limited number of connections. A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host thus making the system crash or becoming unavailable to other legitimate connections. The ability of removing a host from the network for at least 75 seconds can be used as a denial-of-service attack, or it can be used as a tool to implement other attacks, like lP Spoofing (Rouiller, 2003). Mitigating this attack requires the implementation of several solutions such as network address translation (NAT), Access control lists (ACL), and routers.

Another attack, which is known as lP address spoofing or lP spoofing, refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of hiding the true identity of the packet (sender) or impersonating another host on the network. TP address spoofing is a form of denial of service attacks where attackers attempt to flood the network with overwhelming amounts of traffic without being concerned about receiving responses to attack packets. Implementing packet filters at the router using ingress and egress (blocking illegitimate packets from inside and outside the network) is the best defense against the TP spoofing attack. It's also a good practice to design network protocols in a way that they are not reliant on the lP address source for authentication (Surman, 2002).

Issues with Android Phones and Other Mobile Devices

Smartphones are becoming a more integrated and prevalent part of people's daily lives due to their highly powerful computational capabilities, such as email applications, online banking, online shopping, and bill paying. With this fast adoption of smartphones, imminent security threats arise while communicating sensitive personally identifiable information (PH), such as bank account numbers and credit card numbers used when handling and performing those advanced tasks (Wong, 2005; Brown, 2009). Traditional attacks (worms, viruses, and Trojan horses) caused privacy violations and disruptions of critical software applications (e.g., deleting lists of contact numbers and personal data). Malware attacks on smartphones were generally "proof of concept" attempts to break through the phone's system and cause damage (Omar & Dawson, 2013). However, the new generation of smartphone malware attacks has increased in sophistication and is designed to cause severe financial losses (caused by identity theft) and disruption of critical software applications (Bose, 2008). Because smartphones are becoming more diverse in providing general purpose services (i.e., instant messaging and music), the effect of malware could be extended to include draining batteries, incurring additional charges, and bringing down network capabilities and services (Xie, Zhang, Chaugule, Jaeger, & Zhu, 2009).

Smartphones are rapidly becoming enriched with confidential and sensitive personal information, such as bank account information and credit card numbers, because of the functionality and powerful computational capabilities built into those mobile devices. Cyber criminals, in turn, launch attacks especially designed to target smartphones, exploiting vulnerabilities and deficiencies in current defense strategies built into smartphones' operating systems. Bhattacharya (2008) indicated that because of skill and resource constraints, businesses are ill-prepared to combat emerging cyber threats; this claim is true for smartphones as well, given the fact that those mobile devices are even less equipped with necessary protections, such as antivirus and malware protection software. Some services and features, such as Bluetooth and SMS, create attack vectors unique to smartphones and thus expand the attack surface. For example, in December, 2004, A Trojan horse was disguised in a video game and was intended to be a "proof of concept," which signaled the risks associated with smartphones that could potentially compromise the integrity and confidentiality of personal information contained in smartphones (Rash, 2004). Attackers can easily take advantage of those services provided by smartphones and subvert their primary purpose because they can use Bluetooth and SMS services to launch attacks by installing software that can disable virus protection and spread via Bluetooth unbeknownst to smartphone users.

With the development of it to movative features and services for smartphones, security measures deployed are currently not commensurate because those services and features, such as MMS and Bluetooth, are driven by market and user demands, meaning that companies are more inclined to provide more entertainment features than security solutions. In turn, this further increases vulnerabilities and opens

doors for hackers to deploy attacks on smartphones. Furthermore, Mulliner & Miller (2009) argue that the operating systems of smartphones allow the installation of third-party software applications, coupled with the increase in processing power as well as the storage capacity. Scenarios like this pose worse security challenges because hackers could exploit those vulnerabilities, which are further compounded by users' lack of security awareness. Smartphone attackers are becoming more adept in designing and launching attacks by applying attack techniques already implemented on desktop and laptop computers; smartphones' enhanced features, such as music players and video games, produce easy-to exploit targets by sending seemingly benign files via music or video game applications to users and luring them into downloading such files. Becher, Freiling, and Leider (2007) indicated that attackers could exploit such vulnerabilities to spread worms autonomously into smartphones. Therefore, hackers usually use a combination of technical expertise along with some social engineering techniques to trap users into accepting and downloading benign applications, which are used later to execute malicious code and affect critical applications running on smartphones.

Android's core components, such as Linux and connectivity media, are vulnerable to attacks through which personal and confidential information is likely to be compromised. Android's threats are further amplified by the fact that users are limited to using their smartphones for basic services and functions, such as email and SMS/MMS. Users lack the programming mind-set to protect their Android smartphones and stay current with the latest security software updates. This gives hackers an edge to target Android smartphones in the hope of gaining unauthorized access to disable core services (email and web browsing); abuse costly services (i.e., sending MMS/SMS and making calls to high-rate numbers); eavesdrop on calls and most importantly compromise sensitive information to be sold for a price. Android's open-source nature further increases security vulnerabilities because attackers can easily exploit this feature to modify the core applications and install malicious software, which could be used to compromise Android-based smartphones and ultimately cause disruption and monetary loss.

Dangers of Social Networks

Virtual communication has become a distinct area of interest for many as it has become second nature and also weaved into our everyday life. People tend to create a social reality that is based on the connection to the Internet and using tools that assist communication. These tools have danger sides that a vast majority does not see or think about on a daily basis. Currently, there has never been a higher danger **in** the social networks for the public than there is now. This danger is easily spread to everyone who use this mode of communication based that people unintentionally make themselves vulnerable. With a connection to a vast number of social networks, people are easily consumed by submitting personal information via the Internet. The time is now for the public to understand where they stand in the future of the Internet connectivity and what they can do to assist or lessen this danger.

Trend in Social Networks

People of all ages are beginning to learn to use social networks to stay in touch, reconnect, and meet new people and find out about new places. These websites usually allow the user to present a profile of himself through a long list of very detailed information (Conti, Hasani, & Crispo, 2011). A vast majority of businesses are beginning to use these social networks to find new employees, expand and market and product line, and also to advertise their brand. These primary reasons are based on several distinctions

that will help companies grow and expand due to the majority of customers who search for products via social networks. Customers are becoming more tech savvy by using mobile devices to gain Internet connectivity in various locations. This helps create a realistic and educational feel to understand specific product information that is only based online.

Social networks have become the largest branding and marketing areas for this era. Sites such as Twitter, Facebook, lnstagram, Pinterest, and many others have risen in this past decade and have continued to increase with customers based on their usability and features. These sites have risen in popularity in the last few years, typically growing from basic technologies as participation increases and user expectations shape and form the media (Fitzgerald, 2008). Increase use within these sites also dictates an increase in the population in users who are becoming friendlier in the social media aspect.

Online social networking sites have become integrated into the routine of modern-day social interactions and are widely used as a primary source of information for most. Research found that Facebook is deeply integrated in user's daily lives through specific routines and rituals (Debatin, Lovejoy, Horn, & Hughes, 2009). Facebook is a social networking tool that is used in various instances that help people connect to people or businesses connect to people. It is the mere change in security that people and businesses will need the most help. These areas are vital to the metamorphic adaptions of today's society. Change is needed, and with this change, new adaptions for online security are required and mandated in some instances.

Online security can be looked at by a virtual standpoint in the relation of consumers and businesses. Many businesses use social media and online social networks to communicate to one another in a sense that many users are also using the same technology to find new information. Online information security risks, such as identity theft, have increasingly become a major factor inhibiting the potential growth of e commerce (Wang, 2010). A base system of online security is needed to help fulfill many business expectations and also promote or generate business in different geographic locations.

A Geographic Location

In definition, Hochman et al (2012) defines lnstagram as a recent fad in mobile photo sharing applications that provide a way to snap photos, tweak their images and share then on various social networks with friends, family, and complete strangers (2012). This type of social media helps create a realistic feel for people to see photos of specific areas where people are located. This also helps create a uniformed timeline scheduled photos that describe a story of one's life. As security is a high need in this type of online social media, it is best used in personal and business use.

Pinterest is also a varying tool of online social media that houses has many users who also use other networking tools. Pinterest allows members to "pin" items or images found on the Internet to a pin board, which can then be easily shared through an email link or by following the creator (Dudenhoffer, 2012). This networking tool can also be paired up with other social media tools such as Instagram, Twitter, and Facebook. These networking tools also create a justification that helps creates a total profile immersion for people virtually. Security within this profile is currently weak; changes and adaptions can help create a justification for areas of higher influences such as these networks.

The popularity of these sites provides an opportunity to study the characteristics of online social network graphs at large scale (Mislove, Marcon, Gummadi, Drushel, & Bhattacharjee, 2007). A leading cause of the rise of these sites has been with consumers fining it easy to use and navigate to find information on and within these sites. The usability of these sites makes it very easy for customers of

all ages to navigate through processes, which require personal information. When people subject themselves into giving information to the virtual world, they also subject themselves in becoming vulnerable for virtual threats.

No matter how easy an Internet site can be to submit sensitive information, no site is purely safe and danger free. This is why the connection to Internet connectivity is a matter that needs to be handled with high importance. A dire need to have security at its maximum has never been such an item then it is today. From every angle, people are becoming vulnerable to attacks from predators who deem themselves capable of obtaining information. As vital information is spread throughout the system of technology based environments, this information can also be spread throughout the world.

WHO IS CONNECTED AND WHY?

The main focus for the impact of the digital age is the critical mass population of the people in the world. People are beginning to use, read, analyze, and interact virtually younger and more often than ever before. This preliminary change occurs because now people begin to interact with social networks at a younger age. Learning starts to develop at a younger age because many of the cognitive abilities are beginning to be developed and acquired when children are younger, thus giving them the ability to develop an interest in fields they may want to work in as an adult.

Businesses

Businesses begin to look at the advertising site of their work in relation to how it can assist them with sales and goals. Since marketing is such a large portion of business, brands especially need to look and see what advertisements they can use to assist them in reaching their goals. The future of advertisements and marketing is based on the consumer today, and where they look to find information in regards to their purchases. The future of the Internet connectivity and adaptation is directly linked through the suitability of use for the Internet.

An important factor to look at when it comes to firm development is to look at the dire need for firms to develop their niche successfully. The virtual sector of businesses is extremely dependent on the absolute use of the user and the Internet. Businesses tend to adapt to a series of modules that are formulated with their overall mission as a company. Leaning to technology-based marketing is one way to look at the overall spectrum of the businesses.

Companies are moving online media to the core of their programs because of how often consumers use social media for information-gathering purposes (Grainger, 2010). A feature that gives customers a more realistic feel such that they can obtain information in quickly is an online feature. This feature is used in many tactics for marketing and advertising based that many customers are prone to find items that assist them with what they are looking for via online. The connection must also be secure and safe for consumers such that viable personal information is used for online purchases.

Internet connectivity can also create justifications for businesses that have a niche for merchandising to customers, not on location. This avenue also needs an increase in data that are transmitted through various servers and websites. Servers are the basis of information modification; they help provide a space and location for all information to be transmitted within a network. Businesses are taking part of this big shift based that the value of information to be able to be moved with this the-savvy environment is easier

than ever. Servers also offer a sense of protection for business material to be saved and updated. Since safety is a big issue due to weather, it is feasible for businesses to purchase servers. Moreover, prices have also decreased with reflection to the safety of a server. Not only does a price reflect an adjustment towards the quality and value of the item at hand, but it is also noted on the overall performance of the machine or equipment.

Institutions are also a main contributor or purchaser of servers and Internet connections based that they using online connections more than ever. A main factor that needs to be adjusted with institutions is the feasibility factor of what has been given at hand for the item to be installed, adjusted, and used with the institution. This feasibility also dictates a specific privacy that needs to be labeled at a specific standard for the institution to use. If these privacy areas are not up to a specific level, the institution is not and will not be able to use these items in conjunction with its mission or vision values.

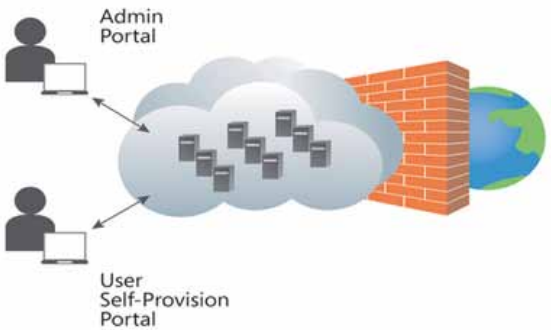
Schools

The future of institutions is founded via the Internet and the connectivity that these institutions have with the Internet. With this, more schools are using web design formats that are very user friendly, such that more information can be placed virtually. With more information being placed virtually, more students will have access virtually to this sort of information. This also gives the institution the power to place a majority of their application processes; faculty related work, as well as communication online and able to be accessed by any faculty member or student at any time.

The vulnerability of this information being accesses by outside threats is high in regards to how secure the information is. Many institutions place a restriction to the limitation of the access of where it can be obtained. This limits the user capability of accessing information. Limiting this information can lead to problems internally as opposed to externally based that not all users will agree and comply with the polity regulations.

Institutions can create a wall that assists the blockage of information sharing through a semi-permeable layer, which is accessed by users and administrators. This barrier helps to control the amount of information sharing that can be displayed accordingly in regards to virtual threats. Creating this wall helps give administrators more control to information that is shared as well as provides a sate avenue for users at the lower level. When a barrio is promoted, it can also create a justification or rule that helps threats stay at bay and never reach core areas of information. The vital elements of this can be displayed Figure 4.

Figure 4. Private cloud enterprise data center
(Social-Cast VMware, 2012)



WHERE DO PEOPLE CONNECT?

A rise in the digital social media arena has a direct impact towards the world, and with this many of the companies are beginning to respond with technological changes. With increasing technological advances. business can operate more smoothly, more effectively, and more efficiently to better facilitate operations and management. More tools are available for businesses that have the desire to take their business and marketing virtually. This has led to the increase of mobile device use since most users of social media use these applications in various locations.

Marketing has become a direct and distinct changing factor in business competition. With this, more businesses have begun to change their style rule location of advertisements. It is a clear example that more customers arc beginning to change their overall plans based on how they are able to obtain information on a general basis. With this, it is assumed that many businesses are also creating new, avenues and paths for marketing advertisements to be able to reach customers at various distances. This is also why it is very important for a business to have the ability to connect over a large geographic area with ease.

It can be determined that social networks via Internet connectivity are the best ways for businesses to connect to people. Businesses of all stature are beginning to look at the possibility of marketing strategies reaching customers in geographic locations. A large trend for mass adoption for businesses is to connect to customers via mobile devices; this in turn will lead to customers being able to connect to businesses at various levels. This trend increases the use of mobile devices based that a majority of the users are using these devices for a purpose.

One item that can be dictated with the high use of Internet connectivity and mobile devices is the ability for outside sources to obtain information via mobile. This path will change the overall spectrum of how customers can purchase goods via online and where they can go to gain security for their purchases. It is then up to the providers of the mobile devices to create secure Internet services for the customers' sake depending on how the customer is able to cooperate with technology. Even as the security of the Internet service increases for the customer, it also must increase at the business end. This is to ensure that all employees and persons involved in online transactions are being monitored by a service that can provide safety throughout the purchase and delivery of the product.

Internet Stalking

The increase of the social networking trend can be based on the security features of for every user.

Internet stalking can be noted by a threat from an outside source that harms or conflicts harm to a piece of information or person. These threats can international or nation depending on where the organization or user is geographically located. With Internet stalking being noted more often in today's society; it is also presumed that people are also becoming more vulnerable to attacks from Internet insecurity. Insecure Internet can be looked at based on what the user currently is using in terms of connectivity but can always be looked at as a threat to any customer.

When international threats are aimed at consumers, it can be perceived as a threat that is directed to the nation based that it is from outside the country. These circumstances can be legal or illegal based on the source of the threat. Many users see these types of threats as being identified as acts of terror based that many users do not know much information about the types of threats that are visible.

An example is noted from a post on social media that included valuable and private information. Any post can be noted in becoming a threat to outside sources such as a tweet from twitter, a picture from

Figure 5. Post on Facebook, a social media application
(Mustafa, 2012)

lnstagram, or a post on Facebook. Twitter is less than three years old, commands more than 41 million users as of July 2009 and is growing fast (Kwak, 2010). An example of a post can be noted in Figure 5.

From this point, an invader or Internet stalker can take into account the vital information and begin to look up where the user lives or where the user is updating his or her status. This can be done by researching with the Internet for items which are displayed virtually and can denote where the user lives. In this example, it is noted that the user Mustaza Mustafa is posting this status with Hongkait. Location information for users is stored in the About section of a user's profile on Facebook.

Google earth is an application that can help look up locations and geographic areas on maps to help determine where items, businesses, and people are located. With this application, Internet stalking can be made easier by a method of inputting a location for a specific item, person, place or business to locate where it is. Since there is a very low security with this application, this option can be used with most location-based information given specific circumstances.

A phenomenon of cyber-stalking and virtual harassment will be the set of focus for the next generation. It is with this type of harassment that schools and institutions become the most vulnerable based on the population of these locations. Areas of improvement will be creating secure environments for students and faculty based on online communication. These areas will be an avenue for major threats as long as they are unsecure for cyber stalkers to pass through and obtain information.

Schools

Institutions, schools, colleges and universities can be noted as main areas for Internet stalking based on the number of users who use the Internet to connect, obtain information, and to communicate. With the increase in interest on the social trend, schools and institutions are adapting to modify more programs

to be taught online. This adaption has the ability to help increases the student population for the school as well as increases the amount of adult learners who will use the Internet to obtain information. This increase can also upset and hurt the population by leading stalker and other predators into getting involved with or becoming involved with Internet stalking. As schools and universities become the highest areas for teens and students, they also become the most vulnerable.

Finn (2004) conducted an exploratory study to show that 339 students at the University of New Hampshire, about 10% to 15% of students reported repeated communication threatened, insulted, or harassed, them (Finn, 2004). This type of negative communication can result in various types of lawsuits, endangerment, or even physical harassment, which can lead into negative effects and/or reputations for institutions. Internal and even external customers can be the main causes of threats to the institution based on what information is current stored and what information is being obtained.

University communication and connectivity systems need to be impeccable in order to ensure secure networks for students and faculty. In terms of financially affordable, these systems need to have various departments that are capable of tracking of where the sources are going towards, coming from, and how they are able to obtain information. This type of security is currently necessary and will be necessary for the future with the increase in students and the usability of online platforms. This type of security also creates a unified system with the university's reputation to promote a positive secure environment.

Internet stalking also increases the risk of vulnerability for the institution in terms of international attacks from outside sources. These attacks or acts of terror can be terminated or at the least lessened by having a secure server Internet connection. A secure Internet connection needs to be set up with many specific requirements such that all users have access to information and communication within this method. Internet connectivity is increasingly moving off the desktop and into the mobile and wireless environment, particularly for specific demographic groups (Lenhart, Purcell, Smith, & Zickuhr, 2010). As the Internet connections become a main target point of importance for institutions, security in these areas will also increase based on the amount of users.

Leading to Intelligence Gathering

The various types of information that social media customers input via the Internet can be viewed and retrieved by outside sources. The information gathered leads to a negative activity from international customers. In various instances, personal, financial information can be gathered and used against the user for purposes of threats that can harm or steal the identity of the user.

Intelligence Gathering from other Countries via Internet Connectivity

With the high trend of social networking scattering the Internet's surface, social media are available in every country, thus increasing the use of Internet connectivity. This availability of information helps create a mix between businesses and customers **in** terms of how information is related. Intelligence gathering is one way of using the available information and putting it to good use depending on the source of the receiver. Businesses can use this type of work by targeting special performance enhancing customers who are local and idealistic to the values that the company brings to the table. lt is also valuable in terms of online social marketing because it is feasible for businesses to assist with advertising online as compared to physical.

An international point of view that collaborates intelligence gathering can be noted based that Internet connectivity is what brings users from various locations together in one normal new setting. This virtual environment setting becomes a normal atmosphere for many users based that most users are not currently satisfied with physical aspects of businesses. Using intelligence gathering from other countries helps institutions and businesses gather a list of potential customers from varying backgrounds that can help modify the existing performance of the business. A modification for a business is looked at by an increased way information is displayed and given to customers. This method should increase sales within the business, such that there is an absolute return on investment for the business.

Institutions can use intelligence gathering to help create new avenues for students to prosper. With this, distance learning and online collaborative learning can be assisted such that these are the main areas that are affected by the online networking. These changes also increase the power and connectivity of the specific institution to the student learner in the sense that they feel connected and secure. These are the most important items in any aspect of online networking in a business or educational field.

Privacy Laws

The U.S., Canada, and European Union (EU) provide a useful launching pad for the examination of cross-border privacy issues. With this, the U.S. has maintained a severe high maintenance cost for its security in the Internet connections. This is a main reason why many institutions and businesses have created variances for what is allowed to be passed via the Internet. ln creating these variances, it also can be noted on how businesses prepare media and advertisements and also the security in these messages.

With Europe's high trade cost and online businesses, there is a high need for privacy to be placed in situations where customers will feel safe. It is this need that the European Union uses to assume and vary its security online. Many businesses are accustomed to this type of development processes such that it is now accustomed to the normal activity for online marketing. Even the applications used via the Internet connection do not use instances where privacy can be breached. It is with this type of process that businesses become safe from outside attacks.

Future of Internet Connectivity: Social Networks

As Internet connectivity becomes the more favorable and usable feature in a business industry, many businesses, customers, and people in general will begin to look for more ways to use this type of connection. The basis of a secure Internet connection service begins with several items, which dictate how people use the connectivity, what they use it for, and where they use it. Many businesses will also become more conformable with the adaptability of Internet usage in terms of security, mobility, and marketing. Overall, social networking is keen to fir development in businesses and keen for connections for people.

EMERGING TECHNOLOGIES AND THE INTERNET

Innovations and Numbers on the Growth of Ubiquitous and Mixed Reality Related Technologies

Google Glass is a wearable computer and a variant of the head mounted display (HMD). What is interesting about this innovation is that it is more than the headset. Google has connected this to the Internet in many ways, not the least of which is being connected to the users Google+ account, which enables the user to share photos and videos with others. Using Google+ the user is connected to all their contacts from their Gmail account. Glass provides a way for the user to interact in different ways with the Internet, through the rich media environment that is supported by Google. Google glass could be integrated into Internet security in many of the same ways in which the traditional mixed reality system that has been described in this chapter.

Google Glass may not have its uses defined, yet many have made prognostications on uses for the augmented reality system. Tt is quite a visionary type of product with associated services. Many have recently written about potential uses for Google Glass. Some of the best ideas arc very close to some of the existing fields of virtual and augmented reality. The fact that the actual headset is so innovative, small, and connected, is intriguing and opens the door for many types of new applications or revisiting the old applications with the new technologies. Many envision that Google Glass will be used in the operating room to provide real time information to surgeons, as well as, augmenting education on many different levels.

Emerging technologies that are changing things as we speak is the idea of content centric networking. Xerox PARC is currently developing Content Centric Network (CCN), and making the software open source. One of the advantages of this technology is going to be that the data maintains its integrity no matter where it is transmitted; as there are security keys that are incorporated in their peer to peer demonstration of the CCN, which can ride on top of protocols or run natively. Such technology is essentially for mixed reality environments which necessitates a need for sharing information locally and quickly.

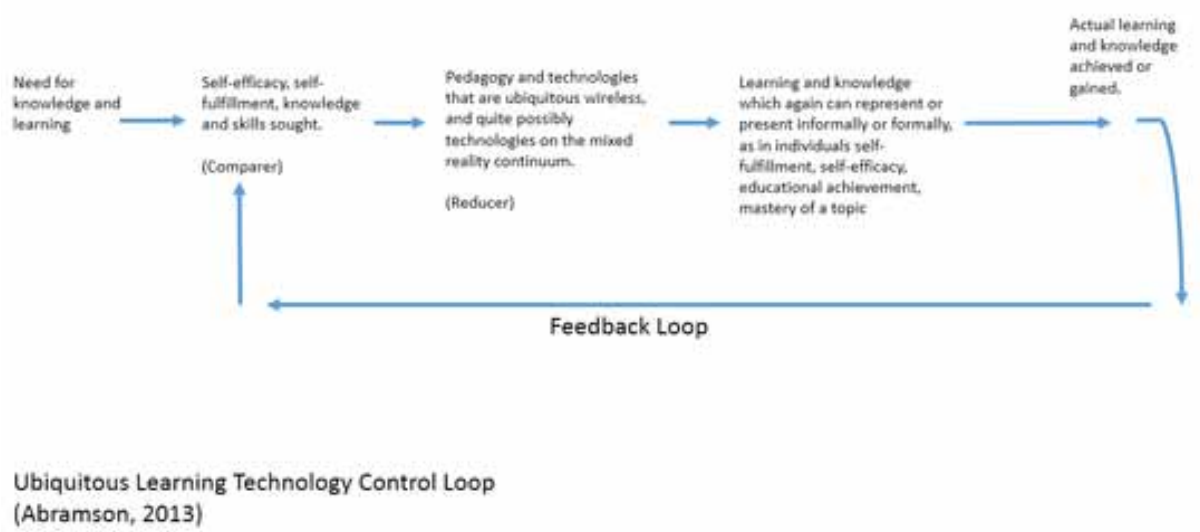
An interesting way that we conceived to view ubiquitous wireless technologies and technologies that represent mixed reality is to view the specific technology or group technologies in a feedback control loop. Using such a model we can construct the following control loop using.

At the beginning of the loop is the need for knowledge and learning, which may be in individuals need, and or a formalized educational program. The next step in the feedback loop is the comparer; in this model it will represent grades, 21st-century technology skills, self-fulfillment and self-efficacy. To the right of the compare is the reducer, which consists of pedagogy and technologies that are ubiquitous

Wireless, and quite possibly on the mixed reality continuum. Lastly is learning and knowledge which again can represent or present informally or formally, as in individuals self-fulfillment, self-efficacy, educational achievement, mastery of a topic. The feedback control loop moves left to right, in the feedback loop itself runs from learning and knowledge back to the need for knowledge and learning. A chart has been created to help visualize the model (Figure 6.).

Using this model we make some assumptions, the first is that this is an activity that individuals want to engage in. The second which is illustrated by the comparer, they have a need. The reducer once again is going to representative of the technologies that we arc looking at in this chapter. We arc looking at mobile devices, different types of mixed reality that are used for knowledge creation and collaboration. Therefore we are looking at the technologies in this paper as a reducer in the Ubiquitous Learning Tech-

Figure 6. Ubiquitious learning technology control loop



nology Control Loop (ULTCL). While this framework is not predictive in nature, or does not prescribe, it does segment or compartmentalize the topical area which makes it useful for analysis of new and emerging technologies that are found in mixed reality environments.

Dangers

Cyber-attacks happen on all types of organizations and individuals. They can start in many different places, including any device that's connected to the Internet. This becomes highly problematic in our modern society when we have devices such as copy machines that are hooked up to the Internet in order to update themselves report usage, install software, etc. Having all these devices connected to the Internet increases our exposure and vulnerability. With so many targets we need to create an orderly way to look for threats. As the threats have increased through the years, we become more vulnerable to these threats. An interesting point about the intrusion detection systems is that they are part hardware and part software. Therefore when we implement one of these solutions we need to make sure that we are up to date with the hardware and software maintenance so that we get the updates that will keep the organization safe.

There are many research papers and projects that have demonstrated the usefulness of virtual and mixed reality environments in many different fields. It is important that the cyber warrior believes that they are in a different environment. Believability has been a requirement for successful implementations of mixed reality and virtual reality. Human computer interaction (HCI) is essential to making the cyber warriors feel that they are immersed **in** cyberspace. Since cyberspace cannot be seen by the naked eye, we need to gather the data and information that is necessary and make the user be able to see it in a virtual and productive environment. The potential of ubiquitous, mobile and mixed reality technologies to deter Internet threats is enhanced by these characteristics, as we now have the ability to have individuals who are in geographically separate areas, work together as one to solve new threats and problems. Mixed reality may be able to bridge the gap of recognition of security threats.

Incorporation of mixed reality should only require the changing of the inputs to the user or cyber warrior from game to actual data and information and the integration and implementation of a head mounted device (HMO) and quite possibly new input devices including brain to game interfacing. The process of creating a visual environment in which users can be active participants with real data with the purpose of solving problems and deterring threats, opens the process up to gamification. This permits the analysis of threats and also using the threat log and data for training as well, including one excited in a game based scenario.

Device Innovation

The characteristics of the devices that we use to connect to the Internet are becoming smaller and more powerful. Contemporary mobile devices are extremely powerful, students can gather information off the Internet, download files, take pictures, email, and alter .pdf (portable document format) files of any document that they have downloaded, analyze, synthesize and type up documents, all without any intervention or training from the university. They can also participate in an online discussion, call, email, text, video chat on certain phones and devices, including Apple iPhone and iPod touch. Such areas and technologies are mentioned, as these platforms illustrate what is possible from a technological standpoint, the critical mass of the technology, and show how they have been adopted into organizations and more importantly the individual as many of the changes that we have seen have been driven by the adoption of the individual and used without any intervention of the organization or university. This makes technology or technological forces great. Thus combined with other forces has helped changed our society, no matter where we live. A ubiquitous device is one that is defined as always connected and allows access to content, anytime and anywhere (Hummel and Hlavacs, 2003). Internet bandwidth has become fast and more importantly wireless and ubiquitous, which has provided for the growth of many types of mobile wireless devices (Figures 7 and 8).

Figure 7. Cyber warrior technolo. (Jy Infrastructure)

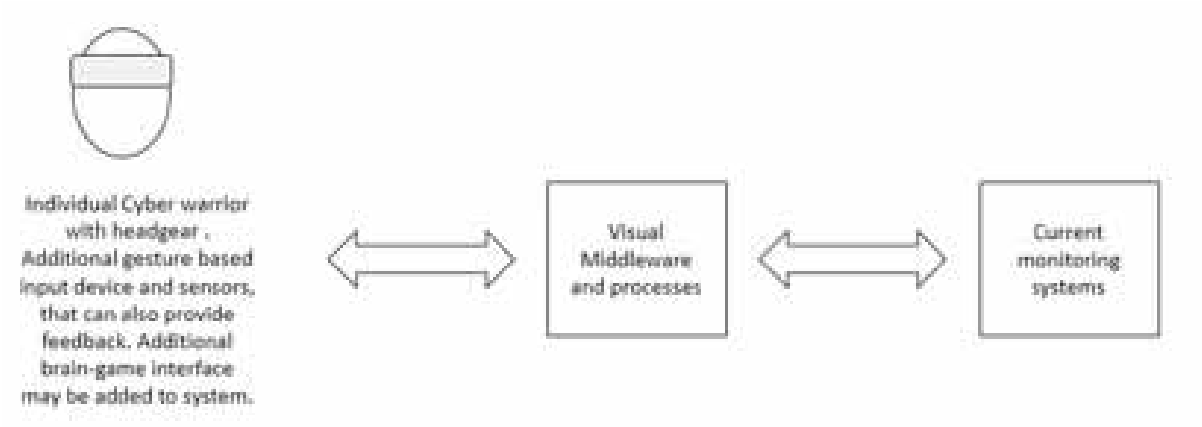
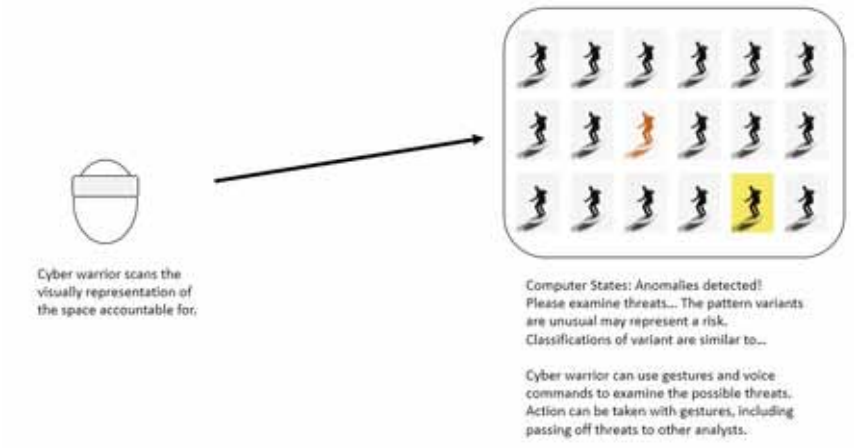


Figure 8. Cyber warrior scanning and interaction processes



EMERGING AREAS IN HUMAN COMPUTER INTERACTION FOR COUNTERING CYBER ATTACKS

One of these areas is the use of head mounted displays (HIVIIJs) which may use spatial immersive display technology. By using these types of devices we can create environments which help reduce some of the complexity that is involved with detection of cyber threats. Seeing mixed reality used in this capacity has been seen in popular fiction literature. Ender's Game (1985) is a science fiction novel by Orson Scott Card. In the novel the most talented young are trained using vit1ual reality and augmented reality games. The US military has been using virtual reality for training and development. Specific examples include soldiers shooting and field training with armor, infantry, aviation, artillery, and air defense. One of the first modern implementations of this was at the Defense Advanced Research Projects Agency (DARPA) Simnet facility at Ft. Knox, K Y in 19ROs. Inside ofthe facility were multiple types of units that had a representation of the vehicle and tools that they would use on the battlefield. As one of the authors was a participants in this event, computers made a compelling and immersive environment for units to train together and against one another. It is not hard to imagine extending this type of technology in order to create an immersive environment that makes the detection of cyber threats easier to identify from the mass of data and information that may or may not be detected using more conventional means.

Mixed reality will make it easier to find these threats by a reduction of the complexity. Reducing complexity and increasing the understandability of threats will make it easier to work in an environment in which portions can be turned on and off. Current virtual reality and gaming technologies allow for the generation of the monitoring and subsequent training environments described. Of the first elements in a project that would be used to protect and monitor cyber-attacks would be to create a 3-D world in which systems/cyberspace can be modeled. Since many of the cyberspace attacks cyber-attacks target specific cities towns and businesses, we can use the geography as a starting point. From the generalized location we can create a highly granular or defined area of vulnerability and concern. This can be done by using many existing geographical databases such as Google. After this step we can focus on the mechanics of the 3-D world many tools are available for this purpose including dark basic which is a game engine that can house the navigation and parameters of the 3-D world. Therefore most if not all of the hardware and software systems and technology do exist for the creation and implementation of such a system.

Currently there are many open source and commercial versions of software that will permit the player/user to work against an AT or human opponent in order for the development of their ethical hacking skills. Users that immerse themselves in this type of technology are helping develop their skills sets, the future use of virtual and mixed reality to these types of systems will only enhance the understanding and help the user prepare for work as a cyber-warrior. Google code currently has a project emu-os that is a simulation ("Emu-os- EmuOS is an open-source hacking game and simulator. - Google Project Hosting," 2012) that pits hacker against hacker, by doing this the user is gaining real-world and real-time experience.

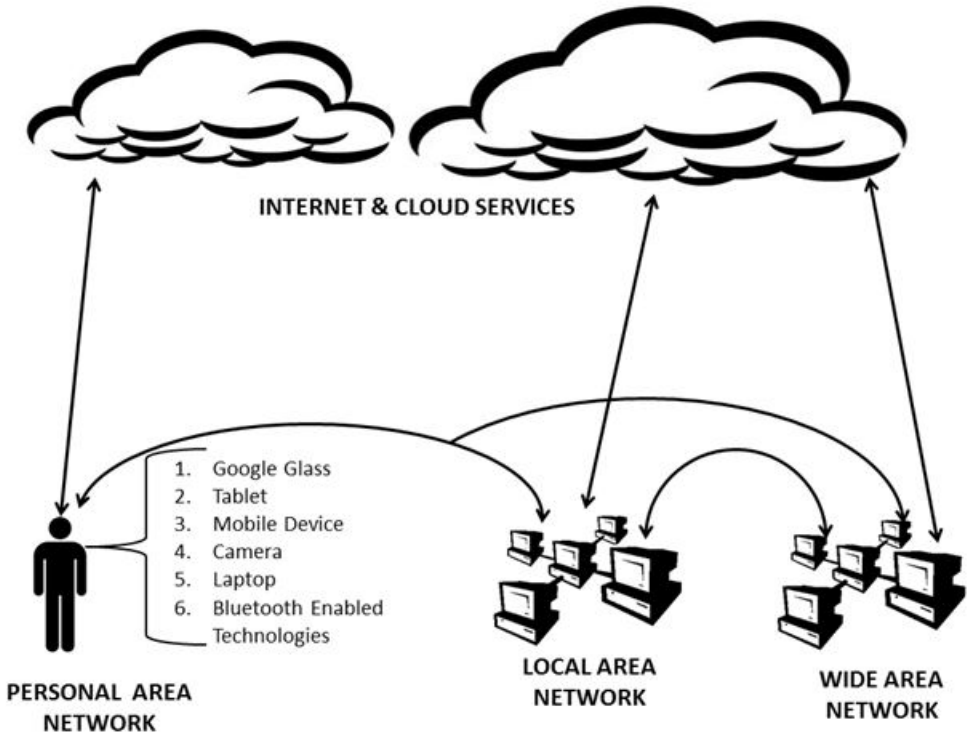
The latest IDC predictions at the time of writing this chapter show that mobile devices are passing out PCs in how users connect to the Internet. Software as a service (SaaS) and Platforms as a service (PaaS) are all reporting exponential growth which helps confirm the mobile computing trends that we are seeing. There are many different reports out that describe the most popular mobile devices, a common theme among all of them is the smart phone and tablets ("IDC Predicts 2013", 2012). Therefore we can see that the Internet infrastructures are changing to meet the needs of a more mobile device oriented market. Mobile device security is going to become even more important as more people are going to be using these devices for all sorts of tasks, including those oriented around virtual and mixed reality.

Enhanced Collaboration and Learning with New Technologies

Collaboration is important and is enhanced with virtual and mixed reality systems. Collaboration is an important part of the new learning paradigm and has been proven effective in the supporting collaboration as e-learning tools are readily available on most mobile devices. Collaboration is enhanced by the use of mobile technologies and is a key intention of the knowledge age. Turoff (2000) proposed that collaboration provides a solution to learning outside of the physical classroom. Tn addition to collaboration, facilitation, and updated educational methodologies are key components to E-learning and M-learning (Hiltz, Benbunan-Fich, Coppola, Rotter, & Turoft2000). Collaborative learning is the promotion of learning through social interaction; it is one of the five properties identified by Klopfer et al., (2004), which support the established forms of learning through the use of mobile technologies (Figure 9.) (Naismith, Lonsdale, Vavoula, & Sharples, 2004).

Figure 9. Post university cyber lab

Figure 10. Systems of systems



Systems of Systems Concepts

When discussing hyperconnectivity **it** is necessary to discuss systems of systems concepts. Systems of systems is a collection of systems tied together to create a more complex system (Popper, Bankes, Callaway, & DeLaurentis, 2004). An example of this is the figure below which displays a few methods to be connected to the Internet and network traffic scenarios. When thinking about the possibilities of hyperconnectivity the personal area network (PAN) is an excellent example as it allows multiple technologies to be interconnected with soil ware applications. The Google Glass has the potential to all global positioning system (GPS), social media, digital terrain overlays, and synchronization with other devices. This increases the complexity of the system as it becomes part of a larger systems which multiples the number of potential vulnerabilities (Figure 10.).

CONCLUSION

The futures of national and international security depend on multiple complex countermeasures to ensure that a proper security posture throughout its lifecycle. To effectively protect these systems from exploitation of vulnerabilities, it is a necessity to further comprehend all the current threats and how they exploit the current vulnerabilities. Additionally, one must be able to effectively gauge the future threats and

have a strong grasp on the laws that drive their need to be secured such as enhanced privacy laws by the national governments. Examined within this chapter are the potential security related threats with the use of social media, mobile devices, virtual worlds, augmented reality, and mixed reality. Further reviewed were examples of the complex attacks that could interrupt human-robot interaction, children computer interaction, mobile computing, social networks, and more through human centered issues in security design. This book chapter serves as a guide to those who use multiple wired and wireless technologies but fail to realize the dangers of being hyperconnected.

REFERENCES

Armbrust, M., Fox, A., Griftlth, R., Joseph, A. D., Katz, R., Konwinski, A., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50-58.

BackTrack Linux. (2011). *BackTrack Linux*. Retrieved March 22, 2013, from www.backtrack linux.org.

Becher, M., Freiling, F., & Leider, B. (2007). On the effort to create smartphone worms in Windows Mobile. *Proceedings of the 2007 IEEE workshop on Information Assurance*. United States Military Academy. Retrieved March 22, 2013, from http://pil.informatik.uni-mannheim. de/filepool/publications/on-the-effort-to-create-smartphone-worms-in-windows-mobile.pdf

Beidleman, S. W. (2009). *Defining and Deterring Cyber War*. Barracks, PA: Army War College. Retrieved March I0, 2013, from http://www.hsdl.org/?abstract&doc=ll8653&coll=limited

Bhattacharya, D. (2008). *Leadership styles and information security in small businesses: An empirical investigation* (Doctoral dissertation, University of Phoenix). Retrieved March 9, 2013, from www.phoenix.edu/apololibrary

Bishop, M., & Taylor, C. (2009). A Critical Analysis of the Centers of Academic Excellence Program. In *Proceedings of the 13th Colloquium for Information Systems Security Education* (pp. 1-3). Retrieved March 9, 2013, from http://nob.cs.ucdavis.edu/bishop/papers/2009-cisse/

Bose, A. (2008). *Propagation, detection and containment of mobile mal ware* (Doctoral dissertation, University of Michigan). Retrieved March 11, 2013, from www.phoenix.edu/apololibrary

Brown, B. (2009). *Beyond Downadup: Security expert worries about smart phone, TinyURL threats: Malware writers just waiting for financial incentive to strike, F-Secure exec warns.* Retrieved March 20, 2013, from http://business.highbeam.com/409220/article-1G1-214585913/beyond-downadup-securityexpert-worries-smart-phone

Bullock, J., Haddow, G., Coppola, D., & Yeletaysi, S. (2009). *Introduction to homeland security: Principles of all-hazards response* (3rd ed.). Burlington, MA: Elsevier Inc.

Cavelty, M. D. (2008). Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics*, *4*(1), 19–36. doi:10.1300/J516v04n01_03

CCEVS. National Security Agency, Common Criteria Evaluation and Validation Scheme. (2008). *Common criteria evaluation and validation scheme -- organization, management, and concept of operations* (Version 2.0). Retrieved from National Information Assurance Partnership website: http://www.niap-ccevs.org/policy/ccevs/scheme-pub-l.pdf

Celeda, P. (2011). *Network security monitoring and behavior analysis*. Retrieved March 22nd, 2013 from http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-cbpd133.pdf

Cheok, A., Fernando, O., & Liu, W. (2008). The magical world of mixed reality. Innovation: The Magazine ofResearch and Technology. *National University of Singapore and World Scientific Publishing*, *8*(1), 70–73.

Cheok, A. (2009). Mixed Reality Entertainment and Art. *International Journal Of Virtual Reality*, *8*(2), 83–90.

Cheok, A., Man Fung, H., Yustina, E., & Shang Ping, L. (2005). Mobile Computing With Personal Area Network and Human Power Generation. *International Journal of Software Engineering and Knowledge Engineering*, *15*(2), 169–175. doi:10.1142/S0218194005002348

Clarke, R. & Knake, R. (2010). *Cyber war: the next threat to national security and what to do about it.* New York, NY: Ecco.

Conti, M., Hasani, A., & Crispo, B. (2011). Virtual Private Social Networks. *Proceedings of the first ACM Conference on Data and Application Security and Privacy*.

Dawson, M. (2011). Applicability of Web 2.0: Training for Tactical Military Applications. Global TIME, 1, 395-398.

Dawson, M. E. Jr, Crespo, M., & Brewster, S. (2013). DoD cyber technology policies to secure automated information systems. *International Journal of Business Continuity and Risk Management*, *4*(1), 1–22. doi:10.1504/IJBCRM.2013.053089

Dawson, M. E., & Saeed, A. I. (2012). Use of Open Source Software and Virtualization in Academia to Enhance Higher Education Everywhere. *Culling-edge Technologies in Higher Education*, *6*, 283–313. doi:10.1108/S2044-9968(2012)000006C013

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. doi:10.1111/j.1083-6101.2009.01494.x

Denning, D. E. (2012). Stuxnet: What Has Changed? *Future Internet*, *4*(3), 672–687. doi:10.3390/fi4030672

Dudenhoffer, C. (2012). Pin It! Pinterest as a Library Marketing Information Literacy Tool. *College & Research Libraries News*, *73*(6), 328–332.

Dyck, J., Pinelle, D., Brown, B., & Gutwin, C. (2003). Learning from Games: HCI Design Innovations in Entertainment Software. In *Proceedings of Graphics Interface*, (pp. 237-246). Retrieved March 18, 2013, from http:/lhci.usask.ca/publica tions/view.php?id=88

Emu-as- EmuOS Is an Open-source Hacking Game and Simulator. (2012). Google Project Hosting. Retrieved March 11,2013, from http://code.google.com/p/emu-os/

EPOC Features. (2012). Retrieved from http://www.emotiv.com/epoc/features.php

Finn, J. (2004). A Survey of Online Harassment at University Campus. *Journal of Interpersonal Violence, 19*(4), 468-483. Retrieved March 9, 2013, from: http://jiv.sagepub.com /content/19/4/468

Fitzgerald, D. C. (2008). *Intersections of the Self: Identity in the Boom of Social Media* (Doctoral Dissertation). Available from ProQuest Dissertations and Thesis Full Texts Database. lllinois State University. Retrieved March 20, 2013, from http!/search.proguest.com/docview/304607151

Fraser, M., Hindmarsh, J., Best, K., Heath, C., Biegel, G., Greenhalgh, C., & Reeves, S. (2006). Remote Collaboration Over Video Data: Towards Real-Time e-Social Science. *Computer Supported Cooperative Work*, *15*(4), 257–279. doi:10.1007/s10606-006-9027-y

Grainger, J. (2010). *Social Media and the Fortune 500: How the Fortune 500 Uses, Perceives and Measures Social Media as a Marketing Tool* (Doctoral Dissertation). Available from ProQuest Dissertations and Thesis Full Texts Database. University of North Carolina at Chapel Hill. Retrieved March 18, 2013, from https://cdr.lib.unc.edu/indexablecontent?id=uuid:ae530f99-9b8d-43a4-9fa4-9fl2c5b00a2l&ds=DATAFILE

Hiltz, S. R., Benbunan-Fich, R., Coppola, N., Rotter, N., & Turoff, M. (2000). Measuring the Importance of Collaborative Learning for the Effectiveness of ALN: A Multi-Measure, Multi-Method Approach. *The Journal of Asynchronous Learning*, *4*(2), 103–125. Retrieved from http://www.aln.org/alnweb/journa1/jaln-vo14issue2-3.htm

Hochman, N., & Schwartz, R. (2012). Visualizing Instagram: Tracing Cultural Visual Rhythms, Association for the Advancement of Artificial Intelligence. *Sixth International AAAI Conference on Weblogs and Social Media*. Retrieved March 18, 2013 from, http://www.aaai.org/ocs/index.php/lCWSM/lCWSM12/paper/viewFile/4782/5091

Hsu, J. (2011). *U.S considers open-source software for Cyber security*. Retrieved March 22, 2013, from http://www.teclmewsdaily.com/2644-cybersecurity-open-source.html

Hummel, K. A., & Hlavacs, H. (2003). *Anytime, Anywhere Learning Behaviour Using a Web Based Platform for a University Lecture. SSGRR 2003, 7th- 12th of January*. Aquila.

IDC Predicts 2013 Will Be Dominated by Mobile and Cloud Developments as the IT Industry Shifts Tnto Full-Blown Competition on the 3rd Platform. (2012). TDC- Press Release. Retrieved March 22, 2013, from https://www.idc.com/ getdoc. jsp?containerld=prUS23814112

Kwak, H., Lee, C., Park, H., & Moon, S. (2010). What is Twitter, a Social Network of News Media? *Proceedings of the 19111 International Conference on World Wide Web*. doi:10.1145/1772690.1772751

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). *Social Media & Mobile Internet Use Among Teens and Young Adults*. Pew Research Center. Retrieved March 20, 2013, from: http://web.pewinternet.org//media/Files/Reports/2010/PlPSocialMediaandYoungAdultsReportFina!withtoplines.pdf

Lewis, B. K. (2012). *Social Media and Strategic Communications: Attitudes and perceptions Among College Students* (Doctoral Dissertation). Available from ProQuest Dissertations and Thesis Full Texts Database. Oklahoma State University. Retrieved March 19, 2013, from http://www.prsa.org/Intelligence/PRJ ournal/Documents/2012LewisN ichols.pdf

Lopez, C. (2009). Immersive technology melds Hollywood, warrior training. *Soldiers*, *64*(5), 27.

Lotring, A. (2005). Training the MlLLENNlAL SAILOR. *U.S. Naval Institute Proceedings*, *131*(12), 36–37.

Mac, R. (2013). *No One Is More Excited For Google Glass Than Facebook CEO Mark Zuckerberg*. Retrieved March 28, 2013 from http:// www.forbes.com/sites/ryanmac/2013/02/21/no-one-is-more excited-for-google-glass-than-facebook-ceo-mark-zuckerberg/

Maxwell, D., & McLennan, K. (2012). Case Study: Leveraging Government and Academic Partnerships in MOSES (Military Open Simulator [Virtual World] Enterprise Strategy). In *World Conference on Educational Multimedia, Hypermedia and Telecommunications*.

Mislove, A., Marcon, M., Gummadi, K. P., Drushel, P., & Bhattacharjee, B. (2007). Measurement and Analysis of Online Social Networks.*Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement*. doi:10.1145/1298306.1298311

Mulliner, C., & Miller, C. (2009). Injecting SMS messages into smartphones for security analysis. *Proceedings of the 3rd USENlX Workshop on Offensive Technologies*. Retrieved March 22,2013 from https://www.usenix.org/legacy/events/woot09/tech/full papers/mulliner.pdf

Muniz, J. (2013). *Web Penetration Testing with Kali Linux*. Packt Publishing Ltd.

Mustafa, M. (2012). *How to Customize the 'Via' Status on Facebook Posts*. Hongkait.com Inspiring Technology. Retrieved on April18, 2013, from; http:// www.hongkiat.com/blog/customize-facebook status/

Myers, S. (2012). Operative BackTrack. *Journal of On Demand Hacking, 1*(3), 60-66. Retrieved March 19, 2013, from http://www.backtrack-linux.org/documents/Hakin9 On Deman 03 2012 Teasers.pdf

Naismith, L., Lonsdale, P., Vavoula, G., & Sharples, M. (2006). *Literature review in mobile technologies and learning*. Futurelab Series. Retrieved March 22, 2013, from http://www2.futurelab.org.uk/resources/ documents/1it reviews/Mobile Rev iew.pdf

Omar, M., & Dawson, M. (2013, April). Research in Progress- Defending Android Smartphones from Malware Attacks. *2013 Third International Conference on Advanced Computing and Communication Technologies* (pp. 288-292). Rohtak, India: IEEE.

Park, S. R., Nah, F. F., Dewester, D., & Eschenbrenner, B. (2008). Virtual World Affordances: Enhancing Brand Value. *Journal of Virtual Worlds Research*, *I*(2), 1–18.

Parti, K. (2011). Actual Policing in Virtual Reality - A Cause of Moral Panic or a Justitied Need? In *Virtual Reality*. InTech. Retrieved March 22, 2013, from http://www.intechopen.com/books/virtua1-reality/actua1-poIicing-in-virtua1-reality-a-cause-of-moral panic-or-a-justified-need

Patel, R. S. (2013). *Kali Linux Social Engineering*. Packt Publishing Ltd.

Perens, B. (1999). The open source definition. *Open sources: voices.from the open source revolution,* 171-85.

Popper, S., Bankes, S., Callaway, R., & DeLaurentis, D. (2004). *System-of-Systems Symposium: Report on a Summer Conversation*. Arlington, VA: PotomacInstitute for Policy Studies.

Qualman, E. (2013). *Socialnomics: How Social Media Transforms the Way We Live and Do Business* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Raento, M., Oulasvirta, A., & Eagle, N. (2009). Smartphones: An Emerging Tool for Social Scientists. *Journal of Social Methods & Research*, *37*(3), 426–454. doi:10.1177/0049124108330005

Rajabhushanam, C. C., & Kathirvel, A. A. (2011). System of One to Three Umpire Security System for Wireless Mobile Ad hoc Network. *Journal of Computer Science, 7*(12), 1854-1858.

Rash, W. (2004). Latest skulls Trojan foretells risky smartphone future. Retrieved from www.eweek.com

Reed, D. (2003). *Applying the OSI seven layer network model to information security*. Retrieved March 22, 2013, from http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/7-Sep- 2004/0SI.pdf

Roesch, M. (1999). SNORT-Lightweight Intrusion Detection for Networks. In *Proceedings of LISA '99: 13th USENlX conference on System administration*. Retrieved March 18, 2013, from https://www.usenix.org/legacy/events/!isa99/fuII papers/roesch/roesch.pdf

Sadasivam, K., Samudrala, B., & Yang, A. (2005). Design of Network Security Projects Using Honeypots. *Journal of Computing Sciences in Colleges*, *20*(4), 282–293.

Salah, K., & Kahtani, A. (2009). Improving snort performance under linux. *Communications, JET*, *3*(12), 1883–1895.

Sexton, S. (2011). *What is the Percieved Impact of Social Media on Personal Relationships in Adolescence?* (Doctoral Dissertation). Available from ProQuest Dissertations and Thesis Full Texts Database. Gonzaga University. Retrieved March 20, 2013, from http://gradworks.umi.com/15/03/1503092.html

Siegel, A., Denny, W., Poff, K. W., Larose, C., Hale, R., & Hintze, M. (2009). Survey on Privacy Law Developments in 2009: United States Canada, and the European Union, The American Bar Association Press. *The Business Lawyer*, *65*(1), 285–307.

Snort. (2012). *What is Snort?* Retrieved March 20,2013, from www.snort.org

Socialcast. (2012). *Managing and Control Your Private Network*. Retrieved on April 22, 2013, from http://www.socialcast.com/administration

Surman, G. (2002). *Understanding Security using the OSI Model*. Retrieved March 25, 2013, from http://www.sans.org/reading room/whitepapers/protocols/understanding-security-osi-model377

Turoff, M. (2000). An End to Student Segregation: No more separation between distance learning and regular courses. *On the Horizon*, *8*(I), 1–7. doi:10.1108/10748120010803294

Tuteja, A. & Shanker, R. (2012). Optimization of Snort for Extrusion and Intrusion Detection and Prevention. *International Journal of Engineering Research and Applications, 2*(3), 1768-1774.

Uitzil, L. (2012). Wireless security system implemented in a mobile robot. *International Journal of Computer Science Issues*, *9*(4), 16.

Walker, J. J. (2012). *Cyber Security Concerns for Emergency Management, Emergency Management*. Retrieved from http://www.intechopen.com/books/emergency-management/cyber-security-concerns-for-emergeneymanagement

Wang, P. A. (2010). The Effect of Knowledge of Online Security Risks on Consumer Decision Making in B2C e-Commerce (Dissertation Thesis). ProQuest LLC, Nova Southeastern University.

Weiser, M. (1991).The computer for the 21st century. *Scientific American*, *265*(3), 94–104.

Wong, L. (2005). *Potential Bluetooth vulnerabilities in smartphones*. Retrieved March 18, 2013, from http://citeseerx. ist.psu.edu

Xie, L., Zhang, X., Chaugule, A., Jaeger, T., & Zhu, S. (2009). *Designing system-level defenses against cellphone malware.* Retrieved March 21, 2013, from www.cse.psu.edu

KEY TERMS AND DEFINITIONS

Availability: Timely, reliable access to data and information services for authorized users.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Cloud Computing: Comprised of both the application delivered as services over the Internet and the hardware and systems software housed in the datacenters that provide those services (Armbrust, et al, 2010).

Confidentiality: Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

Hyperconnectivity: Use of multiple means of communications such as instant messaging, phones, Web 2.0, Web 3.0, and other communication methods.

Integrity: Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Non Repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Open Source Software: Software that allows the original source code to be free available which may be freely redistributed or modified (Perens, 2009).

Developing Next-Generation Countermeasures for Homeland Security Threat Prevention

Maurice Dawson
University of Missouri-St. Louis, USA

Dakshina Ranjan Kisku
National Institute of Technology, India

Phalguni Gupta
National Institute of Technical Teachers' Training & Research, India

Jamuna Kanta Sing
Jadavpur University, India

Weifeng Li
Tsinghua University, China

A volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

IGI GLOBAL
DISSEMINATOR OF KNOWLEDGE

www.igi-global.com

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Dawson, Maurice, 1982- editor.
Title: Developing next-generation countermeasures for homeland security threat prevention / Maurice Dawson, Dakshina Ranjan Kisku, Phalguni Gupta, Jamuna Kanta Sing and Weifeng Li, editors.
Description: Hershey, PA : Information Science Reference, [2017] | Includes bibliographical references and index.
Identifiers: LCCN 2016023422| ISBN 9781522507031 (hardcover) | ISBN 9781522507048 (ebook)
Subjects: LCSH: Terrorism--United States--Prevention. | Terrorism--Prevention. | National security--United States. | Internal security--United States.
Classification: LCC HV6432 .D48 2017 | DDC 363.325/170973--dc23 LC record available at https://lccn.loc.gov/2016023422

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 5
Islamic Extremists in Africa:
Security Spotlight on Kenya and Nigeria

Maurice Dawson
University of Missouri – St. Louis, USA

Wale Adeboje
South Wesleyan University, USA

ABSTRACT

Security is a growing concern on the African continent as the Regional Economic Communities (REC) move toward economic integration. Furthermore, these regions collectively make up the African Union (AU) which has an objective to promote peace, security, and stability on the African continent. In recent years, Africa has been plagued with political uprisings, civil wars, extremists, corrupt politicians, and the battle for natural resources. In particular, Kenya and Nigeria are facing Islamic extremists that threaten the foundation of multiple nations. In both countries, they are using military force to combat these threats. This chapter provides insight into these West and East African nations and their means to provide security assurances to their citizens.

INTRODUCTION

The AU has released some press statements regarding matters dealing with national security to the exploitation of natural resources (African Union Peace and Security, n.d.). Of these issues the Somali originated group Al-Shabaab, and Nigerian originated group Boko Haram appear to be taking international headlines. The groups have continuously shaken the foundation for these countries. Also these groups have expanded their reach to other neighboring states. Boko Haram has attacked not only Nigeria but Cameroon, Chad, Niger, and the Republic of Benin (Mantzikos, 2014). Their insurgency has cost more than 4,000 lives in the years of 2010 to 2014. Al-Shabaab is yet another result of a growing insurgency which is attracting global jihadists with shared ideology than ethnic or nationalist sentiments (Vidino, Pantucci, & Kohlmann, 2010).

DOI: 10.4018/978-1-5225-0703-1.ch005

The AU's African Peace and Security Architecture (APSA) has implemented the African Standby Force (ASF) to be divided into tasks with various regions. APSA provided the following recommendations; 1. clarify PSC relationship with panel, 2. enforce criteria for appointing PSC members, 3. improve synergy between PSC and other APSA components, 4. provide additional analysts for the CEWS and early warning, 5. provide joint training and skills development, 6. ensure connectivity between AUC and RECs, 7. increase and strengthen collaboration with other actors, and 8. increase flexibility and reliability of external support (Fisher, et al, & 2010). Recommendations covered that cover the ASSF were the following: 1. adopt binding legal instrument with member states, 2. harmonize membership of standby arrangements, 3. improve staffing of PLANELMs at AU and RECs/RMs, 4. strengthen management of the ASF, 5. address logistics gap as priority, and 6. provide guidance and leadership for centers for excellence (Fisher, et al., & 2010).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The Organisation for Economic Co-operation and Development (OECD) is an international economic organization that is comprised of 34 countries. OECD publishes reports, books, and other statistics that allow for further understanding various markets. Key artifacts published are the OCED Economic Outlooks, Main Indicators, OECD Communications Outlook and the OECD Internet Economy Outlook (OECD, 2012). Significant amounts of reports are created for Kenya and Nigeria. These reports include economics, corruption indicators, and key events such as the Trans-Saharan gas pipeline which affects Nigeria significantly. This pipeline could pose a security issue as Nigeria is known for ongoing conflicts in the Niger Delta. The data contained within OECD can be mined, and literature analyzed to assist in making key strategic military decisions.

AFRICAN UNION

The African Union (AU), formally called Organization of African Unity (OAU) was founded in Cairo in the 29th Ordinary Session of the Assembly of Heads of State and Government of the organization that was held from the 28th to 30th of June 1993. The name of the union was changed from OAU to AU in May 2001. AU is a union of fifty-four countries in the African continent with its headquarters in Addis Ababa, Ethiopia. All the countries in Africa are members of the AU except Morocco due to the present status of the Western Sahara. The highest level decision-making body of the African Union is the Assembly of the African Union (AAU). The AAU is made up of all members of states and is currently headed by Robert Mugabe, the president of Zimbabwe.

The objectives of the AU include:

1. To defend the African territory and its member states.
2. Promote peace, security and unity among its member states.
3. To encourage and promote political and socio-economic cooperation among its member states.
4. To promote development in the African continent by encouraging research in all fields most especially in the areas of science and technology.
5. To eradicate and combat preventable disease and encourage the promotion of good health on the African continent.

PARTICIPATING AND NONPARTICIPATING COUNTRIES

The member states of the AU includes Algeria, Egypt, Madagascar, Seychelles, Angola, Equatorial Guinea, Malawi, Sierra Leone, Benin, Eritrea, Mali, Somalia, Botswana, Ethiopia, Mauritania, South Africa, Burundi, Gabon, Mauritius South Sudan, Cabo Verde, Gambia, Mozambique, Sudan, Cameroon, Ghana, Namibia, Swaziland, Chad, Guinea, Niger, Tanzania, Comoros, Guinea-Bissau, Nigeria, Togo, Congo-Brazzaville, Kenya, Rwanda, Tunisia, Cote d'Ivoire, Lesotho, Sahrawi Arab Democratic Republic, Uganda, Democratic Republic of Congo, Liberia, Zambia, Djibouti, Libya, Sao Tome and Principe, Zimbabwe, and Senegal (Union, 2000). Morocco is not a member state due to a dispute over the Western Sahara. The Central African Republic and Burkina Faso are also currently suspended. With Haiti having the status of Member Observer with the AU making it the first member country outside of the African continent.

MILITARY

The promotion of peace, stability and security among its member of states is one of the major objectives of the AU. The peace and security council arm of the African Union is the unit charged with ensuring the peace, stability and security of its members states. The peace and security council arm of the African Union has the authority to issue peace support missions among its member states, impose sanctions on member states where there is an unconstitutional change in government and to take initiatives in responding and taking actions when there are conflicts among members states. Article 4(h) of the Constitutive Act, repeated in Article 4 of the Protocol to the Constitutive Act on the Peace, Stability and Security (PSC) arm of the AU give the AU the authority to intervene in its members' states in situations where there is genocide, a crime against humanity and war crime. The Assembly of the AU has the ultimately authority to intervene in member states based on the recommendation of the peace and security council of African Union. In the past, African Union have intervened in conflicts in Sudan and Somalia sending about 7,000 peacekeeping armed forces to Sudan and about 8,000 peacekeeping armed forces to Somalia.

REPUBLIC OF KENYA AND THE EAST AFRICAN COMMUNITY OF STATES

The Republic of Kenya (Figure 1.) is located in Eastern Africa between Somalia and Tanzania. Kenya shares borders with five countries which are the following: Ethiopia, Somalia, South Sudan, Uganda, and Tanzania (CIA, 2015a; CIA, 2015b; Knox, 1996). In 2013, the World Bank estimated the population to be 44.35 million people. Thus, the population is slightly lower than Tanzania but larger than that of Uganda. Kenya belongs to the East African Community (EAC) which is a regional intergovernmental organization that consists of the Republics of Burundi, Kenya, Rwanda, the United Republic of Tanzania, and the Republic of Uganda (East African Community, 2015). The headquarters for the EAC is in Arusha, Tanzania. In 1979, integration issues were studied concerning the East African Community, which is still in existence today (Hazlewood, 1979). The membership is important as this allows member countries to move freely between the countries without the need for a visa. Other benefits include those that affect mobility. This includes the ability to utilize current driver license in residing EAC state anywhere within the EAC Partner States (East African Community, 2015). The mobile phone can be used anywhere through the EAC region due to a series of inter-operator roaming agreements (East African Community, 2015).

Figure 1. Kenya

RELATIONSHIP WITH SOMALIA

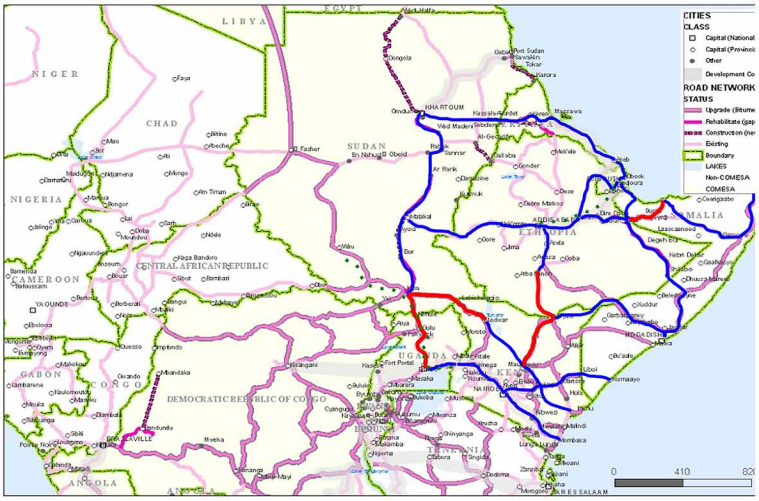
Kenya shares a border with Somalia to the east while the largest borders are shared with Ethiopia, Uganda, and Tanzania (Bradbury & Kleinman, 2010). Kenya and Ethiopia are key decision makers on Somali polices with significant influence comparable to the country's Mogadishu-based Federal Government of Somalia (FGS). The strategic concerns of both nations differ than one another. Some of AU members have their military active in Somalia. Placing the military here is to reduce the number extremist incidents in the country and to neighboring countries.

Even though there is unrest with the extremist organization in East Africa economic development continues in the region (Figure 2.). These initiatives originate from the European Union (EU) regional political partnership for peace and security region in this area. The Intergovernmental Authority on Development (IGAD) is a trade block in Africa that includes member countries Djibouti, Eritrea, Ethiopia, Kenya, Somalia, Sudan, and Uganda (Shah, Banerjee, & Larson, 2007). As the United Nations (U.N.) General Assembly admitted South Sudan as the 193rd member of the U.N. the IGAD recognized South Sudan as a member. (Reuters Africa, 2011). The IGAD is focused on projects such as those focused on improving infrastructure to increase trade in the area. These projects include four new roads that are part of the ring corridor, four energy links, four renewable energy projects, and six water-food security projects estimated at 5.4 billion Euros (IGAD, 2011).

AL-SHABAAB

Al-Shabaab is a Somalian terror group has been identified as an al Qaeda affiliate. The name Al-Shabaab rough translates into The Youth (Shinn, 2011). The FGS control very little territory in Somalia (Shinn, 2011). It is Al-Shabaab that controls nearly all of central and southern Somalia. The end goal is to

Figure 2. Horn of Africa Infrastructure Projects
(Source: IGAD, 2011).

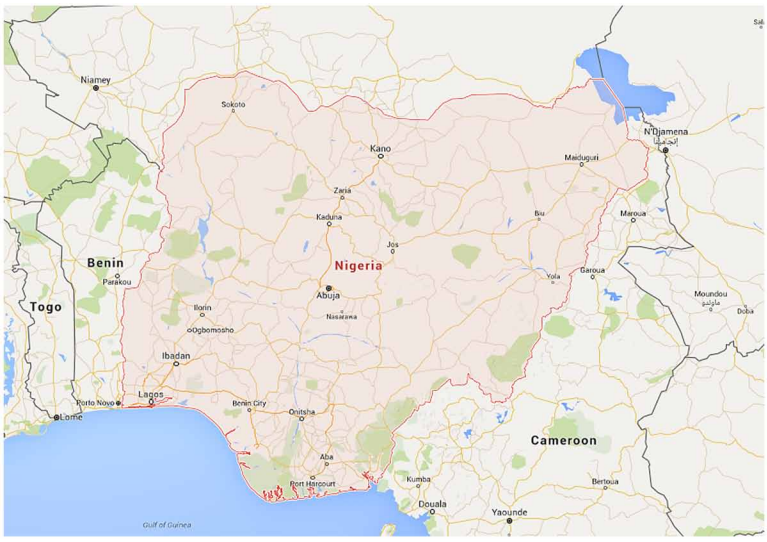


incorporate Somali-inhabited areas of Kenya and Ethiopia to bring into existence an Islamic caliphate (Shin, 2011). In 2010, Uganda suffered approximately 80 casualties tied to Al-Shabaab. Somalia has had terrorists and extremist groups for years. It wasn't until the failure of the Somali state that offered an opportunity to Islamist groups. Based on declassified al Qaeda documents, shown is that Abu Hafs al Masri made multiple trips to Somalia in 1992 (Shin, 2011). He conducted capabilities assessments, created arrangements for training, and arms for fighters. Masri has been identified as a key lieutenant to Osama Bin Laden traveling to multiple countries in Africa and the Middle East spreading extremist ideology.

NIGERIA

Nigeria is Africa's most populous nation and largest economy. Nigeria is a country in the western part of Africa, bordering the Gulf of Guinea, between Benin and Cameroon [See Figure 3.]. It has an estimated population of over 160 million people, with the largest black population in the world. It is one of the major oil producing counties in the world and has a lot of natural resources. The land area of Nigeria is approximately 900,000 square kilometers and has Abuja as its capital since 1991. Nigeria has more than 250 ethnic groups with Hausa and the Fulani tribes making up 29% of the population. The Yoruba tribes have about 21%, Igbo or Ibo has 18%, Ijaw has a little over 10%, Kanuri has over 4%, Ibibio has about 3.5%, and the Tiv with about 2.5%. The major religions in Nigeria are Christianity and Islam. The Northern part of Nigeria are majority Muslim while the southern part of Nigeria is made of mostly Christians and Muslims. In the north of Nigeria, where the population are mostly Muslims, there is a lot of unrest today due to the presence of a group called Boko Haram.

Figure 3. Nigeria



OIL

Nigeria is a major producer of oil and is a member of the Organization of Petroleum Producing Countries (OPEC). Nigeria is one of the leading oil and gas producers in Africa and is the seventh highest producer of oil and gas in the world (Taiwo, 2010). The oil sectors account for over 70% of government revenue and over 90% of exports. Nigeria has an enormous deposit of oil and gas within the country. The exploitation of the deposits of oil and gas has improved the economic status of the country however Nigeria's economy is very dependent on oil and gas which is the primary source of funding for the economy. Most of Nigeria's oil are in the Niger Delta region of the country. The exploration of the oil in Nigeria is carried out on a joint venture between Nigeria and some foreign multi-national organizations such as Shell, Exxon-Mobil, Agip, Chevron, Total, Texaco among others. There is major rural-urban and regional tensions due to natural resource endowments, unequal access to political powers, poor federal services to various groups, and uneven shares of national wealth (AfDB, OECD, UNDP, & ECA, 2013). Nigeria has (Barungi, Ogunleye, & Zamba, 2015).

NIGERIAN MILITARY

The Nigerian Military Forces are the armed security forces of the country called Nigeria and currently has over 200,000 military personnel in three armed service groups. The three armed service groups are the Army, Navy, and the Air Forces. The military group in Nigeria has the major responsibility for protecting the citizens and borders of the Federal Republic of Nigeria. The Nigerian military forces have been involved in various combat efforts in the past in protecting the sovereignty of the country including the Nigerian civil war (1967-1970), conflicts in the Niger Delta and recently the Boko Haram insurgency in the northern part of the country.

BOKO HARAM

The Boko Haram is a religious terrorist group in Nigeria that started in 2002. It is an Islamic conservative group that attempts to impose its religious ideology in the country (Adesoji, 2010). The name Boko Haram means "non-Islamic education is a sin" and it is the beliefs of this group that Muslims should avoid the Western education but embrace Islamic education. Boko Haram is derived from the Hausa word "boko" meaning book and the Arabic word "haram" meaning sinful or ungodly. The first internationally publicized Boko Haram crisis started on the 25th of July, 2009 and went on till the 30th of July, 2009, with the crisis spreading through four states including Bauchi, Kano, Yobe and Borno (Adesoji, 2010). Borno State has received a number of causalities, serves as the base of the leadership. Boko Haram has grown to other states in Nigeria over time and has been involved in a number of terrorist acts since 2009. Boko Haram have attacked cities like Abuja the capital of Nigeria and Chibok (Borno State) where 276 female students were abducted by the Islamist militants. The kidnapping of the Chibok female students have attracted a lot of international attention, with a many of human rights organizations calling on the Boko Haram sects to release the kidnapped children.

Although Boko Haram has its main base in Nigeria, it has also carried out attacks in Nigeria's neighboring countries like Chad, Benin, Niger and Cameroon. It is reported that the terror group have killed about 17,000 people and is responsible for the displacement of more than two million inhabitants (most of the northern hemisphere of Nigeria). Today, Boko Haram is causing a lot of unrest in Nigeria (mostly in the north part of Nigeria) and the government is Nigeria has dispatched a lot of military personnel to combat rising cases of Boko Haram attacks. The United States of America (USA) has also launched a surveillance and intelligence mission in Nigeria against the militant group as part of its support for Nigeria in its combat against Boko Haram. Nigeria and its neighboring countries have also formed a joint task force to combat the efforts of the militant group in the region. This has resulted in the reduction of Boko Haram attacks in Nigeria. However, the Islamic State of Iraq (ISIS) is overtaken by Boko Haram as the world's deadliest terror organization (Buchanan, 2015). In 2015, Boko Haram, changed its named to Islamic State West Africa Province (ISWAP).

FULANI MILITANTS

Nigeria is not only home to the terrorist group Boko Haram, but also to the Fulani Militants, which is another Islamic militant group. This is not to be confused with the Fula people or Fulana, who are a nomadic tribe dispersed all over western Africa. The Fula are also found in Egypt and Sudan. As of November 2015, the Global Terrorism Index (GTI) lists the Fulani Militants as the fourth deadliest terror group in the world (Buchanan, 2015).

GLOBAL TERRORISM DATABASE

University of Maryland's National Consortium of the Study of Terrorism and Responses to Terrorism retains an open source database on events from 1970 through 2014 (START, n.d.). START (n.d.) maintains the Global Terrorism Database (GTD) which more than 140,000 terrorist events. These events can be further examined to display explore connections between people, places, and events.

From the years, 1975 to 2013 GTD reports 2482 incidents within Somalia with 446 incidents from 1973 to 2013 in Kenya. The Kenya events saw a huge increase starting in 2010 (START, n.d.). During those dates cities affected the most were Garissa, Ifo, Lami, Libooi, Likoni, Madio Gashi, and Mandera (START, n.d.). In the same time frame Nigeria has had 2251 incidents specifically during the years of 1991 to 2013. The spike in incidents occurs in the years of 2007 to 2013. Those responsible for the terrorist incidents in Nigeria are Boko Haram, Fulani Militants, and other unknown identified groups. Some of the cities with fatalities of at least 15 are Kano, Gwoza, Bama, Jaji, Yelwa, Ife, Kautikiri, Fadama-Bona, Abulagu, Damboa Kampani, Maidurguri, Daku, Bantji, Shengev, Gajiram, Maikkadiri, Sangan Atakar, Kiyak, Musari, Ndongo, and Kuzen (START, n.d.). During the dates of September 17, 2014, Konduga experienced 201 fatalities on a private citizens and property by armed assault. The armed attack included explosives, bombs, dynamite, and farmers (START, n.d.). Before that attack on September 12, 2014, the results were 81 casualties due to a similarly armed assault. In Ethiopia, Al-Shabaab is responsible for approximately 114 fatalities in the years of 2007-2014 (START, n.d.). The majority of the casualties caused in Ethiopia are due to violent political parties such as the Ethiopian People's Revolutionary Party, and the Tigray People's Liberation Front (TPLP). Together the groups have claimed more than 400 lives.

It is essential that you look at the number of casualties caused by terrorist groups to understand the deadliest organization. In reviewing the data from the Institute for Economics & Peace's Global Terrorism Database (GTD) another view is provided. Boko Haram has claimed a total of 6,644 lives while Isis claimed 6,073 [See Figure 4.]. Looking at the Nigerian combined terrorist groups Boko Haram and Fulani Militants the total count is 7,873. The threat of deadliest terror organizations on the continent of Africa is 8,894.

In reviewing deaths that have occurred from 2013 - 2014 it is clear that Nigeria has the highest count at 5.662 with Iraq at 3,532 following by Afghanistan at 1,391 [See Figure 5.]. These deaths show how extreme the groups Boko Haram and Fulani Militants are in Nigeria to include surrounding areas. The stability of this region is dependent upon neutralizing this threat which has claimed so many lives in a short period.

Figure 4. World's Deadliest Terror Organization
(Source Institute for Economics & Peace, 2015)

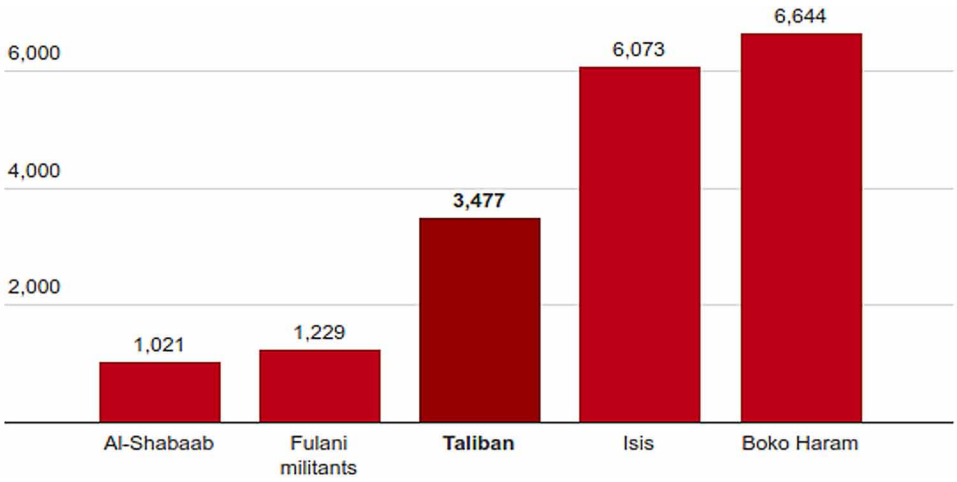
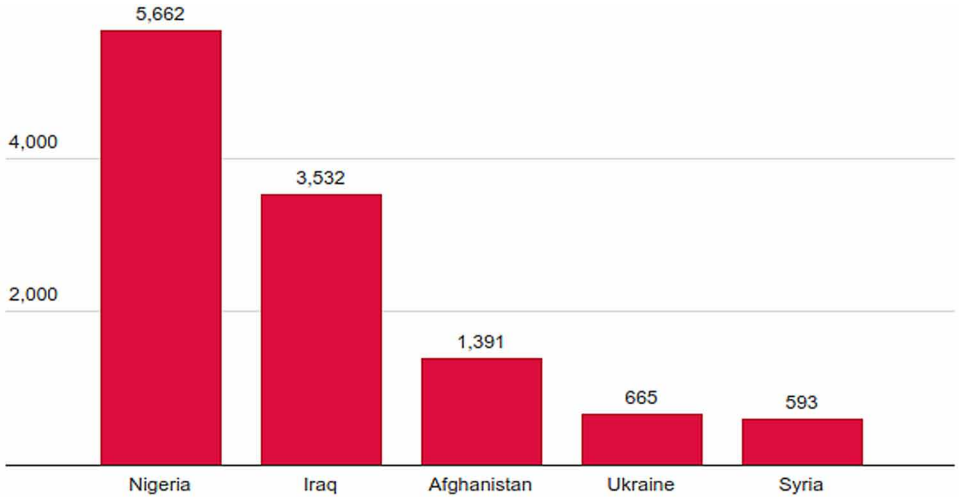


Figure 5. 2013-2014 Deaths
(Source Institute for Economics & Peace, 2015)



CONCLUSION

The countries of Nigeria and Somalia are home to three of the most violent terrorist organizations in the world. It is essential to correct this issue if Africa is to move toward economic integration in the future. As the AU has an objective to promote peace, security, and stability on the African continent these organizations need to be neutralized. As Nigeria has surpassed South Africa as Africa's largest economy, it is important for this country to become a role model for ECOWAS nations and the rest of Africa. Kenya must find a balance in proper integration of Somalis while neutralizing the threat of Al Shabaab.

REFERENCES

Adesoji, A. (2010). The Boko Haram Uprising and Islamic Revivalism in Nigeria / Die Boko-Haram-Unruhen und die Wiederbelebung des Islam in Nigeria. *Africa Spectrum, 45*(2), 95–108. Retrieved from http://www.jstor.org/stable/25798918

AfDB, OECD, UNDP, & ECA. (2013). African Economic Outlook 2013. African Development Bank, Organisation for Economic Co-Operation and Development, United Nations Development Programme, United Nations Economic Commission for Africa, Nigeria.

African Union. Peace and Security. (n.d.). *Ending conflicts, sustaining peace - African Union - Peace and Security Department*. Retrieved December 15, 2015, from http://www.peaceau.org/en/

Barungi, B., Ogunleye, E., & Zamba, C. (2015). *Nigeria 2015; African Economic Outlook*. Retrieved March 07, 2016, from http://www.africaneconomicoutlook.org/en/country-notes/west-africa/nigeria/

Bradbury, M., & Kleinman, M. (2010). *Winning Hearts and Minds?: Examining the Relationship Between Aid and Security in Kenya*. Medford, MA: Feinstein International Center, Tufts University.

Buchanan, R. T. (2015, November 17). *Isis overtaken by Boko Haram as world's deadliest terror organisation*. Retrieved March 16, 2016, from http://www.independent.co.uk/news/world/africa/boko-haram-overtakes-isis-as-worlds-deadliest-terror-organisation-a6737761.html

Buchanan, R. T. (2015, November 18). *Global Terrorism Index: Nigerian Fulani militants named as fourth deadliest terror group in world*. Retrieved March 16, 2016, from http://www.independent.co.uk/news/world/africa/global-terrorism-index-nigerian-fulani-militants-named-as-fourth-deadliest-terror-group-in-world-a6739851.html

Chothia, F. (2012). Who are Nigeria's Boko Haram Islamists?. *BBC News, 11*.

CIA. (2015a, December 9). *Africa: Kenya*. Retrieved December 14, 2015, from https://www.cia.gov/library/publications/the-world-factbook/geos/ke.html

CIA. (2015b, December 9). *Africa: Nigeria*. Retrieved December 14, 2015, from https://www.cia.gov/library/publications/the-world-factbook/geos/ke.html

East African Community. (2015). *East African Community - Burundi, Kenya, Rwanda, Tanzania, Uganda*. Retrieved December 15, 2015, from http://www.eac.int/

El Fadl, K. A. (2005). *The great theft: Wrestling Islam from the extremists*. New York: HarperSanFrancisco.

Fisher, L. M., Bah, A. S., Mniema, A., Okome, H. N., Tamba, M., Frederiksen, J., & Reeve, R. et al. (2010). *African peace and security architecture (apsa): 2010 assessment study*. Tanzania: Zanzibar.

Griffin, A. (2015, November 18). *Facebook Safety Check turned on for Nigeria Boko Haram bombing, after Paris attacks controversy*. Retrieved March 16, 2016, from http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-safety-check-turned-on-for-nigeria-boko-haram-bombing-after-paris-attacks-controversy-a6738736.html

Hazlewood, A. (1979). The end of the East African Community: What are the lessons for regional integration schemes? *JCMS: Journal of Common Market Studies*, *18*(1), 40–58.

IGAD. (2011, August 1). *About Horn of Africa Initiative (HOAI)*. Retrieved March 16, 2016, from http://igad.int/index.php?option=com_content

Institute for Economics & Peace. (2015). *Global Terrorism Index*. Retrieved March 17, 2016, from http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf

Knox, A. (1996). Nigeria country profile. *Country profiles of land tenure. Africa*, 110–115.

Mantzikos, I. (2014). Boko Haram Attacks in Nigeria and Neighbouring Countries: A Chronology of Attacks. *Perspectives on Terrorism, 8*(6).

OECD. (2012, January 16). *Guidelines for multinational enterprises*. Retrieved December 14, 2015, from http://www.oecd.org/daf/inv/mne/

Reuters Africa. (2011, November 25). *East African bloc admits South Sudan as member*. Retrieved March 14, 2016, from http://af.reuters.com/article/investingNews/idAFJOE7AO0A820111125

Shah, P., Banerjee, S. S., & Larson, G. (2007). *Inter-Governmental Authority on Development (IGAD), Africa-IGAD Regional HIV/AIDS Partnership Program (IRAPP)*. Support Project.

Shinn, D. (2011). Al Shabaab's Foreign Threat to Somalia. *Orbis*, *55*(2), 203–215. doi:10.1016/j.orbis.2011.01.003

START. (n.d.). *Information on more than 140,000 Terrorist Attacks*. Retrieved March 16, 2016, from http://apps.start.umd.edu/gtd/

Taiwo, A. S. (2010). The influence of work environment on workers productivity: A case of selected oil and gas industry in Lagos, Nigeria. *African Journal of Business Management*, *4*(3), 299–307.

Union, A. (2000). *The Constitutive Act*. Addis Ababa: African Union.

Vidino, L., Pantucci, R., & Kohlmann, E. (2010). Bringing Global Jihad to the Horn of Africa: Al Shabaab, western fighters, and the sacralization of the Somali Conflict. *African Security*, *3*(4), 216–238. doi:10.1080/19392206.2010.533071

KEY TERMS AND DEFINITIONS

African Union: A continental union consisting of fifty four countries in Africa (Union, 2010).

Al-Shabaab: An al Qaeda affiliate in Somalia that has conducted terrorist attacks in Ethiopia, Kenya, and Somalia.

Boko Haram: A terrorist group founded in 2002 in northern Nigeria that promotes a version of Islam that makes it forbidden for Muslims to take part in any political activities association with the western society (Chothia, 2012).

Extremists: A person or group holding extreme political or religious views that can resort to extreme action (El Fadl & K, 2005).

Fulani Militants: A terrorist group in Nigeria that also operates in the Central African Republic (CAR).

Islamic States West Africa Province: New name for Nigerian terrorist group Boko Haram.

Organization of African Unity: Former international organization, established in Ethiopia, by thirty seven independent members focused on removing all forms of colonialism.

Union: The African Union established by the present Constitutive Act (Union, 2010).

2016

The Case for UBUNTU Linux Operating System Performance and Usability for Use in Higher Education in a Virtualized Environment

Maurice Dawson
University of Missouri-St. Louis, dawsonmau@umsl.edu

Brittany DeWalt
Alabama A&M University, bdewalt@bulldogs.aamu.edu

Simon Cleveland
Nova Southeastern University, sc1674@nova.edu

THE CASE FOR UBUNTU: LINUX OPERATING SYSTEM PERFORMANCE AND USABILITY FOR USE IN HIGHER EDUCATION IN A VIRTUALIZED ENVIRONMENT

Maurice Dawson University of Missouri-St. Louis
dawsonmau@umsl.edu

Brittany DeWalt Alabama A&M University
bdewalt@bulldogs.aamu.edu

Simon Cleveland
Nova Southeastern University
sc1674@nova.edu

ABSTRACT

The use of Linux based Operating Systems (OS) in the classroom is increasing, but there is little research to address usability differences between Windows and Linux based OSs. Moreover, studies related to the ability for students to navigate effectively between Ubuntu 14.04 Long Term Support (LTS) and Windows 8 OSs are scant. This research aims to bridge the gap between modern Linux and Windows Oss, as the former represents a viable alternative to eliminate licensing costs for educational institutions. Preliminary findings, based on the analysis of the System Usability Scale results from a sample of 14 students, demonstrated that Ubuntu users did not require technical support to use the system, while the majority found little inconsistency in the system and regarded it as well integrated.

Keywords

Usability; Linux; Computers; Information Systems; Performance; Human Computer Interaction; UX; Ubuntu; SUS

INTRODUCTION

Presently, adoption of Linux in the personal computers market is limited when compared to the Microsoft Windows OS. For example, a recent study found that Linux held only 1% of the market share, while Microsoft Windows retained 87% (Net Market Share, 2011). When it comes down to ownership of OS, a client has two options: to buy proprietary OS, such as those offered by Microsoft, or to use open source OS free of charge (Boitor and Bratucu, 2011). Microsoft Windows is a proprietary software, which means it is closed, available at a cost, and its copyright is owned by the developers (Haider and Koronios, 2008). As a result, the source code is not available to the end user and changes cannot be made. In contrast, open source systems (OSS) allow end users access to the source code and customizing privileges for their personal use.

Considering the access to the source code as a major advantage (O'Hara and Kay, 2003), it is puzzling that Linux market share is still limited. This confusion is further compounded since a number of studies demonstrate that adoption of open source software yields reduction in costs and ease of customization (Li et al., 2011; Ven et al., 2008). Moreover, Linux has been found to be superior in customizability, security and even reliability (Ebert, 2008).

Prior research has examined the motivations of users to adopt OSS (Gallego et Al., 2008), adoption of OSS by organizations (Macredie and Mijinyawam 2011) and resistance of users (Kim et al., 2014). Areas that still remain unexplored include integration of system functionality and need for technical support. As a result, a key research question that demands an answer is: how is Linux OS perceived by users in terms of usability, integration of functionality and need for technical support in educational institutions when compared to Windows OS?

To address this question, we leverage the System Usability Survey (SUS) to examine these factors among users of Ubuntu 14.04 LTS and Windows 8.1 OS. The limited preliminary findings suggest that further research into the proposed factors is necessary to help determine lack of adoption of Linux into educational institutions.

The rest of this study is structured as follows. First, identification of key components of the OS are outlined. Next, a brief review of the instrument used for the study and preliminary results are provided. The study concludes with recommendations for future research.

OPERATING SYSTEM

An Operating System (OS) is defined as a program that acts as an intermediary between a user of a computer and the computer hardware (Silberschatz and Galvin, 1994). It is a software component that is responsible for the coordination of activities and sharing of computer resources. An OS is a collection of system programs, tools and utilities that manage computer hardware and offer general services for client application software (Bassil, 2012). The operating system is the first program to do several tasks while focusing on the current task at hand. The first task is prompting the OS to boot the computer. Within minutes, the computer will manage tests to make sure everything is working properly, check for new hardware updates and then start the operating system. Once the OS is working, its main focus is to handle the specifics and writing capabilities. The operating system will coordinate with each computer's central processing unit (CPU), memory and storage to make sure that every program functions properly. An OS runs user application programs and provides a suitable interface to communicate with the computers' hardware (Bassil, 2012).

The main purpose of an OS is to provide management of computer resources and control data flow. These resources include but are not limited to memory, processors, input and output devices and abiding storage devices. The concept provided for the operating system is usually in sets providing access. Technologist uses their concepts when writing codes that are needed to obtain the operating system.

Technical Support

Technical support is defined as the need for help provided by knowledgeable individuals to users of computer hardware and software products (Wilson, 1991). In this study, technical support is regarded as coaching and consultation for the installation of OS on a virtual environment. Moreover, lack of need for technical support can be regarded as a positive factor toward cost reduction and ease of use.

Virtualization is referred to as the use of virtualization software that allows physical hardware of a single PC to run numerous operating systems simultaneously on virtual machines (VM). A VM is a fully protected and isolated copy of the underlying physical machine's hardware (Sugerman et al., 2001). In essence, each user is given the impression of having a decent physical computer. This study argued that lack of need for technical support during the installation of the system. Figure 1 provides a screenshot of Ubuntu 14.04 LTS running on a VM on the Windows 8.1 desktop.

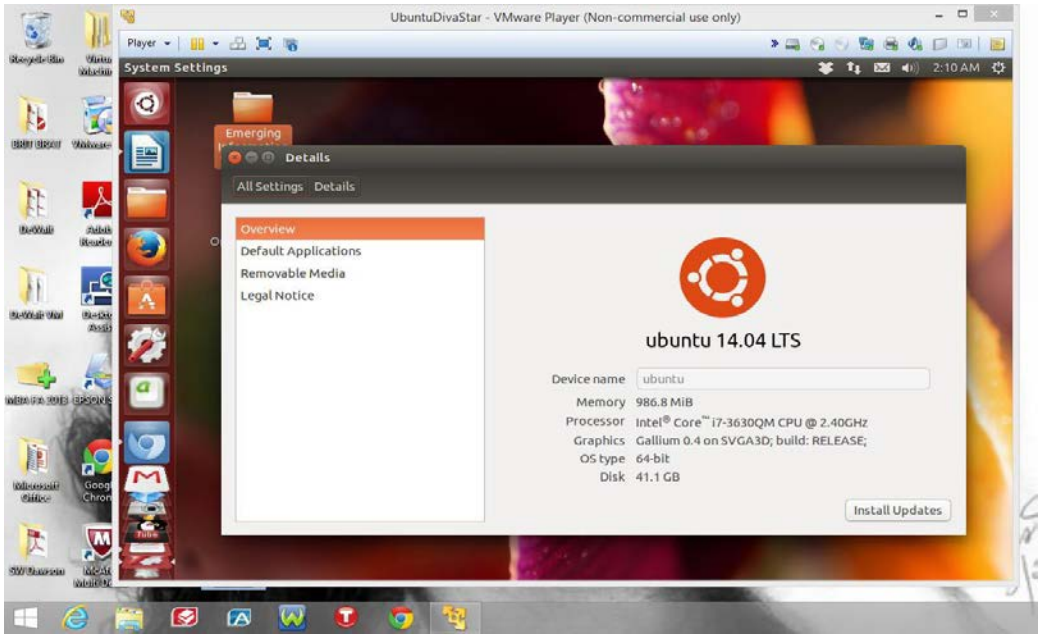


Figure 1: Screenshot of Ubuntu 14.04 VMware VM Running on Windows 8.1 Desktop.

Performance

The significance of the term "performance" is the speed in which a computer operates during a benchmark test. The test utilizes several working styles that imitate the work the computer should be doing. A majority of the software specifications has two types of system requirements: minimum or recommended. In addition, the demand for higher processor power and resources are included in the newer system requirements. Ubuntu 14.10 LTS and Windows 8.1 need certain hardware components and these prerequisites are known as system requirements.

The system requirements vary among Ubuntu products. The minimum system requirements for Ubuntu 14.04 LTS supports Integrated Electronics (Intel) and an Advanced Micro Devices (AMD) processors based on computers that run Microsoft Windows and Apple Macintosh systems ("Ubuntu 14.04 (Trusty Tahr) Daily Build"). Table 1 lists hardware specifications that the computer should meet as a minimum requirement. Depending on the computer needs, there are other Ubuntu distributions such as Lubuntu and Xubuntu for less processor power.

Processor	1 gigahertz (GHz) x 86 processor (Pentium 4 or better)
RAM	1 gigabyte (GB)
Hard Disk Space	5 gigabyte (GB) (15 GB is recommended)
Video Support Capable	1024×768 resolution

Table 1. Ubuntu 14.04 LTS Minimum System Requirements

In contrast, Windows 8.1 is a personal operating system that is geared toward Intel-based PC architectures. The minimum system requirements for Windows 8.1 are higher than Windows 7. The CPU supports the Physical Address Extension (PAE), NX processor bit (NX) and Streaming SIMD Extensions 2 (SSE2) (System Requirements, 2014). Windows Store application requires a screen resolution of 1024×768 or higher to run. Table 2 lists the recommended hardware specifications.

Processor	1 gigahertz (GHz) or faster
RAM	1 gigabyte (GB) (32-bit) or 2 GB (64-bit)
Hard Disk Space	16 GB (32-bit) or 20 GB (64-bit)
Graphic Card	Microsoft DirectX 9 graphics device with WDDM driver

Table 2. Windows 8.1 Minimum System Requirements

Usability

Usability is considered the effectiveness, efficiency and satisfaction specified when users achieve specific goals in a particular environment (Bevan, 2009). Research has proposed a number of methods to measure usability. These include product-oriented (e.g. ergonomic attributes) and user-oriented (user mental effort and attitude, user performance and user interaction) (Bevan, 2009). In this study, the usability of Ubuntu 14.04 LTS was approached from the perspective of the user-oriented approach.

Integration

In this study, integration of the OS was examined from the perspective of the Human User Interface (HUI) and Graphical User Interface (GUI). User interface simply means a person controls a software application or hardware device at their own disposal. The human interface guidelines (HIG) are software documents that are developed with application recommendations. Their role is to improve the user experience by devising interface applications that are more creative, learnable and consistent.

The GUI for both OSs is unique in their own way. Windows 8.1 gives users a similar graphical user interface like Ubuntu 14.04 LTS. For years, Windows has tried to change, cut-down and get rid of their versions of its operating systems and standard Windows desktop interface. They have completely changed their interfaces with pop-up windows, scroll bars, buttons and tiny Start buttons just to make them different from the next competitor in their market. Previous Windows graphical user interfaces had four or more applications on one single screen at one time, but not anymore. Windows 8 eliminates all of that and introduces touch-based text labels and controls. The interface for all of these applications are sparse. For example, email, calendar and address book are now present on the screen. There is no need to go to the menu button and scroll up or down for it. Windows 8.1 has presented a new way to any application easier than previous Windows operating systems. Figure 1 displays the differences in both graphical user interfaces for each operating systems.

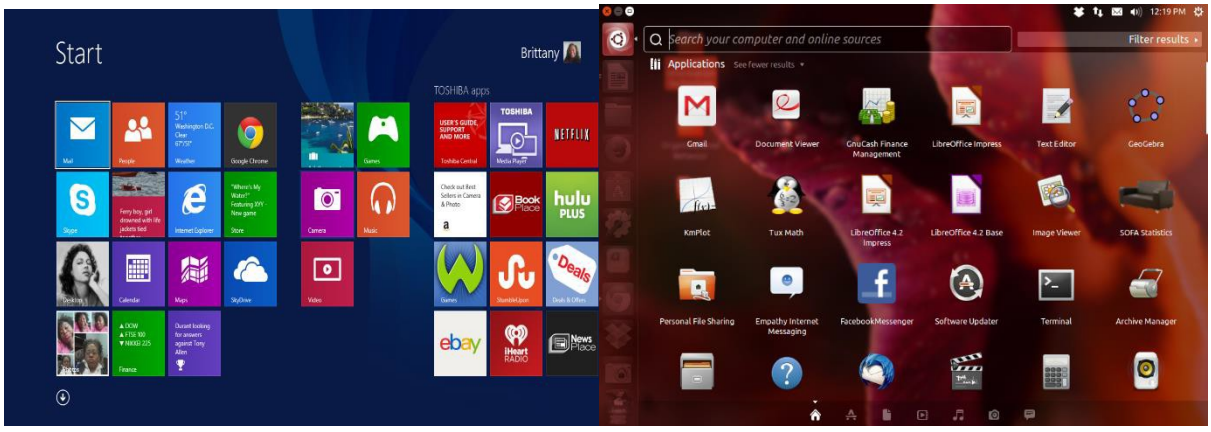


Figure 2: Displays Graphical User Interfaces for both operating systems

RESEARCH METHODOLOGY

Target Population and Data Size

The target population for this study consisted of 14 undergraduate and graduate students from two intermediate information systems course at a Midwestern university. Each participant was familiar with the use of either OS. Participant ages ranged from 18-30 years old.

System Usability Scale (SUS)

To determine usability, integration and need for technical support, this study used the System Usability Scale (SUS). SUS was originally created in 1986 by John Brooke (System Usability Scale, 2014). The scale has been used to evaluate a wide range of products and services, including software, mobile devices, hardware, websites and applications. The reliability of SUS has been demonstrated with smaller sample sizes (Bangor et al., 2009).

In this study, the participants were asked the following 10 questions adopted from the SUS, with responses ranging from Strongly Agree to Strongly Disagree on a 5-point Likert scale:

1. I think that I would like to use this system frequently.
2. I found the system unnecessarily complex.
3. I thought the system was easy to use.
4. I think that I would need the support of a technical person to be able to use this system.
5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system.

To interpret the results, participant's scores for each question were converted to a new number, added together, and then multiplied by 2.5 to convert the original scores of 0-40 to 0-100 (Sauro and Lewis, 2011). The scores were considered in terms of percentile ranking. A SUS score above a 68 was considered above average, while anything below 68 was regarded as below average. Scores were normalized to produce a percentile ranking.

PRELIMINARY FINDINGS

While Ubuntu 14.04 LTS is not difficult to learn, it is different from traditional operating systems. Ubuntu's interface has been developed with features that make it easily adoptable by Window's users (Noyes, 2011). While both interfaces appear different, certain GUI features remain similar. This study found that the majority of users (44%) considered Ubuntu not complex. In terms of difficulty to use, the results showed that while nearly a quarter (22%) found the system not easy to use, over half (56%) where undecided. It can be argued that Ubuntu's interface lacks complexity.

The most important findings of this study were that 78% of the participants strongly disagreed with the statement that they would need the support of a technical person to be able to use the system. Moreover, no respondents disagreed in their perception that the various functions of the system were well integrated. Over half of the respondents (55%) reported that they felt very confident with using the system and didn't need to learn a lot of things to get going with the system. Finally, the majority of the respondents (77%) disagreed with the statement that there was too much inconsistency in the Ubuntu system.

A limitation of this study is the sample, as it is possible that the results are skewed due to the potential presence of power users. In a future study, the researchers will replicate the study using random larger sample and include structured interviews to improve reliability of the results.

CONCLUSION

This research attempted to answer the following research question: how is Linux OS perceived by users in terms of usability, integration of functionality and need for technical support in educational institutions when compared to Windows OS? For this purpose, several factors from the OS were examined (mainly performance, usability, integration and technical support) and the SUS instrument was used to observe users' perceptions of the Linux OS Ubuntu. While the preliminary findings demonstrate that Ubuntu users do not require technical support and perceive the system as well integrated and not inconsistent, the study is limited. Future studies should attempt to examine the factors through the prism of different instruments and with a greater number of subjects.

REFERENCES

1. Bangor, A., Kortum, P., and Miller, J. (2009). Determining what individual SUS scores mean: Adding an adjective rating scale. Journal of usability studies, 4(3), 114-123.
2. Bassil, Y. (2012). Windows and Linux operating systems from a security perspective. Journal of Global Research in Computer Science, 3, 17-24.
3. Bevan, N. (2009). Usability. Encyclopedia of database systems. Springer US. 3247-3251.
4. Boitor, A., and Bratucu, G. (2011). Competition analysis on the operating system market using principal component analysis. Bulletin of the Transilvania University of Brasov, 4(53), 15-22.
5. Ebert, C. (2008). Open source software industry. IEEE Software, 25(3), 52–53. doi:10.1109/MS.2008.67.
6. Gallego, M., Luna, P., and Bueno, S. (2008). User acceptance model of open source software. Computers in Human Behavior, 24(5), 2199–2216. doi:10.1016/j.chb.2007.10.006.
7. Haider, A., and Koronios, A. (2008). Issues of open source software uptake in Australian government agencies (Doctoral dissertation, International Business Information Management Association).
8. Noyes, K. (2011, May 3). Is Linux really harder to use?. PC World, Retrieved April 25, 2014, from http://www.pcworld.com
9. Kim, H. W., Chan, H. C., and Lee, S. H. (2014). User resistance to software migration: The case on Linux. Journal of Database Management (JDM), 25(1), 59-79.
10. Li, Y., Yan, C., Xu, H., and Teo, H. (2011). Open source software adoption: Motivations of adopters and a motivations of non-adopters. The Data Base for Advances in Information Systems, 42(2), 76–94. doi:10.1145/1989098.1989103.
11. Macredie, R. A., and Mijinyawa, K. (2011). A theory grounded framework of open source software adoption in SMEs. European Journal of Information Systems, 20(2), 237–250. doi:10.1057/ejis.2010.60.
12. Net Market Share. (2011). Market share statistics for internet technologies. Retrieved from http:// marketshare.hitslink.com/operating-system-marketshare.aspx?qprid=8

13. O'Hara, K. J., and Kay, J. S. (2003). Open source software and computer science education. Journal of Computing Sciences in Colleges, 18(3), 1-7.
14. Sauro, J., and Lewis, J. R. (2011, May). When designing usability questionnaires, does it hurt to be positive?. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2215-2224). ACM.
15. Silberschatz, A., Galvin, P. B., and Gagne, G. (2013). Operating system concepts (Vol. 8). Wiley.
16. Sugerman, J., Venkitachalam, G., and Lim, B. H. (2001, June). Virtualizing I/O devices on VMware workstation's hosted virtual machine monitor. In USENIX Annual Technical Conference, General Track (pp. 1-14).
17. System requirements - Microsoft Windows. (n.d.). windows.microsoft.com. Retrieved April 24, 2014, from http://windows.microsoft.com/en-us/windows-8/system-requirements
18. System Usability Scale (SUS). (n.d.). Home. Retrieved April 25, 2014, from http://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html
19. Ven, K., Verelst, J., and Mannaert, H. (2008). Should you adopt open source software? IEEE Software, 25(3), 54–59. doi:10.1109/MS.2008.73
20. Wilson, R. (1991). Help!: The art of computer technical support, Peachpit Press, Berkeley, CA.

New Threats and Countermeasures in Digital Crime and Cyber Terrorism

Maurice Dawson
University of Missouri–St. Louis, USA

Marwan Omar
Nawroz University, Iraq

A volume in the Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series

Information Science REFERENCE
An Imprint of IGI Global

Managing Director: Lindsay Johnston
Managing Editor: Austin DeMarco
Director of Intellectual Property & Contracts: Jan Travers
Acquisitions Editor: Kayla Wolfe
Production Editor: Christina Henning
Development Editor: Brandon Carbaugh
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

New threats and countermeasures in digital crime and cyber terrorism / Maurice Dawson and Marwan Omar, editors.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4666-8345-7 (hardcover) -- ISBN 978-1-4666-8346-4 (ebook) 1. Computer crimes--Prevention. 2. Cyberterrorism--Prevention. 3. Computer security. I. Dawson, Maurice, 1982- II. Omar, Marwan, 1982-
HV6773.N4745 2015
005.8--dc23

2015006753

This book is published in the IGI Global book series Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) (ISSN: 2327-0381; eISSN: 2327-0373)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 1
A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism

Maurice Dawson
University of Missouri – St. Louis, USA

ABSTRACT

Cyber security is becoming the cornerstone of national security policies in many countries around the world as it is an interest to many stakeholders, including utilities, regulators, energy markets, government entities, and even those that wish to exploit the cyber infrastructure. Cyber warfare is quickly becoming the method of warfare and the tool of military strategists. Additionally, it is has become a tool for governments to aid or exploit for their own personal benefits. For cyber terrorists there has been an overwhelmingly abundance of new tools and technologies available that have allowed criminal acts to occur virtually anywhere in the world. This chapter discusses emerging laws, policies, processes, and tools that are changing the landscape of cyber security. This chapter provides an overview of the research to follow which will provide an in depth review of mobile security, mobile networks, insider threats, and various special topics in cyber security.

INTRODUCTION

Cyber security has become an important subject of national, international, economic, and societal importance that affects multiple nations (Walker, 2012). Since the early 90s users have exploited vulnerabilities to gain unauthorized access to networks for malicious purposes. In recent years the number of attacks on United States (U.S.) networks has continued to grow at an exponential rate. This includes malicious embedded code, exploitation of backdoors, and more. These attacks can be initiated from anywhere in the world from behind a computer with a masked Internet Protocol (IP) address. This type of warfare, cyber warfare, changes the landscape of war itself (Beidleman, 2009). This type of warfare removes the need to have a physically capable military and requires the demand for a force that has a strong technical capacity e.g. computer science skills. The U.S. and other countries have come to understand that this is an issue and has developed policies to handle this in an effort to mitigate the threats (Dawson, Omar, & Abramson, 2015).

DOI: 10.4018/978-1-4666-8345-7.ch001

In Estonia and Georgia there were direct attacks on government cyber infrastructure (Beildleman, 2009). The attacks in Estonia rendered the government's digital infrastructure useless (Dawson, Omar, & Abramson, 2015). The government and other associated entities heavily relied upon this e-government infrastructure. These attacks help lead to the rapid development of cyber defense organizations throughout Europe which has raised the profile of cyber attacks to include awareness to the potential severity of attacks (Dawson, Omar, & Abramson, 2015).

MOBILE NETWORKS

Mobile networks are found in large cities in America to villages in West Africa. Thus the importance of security in mobile networking is essential to maintaining security and privacy for everyday citizens. Mobile devices have become the preferred device for web browsing, emailing, using social media and making purchases (Wright et al, 2012). Many individuals rely on their mobile devices for texting, checking email, making online purchases, and even remote controlling their home alarm system. Thus attackers have developed malware to specifically target these platforms. Understanding the Human Computer Interaction (HCI) and behavioral issues with mobile devices is a start in understanding human pitfalls in security.

DIGITAL CURRENCY

Digital currency has become a new commerce that is growly quickly and gaining the attention of large financial institutions. This crypto currency has been termed "memory" in monetary economics literature (Luther & Olson, 2013). Bitcoin is a peer to peer electronic cash system in which no one controls and there are not an associated printed currency(Nakamoto, 2008). Bitcoin allows for anonymity to occur in this peer to peer electronic currency systems (Reid & Harrigan, 2013). Some argue that the main benefits are lost if a trusted third party is necessary to prevent the action of double spending (Nakamoto, 2008). The technical infrastructure of this decentralized digital currency relies on several cryptographic technologies.

Luther and Olson state that the principle finding of the money and memory literature is that both devices are capable of facilitating exchange (Luther & Olson, 2013). What is missing from the literature is data concerning the use of Bitcoin for illicit activities. However some researchers attempt to assess potential damages and threats to national security, banking industry, child pornography, drug trade, financial fraud, and more. In relation to cyber warfare Bitcoin could pose as an enabler for plausible deniability of foreign governments and institutions for involvement in cyber attacks (Hilse, 2013). Further cyber criminals could store stolen digital funds on any device that can be used as storage (Hilse, 2013). This could pose a threat as laundered, stolen, or self generated funds can be taken anywhere on a storage device such as a micro Secure Digital (SD) that can hold up to 64 Giga Bytes (GB). This could pose an issue in terms of search and seizure of assets as many police forces have inadequate training and personnel to pull off such measures of cyber forensics on a large scale.

In recent year researchers tackle what they have coined the dark side of cyber finance (Bronk, Monk, & Villasenor, 2012). The key theme to take away is that government and industry will need to be able to react quickly and adapt as the criminals and terrorists to meet the threat (Bronk, Monk, & Villase-

nor, 2012). In a world where monetary funds are difficult to track down through foreign bank accounts digital currency has added yet another lawyer of difficult that allows illicit funds to hide in plain sight. Therefore the only limitations placed the criminals their imagination and skill of individuals who come up with new innovative ways to use technology.

CYBER ESPIONAGE AND SECRECY

Cyber espionage or cyber spying is yet another method of cyber warfare. This method allows for the ability to obtain secrets without the permission of the data owner. The rise in cyber espionage is yet another reason governments must improve cyber security infrastructure. Nakashima details that the U.S. was the target of a massive cyber espionage campaign (Nakashima, 2013). During the Obama Administration the U.S. expanded its cyber reach and infrastructure. However this expanded reach has received negative reviews due to Wikileaks and Edward Snowden.

WikiLeaks and FinSpy

WikiLeaks is an international, online, non profit, journalistic organization that has published classified and sensitive information. This organization claimed to have a database or more than 1 million documents archived from 2006-2010. The servers that were pointing to the website were being shut down on by one (Benkler, 2011). The site contains a sectioned labeled SpyFiles. This section on the site contains SpyFiles with 2 releases in 2011, 1 in 2013, and a release September 2014. The recent release provides insight on FinFisher which is a German company that produces and sells exploitation tools that can take data from multiple Operating Systems (OSs) such as OS X, WIndows, Linux, Android, iOS, Blackberry, Symbian, and WIndows Mobile devices. FinSpy appears to be a malicious trojan designed to intercept and record a variety of information from an infected computer and applications. This software application has been found in Ethiopia aimed at political dissidents (Hankey & Clunaigh, 2013). Even more alarming is that this malicious application has been found within the hands of 25 governments that have questionable records on human rights (Pelroth, 2013). The application has been used to spy own their own citizens. Even Egyptian government members had been given a proposal by the Gamma Group to purchase this Trojan. More troubling is how this application is running on multiple servers with little oversight.

Edward Snowden

Edward Snowden actions will have people regarding him as a patriot or traitor (Goldfarb et al., 2015). Snowden's leak displayed just how big the reach was of the Intelligence Community (IC) into the American public. Snowden's use of a Linux distribution, Tails, that was originally developed as a research project by the U.S. Navy Research Laboratory (NRL) displays the ability to evade detection.

Cyber Weapons: Stuxnet Worm and Flame Malware

During the fall of 20 l 0 many headlines declared that Stuxnet was the game-changer in terms of cyber warfare (Denning, 2012). This malicious worm was complex and designed to target only a specific system. This worm had the ability to detect location, system type, and more. And this worm only attacked

the system if it met specific parameters that were designed in the code. Stuxnet tampered directly with software in a programmable logic controller (PLC) that controlled the centrifuges at Natanz. This tampering ultimately caused a disruption in the Iranian nuclear program.

Flame was yet another highly sophisticated malicious program being used as a cyber weapon in various countries. This program was discovered by Kaspersky and it was the largest weapon to date uncovered of its type. Flame was designed to carry out espionage by stealing information about systems, stored files, contact data, and audio conversations (Munro, 2012). Flame conducted as series of attacks against Iran's oil industry. Attacking a nation's critical infrastructure and resources are military strategic tactics that have known been successfully conducted via thousands of line of code.

OPEN SOURCE INTELLIGENCE (OSINT) AND OPEN SOURCE SOFTWARE (OSS)

Open Source Intelligence (OSINT), which is one of several sub-intelligence collection disciplines, is intelligence collected from publicly available sources. Publicly available sources can be but are not limited to newspapers, magazines, industry newsletters, online forums, social media, and web queries. OSINT is the opposite of what is known to many as covert intelligence or intelligence gathered through classified means. However OSINT does not mean the information in the publicly available domain does not have a classified value. It only means that we all have access to it but the associated labels of combined information still remains secret or tied to another unknown data classification per the associated agency.

Open Source Software (OSS) can be defined as software that is made available in source code form. This is important as this source code may fall under the General Public License (GPL) which is a widely used free software license that is managed under the GNU Not Linux (GNU) Project (Dawson et al, 2014). There are currently thousands of active projects on sites such as SourceForge that provide access to innovative tools that make OSINT techniques relatively painless. Chinese and Australian researchers have reviewed the many OSS applications available for data mining and published an extensive review discussing findings (Chen, et al, 2007). These researchers note issues such as usability, maintainability, and stability as an issue (Chen et al, 2007). However OSS applications such as the R programming language, also identified as GNU S, has become one of the most powerful tools among statisticians in industry and academia. Table 1 below provides a review of power software applications that can be used in a variation of cyber related activities.

LAWS AND POLICIES TO COMBAT TERRORISM

The events of 9/11 not only changed policies with the U.S. but also policies with other countries in how they treat and combat terrorism. The United Nations (U.N.) altered Article 51 of the U.N. charter. This article allows members of the U.N. to take necessary measures to protect themselves against an armed attack to ensure international peace and security. However this article raises important issues under international law regarding the use of force (Murphy, 2002). The United Kingdom (U.K.) has the Prevention of Terrorism Act 2005 and the Counter-Terrorism Act 2008 which was issued by Parliament. The first act was created to detain individuals who were suspected in acts of terrorism. This act was intended to replace the Anti-terrorism, Crime and Security Act 200 I as it was deemed unlawful. These acts seem to mirror the same ones, created in the U.S., to monitor potential terrorists and terrorists. The U.K. also shared their information with the U.S. for coordinating individual that may be of risk.

Table 1. BI and OSS tools

Software Application	Description and Potential Use
Python Programming Language	Python is a general purpose, high level programming language that allows developers to write programs in fewer lines. Python has a community based development model which includes almost of all its alternative implementations. In the cyber security community this language is used extensively and especially in tasks of exploitation.
Ruby Programming Language	Ruby is a cross platform language that is licensed by Ruby, GPLv2, and BSD license. This language was developed to match behaviors familiar from other languages.
R Programming Language	R is a free software programming language and environment for statistical computing and graphics. R is powerful and feeds multiple statistical Graphical User Interfaces (GUIs). This language uses a command line interface.
R Studio	RStudio is an open source and enterprise software application for the R statistical computing environment. This application is available for Mac, Windows, and multiple Linux distributions regardless of package manager.
RKward	RKward is an open source GUI and Integrated Development Environment (IDE) for the R statistical computing environment. RKward was originally designed for the K Desktop Environment (KDE) but is found operating in multiple environments.
KaliLinux	Described as the rebirth of BackTrack Linux, this is a Debian Linux distribution for digital forensics, penetration testing, and offensive security. This OS contains many preinstalled programs such as port scanners, packet analyzers, password crackers, and tools to escalate privileges.
Tails	Tails, a Debian Linux based distribution, was originally developed as a research project by the U.S. Navy Research Laboratory (NRL) displays the ability to evade detection. This OS is aimed at preserving privacy and anonymity.It can be booted as a liveUSB or LiveDVD leaving no digital footprint.
RapidMiner	RapidMiner is a program that supports all steps for data mining, text mining, and business analytics.

In the U.S., the methods for national security were enhanced to ensure no threats occur on U.S. soil. These changes include enhanced security in all ports of entry. The signing of the Homeland Security Act of 2002 (HS Act) (Public Law 07-296) created an organization that received funding and lots of resources for monitoring the security posture of this country. Additional changes include enhanced monitoring of citizens and residents within the country to prevent terrorist activities by the mention of keywords e.g. bomb, terrorism, explosive, or Al Qaeda. The USA Patriot was signed into law by President George W. Bush in 2001 after September 11, 2001 (Bullock, Haddow, Coppola, & Yeletaysi, 2009). This act was created in response to the event of 9/11 which provided government agencies increased abilities. These increased abilities provided the government rights to search various communications such as email, telephone records, medical records, and more of those who were thoughts of terrorist acts (Bullock, Haddow, Coppola, & Yeletaysi, 2009). This allowed law enforcement to have the upper hand in being proactive to stopping potential acts against U.S. soil. In the 2011 year, President Obama signed an extension on the USA Patriot Act. This act has received criticism from the public due to the potential to be misused or abused by those in power. This act has allowed government agencies to impede on constitutional rights. The Protecting Cyberspace as a National Asset Act of 2010 was an act that also amends Title 11 of the Homeland Security Act of 2002. This act enhanced security and resiliency of the cyber and communication infrastructure within the U.S. This act is important as the President declared that any cyber aggressions would be considered an act of war. This is also important as Estonia's entire digital infrastructure was taken down by hackers who supported the former Soviet rule. This type of attack could be damaging to the infrastructure in the U.S. causing loss of power for days or more which could result in death.

REFERENCES

Benkler, Y. (2011). Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate. *Harvard Civil Rights-Civil Liberties Law Review*, *46*, 311.

Bronk, C., Monk, C., & Villasenor, J. (2012). The Dark Side of Cyber Finance. *Survival*, *54*(2), 129–142. doi:10.1080/00396338.2012.672794

Bullock, J., Haddow, G., Coppola, D., & Yeletaysi, S. (2009). *Introduction to homeland security: Principles of all-hazards response* (3rd ed.). Burlington, MA: Elsevier Inc.

Chen, X., Ye, Y., Williams, G., & Xu, X. (2007). A survey of open source data mining systems. In *Emerging Technologies in Knowledge Discovery and Data Mining* (pp. 3–14). Springer Berlin Heidelberg. doi:10.1007/978-3-540-77018-3_2

Dawson, M., Al Saeed, I., Wright, J., & Onyegbula, F. (2014). Open Source Software to Enhance the STEM Learning Environment. In V. Wang (Ed.), *Handbook of Research on Education and Technology in a Changing Society* (pp. 569–580). Hershey, PA: Information Science Reference; doi:10.4018/978-1-4666-6046-5.ch042

Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the Methods behind Cyber Terrorism. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology* (3rd ed., pp. 1539–1549). Hershey, PA: Information Science Reference; doi:10.4018/978-1-4666-5888-2.ch147

Denning, D. E. (2012). Stuxnet: What has changed? *Future Internet*, *4*(3), 672–687. doi:10.3390/fi4030672

Goldfarb, R., Wasserman, E., Cole, D., Carter, H., Blanton, T., Mills, J., & Siegel, B. (2015). *After Snowden: Privacy, Secrecy, and Security in the Information Age*. Macmillan.

Hankey, S., & Clunaigh, D. Ó. (2013). Rethinking Risk and Security of Human Rights Defenders in the Digital Age. *Journal of Human Rights Practice*, *5*(3), 535–547. doi:10.1093/jhuman/hut023

Harris, S., & Meyers, M. (2002). *CISSP*. McGraw-Hill/Osborne.

Hilse, L. (2013). *Threat-Assessment: Bitcoin: Danger to the United States' National Security and her Economic & Commercial Interests*. Lars Hilse.

Janczewski, L., & Colarik, A. (2007). *Cyber Warfare and Cyber Terrorism*. Hershey, PA: IGI Global; doi:10.4018/978-1-59140-991-5

Luther, W. J., & Olson, J. (2013). *Bitcoin is Memory*. Available at SSRN 2275730.

Munro, K. (2012). Deconstructing Flame: The limitations of traditional defences. *Computer Fraud & Security*, *2012*(10), 8–11. doi:10.1016/S1361-3723(12)70102-1

Murphy, S. D. (2002). Terrorism and the Concept of Armed Attack in Article 51 of the UN Charter. *Harvard International Law Journal*, *43*, 41.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Consulted, 1*(2012), 28.

Nakashima, E. (2013). US Target of Massive Cyber-Espionage Campaign. *Washington Post*.

Perloth, N. (2013). Researchers Find 25 Countries Using Surveillance Software. *New York Times*, Bits blog. 10 December. Retrieved from http://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software

Reid, F., & Harrigan, M. (2013). *An analysis of anonymity in the bitcoin system* (pp. 197–223). Springer New York. doi:10.1007/978-1-4614-4139-7_10

Wright, J., Dawson, M. E. Jr, & Omar, M. (2012). Cyber Security and Mobile Threats: The Need For Antivirus Applications For Smart Phones. *Journal of Information Systems Technology and Planning*, *5*(14), 40–60.

KEY TERMS AND DEFINITIONS

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (Harris, 2002).

Availability: Timely, reliable access to data and information services for authorized users (Harris, 2002).

Bitcoin: Bitcoin is a peer to peer electronic cash system that no one controls and there are not printed currency (Nakamoto, 2008).

Confidentiality: Assurance that information is not disclosed to unauthorized individuals, processes, or devices (Harris, 2002).

Cyber Terrorism: Attacks with the use of the Internet for terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses, worms, Trojans, and zombies (Janczewski & Colarik, 2008).

Integrity: Quality of an IS reflecting the logical correctness and reliability of the OS; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (Harris, 2002).

Non-Repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (Harris, 2002).

Open Source Intelligence: Intelligence collected from publicly available sources.

New Threats and Countermeasures in Digital Crime and Cyber Terrorism

Maurice Dawson
University of Missouri–St. Louis, USA

Marwan Omar
Nawroz University, Iraq

A volume in the Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series

Information Science REFERENCE
An Imprint of IGI Global

Managing Director: Lindsay Johnston
Managing Editor: Austin DeMarco
Director of Intellectual Property & Contracts: Jan Travers
Acquisitions Editor: Kayla Wolfe
Production Editor: Christina Henning
Development Editor: Brandon Carbaugh
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

New threats and countermeasures in digital crime and cyber terrorism / Maurice Dawson and Marwan Omar, editors.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4666-8345-7 (hardcover) -- ISBN 978-1-4666-8346-4 (ebook) 1. Computer crimes--Prevention. 2. Cyberterrorism--Prevention. 3. Computer security. I. Dawson, Maurice, 1982- II. Omar, Marwan, 1982-
HV6773.N4745 2015
005.8--dc23

2015006753

This book is published in the IGI Global book series Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) (ISSN: 2327-0381; eISSN: 2327-0373)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 2
Mobile Devices:
The Case for Cyber Security Hardened Systems

Maurice Dawson
University of Missouri – St. Louis, USA

Jorja Wright
Florida Institute of Technology, USA

Marwan Omar
Nawroz University, Iraq

ABSTRACT

Mobile devices are becoming a method to provide an efficient and convenient way to access, find and share information; however, the availability of this information has caused an increase in cyber attacks. Currently, cyber threats range from Trojans and viruses to botnets and toolkits. Presently, 96% of mobile devices do not have pre-installed security software while approximately 65% of the vulnerabilities are found within the application layer. This lack in security and policy driven systems is an opportunity for malicious cyber attackers to hack into the various popular devices. Traditional security software found in desktop computing platforms, such as firewalls, antivirus, and encryption, is widely used by the general public in mobile devices. Moreover, mobile devices are even more vulnerable than personal desktop computers because more people are using mobile devices to do personal tasks. This review attempts to display the importance of developing a national security policy created for mobile devices in order to protect sensitive and confidential data.

INTRODUCTION

Currently, mobile devices are the preferred device for web browsing, emailing, using social media and making purchases. Due to their size, mobile devices are easily carried in people's pockets, purses or briefcases. Unfortunately, the popularity of mobile devices is a breeding ground for cyber attackers. Operating systems on mobile devices do not contain security software to protect data. For example,

DOI: 10.4018/978-1-4666-8345-7.ch002

traditional security software found in personal computers (PCs), such as firewalls, antivirus, and encryption, is not currently available in mobile devices (Ruggiero, 2011). In addition to this, mobile phone operating systems are not frequently updated like their PC counterparts. Cyber attackers can use this gap in security to their advantage. An example of this gap in security is seen in the 2011 Valentine's Day attack. Cyber-attackers dispersed a mobile picture-sharing application that covertly sent premium-rate text messages from a user's mobile phone (Ruggiero, 2011). Thus, this example illustrates the importance of having a security policy for mobile phones.

Social Networking and Electronic Commerce (E-Commerce) Applications

Many people rely on their mobile devices to do numerous activities, like sending emails, storing contact information, passwords and other sensitive data. In addition to this, mobile devices are the device of choice when it comes to social networking; thus, mobile applications for social networking sites (Facebook, Twitter, Google+) are another loophole for cyber attackers to gain personal data from unsuspecting users (Ruggiero, 2011). Social networking sites are host to a surplus of personal data. That is why malicious applications that use social networking sites to steal data yield severe consequences. Recently, M-Commerce or "mobile e-commerce" has gained popularity in our society. Many smartphone users can now conduct monetary transactions, such as buying goods and applications (apps), redeeming coupons and tickets, banking and processing point-of-sale payments (Ruggiero, 2011). Again, all of these smartphone functions are convenient for the user but advantageous for malicious cyber attackers. Ultimately, there is a niche in technology for cyber security software that is specifically designed for the mobile operating system.

Hypothetical Consequences of Cyber Attacks on Smartphones

The consequences of a cyber attack on a smartphone can be just as detrimental, or even more detrimental than an attack on a PC. According to Patrick Traynor, a researcher and assistant professor at the Georgia Tech School of Computer Science, mobile apps rely on the browser to operate (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). As a result of this, more Web-based attacks on mobile devices will increase throughout the year. Traynor also states that IT professionals, computer scientists and engineers still need to explore the variations between mobile and traditional desktop browsers to fully understand how to prevent cyber attacks (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012).

Challenges with a Mobile Browser

One cyber security challenge for mobile devices is the screen size. For example, web address bars (which appear once the user clicks on the browser app) disappear after a few seconds on a smartphone because of the small screen size (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This is usually the first-line of defense for cyber security. Checking the Uniform Resource Locator (URL) of a website is the first way users can insure that they are at a legitimate website. Moreover, SSL certificates for a website are usually more difficult to find on a mobile phone browser (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This adds another gap in security for mobile devices. Furthermore, the touch-screen

attribute of mobile phones can be cause for concern when dealing with cyber attackers. Traynor states that the way elements are placed on a page and users' actions are all opportunities to implant an attack. An illustration of this is seen when an attacker creates an attractive display content (i.e. an advertisement for an app or a link to a social media app) in which the malicious link is carefully hidden underneath a legitimate image. Unfortunately, once the user clicks the image they can be redirected to the malicious content via the link (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012).

Common Mobile Device OS: iOS and Linux

Apple debuted iOS, or iPhone OS, in 2007, with the inception of the iPhone to the cell phone market (Barrera & Van Oorschot, 2011). Presently, the iOS platform not only runs on iPhone but also iPod Touch and iPad (Barrera & Van Oorschot, 2011). Apple developers specifically write apps to run on all iOS devices. Apple's iOS popularity stems from an easy user interface, including "onscreen interactive menus, 2D and 3D graphics, location services, and core OS functionality such as threads and network sockets" (Barrera & Van Oorschot, 2011).

Apple utilizes various techniques to ensure that the security and quality of their applications are not compromised by malicious cyber attackers. Unlike Android's OS, iOS prevents third-party apps from accessing external data by utilizing a "sandbox mechanism" (Barrera & Van Oorschot, 2011). This mechanism employs policy files that restrict access to certain device features and data (Barrera & Van Oorschot, 2011). App developers use registered Application Programming Interface (APIs) to restrict apps from accessing protected resources (Barrera & Van Oorschot, 2011). Finally, Apple approves every iOS app developers create. The approval process has not been published by Apple, however it is believed that "the company employs both automated and manual verification of submitted apps" (Barrera & Van Oorschot, 2011). Once Apple approves a potential app, Apple "digitally signs it and releases it" to the App Store (Barrera & Van Oorschot, 2011). Ultimately, Apple has the final say pertaining to which apps are available for download in the App Store – "apps that Apple hasn't digitally signed can't run on the device" (Barrera & Van Oorschot, 2011).

Linux is a Unix like Operating System (OS) that is built on the Linux kernel developed by Linus Torvalds with thousands of software engineers. As of 2012 there are over two hundred active Linux distributions. The majority of the kernel and associated packages are free and OSS. This type of software provides a license which allows users the right to use, copy, study, change, and improve the software as the source code is made available. Providing source code allows developers or engineers to understand the inner workings of development. Imagine being able to study Mac or Windows by viewing all the source code to replicate similar developments. This exercise is great for a developer to learn low level coding techniques, design, integration, and implementation. This is also a great method for penetration testing with the ability to test all available back doors within the software.

In terms of associated cost the majority of Linux distributions are free. However some distributions require a cost for updates or assistance that related to specific needs such as OS modifications for server hosting. In software, there is a packet management system that automates the process of installing, configuring, upgrading, and removing software packages from an OS. In the Linux OS builds the most common packet management systems are Debian, Red Hat Package Manager (RPM), Knoppix, and netpkg. The most popular Linux distributions for mobile use are Android IOS and Ubuntu.

Malware Attacks on Smartphone OS

Along with this, malware that targets smartphone operating systems is constantly evolving. An example of this is seen with "Zeus-in-the-Mobile" (ZitMo), a specific form of malware common to the Android operating system. ZitMo targeted Android users' bank apps; it attempted to bypass the banking two-factor authentication, steal credentials and gain access to users' bank accounts, and ultimately money (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This is just one form of cyber attacks that IT professionals are trying to prevent from occurring.

Lastly, it is believed that mobile devices will be the new vector for targeting network and critical systems (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). According to the report, mobile devices are an excellent way to spread malware because phones are great storage devices. A hypothetical example of a wsoncyber attack against a company's network is seen when malware is implanted in a smartphone. For example, a clever cyber attacker can write code to remotely control wireless connectivity technology and plant malware on the mobile phone. If that same phone is connected to a corporate network, i.e. the user is charging the phone on the company's computer; the malware can now attack the company's network. IT professionals want to prevent attacks like that from occurring because the economic consequences of such an event would be catastrophic. Ultimately, it is imperative that a national security standard is created for mobile devices in order to protect personal data.

The Android Platform

According to Shabtai et al. (2010), Android is an open-source application execution environment that includes an operating system, application framework, and core applications. Android was designed and released originally by Android Inc. to provide a user-friendly, open, and easy-to-use mobile-based development environment. This open-source mobile development framework is user-centric because it provides a variety of developments, tools, and features. However, this open-development feature also poses challenges to securing sensitive user data and protecting users from malicious attacks, such as phishing applications that are usually sent to users to trick them into providing their financial information and credentials while accessing malicious websites that look the same as the legitimate banking sites.

The Android operating system was first released in October, 2008 by T-Mobile 1G, and soon major telecommunications companies (such as T-Mobile) in both the U.S. and Europe adopted it because of its rich capabilities exemplified by core applications (i.e., email, web browsing, and MMS), entertainment features, and services, such as camera and Bluetooth. This has also led to Android's popularity amongst developers due to the open-source nature of Android, which offers the capability of developing and programming rich applications at the lowest level of Android's operating system. Since its initial release in 2008, Android has undergone many releases, the last being Android 2.2; this latest version of the Android platform brings many new and existing features and technologies to make both users and developers productive. Some of the new services and applications included in the new version aim at increasing speed (CPU is about 2-5 times faster), performance, and browsing (using version 8 engine that provides 2-3 times faster java script heavy page load). This new version also offers improved security features by allowing users to unlock their device using a password policy and the ability to wipe data from devices in case of theft or loss.

The Android Security Model

Android is a multi-process system where each application (and parts of the system) runs its own process. The standard Linux facilities enforce security between applications and the system at the process level; those applications are assigned by users and group IDs. Applications are restricted in what they can perform by a permission mechanism, called permission labels, that uses an access control to control what applications can be performed. This permission mechanism is fine-grained in that it even controls what operations a particular process can perform (Shabtai et al., 2010). The permission labels are part of a security policy that is used to restrict access to each component within an application. Android uses security policies to determine whether to grant or deny permissions to applications installed on Android OS.

Those security policies suffer from shortcomings in that they cannot specify to which application rights or permissions are given because they rely on users and the operating system to make that guess. They are therefore taking the risk of permitting applications with malicious intentions to access confidential data on the phone. Ongtang, McLaughlin, Enck, and McDaniel (2009) best described this security shortcoming by their hypothetical example of "PayPal service built on Android. Applications such as browsers, email clients, software marketplaces, music players, etc. use the PayPal service to purchase goods. The PayPal service in this case is an application that asserts permissions that must be granted to the other applications that use its interfaces" (Ontang, McLaughlin, Enck, & McDaniel, 2009). In this hypothetical scenario, it is unknown whether the PayPal application is legitimate or not because there is no way to determine whether this is the actual PayPal service application or another malicious program. Again, Android lacks security measures to determine and enforce how, when, where, and to whom permissions are granted.

Android's Permissions

Android uses permission mechanisms to determine what users are allowed to do in applications; this is achieved via the manifest permission that grants permissions to applications independently, which in turn, allows applications to run independently from each other as well as from the operating system. This could be a good security feature since the operations run by one application cannot interfere or otherwise impact operations within other applications. For example, users sending email messages will not be allowed (by default) to perform any operation within an application (such as reading a file from another application) that could adversely impact the email application (Developers, n.d). Applications achieve that using the "sandbox" concept, where each application is given the basic functions needed to run its own process; however, if the sandbox does not provide the needed functions to run a process, then the application can interfere with the operations of another process and request the needed functions to run a process. This capability of allowing applications to request permissions outside of their sandbox capabilities could be harmful to Android mobile devices because it opens a window of opportunity for malware to exploit the privilege of accessing sensitive data on Android handsets and thus install malicious software (Vennon, 2010).

METHODOLOGY

This is a conceptual paper; thus the main scope of this paper is to illustrate the importance of security software for smartphone operating systems. Case studies in scholarly journals and reports were used in the construction of this paper. Most sources contain qualitative information, describing predictions of various cyber attacks on mobile devices that may occur by the end of 2012. Quantitative methods were also used to assess the statistical increase in cyber attacks.

RESEARCH RESULTS

The current smartphone statistics are quite daunting due to the widespread lack of security software for mobile devices. The result of this void in security software is vulnerable mobile devices and tablets that are easily susceptible to cyber attacks. According to Andy Favell, editor of the website "MobiThinking," in 2010, 96% of mobile devices and tablets do not contain security software (Favell, 2011). Moreover, the article states that over 2000 various types of mobile malware have been identified in the past two years (Favell, 2011). For example, Hydraq and Stuxnet, specific cyber attacks, "leveraged zero-day vulnerabilities to break into computer systems... Stuxnet alone exploited four different zero-day vulnerabilities to attack its targets" (Symantec, Inc., 2011). Moreover, many enterprises experienced a multitude of targeted attacks against their collection of corporate data in 2010 (Symantec, Inc., 2011).

Figure 1 depicts the current status of security for the majority of today's mobile devices. This is an alarming statistic because, as mentioned earlier, mobile devices are the most popular way to communicate in our society. Malware is increasing at an exponential rate, and consumers' nonchalant attitudes towards mobile security provide the perfect opportunity for cyber attackers to create and spread malware quickly. This breach in cyber security puts businesses at risk also. According to Favell, when consumers use smart devices for work purposes, the devices can access and/or store company emails and sensitive information (2011). This scenario is detrimental to the success and welfare of any company; hopefully, the fact that in 2010 only 4% of all mobile devices contained security software will alert consumers and businesses of the importance of having a secured smart device (Favell, 2011).

Figure 1. The current status of security for the majority of today's mobile devices

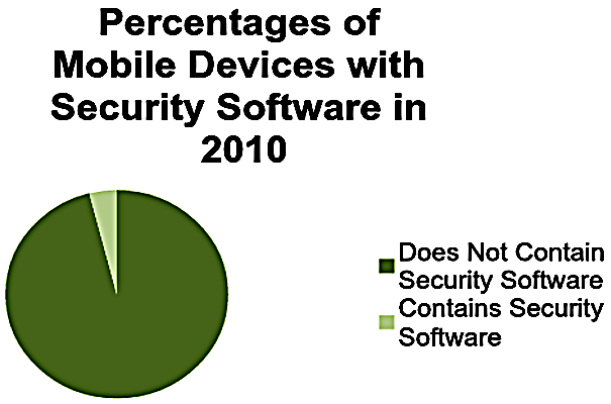


Table 1. Malware programs commonly used to hack into smartphones

Type	Definition	Examples
Trojan	Programs that pose as legitimate applications (Symantec, Inc., 2011).	Android.Pjapps Trojan, Rogue apps, Hydraq
Virus	Software program that can replicate itself and damage files and other programs on host computer.	Stuxnet
Botnet	A network of infected private computers controlled by cyber attackers who sell sensitive data to the highest bidder. Social media applications on mobile devices are now a new avenue for botnets to control devices (Trend Micro, 2009).	Opt-in botnets, Aurora botnet, Rustock
Toolkit	Software programs that can be used to assist with the launch of widespread attacks on networked computers or mobile devices; exploits Java vulnerabilities (Symantec, Inc., 2011).	Phoenix toolkit
Malvertising	Authentic looking advertisements that are linked to false sites (Rao, 2011).	Malicious Ad on social network apps, such as TweetMeme
Worms	Malware programs that self-replicate and is spread over the air (via mobile networks) (Favell, 2011).	iPhoneOS.Ikee.B; iPhoneOS.Ikee

Table 1 illustrates the various malware programs that now infect mobile devices. Originally, trojans, viruses, botnets and toolkits were common infections of personal computers; now, mobile devices are plagued with these various malware programs. In 2010, Favell stated that 2,500 different mobile malware programs exist (Favell, 2011). The majority of existing malware programs target Android apps because Android is the most popular OS, and it is easier for app developers to distribute apps through GooglePlay (Android's App Market) due to Android's lenient verification process (Favell, 2011). In 2009, iPhoneOS.Ikee.B and iPhoneOS.Ikee infected "jailbroken" Apple devices. "Jailbreaking" means to remove Apple's restrictions; this grants the user freedom to use the phone as he/she pleases (Favell, 2011). Now, consumers must be aware of the various malware programs that are prevalent; consumers must also be vigilant to protect their data while using their device.

Figure 2. Illustrates various cyberthreats in 2010
(Symantec, 2011).

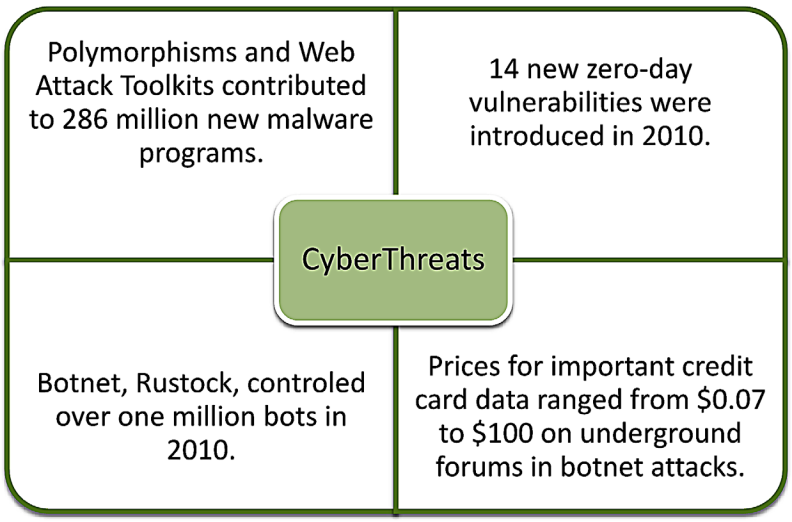
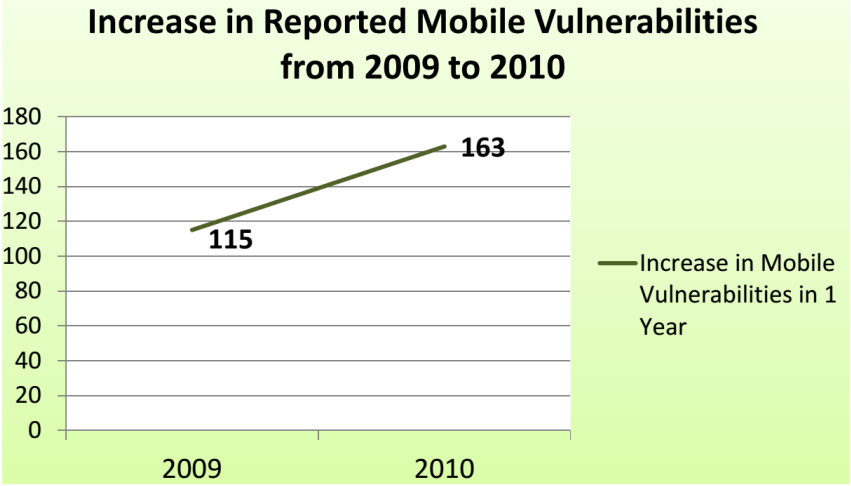


Figure 3. 42% increase in mobile vulnerabilities
(Symantec, 2011)

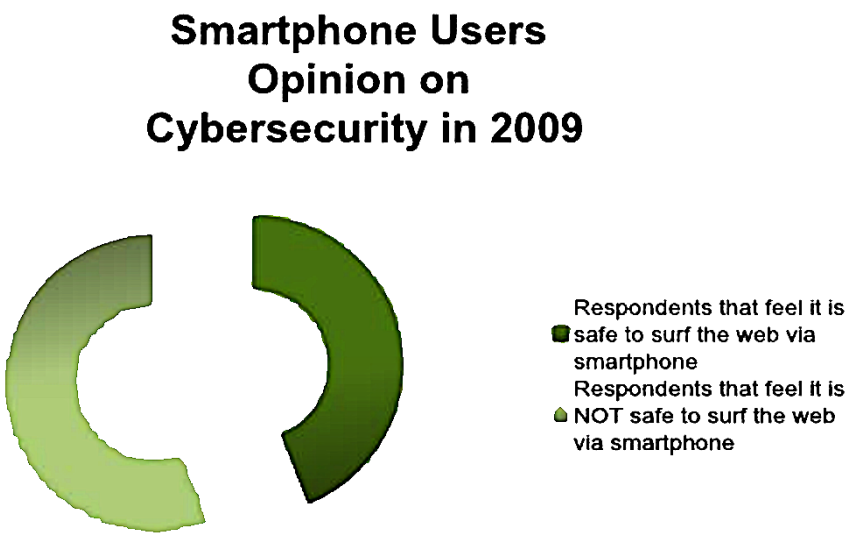


Cyber threats are increasing at an alarming rate. According to Symantec, polymorphisms and toolkits have contributed to the increase in malware programs in 2010. Also, over 200 million malicious programs were created during 2010 (Symantec, Inc., 2011). Moreover, cyber criminals are exploiting the gaps in security with the Android OS. In fact, many zero-day exploits have increased since the inception of the Android Market. Unfortunately, with zero-day vulnerabilities, the attack happens the same day; hence, IT specialists cannot distribute software updates in a timely manner to block such attacks (Symantec, Inc., 2011). Other harmful malware programs, botnets, have wreak havoc on many smartphone OS. The botnet, Rustock, controlled over a million bots at one point in 2010; Grum and Cutwail, other botnet attacks, controlled hundreds of thousands bots (Symantec, Inc., 2011). Lastly, cyber threats that steal bank and credit card information has greatly increased in the past four years. Symantec's Internet Security Threat Report states that black market forums pay top dollars for personal credit card data. The majority of this information is stolen through extensive botnet attacks (2011).

Above is a numerical depiction of the increase in mobile cyber attacks in one year. From 2009 to 2010 there was a 42% increase in the number of mobile vulnerabilities (Symantec, Inc., 2011). Cyber criminals are capitalizing on the popularity of mobile devices; thus, this trend is an indication that will not falter without an intervention. Furthermore, most reported mobile vulnerabilities occurred in the form of Trojan Horse programs that acted as legitimate applications (Symantec, Inc., 2011). While many cyber attackers created some of the most pertinent malware from scratch, "in many cases, they [cyber attackers] infected users by inserting malicious logic into existing legitimate applications" (Symantec, Inc., 2011). Next, the hacker will distribute these malicious apps through public app stores, such as Google Play or Apple's App Store. Pjapps Trojan is a recent example of a malicious app distributed through public app stores (Symantec, Inc., 2011).

Trend Micro, an international leader in data security, surveyed 1,000 smartphone and iPhone owners that were over the age of 18. The data revealed that nearly half (56 percent) of the respondents believe it is safe, if not safer, to browse the Internet from their mobile device as opposed to a PC (Trend Micro, 2009). Contrasting with this, 44 percent of respondents do not feel it is safe to surf the web using a

Figure 4. Percentage of smartphone users that perceive it is safer to surf the Internet via mobile browser (Smartphone Users, 2009).

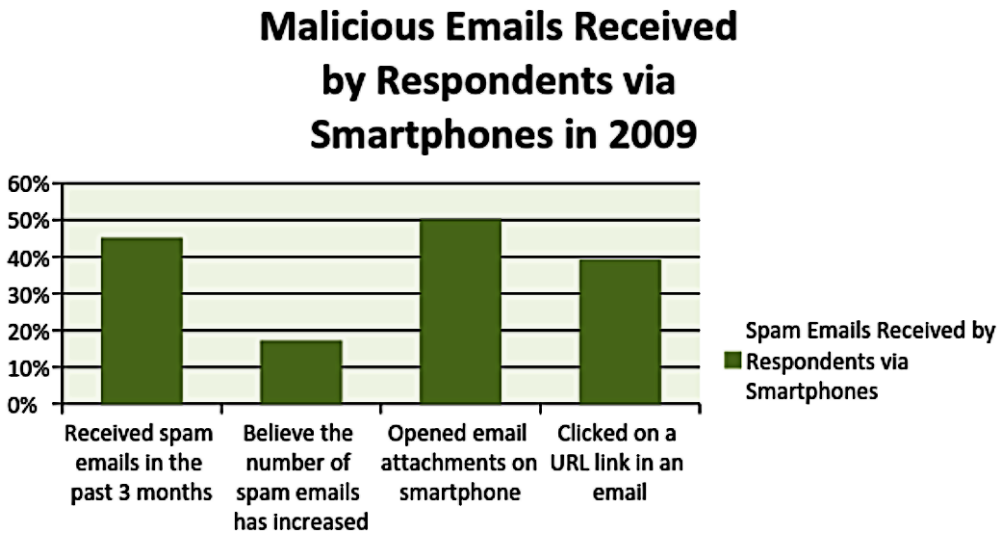


smartphone (Trend Micro, 2009). Moreover, according to the survey, only 23% of the respondents use security software that is installed on their smartphone (Trend Micro, 2009). In addition to this, another 20% of respondents "don't think installing security software program[s] on their phones would be very effective (Trend Micro, 2009)." The same respondents feel that there is limited risk when using a mobile web browser. As stated earlier, this false mentality of a safe mobile browser environment has created many opportunities for cyber criminals to steal personal data. Contrasting with this, the majority of the survey respondents are aware of mobile Web threats, and nearly half of them have been infected by some form of malware (Trend Micro, 2009).

spam emails are another prevalent form of cyber threats. As illustrated in Figure 5, out of the 1,000 respondents, 450 (45%) of them received spam emails in the past 3 months (Trend Micro, 2009). 170 (17%) respondents believe there is an increase in the amount of spam emails they have received (Trend Micro, 2009). 500 (50%) of respondents open email attachments on their smartphone; and 390 (39%) respondents click on URL links in emails they received on their phone (Trend Micro, 2009). These statistics can be projected onto the general smartphone user community. In fact, it can be assumed that nearly half of all smartphone users receive spam emails quite often throughout the year, and half of all smartphone users carelessly open email attachments on their phone. Since spam has become a common nuisance in the email environment; it is obvious it would be a nuisance for mobile devices.

Thus, the lack of installed security software coupled with the laissez-faire attitude of today's smartphone users, leads to advantageous loopholes for malicious cyber attackers. 20% of smartphone users do not think installing security software to their phone will reduce their chances of malware attacks (Trend Micro, 2009). Another 20% of users have encountered phishing scams when surfing the internet on their mobile browser (Trend Micro, 2009). Phishing scams lure users into supplying ID information, bank account numbers, usernames and passwords by replying to false email messages (Trend Micro, 2009). Lastly, Apple aficionados must take necessary precautions when using the Safari web browser on their iPhone. Apple's claim to fame is their stylish hardware, iOS Operating System (OS) and sleek

Figure 5. Percentage of smartphone survey respondents that received spam in 2009 (Smartphone Users, 2009).



functionality. Unfortunately, the traits that make Apple popular are also the same traits that make the iPhone susceptible to cyber attacks (Trend Micro, 2009). A recent example of this is seen in a reported SMS vulnerability for the iPhone, in which hackers have the ability to control the device if the user is on a malicious site or connecting to the internet through unsecured 3G or Wifi connections (Trend Micro, 2009).

ANALYSIS AND DISCUSSION

Various security services project that cyber attacks on mobile devices will increase exponentially by 2015. This is obvious based on the fact that the majority of mobile devices have no security software at all. Lookout Mobile Security company analyzed the current data on smartphone cyber attacks and released their malware predictions for 2011 (Rao, 2011). Lookout offers various security services for many smartphone operating systems, such as Android, Windows Mobile, Blackberry and iOS (Rao, 2011). Unfortunately, Android users, internationally, had a 36% chance of clicking an unsafe link in 2011 (Rao, 2011).

Lookout also identified the first U.S. mobile malware that steals money from Android smartphone users – GGTracker; and RuFraud, which steals money from Eastern European Android smartphone users (Rao, 2011). Lookout believes that malware creators will furtively combine thousands of mobile devices into extensive botnet-like networks, such as DroidDream, to spread spam, steal personal data and install more malware (Rao, 2011). Moreover, Lookout has predicted the likelihood that smartphone users will click on unsafe links (Rao, 2011). They predict the increase in "malvertising" – malware advertising, advertisements that link back to counterfeit websites – will continue to increase by the end of this year.

Predictions of the Mobile Security Market

Consistent with this, Canalys, an IT research company that specializes in "mobility services, data centers, networking, security, unified communications, client PC markets and go-to strategies," did more research on mobile security. From a business perspective, they predict that mobile security investment will increase by 44% each year to 2015 (Canalys, 2011). They expect the mobile security market to become a $3 billion investment opportunity in 2015. Fortunately, by 2015, Canalys believes that 20% of smart phones and tablets will have mobile security software installed (Canalys, 2011). Canalys also states that device management will drive the incorporation of security-related products (secured-approved mobile devices) in the business sector (Canalys, 2011). For example, it is projected that corporate device management will increase implementation of security-related products. Businesses will use solutions "to track, monitor and authorize corporate data access, as consumers bring their devices into the workplace" (Canalys, 2011). Canalys recommends that it is advantageous for businesses to link the solutions to "enterprise app stores" so that only "approved apps" can be downloaded and mobile devices with corporate-approved apps installed will have the ability to access corporate data (Canalys, 2011). Lastly, Canalys experts predict mobile client security to increase by 54.6% every year until 2015 (Canalys, 2011). Mobile client security includes: anti-virus, firewall, messaging security (due to SMS texting capabilities), web threat security, VPN functionality and encryption (Canalys, 2011).

Presently, the U.S. and Canada are the leaders of mobile security implementation due to their need to adhere with data compliance policies (Canalys, 2011). Nevertheless, the Western European market is expected to grow as globalization, "enterprise mobility and consumerization trends" increase (Canalys, 2011). From 2013 to 2015, mobile security investment will sharply increase in developing countries such as Latin America, Asia, Africa and the Middle East, due to the instant popularity of the price-sensitive operating system, Android (Canalys, 2011). Unfortunately, as the steady growth of Android OS increases so does the volume of mobile malware threats because more consumers can download compromised applications (Canalys, 2011).

Corporations, Cyber Security, and Mobile Devices

Currently, corporations around the world are trying to manage a growing mobile workforce, in which employees are using multiple devices and operating systems (Canalys, 2011). This increase in data consumption exponentially increases the amount of vectors open to cyber attacks and leaves corporate data more vulnerable due to tangible loss of devices (Canalys, 2011). Ultimately, to counteract the era of cyber crimes, enterprises must have a holistic approach to mobile security – every layer of security must be analyzed in order to protect sensitive data. Lastly, Canalys urges service providers to provide security from a "network perspective, regardless of device or operating system type" (Canalys, 2011). Protecting the network of service providers is a key element in providing top notch security for the plethora of mobile devices that are currently on the market.

LIMITATIONS

It is a daunting task to establish a national cyber security standard to counteract the multitude of cyber attacks that exist today. There are quite a few limitations that must be addressed in order to move forward.

Legitimate Applications that Can Be Used to Retrieve Information

Presently, there is valid spy software available for various mobile devices. An example of this is FlexiSpy, a legitimate commercial spyware program that cost over $300 (United States Computer Emergency Readiness Team, 2010). FlexiSpy can:

- Listen to actual phone calls as they happen;
- Secretly read Short Message Service (SMS) texts, call logs, and emails;
- Listen to the phone surroundings (use as remote bugging device);
- View phone GPS location;
- Forward all email events to another inbox;
- Remotely control all phone functions via SMS;
- Accept or reject communication based on predetermined lists; and
- Evade detection during operation (United States Computer Emergency Readiness Team, 2010).

The creators of FlexiSpy claim that this application can help protect young children (that have a cell phone) or catch unfaithful spouses. However, the dangers of this software outweigh the positives once it is in the hands of a malicious cyber attacker. This example demonstrates the need for a federal implemented cyber security act to dictate the types of applications that can be available to the general public. For parents, FlexiSpy has wonderful attributes in terms of monitoring the whereabouts of underage children, but these same attributes can be abused by a cyber attacker to gain extremely personal data of a smartphone user.

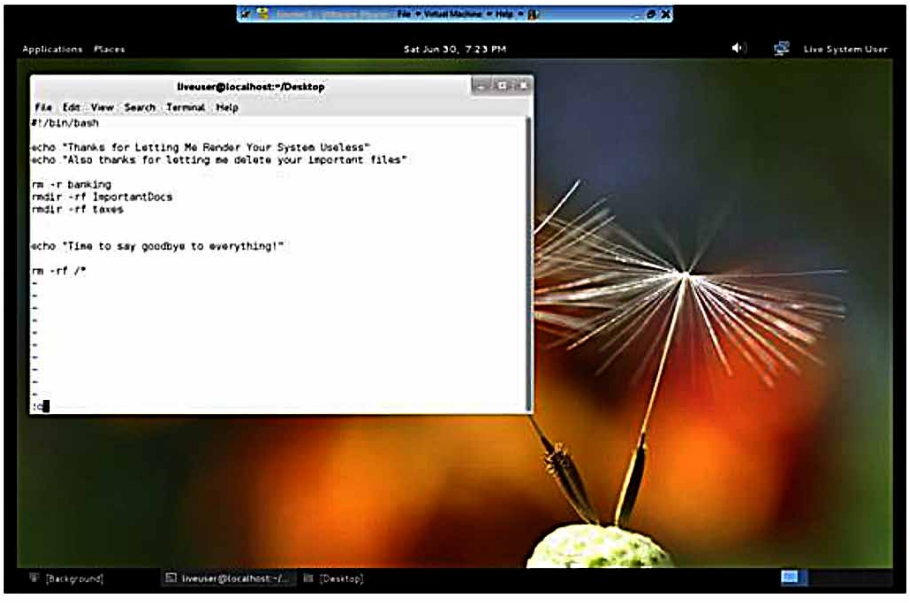
Another example of a legitimate application that can be exploited by malicious cyber hackers is mobile e-commerce apps (M-commerce). M-commerce involves using a mobile device "to research product information, compare prices, make purchases, and communicate with customer support" (United States Computer Emergency Readiness Team, 2010). In addition to this, merchants can use mobile devices for checking prices, inquiring inventory and processing payments (United States Computer Emergency Readiness Team, 2010). Currently, vendors now have the ability to process credit card payments with a new device called "Square" (United States Computer Emergency Readiness Team, 2010). Square is a third-party smartphone attachment that is plugged into a smartphone's headphone jack and is used for swiping credit cards (United States Computer Emergency Readiness Team, 2010). Square subscribers register their device online through the company's website. This way, subscribers can manage their payment processes through their accounts. Unfortunately, Square can be used for malicious cyber activities, such as "skimming" and "carding" (United States Computer Emergency Readiness Team, 2010). According to the article entitled, "Cyber Threats to Mobile Devices," "Skimming is the theft of credit card information using card readers, or skimmers, to record and store victims' data" (2010). Also, carding is a process used to assess "the validity of stolen credit card numbers" (United States Computer Emergency Readiness Team, 2010). Both processes can be done in conjunction with other legitimate transactions, and can be exploited by cyber attackers to gain sensitive financial data.

A third example of a legitimate application that can be used for malicious activity are advertisement libraries, or ad libraries (Grace, Zhou, Jiang, & Sadeghi, 2012). Many app developers incorporate ad libraries into their legitimate applications for monetary compensation. For example, on the Android Market (now known as Google Play), over 60% of the apps are free to download (Grace, Zhou, Jiang, & Sadeghi, 2012). In order for app developers to be compensated for their product, they use ad libraries,

which "communicate[s] with the ad network's servers to request ads for display and might additionally send analytics information about the users of the app" (Grace, Zhou, Jiang, & Sadeghi, 2012). Next, the ad network pays the app developer continuously, based on data that measure "how much exposure each individual app gives to the network and its advertisers" (Grace, Zhou, Jiang, & Sadeghi, 2012). Unfortunately, the Computer Science Department of North Carolina State University revealed that there are many privacy and security issues in some of the most prevalent ad libraries. Granted some of these ad libraries collect information for legitimate purposes, such as a user's location for targeted advertising, a few ad libraries collect personal, sensitive data, such as a user's call logs, account information or cell number (Grace, Zhou, Jiang, & Sadeghi, 2012). Consequently, malicious cyber attackers can use this information to infer the actual identity of the user, and enable greater comprehensive tracking of the user's habits (Grace, Zhou, Jiang, & Sadeghi, 2012). A specific example of an ad library embedded into a popular smartphone app is the game *Angry Birds*, created by Rovio. The company Rovio employed the services from a third-party advertising network to capitalize Angry Birds on the Android Market (Grace, Zhou, Jiang, & Sadeghi, 2012). AdMob is the most popular ad library used by Angry Birds; it sends user's information such as game scores to Google (Grace, Zhou, Jiang, & Sadeghi, 2012). This business arrangement is not uncommon for smartphone app developers. Unfortunately, ad libraries in legitimate applications can be loopholes for cyber attackers to exploit and abuse personal user information. One study discovered that some ad libraries "download additional code at runtime from remote servers and execute it in the context of running the app" (Grace, Zhou, Jiang, & Sadeghi, 2012). It is evident that these results garner the need for additional methods for regulating the behavior of ad libraries on Android apps.

When discussing legitimate applications we should also not forget how easy it is to create malware applications. With the aid of rootkit tools, and freely available malicious code it is easy to create a malware program. Figure 6 displays a simple script that can email as an executable file that will delete targeted files that are necessary for the OS to function. This script took less than four minutes to create.

Figure 6. Example of an executable file



Malware Social Network Exploitation

As stated earlier, the popularity of social networking applications can be a limitation in the fight against cyber threats. The wealth of personal data that social media applications inspire cybercriminals to create malware targeted for these applications. Twitter and Facebook are the main sources of communication and information for today's generation of smartphone users. Unfortunately, accepting shared information on these websites can compromise the security of a user's device. This issue is heightened on Twitter because users are limited to 140 characters when sharing updates or links. So on Twitter, Uniform Resource Locators, or URLs, are shortened severely in order to adhere to the 140 character rule. This is unfortunate because shortened URLs make it more difficult for a user to know if the link is legitimate or malicious. In brief, sharing links via Twitter is an opportunistic way for cyber attackers to lure innocent users into clicking fraudulent links.

Android Malware

Hackers first started to design malware for mobile devices in early 2004 when the Cabir worm came to the scene. Despite the fact that Cabir was only a "proof of concept" attack form and did not cause any serious damage to affected mobile devices, it brought hackers' attention to mobile devices. Android, as a smartphone, is no exception when it comes to mobile malware attacks. Some of the first Android malware was devised by a group of security researchers as an attempt to bring attention to possible malware attacks on the Android platform because Android offers an integrated set of services and functionalities, such as internet access. The researchers were able to create the first Android running malware by exploiting undocumented Android Java functions and using them to create native Linux applications. Specifically, this malware was embodied in a valid, benign, Android application that a user would install. Once the benign application is installed, the malware would propagate the Linux system and execute its malicious payload, thereby wreaking havoc on Android devices. This was an indication of the possible vulnerabilities and risks associated with Android devices (Schmidt, Bye, Clausen et al., 2009).

The most dangerous Android malware is the one that exploits security flaws within the operating system (Linux) to gain root-level access with root privilege. One of the first security flaws was discovered in Android in November of 2008 when security experts found a bug that would allow users and potential attackers to run command-line instructions with root privilege; moreover, the bug, if exploited, would make the Android platform read and interpret actions based on the input text. For example, if an Android user input a simple text message, such as "Hello," it could be interpreted by the operating system as "reboot," which surprisingly reboots the Android device (ZDNet, 2010). This security shortcoming and many other vulnerabilities were discovered in Android over the last two years and have thus continuously raised pressing concerns about the credibility and effectiveness of security controls deployed in Android. Most of those vulnerabilities stem from Android's open-source nature, which allows development of third-party applications without any kind of centralized control or any security oversight.

As a case in point, we can highlight malware risks targeting Android smartphone users. Android smartphone users tend to download and install apps frequently, as all kinds of apps dominate the marketplace; apps usually require access to certain areas of the phone to function, and they ask users to grant permissions at installation time. Many apps tend to request permissions more than they really need to be fully functional. Also, many apps are seemingly benign to users and do not seem to pose any threats to confidential information. Therefore, Android users normally get distracted by enjoying all the features and added functionality offered by apps and do not give adequate attention to the security aspects of those

apps. To make matters worse, hackers target popular apps, modify their source code, and then upload them again to the Android Market after injecting their malicious piece. Unfortunately, Google is not proactive in this area in that it does not remove potentially malicious apps until they receive complaints or until apps have already caused disruption and compromised sensitive data. Therefore, the researcher strongly believes that the greatest security risk lies at the heart of Android apps, where attackers are most capable of passing their malicious apps to end users through the Market and gain unauthorized access to confidential data to achieve financial gains. Furthermore, hackers are known to use attack strategies that tend to send expensive SMS messages and dial prime rate numbers as a quick and efficient way to gain money illegally.

Incorporating Pre-Existing Government Guidance

The Department of Defense (DoD) has addressed software security through governance issued under the Office of Management and Budget (OMB) Circular A-130. The focus of Information Technology security was further derived by DoD Directive 8500.2. It specifically states that all Information Assurance (IA) and IA-enabled IT products incorporated into DoD Information Systems (IS) shall be configured in accordance with DoD-approved security configuration guidelines. On April 26, 2010, the DoD released the third version of the Application Security and Development Security Technical Implementation Guide (STIG) provided by the Defense Information Systems Agency (DISA). This document provides DoD guidelines and requirements for integrating security throughout the software development lifecycle. The STIGs are accompanied by the NSA Guides which provide the configuration guidance for locking down a system. There are guides for multiple Oss to include those for mobile platforms.

In terms of development for mobile devices the commercial sector should employ those who have professional certifications such as International Information Systems Security Certification Consortium (ISC)2 Certified Secure Software Lifecycle Professional (CSSLP). The guidance that drives this requirement and those similar is the DOD 5870.01M Information Assurance Workforce Improvement Program. Organizations employing IA technically competent software developers should help mitigate the overall risk. This could be a requirement that could be levied not just upon the mobile phone developer but also the application developer.

The Common Criteria (CC), an internationally approved set of security standards, provides a clear and reliable evaluation of the security capabilities of Information Technology (IT) products (CCEVS, 2008). By providing an independent assessment of a product's ability to meet security standards, the CC gives customers more confidence in the security of products and leads to more informed decisions (CCEVS, 2008). Security-conscious customers, such as the U.S. Federal Government, are increasingly requiring CC certification as a determining factor in purchasing decisions (CCEVS, 2008). Since the requirements for certification are clearly established, vendors can target very specific security needs while providing broad product offerings. The international scope of the CC, currently adopted by fourteen nations, allows users from other countries to purchase IT products with the same level of confidence, since certification is recognized across all complying nations. Evaluating a product with respect to security requires identification of the customer's security needs and an assessment of the capabilities of the product. The CC aids customers in both of these processes through two key components: protection profiles and evaluation assurance levels (CCEVS, 2008). Utilizing guidance such as the CC could allow organizations to appropriately measure the security of their product. The problem is the cost that surrounds commercial companies meeting rigorous standards but this product certification process could replicated at a more cost efficient manner.

Lastly, another limitation for creating a cyber security environment for mobile devices is due in part to a lack of national cyber security policies. The internet is a brand new frontier with no physical or political boundries (Brechbuhl, Bruce, Dynes, & Johnson, 2010). Furthermore, cyber security is a concern of everybody – common smartphone users, business and government officials; also, security issues have normally been the government's responsibility. Contrasting with this, the sectors that are best equipped at dealing with cyber security issues is private or semiprivate enterprises that operate the information and communication technology (ICT) infrastructure, in other words the internet (Brechbuhl, Bruce, Dynes, & Johnson, 2010). Finally, the creation of a national policy is difficult because we currently "lack a feasible policy framework that systematically arrays the issues and specifies parameters that constrain this development" (Harknett & Stever, 2011). Ultimately, cyber security threats are versatile and constantly changing, we must develop programs to match and counteract the transient attributes of cyber security attacks.

Issues with Android Phones and Other Mobile Devices

Smartphones are becoming a more integrated and prevalent part of people's daily lives due to their highly powerful computational capabilities, such as email applications, online banking, online shopping, and bill paying. With this fast adoption of smartphones, imminent security threats arise while communicating sensitive personally identifiable information (PII), such as bank account numbers and credit card numbers used when handling and performing those advanced tasks (Wong, 2005; Brown, 2009). Traditional attacks (worms, viruses, and Trojan horses) caused privacy violations and disruptions of critical software applications (e.g., deleting lists of contact numbers and personal data). Malware attacks on smartphones were generally "proof of concept" attempts to break through the phone's system and cause damage (Omar & Dawson, 2013). However, the new generation of smartphone malware attacks has increased in sophistication and is designed to cause severe financial losses (caused by identity theft) and disruption of critical software applications (Bose, 2008). Because smartphones are becoming more diverse in providing general purpose services (i.e., instant messaging and music), the effect of malware could be extended to include draining batteries, incurring additional charges, and bringing down network capabilities and services (Xie, Zhang, Chaugule, Jaeger, & Zhu, 2009).

Smartphones are rapidly becoming enriched with confidential and sensitive personal information, such as bank account information and credit card numbers, because of the functionality and powerful computational capabilities built into those mobile devices. Cyber criminals, in turn, launch attacks especially designed to target smartphones, exploiting vulnerabilities and deficiencies in current defense strategies built into smartphones' operating systems. Bhattacharya (2008) indicated that because of skill and resource constraints, businesses are ill-prepared to combat emerging cyber threats; this claim is true for smartphones as well, given the fact that those mobile devices are even less equipped with necessary protections, such as antivirus and malware protection software. Some services and features, such as Bluetooth and SMS, create attack vectors unique to smartphones and thus expand the attack surface. For example, in December, 2004, A Trojan horse was disguised in a video game and was intended to be a "proof of concept," which signaled the risks associated with smartphones that could potentially compromise the integrity and confidentiality of personal information contained in smartphones (Rash, 2004). Attackers can easily take advantage of those services provided by smartphones and subvert their primary purpose because they can use Bluetooth and SMS services to launch attacks by installing software that can disable virus protection and spread via Bluetooth unbeknownst to smartphone users.

With the development of innovative features and services for smartphones, security measures deployed are currently not commensurate because those services and features, such as MMS and Bluetooth, are driven by market and user demands, meaning that companies are more inclined to provide more entertainment features than security solutions. In turn, this further increases vulnerabilities and opens doors for hackers to deploy attacks on smartphones. Furthermore, Mulliner & Miller (2009) argue that the operating systems of smartphones allow the installation of third-party software applications, coupled with the increase in processing power as well as the storage capacity. Scenarios like this pose worse security challenges because hackers could exploit those vulnerabilities, which are further compounded by users' lack of security awareness. Smartphone attackers are becoming more adept in designing and launching attacks by applying attack techniques already implemented on desktop and laptop computers; smartphones' enhanced features, such as music players and video games, produce easy-to exploit targets by sending seemingly benign files via music or video game applications to users and luring them into downloading such files. Becher, Freiling, and Leider (2007) indicated that attackers could exploit such vulnerabilities to spread worms autonomously into smartphones. Therefore, hackers usually use a combination of technical expertise along with some social engineering techniques to trap users into accepting and downloading benign applications, which are used later to execute malicious code and affect critical applications running on smartphones.

Attack Vectors and Infection Mechanisms

- **Bluetooth:** This is a wireless communication protocol used for short-range (about 10 meters) transmissions at 2.4 G.H. Bluetooth is one of the most widely used and preferred attack techniques for infecting smartphones because by pairing Bluetooth-enabled devices, hackers are able to access infected phones' critical applications and files, such as email, contact lists, pictures, and any other private data stored in the smartphone. Bluetooth-enabled smartphones are prone to various kinds of attacks due to security implementation flaws that exist in current security specifications. For example, Wong (2005) reveals that when two Bluetooth-enabled devices communicate after establishing a trusted relationship, all the credential information is left on both devices, even after the session is ended. This implementation hole allows potential hackers to have full access to the device, without the owner's knowledge or consent, based on the previously established trust relationship; attackers then can access confidential data stored on smartphones and manipulate it. The only way smartphone users would be able to detect such security flaws is to observe the Bluetooth icon indicating an established Bluetooth connection; otherwise, attackers will have unauthorized access to the victim's smartphone. This security shortcoming, along with other security flaws found in Bluetooth security architecture, such as device-based authentication rather than user-based authentication, make smartphones vulnerable to direct attacks and threaten privacy and critical personal information.
- **MMS/SMS:** Multimedia message service and short message service are both communication protocols that have become widely used and adopted by smartphone users as the standard for fast and convenient communications. Although it might seem unrealistic to think that hackers would ever be interested in targeting MMS/SMS, recent studies have shown that MMS/SMS can contain confidential information that is exposed to attacks due to lack of security services not provided by the cellular network. SMS suffers from exploitable vulnerabilities, such as lack of mutual authentication methods and non-repudiation. An SMS that is sent from a sender to a receiver cannot be

mutually authenticated by both parties, which opens doors for hackers to exploit. Also, senders who send SMS cannot be held accountable for their sent SMS because there is no mechanism that could be implemented to ensure the sender's true identity. The weak security implementation of SMS can also be used as attack mechanisms by hackers, where an arbitrary computer can be used to inject SMSs into the network, thus exposing smartphones to risks. In addition, SMSs are susceptible to man-in-the middle attacks while they are being transmitted over the air. Therefore, attackers are increasingly relying on MMS/SMS as an effective attack vector (Lockefeer, 2010).

- **File Injection and Downloadable Applications:** Malware authors constantly develop new and innovative ways for attacking smartphones; sending benign files that contain malicious code and downloadable applications have proven to be a successful attack mechanism adopted by hackers. What makes such attack vectors effective is the fact that they come in the form of legitimate applications, luring smartphone users to disclose their private and financial information. For instance, in January, 2010, a group of malicious writers calling themselves "09Droid" developed an application that specifically targeted Google Android phones and mobile banking institutions. The application contained the phrase "happy banking" on the summary statement that each application uses to advertise itself to potential users. The attack tempted users to purchase the mobile banking application from the Android Market in order to log on to their mobile banking accounts. While doing so, users would have to reveal their account numbers and passwords, which would then be sent to the authors of the malicious program (Morrison, 2010). This kind of well-crafted attack underscores the powerful capabilities of emerging attacks and the attackers; they target banking institutions and credit unions and use their logos to lure naive smartphone owners into giving their confidential information to applications that look exactly the same as the legitimate ones.

CONCLUSION AND SUGGESTIONS

Fortunately, there are possible solutions to the rampant cyber security problem with mobile devices. Once our society acknowledges that cyber security threats are detrimental not only to one smartphone user, but to the society as a whole; then the inception of a solution can begin. The value of data is steadily increasing, possibly even more so than actual money. It is imperative to establish a culture of cyber security because this issue is multifaceted and technology is constantly evolving.

Cyber Security Is Multidimensional: Collaboration Is Imperative for Its Success

Security concerns are not exclusive to "economists, political scientist, lawyers, business policy or management experts, or computer specialist" (Brechbuhl, Bruce, Dynes, & Johnson, 2010). In order to establish a policy of cyber security, it will take a collaborative effort from a variety of officials in various disciplines in society. Each official brings a specific set of knowledge to the issue of cyber security, and has a potential role in establishing the different set of functions that are needed to create a general intra-and international cyber security standard (Brechbuhl, Bruce, Dynes, & Johnson, 2010). Ultimately, a decentralized approach is the best way to make cyber security an interconnected, coordinating mechanism that benefits the society as a whole (Brechbuhl, Bruce, Dynes, & Johnson, 2010).

Cell Phone Attributes as Security Features

CTO Dan Schutzer of BITS, the technology policy division of the Financial Services Roundtable, states that mobile devices and other mobile devices are equipped with biometric security measures (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). Biometric is the statistical analysis of biological data using technology. Schutzer suggests that the cameras that are installed in mobile phones can be used for facial recognition or iris detection (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This is actually a great idea because, thanks to DNA, biologically everyone is different. Thus, the authenticated user of a smartphone will be the only person that can unlock his/her phone. Moreover, Shutzer proposes that the microphones installed in mobile devices can be used for voice recognition (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This is another way to secure and lock a cell phone; and only the authorized user of the phone will be able to unlock the device. In brief, using biometric measures to secure mobile devices is one way to prevent theft

CONCLUSION

Lastly, IT companies are seeing the niche in the market for security software specifically designed for mobile operating systems. Recently, a few companies have presented different mobile security software that consumers can purchase. Bullguard Mobile Security, Kaspersky Mobile Security, ESET Mobile Security, and Lookout Premium are mobile security software currently available for purchase (2012 Best Mobile Security Software Comparisons and Reviews, 2012). The programs range in prices from $19.99 to $39.99. These programs are a start; however, it is up to consumers to purchase them to secure their data. As mentioned earlier, cyber security is a multifaceted issue that must be dealt with accordingly. Ultimately, creating a national standard of cyber security is the best way to counteract the increase in cyber attacks.

REFERENCES

Barrera, D., & Van Oorschot, P. (2011). Secure Software Installation on Smartphones. *IEEE Security and Privacy*, *9*(3), 42–48. doi:10.1109/MSP.2010.202

Becher, M., Freiling, F., & Leider, B. (2007, June). On the effort to create smartphone worms in Windows Mobile. *Proceedings of the 2007 IEEE workshop on Information Assurance*. United States Military Academy. West Point, NY. Retrieved from http://pi1.informatik.uni-mannheim.de/filepool/publications/on-the-effort-to-create-smartphone-worms-in-windows-mobile.pdf

2012 Best Mobile Security Software Comparisons and Reviews. (2012). Retrieved April 17, 2012, from Top Ten Reviews: http://mobile-security-software-review.toptenreviews.com/

Bhattacharya, D. (2008) *Leardership styles and information security in small businesses: An empirical investigation* (Doctoral dissertation, University of Phoenix). Retrieved from www.phoenix.edu/apololibrary

Bose, A. (2008). *Propagation, detection and containment of mobile malware*. (Doctoral dissertation, University of Michigan). Retrieved from www.phoenix.edu/apololibrary

Brechbuhl, H., Bruce, R., Dynes, S., & Johnson, E. (2010, January). Protecting Critical Information Infrastructure: Developing Cybersecurity Policy. *Information Technology for Development*, *16*(1), 83–91. doi:10.1002/itdj.20096

Brown, B. (2009). *Beyond Downadup: Security expert worries about smart phone, TinyURL threats: Malware writers just waiting for financial incentive to strike, F-Secure exec warns*. Retrieved from http://business.highbeam.com/409220/article-1G1-214585913/beyond-downadup-security-expert-worries-smart-phone

Canalys. (2011, October 04). *Mobile Security Investment to Climb 44% Each Year Through 2015*. Retrieved April 22, 2012, from Canalys: http://www.canalys.com/newsroom/mobile-security-investment-climb-44-each-year-through-2015

CCEVS. (2008). National Security Agency, Common Criteria Evaluation and Validation Scheme. *Common criteria evaluation and validation scheme -- organization, management, and concept of operations (Version 2.0)*. Retrieved from National Information Assurance Partnership: http://www.niap-ccevs.org/policy/ccevs/scheme-pub-1.pdf

Eeten, M., & Bauer, J. (2009, December). Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications. *Journal of Contingencies and Crisis Management*, *17*(4), 221–232. doi:10.1111/j.1468-5973.2009.00592.x

Favell, A. (Ed.). (2011, November 2). *96 Percent of Smartphones and Tablets Lack Necessary Security Software. Why It Matters to Your Business - A Lot.* Retrieved April 22, 2012, from MobiThinking: http://mobithinking.com/blog/mobile-security-business-implications

Goth, G. (2009). U.S. Unveils Cybersecurity Plan. *Government Policy*, *52*(8), 23.

Grace, M., Zhou, W., Jiang, X., & Sadeghi, A.-R. (2012). Unsafe Exposure Analysis of Mobile In-App Advertisements. *Association for Computing Machinery - Security and Privacy in Wireless and Mobile Networks, 5*, 101-112. doi:10.1145/2185448.2185464

Harknett, R., & Stever, J. (2011). In N. Roberts (Ed.), *The New Policy World of Cybersecurity* (pp. 455–460). Public Administration Review.

Harris, S., & Meyers, M. (2002). *CISSP*. McGraw-Hill/Osborne.

Janczewski, L., & Colarik, A. (2007). *Cyber Warfare and Cyber Terrorism*. Hershey, PA: IGI Global; doi:10.4018/978-1-59140-991-5

Kaplan, J., Sharma, S., & Weinberg, A. (2011). Cybersecurity: A Senior Executive's Guide. *The McKinsey Quarterly*, 4.

Lockefeer, L. (2010). *Encrypted SMS, an analysis of the theoretical necessities and implementation possibilities*. Retrieved from http://www.cs.ru.nl

MacWillson, A. (2011, May 9). *Rethinking Cybersecurity in a Mobile World*. Retrieved March 9, 2012, from Security Week: Internet and Enterprise Security News, Insights & Analysis: http://www.securityweek.com/rethinking-cybersecurity-mobile-world

Mulliner, C., & Miller, C. (2009). Injecting SMS messages into smartphones for security analysis. *Proceedings of the 3rd USENIX Workshop on Offensive Technologies Montreal, Canada*. Retrieved from www.usenix.org

Ontang, M., McLaughlin, S., Enck, W., & McDaniel, P. (2009). *Semantically rich application-centric security in Android*. Retrieved from Proceedings of teh 25th Annual Computer Security Applciations Conference (ACSAC '09): http://dl.acm.org

Rao, L. (2011, December 13). *Lookout's 2012 Mobile Security Threat Predictions: SMS Fraud, Botnets And Malvertising*. Retrieved April 22, 2012, from Tech Crunch: http://techcrunch.com/2011/12/13/lookouts-2012-mobile-security-threat-predictions-sms-fraud-botnets-and-malvertising/

Rash, W. (2004). *Latest skulls Trojan foretells risky smartphone future*. Retrieved from www.eweek.com

Ruggiero, P. a. (2011). *Cyber Threats to Mobile Phones*. Pittsburgh: United States Computer Emergency Readiness Team.

Schmidt, A.-D., Bye, R., Schmidt, H.-G., Clausen, J., & Kiraz, O. (2009). *Static analysis of executables for collaborative malware detecion on Android*. Retrieved from www.dai-labor.de

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., & Glezer, C. (2010, March/April). Android: A comprehensive security assessment. *IEEE Security and Privacy*, *8*(2), 35–44. doi:10.1109/MSP.2010.2

Symantec, Inc. (2011, April 5). Retrieved April 17, 2012, from Symantec Report Finds Cyber Threats Skyrocket in Volume and Sophistication: http://www.symantec.com/about/news/release/article.jsp?prid=20110404_03

Traynor, P., Ahamad, M., Alperovitch, D., Conti, G., & Davis, J. (2012). *Emerging Cyber Threats Report 2012*. Atlanta: Georgia Tech Information Security Center.

Trend Micro. (2009, August 17). *Smartphone Users: Not Smart Enough About Security*. Retrieved April 17, 2012, from Trend Micro: http://newsroom.trendmicro.com/index.php?s=43&news_item=738&type=archived&year=2009

United States Computer Emergency Readiness Team. (2010, April 15). Cyber Threats to Mobile Devices. (TIP - 10-105-01), 1-16.

Vennon, T. (2010). *Android malware*. Retrieved from http://threatcenter.smobilesystems.com/

Wong, L. (2005). *Potential Bluetooth vulnerabilities in smartphones*. Retrieved from http://citeseerx.ist.psu.edu

Xie, L., Zhang, X., Chaugule, A., Jaeger, T., & Zhu, S. (2009). *Designing system-level defenses against cellphone malware*. Retrieved from www.cse.psu.edu

ZDNet. (2010). *Google fixes android root-access flaw*. Retrieved from ZDNet: www.zdnetasia.com

KEY TERMS AND DEFINITIONS

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (Harris, 2002).

Availability: Timely, reliable access to data and information services for authorized users (Harris, 2002).

Confidentiality: Assurance that information is not disclosed to unauthorized individuals, processes, or devices (Harris, 2002).

Cyber Terrorism: Attacks with the use of the Internet for terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses, worms, Trojans, and zombies (Janczewski & Colarik, 2008).

Integrity: Quality of an IS reflecting the logical correctness and reliability of the OS; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (Harris, 2002).

MMS/SMS: Multimedia message service and short message service are both communication protocols that have become widely used and adopted by smartphone users as the standard for fast and convenient communications.

Non-Repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (Harris, 2002).

Rootkit: Malicious software designed to hide the existence of programs or processes from the normal methods of detection and enable privileged access to a computer.

Trojan: Malicious non-self-replicating malware program when executed carries out actions determined by the developer of the program. Trojans act as an backdoor providing unauthorized access to the infected computer.

New Threats and Countermeasures in Digital Crime and Cyber Terrorism

Maurice Dawson
University of Missouri–St. Louis, USA

Marwan Omar
Nawroz University, Iraq

A volume in the Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series

Information Science REFERENCE
An Imprint of IGI Global

Managing Director: Lindsay Johnston
Managing Editor: Austin DeMarco
Director of Intellectual Property & Contracts: Jan Travers
Acquisitions Editor: Kayla Wolfe
Production Editor: Christina Henning
Development Editor: Brandon Carbaugh
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

New threats and countermeasures in digital crime and cyber terrorism / Maurice Dawson and Marwan Omar, editors.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4666-8345-7 (hardcover) -- ISBN 978-1-4666-8346-4 (ebook) 1. Computer crimes--Prevention. 2. Cyberterrorism--Prevention. 3. Computer security. I. Dawson, Maurice, 1982- II. Omar, Marwan, 1982-
HV6773.N4745 2015
005.8--dc23

2015006753

This book is published in the IGI Global book series Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) (ISSN: 2327-0381; eISSN: 2327-0373)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 6
Legal Issues:
Security and Privacy with Mobile Devices

Brian Leonard
Alabama A&M University, USA

Maurice Dawson
University of Missouri – St. Louis, USA

ABSTRACT

Privacy and security are two items being woven into the fabric of American law concerning mobile devices. This chapter will review and analyze the associated laws and policies that are currently in place or have been proposed to ensure proper execution of security measures for mobile and other devices while still protecting individual privacy. This chapter will address the fact that as the American society significantly uses mobile devices, it is imperative to understand the legal actions surrounding these technologies to include their associated uses. This chapter will also address the fact that with 9/11 in the not so distant past, cyber security has become a forefront subject in the battle against global terrorism. Furthermore, this chapter will examine how mobile devices are not like the devices of the past as the computing power is on par with that of some desktops and the fact that these devices have the ability to execute malicious applications. In addition, this chapter will discuss the reality, significance, legal and practical affects of the fact that suspicious programs are being executed offensively and security based attacks can be performed as well with the use of programs such as Kali Linux running on Android.

LEGAL BACKGROUND

Privacy and security are two ideals that are woven into the very fabric of the United States (U.S.) law. This is evidenced by the fact that they are principles that are embodied in the U.S. Constitution (*U.S.* Const., 1787). However, supporting and protecting these ideals is not without challenge, especially as technology and innovation make it increasingly more difficult to navigate these ideals and to continue to protect them. In a post-9/11 era, privacy and security have become increasingly challenging and in some cases have become difficult to reconcile with one another. One such area, is that of the safety and security of the Internet, including the mobile devices that are used more and more to access and

DOI: 10.4018/978-1-4666-8345-7.ch006

transact business and personal matters via the Internet. The dilemma faced by the U.S. is attempting to provide for the protection of the U.S. and its citizens from cyber attacks on the one hand, and trying to ensure that in so doing, the U.S. government does not become too intrusive into the lives of individuals and businesses on the other hand. This difficulty is most likely the reason why the U.S. still has yet to develop consistently broad national policy regarding cyber-security and the protection of U.S. citizens from cyber attacks. Moreover, the swiftness with which technology changes, and new threats emerge, have made it even more difficult for U.S. law and policy to develop comprehensive safeguards to protect the nation's and it's citizens' secure information.

INDUSTRY-SPECIFIC LAWS

Although comprehensive policy remains a challenge, there have been strides made in the passage of laws in specific industries and areas where the U.S. government and by representation, most U.S. citizens have acknowledged and likely accepted the need for national regulation regarding the security and safety of information. An early attempt at protecting electronic information from unauthorized access, is the Electronic Communications Privacy Act ("ECPA"). This Act criminalizes the unauthorized access of the electronic communications of another without the owner's or recipient's permission (Electronic Communications Privacy Act, 1988). Although probably not contemplated by the Act in its inception, mobile devices which transmit electronic communications in the form of e-mail and other forms of communication are likely covered by the ECPA (Electronic Communications Privacy Act,1988). However, this Act does not go far enough in that it does not deal more specifically with the more sophisticated nature of cyber attacks today.

Next, health information is probably for many the most important area of information that needs protection from attacks. Through the Health Insurance Portability and Accountability Act ("HIPAA"), the U.S. Government has provided for the creation of national standards for both the practical and technical security of health information (Health Insurance Portability and Accountability Act, 2000); Security Rule and Privacy Rule, 2003). Through subsequent standards adopted by the U.S government, these technical standards include such safeguards as the use of encryption, passwords, and other means of protecting health information from cyber attacks (Health Insurance Portability and Accountability Act, 2000; Security Rule and Privacy Rule, 2003).

Furthermore, post 9/11, the U.S Government formed the Department of Homeland Security through the Homeland Security Act ("HSCA"). Among other things, this act requires steps to be taken to protect it from terrorist attacks to include cyber attacks (Homeland Security Act, 2006). The Act provides for standards to protect the nation's defense network as well as to share information with private industries and organizations to protect against cyber threats in the private sector (Homeland Security Act, 2006). Along with the HSCA, the Federal Information Security Management Act ("FISMA"), requires all federal agencies to take measures to protect their networks, electronic information, and devices from cyber attacks (Federal Information Security Management Act, 2006). Lastly, the Gramm–Leach–Bliley Act ("GLB") requires banks and financial institutions to maintain the security of financial information and transactions (Gramm–Leach–Bliley Act, 2000).

As is clear from their industry-specific application, outside of national security and defense (HSCA), health services (HIPAA), federal agencies (FISMA), and financial services (GLB), all of these measures fall short in providing for comprehensive reform and policy regarding the protection of individual users of mobile devices and other devices from cyber attacks.

CURRENT CYBER-SECURITY EFFORTS ANDTHREATS

The U.S. government has identified multiple risks associated with cyber terrorism and its impacts. Cyber warfare is not limited to computer grid systems but all systems that are vulnerable such as mobile devices. Lewis (2002) states that the literature on cyber security assumes that the associated vulnerabilities of critical infrastructures and computer networks are the same.

FEDERAL EFFORTS

To that end, there have been some efforts by the U.S. government to deal with the area of cyber-attacks and cyber-security measures. Under his executive authority, for example, the President has issued an Executive Order - Improving Critical Infrastructure Cybersecurity (Executive Order No.13636, 2013) (the "Order"). This Order provides for among other things, information sharing among federal agencies and with the private sector, to include dissemination of reports regarding critical infrastructure assets, consultation, civil liberty protection, critical infrastructure risk reduction, cyber-security framework development, voluntary cyber-security program creation, and critical infrastructure cyber-security risk identification (Executive Order No.13636, 2013).

As required by the Order, the document, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.0,(the "Framework") was developed and issued within one year of the Order, on February 12, 2014. In 41 pages the Framework addressed the issues outlined by the Order (National Institute of Standards and Technology, 2014). The Framework makes clear that it is a living document and due to the constant changing nature of cyber threats that may occur, the Framework would also need to evolve and remain a fluid document (National Institute of Standards and Technology, 2014). The Framework's Core elements are Functions, Categories, Subcategories and Informative References (National Institute of Standards and Technology, 2014). The Functions of the Framework's Core are to Identify, Protect, Detect, Respond, and Recover (National Institute of Standards and Technology, 2014).

After research, it was determined that three agencies, the Environmental Protection Agency ("EPA"), the Department of Health and Human Services ("HHS"), and the Department of Homeland Security ("DHS") were required to submit reports regarding their specific areas of critical infrastructure ("the Reports") (*Assessing Cybersecurity Regulations*, 2014). The White House). The DHS report was comprised of three (3) areas: maritime critical infrastructure cyber-security standards, chemical facility anti-terrorism standards, and transportation critical infrastructure cyber-security standards (U.S. Department of Homeland Security, 2014). The EPA report focused on water and wastewater critical infrastructure cyber-security standards, and the HHS report focused on food and drug critical infrastructure cyber-security standards, and cyber-security standards and exercises designed to handle attacks on medical devices and health organizations. (U.S. Department of Health and Human Services, 2014,) While the federal government acknowledges that there is still more work to do, it is proud of the progress it has made in the area of cyber-security measures for critical infrastructure (The White House, 2014).

While the Order, the Framework, and the Reports are an important step toward national policy on cyber-security, they are limited to those areas considered critical infrastructure, or those areas and/or industries, both physical and virtual, that are "...so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters..." (Executive Order No.13636,

2013). There is a pretty good chance that use of smartphones, tablets, or other mobile devices might not fall into that category. In addition, even in the case of critical infrastructure, the Order specifically excludes any regulation of critical infrastructure security beyond what is already existing under current law, meaning, that it only requires certain actions to be taken but does not provide for greater policy or legal protection than what is already provided by other laws. Moreover, since it is only an Executive Order, it is applicable only to the federal agencies under the executive branch of government's control anyway (Executive Order No.13636, 2013).

STATE EFFORTS

In order to have significant, comprehensive and national policy regarding cyber-security for mobile devices, it is without question, a matter that the U.S. government is likely better equipped to handle and address. However, state efforts are still important and can be useful in this area. Not surprising, for example, the state of California has taken measures to include the passing of a law requiring businesses and organizations that experience a security breach to provide notice of the breach to those affected (Notice of Breach of Security Act, 2003). In addition, the state of California has also passed a provision requiring that businesses that maintain users' secure information, to enact "reasonable" levels of security to prevent the unauthorized access or disclosure of that information, which includes protection from cyber and other attacks on such information (California Assembly Bill No. 1950, 2004). As with the federal initiatives, it is likely that even these steps alone are not sufficient to protect users of mobile devices from cyber attacks.

However the state of California's Attorney General's Office has issued certain public awareness campaigns aimed at helping its citizens protect against cyber attacks using mobile devices. For example, its "Getting Smart about Smartphones" Campaign provides information sheets with Tips for Parents and Tips for Consumers. These information sheets warn parents and consumers of the risks of Apps, and encourages the screening, controlling, and reporting of Apps, as California law requires Apps to have a privacy policy (State of California Department of Justice Office of the Attorney General, 2013,). Furthermore, the Tips for Consumers remind consumers to not only check their Apps, but to check their Network, and that just like the desktop computer, smartphones remain vulnerable to attack from spyware, malware, and hackers. (State of California Department of Justice Office of the Attorney General, 2013, State of California Department of Justice Office of the Attorney General) Similar campaigns could go a long way to inform and educate users of mobile devices about the risks of cyber attacks.

PROPOSED REGULATIONS

Unfortunately, the lack of a national uniform policy regarding cyber security of mobile and other devices largely exists due to the lack of consensus in the U.S. government on the best way to provide such security and protection and at the same time avoid over-involvement of government in citizen's private affairs. This can be see in the failure of legislative efforts on both sides of the isle in Congress and by the President. For example, the Cyber-Intelligence Sharing and Protection Act (CISPA) was passed by the House of Representatives, but not favored by the Senate or the President, over concerns that in requiring the sharing of information, it also failed to protect critical infrastructure, as well as waived several civil liberties and

threatened individual privacy. (Cyber-Intelligence Sharing and Protection Act, 2012; Lardinois, 2012,). Similarly, the Cyber-security Act of 2012 was passed by the Senate and had Presidential support, in an attempt to provide for greater protection from cyber-security attacks. However, just like the CISPA, this bill faced opposition, largely due to concerns over the bill's alleged increased regulation of businesses. (Cybersecurity Act, 2012; *Cybersecurity Bill Wins Key Senate Vote*, 2012).

MODEL NATIONAL POLICY

Despite the failed legislative efforts to adopt national legislation and policy regarding cyber-security for mobile and other devices, there appears to at least be a consensus among the federal legislative and executive branches, of the necessity to enact some federal provision dealing with cyber-security in general. Given the importance and frequency of use of smartphones, tablets and other devices, any federal provision dealing with cyber-security would also most assuredly need to address mobile device security. This is because, as indicated by California's Attorney General, for the purposes of cyber-security, mobile devices are just as vulnerable as desktop computers and similar devices to attack. The main impediment then is what shape such regulation should take, taking into account the individual civil liberties and privacy concerns, business regulation concerns, and the protection of critical infrastructure concerns.

At the outset, a theoretical model policy on cyber-security for mobile and similar devices, would most likely need to emanate from the federal government. While each state has an interest in developing its own policy, a national policy would likely be more consistent and easier to navigate for most consumers and businesses, rather than a state by state approach. Furthermore, a national model policy on cyber-security likely has legal support and is authorized by the U.S. Constitution, under the Commerce clause' s authority to regulate matters that travel in or affect interstate commerce, which would include not only e-commerce but the use of mobile devices almost by definition (*U.S. Const.* 1787). Furthermore, there are likely numerous federal statutes and federal agencies that provide a basis for and could enforce a national model policy on cyber-security for mobile devices. However one possible agency that could be utilized in this national model policy is the the Federal Trade Commission ("FTC"), which was created by and enforces the Federal Trade Commission Act ("FTA"), and other rules promulgated by the FTC.

The FTC seems to be a wise choice not only for enforcing such a model national policy on cyber-security on mobile devices, but it also can assist in evaluation and implementation of such a model national policy. This is because as a bipartisan independent agency, the FTC is uniquely suited to handle the various disputes that have plagued Congress and the President in attempting to come to a consensus about the larger issue of cyber-security and the smaller issue of cyber-security for users of mobile devices. (Federal Trade Commission Act, 1914) Moreover, one of the FTC's primary roles is consumer protection. Consequently the most likely victims of cyber-security attacks and breaches upon mobile devices are consumers, and thus the agency charged with protection of consumers seems to be the likely choice to promulgate and enforce standards of a national model policy to address this issue. Furthermore, the FTC has already taken steps to protect consumers from cyber-attacks through cases it has presented against Twitter and Wyndam, for example. (U.S. Federal Trade Commission, 2011; Egan, 2014).

In addition, the FTC could engage in public education and awareness campaigns designed to assist consumers in becoming more knowledgeable about the existence of and how to prevent cyber attacks similar to those used by California's Attorney General's office mentioned above. While the FTC can develop specific standards, through the public comment and hearing process, there still needs to be a

national model policy which lays the framework for the FTC to utilize. The good news is that there is already a starting point for such a framework in place. However, the Framework developed as a result of the Order issued by the President would need to be expanded to include consumer protection and more specifically the threat of cyber-security attacks on mobile devices used by consumers in order to be developed into a national model policy. This can likely be done with the aid of the FTC, as well as private entities or public interest organizations committed to protecting and ensuring the integrity of mobile devices for their continued use. Once the consumer protection and mobile device provisions are added to the Framework, the final pieces to be added would be provisions to protect individual privacy and business autonomy, which could follow the previous examples of HIPAA and GLB, since these laws are industry-specific, to address such concerns. Critical infrastructure protection is already provided for in the Framework and thus this concern has already been addressed by the document. Once completed, the revised Framework would still need bipartisan support from both houses of Congress and the President, before being adopted. If that can be done, then the U.S. could finally have a national model policy on cyber-security for mobile devices. The national policy could allow states to model their own policy after the national policy, where necessary, but could retain certain minimum standards necessary to ensure continuity and comprehensiveness nation-wide.

Finally, as always the courts as the third and final branch of the federal government would serve their ever-important role of interpreting such provisions of the national policy to ensure that the privacy and other legal concerns are adequately protected as they have done in the past, while still preserving the ideal of cyber-security for consumers using mobile devices (*U.S. Const.*, 1787; Marbury v. Madison, 1803).

GOVERNMENT TECHNICAL GUIDANCE

The National Institute of Standards and Technology (NIST) is charged with promoting innovation and industrial competitiveness by advancing measurement science, standards, and technology to enhance America's economic security. Additionally, it is charged with improving the quality of life. NIST's Computer Security Division publishes the Special Publications (SP) 800 Series that are general interest to the computer security community. These publications represent collaborative efforts between industry, government, and academia. NIST Special Publication (SP) 800-124, Guidelines on Cell Phone and PDA Security provides general insights into securing these devices (Jansen & Scarfone, 2008). Jansen and Scarfone (2008) provide guidance about the threats and technology risks associated with mobile devices to includes potential methods for mitigation. Ayers, Brothers, and Jansen (2013) drafted guidelines for mobile forensics which is important as the U.S. has the right to use forensics techniques at any port of U.S. entry at that particular entry point. An older guidelines NIST SP 800-19 Mobile Agent Security, published Oct 1999, was one of the first guidelines to address security for mobile agent security. Jansen and Karygiannis (1999) identified generic security objectives and various measures for countering the identified threats. It is important to note that the SP 800-19 address specifically mobile code execution.

Other key NIST guidance such as SP 800-164 Guidelines on Hardware-Rooted Security in Mobile Devices provide guidance on how mobile devices can provide strong security assurance to end users and organizations (Draft) (Chen et al, 2012). The aim of the guidance document is to further industry efforts to implement these primitives and capabilities (Chen et al, 2012). As much of the other NIST SPs this SP provides a baseline of security technologies that can be implemented that will aid in securing mobile devices that are used in enterprise environments. The key capabilities in this SP is broken into three sec-

tions which are the following: 1) device integrity, 2) isolation, and 3) protected storage. Device integrity is the absence of corruption in the firmware, hardware, and software in a mobile device. Integrity is one of the three pillars in the Availability, Integrity, and Confidentiality (AIC) triad that Information Assurance (IA) is built upon. Isolation prevents unintended interaction between Information Owners on the same device (Chen et al, 2012). The Information Owner is not to be confused with the Device Owner. Protected storage deals with preserving the confidentiality and integrity of the data while in use, and at rest. However encrypting data has ramifications such as being jailed in certain countries for refusal to give up encryption keys.

Bring Your Own Device (BYOD)

Understanding the legal issues and ramifications are ever more important as organizations are pushing for Bring Your Own Device (BYOD) and security and privacy are a significant factor (Miller et al, 2012). When we think of mobile devices it is essential that the hyperconnectivity trend is taken as a factor (Dawson et al, 2014). As mobile devices connect with corporate networks while still enabling services such as Bluetooth pose a real threat. To be secure and compliant organizations must re-evaluate their wireless security models (Welch & Lathrop, 2003). BYOD will need to address licensing as virtualization must occur for partitioning and security. BYOD has yet to address issues surrounding a data link or confidential data bleed over. An approved architecture must be created to satisfy the policies and laws of that state. Furthermore this architecture must be scalable.

CONCLUSION

In conclusion, legal issues in the area of cyber-security and privacy with respect to mobile devices will have to be continually reviewed and updated where necessary to address and adapt to the changing technological environment. However, a model national policy that provides legal protection, provides for legal standards, promotes education, and information sharing, would be an important and critical first step to protecting consumers and users of mobile devices from the ever-present threat of cyber attacks. Changing trends such as BYOD will force organizations to determine how data is secured and segregated.

REFERENCES

Ayers, R., Brothers, S., & Jansen, W. (2013). Guidelines on Mobile Device Forensics (Draft). *NIST Special Publication*, *800*, 101.

California Assembly Bill No. 1950, (2004). Cal. Civ. Code § 1798.82

Chen, L., Franklin, J., & Regenscheid, A. (2012). Guidelines on Hardware-Rooted Security in Mobile Devices (Draft). *NIST Special Publication*, *800*, 164.

ConstU.S.. art. IV (1787).

ConstU.S.. Pmbl(1787).

U.S. Const. amend. IV (1791).

Cyber-Intelligence Sharing and Protection Act, (2013). H.R. 3523, 112th Congress (2011-2012), (2012), H.R. 624,113th Congress (2013-2014)

Cybersecurity. (2014). Retrieved June 14, 2014 from http://www.phe.gov/Preparedness/planning/cip/Pages/eo13636.aspx

Cybersecurity Act of 2012, (2012). S. 2105, 112th Congress (2011-2012).

Cybersecurity bill wins key Senate vote, upi.com. (2012). Retrieved June 14, 2014 from http://www.upi.com/Top_News/US/2012/07/26/Cybersecurity-bill-wins-key-Senate-vote/UPI-57801343345113/

Cybersecurity Framework. (2014). Retrieved June 14, 2014 from http://www.dhs.gov/publication/eo-13636-improving-ci-cybersecurity

Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). The Future of National and International Security on the Internet. In A. Kayem & C. Meinel (Eds.), *Information Security in Diverse Computing Environments* (pp. 149–178). Hershey, PA: Information Science Reference; doi:10.4018/978-1-4666-6158-5.ch009

Department of Health and Human Services. (2014). *HHS Activities to Enhance.* Author.

Department of Homeland Security. (2014). *Section 10(a) and 10(b) Report on the United States Coast Guard (USCG) and Maritime Critical Infrastructure Cybersecurity Standards,Section 10(b) Report on the Department of Homeland Security's Chemical Facility Anti-Terrorism Standards (CFATS)Section 10(b) Report on the Transportation Security Administration's (TSA's) Approach to Voluntary Industry Adoption of the NIST.* Author.

Egan, M. (2014). *Judge Rules FTC Can Sue Wyndham Over Cyber Security Lapses.* Retrieved June 16, 2014 from http://www.foxbusiness.com/industries/2014/04/08/us-ftc-can-sue-hotel-group-over-poor-data-security-court-rules/

Electronic Communications Privacy Act of 1986, (1988). 18 U.S.C. §§ 2510-2511

Exec. Order No. 13636, (2013). 78 FR 11737, 11737 -11744

Federal Trade Commission Act, (1914). 15 USC §§ 41-58

FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information. (2014). Retrieved June 16, 2014 from http://www.ftc.gov/news-events/press-releases/2011/03/ftc-accepts-final-settlement-twitter-failure-safeguard-personal

Gramm–Leach–Bliley Act of 1999, (2000). 15 U.S.C. §§ 6801-6809; 6821-6827

Harris, S., & Meyers, M. (2002). *CISSP*. McGraw-Hill/Osborne.

Health Insurance Portability and Accountability Act of 1996, (2000). 42 U.S.C. §§1320d-1320d-9

Health Insurance Portability and Accountability Act of 1996, Privacy and Security Rule, (2003). 45 C.F.R. §§ 164.102-164.534

Homeland Security Act of 2002, (2006). 6 U.S.C. §§ 101-613 Federal Information Security Management Act of 2002, (2006). 44 U.S.C. §§ 3541-3549

Janczewski, L., & Colarik, A. (2008). *Cyber Warfare and Cyber Terrorism*. Hershey, PA: IGI Global; doi:10.4018/978-1-59140-991-5

Jansen, W., & Karygiannis, A. T. (1999). *SP 800-19. Mobile Agent Security*. Gaithersburg, MD: National Institute of Standards & Technology.

Jansen, W., & Scarfone, K. (2008). Guidelines on cell phone and PDA security. *NIST Special Publication*, *800*, 124.

Lardinois, F. (2012), *U.S. House passes controversial CISPA cybersecurity bill 248 To 168.* Retrieved June 14, 2014 from http://techcrunch.com/2012/04/26/u-s-house-passes-cispa-248-to-168/

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Center for Strategic & International Studies.

Marbury v. Madison, (1803). 5 U.S. 137

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: security and privacy considerations. *It Professional, 14*(5), 53-55.

National Institute of Standards and Technology (NIST). (2014). *Framework for Improving Critical Infrastructure Cybersecurity*. United States of America.

Notice of Breach of Security Act, (2003). Cal. Civ. Code § 1798.29

Sarker, S., & Wells, J. D. (2003). Understanding mobile handheld device use and adoption. *Communications of the ACM*, *46*(12), 35–40. doi:10.1145/953460.953484

State of California Department of Justice Office of the Attorney General. (2013). *Getting smart about smartphones, tips for parents.* Retrieved June 14, 2014 from http://oag.ca.gov/privacy/facts/online-privacy/smartphones-parents

The White House. (2014). *Assessing Cybersecurity Regulations*. Retrieved June 14, 2014 from http://m.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations

U.S. Const. art. I, § 8, cl. 1 (1787).

U.S. Const. art. I, § 8, cl. 3 (1787).

U.S. Const. art. III, §§ 1-2 (1787).

U.S. Environmental Protection Agency. (2014). *Section 10(b) report on the environmental protection agency's water and wastewater critical infrastructure cyber-security preparedness.* Retrieved June 14, 2014 from http://water.epa.gov/infrastructure/watersecurity/upload/EO_13696_10-b-_EPA_response.pdf

Welch, D., & Lathrop, S. (2003, June). Wireless security threat taxonomy. In *Information Assurance Workshop* (pp. 76-83). IEEE.

KEY TERMS AND DEFINITIONS

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (Harris, 2002).

Availability: Timely, reliable access to data and information services for authorized users (Harris, 2002).

Confidentiality: Assurance that information is not disclosed to unauthorized individuals, processes, or devices (Harris, 2002).

Cyber Terrorism: Attacks with the use of the Internet for terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses, worms, Trojans, and zombies (Janczewski & Colarik, 2008).

Device Owner: Entity that has purchased and maintains ownership of device (Chen et al, 2012).

Information Owner: An application-specific provider, a digital product provider, or an enterprise that allows access to resources from mobile devices, (Chen et al, 2012).

Integrity: Quality of an IS reflecting the logical correctness and reliability of the OS; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (Harris, 2002).

Mobile Device: This device type is usually referred to as a handheld, handheld device or handheld computer (Sarker & Wells, 2003).

Non-Repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (Harris, 2002).

Technology, Innovation, and Enterprise Transformation

Manish Wadhwa
Salem State University, USA

Alan Harper
South University, USA

A volume in the Advances in Business Information Systems and Analytics (ABISA) Book Series

BUSINESS SCIENCE Reference
An Imprint of IGI Global

Managing Director: Lindsay Johnston
Acquisitions Editor: Kayla Wolfe
Production Editor: Christina Henning
Development Editor: Allison McGinniss
Typesetter: Kaitlyn Kulp
Cover Design: Jason Mull

Published in the United States of America by
Business Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Technology, innovation, and enterprise transformation / Manish Wadhwa and Alan Harper, editors.
pages cm
Includes bibliographical references and index.
Summary: “This book addresses the crucial relationship between a business and its technical implementations, and how current innovations are changing how the industry operates by highlighting current theoretical frameworks, novel empirical research discoveries, and fundamental literature surveys”-- Provided by publisher.
ISBN 978-1-4666-6473-9 (hardcover : alk. paper) -- ISBN 978-1-4666-6474-6 (ebook) -- ISBN 978-1-4666-6476-0 (print & perpetual access) 1. Business enterprises--Technological innovations. 2. Organizational change. I. Wadhwa, Manish, 1981- editor. II. Harper, Alan H., 1966- editor.

HD45.T3966 2014
658.5’14--dc23

2014026548

This book is published in the IGI Global book series Advances in Business Information Systems and Analytics (ABISA) (ISSN: 2327-3275; eISSN: 2327-3283)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 16
Advances in Technology Project Management:
Review of Open Source Software Integration

Maurice Dawson
University of Missouri – St. Louis, USA

Brian Leonard
Alabama A&M University, USA

Emad Rahim
Oklahoma State University, USA

ABSTRACT

As organizations must continually drive down costs of software-driven projects, they need to evaluate the Systems Development Life Cycle (SDLC) and other software-based design methodologies. These methodologies include looking at software-based alternatives that could save a significant amount of money by reducing the amount of proprietary software. This chapter explores the use and integration of Open Source Software (OSS) in software-driven projects to include in enterprise organizations. Additionally, the legalities of the GNU General Public License (GPL), Lesser General Public License (LGPL), Berkeley Software Distribution (BSD), and Creative Commons are explored with the integration of these OSS solutions into organizations. Lastly, the chapter covers the software assurance and cyber security controls to associate with OSS to deploy a hardened product that meets the needs of today's dynamically evolving global business enterprise.

DOI: 10.4018/978-1-4666-6473-9.ch016

APPROACH

The authors reviewed multiple Linux distributions and their uses. Reviewed in depth were the copyrights and open sourcing legal implications.

IMPRESSION

As indicated through legal case reviews, there are some very valuable benefits to open source software, in that it allows for collaboration in the development of new software and technology that can undoubtedly spur innovation and improve many processes and functions that individuals and businesses in our society rely on every day. Consequently one purpose of the GNU GPL is to protect and preserve individual rights and the creativity of others while at the same time providing a benefit and contributing to society at large. OSS must be considered in the development process as it is essential in overall license cost reduction with the ability to reuse already constructed software.

PROJECT MANAGEMENT

There are numerous perspectives regarding the concept of project management as this is a field with many employment opportunities in various industries such as defense or aerospace (Dawson & Rahim, 2011). Thus, the definitions generated by these perspectives also vary, according to the context in which it is discussed. However, the purpose of most project management activities is generally similar. Project management is a way of managing and organizing corporate resources so the available resources can generate the completion of a project within given scope, time, and resource constraints (Wideman, 2001).

The understanding behind project management also accounts for the definition of a project. A project is a unique endeavor performed to create certain products, services, or results (Project Management Institute, 2009). This definition is dissimilar to the definitions of process and operation due to several factors. The easiest to define is the time-constraint factor. A project performs the work necessary to complete activities within a limited amount of time, while processes and operations generally account for on-going continuous effort. A project aims to produce a single or a group of products, services, or results and the chain of activities are terminated once these are produced. Thus it is important to understand the acquisition of Information Technology (IT) and Information Systems (IS) in project management (Rahim & Dawson, 2010).

Software Design Methodologies

The SDLC is a process for planning, creating, testing and deploying ISs (Avison & Fitzgerald, 2003). Requirements are an impact factor as they feed the development and serve as an important prerequisite to development. The SDLC is a modified waterfall method as when objectives are not met then the process is to move backward but the goal is to continually move forward into the next process steps such as system deployment. Another design methodology is agile software development. Agile is based on iterative and incremental development, in which requirements and solution evolve through collaborating teams (Cockburn, 2002). In agile it is essential to understand the people factor to ensure success (Cockburn & Highsmith, 2001). A modified agile methodology is Scrum which is an interactive and incremental software development framework (Rising & Janoff, 2000). All methodologies described allow for code reuse and the integration of OSS. As design methodologies continue to grow so does the need for quicker development. To do this effectively one would need to consider using the option of code reuse.

Details of Linux

The definition, terms, and understanding of open-sourcing have been synonymous with the World Wide Linux is an Unix like OS that is built on the Linux kernel developed by Linus Torvalds with thousands of software engineers. As of 2012 there are over two hundred active Linux distributions. The majority of the kernel and associated packages are free and OSS. This type of software provides licenses which allows users the right to use, copy, study, change, and improve the software as the source code is made available. Providing source code allows an organization's developers or engineers to understand the inner workings of development. Imagine being able to study Mac or Windows by viewing all the source code to replicate similar developments. This exercise would be great for a new developer to learn low level coding techniques, design, integration, and implementation. Students and faculty could actively participate in design groups in which they would contribute code or design guidance for the upcoming software releases.. However some distributions require a cost for updates or assistance that related to specific needs such as OS modifications for server hosting. In software, there is a packet management system that automates the process of installing, configuring, upgrading, and removing software packages from an OS. In the Linux OS builds the most common packet management systems are Debian, Red Hat Package Manager (RPM), Knoppix, and netpkg.

Since Linux does not have redistribution limits it can be used to replace proprietary OSs in computer labs to save costs. The cost that would be associated with the proprietary labs can be redirected towards additional hardware instead. With the many variations of Linux one can find the appropriate distribution for their targeted use. Table 1 displays the different distributions to include the potential uses.

Fedora is an OS based on the Red Hat Package Manager (.rpm) (Proffitt, 2010). Fedora has a side development project known as Fedora Spins which contains multiple spin off versions of the Fedora OS. These spins allow academics, researchers, and students the ability to perform tasks such as cyber security, forensics, electronics design, and more (Petersen, 2013). Two of the spins are lightweight distributions which are key to reviving older systems. Kitten Lightweight Kernel (LWK) and other similar kernels allow individuals the ability to practice development on lightweight OSs (Brightwell, Riesen, Underwood, Hudson, Bridges, & Zaharia, 2003). The possibilities are endless for encouraging low level development, integration, and increasing overall lifecycle expertise.

Why Use Open Source

Using OSS such as Linux allows for a significant reduction in the cost of proprietary licensing. Additionally, when coupled with virtualization OS capabilities can be replicated in a virtualized layer (Dawson & Al Saeed, 2012). Much software today is too complex to be developed from scratch thus reuse adds competitiveness allowing for immediate code reuse (German, & González-Barahona, 2009). In addition, OSS provides the ability to allow developers to perform static code analysis on source code as it is readily available (Louridas, 2006). As over half of the vulnerabilities are found in the application using OSS could provide beneficial to all that are stakeholders in the SDLC (Paul, 2011). Additionally, benefits include the ability to capture all known and unknown risks that allow the use of sound software engineering practices (McGraw, 1999).

Argument against the Use of Open Source

One of the most well-known arguments against the use of OSS is that individuals with malicious intent can find flows within the code and exploit them (Carrier, 2002). The issue with this particular

Table 1. Linux distributions and uses

Linux Distributions	Description and Potential Use	Packet Management System
Ubuntu	One of the most popular Linux OS developed to be a complete OS that can be an easily replacement for other comparable OSs.	Debian-based
Edubuntu	OS targeted for grades k-12. Contained in OS are tons of software applications that is useful to those who are education majors.	Debian-based
Damn Small Linux	This OS is designed to as a small OS to be utilized on older hardware. This OS is great for institutions that have old computers and want to revitalize them for use. OS is also great for VMs as DSL requires a low amount of memory	Knoppix-based
BackTrack	OS based on Ubuntu for digital forensics and penetration testing. Great tool for students majoring in technology fields. As cyber security is becoming a hot topic around the world this tool provides students the ability to learn from over thirty software applications that aid in penetration testing and more.	Debian-based
Kali Linux	OS based BackTrack that is a continuation of the popular penetration testing distribution.	Debian-based
Red Hat Enterprise Linux	This OS serves as the standard for many enterprise data centers. OS was developed by Red Hat and targeted for commercial use. Red Hat has a policy against making nonfree software available for the system through supplementary distribution channels. This is different and why this OS is listed as an exception in terms of OSS.	RPM-based
Fedora	This OS is supported by the Fedora Project and sponsored by Red Hat. This OS provides a great resource for learning Red Hat Enterprise Language (RHEL). As there are thousands of jobs requiring expertise specifically with Red Hat this OS is a great tool to prepare students for employment in IT. Fedora has over six Fedora Spins such as Design-suite, Scientific-KDE, Robotics, Electronic-lab, Games, and more.	RPM-based
CentOS	This OS derived entirely from RHEL. The source code is developed from Red Hat which allows a student to learn RHEL with a small number of differences. CentOS can be used for teaching IT students on how to setup, administer, and secure a server.	RPM-based
SUSE Linux	OS is of German origin with the majority of its development in Europe. Novell purchased the SUSE brand and trademarks.	Debian-based
Xubuntu	Xubuntu is based upon Ubuntu however it uses the light weight Xfce desktop environment.	Debian-based
Ubuntu Studio	This OS is derived from Ubuntu. This OS is developed specifically for multimedia production such as audio, video, and graphics. Departments for multimedia could use this OS for multimedia instruction and the development of projects. As many of the tools for multimedia production are expensive this alleviates large license costs for institutions.	Debian-based
Lubuntu	OS is based on Ubuntu and uses the LXDE desktop environment. It replaces Ubuntu's Unity shell and GNOME desktop.	Debian-based
Chromium OS	An open source light weight OS that is targeted for netbooks and mobile devices.	Portage-based

argument is that proprietary software packages or closed OSs are being exploited such as Windows. More importantly more research needs to be understood on the accessibility and human use of the different operating environments (González, Mariscal, Martínez, & Ruiz, 2007). The misconceptions surround ease of use in which individuals feel they need to have a mastery of command line

among other system administrator like abilities to navigate the desktop based OSs. Thus more attention needs to be provided to system usability for industry and home use on the modern open source Linux OS such as Ubuntu 14.04 Long Term Support (LTS) and others (Brooke, 1996).

COPYRIGHTS AND OPEN-SOURCING: ECONOMIC AND LEGAL IMPLICATIONS

Basis of Legal Protection

Copyright Law

The U.S. Constitution provides that, "The Congress shall have Power… [t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries;…"[1] A copyright gives the author, provided certain legal requirements are met, exclusive rights to distribute, sell, license, produce, and publish the copyrighted material (Cheeseman 2013). Moreover, the Copyright Revision Act of 1976, establishes the legal requirements for copyright protection and provides for protection for copyright infringement (Cheeseman 2013). In addition, in 1989, the U.S. and several other countries signed the Berne Convention, which is an international copyright treaty.

Establishing copyright protection is only half the battle. In order to prove copyright infringement, one must show that a party has copied a substantial and material part of the owner's copyrighted work without permission (Cheeseman 2013). If successfully proven, an owner of a copyrighted work may recover profits from the infringement, damages suffered by the owner, and even a court order requiring destruction of the infringing material and/or an order preventing such infringement in the future (Cheeseman 2013).

License Agreement

In its most basic sense, a licensing agreement is a detailed agreement which indicates the terms between a licensor, the owner and/or creator of intellectual property, and a licensee, the party who his granted limited rights in or access to the intellectual property (Cheeseman 2013). A licensing agreement may be a contract, but all licensing agreements may not meet the requirements of a contract. (Stein 2006). The extent to which a licensing agreement meets the legal requirements of a contract may provide greater or lesser legal protection of the intellectual property (Stein 2006).

Traditional Contract Law

Basic contract law requires that in order for an agreement to be legally enforceable, it must contain at minimum, an offer, an acceptance, and must be supported by consideration. An offer is generally a manifestation of intent to be bound, and an acceptance requires an unequivocal assent to the terms of the offer. Consideration is generally defined as bargained for exchange, where each side of the agreement receives some legal value. Generally courts will not inquire into the adequacy of consideration, or in other words the sufficiency of consideration (Cheeseman 2013). If an agreement is a legally enforceable contract, the law provides for several remedies in the event that a party to the agreement does not fully perform the agreement or violates its terms in some way.

Unique Challenges of Open Source Software

Copyleft and Free of Charge

One of the major challenges of "open source software," is the fact that the author or creator of the original source code, makes their source code available to other users to distribute and modify,

free of charge, and in many cases requires that any modification of that source code must also remain free and available to other users down the line, or the concept of copyleft work (Stallman, 2013). The problem for traditional copyright law is that it has primarily been focused on protecting and restricting the use and distribution of copyrighted work rather than the free and open distribution thereof. Furthermore, the fact that the software is made available free of charge creates some problems when it comes to determining whether and to what extent the author or creator has suffered any damages, and is therefore entitled to any compensation as is usually the case in the traditional copyright infringement lawsuit.

Enforceability

Furthermore, given the usual form of the open source licenses utilized by creators and authors of open source software, there is some question as to the availability of proof that the licensee of open source software is even aware or ever assents to the terms of the license. (Stein 2006). For example, if a licensee of open source software is not aware that there is a license or what the terms of the license provide, it may be difficult, in the event that the user modifies the licensed source code and then attempts to restrict its availability to others, for the author or licensor to enforce the license against the licensee. This would not be the case for example, if the licensee was required to download the source code and in doing so had to accept the terms and conditions of the license (Stein 2006).

Lack of Consideration

Another challenge for licensors of open source software is whether and to what extent the license is actually a contract or merely a bare license (Stein 2006; Mandrusiak 2010). If an open source license was considered to be more than just a bare license, but a contract, the author or creator may enjoy greater protection. (Stein 2006; Mandrusiak 2010). The problem however is that in order to be considered more than just a bare license, but a contract, the license would have to meet the traditional contract law requirements, which includes consideration. In order for an open source license to be enforceable as a contract, the author or creator must show that it is supported by consideration. Thus the author or creator or licensor must be able to show some legal value provided and received for the use of the license and source code. Since many of these open source code license are made available free of charge, it may be more difficult for a licensor to make such a showing. There are other arguments that a licensor may have such as that the promise to abide by the terms of the license could be sufficient consideration, but it may be unclear whether courts would agree with this rationale. If not, then the open software license would not be considered a legally enforceable contract and therefore, would not receive the traditional contract law protections or remedies for breach.

Illustrative Cases

There have been a few cases to consider the legal protections afforded to some open source software code materials. For example, in *Computer Associates International v. Quest Software, Inc., et al.*, the court recognized the validity of the GPL involved in that case, and specifically found that any user of the GNU GPL was bound by its terms.[2] Furthermore, the court noted that no copyright protection could be afforded to the modified version of the source code provided based on the terms of the GNU GPL. However, the Court further found that where the GNUGPL provided an exception for the commercial use of the output of that program, the GNUGPL would not be violated and copyright protection may exist for that output.[3]

In addition in *Progress Software Corporation, et al., v. Mysqlab, et al.,* the Court recognized and considered, but did not rule upon at that stage of the case, a GNUGPL that was at issue in that case.[4] Furthermore, in *Planetary Motion, Inc., v. Techplosion, Inc., Michael Gay A.K.A. Michael Carson,* the Court recognized and reiterated that the GNU GPL utilized in that case, "…allows users to copy, distribute and/or modify the Software under certain restrictions, e.g., users modifying licensed files must carry "prominent notices" stating that the user changed the files and the date of any change."[5]

Lastly, but certainly not least, probably the most notable case which dealt with legal protection, specifically copyright protection and open source software, is the *Jacobsen, v. Katzer, et. al.*[6] In *Jacobsen*, the U.S. Court of Appeals for the Federal Circuit, considered whether and to what extent a copyright holder, could use copyright laws to enforce an open source license, with respect to software that that had been made free and available to the public. The District Court held that while the defendant's actions may have been in breach of the nonexclusive Artistic License granted to them, they did not rise to the level of copyright infringement, and thus did not allow the copyright holder to use copyright laws to enforce the open source license.

The U.S. Court of Appeals for the Federal Circuit, on the other hand not only recognized the existence of the Artistic License, but held that despite its nonexclusivity, the Artistic License, did prevent certain other actions from being taken with regard to the source code, specifically use of the information without compliance with the Artistic License, such as indicating the source of the material, and including appropriate notices with any subsequent distribution of the material.[7] The Court specifically held, that "Copyright holders who engage in open source licensing have the right to control the modification and distribution of copyrighted material."[8] The court also held that the mere fact that open source licenses like the Artistic License at issue in the case are free of charge, does not render them devoid of economic value, and does not entitle them to any less protection than other forms of copyrighted material. The Court stated, "[t]he choice to exact consideration in the form of compliance with the open source requirements of disclosure and explanation of changes, rather than as a dollar-denominated fee, is entitled to no less legal recognition."[9]

Thus, the *Jacobsen* case appears to have provided at least one example of where a Court has provided copyright and it appears probably contract protection open source software utilizing open source licenses, in a way that some had believed was not possible given their unique nature. However it should be noted, that it is not clear whether other federal circuits will follow suit, and/or if the U.S. Supreme Court will ultimately agree with the *Jacobsen* Court in its analysis of this issue. As with many issues in the law, we will have to wait and see.

UCITA

In addition to the cases previously discussed, the Uniform Computer Information Transactions Act (UCITA) may also provide some legal protection to open source software and code, in the states where it has been enacted, and except where federal law controls, such as in the area of copyright law. The "…UCITA is a model act that establishes a uniform and comprehensive set of rules governing the creation, performance and enforcement of computer information transactions." (Cheeseman 2013).

Review of the Specific Licenses

GNU GPL v3

After a review of the terms and conditions provided by this license it appears to be more comprehen-

sive in its requirements for use of the licensed software. It contains several more terms and appears to contain many more prohibitions that the previous version of the license terms contained. It contains the requirement to include appropriate notices for distribution of the code. It also contains specific prohibitions regarding restriction on the subsequent use of the code, including modified versions, by downstream users (Kumar, 2006).

GNU GPL v2

After review of the terms and conditions of this license, this version's license does not appear to have as many requirements and certainly is not as long as the newest version of this software's license appears to be. While considerably shorter than the subsequent version's license, this license does still maintain and include the requirement that appropriate notices accompany the distribution of the code (Kumar, 2006).

LGPLv3

After review of the terms and conditions of this license, this version's license does not appear to have as many requirements as either of the licenses under the GNUGPLv3 or v2, but it does maintain several requirements for compliance. Of note, is this license includes an exception to the GNUGPL license, namely that the work produced under this license may be reproduced without compliance with Section 3 of the GNUGPL, which relates to Protecting Users' Legal Rights from Anti-Circumvention Law.

LGPL v2

After review of the terms and conditions of this license, this version's license appears to somewhat longer than the terms and conditions of the subsequent version's license, but it appears to be closer to the GNUGPLv2's license terms than the LGPLv3's terms and conditions, and noticeably does not include the exception to the GNUGPL license as is contained in the subsequent version of this license.

LLGPL

After review of the Lisp Lesser General Public License (LLGPL), this version's license is like the LGPL but with a prequel. This prequel defines the effect in terms more typically used in Lisp programs. This license is grounded in the C programming language as the license specifically calls out functions not present in other languages that are not traditionally compiled (Greenbaum, 2013).

Creative Commons

After review of the terms and conditions of this license, it appears that this license is very similar to that of Modified BSD. It is interesting of note that the license begins by indicating that the company is not a law firm. Additionally, this license appears to include a waiver of copyrights and related rights, and a fall-back in the event that the waiver is invalidated, which appears to be based upon the purpose of promoting the overall ideal of free culture. In addition this license includes a limitation to make sure that neither patent or trademark rights are being waived by this license.

Artistic License 2.0

After review of the terms and conditions of this license, this license appears to be very similar to that at issue in the *Jacobsen* case discussed above. Moreover, it appears that this license makes clear that the copyright holder intends to retain some creative control over the copyrighted work overall,

while still trying to ensure that the copyrighted material remains as open and available to others as possible under the circumstances.

Modified BSD

After review of the terms and conditions of this license, these terms and conditions appear to be the shortest list of terms and conditions of all of the licenses reviewed in this paper. Additionally this license appears to allow reproduction and modification of the copyrighted material provided certain conditions are met, which if subject to legal challenge, a court might construe as being subject to only protection as a contract, at best, and a bare license at worst. Moreover, based upon the legal authorities cited in this paper, it may be unclear whether this license may provide sufficient copyright protection.

Clear BSD License

After review of the terms and conditions of this license, this license appears to be very similar to the Modified BSD License, in that it is very short, and appears to allow reproduction only if certain conditions are met. This license does make clear that no patent rights are granted by this license.

CYBER SECURITY AND SOFTWARE ASSURANCE

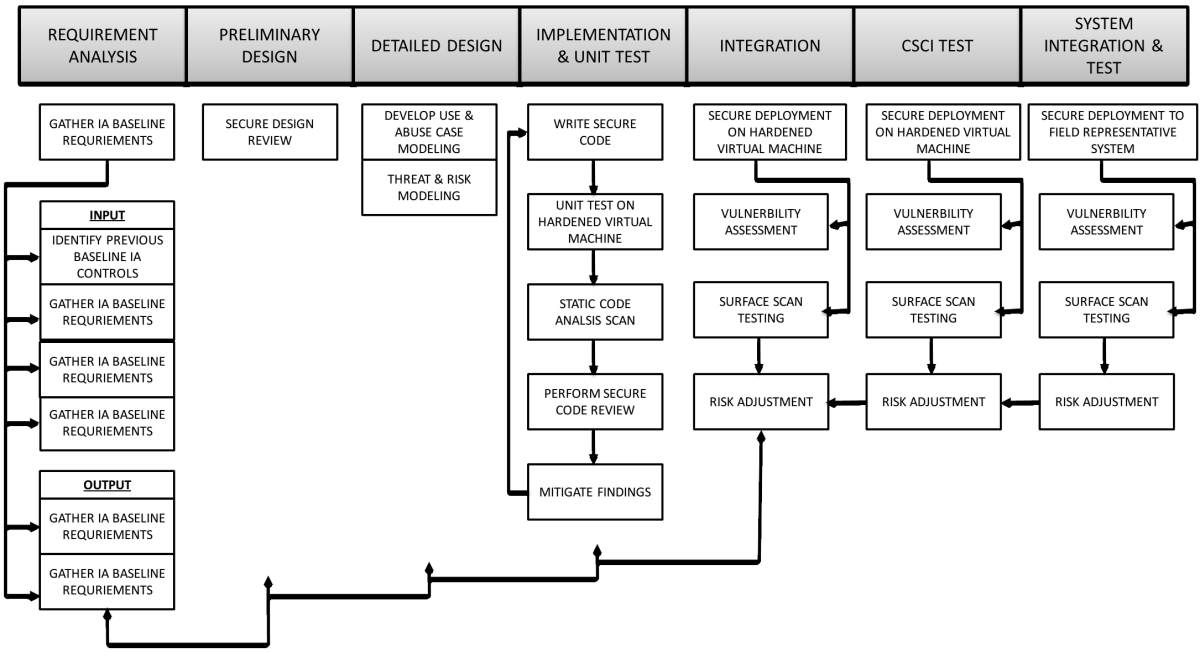
As malicious intent is an issue with OSS it is important to deploy software security in the development lifecycle to ensure proper security posture (McGraw, 2004). To do this effectively while minimizing the effort for developing controls, organizations can adopt government cyber security controls from the National Institute of Standards and Technology (NIST) Special Publications (SP) 900 Series to include the Department of Defense (DoD) (Dawson Jr, Crespo, & Brewster, 2013). On April 26, 2010, the DoD released the third version of the Application Security and Development Security Technical Implementation Guide (STIG) provided by the Defense Information Systems Agency (DISA). This STIG can be used as a baseline for software configuration and development. DISA provides STIGs for other system components that can allow for full system hardening that will provide the OSS additional security through defense in depth. This process allows for Availability, Integrity, and Confidentiality (AIC) of the entire system.

In the event of a vulnerability finding within the OSS, the software code may require redesign and implementation. This iterative cycle is costly in time and resources. To truly understand security threats to a system, security must be addressed beginning with the initiation phase of the development process. For an organization this means they must allow the Information Assurance (IA) controls and requirements to drive design and influence the software requirements. Therefore, any identified security threats found during the requirements and analysis phase will drive design requirements and implementation. Security defects discovered can then be addressed at a component level before implementation. The cost of discovery and mitigation can be absorbed within the review, analysis and quality check performed during the design, and implementation of our SDLC. The resultant product is one with security built in rather than security retrofitted. Figure 1 displays the Secure-SDLC (S-SDLC) process in which OSS can be implemented into the development process. For Agile or Scrum this process must be modified to be aligned with that specific design process.

CONCLUSION

As indicated in the *Jacobsen* case, there are some very valuable benefits to open source software,

Figure 1. Industry standard secure software development life cycle activities



in that it allows for collaboration in the development of new software and technology which can undoubtedly spur innovation and improve many processes and functions that individuals and businesses in our society rely on every day. Consequently one purpose of the law is to protect and preserve individual rights and the creativity of others while at the same time providing a benefit and contributing to society at large. How courts will interpret and protect and/or enforce open source licenses will depend greatly on how well the case can be made that this form of software and use can be beneficial and still comports with the overall interests that copyright law was intended to accomplish in the first place. As with any new development, the law will have to endeavor to ensure that it strikes a delicate balance between the good of the many and the good of the few or the individual. The use of OSS proves to be a positive and viable option with the addition of appropriate cyber security controls to mitigate risks of use in projects.

REFERENCES

Avison, D., & Fitzgerald, G. (2003). *Information systems development: methodologies, techniques and tools*. McGraw Hill.

Brightwell, R., Riesen, R., Underwood, K., Hudson, T. B., Bridges, P., & Maccabe, A. B. (2003, December). A performance comparison of Linux and a lightweight kernel. In *Proceedings of Cluster Computing,* (pp. 251-258). IEEE. doi:10.1109/CLUSTR.2003.1253322

Brooke, J. (1996). SUS-A quick and dirty usability scale. *Usability Evaluation in Industry*, *189*, 194.

Carrier, B. (2002). *Open source digital forensics tools: The legal argument*. Stake Research Report.

Cheeseman, H. (2013). *The Legal Environment of Business and Online Commerce*. Academic Press.

Cockburn, A. (2002). *Agile software development*. Boston: Addison-Wesley.

Cockburn, A., & Highsmith, J. (2001). Agile software development, the people factor. *Computer*, *34*(11), 131–133. doi:10.1109/2.963450

Computer Associates International v. Quest Software, Inc., et al. 333 F.Supp.2d 688, 698 (N.D.Ill. 2004).

Dawson, M Jr, E., Crespo, M., & Brewster, S. (. (2013). DoD cyber technology policies to secure automated information systems. *International Journal of Business Continuity and Risk Management*, *4*(1), 1–22. doi:10.1504/IJBCRM.2013.053089

Dawson, M., & Rahim, E. (2011). Transitional leadership in the defence and aerospace industry: A critical analysis for recruiting and developing talent. *International Journal of Project Organisation and Management*, *3*(2), 164–183. doi:10.1504/IJPOM.2011.039819

Dawson, M. E., & Al Saeed, I. (2012). Use of Open Source Software and Virtualization in Academia to Enhance Higher Education Everywhere. *Cutting-edge Technologies in Higher Education*, *6*, 283–313. doi:10.1108/S2044-9968(2012)000006C013

German, D. M., & González-Barahona, J. M. (2009). An empirical study of the reuse of software licensed under the GNU General Public License. In Open Source Ecosystems: Diverse Communities Interacting (pp. 185-198). Springer. doi:10.1007/978-3-642-02032-2_17

González, Á. L., Mariscal, G., Martínez, L., & Ruiz, C. (2007). Comparative analysis of the accessibility of desktop operating systems. In Universal Acess in Human Computer Interaction. Coping with Diversity (pp. 676-685). Springer. doi:10.1007/978-3-540-73279-2_75

Greenbaum, E. (2013). Lisping Copyleft: A Close Reading of the Lisp LGPL. *International Free and Open Source Software Law Review*, *5*(1), 15–30.

Jacobsen, v. Katzer, et al 535 F.3d 1373 (Fed. Cir. 2008)

Kumar, S. (2006). Enforcing the Gnu GPL. *U. Ill. JL Tech. & Pol'y*, 1.

Louridas, P. (2006). Static code analysis. *Software, IEEE*, *23*(4), 58–61. doi:10.1109/MS.2006.114

Mandrusiak, L. (2010). Balancing Open Source Paradigms And Traditional Intellectual Property Models to Optimize Innovation. *Maine Law Review*, *63*(1), 303.

McGraw, G. (1999). Software assurance for security. *Computer*, *32*(4), 103–105. doi:10.1109/2.755011

McGraw, G. (2004). Software security. *Security & Privacy, IEEE*, *2*(2), 80–83. doi:10.1109/MSECP.2004.1281254

Paul, M. (2011). *Official (ISC) 2 Guide to the CSSLP*. CRC Press. doi:10.1201/b10978

Perens, B. (1999). The open source definition. In *Open sources: Voices from the open source revolution*, (pp. 171-85). Academic Press.

Petersen, R. (2013). Social Networking: Microblogging, IM, VoIP, and Social Desktop. In Beginning Fedora Desktop (pp. 219-227). Apress.

Planetary Motion, Inc., v. Techplosion, Inc., Michael Gay A.K.A. Michael Carson 261 F.3d 1188, 1191 (11th Cir. 2001).

Proffitt, B. (2010). *Introducing Fedora: Desktop Linux*. Course Technology Press.

Progress Software Corporation, et al., v. Mysqlab, et al., 195 F.Supp.2d 328 (D.Mass. 2002)

Project Management Institute (PMI). (2009). *A Guide to the Project Management Body of Knowledge* (4th ed.). Philadelphia: PMBOK Guide.

Rahim, E., & Dawson, M. (2010). IT Project Management Best Practices In A Expanding Market. *Journal of Information Systems Technology and Planning*, *3*(5), 59–65.

Rising, L., & Janoff, N. S. (2000). The Scrum software development process for small teams. *IEEE Software*, *17*(4), 26–32. doi:10.1109/52.854065

Stallman, R. (1991). *GNU general public license.* Free Software Foundation, Inc. Retrieved from http://www.gnu.org/licenses/licenses.html#GPL

Stallman, R. M. (2013). *GNU free documentation license*. Academic Press.

Stein, M. (2006). Rethinking the UCITA: Lessons from the Open Source Movement. *Maine Law Review*, *58*(1), 157.

Wideman, R. M. (2001). *The Future of Project Management*. AEW Services. Retrieved February 23, 2014 from http://www.maxwideman.com/papers/future/future.htm

KEY TERMS AND DEFINITIONS

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Availability: Timely, reliable access to data and information services for authorized users.

Confidentiality: Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

GNU Public License: A widely used free software license that is managed under the GNU Not Linux Project (Stallman, 1991).

Integrity: Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Linux: An open source version of the UNIX OS (Perens, 2009).

Open Source Software: Software that allows the original source code to be free available which may be freely redistributed or modified (Perens, 2009).

Project Management: The discipline of planning, organizing, motivating, and controlling resources to achieve project success (PMI, 2009).

ENDNOTES

1 Article I, Section 8, U.S. Constitution.
2 333 F.Supp.2d 688, 698 (N.D.Ill. 2004).
3 See Id.
4 195 F.Supp.2d 328 (D.Mass. 2002).
5 261 F.3d 1188, 1191 (11th Cir. 2001).
6 535 F.3d 1373 (Fed. Cir. 2008).
7 535 F.3d 1373, 1382 (Fed. Cir. 2008).
8 See Id.
9 See Id.

Encyclopedia of Information Science and Technology, Third Edition

Mehdi Khosrow-Pour
Information Resources Management Association, USA

A volume in the

Information Science REFERENCE
An Imprint of IGI Global

Managing Director: Lindsay Johnston
Production Editor: Jennifer Yoder & Christina Henning
Development Editor: Austin DeMarco & Jan Travers
Acquisitions Editor: Kayla Wolfe
Typesetter: Mike Brehm, John Crodian, Lisandro Gonzalez, Deanna Zombro
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Encyclopedia of information science and technology / Mehdi Khosrow-Pour, editor.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4666-5888-2 (hardcover) -- ISBN 978-1-4666-5889-9 (ebook) -- ISBN 978-1-4666-5891-2 (print & perpetual access) 1. Information science--Encyclopedias. 2. Information technology--Encyclopedias. I. Khosrow-Pour, Mehdi, 1951-
Z1006.E566 2015
020.3--dc23

2014017131

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Understanding the Methods behind Cyber Terrorism

C

Maurice Dawson
University of Missouri-St. Louis, USA

Marwan Omar
Nawroz University, Iraq

Jonathan Abramson
Colorado Technical University, USA

INTRODUCTION

Cyber terrorism is on the rise and is constantly affecting millions every day. These malicious attacks can affect one single person to government entities. These attacks can be done with a few lines of code or large complex programs that have the ability to target specific hardware. The authors investigate the attacks on individuals, corporations, and government infrastructures throughout the world. Provided will be specific examples of what a cyber terrorist attack is and why this method of attack is the preferred method of engagement today. The authors will also identify software applications which track system weaknesses and vulnerabilities. As the United States (U.S.) government has stated an act of cyber terrorism is an act of war it is imperative that we explore this new method of terrorism and how it can be mitigated to an acceptable risk.

BACKGROUND

Cyber security has become a matter of national, international, economic, and societal importance that affects multiple nations (Walker, 2012). Since the 1990s users have exploited vulnerabilities to gain access to networks for malicious purposes. In recent years the number of attacks on U.S. networks has continued to grow at an exponential rate. This includes malicious embedded code, exploitation of backdoors, and more. These attacks can be initiated from anywhere in the world from behind a computer with a masked Internet Protocol (IP) address. This type of warfare, cyber warfare, changes the landscape of war itself (Beidleman, 2009). This type of warfare removes the need to have a physically capable military and requires the demand for a force that has a strong technical capacity e.g. computer science skills. The U.S. and other countries have come to understand that this is an issue and has developed policies to handle this in an effort to mitigate the threats.

In Estonia and Georgia there were direct attacks on government cyber infrastructure (Beildleman, 2009). The attacks in Estonia rendered the government's infrastructure useless. The government and other associated entities heavily relied upon this e-government infrastructure. These attacks help lead to the development of cyber defense organizations within Europe.

Laws and Policies to Combat Terrorism

The events of 9/11 not only changed policies with the United States (U.S.) but also policies with other countries in how they treat and combat terrorism. The United Nations (U.N.) altered Article 51 of the U.N. charter. This article allows members of the U.N. to take necessary measures to protect themselves against an armed attack to ensure international peace and security.

Israel is a country with some of the most stringent policies towards national and international security. This country requires all citizens to serve in the military to include multiple checkpoints throughout the country. This country has utilized stringent checks in the airport long before 9/11 however now they have additional measures to ensure security as they are surrounded by countries that have tried to invade before. Israel has

DOI: 10.4018/978-1-4666-5888-2.ch147

also deployed more Unmanned Air Vehicles (UAVs), and Unmanned Ground Vehicles (UGVs) to patrol the border in the event something occurs.

The United Kingdom (U.K.) has the Prevention of Terrorism Act 2005 and the Counter-Terrorism Act 2008 which was issued by Parliament. The first act was created to detain individuals who were suspected in acts of terrorism. This act was intended to replace the Anti-terrorism, Crime and Security Act 2001 as it was deemed unlawful. These acts seem to mirror the same ones created in the U.S. to monitor potential terrorists and terrorists. The U.K. also shared their information with the U.S. for coordinating individual that may be of risk.

In the U.S. the methods for national security were enhanced to ensure no threats occur on U.S. soil. These changes include enhanced security in all ports of entry. The signing of the Homeland Security Act of 2002 (HS Act) (Public Law 107-296) created an organization that received funding and lots of resources for monitoring the security posture of this country. Additional changes include enhanced monitoring of citizens and residents within the country to prevent terrorist activities by the mention of key words e.g. bomb, explosive, or Al Qaeda.

The USA PATRIOT was signed into law by President George W. Bush in 2001 after September 11, 2001 (Bullock, Haddow, Coppola, & Yeletaysi, 2009). This act was created in response to the event of 9/11 which provided government agencies increased abilities. These increased abilities provided the government rights to search various communications such as email, telephone records, medical records, and more of those who were thoughts of terrorist acts (Bullock, Haddow, Coppola, & Yeletaysi, 2009). This allowed law enforcement to have the upper hand in being proactive to stopping potential acts against U.S. soil. In 2011 President Obama signed an extension on the USA PATRIOT Act. This act has received criticism from the public due to the potential to be misused or abused by those in power. This act has allowed government agencies to impede on constitutional rights.

The Protecting Cyberspace as a National Asset Act of 2010 was an act that also amends Title II of the Homeland Security Act of 2002. This act enhanced the security and resiliency of the cyber and communication infrastructure within the U.S. This act is important as the President declared that any cyber aggressions would be considered an act of war. This is also important as Estonia's entire digital infrastructure was taken down by hackers who supported the former Soviet rule. This type of attack could be damaging to the infrastructure in the U.S. causing loss of power for days or more which could result in death. In an area such as the Huntsville Metro we could have multiple nuclear facility melt downs, loss of ISR capabilities, and communication to the war fighter that we are supporting.

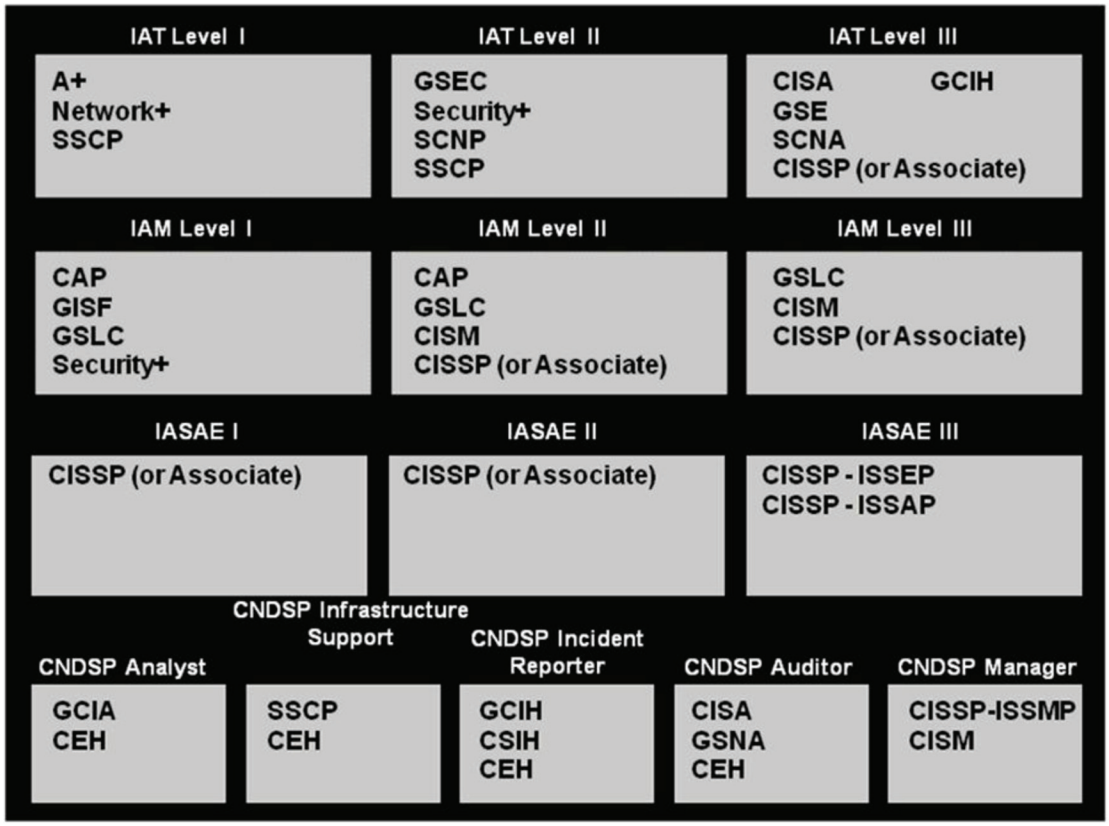
Additional changes from this act include the ability to carry out a research and development program to improve cyber security infrastructure. At the moment all government organizations must comply with the Federal Information Security Management Act (FISMA) of 2002. This act has shown many holes within the U.S. cyber security infrastructure to include those organizations that are leads. This act provides DHS the ability to carry out the duties described in the Protecting Cyberspace as a National Asset Act of 2010.

The most significant policy created to ensure that technically competent individuals are working on national infrastructure is the Information Assurance Workforce Improvement Program, Department of Defense (DoD) 8570.01-Mandate (M) (Directive, 2005). This mandate provides guidance for the identification and categorization of Information Assurance (IA) positions and associated certifications (Directive, 2010). However this mandate only provides the baseline certifications required to perform specialized IA functions. The certification categories are broken down in the following; Information Assurance Technical (IAT), Information Assurance Manager (IAM), Information Assurance System Architect and Engineer (IASAE), and Computer Network Defense (CND). Figure 1 displays all the specific certifications that can be used as of the updates to the DoD8570.01-M.

Stuxnet Worm

During the fall of 2010 many headlines declared that Stuxnet was the game changes in terms of cyber warfare (Denning, 2012). This malicious worm was complex and designed to target only a specific system. This worm had the ability to detect location, system type, and more. And this worm only attacked the system if it met specific parameters that were designed in the code. Stuxnet tampered directly with software in a programmable logic controller (PLC) that controlled the centrifuges at Natanz. This tampering ultimately caused a disruption in the Iranian nuclear program.

Figure 1. DoD 8570 certification chart



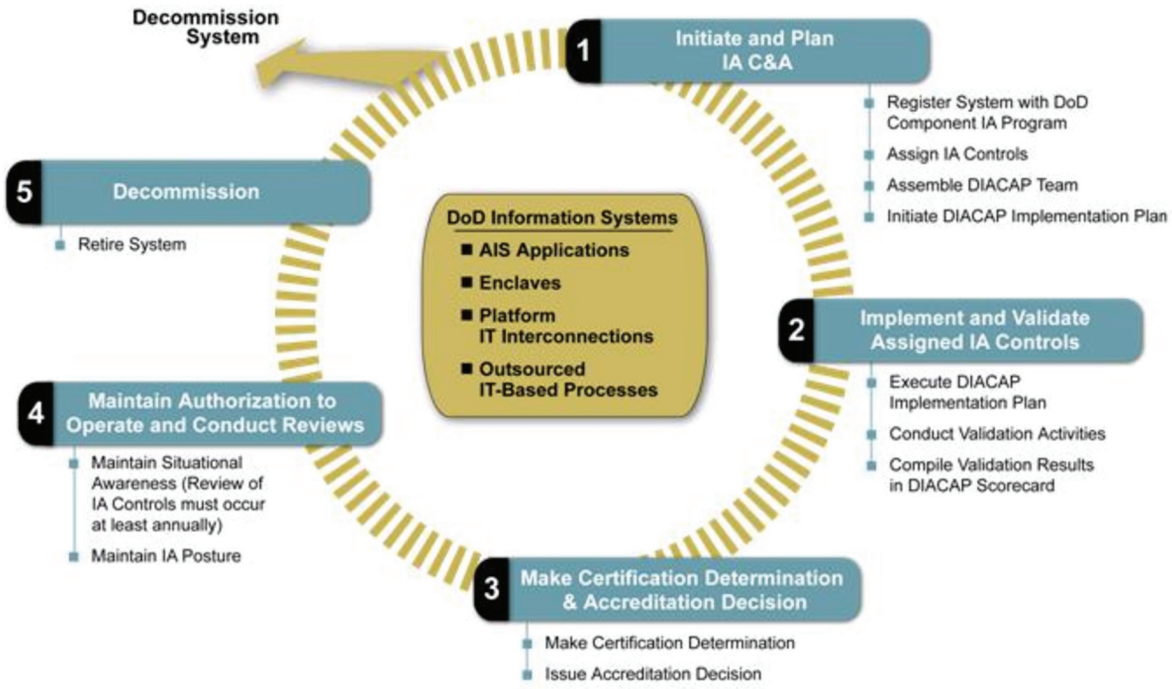
America's Homeland Security Preparing for Cyber Warfare

The Department of Homeland Security (DHS) is concerned with cyber attacks on infrastructure such as supervisory control and data acquisition (SCADA) systems. SCADA systems are the systems that autonomously monitor and adjust switching among other processes within critical infrastructures such as nuclear plants, and power grids. DHS is worried about these systems as they are unmanned frequently and remotely accessed. As they are remotely accessed this could allow anyone to take control of assets to critical infrastructure remotely. There has been increasing mandates and directives to ensure any system deployed meets stringent requirements. As the Stuxnet worm has become a reality future attacks could be malicious code directly targeting specific locations of critical infrastructure.

Cyber Security Certification and Accreditation Processes

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is the process that the DoD utilizes to ensure that risk management is applied to Automated Information Systems (AIS) to mitigate IA risks and vulnerabilities. DIACAP is the standard process that all services utilize to ensure that all DoD systems maintain IA posture throughout the systems life cycle. DIACAP is the replacement of the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). Figure 2 displays the process which includes five key steps. The first step is to initiate and plan the IA C&A process. The second step is to implement and validate the assigned IA controls. The third step is to make the certification determination and

Figure 2. DIACAP stages (Source Department of Defense (November 2007)



accreditation decision. The fourth step is to maintain authorization to operate and conduct reviews. The final step is to decommission the system.

The Common Criteria (CC), an internationally approved set of security standards, provides a clear and reliable evaluation of the security capabilities of Information Technology (IT) products (CCEVS, 2008). By providing an independent assessment of a product's ability to meet security standards, the CC gives customers more confidence in the security of products and leads to more informed decisions (CCEVS, 2008). Security-conscious customers, such as the U.S. Federal Government, are increasingly requiring CC certification as a determining factor in purchasing decisions (CCEVS, 2008). Since the requirements for certification are clearly established, vendors can target very specific security needs while providing broad product offerings. The international scope of the CC, currently adopted by fourteen nations, allows users from other countries to purchase IT products with the same level of confidence, since certification is recognized across all complying nations. Evaluating a product with respect to security requires identification of the customer's security needs and an assessment of the capabilities of the product. The CC aids customers in both of these processes through two key components: protection profiles and evaluation assurance levels (CCEVS, 2008).

The CC is the process that replaced the Orange Book. The CC has Evaluated Assurance Levels (EAL) 1 through 7. EAL products 1 through 4 may be used and certified in any of the participating countries. But EAL 5 through 7 must be certified by the countries national security agency i.e. United States' national agency is the National Security Agency and United Kingdom's national agency is the Communication Electronics Security Group (CESG). By all accounts, the NSA's Orange Book program, in which the National Security Agency (NSA) forced vendors through prolonged product testing at Ft. Meade, MD., was a dismal failure. And the government's failure to buy Orange-Book-tested products, which were often out of date after years of testing, was a blow to vendors that invested huge sums in the Orange Book Evaluations.

Additionally the NSA and DHS sponsors a joint venture known as the National Centers of Academic Excellence in IA Education (CAE/IAE), IA 2-year Education and Training (CAE/2Y) and IA Research (CAE/R) programs. Students that attend institutions with these designations are eligible to apply for schol-

arships and grants which they repay through government service. These programs were created to address the lack of available talent in IA. Table 1 shows the Committee on National Security Standards (CNSS) that institutions must map to in order to receive the designation as a NSA/IAE.

As the purpose was to expand the numbers of IA personnel it is hard to evaluate the program's real success (Bishop & Taylor, 2009). One of the major problems is the lack of resources to all institutions who are NSA/IAE. Even though this program is targeted towards post high school efforts more reforms are currently taking place in the K-12 educational areas.

Tools and Methods for Monitoring Networks

Snort is open source software developed by Sourcefire and used for intrusion detection and prevention (Snort.org, 2012). Snort is one of the most widely adopted network monitoring technologies that can be used by network administrators as a defensive technique to report suspicious network traffic activity and alert system administrators about potential cyber attacks. Snort has gained considerable popularity and attention among other network monitoring tools because its combines the benefits of signature based tools and anomaly detection techniques (Roesch, 1999). Another reason behind Snort popularity and success is that Snort is capable of performing real time traffic analysis and packet logging on IP networks (Tuteja & Shanker, 2012).

Table 1. CNSS training standards

Standard Name	Year	Description
NSTISSI 4011	1994	Information Systems Security Professionals
CNSSI 4012	2004	Senior Systems Manager
CNSIS 4013	2004	System Administrators in Information Systems Security
CNSSI 4014	2004	Information Systems Security Officers (ISSO)
NSTISSI 4015	2000	System Certifiers
CNSSI 4016	2005	Risk Analysis

Network Mapper (Nmap) is a free open source utility for discovering networks and performing security auditing (Sadasivam, Samudrala, & Yang, 2005). Nmapis a valuable and widely used network scanner that has the ability to rapidly scan and discover hosts and services by sending specially designed packets to the target host, analyzes and respond. Nmap is different than other port scanner software applications in that it does not just send packets at some predefined constant rate, instead, Nmap takes into account network conditions such as latency fluctuations, network congestion, and the target interference with the scan during the run time. Nmap has some advanced network discovery capabilities that go beyond basic port scanning and host scanning; Nmap can identify the type and version of operating system (OS), what type of firewalls are being used on the network, and what listening services are running on the hosts. Nmap runs on major OS such as Microsoft windows, Linux, and Solaris. Nmap has become one of the most useful network scanning tools that network administrators cannot afford to ignore especially because this tool has proven to be flexible, intuitive interface, deployable, cross platform and most importantly it is free.

Tools and Methods for Network Attacks

A port scan attack one of the most popular reconnaissance techniques used by hackers to break into vulnerable services and applications. Most of the network services need to use TCP or UPD ports for their connections, a port scan allows hackers to listen to open and available ports by sending a message to each port at a time and wait for a response to be received. Once the port replies to a message, a hacker would then dig further and attempt to find flaws or weaknesses in that port and ultimately launch a port scan attack. Combating a port scan attack requires deploying Firewalls at critical locations of a network to filter suspicious or unsolicited traffic. Also, security gateways must be able to raise alerts, and block or shutdown communications from the source of the scan.

A SYN attack which is also known as SYN Flooding that targets the TCP/IP stack. It exploits a weakness in the way that most hosts implement the TCP three-way handshake. When Host Y receives the SYN request from X, it maintains the opened connection in a "listen

queue" for at least 75 seconds (Reed, 2003). Many implementations can only keep track of a very limited number of connections. A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host thus making the system crash or become unavailable to other legitimate connections. This ability of removing a host from the network for at least 75 seconds can be used as a denial-of-service attack, or it can be used as a tool to implement other attacks, like IP Spoofing (Rouiller, 2006). Mitigating this attack requires the implementation of several solutions such as network address translation (NAT), access control lists (ACL), and routers.

Another attack which is known as IP address spoofing or IP spoofing refers to the creation of IP packets with a forged source IP address, called spoofing, with the purpose of hiding the true identity of the packet (sender) or impersonating another host on the network. IP address spoofing is a form of denial of service attacks where attackers attempt to flood the network with overwhelming amounts of traffic without being concerned about receiving responses to attack packets. Implementing packet filters at the router using ingress and egress (blocking illegitimate packets from inside and outside the network) is the best defense against the IP spoofing attack.

There is one widely available tool that allows one to successfully conduct an analysis on the vulnerabilities detailed at the application layer multiple tools. This tool suite is an.iso image known as Back Track Linux. Backtrack Linux is utilized for digital forensics and penetration testing. This tool provides individuals with the ability to perform a comprehensive attack (Haines & Thorton, 2008). There are approximately eleven categories which are broken down into: 1) information gathering, 2) network mapping, 3) vulnerability identification, 4) web application analysis, 5) radio network analysis (802.11, Bluetooth, Radio Frequency Identification (RFID)), 6) penetration (exploit & social engineering toolkit), 7) privilege escalation, 8) maintaining access, 9) digital forensics,10) reverse engineering, and 11) Voice over Internet Protocol (VoIP). All of these items provide a true in depth analysis of the mobile device.With advanced tools such as Backtrack Linux cyber terrorists have a capability like never before as this tool does not require expert knowledge to command it. Since VM's can support their own OS and applications tools such as Oracle Virtual Box become sandbox environments for hackers (Dawson & Al Saeed, 2012).

Issues with Android Phones and Other Mobile Devices

Smartphones are becoming a more integrated and prevalent part of people's daily lives due to their highly powerful computational capabilities, such as email applications, online banking, online shopping, and bill paying (Omar & Dawson, 2013). With this fast adoption of smartphones, imminent security threats arise while communicating sensitive personally identifiable information (PII), such as bank account numbers and credit card numbers used when handling and performing those advanced tasks (Wong, 2005; Brown 2009). Traditional attacks (worms, viruses, and Trojan horses) caused privacy violations and disruptions of critical software applications (e.g., deleting lists of contact numbers and personal data). Malware attacks on smartphones were generally "proof of concept" attempts to break through the phone's system and cause damage. However, the new generation of smartphone malware attacks has increased in sophistication and is designed to cause severe financial losses (caused by identity theft) and disruption of critical software applications (Bose, 2008). Because smartphones are becoming more diverse in providing general purpose services (i.e., instant messaging and music), the effect of malware could be extended to include draining batteries, incurring additional charges, and bringing down network capabilities and services (Xie, Zhang, Chaugule, Jaeger, & Zhu, 2009).

Smartphones are rapidly becoming enriched with confidential and sensitive personal information, such as bank account information and credit card numbers, because of the functionality and powerful computational capabilities built into those mobile devices. Cyber criminals, in turn, launch attacks especially designed to target smartphones, exploiting vulnerabilities and deficiencies in current defense strategies built into smartphones' OS. Bhattacharya (2008) indicated that because of skill and resource constraints, businesses are ill-prepared to combat emerging cyber threats; this claim is true for smartphones as well, given the fact that those mobile devices are even less equipped with necessary protections, such as antivirus and malware protection software. Some services and features, such as Bluetooth and SMS, create attack vectors unique to smartphones and thus expand the attack surface. For example, in December, 2004, A Trojan horse was disguised in a video game and was intended to be a

"proof of concept," which signaled the risks associated with smartphones that could potentially compromise the integrity and confidentiality of personal information contained in smartphones (Rash, 2004). Attackers can easily take advantage of those services provided by smartphones and subvert their primary purpose because they can use Bluetooth and SMS services to launch attacks by installing software that can disable virus protection and spread via Bluetooth unbeknownst to smartphone users (Omar & Dawson, 2013).

With the development of innovative features and services for smartphones, security measures deployed are currently not commensurate because those services and features, such as MMS and Bluetooth, are driven by market and user demands, meaning that companies are more inclined to provide more entertainment features than security solutions. In turn, this further increases vulnerabilities and opens doors for hackers to deploy attacks on smartphones. Furthermore, Mulliner & Miller (2009) argue that the OS of smartphones allow the installation of third-party software applications, coupled with the increase in processing power as well as the storage capacity. Scenarios like this pose worse security challenges because hackers could exploit those vulnerabilities, which are further compounded by users' lack of security awareness. Smartphone attackers are becoming more adept in designing and launching attacks by applying attack techniques already implemented on desktop and laptop computers; smartphones' enhanced features, such as music players and video games, produce easy-to exploit targets by sending seemingly benign files via music or video game applications to users and luring them into downloading such files. Becher, Freiling, and Leider (2007) indicated that attackers could exploit such vulnerabilities to spread worms autonomously into smartphones. Therefore, hackers usually use a combination of technical expertise along with some social engineering techniques to trap users into accepting and downloading benign applications, which are used later to execute malicious code and affect critical applications running on smartphones.

Android's core components, such as Linux and connectivity media, are vulnerable to attacks through which personal and confidential information is likely to be compromised. Android's threats are further amplified by the fact that users are limited to using their smartphones for basic services and functions, such as email and SMS/MMS. Users lack the programming mind-set to protect their Android smartphones and stay current with the latest security software updates. This gives hackers an edge to target Android smartphones in the hope of gaining unauthorized access to disable core services (email and web browsing); abuse costly services (i.e., sending MMS/SMS and making calls to high-rate numbers); eavesdrop on calls and most importantly compromise sensitive information to be sold for a price. Android's open-source nature further increases security vulnerabilities because attackers can easily exploit this feature to modify the core applications and install malicious software, which could be used to compromise Android-based smartphones and ultimately cause disruption and monetary loss.

Mixed Reality Dangers

Cyber-attacks happen on all types of organizations and individuals. They can start in many different places, including any device that's connected to the Internet. This becomes highly problematic in our modern society when we have devices such as copy machines that are hooked up to the Internet in order to update themselves report usage, install software, etc. Having all these devices connected to the Internet increases our exposure and vulnerability. With so many targets we need to create an orderly way to look for threats.

As the threats have increased through the years, we become more vulnerable to these threats. An interesting point about the intrusion detection systems (IDS) is that they are part hardware and part software. Therefore when we implement one of these solutions we need to make sure that we are up to date with the hardware and software maintenance so that we get the updates that will keep the organization safe.

There are many research papers and projects that have demonstrated the usefulness of virtual and mixed reality environments in many different fields. It is important that the cyber warrior believes that they are in a different environment. Believability has been a requirement for successful implementations of Mixed Reality (MR) and Virtual Reality (VR). Human Computer Interaction (HCI) is key to making the cyber warriors feel that they are immersed in cyberspace. Since cyberspace cannot be seen by the naked eye, we need to gather the data and information that is necessary and make the user be able to see it in a virtual and productive environment. The potential of ubiquitous,

mobile and mixed reality technologies to deter Internet threats is enhanced by these characteristics, as we now have the ability to have individuals who are in geographically separate areas, work together as one to solve new threats and problems. Mixed reality may be able to bridge the gap of recognition of security threats.

Incorporation of mixed reality should only require the changing of the inputs to the user or cyber warrior from game to actual data and information and the integration and implementation of a head mounted device (HMD) and quite possibly new input devices including brain to game interfacing. The process of creating a visual environment in which users can be active participants with real data with the purpose of solving problems and deterring threats, opens the process up to gamification. This permits the analysis of threats and also using the threat log and data for training as well, including one excited in a game based scenario.

FUTURE RESEARCH DIRECTIONS

With the continual rise of virtual words environments such as OpenSimulator (OpenSim) and Second Life (SL) have the ability to be used for positive or negative gains in military warfare in the areas of training (Dawson, 2011). For example, a terrorist could create a virtual representation of a building by using publicly available drafting plans. This virtual representation would serve as scenario based training for terrorists. Additionally this would allow for terrorists of different cells or groups to communicate freely. Policing the virtual worlds may become a necessity to maintain national security (Parti, 2010). The U.S. Army is currently implementing a program known as Military Open Simulator Enterprise Strategy (MOSES). MOSES runs on OpenSim and is moving towards a Common Access Card (CAC) enabled environment for secure and

Figure 3. MOSES interrogation scenario

encrypted communications (Maxwell & McLennan, 2012). In Figure 3 displayed is an interrogation scenario in MOSES. Additionally the U.S. could follow a model similar to Estonia where kids from the age of seven to nineteen learn how to develop software programs. This would help in deterring threats to include having future developers build security into the software from the beginning.

CONCLUSION

Cyber terrorism is real threat and countries should develop a culture of cyber defense. This defense should not only be one that deters threats but one that has offensive capability as well. It is essential that countries implement a plan that includes developing more talent in Science, Technology, Engineering, & Mathematics (STEM) fields. In this article, we have examined existing threats to include policies as well as critically exam their strengths and shortcomings.

REFERENCES

Beidleman, S. W. (2009). *Defining and Deterring Cyber War*. Carlisle Barracks, PA: ArmyWar College.

Bhattacharya, D. (2008) *Leadership styles and information security in small businesses: An empirical investigation*. Doctoral dissertation, University of Phoenix. Retrieved from www.phoenix.edu/apololibrary

Bishop, M., & Taylor, C. (2009).A Critical Analysis of the Centers of Academic Excellence Program. In *Proceedings of the 13th Colloquium for Information Systems Security Education* (pp. 1-3).Seattle, WA.

Bose, A. (2008). *Propagation, detection and containment of mobile malware*. Doctoral dissertation, University of Michigan. Retrieved from www.phoenix.edu/apololibrary

Brown, B. (2009). *Beyond Downadup: Security expert worries about smart phone, TinyURL threats: Malware writers just waiting for financial incentive to strike, F-Secure exec warns* Retrieved from http://business.highbeam.com/409220/article-1G1-214585913/beyond-downadup-security-expert-worries-smart-phone

Bullock, J., Haddow, G., Coppola, D., & Yeletaysi, S. (2009). *Introduction to homeland security: Principles of all-hazards response* (3rd ed.). Burlington, MA: Elsevier Inc.

Dawson, M. (2011). Applicability of Web 2.0: Training for Tactical Military Applications. *Global TIME*, (1), 395-398.

Dawson, M. E., & Al Saeed, I. (2012). Use of Open Source Software and Virtualization in Academia to Enhance Higher Education Everywhere. *Cutting-edge Technologies in Higher Education*, *6*, 283–313. doi:10.1108/S2044-9968(2012)000006C013

Denning, D. E. (2012). Stuxnet: What Has Changed? *Future Internet*, *4*(3), 672–687. doi:10.3390/fi4030672

Department of Defense Assistant Secretary of Defense for Networks and Information Integration, & Department of Defense Chief Information Officer. (2007). DoD information assurance certification and accreditation process (diacap). DoDI 8510.01. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf

Directive, D. (2005, December 19). 8570. 01, Information Assurance Training. *Certification, and Workforce Management*.

Directive, D. (2010, August 20).8570. 01, Information Assurance Training. *Certification, and Workforce Management*.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, *45*(1), 67–87. doi:10.2307/41166154

Haddow, G., Bullock, J., & Coppola, D. P. (2010). *Introduction to emergency management*. Butterworth-Heinemann.

Haines, B., & Thornton, F. (2008). *Kismet Hacking*. Syngress Publishing.

Harris, S., & Meyers, M. (2002). *CISSP*. McGraw-Hill/Osborne.

In *Proceedings of the3rd USENIX Workshop on Offensive Technologies.* Montreal, Canada. Retrieved from www.usenix.org

Janczewski, L., & Colarik, A. (2007). *Cyber Warfare and Cyber Terrorism*. Hershey, PA: IGI Global. doi:10.4018/978-1-59140-991-5

Maxwell, D., & McLennan, K. (2012, June). Case Study: Leveraging Government and Academic Partnerships in MOSES (Military Open Simulator [Virtual World] Enterprise Strategy). In *Proceedings of the World Conference on Educational Multimedia, Hypermedia and Telecommunications* (pp. 1604-1616).

Mulliner, C., & Miller, C. (2009). Injecting SMS messages into smartphones for security analysis.

National Security Agency, Common Criteria Evaluation and Validation Scheme (CCEVS). (2008).Common criteria evaluation and validation scheme -- organization, management, and concept of operations (Version 2.0). Retrieved from http://www.niap-ccevs.org/policy/ccevs/scheme-pub-1.pdf

Omar, M., & Dawson, M. (2013, April). Research in progress - defending android smartphones from malware attacks. In *Proceedings of the 2013 third international conference on advanced computing and communication technologies (ACCT).* Rohtak, India. doi: 10.1109/ACCT.2013.69.

Parti, K. (2010). Actual Policing in Virtual Reality - A Cause of Moral Panic or a Justified Need? In J.-J. Kim (Ed.), *Virtual Reality.* In Tech. ISBN: 978-953-307-518-1. Retrieved from http://www.intechopen.com/books/virtual-reality/actual-policing-in-virtual-reality-a-cause-of-moral-panic-or-a-justified-need-

Rash, W. (2004). Latest skulls Trojan foretells risky smartphone future. Retrieved from www.eweek.com

Roesch, M. (1999, November).Snort-lightweight intrusion detection for networks.In *Proceedings of the 13th USENIXconference on System administration* (pp. 229-238).

Rouiller, S. A. (2006). Virtual LAN Security: weaknesses and countermeasures. Retrieved from askapache.com/2006/12/vlan-security-3.pdf.

Snort. (2012). what is snort. Retrieved October 14, 2012, from www.snort.org

Tuteja, A., & Shanker, R. (2012). Optimization of Snort for Extrusion and Intrusion Detection and Prevention. *Optimization*, *2*(3), 1768–1774.

Walker, J. J. (2012). Cyber Security Concerns for Emergency Management. In B. Eksioglu (Ed.), *Emergency Management.* In Tech. ISBN: 978-953-307-989-9. Retrieved from http://www.intechopen.com/books/emergency-management/cyber-security-concerns-for-emergency-management

Wong, L. (2005). Potential Bluetooth vulnerabilities in smartphones. Retrieved from http://citeseerx.ist.psu.edu

Xie, L., Zhang, X., Chaugule, A., Jaeger, T., & Zhu, S. (2009). *Designing system-level defenses against cellphone malware*. Retrieved from www.cse.psu.edu

ADDITIONAL READING

Anderson, R., & Fuloria, S. (2010). Security economics and critical national infrastructure. In Economics of Information Security and Privacy (pp. 55-66). Springer US.

Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. *In Proceedings of the VDE Kongress* (Vol. 116).

Ericsson, G. N. (2010). Cyber security and power system communication - essential parts of a smart grid infrastructure. *Power Delivery. IEEE Transactions on*, *25*(3), 1501–1507.

Lynn, W. F. III. (2010). Defending a New Domain-The Pentagon's Cyberstrategy. *Foreign Affairs*, *89*, 97.

Prichard, J. J., & MacDonald, L. E. (2004). Cyber terrorism: A study of the extent of coverage in computer security textbooks. *Journal of Information Technology Education*, *3*, 279–289.

Ralston, P. A. S., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions*, *46*(4), 583–594. doi:10.1016/j.isatra.2007.04.003 PMID:17624350

KEY TERMS AND DEFINITIONS

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (Harris, 2002).

Availability: Timely, reliable access to data and information services for authorized users (Harris, 2002).

Confidentiality: Assurance that information is not disclosed to unauthorized individuals, processes, or devices (Harris, 2002).

Cyber Terrorism: Attacks with the use of the Internet for terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses, worms, Trojans, and zombies (Janczewski & Colarik, 2008).

Integrity: Quality of an IS reflecting the logical correctness and reliability of the OS; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (Harris, 2002).

Non-Repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (Harris, 2002).

Information Security in Diverse Computing Environments

Anne Kayem
Department of Computer Science, University of Cape Town, South Africa

Christoph Meinel
Hasso-Plattner-Institute for IT Systems Engineering, University of Potsdam, Potsdam, Germany

A volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

Information Science REFERENCE
An Imprint of IGI Global

Managing Director: Lindsay Johnston
Production Editor: Jennifer Yoder
Development Editor: Erin O'Dea
Acquisitions Editor: Kayla Wolfe
Typesetter: Thomas Creedon
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Information security in diverse computing environments / Anne Kayem and Christoph Meinel, editors.
pages cm
Includes bibliographical references and index.
Summary: "This book provides the latest empirical research and theoretical frameworks in the area of information security, presenting research on developing sufficient security measures for new environments by discussing challenges faced by researchers as well as unconventional solutions to these problems"-- Provided by publisher.
ISBN 978-1-4666-6158-5 (hardcover) -- ISBN 978-1-4666-6159-2 (ebook) -- ISBN 978-1-4666-6161-5 (print & perpetual access) 1. Computer security. 2. Data protection. 3. Information technology--Security measures. I. Kayem, Anne, 1975- II. Meinel, Christoph, 1954-
QA76.9.A25.I54154 2014
005.8--dc23

2014013850

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 9
The Future of National and International Security on the Internet

Maurice Dawson
University of Missouri – St. Louis, USA

Jonathan Abramson
Colorado Technical University, USA

Marwan Omar
Nawroz University, Iraq

Dustin Bessette
National Graduate School of Quality Management, USA

ABSTRACT

Hyperconnectivity is a growing trend that is driving cyber security experts to develop new security architectures for multiple platforms such as mobile devices, laptops, and even wearable displays. The futures of national and international security rely on complex countermeasures to ensure that a proper security posture is maintained during this state of hyperconnectivity. To protect these systems from exploitation of vulnerabilities it is essential to understand current and future threats to include the laws that drive their need to be secured. Examined within this chapter are the potential security-related threats with the use of social media, mobile devices, virtual worlds, augmented reality, and mixed reality. Further reviewed are some examples of the complex attacks that could interrupt human-robot interaction, children-computer interaction, mobile computing, social networks, and human-centered issues in security design.

CYBER SECURITY

Cyber terrorism is on the rise and is constantly affecting millions every day. These malicious attacks can affect one single person to entire government entities. These attacks can be done with a few lines of code or large complex programs that have the ability to target specific hardware. The authors investigate the attacks on individuals, corporations, and government infrastructures throughout the world. Provided will be specific examples of what a cyber terrorist attack is and why this method of attack is the preferred method of engagement today. The authors will also identify software applications, which track system weaknesses and vulnerabilities. As the United States (U.S.) government has stated, an act of cyber terrorism is an act of war; it is imperative that we explore this new method of terrorism and how it can be mitigated to an acceptable risk.

DOI: 10.4018/978-1-4666-6158-5.ch009

Information assurance (IA) is defined as the practice of protecting and defending information and information systems by ensuring their availability, integrity, authentication, confidentiality and non repudiation. This definition also encompasses disaster recovery, physical security, cryptography, application security, and business continuity of operations. To survive and be successful, an enterprise must have a disaster recovery strategy and response plan in place to mitigate the effects of natural disasters (e.g., floods, fires, tornadoes, earthquake, etc.), inadvertent actions by trusted insiders, terrorist attacks, vandalism, and criminal activity. In order to lay the groundwork for this review properly, it is essential to detail current processes techniques being utilized by officials within the government to accredit and certify systems to include their IA enabled products (Dawson, Jr., Crespo, & Brewster, 2013).

BACKGROUND

Cyber security has become a matter of national, international, economic, and societal importance that affects multiple nations (Walker, 2012). Since the 1990s users have exploited vulnerabilities to gain access to networks for malicious purposes. In recent years, the number of attacks on United States networks has continued to grow at an exponential rate. This includes malicious embedded code, exploitation of backdoors, and more. These attacks can be initiated from anywhere in the world from behind a computer with a masked Internet Protocol (IP) address. This type of warfare, cyber warfare, changes the landscape of war itself (Beidleman, 2009). This type of warfare removes the need to have a physically capable military and requires the demand for a force that has a strong technical capacity e.g. computer science skills. The U.S. and other countries have come to understand that this is an issue and has developed policies to handle this in an effort to mitigate the threats.

In Estonia and Georgia there were direct attacks on government cyber infrastructure (Beidleman, 2009). The attacks in Estonia rendered the government's infrastructure useless. The government and other associated entities heavily relied upon this e-government infrastructure. These attacks help lead to the development of cyber defense organizations that drive laws and policies within Europe.

LAWS AND POLICIES TO COMBAT TERRORISM

The events of 9/ll not only changed policies with the U.S. but also policies with other countries in how they treat and combat terrorism. The United Nations (U.N.) altered Article 51 of the U.N. charter. This article allows members of the U.N. to take necessary measures to protect themselves against an armed attack to ensure international peace and security.

Israel is a country with some of the most stringent policies towards national and international security. This country requires all citizens to serve in the military to include multiple checkpoints throughout the country. This country has utilized stringent checks in the airport long before 9/11, however, now they have additional measures to ensure the nation's security as they are surrounded by countries that have tried to invade before. Israel has also deployed more Unmanned Air Vehicles (UAVs), and Unmanned Ground Vehicles (UGVs) to patrol the border in the event something occurs.

The United Kingdom (U.K.) has the Prevention of Terrorism Act 2005 and the Counter-Terrorism Act 2008 which was issued by Parliament. The first act was created to detain individuals who were suspected in acts of terrorism. This act was intended to replace the Anti-terrorism, Crime and Security Act 200 I as it was deemed unlawful. These acts seem to mirror the same ones, created in the U.S., to monitor potential terrorists and terrorists. The U.K. also shared their information with the U.S. for coordinating individual that may be of risk.

In the U.S., the methods for national security were enhanced to ensure no threats occur on U.S. soil. These changes include enhanced security in all ports of entry. The signing of the Homeland Security Act of 2002 (HS Act) (Public Law 07-296) created an organization that received funding and lots of resources for monitoring the security posture of this country. Additional changes include enhanced monitoring of citizens and residents within the country to prevent terrorist activities by the mention of key words e.g. bomb, explosive, or Al Qaeda.

The USA Patriot was signed into law by President George W. Bush in 2001 after September 11, 200 I (Bullock, Haddow, Coppola, & Yeletaysi, 2009). This act was created in response to the event of 9111 which provided government agencies increased abilities. These increased abilities provided the government rights to search various communications such as email, telephone records, medical records, and more of those who were thoughts of terrorist acts (Bullock, Haddow, Coppola, & Yeletaysi, 2009). This allowed law enforcement to have the upper hand in being proactive to stopping potential acts against U.S. soil. In the 2011 year, President Obama signed an extension on the USA Patriot Act. This act has received criticism from the public due to the potential to be misused or abused by those in power. This act has allowed government agencies to impede on constitutional rights.

The Protecting Cyberspace as a National Asset Act of 2010 was an act that also amends Title 11 of the Homeland Security Act of 2002. This act enhanced security and resiliency of the cyber and communication infrastructure within the U.S. This act is important as the President declared that any cyber aggressions would be considered an act of war. This is also important as Estonia's entire digital infrastructure was taken down by hackers who supported the former Soviet rule. This type of attack could be damaging to the infrastructure in the U.S.- causing loss of power for days or more which could result in death. In an area, such as the Huntsville Metro, we could have multiple nuclear facility melt downs, loss of lSR capabilities, and communication to the warfighter that we are supporting.

Additional changes from this act include the ability to carry out a research and development program to improve cyber security infrastructure. At the moment all government organizations must comply with the Federal Information Security Management Act (FlSMA) of 2002. This act has shown many holes within the U.S. cyber security infrastructure to include those organizations that are leads. This act provides DHS the ability to carry out the duties described in the Protecting Cyberspace as a National Asset Act of 2010.

Stuxnet Worm

During the fall of 20l 0 many headlines declared that Stuxnet was the game-changer in terms of cyber warfare (Denning, 2012). This malicious worm was complex and designed to target only a specific system. This worm had the ability to detect location, system type, and more. And this worm only attacked the system if it met specific parameters that were designed in the code. Stuxnet tampered directly with software in a programmable logic controller (PLC) that controlled the centrifuges at Natanz. This tampering ultimately caused a disruption in the Iranian nuclear program.

America's Homeland Security Preparing for Cyber Warfare

The Department of Homeland Security (DHS) is concerned with cyber attacks on infrastructure such as supervisory control and data acquisition (SCADA) systems. SCADA systems are the systems that autonomously monitor and adjust switching among other processes within critical infrastructures such as nuclear plants, and power grids. DHS is worried about these systems as they are unmanned frequently and remotely accessed. As they are remotely accessed, this could

allow anyone to take control of assets to critical infrastructure remotely. There has been increasing mandates and directives to ensure any system deployed meets stringent requirements. As the Stuxnet worm has become a reality, future attacks could be malicious code directly targeting specific locations of critical infrastructure.

Cyber Security Certification and Accreditation Processes to Secure Systems

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is the process that the Department of Defense (DoD) utilizes to ensure that risk management is applied to Automated Information Systems (AIS) to mitigate IA risks and vulnerabilities (Dawson, Jr., Crespo, & Brewster, 2013). DIACAP is the standard process that all services utilize to ensure that all DoD systems maintain IA posture throughout the systems life cycle. DIACAP is the replacement of the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). Figure 2 displays the process which includes five key steps. The first step is to initiate and plan the IA C & A process. The second step is to implement and validate the assigned IA controls. The third step is to make the certification determination and accreditation decision. The fourth step is to maintain authorization to operate and conduct reviews. The final step is to decommission the system.

The Common Criteria (CC), an internationally approved set of security standards, provides a clear and reliable evaluation of security capabilities of Information technology (IT) products (CCEVS, 2008). By providing an independent assessment of a product's ability to meet security standards, the CC gives customers more confidence in the security of products and leads to more informed decisions (CCEVS, 2008). Since the requirements for certification are clearly established, vendors can target very specific security needs while

Figure 1. DIACAP stages (Department of Defense, 2007)

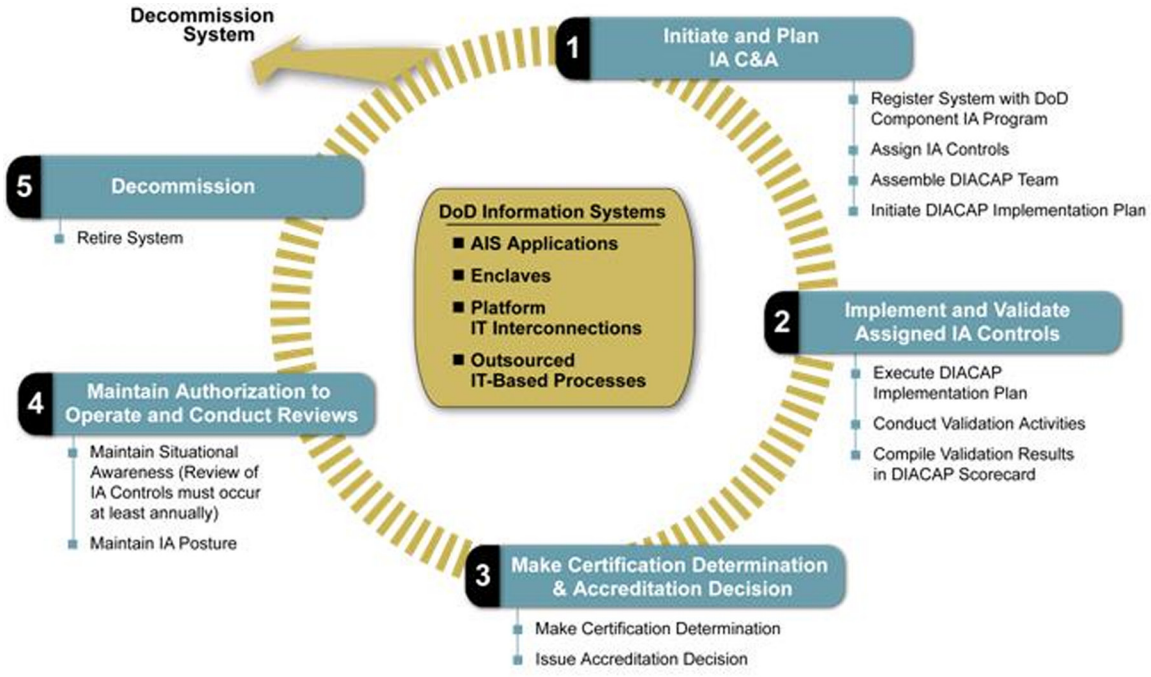
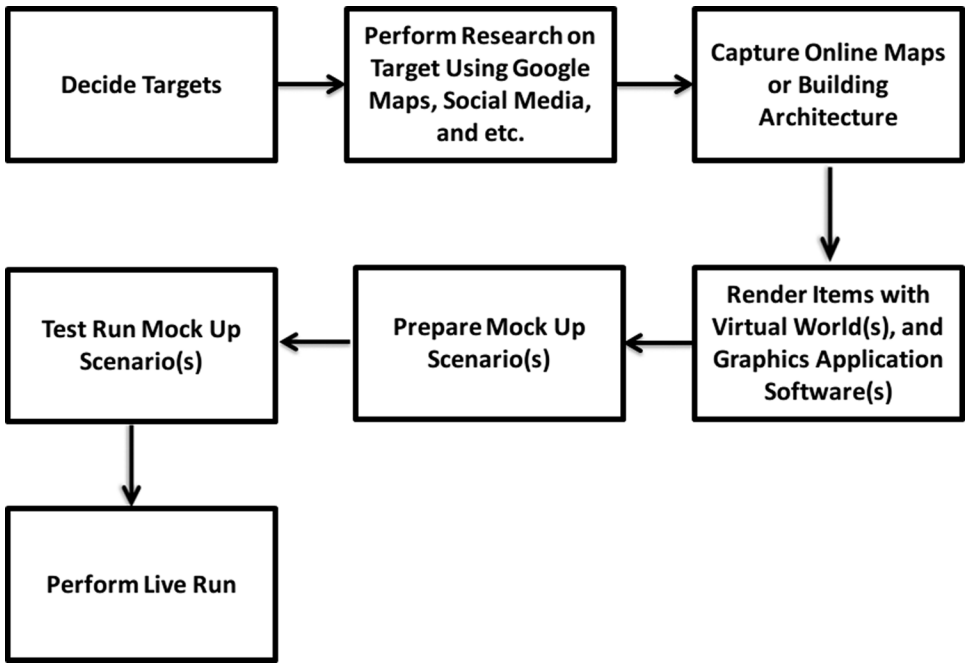


Figure 2. Process for building virtual world representations of real world items



providing users from other countries to purchase IT products with the same level of confidence, since certification is recognized across all complying nations. Evaluating a product with respect to security requires identification of customer's security needs and an assessment of the capabilities of the product. The CC aids customers in both of these processes through two key components: protection profiles and evaluation assurance levels (CCEVS, 2008).

The CC is the process that replaced the Orange Book. The CC has evaluated assurance levels (EAL) 1 through 7. EAL products 1 through 4 may be used and certified in any of the participating countries. However, EAL 5 through 7 must be certified by the countries national security agency, that is the United States' national agency is the National Security Agency and United Kingdom's national agency is the Communication Electronics Security Group (CESG). By all accounts, the NSA'a Orange Book program, in which the NSA forced vendors through prolonged product testing at Fort Meade, MD was a dismal failure. Also, the government's failure to Orange-Book-tested products, which were often out of date after years of testing, was a blow to the vendors that invested huge sums in the Orange Book Evaluations.

Additionally the National Security Agency (NSA) and DHS sponsors a joint venture known as the National Centers of Academic Excellence in IA Education (CAE/IAE), IA 2-year Education and Training (CAE/2Y) and lA Research (CAE/R) programs. Students that attend institutions with these designations are eligible to apply for scholarships and grants which they repay through government service. These programs were created to address the lack of available talent in lA. Table 1 shows the Committee on National Security Standards (CNSS) that institutions must map to in order to receive the designation as a NSA/IAE.

Since the purpose was to expand the numbers of lA personnel, it is hard to evaluate the program's real success (Bishop & Taylor, 2009). One of the major problems is the lack of resources to all institutions who are NSA/IAE. Even though this program is targeted towards post high school efforts, more reforms are currently taking place in the K-12 educational areas.

Table 1. CNSS training standards

Standard	Year	Description
NSTISSI 4011	1994	Information Systems Security Professionals
CNSS 4012	2004	Senior Systems Manager
CNSS 4013	2004	System Administrators in Information Systems Security
CNSS 4014	2004	Information Systems Security Officers (ISSOs)
NSTISSI 4015	2000	System Certifiers
CNSS 4016	2005	Risk Analysis

Human Computer Interaction

Future national and international threats that will be directly correlated to the Internet will be many as more devices are added to the Internet the problem of security also multiplies. Richard Clarke mentions that there are currently 12 bill ion devices currently connected to the Internet; this figure is supposed to grow to 50 billion in ten years (Clarke, 2012). Our dependence and interdependence with the internet creates new challenges as the more devices that are put online, the more exposure or vectors we are creating. The number of devices on the Internet is growing exponentially. As more applications for technology and wireless technologies are adopted, we are going to see this grow even further. What comes to mind are the self-driving vehicles that will be coming in a few years. We already have some self-driving cars, but they are not widely adopted yet or available to the public. When this does happen, we are going to see another exponential growth rate and the number of connected devices as each automobile will constitute at least a single IP address if not probably more.

Communication is the on-going and never ending process through which we create our social reality. Never in history has this been truer, as the computing and communication platforms that we have today far exceed anything that has ever been planned or projected. Information technology has radically altered the process in the way people learn and communicate. Weiser notes the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it (Weiser, 1991). An example has been the explosive growth of SMS texting, email, and social media. As these technologies are weaved into our lives, so are the dangers.

Research Projects

Many of the research projects that have taken place in mixed reality have been in educational domains and military domains. The focus of mixed reality research and education is to expand the capability of students to learn and interact and retain constructed knowledge and for businesses to maximize the knowledge that they have. Interesting new ways of looking at problems and topical areas enhance the learning experience and enhance capabilities, such as the ability to create a physical environment when it does not exist in the real world. Researchers (Park et al., 2008) studied human behavior in urban environments using human subjects in a virtual environment which demonstrated that virtual reality and mixed reality have the capability to model human behavior and that the products of these research projects are useful and may save time and money. Tn many situations, they provide an environment for simulation and analysis and design that would not be possible in the real world.

Most mixed reality devices, at this point, are ru1ming on the internet or another network in order to communicate with one another, connectivity is very important. Since the devices are entering cyberspace, they are going to be exposed to the same sorts of risks that any device connecting to cyberspace will encounter. Researchers (Cheok et al., 2005) state that mixed reality is "the fusion of augmented and virtual realities". Mixed reality is

more than virtual and more than augmented reality, by combining the two we are able to create real time learning environments, research experiments, and knowledge based collaboration areas that are enhanced by the application of mixed reality.

Using games for learning and for entertainment is one of the areas for different types of mixed reality applications. Researchers (Pellerin et al., 2009) describe a profile management technique for multiplayer ubiquitous games. Multiplayer ubiquitous games use different types of net aware skills me network aware objects and network objects such as an RFTD tag which allows the participant to interact with the physical environment. Hardware and software to support multiplayer ubiquitous game MUG is dependent on planning out the architecture in this specific example and NFC smartcard is used as well as a reader and a HTTP server the NFC smartcard communicates with NFC reader which in turn communicates with the HTTP server. This is done in order to create a mechanism which as the authors state's guarantees a stronger identification scheme than just a login password and might help Fortson common online game cheats". The previous was an example of an approach that is used to handling player profiles and allows interactions and centralized and decentralized ways. This is very similar to the CCNx 1.0 protocol which is also or which also has a goal of allowing centralized and decentralized interactions are communication.

Virtual Worlds

With the continual rise of virtual world environments, such as OpenSimulator (OpenSim) and Second Life (SL), they have the ability to be used for positive or negative gains in military warfare in the areas of training (Dawson, 2011). OpenSim is an open source multi-user 3D application server designed by taking the advantage and making a reverse-engineering to the published Application Programming Interface functions (APIs) and specific Linden Lab open source parts of the SL code (Dawson & AI Saeed, 2012). One of the strengths for creating any virtual environment is making it accessible by a variety of users through using various protocols. OpenSim provides a method for virtual world developers to create customized virtual worlds easily extensible through using the technologies that fit with their needs. For example, a terrorist could create a virtual representation of a building by using publicly available drafting plans. This virtual representation would serve as scenario based training for terrorists. Additionally, this would allow for terrorists of different cells or groups to communicate freely. The first step would be for the terrorists to decide their targets. Once targets are decided then they would perform research on the target. This research would be on all related items such as technologies, physical infrastructure, and personnel. In the next steps the individual would capture any online maps or building architectural diagrams that would allow these areas to be rendered with the virtual world. Once the rendering of these areas has been completed a mock up scenario would be prepared. This would allow a test run to occur and later a live run. These steps can be prepared with the use of open source technology at no expense to the terrorist. See the figure below which outlines the processes described.

With the possible scenario presented policing the virtual worlds may become a necessity to maintain national security (Parti, 2010). The U.S. Army is currently implementing a program known as Military Open Simulator Enterprise Strategy (MOSES). MOSES runs on OpenSim and is moving towards a Common Access Card (CAC) enabled environment for secure and encrypted communications (Maxwell & McLennan, 2012). In Figure 3 displayed is an interrogation scenario in MOSES. Additionally the U.S. could follow a model similar to Estonia where kids from the age of seven to nineteen learn how to develop software programs. This would help in deterring threats to include having future developers build security into the software from the beginning.

Figure 3. MOSES incerro_qacion scenario

Open-Source Software for Cyber Security

Researchers, as well as scientists, have long advocated for the use of open source software for improving the nation's security posture. Open source software can be used as an effective tool in order to protect government networks and defend them against cyber criminals. Corporation, government agencies, and educational institutions have been seriously considering incorporating open source security into their systems security because of the many advantages offered by open-source software; those advantages are exemplified by lower cost ownership, customizability (the ability of modifying the code to meet security requirement) and reasonable security. In fact, DHS has already established a $10 million program to fund research efforts aimed at finding open-source software that could be used for security purposes and boost existing cyber defenses (Hsu, 2011). What is encouraging about the future of open source software for security is that the threat landscape is rapidly changing attacks are becoming highly organized as well as sophisticated, and the cost of commercial software security continues to rise; this trend, in turn gives open source software a cutting edge where businesses and governments are enticed to take advantage of the many benefits offered by open source software. Since the US government is looking for ways to cut costs and business organizations are looking at security as a financial burden; it is a matter of time before open-source software becomes mainstream and a competitive security solution.

Back Track Linux

Back track is a Linux-based operating system designed for digital forensics and network penetration testing (Myers, 2012). It is named after the search algorithm, "Backtrack" and is considered

an essential security component for all security professionals. Backtrack has become a very popular open source security component for all security professionals and hacker because it contains a set of security tools that can perform virtually any security task ranging from attack simulation and vulnerability assessment to web application security and wireless hacking. Backtrack is mainly a penetration testing tool which is used to assess the security of a network, application or system.

Backtrack Linux is a free open-source software that can be downloaded free from http://www.backtrack linux.org. This security software comes bundled with many other tools that could be installed and run separately from Backtrack; those tools include Nmap, Wireshark, and Metasploit, just to name a few. Backtrack was designed with security in mind, which includes an environment that makes security testing an easy and efficient task for security professionals. It is considered a one-stop-shop and a superior security solution for all security requirements because it offers capabilities that can be used for a variety of security activities such as server exploitation, web application security assessment, and social engineering (BackTrack Linux, 2011).

Tools and Methods for Monitoring Networks

Monitoring traffic across networks is of great interest to systems administrators due to the fact that this traffic has a tremendous impact on the security of networks and provides them with network situational awareness. The ability to monitor and analyze network traffic in real time can help detect and possibly prevent cyber criminals from breaking into information systems networks. Network monitoring software enables us to understand the state of network and determine the potential existence of malicious or abnormal network behavior. Network monitoring tools can prove valuable in preventing unauthorized access by providing insight into the volume of data traffic that flows over a network, examining and analyzing such data, and ultimately preventing security incidents. Over the years, the open -source security community has developed published open-source tools that are capable of monitoring network traffic and deterring possible attacks. More specifically, open-source software tools are capable of examining most activities within a computer network including malicious activity such as scanning attempts, exploits, network probing, and brute force attacks (Celeda, 2011). Described are some of the most common open-source software tools that are being used for network security monitoring. An example of this is Snort, the open source software developed by Sourcetire and used for intrusion detection and prevention (Snort, 2012). Snort is one of the most widely adopted network monitoring technologies that can be used by network administrators as a defensive technique to report suspicious network traffic activity and alert system administrators about potential cyber-attacks. Snort has gained considerable popularity and attention among other network monitoring tools because it combines the benefits of signature based tools and anomaly detection techniques (Roesch, 1999). Another reason behind Snort popularity and success is that Snort is capable of performing real time traffic analysis and packet logging on IP networks (Tuteja & Shanker, 2012). Furthermore, Snort's strength comes from its intrusion prevention capabilities which is a new feature added to Snort. The intrusion prevention feature allows Snort to take preventive actions, such as dropping or re-directing data packets, against potentially malicious traffic (Salah & Kahtani, 2009).

Nmap ("Network Mapper") is a free open source utility for discovering networks and performing security auditing (Sadasivam, Samudrala, &Yang, 2005). Nmap is a valuable and widely used network scanner that has the ability to scan rapidly and discover hosts and services by sending specially designed packets to the target host analyzes and responds. NMAP is different from other port scanner software applications in that

it does not just send packets at some predefined constant rate, instead, nmap takes into account network conditions such as latency fluctuations, network congestion, and the target interference with the scan during the run time. Nmap has some advanced network discovery capabilities that go beyond basic port scanning and host scanning; Nmap can identify the type and version of an operating system, what type of firewalls are being used on the network, and what listening services are rum1ing on the hosts. Nmap runs on major operating system such as Microsoft windows, Linux, and Solaris. NMAP has become one of the most useful network scanning tools that network administrators cannot afford to ignore especially because this tool has proven to be flexible, intuitive interface (the new Zenmap with the graphical user interface), deployable, cross platform and most importantly it is free.

TOOLS AND METHODS FOR NETWORK ATTACKS

Network attacks pose a significant challenge to information systems due to the dramatic impact such attacks have on computer networks. Network attacks could paralyze entire networked systems, disrupt services, and bring down entire networks. In the recent years, network attacks have increased exponentially and have evolved rapidly in complexity to evade traditional network defenses (e.g. intrusion detection systems, amd firewalls). As computer networks grow and evolve to include more applications and services; malicious hackers continue to exploit inevitable vulnerabilities in network based applications. This, in turn, creates a fertile ground for hackers to develop and implement complex attacks and break into critical information assets. Below are a few network attacks illustrating the dangers and consequences of network attacks to include methods to defend against those attacks.

Hackers use a portscan attack, one of the most popular reconnaissance techniques, to break into vulnerable network services and applications. Most of the network services need to use TCP or UPD ports for their connections. Further, a port scan allows hackers to listen via open and available ports by sending a message to each port one at a time and waiting to receive a response. Once the port replies to a message, a hacker would then dig further and attempt to find potential vulnerabilities, flaws, or weaknesses in that port and ultimately launch a port scan attack which can compromise a remote host. The consequences of port scans are numerous and diverse ranging from draining network resources, to congesting network traffic, to actual exploitation of network devices. Cyber criminals utilize a plethora of free, open-source software tools to launch a port scan attack; one of the most popular security tools is Nmap (as explained in the section above). Nmap provides some attractive probing capabilities, such as the ability to determine a host's operating system and to provide a list of potential flaws in a port, all of which could help hackers launch a port scan attack.

Combating a port scan attack requires deploying firewalls at critical locations of a network to filter suspicious or unsolicited traffic. Also, security gateways must be able to raise alerts, and block or shutdown communications from the source of the scan (Check point security, 2004).

A SYN attack which is also known as SYN Flooding targets the TCP/IP stack. It exploits a weakness in the way that most hosts implement the TCP three-way handshake. When Host Y receives the SYN request from X, it maintains the opened connection in a listen queue for at least 75 seconds (Reed, 2003). Many implementations can only keep track of a very limited number of connections. A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host thus making the system crash or becoming unavailable to other legitimate connections. The ability of removing a host from the network for at least 75 seconds can be used as

a denial-of-service attack, or it can be used as a tool to implement other attacks, like lP Spoofing (Rouiller, 2003). Mitigating this attack requires the implementation of several solutions such as network address translation (NAT), Access control lists (ACL), and routers.

Another attack, which is known as IP address spoofing or IP spoofing, refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of hiding the true identity of the packet (sender) or impersonating another host on the network. IP address spoofing is a form of denial of service attacks where attackers attempt to flood the network with overwhelming amounts of traffic without being concerned about receiving responses to attack packets. Implementing packet filters at the router using ingress and egress (blocking illegitimate packets from inside and outside the network) is the best defense against the IP spoofing attack. It's also a good practice to design network protocols in a way that they are not reliant on the IP address source for authentication (Surman, 2002).

Issues with Android Phones and Other Mobile Devices

Smartphones are becoming a more integrated and prevalent part of people's daily lives due to their highly powerful computational capabilities, such as email applications, online banking, online shopping, and bill paying. With this fast adoption of smartphones, imminent security threats arise while communicating sensitive personally identifiable information (PII), such as bank account numbers and credit card numbers used when handling and performing those advanced tasks (Wong, 2005; Brown, 2009).

Traditional attacks (worms, viruses, and Trojan horses) caused privacy violations and disruptions of critical software applications (e.g., deleting lists of contact numbers and personal data). Malware attacks on smartphones were generally "proof of concept" attempts to break through the phone's system and cause damage (Omar & Dawson, 2013). However, the new generation of smartphone malware attacks has increased in sophistication and is designed to cause severe financial losses (caused by identity theft) and disruption of critical software applications (Bose, 2008). Because smartphones are becoming more diverse in providing general purpose services (i.e., instant messaging and music), the effect of malware could be extended to include draining batteries, incurring additional charges, and bringing down network capabilities and services (Xie, Zhang, Chaugule, Jaeger, & Zhu, 2009).

Smartphones are rapidly becoming enriched with confidential and sensitive personal information, such as bank account information and credit card numbers, because of the functionality and powerful computational capabilities built into those mobile devices. Cyber criminals, in turn, launch attacks especially designed to target smartphones, exploiting vulnerabilities and deficiencies in current defense strategies built into smartphones' operating systems. Bhattacharya (2008) indicated that because of skill and resource constraints, businesses are ill-prepared to combat emerging cyber threats; this claim is true for smartphones as well, given the fact that those mobile devices are even less equipped with necessary protections, such as antivirus and malware protection software. Some services and features, such as Bluetooth and SMS, create attack vectors unique to smartphones and thus expand the attack surface. For example, in December, 2004, A Trojan horse was disguised in a video game and was intended to be a "proof of concept," which signaled the risks associated with smartphones that could potentially compromise the integrity and confidentiality of personal information contained in smartphones (Rash, 2004). Attackers can easily take advantage of those services provided by smartphones and subvert their primary purpose because they can use Bluetooth and SMS services to launch attacks by installing software that can disable virus protection and spread via Bluetooth unbeknownst to smartphone users.

With the development of it to movative features and services for smartphones, security measures deployed are currently not commensurate because those services and features, such as MMS and Bluetooth, are driven by market and user demands, meaning that companies are more inclined to provide more entertainment features than security solutions. In turn, this further increases vulnerabilities and opens doors for hackers to deploy attacks on smartphones. Furthermore, Mulliner & Miller (2009) argue that the operating systems of smartphones allow the installation of third-party software applications, coupled with the increase in processing power as well as the storage capacity. Scenarios like this pose worse security challenges because hackers could exploit those vulnerabilities, which are further compounded by users' lack of security awareness. Smartphone attackers are becoming more adept in designing and launching attacks by applying attack techniques already implemented on desktop and laptop computers; smartphones' enhanced features, such as music players and video games, produce easy-to exploit targets by sending seemingly benign files via music or video game applications to users and luring them into downloading such files. Becher, Freiling, and Leider (2007) indicated that attackers could exploit such vulnerabilities to spread worms autonomously into smartphones. Therefore, hackers usually use a combination of technical expertise along with some social engineering techniques to trap users into accepting and downloading benign applications, which are used later to execute malicious code and affect critical applications running on smartphones.

Android's core components, such as Linux and connectivity media, are vulnerable to attacks through which personal and confidential information is likely to be compromised. Android's threats are further amplified by the fact that users are limited to using their smartphones for basic services and functions, such as email and SMS/MMS. Users lack the programming mind-set to protect their Android smartphones and stay current with the latest security software updates. This gives hackers an edge to target Android smartphones in the hope of gaining unauthorized access to disable core services (email and web browsing); abuse costly services (i.e., sending MMS/SMS and making calls to high-rate numbers); eavesdrop on calls and most importantly compromise sensitive information to be sold for a price. Android's open-source nature further increases security vulnerabilities because attackers can easily exploit this feature to modify the core applications and install malicious software, which could be used to compromise Android-based smartphones and ultimately cause disruption and monetary loss.

Dangers of Social Networks

Virtual communication has become a distinct area of interest for many as it has become second nature and also weaved into our everyday life. People tend to create a social reality that is based on the cmmection to the internet and using tools that assist communication. These tools have danger sides that a vast majority does not see or think about on a daily basis. Currently, there has never been a higher danger in the social networks for the public than there is now. This danger is easily spread to everyone who use this mode of communication based that people unintentionally make themselves vulnerable. With a connection to a vast number of social networks, people are easily consumed by submitting personal information via the Internet. The time is now for the public to understand where they stand in the future of the internet connectivity and what they can do to assist or lessen this danger.

Trend in Social Networks

People of all ages are beginning to learn to use social networks to stay in touch, reconnect, and meet new people and find out about new places. These websites usually allow the user to present

a profile of himself through a long list of very detailed information (Conti, Hasani, & Crispo, 2011). A vast majority of businesses are beginning to use these social networks to find new employees, expand and market and product line, and also to advertise their brand. These primary reasons are based on several distinctions that will help companies grow and expand due to the majority of customers who search for products via social networks. Customers are becoming more tech savvy by using mobile devices to gain internet connectivity in various locations. This helps create a realistic and educational feel to understand specific product information that is only based online.

Social networks have become the largest branding and marketing areas for this era. Sites such as Twitter, Facebook, lnstagram, Pinterest, and many others have risen in this past decade and have continued to increase with customers based on their usability and features. These sites have risen in popularity in the last few years, typically growing from basic technologies as participation increases and user expectations shape and form the media (Fitzgerald, 2008). Increase use within these sites also dictates an increase in the population in users who are becoming friendlier in the social media aspect.

Online social networking sites have become integrated into the routine of modern-day social interactions and are widely used as a primary source of information for most. Research found that Facebook is deeply integrated in user's daily lives through specific routines and rituals (Debatin, Lovejoy, Horn, & Hughes, 2009). Facebook is a social networking tool that is used in various instances that help people connect to people or businesses connect to people. It is the mere change in security that people and businesses will need the most help. These areas are vital to the metamorphic adaptions of today's society. Change is needed, and with this change, new adaptions for online security are required and mandated in some instances.

Online security can be looked at by a virtual standpoint in the relation of consumers and businesses. Many businesses use social media and online social networks to communicate to one another in a sense that many users are also using the same technology to find new information. Online information security risks, such as identity theft, have increasingly become a major factor inhibiting the potential growth of e commerce (Wang, 2010). A base system of online security is needed to help fulfill many business expectations and also promote or generate business in different geographic locations.

A Geographic Location

In definition, Hochman et al (2012) defines lnstagram as a recent fad in mobile photo sharing applications that provide a way to snap photos, tweak their images and share then on various social networks with friends, family, and complete strangers (2012). This type of social media helps create a realistic feel for people to see photos of specific areas where people are located. This also helps create a uniformed timeline scheduled photos that describe a story of one's life. As security is a high need in this type of online social media, it is best used in personal and business use.

Pinterest is also a varying tool of online social media that houses has many users who also use other networking tools. Pinterest allows members to "pin" items or images found on the internet to a pin board, which can then be easily shared through an email link or by following the creator (Dudenhoffer, 2012). This networking tool can also be paired up with other social media tools such as Tnstagram, Twitter, and Facebook. These networking tools also create a justification that helps creates a total profile immersion for people virtually. Security within this profile is currently weak; changes and adaptions can help create a justification for areas of higher influences such as these networks.

The popularity of these sites provides an opportunity to study the characteristics of online social network graphs at large scale (Mislove, Marcon, Gummadi, Drushel, & Bhattacharjee, 2007). A leading cause of the rise of these sites has been with consumers fining it easy to use and navigate to find information on and within these sites. The usability of these sites makes it very easy for customers of all ages to navigate through processes, which require personal information. When people subject themselves into giving information to the virtual world, they also subject themselves in becoming vulnerable for virtual threats.

No matter how easy an internet site can be to submit sensitive information, no site is purely safe and danger free. This is why the connection to internet connectivity is a matter that needs to be handled with high importance. A dire need to have security at its maximum has never been such an item then it is today. From every angle, people are becoming vulnerable to attacks from predators who deem themselves capable of obtaining information. As vital information is spread throughout the system of technology based environments, this information can also be spread throughout the world.

WHO IS CONNECTED AND WHY?

The main focus for the impact of the digital age is the critical mass population of the people in the world. People are beginning to use, read, analyze, and interact virtually younger and more often than ever before. This preliminary change occurs because now people begin to interact with social networks at a younger age. Learning starts to develop at a younger age because many of the cognitive abilities are beginning to be developed and acquired when children are younger, thus giving them the ability to develop an interest in fields they may want to work in as an adult.

Businesses

Businesses begin to look at the advertising site of their work in relation to how it can assist them with sales and goals. Since marketing is such a large portion of business, brands especially need to look and see what advertisements they can use to assist them in reaching their goals. The future of advertisements and marketing is based on the consumer today, and where they look to find information in regards to their purchases. The future of the internet connectivity and adaptation is directly linked through the suitability of use for the internet.

An important factor to look at when it comes to firm development is to look at the dire need for firms to develop their niche successfully. The virtual sector of businesses is extremely dependent on the absolute use of the user and the internet. Businesses tend to adapt to a series of modules that are formulated with their overall mission as a company. Leaning to technology-based marketing is one way to look at the overall spectrum of the businesses.

Companies are moving online media to the core of their programs because ofhow often consumers use social media for information-gathering purposes (Grainger, 2010). A feature that gives customers a more realistic feel such that they can obtain information in quickly is an online feature. This feature is used in many tactics for marketing and advertising based that many customers are prone to find items that assist them with what they are looking for via online. The connection must also be secure and safe for consumers such that viable personal information is used for online purchases.

Internet connectivity can also create justifications for businesses that have a niche for merchandising to customers, not on location. This avenue also needs an increase in data that are transmitted through various servers and websites. Servers are the basis of information modification; they help

provide a space and location for all information to be transmitted within a network. Businesses are taking part of this big shift based that the value of information to be able to be moved with this the-savvy environment is easier than ever. Servers also offer a sense of protection for business material to be saved and updated. Since safety is a big issue due to weather, it is feasible for businesses to purchase servers. Moreover, prices have also decreased with reflection to the safety of a server. Not only does a price reflect an adjustment towards the quality and value of the item at hand, but it is also noted on the overall performance of the machine or equipment.

Institutions are also a main contributor or purchaser of servers and internet connections based that they using online connections more than ever. A main factor that needs to be adjusted with institutions is the feasibility factor of what has been given at hand for the item to be installed, adjusted, and used with the institution. This feasibility also dictates a specific privacy that needs to be labeled at a specific standard for the institution to use. If these privacy areas are not up to a specific level, the institution is not and will not be able to use these items in conjunction with its mission or vision values.

Schools

The future of institutions is founded via the internet and the connectivity that these institutions have with the internet. With this, more schools are using web design formats that are very user friendly, such that more information can be placed virtually. With more information being placed virtually, more students will have access virtually to this sort of information. This also gives the institution the power to place a majority of their application processes; faculty related work, as well as communication online and able to be accessed by any faculty member or student at any time.

The vulnerability of this information being accesses by outside threats is high in regards to how secure the information is. Many institutions place a restriction to the limitation of the access of where it can be obtained. This limits the user capability of accessing information. Limiting this information can lead to problems internally as opposed to externally based that not all users will agree and comply with the polity regulations.

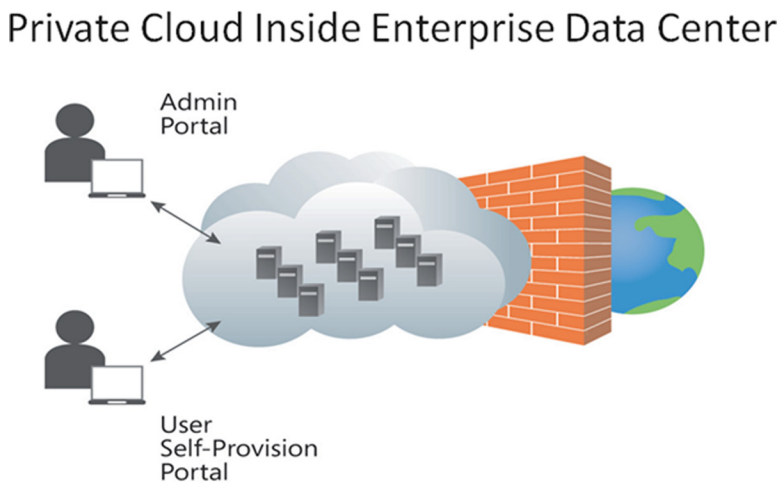
Institutions can create a wall that assists the blockage of information sharing through a semi-permeable layer, which is accessed by users and administrators. This barrier helps to control the amount of information sharing that can be displayed accordingly in regards to virtual threats. Creating this wall helps give administrators more control to information that is shared as well as provides a sate avenue for users at the lower level. When a barrio is promoted, it can also create a justification or rule that helps threats stay at bay and never reach core areas of information. The vital elements of this can be displayed in Figure 4.

WHERE DO PEOPLE CONNECT?

A rise in the digital social media arena has a direct impact towards the world, and with this many of the companies are beginning to respond with technological changes. With increasing technological advances. business can operate more smoothly, more effectively, and more efficiently to better facilitate operations and management. More tools are available for businesses that have the desire to take their business and marketing virtually. This has led to the increase of mobile device use since most users of social media use these applications in various locations.

Marketing has become a direct and distinct changing factor in business competition. With this, more businesses have begun to change their style ru1d location of advertisements. It is a clear example that more customers arc beginning to change their overall plans based on how they are able to obtain information on a general basis. With this, it is assumed that many businesses are

Figure 4. Private cloud enterprise data center (Social-Cast VMware, 2012)



also creating new, avenues and paths for marketing advertisements to be able to reach customers at various distances. This is also why it is very important for a business to have the ability to connect over a large geographic area with ease.

It can be determined that social networks via Internet connectivity are the best ways for businesses to connect to people. Businesses of all stature are beginning to look at the possibility of marketing strategies reaching customers in geographic locations. A large trend for mass adoption for businesses is to connect to customers via mobile devices; this in turn will lead to customers being able to connect to businesses at various levels. This trend increases the use of mobile devices based that a majority of the users are using these devices for a purpose.

One item that can be dictated with the high use of internet connectivity and mobile devices is the ability for outside sources to obtain information via mobile. This path will change the overall spectrum of how customers can purchase goods via online and where they can go to gain security for their purchases. It is then up to the providers of the mobile devices to create secure internet services for the customers' sake depending on how the customer is able to cooperate with technology. Even as the security of the internet service increases for the customer, it also must increase at the business end. This is to ensure that all employees and persons involved in online transactions are being monitored by a service that can provide safety throughout the purchase and delivery of the product.

INTERNET STALKING

The increase of the social networking trend can be based on the security features of for every user.

Internet stalking can be noted by a threat from an outside source that harms or conflicts harm to a piece of information or person. These threats can international or nation depending on where the organization or user is geographically located. With internet stalking being noted more often in today's society; it is also presumed that people are also becoming more vulnerable to attacks from internet insecurity. Insecure internet can be looked at based on what the user currently is using in terms of connectivity but can always be looked at as a threat to any customer.

When international threats are aimed at consumers, it can be perceived as a threat that is directed to the nation based that it is from outside the country. These circumstances can be legal or illegal based on the source of the threat. Many users see these types of threats as being identi-

fied as acts of terror based that many users do not know much information about the types of threats that are visible.

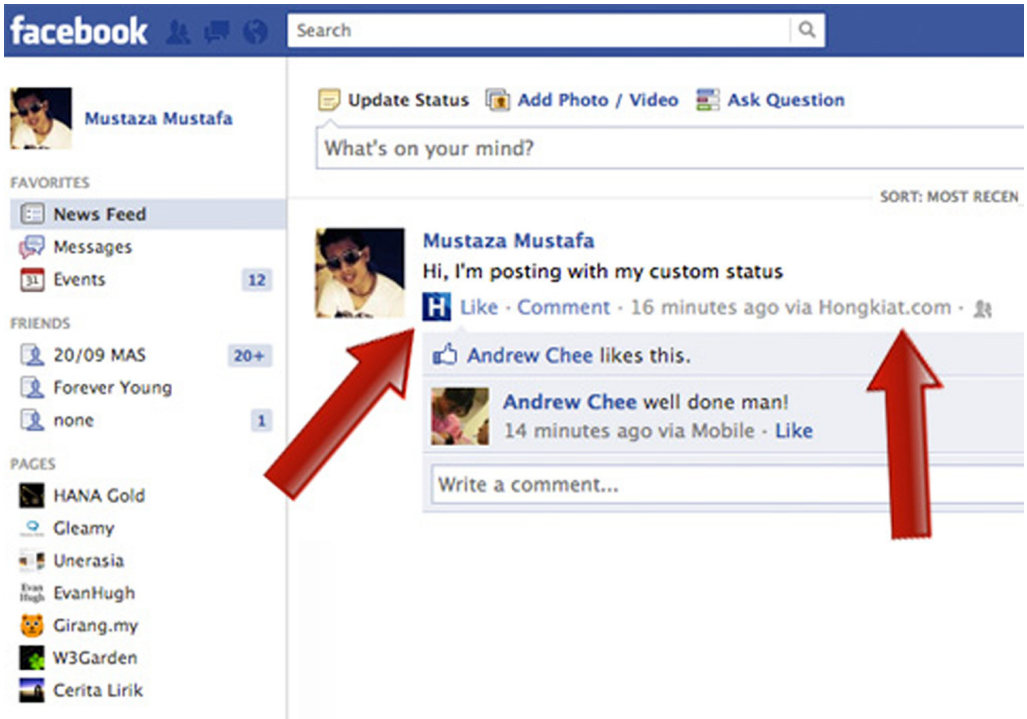
An example is noted from a post on social media that included valuable and private information. Any post can be noted in becoming a threat to outside sources such as a tweet from twitter, a picture from lnstagram, or a post on Facebook. Twitter is less than three years old, commands more than 41 million users as of July 2009 and is growing fast (Kwak, 2010).

From this point, an invader or Internet stalker can take into account the vital information and begin to look up where the user lives or where the user is updating his or her status. This can be done by researching with the Internet for items which are displayed virtually and can denote where the user lives. In this example, it is noted that the user Mustaza Mustafa is posting this status with Hongkait. Location information for users is stored in the About section of a user's profile on FaceBook.

Google earth is an application that can help look up locations and geographic areas on maps to help determine where items, businesses, and people are located. With this application, Internet stalking can be made easier by a method of inputing a location for a specific item, person, place or business to locate where it is. Since there is a very low security with this application, this option can be used with most location-based information given specific circumstances.

A phenomenon of cyber-stalking and virtual harassment will be the set of focus for the next generation. It is with this type of harassment that schools and institutions become the most vulnerable based on the population of these locations. Areas of improvement will be creating secure environments for students and faculty based on online communication. These areas will be an avenue for major threats as long as they are unsecure for cyber stalkers to pass through and obtain information.

Figure 5. Post on Facebook, a scoial media application (Mustafa, 2012)



Schools

Institutions, schools, colleges and universities can be noted as main areas for Internet stalking based on the number of users who use the Internet to connect, obtain information, and to communicate. With the increase in interest on the social trend, schools and institutions are adapting to modify more programs to be taught online. This adaption has the ability to help increases the student population for the school as well as increases the amount of adult learners who will use the internet to obtain information. This increase can also upset and hurt the population by leading stalker and other predators into getting involved with or becoming involved with internet stalking. As schools and universities become the highest areas for teens and students, they also become the most vulnerable.

Finn (2004) conducted an exploratory study to show that 339 students at the University of New Hampshire, about 10% to 15% of students reported repeated communication threatened, insulted, or harassed, them (Finn, 2004). This type of negative communication can result in various types of lawsuits, endangerment, or even physical harassment, which can lead into negative effects and/or reputations for institutions. Internal and even external customers can be the main causes of threats to the institution based on what information is current stored and what information is being obtained.

University communication and connectivity systems need to be impeccable in order to ensure secure networks for students and faculty. In terms of financially affordable, these systems need to have various departments that are capable of tracking of where the sources are going towards, coming from, and how they are able to obtain information. This type of security is currently necessary and will be necessary for the future with the increase in students and the usability of online platforms. This type of security also creates a unified system with the university's reputation to promote a positive secure environment.

Internet stalking also increases the risk of vulnerability for the institution in terms of international attacks from outside sources. These attacks or acts of terror can be terminated or at the least lessened by having a secure server internet connection. A secure internet connection needs to be set up with many specific requirements such that all users have access to information and communication within this method. Internet connectivity is increasingly moving off the desktop and into the mobile and wireless environment, particularly for specific demographic groups (Lenhart, Purcell, Smith, & Zickuhr, 2010). As the internet connections become a main target point of importance for institutions, security in these areas will also increase based on the amount of users.

Leading to Intelligence Gathering

The various types of information that social media customers input via the internet can be viewed and retrieved by outside sources. The information gathered leads to a negative activity from international customers. In various instances, personal, financial information can be gathered and used against the user for purposes of threats that can harm or steal the identity of the user.

Intelligence Gathering from Other Countries via Internet Connectivity

With the high trend of social networking scattering the internet's surface, social media are available in every country, thus increasing the use of internet connectivity. This availability of information helps create a mix between businesses and customers in terms of how information is related. Intelligence gathering is one way of using the available information and putting it to good use depending on the source of the receiver. Businesses can use this type of work by targeting special performance enhancing customers who are local and idealistic to the values that the company brings to the table. lt is also valuable in terms of online social market-

ing because it is feasible for businesses to assist with advertising online as compared to physical.

An international point of view that collaborates intelligence gathering can be noted based that internet connectivity is what brings users from various locations together in one normal new setting. This virtual environment setting becomes a normal atmosphere for many users based that most users are not currently satisfied with physical aspects of businesses. Using intelligence gathering from other countries helps institutions and businesses gather a list of potential customers from varying backgrounds that can help modify the existing performance of the business. A modification for a business is looked at by an increased way information is displayed and given to customers. This method should increase sales within the business, such that there is an absolute return on investment for the business.

Institutions can use intelligence gathering to help create new avenues for students to prosper. With this, distance learning and online collaborative learning can be assisted such that these are the main areas that are affected by the online networking. These changes also increase the power and connectivity of the specific institution to the student learner in the sense that they feel connected and secure. These are the most important items in any aspect of online networking in a business or educational field.

Privacy Laws

The U.S., Canada, and European Union (EU) provide a useful launching pad for the examination of cross-border privacy issues. With this, the U.S. has maintained a severe high maintenance cost for its security in the internet connections. This is a main reason why many institutions and businesses have created variances for what is allowed to be passed via the internet. In creating these variances, it also can be noted on how businesses prepare media and advertisements and also the security in these messages.

With Europe's high trade cost and online businesses, there is a high need for privacy to be placed in situations where customers will feel safe. It is this need that the EU uses to assume and vary its security online. Many businesses are accustomed to this type of development processes such that it is now accustomed to the normal activity for online marketing. Even the applications used via the internet connection do not use instances where privacy can be breached. It is with this type of process that businesses become safe from outside attacks.

FUTURE OF INTERNET CONNECTIVITY: SOCIAL NETWORKS

As internet connectivity becomes the more favorable and usable feature in a business industry, many businesses, customers, and people in general will begin to look for more ways to use this type of connection. The basis of a secure internet connection service begins with several items, which dictate how people use the connectivity, what they use it for, and where they use it. Many businesses will also become more conformable with the adaptability of internet usage in terms of security, mobility, and marketing. Overall, social networking is keen to fir development in businesses and keen for connections for people.

EMERGING TECHNOLOGIES AND THE INTERNET

Innovations and Numbers on the Growth of Ubiquitous and Mixed Reality Related Technologies

Google Glass is a wearable computer and a variant of the head mounted display (HMD). What is interesting about this innovation is that it is more than the headset. Google has connected this to the internet in many ways, not the least of which is

being connected to the users Google+ account, which enables the user to share photos and videos with others. Using Google+ the user is connected to all their contacts from their Gmail account. Glass provides a way for the user to interact in different ways with the internet, through the rich media environment that is supported by Google. Google glass could be integrated into internet security in many of the same ways in which the traditional mixed reality system that has been described in this chapter.

Google Glass may not have its uses defined, yet many have made prognostications on uses for the augmented reality system. It is quite a visionary type of product with associated services. Many have recently written about potential uses for Google Glass. Some of the best ideas arc very close to some of the existing fields of virtual and augmented reality. The fact that the actual headset is so innovative, small, and connected, is intriguing and opens the door for many types of new applications or revisiting the old applications with the new technologies. Many envision that Google Glass will be used in the operating room to provide real time information to surgeons, as well as, augmenting education on many different levels.

Emerging technologies that are changing things as we speak is the idea of content centric networking. Xerox PARC is currently developing Content Centric Network (CCN), and making the software open source. One of the advantages of this technology is going to be that the data maintains its integrity no matter where it is transmitted; as there are security keys that are incorporated in their peer to peer demonstration of the CCN, which can ride on top of protocols or run natively. Such technology is essentially for mixed reality environments which necessitate a need for sharing information locally and quickly.

An interesting way that we conceived to view ubiquitous wireless technologies and technologies that represent mixed reality is to view the specific technology or group technologies in a feedback control loop. Using such a model we can construct the following control loop using.

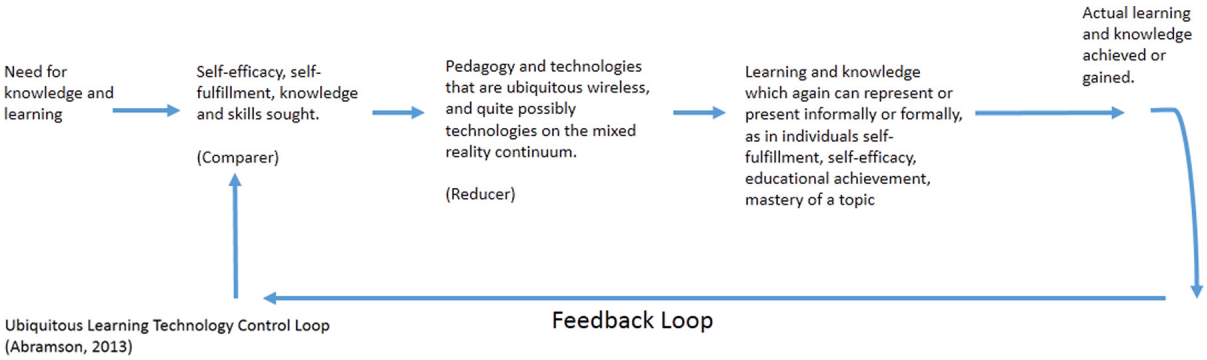
At the beginning of the loop is the need for knowledge and learning, which may be in individuals need, and or a formalized educational program. The next step in the feedback loop is the comparer; in this model it will represent grades, 21st-century technology skills, self-fulfillment and self-efficacy. To the right of the compare is the reducer, which consists of pedagogy and technologies that are ubiquitous wireless, and quite possibly on the mixed reality continuum. Lastly is learning and knowledge which again can represent or present informally or formally, as in individuals self-fulfillment, self-efficacy, educational achievement, mastery of a topic. The feedback control loop moves left to right, in the feedback loop itself runs from learning and knowledge back to the need for knowledge and learning. A chart has been created to help visualize the model.

Using this model we make some assumptions, the first is that this is an activity that individuals want to engage in. The second which is illustrated by the comparer, they have a need. The reducer once again is going to representative of the technologies that we arc looking at in this chapter. We arc looking at mobile devices, different types of mixed reality that are used for knowledge creation and collaboration. Therefore we are looking at the technologies in this paper as a reducer in the Ubiquitous Learning Technology Control Loop (ULTCL). While this framework is not predictive in nature, or does not prescribe, it does segment or compartmentalize the topical area which makes it useful for analysis of new and emerging technologies that are found in mixed reality environments.

Dangers

Cyber-attacks happen on all types of organizations and individuals. They can start in many different places, including any device that's connected to the Internet. This becomes highly problematic in our modern society when we have devices such as copy machines that are hooked up to the Internet in order to update themselves report usage, install

Figure 6. Ubiquitious learning technology control loop



software, etc. Having all these devices connected to the Internet increases our exposure and vulnerability. With so many targets we need to create an orderly way to look for threats. As the threats have increased through the years, we become more vulnerable to these threats. An interesting point about the intrusion detection systems is that they are part hardware and part software. Therefore when we implement one of these solutions we need to make sure that we are up to date with the hardware and software maintenance so that we get the updates that will keep the organization safe.

There are many research papers and projects that have demonstrated the usefulness of virtual and mixed reality environments in many different fields. It is important that the cyber warrior believes that they are in a different environment. Believability has been a requirement for successful implementations of mixed reality and virtual reality. Human computer interaction (HCI) is essential to making the cyber warriors feel that they are immersed in cyberspace. Since cyberspace cannot be seen by the naked eye, we need to gather the data and information that is necessary and make the user be able to see it in a virtual and productive environment. The potential of ubiquitous, mobile and mixed reality technologies to deter Internet threats is enhanced by these characteristics, as we now have the ability to have individuals who are in geographically separate areas, work together as one to solve new threats and problems. Mixed reality may be able to bridge the gap of recognition of security threats.

Incorporation of mixed reality should only require the changing of the inputs to the user or cyber warrior from game to actual data and information and the integration and implementation of a head mounted device (HMO) and quite possibly new input devices including brain to game interfacing. The process of creating a visual environment in which users can be active participants with real data with the purpose of solving problems and deterring threats, opens the process up to gamification. This permits the analysis of threats and also using the threat log and data for training as well, including one excited in a game based scenario.

Device Innovation

The characteristics of the devices that we use to connect to the internet are becoming smaller and more powerful. Contemporary mobile devices are extremely powerful, students can gather information off the Internet, download files, take pictures, email, and alter portalble document format (.pdf) files of any document that they have downloaded, analyze, synthesize and type up documents, all without any intervention or training from the

university. They can also participate in an online discussion, call, email, text, video chat on certain phones and devices, including Apple iPhone and iPod touch. Such areas and technologies are mentioned, as these platforms illustrate what is possible from a technological standpoint, the critical mass of the technology, and show how they have been adopted into organizations and more importantly the individual as many of the changes that we have seen have been driven by the adoption of the individual and used without any intervention of the organization or university. This makes technology or technological forces great. Thus combined with other forces has helped changed our society, no matter where we live. A ubiquitous device is one that is defined as always connected and allows access to content, anytime and anywhere (Hummel and Hlavacs, 2003). Internet bandwidth has become fast and more importantly wireless and ubiquitous, which has provided for the growth of many types of mobile wireless devices. Figure 7 and 8 displays the cyber warrior enviornments to include associated processes.

Figure 7. Cyber warrior technolgy infrastructure

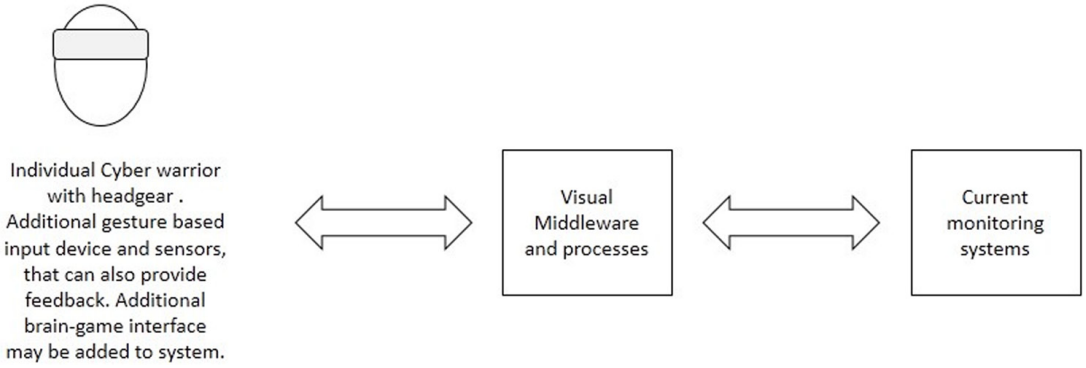
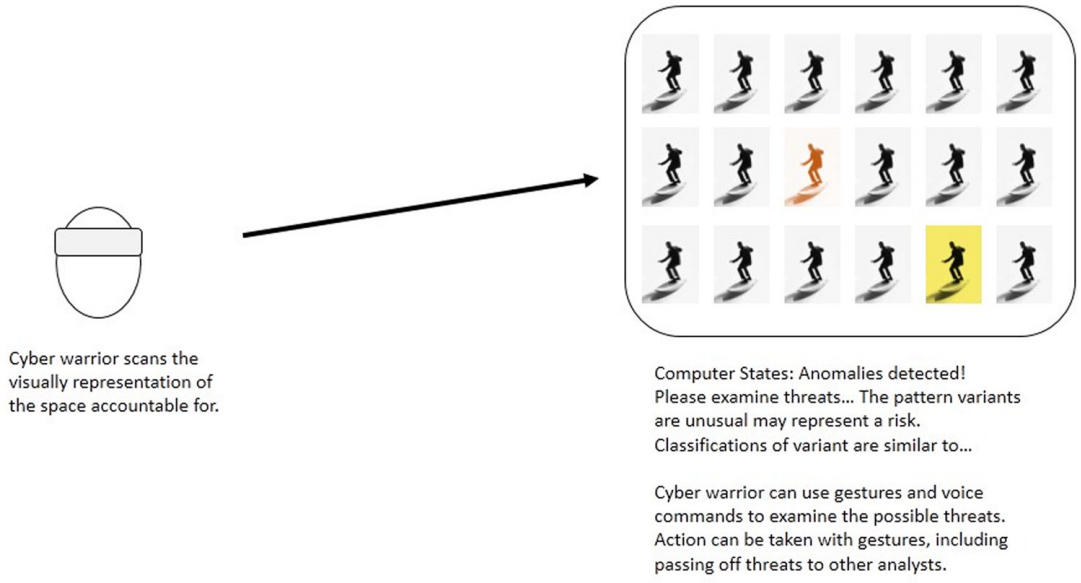


Figure 8. Cyber warrior scanning and interaction processes



EMERGING AREAS IN HUMAN COMPUTER INTERACTION FOR COUNTERING CYBER ATTACKS

One of these areas is the use of head mounted displays (HMDSs) which may use spatial immersive display technology. By using these types of devices we can create environments which help reduce some of the complexity that is involved with detection of cyber threats. Seeing mixed reality used in this capacity has been seen in popular fiction literature. Ender's Game (1985) is a science fiction novel by Orson Scott Card. In the novel the most talented young are trained using vit1ual reality and augmented reality games. The US military has been using virtual reality for training and development. Specific examples include soldiers shooting and field training with armor, infantry, aviation, artillery, and air defense. One of the first modern implementations of this was at the Defense Advanced Research Projects Agency (DARPA) Simnet facility at Ft. Knox, KY in 199Os. Inside ofthe facility were multiple types of units that had a representation of the vehicle and tools that they would use on the battlefield. As one of the authors was a participant in this event, computers made a compelling and immersive environment for units to train together and against one another. It is not hard to imagine extending this type of technology in order to create an immersive environment that makes the detection of cyber threats easier to identify from the mass of data and information that may or may not be detected using more conventional means.

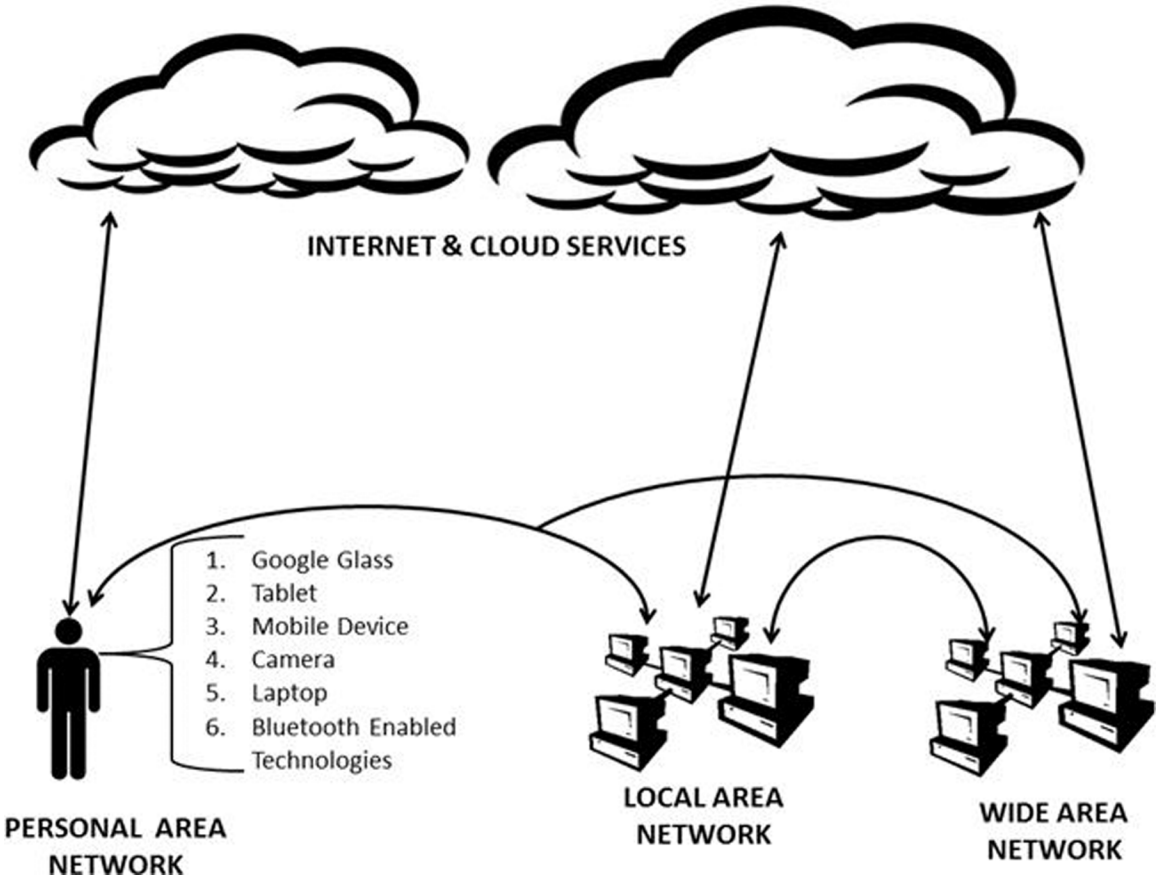
Mixed reality will make it easier to find these threats by a reduction of the complexity. Reducing complexity and increasing the understandability of threats will make it easier to work in an environment in which portions can be turned on and off. Current virtual reality and gaming technologies allow for the generation of the monitoring and subsequent training environments described. Of the first elements in a project that would be used to protect and monitor cyber-attacks would be to create a 3-D world in which systems/cyberspace can be modeled. Since many of the cyberspace attacks cyber-attacks target specific cities towns and businesses, we can use the geography as a starting point. From the generalized location we can create a highly granular or defined area of vulnerability and concern. This can be done by using many existing geographical databases such as Google. After this step we can focus on the mechanics of the 3-D world many tools are available for this purpose including dark basic which is a game engine that can house the navigation and parameters of the 3-D world. Therefore most if not all of the hardware and software systems and technology do exist for the creation and implementation of such a system.

Currently there are many open source and commercial versions of software that will permit the player/user to work against an AT or human opponent in order for the development of their ethical hacking skills. Users that immerse themselves in this type of technology are helping develop their skills sets, the future use of virtual and mixed reality to these types of systems will only enhance the understanding and help the user prepare for work as a cyber-warrior. Google code currently has a project emu-os that is a simulation ("Emu-os- EmuOS is an open-source hacking game and simulator. - Google Project Hosting," 2012) that pits hacker against hacker, by doing this the user is gaining real-world and real-time experience.

The latest IDC predictions at the time of writing this chapter show that mobile devices are passing out PCs in how users connect to the internet. Software as a service (SaaS) and Platforms as a service (PaaS) are all reporting exponential growth which helps confirm the mobile computing trends that we are seeing. There are many different reports out that describe the most popular mobile devices, a common theme among all of them is the smart phone and tablets ("IDC Predicts 2013", 2012). Therefore we can see that the internet infrastructures are changing to meet the needs of a more mobile device oriented market.

Figure 9. Post university cyber lab

Figure 10. Systems of systems



Mobile device security is going to become even more important as more people are going to be using these devices for all sorts of tasks, including those oriented around virtual and mixed reality.

Enhanced Collaboration and Learning with New Technologies

Collaboration is important and is enhanced with virtual and mixed reality systems. Collaboration is an important part of the new learning paradigm and has been proven effective in the supporting collaboration as e-learning tools are readily available on most mobile devices. Collaboration is enhanced by the use of mobile technologies and is a key intention of the knowledge age. Turoff (2000) proposed that collaboration provides a solution to learning outside of the physical classroom. In addition to collaboration, facilitation, and updated educational methodologies are key components to E-learning and M-learning (Hiltz, Benbunan-Fich, Coppola, Rotter, & Turoft, 2000). Collaborative learning is the promotion of learning through social interaction; it is one of the five properties identified by Klopfer et al., (2004), which support the established forms of learning through the use of mobile technologies (Naismith, Lonsdale, Vavoula, & Sharples, 2004). Figure 9 shows the Post University Cyber Lab with network forensics sosfteware running during a live class demonostartion.

Systems of Systems Concepts

When discussing hyperconnectivity it is necessary to discuss systems of systems concepts. Systems of systems is a collection of systems tied together to create a more complex system (Popper, Bankes, Callaway, & DeLaurentis, 2004). An example of this is Figure 10 below which displays a few methods to be connected to the internet and network traffic scenarios. When thinking about the possibilities of hyperconnectivity the personal area network (PAN) is an excellent example as it allows multiple technologies to be interconnected with soil ware applications. The Google Glass has the potential to all global positioning system (GPS), social media, digital terrain overlays, and synchronization with other devices. This increases the complexity of the system as it becomes part of a larger systems which multiples the number of potential vulnerabilities.

CONCLUSION

The futures of national and international security depend on multiple complex countermeasures to ensure that a proper security posture throughout its lifecycle. To effectively protect these systems from exploitation of vulnerabilities, it is a necessity to further comprehend all the current threats and how they exploit the current vulnerabilities. Additionally, one must be able to effectively gauge the future threats and have a strong grasp on the laws that drive their need to be secured such as enhanced privacy laws by the national governments. Examined within this chapter are the potential security related threats with the use of social media, mobile devices, virtual worlds, augmented reality, and mixed reality. Further reviewed were examples of the complex attacks that could interrupt human-robot interaction, children computer interaction, mobile computing, social networks, and more through human centered issues in security design. This book chapter serves as a guide to those who use multiple wired and wireless technologies but fail to realize the dangers of being hyperconnected.

REFERENCES

Armbrust, M., Fox, A., Griftlth, R., Joseph, A. D., Katz, R., Konwinski, A., & Zaharia, M. (201 0). A view of cloud computing. *Communications oft he ACM, 53*(4), 50-58.

BackTrack Linux. (2011). *BackTrack Linux*. Retrieved March 22, 2013, from www.backtrack-linux.org

Becher, M., Freiling, F., & Leider, B. (2007). On the effort to create smartphone worms in Windows Mobile. In *Proceedings ofthe 2007 IEEE Workshop on Information Assurance*. United States Military Academy. Retrieved March 22, 2013, from http://pil.informatik.uni-mannheim.de/filepool/publications/on-the-effort-to-create-smartphone-worms-in-windows-mobile.pdf

Beidleman, S. W. (2009). Defining and Deterring Cyber War. Barracks, PA Army War College. Retrieved March I0, 2013, from http://www.hsdl.org/?abstract&doc=ll8653&coll=limited

Bhattacharya, D. (2008) *Leardership styles and information security in small businesses: An empirical investigation.* (Doctoral dissertation, University of Phoenix). Retrieved March 9, 2013, from www.phoenix.edu/apololibrary

Bishop, M., & Taylor, C. (2009). A Critical Analysis of the Centers of Academic Excellence Program. In *Proceedings ofthe 13th Colloquium for Information Systems Security Education* (pp. 1-3). Retrieved March 9, 2013, from http://nob.cs.ucdavis.edu/bishop/papers/2009-cisse/

Bose, A. (2008). *Propagation, detection and containment of mobile mal ware*. (Doctoral dissertation, University of Michigan). Retrieved March 11, 2013, from www.phoenix.edu/apololibrary

Brown, B. (2009). *Beyond Downadup: Security expert worries about smart phone, TinyURL threats: Malware writers just waiting for financial incentive to strike, F-Secure exec warns*. Retrieved March 20, 2013, from http://business.highbeam.com/409220/article-1G1-214585913/beyond-downadup-securityexpert-worries-smart-phone

Bullock, J., Haddow, G., Coppola, D., & Yeletaysi, S. (2009). *Introduction to homeland security: Principles of all-hazards response* (3rd ed.). Burlington, MA: Elsevier Inc.

National Security Agency, Common Criteria Evaluation and Validation Scheme (CCEVS). (2008). *Common criteria evaluation and validation scheme -- Organization, management, and concept of operations* (Version 2.0). Retrieved from National Information Assurance Partnership website: http://www.niap-ccevs.org/policy/ccevs/scheme-pub-l.pdf

Celeda, P. (20II). *Network security monitoring and behavior analysis*. Retrieved March 22nd, 2013 from http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-cbpd133.pdf

Cheok, A., Fernando, 0., & Liu, W. (2008). The magical world of mixed reality. Innovation: The Magazine ofResearch and Technology. *National University of Singapore and World Scientific Publishing*, *8*(1), 70–73.

Cheok, A. (2009). Mixed Reality Entertainment and Art. *International Journal Of Virtual Reality*, *8*(2), 83–90.

Cheok, A., Man Fung, H., Yustina, E., & Shang Ping, L. (2005). Mobile Computing With Personal Area Network and Human Power Generation. *International Journal of Software Engineering and Knowledge Engineering*, *15*(2), 169–175. doi:10.1142/S0218194005002348

Clarke, R. & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it.* New York, NY: Ecco.

Conti, M., Hasani, A., & Crispo, B. (2011). Virtual Private Social Networks. In *Proceedings of the First ACM Conference on Data and Application Security and Privacy*. New York, NY: ACM.

Dawson, M. (2011). Applicability of Web 2.0: Training for Tactical Military Applications. Global TIME, 1, 395-398.

Dawson, M. E. Jr, Crespo, M., & Brewster, S. (2013). DoD cyber technology policies to secure automated information systems. *International Journal of Business Continuity and Risk Management*, *4*(1), 1–22. doi:10.1504/IJBCRM.2013.053089

Dawson, M. E., & Saeed, AI, T. (2012). Use of Open Source Software and Virtualization in Academia to Enhance Higher Education Everywhere. *Culling-edge Technologies in Higher Education*, *6*, 283–313. doi:10.1108/S2044-9968(2012)000006C013

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. doi:10.1111/j.1083-6101.2009.01494.x

Denning, D. E. (2012). Stuxnet: What Has Changed? *Future Internet*, *4*(3), 672–687. doi:10.3390/fi4030672

Dudenhoffer, C. (2012). Pin lt! Pinterest as a Library Marketing Information Literacy Tool. *College & Research Libraries News*, *73*(6), 328–332.

Dyck, J., Pinelle, D., Brown, B., & Gutwin, C. (2003). Learning from Games: HCI Design Innovations in Entertainment Software. In Proceedings of Graphics Interface, (pp. 237-246). Retrieved March 18, 2013, from http:/lhci.usask.ca/publications/view.php?id=88

EPOC Features. (2012). Retrieved from http://www.emotiv.com/epoc/features.php

Finn, J. (2004). A Survey of Online Harassment at University Campus. *Journal of Interpersonal Violence*, *19*(4), 468–483.

Fitzgerald, D. C. (2008). *Intersections of the Self: Identity in the Boom of Social Media* (Doctoral Dissertation). Available from ProQuest Dissertations and Thesis Full Texts Database: http:!/search.proguest.com/docview/304607151

Fraser, M., Hindmarsh, J., Best, K., Heath, C., Biegel, G., Greenhalgh, C., & Reeves, S. (2006). Remote Collaboration Over Video Data: Towards Real-Time e-Social Science. *Computer Supported Cooperative Work*, *15*(4), 257–279. doi:10.1007/s10606-006-9027-y

Google Project Hosting. (2012). *Emu-as- EmuOS Is an Open-source Hacking Game and Simulator*. Retrieved March 11,2013, from http://code.google.com/p/emu-os/

Grainger, J. (2010). *Social Media and the Fortune 500: How the Fortune 500 Uses, Perceives and Measures Social Media as a Marketing Tool* (Doctoral Dissertation). Available from ProQuest Dissertations and Thesis Full Texts Database: https://cdr.lib.unc.edu/indexablecontent?id=uuid:ae530f99-9b8d-43a4-9fa4-9fl2c5b00a2l&ds=DATAFILE

Hiltz, S. R., Benbunan-Fich, R., Coppola, N., Rotter, N., & Turoff, M. (2000). Measuring the Importance of Collaborative Learning for the Effectiveness of ALN: A Multi-Measure, Multi-Method Approach. *The Journal of Asynchronous Learning*, *4*(2), 103–125.

Hochman, N., & Schwartz, R. (2012). Visualizing Instagram: Tracing Cultural Visual Rhythms, Association for the Advancement of Artificial Intelligence. In *Proceedings of Sixth International AAAI Conference on Weblogs and Social Media*. Retrieved March 18, 2013 from, http://www.aaai.org/ocs/index.php/lCWSM/lCWSM12/paper/viewFile/4782/5091

Hsu, J. (n.d.). U.*S considers open-source software for Cyber security*. Retrieved March 22, 2013, from http://www.teclmewsdaily.com/2644-cybersecurity-open-source.html

Hummel, K. A., & Hlavacs, H. (2003). *Anytime, Anywhere Learning Behaviour Using a Web Based Platform for a University Lecture. In Proceedings of SSGRR 2003*. Aquila.

Kwak, H., Lee, C., Park., H., & Moon, S. (2010). What is Twitter, a Social Network of News Media?. In *Proceedings of the 19111 International Conference on World Wide Web*. Academic Press.

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). *Social Media & Mobiler Internet Use Among Teens and Young Adults*. Pew Research Center. Retrieved March 20, 2013, from http://web.pewinternet.org//media/Files/Reports/2010/PlPSocialMediaandYoungAdultsReportFina!withtoplines.pdf

Lewis, B. K. (2012). *Social Media and Strategic Communications: Attitudes and perceptions Among College Students* (Doctoral Dissertation). Available from ProQuest Dissertations and Thesis Full Texts Database: http://www.prsa.org/Intelligence/PRJournal/Documents/2012LewisNichols.pdf

Lopez, C. (2009). Immersive technology melds Hollywood, warrior training. *Soldiers*, *64*(5), 27.

Lotring, A. (2005). Training the millennlal sailor. *U.S. Naval Institute Proceedings*, *131*(12), 36–37.

Mac, R. (2013). *No One Is More Excited For Google Glass Than Facebook CEO Mark Zuckerberg*. Retrieved March 28, 2013 from http://www.forbes.com/sites/ryanmac/2013/02/21/no-one-is-moreexcited-for-google-glass-than-facebook-ceo-mark-zuckerberg/

Maxwell, D., & McLennan, K. (2012). Case Study: Leveraging Government and Academic Partnerships in MOSES. In *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications*, (pp. 1604-1616). Academic Press.

Mislove, A., Marcon, M., Gummadi, K. P., Drushel, P., & Bhattacharjee, B. (2007). Measurement and Analysis of Online Social Networks. In *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement*, (pp. 29-42). ACM.

Mulliner, C., & Miller, C. (2009). Injecting SMS messages into smartphones for security analysis. In *Proceedings of the 3rd USENlX Workshop on Offensive Technologies*. Retrieved March 22,2013 from https://www.usenix.org/legacy/events/woot09/tech/full papers/mulliner.pdf

Mustafa, M. (2012). *How to Customize the 'Via' Status on Facebook Posts, Hongkait.com Inspiring Technology*. Retrieved on April 18, 2013, from http://www.hongkiat.com/blog/customize-facebookstatus/

Myers, S. (2012). Operative BackTrack. *Journal of On Demand Hacking, 1*(3), 60-66.

Naismith, L., Lonsdale, P., Vavoula, G. & Sharples, M. (2006). *Literature review in mobile technologies and learning*. Futurelab Series. Retrieved March 22, 2013, from http://www2.futurelab.org.uk/resources/documents/1itreviews/MobileReview.pdf

Omar, M., & Dawson, M. (2013, April). Research in Progress- Defending Android Smartphones from Malware Attacks. In *Proceedings of 2013 Third International Conference on Advanced Computing and Communication Technologies* (pp. 288-292). Rohtak, India: IEEE.

Park, S. R., Nah, F. F., Dewester, D., & Eschenbrenner, B. (2008). Virtual World Affordances: Enhancing Brand Value. *Journal of Virtual Worlds Research*, *1*(2), 1–18.

Parti, K. (2011). Actual Poling in Virtual Reality - A Cause of Moral Panic or a Justitied Need?. InTech. Retrieved March 22, 2013, from http://www.intechopen.com/books/virtua1-real ity/actua1poIicing-in-virtua1-real ity-a-cause-of-moralpanic-or-a-justified-need-

Perens, B. (1999). The open source definition. In *Open sources: Voices.from the open source revolution,* (pp. 171-85). Academic Press.

Popper, S., Bankes, S., Callaway, R., & DeLaurentis, D. (2004). *System-of-Systems Symposium: Report on a Summer Conversation*. Arlington, VA: Potomac Institute for Policy Studies.

Qualman, E. (2013). *Socialnomics: How Social Media Transforms the Way We Live and Do Business* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Raento, M., Oulasvirta, A., & Eagle, N. (2009). Smartphones: An Emerging Tool for Social Scientists. *Journal of Social Methods & Research*, *37*(3), 426–454. doi:10.1177/0049124108330005

Rajabhushanam, C. C., & Kathirvel, A. A. (2011). System of One to Three Umpire Security System for Wireless Mobile Ad hoc Network. *Journal Of Computer Science, 7*(12), 1854-1858.

Rash, W. (2004). *Latest skulls Trojan foretells risky smartphone future*. Retrieved from www.eweek.com

Reed, D. (2003). *Applying the OSI seven layer network model to information security*. Retrieved March 22, 2013, from http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/7-Sep-2004/0SI.pdf

Roesch, M. (1999). SNORT-Lightweight Intrusion Detection for Networks. In *Proceedings of LISA '99: 13th USENlX conference on System administration*. Retrieved March 18, 2013, from https://www.usenix.org/legacy/events/!isa99/fuII papers/roesch/roesch.pdf

Sadasivam, K., Samudrala, B., & Yang, A. (2005). Design of Network Security Projects Using Honeypots. *Journal of Computing Sciences in Colleges*, *20*(4), 282–293.

Salah, K., & Kahtani, A. (2009). Improving snort performance under linux. *Communications, JET*, *3*(12), 1883–1895.

Sexton, S. (2011). *What is the Percieved Impact of Social Media on Personal Relationships in Adolescence?* (Doctoral Dissertation). Available from ProQuest Dissertations and Thesis Full Texts Database: http://gradworks.umi.com/15/03/1503092.html

Siegel, A., Denny, W., Poff, K. W., Larose, C., Hale, R., & Hintze, M. (2009). Survey on Privacy Law Developments in 2009: United States Canada, and the European Union, The American Bar Association Press. *The Business Lawyer*, *65*(1), 285–307.

Snort. (2012). *What is Snort?*. Retrieved March 20, 2013, from www.snort.org

Socialcast. (2012). *Managing and Control Your Private Network*. Retrieved on April 22, 2013, from http://www.soc ialcast.com/adm in istration

Surman, G. (2002). *Understanding Security using the OSI Model*. Retrieved March 25, 2013, from http://www.sans.org/reading room/whitepapers/protocols/understanding-security-osi-model 377

TDC. (2012). *IDC Predicts 2013 Will Be Dominated by Mobile and Cloud Developments as the IT Industry Shifts Tnto Full-Blown Competition on the 3rd Platform*. Retrieved March 22, 2013, from https://www.idc.com/getdoc.jsp?containerld=prUS23814112

Turoff, M. (2000). An End to Student Segregation: No more separation between distance learning and regular courses. *Horizon*, *8*(1), 1–7. doi:10.1108/10748120010803294

Tuteja, A. & Shanker, R. (2012). Optimization of Snort for Extrusion and Intrusion Detection and Prevention. *International Journal ofEngineering Research and Applications, 2*(3), 1768-1774.

Uitzil, L. (2012). Wireless security system implemented in a mobile robot. *International Journal of Computer Science Issues*, *9*(4), 16.

Walker, J. J. (2012). Cyber Security Concerns for Emergency Management, Emergency Management. InTech. Retrieved April 2013, from http://www.i ntec hopen.com/books/emergency-management/cy ber-secu rity-concerns-for-emer gene ymanagement

Wang, P. A. (2010). *The Effect of Knowledge of Online Security Risks on Consumer Decision Making in B2C e-Commerce* (Dissertation Thesis). ProQuest LLC.

Weiser, M. (1991). The computer for the 21st century. *Scientific American, 265*(3), 94-104.

Wong, L. (2005). *Potential Bluetooth vulnerabilities in smartphones*. Retrieved March 18, 2013, from http://citeseerx. ist.psu.edu

Xie, L., Zhang, X., Chaugule, A., Jaeger, T., & Zhu, S. (2009). *Designing system-level defenses against cellphone malware*. Retrieved March 21, 2013, from www.cse.psu.edu

KEY TERMS AND DEFINITIONS

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Availability: Timely, reliable access to data and information services for authorized users.

Cloud Computing: Comprised of both the application delivered as services over the internet and the hardware and systems software housed in the datacenters that provide those services (Armbrust, et al, 2010).

Confidentiality: Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

Hyperconnectivity: Use of multiple means of communications such as instant messaging, phones, Web 2.0, Web 3.0, and other communication methods.

Integrity: Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Non Repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Open Source Software: Software that allows the original source code to be fi·ee available which may be freely redistributed or modified (Perens, 2009).

Handbook of Research on Education and Technology in a Changing Society

Victor C.X. Wang
Florida Atlantic University, USA

A volume in the Advances in Educational Technologies and Instructional Design (AETID) Book Series

Information Science REFERENCE
An Imprint of IGI Global

Managing Director: Lindsay Johnston
Production Editor: Jennifer Yoder
Development Editor: Austin DeMarco
Acquisitions Editor: Kayla Wolfe
Typesetter: Thomas Creedon
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Handbook of research on education and technology in a changing society / Victor C.X. Wang, editor.
2 volumes ; cm
Includes bibliographical references and index.
ISBN 978-1-4666-6046-5 (hardcover) -- ISBN 978-1-4666-6047-2 (ebook) -- ISBN 978-1-4666-6049-6 (print & perpetual access) 1. Educational technology. 2. Information technology. I. Wang, Victor C. X. LB1028.3.H3553 2014
371.33--dc23

2014007983

This book is published in the IGI Global book series Advances in Educational Technologies and Instructional Design (AETID) (ISSN: 2326-8905; eISSN: 2326-8913)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 42
Open Source Software to Enhance the STEM Learning Environment

Maurice Dawson
University of Missouri-St. Louis, USA

Jorja Wright
Florida Institute of Technology, USA

Imad Al Saeed
Colorado Technical University, USA

Festus Onyegbula
University of Maryland University College, USA

ABSTRACT

This chapter examines the use of Open Source Software (OSS) technologies that can be used to improve the learning of Science, Technology, Engineering, and Mathematics (STEM). Explored are the various methods that can be utilized to improve the percentage of STEM majors in the American educational system with resources such as: Open Source as Alternative (OSALT), virtualization, cloud computing, Linux distributions, open source programming, and open source hardware platforms. Increasing the amount of students that pursue STEM majors is important because the projected job growth in the STEM field compared to non-STEM jobs is 33%. OSALT provides cost-effective alternatives to commercial products such as Microsoft Office Suite and Adobe Photoshop. Second, creating Virtual Machines (VMs) is another avenue to teach complex concepts in computer science, engineering, and Information Technology (IT). Third, cloud computing is an inexpensive way for clients to access information from multiple locations and devices. Fourth, universities can use the Operating System (OS) Linux and its various distributions as replacements for commercial operating systems like Windows in order to reduce IT costs. Lastly, open source programming languages like Python and their associated Integrated Development Environments (IDEs) provide comprehensive facilities for software engineers for application development or testing.

INTRODUCTION

This encyclopaedia chapter focuses on the evaluation and integration of OSS technologies to enhance the learning of STEM majors in the classroom. As the STEM majors at various institutions are looking for creative methods to increase their footprint at a fraction of the cost then OSS is vital to continued growth. Technologies reviewed include software languages, IDEs, virtualization, and integrated learning management systems (LMS). This chapter will review multiple methods of implementing OSS into curriculum to enhance the learning environment.

DOI: 10.4018/978-1-4666-6046-5.ch042

OVERVIEW

This chapter will cover the utilization of virtualization, OSS and simulation tools that are also open source. OSS can be defined as software that is made available in source code form. This is important as this source code may fall under the General Public License (GPL) which is a widely used free software license that is managed under the GNU Not Linux (GNU) Project. Virtualization is important as this is an effective method to reproduce system learning environments on the same systems the learner is using reducing the overall hardware footprint and need to for a massive lab. This chapter will also cover various software applications that can be integrated into the university system

STEM Outreach

The new millennium was the dawn of a new era in terms of technological advances. Technology impacts various aspects of our lives. In fact, President Obama believes that the key to enhancing our economy is by fostering education in the STEM areas. Pres. Obama stated recently stated,."..We must create an environment where invention, innovation, and industry can flourish... I am committed to doubling funding for key research agencies to support scientists and entrepreneurs, so that we can preserve America's place as the world leader in innovation, and strengthen U.S. leadership in the 21stcentury's high-tech knowledge-based economy" (Otto, 2012). Thus, federal policies are catering to the growing need for STEM based education that incorporates technology as a way to teach our 21st century youth. Moreover, the projected job growth for STEM careers is estimated to be three times as fast as job growth for non-STEM jobs (Langdon, McKittrick, Beede, Khan, & Doms, 2011). Along with this, the Economics and Statistics Administration states that STEM workers are less likely to experience unemployment than their non-STEM counterparts. Finally, workers with STEM degrees tend to earn higher salaries regardless of if they work in STEM or non-STEM careers. Furthermore, the numerous advances in technology have made our computers smaller, quicker and more accurate. From the premiere of the iPad three years ago, to the surge of smartphones in the market, mobile technology is permanently embedded in our daily lives. In fact, mobile Internet, digital textbooks and cloud computation are three technological advances that can positively change our educational approach.

When thinking about the long term goal of IT related employment it is necessary to view the Forbes 2013 Jobs List to understand the job demands. The number one position is software developer for applications and systems software with 70,872 jobs added since 2010, and overall 7% growth (Smith, 2012b). The number four position listed is computer systems analyst with 26,937 jobs added since 2010, and overall 5% growth (Smith, 2012b). The number six position listed is network and computer system administrators with 18,626 jobs added since 2010, and overall 5% growth (Smith, 2012a). In 2012, the number one position was software engineering with a midlevel pay of $88,142 (Smith, 2012a). The number nine position was computer systems analyst with a midlevel pay of $78,148 (Smith, 2012a).

OSALT and SourceForge

OSALT provides open source alternatives to popular commercial products (OSALT, n.d.). The open source programs LibreOffice, OpenOffice Draw, StarUML and Avidemux respectively are open source alternatives for Adobe Photoshop, Dreamweaver and iTunes. Sourceforge is an open source development Website that provides free services to aid developers create open source products and share it on a global scale (Sourceforge, n.d.). Community collaboration is important for the proper implementation of open source projects. Consequently, Sourceforge's directory provides the tools needed for 3.4 million develop-

ers to create open source software. This directory connects over 46 million consumers with various open source projects (Sourceforge, n.d.). This can greatly enhance the ability for an institution to expose students to a large variety of programs

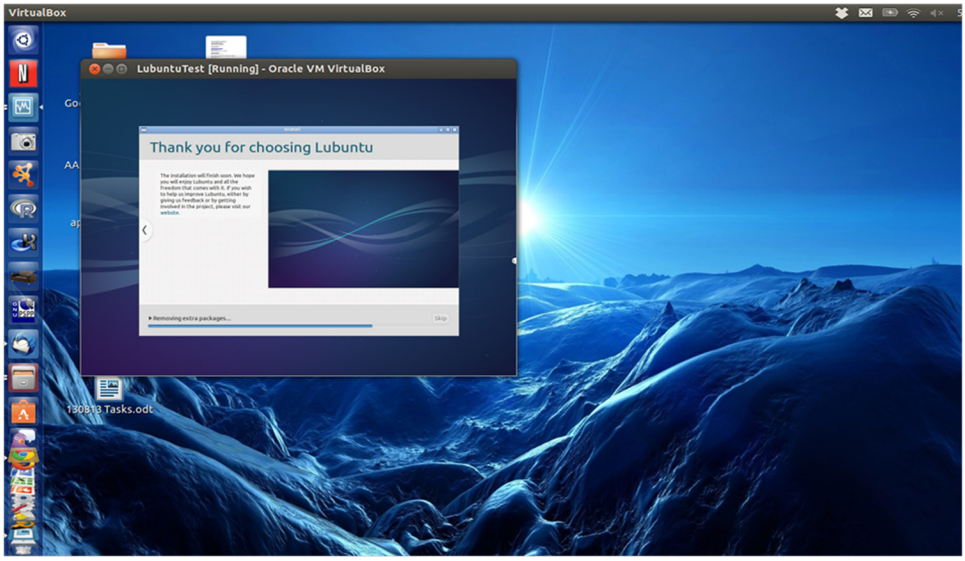
VIRTUALIZATION

In terms of virtualization there are available tools to create a virtual version of a system. In terms of educational resources this provides a method for institutions to train on VMs. This allows a university to teach students complex techniques to computer science, engineering, or IT students such as networking, programming, system administration, and information assurance (IA). There are multiple types of virtualization such as hardware, desktop, memory, storage, data, and network. In Figure 1 displayed is a screenshot of Lubuntu 12.04 running in a VM on the Ubuntu 13.04 desktop.

For institutions that would like the opportunity to provide a cloud like environment tools then Oracle Virtual Box and VMware Player provide that ability at a small fraction of the cost. However it should be noted that new Linux distributions running that require GNOME 3.10 will have issues running on older hardware. With older hardware as a constrained there are bare minimal Linux distributions such as Puppy Linux and Damn Small Linux (DSL). VMs provide the ability for a student to experiment with hundreds of OSs without installing uninstalling the base OS. Puppy Linux and DSL will allow an institution to take full advantage of older computers.

Additionally, this allows for the creation of baseline OS images for classes (Dawson & Al Saeed, 2012). For example, a data analytics course would have an OS created with all the predictive analysis software, case studies, statistical packages, design tools, and etc. preloaded. This would allow an institution to have image ready for every class to ensure consistency, and that the students have all required tools needed which would ease the process for program accreditation (Dawson & Al Saeed, 2012). In the case for a more technical course such as systems engineering the students would have a baseline OS image with all the programming software, the IDE, the Unified Model-

Figure 1. Screenshot of Lubuntu installation on Oracle Virtual Box VM running on Ubuntu 13.04 desktop

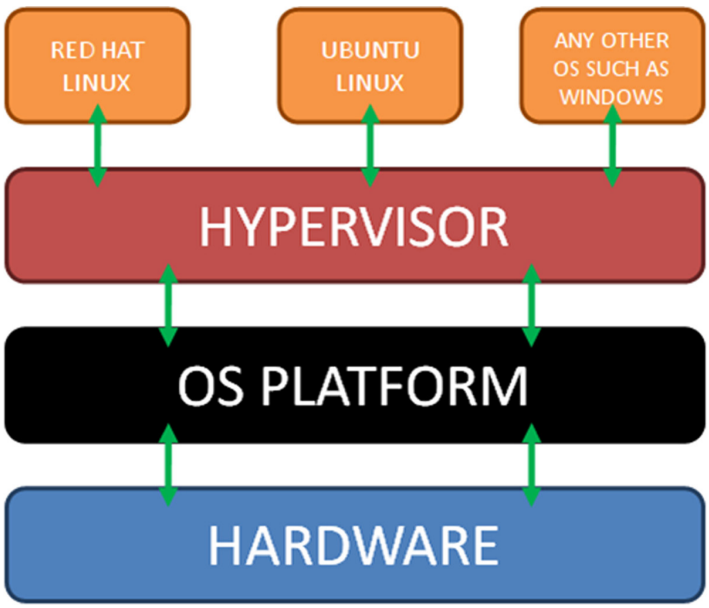


ing Language (UML), project management tools, quality testing tools, and etc. preloaded.

For professors, this virtualized environment would allow for the monitoring, distribution, and quicker deployment of available tools. This environment would be a cloud computing solution. Cloud computing is based on concepts of virtualization, distributed computing, networking and is underpinned in the latest Web and software technologies (Vouk, 2008). A useful definition of cloud computing is that it is a way of delivering applications as services over the Internet as well as a way of providing for the hardware and system software that act as platforms for these applications and services (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, & Zaharia, 2009). Cloud is also used to refer to a network of computers that are linked together and distribute processing capacity and applications to different systems (Johnson, Levine, & Smith, 2009). Cloud computing lets organizations add on to their IT and computing capacity without having to invest in new architecture, software or hardware or in training and developing personnel (Glotzbach, Mordkovich, & Radwan, 2008). A cloud environment could prove to be a cost effective implementation of which would allow for scalability if these right tools are utilized. Figure 2 provides an overview of how a VM environment looks like. The hardware is loaded with the selected OS platform. The OS platform can be Linux, Mac, Solaris, or Windows. Once the OS is loaded onto the hardware then the hypervisor is loaded. The hypervisor allows for multiple VMs to be hosted. The VMs act independently from the OS platform. This environment allows for testing, development, and integration of new OSs.

When constructing the VM environment it is important to think about the overall architecture which includes the hypervisor (Sailer, Jaeger, Valdez, Caceres, Perez, Berger, & van Doorn, 2005). There are two distinct types of hypervisors which are Type 1 and Type 2. The Type 1 hypervisor runs directly on the system's hardware to control the hardware to include managing the guest OS. An example of this would be XenServer or VMware ESXi. The Type 2 hypervisor runswithin the OS environment with the hypervisor layer as the

Figure 2. Scenario of VM environment



second application software layer. The guest OSs runs on the third layer above the hardware which is displayed in Figure 3 Two Types of Hypervisors.

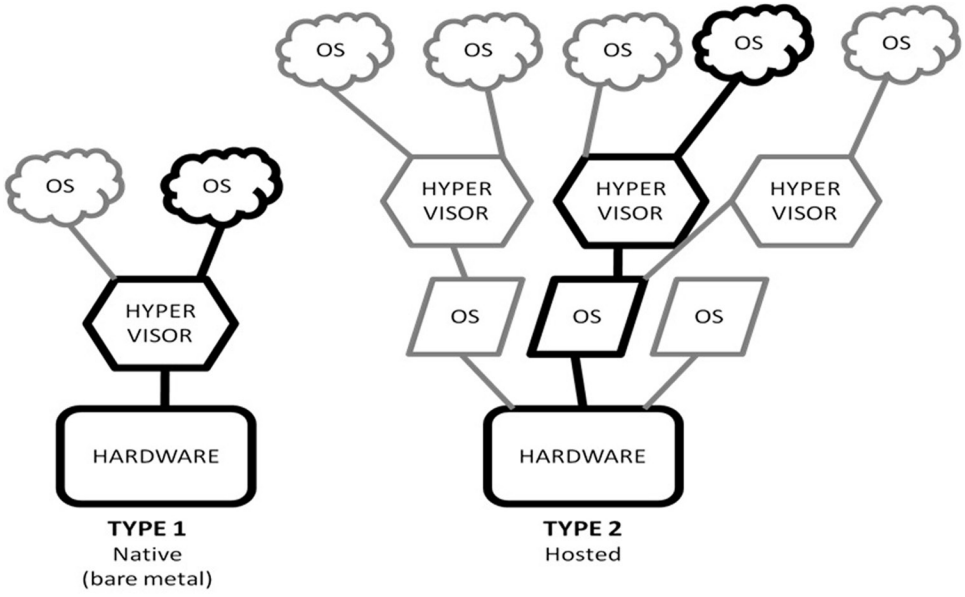
CLOUD COMPUTING

Cloud computing provides services that are available over the Internet or the intranet and the customers can access them using their computers or even mobile devices like the PDAs or phones. Cloud computing also makes it possible for the employees of the organization to access the services from diverse locations instead of being tied to their desks. Cloud computing is therefore characterized by On-demand availability of the service and on the concept of self service. The cloud computing services are to be automated so that there is little interaction of the service provider or the service users. In cloud computing, the service provider pools resources and makes them available to different customers while these customers do not concern themselves about how and where the resources are getting pooled from.

Cloud computing is marked by the high elasticity of service – the services can be automatically scaled up or down and distributed among the different customers based on their demands. Cloud computing provides flexibility in terms of elasticity and scalability, meaning that the services can be increased or decreased on need basis and in an automated manner without the intervention of the IT personnel. As such, organizations that deploy cloud computing do not have to buy additional computing resources if they expect an increase in demand. The organizations also do not have to fear for redundant resources as the cloud services are paid for only on the basis of usage (Kundra, 2010).

The automation and the freeing of the IT personnel from the task of managing, updating and maintaining the IT systems means that organizational resources are freed up and there are additional benefits of using the resources for other business related needs. In addition to the benefits of automation, cloud computing also means that there is no requirement for the customers to go for selection of resources from individual service

Figure 3. Two types of hypervisors



providers or for getting certifications from them. The cloud computing service provider provides a pool of diverse service in a ready to use form that the customers simply have to access and start using (Kundra, 2010).

Cloud computing also leads to a reduced information technology overhead for the end-user, as the service provider takes the responsibility of maintaining, managing, developing and integrating the systems and the services that the end-users use. Also, as the resources are pooled, it means that less organizations or departments are using their own resources and hence there is a tremendous scope for energy and power savings (Kundra, 2010).Cloud Computing, being managed and provided for by the service provider is managed in a highly professional manner that ensures that there are no or minimum service outages and the problems if any are rectified immediately. The service providers, being experts professionals in their field, are better equipped with the resources and facilities to ensure that the service is provided without any disruption (Kundra, 2010).

Cloud computing leads to reduced costs as the services may be shared by many organizations and thus reduce the cost of access and maintenance. The services are also paid-for on the basis of need, and organization's can better plan their IT budgets and tailor it to their specific requirements. It is also cost effective as it is easier to quantify and measure the usage of the services and thus it is easy to track the revenue and costs associated with that particular service (Kundra, 2010).

LINUX

Linux is an Unix like OS that is built on the Linux kernel developed by Linus Torvalds with thousands of software engineers. As of 2012 there are over two hundred active Linux distributions. The majority of the kernel and associated packages are free and OSS. This type of software provides licenses which allows users the right to use, copy, study, change, and improve the software as the source code is made available. Providing source code allows developers or engineers to understand the inner workings of development. Imagine being able to study Mac or Windows by viewing all the source code to replicate similar developments. This exercise would be great for a developer to learn low level coding techniques, design, integration, and implementation. Students and faculty could actively participate in design groups in which they would contribute code or design guidance for the upcoming software releases. This would be an added exposure for the university, students, and faculty internationally. In terms of associated cost the majority of Linux distributions are free. However some distributions require a cost for updates or assistance that related to specific needs such as OS modifications for server hosting. In software, there is a packet management system that automates the process of installing, configuring, upgrading, and removing software packages from an OS. In the Linux OS builds the most common packet management systems are Debian, Red Hat Package Manager (RPM), Knoppix, and netpkg.

Since Linux does not have redistribution limits it can be used to replace proprietary OSs in computer labs to save costs. The cost that would be associated with the proprietary labs can be redirected towards additional hardware instead. With the many variations of Linux one can find the appropriate distribution for their targeted use. Tables 1 and 2 display the different distributions to include the potential uses.

Fedora is an OS based on the Red Hat Package Manager (.rpm) (Proffitt, 2010). Fedora has a side development project known as Fedora Spins which contains multiple spin off versions of the Fedora OS. These spins allow academics, researchers, and students the ability to perform tasks such as cyber security, forensics, electronics design, and more (Petersen, 2013). Two of the spins are lightweight distributions which are essential to reviving older systems. Kitten Lightweight Kernel (LWK) and other similar kernels allow individuals the ability to

Table 1. Linux distributions and uses

Linux Distributions	Description and Potential Use	Packet Management System
Ubuntu	One of the most popular Linux OS developed to be a complete OS that can be an easily replacement for other comparable OSs.	Debian-based
Edubuntu	OS targeted for grades k-12. Contained in OS are tons of software applications that is useful to those who are education majors.	Debian-based
Damn Small Linux	This OS is designed to as a small OS to be utilized on older hardware. This OS is great for institutions that have old computers and want to revitalize them for use. OS is also great for VMs as DSL requires a low amount of memory	Knoppix-based
BackTrack	OS based on Ubuntu for digital forensics and penetration testing. Great tool for students majoring in technology fields. As cyber security is becoming a hot topic around the world this tool provides students the ability to learn from over thirty software applications that aid in penetration testing and more.	Debian-based
Fedora	This OS is supported by the Fedora Project and sponsored by Red Hat. This OS provides a great resource for learning Red Hat Enterprise Language (RHEL). As there are thousands of jobs requiring expertise specifically with Red Hat this OS is a great tool to prepare students for employment in IT. Fedora has over six Fedora Spins such as Design-suite, Scientific-KDE, Robotics, Electronic-lab, Games, and more.	RPM-based
CentOS	This OS derived entirely from RHEL. The source code is developed from Red Hat which allows a student to learn RHEL with a small number of differences. CentOS can be used for teaching IT students on how to setup, administer, and secure a server.	RPM-based
Ubuntu Studio	This OS is derived from Ubuntu. This OS is developed specifically for multimedia production such as audio, video, and graphics. Departments for multimedia could use this OS for multimedia instruction and the development of projects. As many of the tools for multimedia production are expensive this alleviates large license costs for institutions.	Debian-based
Lubuntu	OS is based on Ubuntu and uses the LXDE desktop environment. It replaces Ubuntu's Unity shell and GNOME desktop.	Debian-based

practice development on lightweight OSs (Brightwell, Riesen, Underwood, Hudson, Bridges, & Zaharia, 2003). The possibilities are endless for encouraging low level development, integration, and increasing overall lifecycle expertise.

OPEN SOURCE PROGRAMMING

Programming languagessuch as Python, Ruby, and Java have open source IDEs associated with them. These open source IDEs provide comprehensive facilities for software engineers for application development and testing. Eclipse, a popular IDE for Java developers, has gained a significant amount of popularity over the years (Murphy, Kersten, & Findlater, 2006). There are over twenty active IDEs that are maintained and distributed amongst the software community. Figure 4 displays the two Python IDEs in an Ubuntu Linux environment.

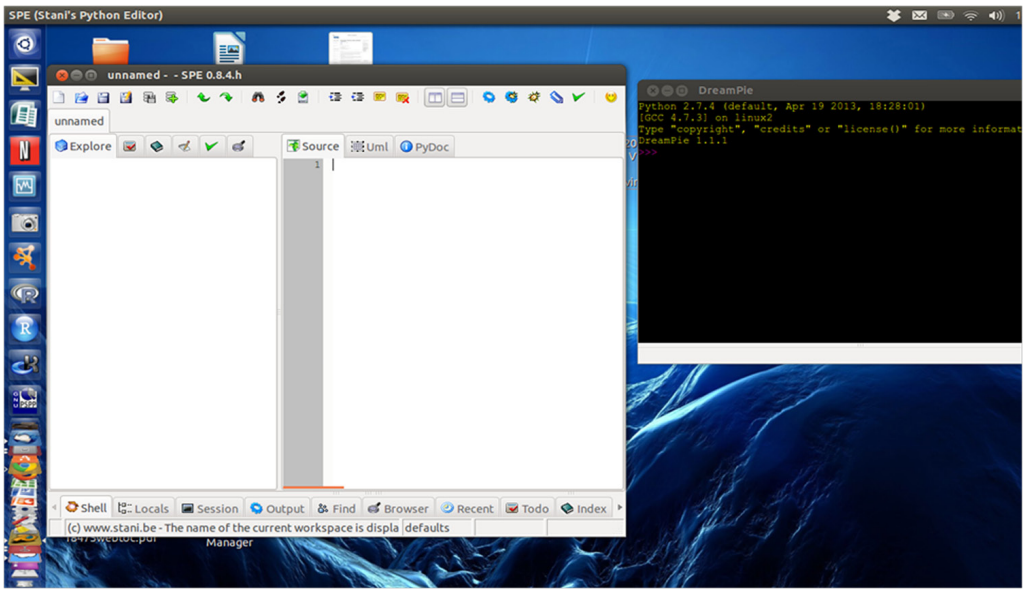
OPEN SOURCE HARDWARE PLATFORMS

Ouya is the Android-powered solution to the lucrative gaming arena that is open source. Ouya is a black and silver gaming console designed by Yves Behar, industrial designer and philanthropist (Benedetti, 2012). Ouya is an inexpensive

Table 2. Fedora spins and uses

Fedora Spins	Description and Potential Use	Packet Management System
Electronic Lab	This spin is for designing, simulating, and programming electronics. This spin is dedicated to support the innovation and development of the Electronic Design Automation (EDA) community. Some of the design tools included as ASIC layout, circuit layout, Computer Aided Drafting (CAD) tools, project management, peer review, and budget tracking.	RPM-based
Security	Spin targeted for cyber security and forensics professionals. Contained are tools for code analysis, forensics, intrusion detection, network statistics, password tools, reconnaissance, Web application testing, wireless, and Voice over Internet Protocol (VoIP).	RPM-based
SoaS	Sugar on a Stick (Soas) features the Sugar Leaning Platform which promotes collaborative learning that encourages critical thinking. This spin is available in more than 20 languages and originally developed for the One Laptop per Child XO-1 netbook. SoaS can be downloaded as a 54K torrent file which can fit on a small USB thumbdrive.	RPM-based
Design-Suite	This Fedora Spin focuses on open creativity. Contained are free and open source software for design activities. The tools available are graphics editors, photograph managers, flowchart creation, document annotation, diagram creation, 3D modeling, animation, rendering, and post production.	RPM-based
Robotics	This spin supports STEM students interested in robotics as it contains a variety of free and open robotics software packages. Contained is a free and open robot server with hardware support for over 100 devices.	RPM-based
Xfce	This spin is a lightweight desktop that has aims to be fast and low on system resources.	RPM-based
LXDE	Spin is an extremely fast, performance, and energy saving desktop environment designed to keep computer resource usage low. The Lightweight SX11 Desktop Environment (LXDE) is targeted for computers with low hardware specifications like netbooks, mobile devices, and older computers. LXDE can be used to revive older labs with functioning systems.	RPM-based

Figure 4. Python IDEs



alternative for gaming aficionados, in that Ouya is based on open source development. Currently, Ouya retails for $99 and that is one of the least inexpensivetelevision (TV) gaming console available. Unlike, the major gaming company, such as Playstation and Nintendo, Ouya does not require any licensing fees, retail fees or publishing fees (Benedetti, 2012). Ultimately, Ouya's creators want to create a developer-friendly environment in which hackers and hobbyists are all welcome to create games for Ouya. The only condition developers must meet is that the games they create must offer some free elements, such as free demos which work well in terms of advertising the product (Benedetti, 2012). This opens up the market which allows for universities to truly afford to teach courses on game design and allow students to develop their own custom game to market. As gaming is a popular pastime among young adults this would be a method to inject a desire for STEM recruitment.

As for academia, Ouya has the potential to transform the educational system in the 21st century. Technology has advanced at an exponential rate in the past 20 years, and continues to improve in the near future. The skill sets that are required for successful 21st century students include proficient computer literacy. In fact, the next generation of jobs will be characterized by increased use of technology, in depth problem solving and complex communication (McClarty, Orr, Frey, Dolan, Vassileva, &McVay, 2012). What students learn is no longer the focal point of their education, how and when they learn is just as important. Today's students have grown up with laptops, cell phones, tablets, and mobile Internet; naturally this technology should be applied to their learning environment as well. Advocates of game-based learning in education assert that digital games can teach students important skills, like thinking, planning, learning and technical skills that are vital for today's workforce (McClarty et al., 2012).

Lastly, Fedora's Electronic Lab (FEL) is a possible platform to utilize the Ouya gaming system. FEL is a free open source hardware design and simulation platform that is dedicated to supporting the Electronic Design Automation (EDA) community through innovation and development (Negus, 2010). FEL is important for the implementation of Ouya for various reasons. First, FEL "provides a complete electronic laboratory setup with reliable open source tools" to keep users current with technology (Negus, 2010). FEL solves a major problem for the open source community by providing real life open source EDA solutions. FEL utilizes three methodologies – design, simulation and verification – in order to give a better hardware design. Also, FEL bridges the two major open source communities: open source software community and open source hardware community. Finally, Fedora is available in alternate versions known as "spins" (Negus, 2010). The "Design-suite" spin for Fedora allows open creativity for users; "Security" spin has security analysis tools; "LXDE" spin is a faster, less demanding desktop environment; while "Games" spin is tailor-made for games in Fedora (Negus, 2010).

Raspberry Pi is "a credit card sized single-board computer" developed in 2006 by Eben Upton and three of his colleagues. Their intention was to stimulate interest in teaching of basic computer science in schools. Raspberry Pi has a Broadcom BCM2835 system on a chip (SoC) that contains an ARM1176JZFS; VideoCore IV GPU; and 256 megabytes of RAM (Raspberry Pi, n.d.). Lastly, Raspberry Pi uses an SD card for booting and long-term storage. Currently, two versions are available, Model A, which cost $25 and has 256 Mb RAM, one USB port and no Ethernet connection and Model B, which cost $35 and has 512 Mb RAM, 2 USB port and an Ethernet connection (Pi, 2012). The Pi makes it affordable for everyone STEM student to build on their own open source hardware platform. The possibilities for lab uses are limitless.

CONCLUSION

Open source technology is an avenue with unlimited potential to improve our educational system (Dawson & Al Saeed, 2012). Virtualization is a way to teach intricate computer science, engineering, or IT problems using a virtual machine (VM) (Dawson & Al Saeed, 2012). Also, VMs allows students to experiment with various OSSs without uninstalling the base OS. As mentioned earlier, this baseline OS can be equipped with tools that are needed for that discipline. Examples of these tools are statistics software, graphic design software, social marketing tools and case studies that are preloaded on to computers for business students. Cloud computation is a cost effective implementation of virtualization. Further, using Linux as the operating system will significantly reduce the cost of implementing virtualization into our educational system.

Since the majority of OSS is free, the money that is saved from technology can be used elsewhere. Open source is continually gaining popularity overseas in areas such as education and city government. In China, Germany, Estonia, and Russia, various versions of Linux are on the verge of becoming the main OS in the upcoming years. OSS is prevalent in the Spanish educational system as well. Open source software is changing the nature of organizational industries in project management. Lastly, gaming industry is another avenue that can be utilized in today's educational system. Ouya and Linux are cost effective open source alternatives to popular commercial gaming hardware and software, respectively. Gaming may be utilized to teach important skills such as thinking, planning and technical skills for today's job market. Finally, Raspberry Pi is a revolutionary computing device that may change the way education and technology are used in our society. Raspberry Pi is a way for students to access cheap programmable computers for today's society. Ultimately, open source software and/or hardware are low cost and is an excellent opportunity to integrate technology into academia (Dawson & Al Saeed, 2012). With security risks to mobile devices (Marwan & Dawson, 2013) to technology entrepreneurship it is clear that open source is a way to accomplish the goal of enhancing the STEM environment.

REFERENCES

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., & Konwinski, A. et al. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58. doi:10.1145/1721654.1721672

Benedetti, W. (2012). *Meet Ouya: The $99 game machine everyone is talking about*. Retrieved from http://www.nbcnews.com/technology/ingame/meet-ouya-99-game-machine-everyone-talking-about-876224

Brightwell, R., Riesen, R., Underwood, K., Hudson, T. B., Bridges, P., & Maccabe, A. B. (2003). A performance comparison of Linux and a lightweight kernel. In *Proceedings of Cluster Computing* (pp. 251–258). IEEE. doi:10.1109/CLUSTR.2003.1253322

Dawson, M. E., & Al Saeed, I. (2012). Use of Open Source Software and Virtualization in Academia to Enhance Higher Education Everywhere. *Cutting-edge Technologies in Higher Education*, *6*, 283–313. doi:10.1108/S2044-9968(2012)000006C013

Glotzbach, R., Mordkovich, D., & Radwan, J. (2008). Syndicated rss feeds for course information distribution. *Journal of Information Technology Education*, 7.

Kundra, V. (2010). State of Public Sector Cloud Computing. *CIO Council*. Retrieved from http://www.cio.gov/pages.cfm/page/State-of-Public-Sector-Cloud-Computing-HHS

Langdon, D., McKittrick, G., Beede, D., Khan, B., & Doms, M. (2011). STEM: Good Jobs Now and for the Future (ESA Issue Brief# 03-11). US Department of Commerce.

Leshner, A. I. (2007). Editorial: Outreach training needed. *Science*, *315*, 161. doi:10.1126/science.1138712 PMID:17218495

McClarty, K. L., Orr, A., Frey, P. M., Dolan, R. P., Vassileva, V., & McVay, A. (2012). *A literature review of gaming in education*. Retrieved from http://formative.pearsonassessments.com/hai/Images/tmrs/Lit_Review_of_Gaming_in_Education.pdf

Murphy, G. C., Kersten, M., & Findlater, L. (2006). How are Java software developers using the Elipse IDE? *IEEE Software*, *23*(4), 76–83. doi:10.1109/MS.2006.105

Negus, C. (2010). *Linux Bible 2010 Edition: Boot Up to Ubuntu, Fedora, KNOPPIX, Debian, openSUSE, and 13 Other Distributions* (Vol. 682). Indianapolis, IN: Wiley Publishing Inc.

Omar, M., & Dawson, M. (2013). Research in Progress - Defending Android Smartphones from Malware Attacks. In *Proceedings of 2013 Third International Conference on Advanced Computing and Communication Technologies* (pp. 288-292). Rohtak, India: IEEE.

OSALT. (n.d.). *About*. Retrieved from http://www.osalt.com/about

Otto, S. L. (2012). America's Science Problem. *Scientific American*, *307*(5), 62–71. doi:10.1038/scientificamerican1112-62 PMID:23120897

Perens, B. (1999). The open source definition. In *Open sources: Voices from the open source revolution* (pp. 171–185). Academic Press.

Petersen, R. (2013). *Fedora 18 desktop: Applications and administration*. Alameda, CA: Surfing Turtle Press. doi:10.1007/978-1-4302-6563-4

Pi, R. (2012). *An ARM GNU/Linux box for $25: Take a byte*. Retrieved from http://www.raspberrypi.org/quick-start-guide

Proffitt, B. (2010). *Introducing fedora: Desktop linux*. Boston, MA: Course Technology Press.

Sailer, R., Jaeger, T., Valdez, E., Caceres, R., Perez, R., Berger, S., & van Doorn, L. (2005). Building a MAC-based security architecture for the Xen open-source hypervisor. In *Proceedings of Computer Security Applications Conference,* (pp. 275-285). IEEE.

Smith, J. (2012a, April 10). *The best and worst jobs for 2012*. Retrieved from http://www.forbes.com/sites/jacquelynsmith/2012/04/10/the-best-and-worst-jobs-for-2012/

Smith, J. (2012b). *The top jobs for 2013*. Retrieved from http://www.forbes.com/sites/jacquelynsmith/2012/12/06/the-top-jobs-for-2013

Sourceforge. (n.d.). *About*. Retrieved from http://sourceforge.net/about

Stallman, R. (1991). *Gnu general public license.* Free Software Foundation, Inc. Retrieved from http://www.gnu.org/licenses/licenses.html#GPL

Vouk, M. A. (2008). Cloud Computing – issues, research and implementations. *Journal of Computing and Information Technology*, *16*(4), 235–246.

KEY TERMS AND DEFINITIONS

Cloud Computing: Comprised of both the application delivered as services over the Internet and the hardware and systems software housed in the datacenters that provide those services (Armbrust, et al, 2010).

GNU Public License: A widely used free software license that is managed under the GNU Not Linux Project (Stallman, 1991).

Hypervisor: Allows for multiple OSs to run concurrently on a host computer. There are two types of hypervisors that are used in computing (Sailer, Reiner, et al, 2005). The two types of hypervisors are Type 1 and Type 2 which differ in the way they are hosted on the machine.

Linux: An open source version of the UNIX OS (Perens, 2009).

Open Source Software: Software that allows the original source code to be free available which may be freely redistributed or modified (Perens, 2009).

Stem Education: Defined as educational fields in science, technology, engineering, and math.

Virtual Machine: Self contained operating environment that behaves as a separate computer but hosted on a host OS. The VM has no access to the host OS thus both entities exhibit separate behavior.

DoD cyber technology policies to secure automated information systems

Maurice Eugene Dawson Jr.*

Department of Management and Marketing,
College of Business and Public Affairs,
Alabama A&M University,
P.O. Box 429, Normal, AL 35762, USA
E-mail: dr.mauricedawson@yahoo.com
*Corresponding author

Miguel Crespo

Ernst & Young,
2005 Market Street #700,
Philadelphia, PA 19103, USA
E-mail: miguel.crespo3@gmail.com

Stephen Brewster

Textron Systems – AAI UAS,
124 Industry Lane,
Cockeysville, MD 21030, USA
E-mail: srbrewster@gmail.com

Abstract: Availability, integrity, and confidentiality (AIC) is a key theme everywhere as cyber security has become more than an emerging topic. The Department of Defense (DoD) has implemented multiple processes such as the Department of Defense information assurance certification and accreditation process (DIACAP), common criteria (CC), and created proven baselines to include information assurance (IA) controls to protect information system (IS) resources. The aim of this research study shall provide insight to the applicable processes, IA controls, and standards to include providing a method for selecting necessary government models and for system development.

Keywords: cyber security; risk management; information assurance; IA; enterprise governance; security controls; certification and accreditation; C&A.

Reference to this paper should be made as follows: Dawson Jr., M.E., Crespo, M. and Brewster, S. (2013) 'DoD cyber technology policies to secure automated information systems', *Int. J. Business Continuity and Risk Management*, Vol. 4, No. 1, pp.1–22.

Biographical notes: Maurice Eugene Dawson Jr. is currently employed as an Assistant Professor of Management Information Systems at Alabama A&M University. In addition, he serves as a Technical Lead at Reynolds Research and Technology Corporation for cyber security. He obtained his Doctor of Computer Science (DCS) from Colorado Technical University's College of Engineering and Computer Science. He has over a decade of experience within

the defence and aerospace industry in roles from intelligence, cyber security, and programme management. He has published widely on the topics of project management, information security, DoD, higher education, engineering and software assurance.

Miguel Crespo is currently employed at Ernst & Young as a Manager of the Information Security Center of Excellence. He completed a graduate degree in Information Assurance (IA) from Norwich University, and additionally he holds multiple professional certifications such as the Certified Information Systems Security Professional (CISSP). He has over a decade of experience with defence and commercial-based cyber security organisations as a lead with a specific focus on security risk management.

Stephen Brewster is currently employed as an Engineering Manager at Textron Systems' AAI UAS division where he is responsible for system engineering and integration for unmanned technologies. He holds an undergraduate degree in Computer Science from Athens State University. In addition, he has over eight years of experience with software and systems engineering in the defence community.

1 Introduction

Information assurance (IA) is defined as the practice of protecting and defending information and information systems (ISs) by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This definition also encompasses disaster recovery, physical security, cryptography, application security, and business continuity of operations. To survive and be successful, an enterprise must have a disaster recovery strategy and response plan in place to mitigate the effects of natural disasters (e.g., floods, fires, tornadoes, earthquake, etc.), inadvertent actions by trusted insiders, terrorist attacks, vandalism, and criminal activity. To properly lay the groundwork for this review it is essential to detail current processes techniques being utilised within the government to accredit and certify systems to include their IA-enabled products.

1.1 Research design

Research methods can consist of quantitative, qualitative, mixed methods, or case study. For the purpose of this research study the case study method was utilised. Below are the six steps that were conducted to complete the research study.

Step 1 Determine and define the research questions.

Step 2 Select the cases and determine data gathering and analysis techniques.

Step 3 Prepare to collect the data.

Step 4 Collect data in the field.

Step 5 Evaluate and analyse the data.

Step 6 Prepare the report.

1.2 Scope and limitations

The scope of this research shall include a limited number of security processes. Only the two major processes shall be researched. The information will only cover the scenario of an Unclassified (U) Mission Assurance Category (MAC) III, Public system. The Department of Navy (DoN) shall be the government organisation in which the IA processes and techniques will be reviewed in depth for this study.

1.3 Assumptions

The assumption of this research study is the security process utilised to secure the DoN is also the same process for the other service agencies. The data displayed is this research study is assumed to be (U) and not attached to any classified or deployed system.

1.4 Research questions and hypothesis

RQ1 Is there a common theme amongst the certification and accreditation (C&A) processes?

HY1 There will be a common them amongst the C&A processes.

RQ2 Are there IA controls that are applicable to IA enabled products and systems?

HY2 At least 60% of the IA controls will be applicable to both IA enabled products and systems.

2 Review of C&A processes

2.1 DIACAP for systems level development and deployment

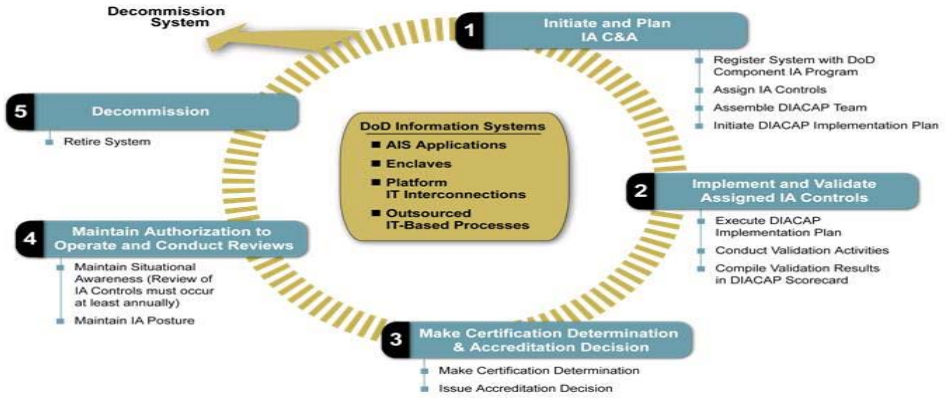
The Department of Defense information assurance certification and accreditation process (DIACAP) is the process that the Department of Defense (DoD) utilises to ensure that risk management is applied to automated information systems (AIS). DIACAP is the standard process that all services utilise to ensure that all DoD systems maintain IA posture throughout the systems life cycle. DIACAP is the replacement of the DoD information technology security certification and accreditation process (DITSCAP). Figure 1 displays the process which includes five key steps. The first step is to initiate and plan the IA C&A process. The second step is to implement and validate the assigned IA controls. The third step is to make the certification determination and accreditation decision. The fourth step is to maintain authorisation to operate and conduct reviews. The final step is to decommission the system.

The DIACAP process incorporated multiple artefacts to capture system data, network connections, data classification, and more.

- Plan of actions and milestones (POA&M) (see Appendix B).
- DIACAP scorecard (see Appendix C).

- Systems identification plan (SIP) (see Appendix D).
- DIACAP implementation plan (DIP) (see Appendix E).

Figure 1 DIACAP stages (see online version for colours)



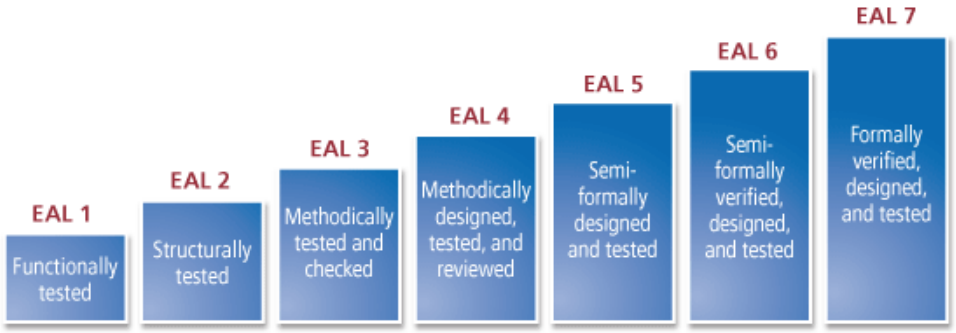
Source: DoD (2007)

2.2 Common criteria (CC) certification process for technology products

The common criteria (CC), an internationally approved set of security standards provides a clear and reliable evaluation of the security capabilities of information technology (IT) products (CCEVS, 2008). By providing an independent assessment of a product's ability to meet security standards, the CC gives customers more confidence in the security of products and leads to more informed decisions (CCEVS, 2008). Security-conscious customers, such as the US Federal Government, are increasingly requiring CC certification as a determining factor in purchasing decisions (CCEVS, 2008). Since the requirements for certification are clearly established, vendors can target very specific security needs while providing broad product offerings. The international scope of the CC, currently adopted by fourteen nations, allows users from other countries to purchase IT products with the same level of confidence, since certification is recognised across all complying nations. Evaluating a product with respect to security requires identification of the customer's security needs and an assessment of the capabilities of the product. The CC aids customers in both of these processes through two key components: protection profiles (PPs) and evaluation assurance levels (CCEVS, 2008).

The CC is the process that replaced the Orange Book. The CC has evaluated assurance levels (EAL) 1 through 7. EAL products 1 through 4 may be used and certified in any of the participating countries. But EAL 5 through 7 must be certified by the countries national security agency, i.e., US' national agency, the National Security Agency and UK's national agency, the Communication Electronics Security Group (CESG). By all accounts, the NSA's Orange Book programme, in which the NSA forced vendors through prolonged product testing at Ft. Meade, MD, was a dismal failure. And the government's failure to buy Orange Book-tested products, which were often out of date after years of testing, was a blow to vendors that invested huge sums in the Orange Book evaluations.

Figure 2 Common criteria EAL Levels (see online version for colours)



PP defines a standard set of security requirements for a specific type of product, e.g., operating systems (OS), databases, firewalls, etc. (CCEVS, 2008). These profiles form the basis for the CC evaluation. By listing required security features for product families, the CC allows products to state conformity to a relevant PP. During CC evaluation, the product is tested against a specific PP, providing reliable verification of the security capabilities of the product. Since technology enabled products can be linked to specific PPs, customers can compile a list of critical security features by examining the details of a relevant PP. In addition, since the CC certification verifies that a product meets the requirements of a PP. Customers can rapidly assess the product's ability to meet their security needs, and compare the security capabilities of any validated products.

A security target (ST) contains the IT security objectives and requirements of a specific identified TOE and defines the functional and assurance measures offered by that TOE to meet stated requirements. Unlike the PP, ST is more product-specific as it is used as a basis for agreement between developers, evaluators and sometimes consumers on the TOE security properties. ST answers the question of 'what I have to offer' from the point of view of product vendors, developers or integrators. The content of an ST is an extension to that of a PP. The additional information is TOE summary specification (TSS) and statement of conformance to one PP or more. The TSS describes TOE security functions and its assurance measures. Any PP conformance claims must be complete as no partial conformant is permitted for CC evaluation. The underlying requirement is such that an ST has a clear, complete and unambiguous content. This is to ensure ST evaluation can be carried out.

TOE is an enabled technology product or system, which is subject to an evaluation (CCEVS, 2008). TOE includes all material like documentation and administrator guides that are delivered with it. TOE might not be a full system or product as it could be referring to only a particular module or part of it. The security features in a TOE would be corresponding to the requirements as claimed in a ST in the case of a vendor. It could also be addressing the requirements put forth by a PP from a consumer point of view.

3 Navy IA processes

The DoN begins its IA programme with a definition of roles and responsibilities within the organisation. Daryl Edgar's article depicts the need for a security compliance programme (Dodson-Edgars, 2002). His survey found, "Companies with a compliance

program have the opportunity to greatly reduce penalties for violations of almost all federal statutes. Companies are expected to exercise due diligence and be innovative in designing and implementing their own security programs" (Dodson-Edgars, 2002). This practice is vital to successful network defence and avoids liability for failing to exercise due care and diligence in protecting Navy assets and national security. All DoN entities must adhere to Secretary of the Navy (SECNAV) instruction 5239.1, the Navy IA Program Guideline. Under this instruction, the DoN Chief Information Office (CIO) is responsible for developing and disseminating the DoN's IA strategy and policy and coordinating IA within the DoN and with other DoD commands. The DoN CIO is also in charge of evaluating Navy enterprise and system level IA posture and performance and reporting to the SECNAV on the effectiveness of DoN IA activities. Under SECNAV 5239.1, the DoN CIO reports directly to the SECNAV and has the responsibility to ensure compliance with applicable IA requirements including the development and maintenance of a department-wide IA programme.

The Navy Deputy Chief Information Officer for Policy and Integration is designated as the Department of Navy Senior Information Assurance Officer (DoN Senior IA Officer). The DoN CIO focuses its efforts on the development of IA policy, strategy, tools, and oversight (Department of Navy, 2005). The DoN information management vision is to provide a joint environment that delivers information dominance to the US Navy (USN). The DoN CIO achieves that vision by ensuring that all personnel have the full and best use of world-leading information technology assets at their disposal. The DoD IA Strategic Plan is a joint, enterprise-wide effort to identify the major goals and objectives of DoN-wide IA efforts. The major goals of the DoN IA strategy are (Department of Navy, 2005):

- protect information
- defend systems and networks
- provide integrated IA situational awareness/IA command and control
- transform and enable IA capabilities
- create an IA-empowered workforce.

The DoN achieves its IA goals by deploying a team-centric approach. Each team is responsible for specific tasks to ensure IA practices are enforced and implemented correctly. The following outlines and describes each DoN IA team member:

- DoN Deputy CIOs: This team implements and enforces policies, standards, and procedures to ensure the DoN complies with DoD statutes, regulations, and directives.
- Chief of Naval Operations (CNO): The CNO is responsible for developing and implementing IA-related programmes and controls, ensuring that IA is incorporated throughout the system development lifecycle, assigning designated approval authorities (DAAs), providing enterprise-wide vulnerability mitigation solutions, and providing an incident reporting.

- Designated Approving Authority (DAA): The DAA is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. DAAs accredit IT system security postures throughout the system development lifecycle, and in accordance with risk-management principles.
- Certification Authority (CA): The CA is the official responsible for performing the comprehensive evaluation of the technical and non-technical security features and safeguards of an IT system, application, or network. This evaluation is made in support of the accreditation process to establish the extent that a particular design and implementation meets IA requirements. The CA is responsible for managing the certification process.
- Programme Manager (PM): The PM is the person who owns the business process and controls the funding for the system. The PM is the individual with overall responsibility for the system/application.
- IA Manager (IAM): The IAM is responsible for the IA programme within a command, site, system, or enclave. The IAM is responsible to the local IA command authority and DAA for ensuring the security of an IT system, and that it is approved, operated, and maintained throughout its life cycle in accordance with IT system security C&A documentation.
- IA Officers (IAOs): IAOs are responsible to an IAM for ensuring the appropriate operational IA posture is maintained for a command, organisation, site, system, or enclave. IAOs assist in creating accreditation packages. They implement and enforce system level IA controls in accordance with programme and policy guidance.

3.1 Risk assessment process

Once the roles and responsibilities are defined, the next step is identifying the risks involved in DoN operations. The DoN deploys an effective risk management programme to address the need for identifying potential problems before they occur so that the organisation can plan risk-handling activities and invoke them as needed across the life of the product or project. The DoN's risk management programme is a continuous, forward-looking process that is an important part of military and technical management processes. The DoN risk programme is implemented into three sectors:

1 risk management methodology

2 identifying and analysing risks

3 handling identified risks.

To begin identifying and analysing risks, the DoN executes risk assessments of enterprise systems. Stephen Cobb, contributing author of the *Computer Security Handbook*, 4th edition, defines risk assessments as:

> "Evaluation involving imagining what could go wrong, then estimating the chances of it actually happening. For each of the possible problems, the question of probability needs to be considered. In this way, the problems and their potential costs can be prioritised and an appropriate plan of action developed." (Cobb, 2006)

Executing risk assessments is a vital task to the successful implementation of an effective IA programme. The United States Government Accountability Office (USGAO) highlights this importance during an analysis of information security practices of leading organisations:

> "Risk assessments provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Since risks and threats change over time, it is important that organisations periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected." (Brock, 1999)

The DoN's risk assessment methodology helps identify, prioritise, mitigate and manage risk.

3.2 Risk assessment methodology

The Navy risk assessment methodology was developed by the Space and Naval Warfare Systems Center (SPAWAR). SPAWAR is the inventing, acquisition, and development command for new technology within the DoN (SPAWAR, 2002). The purpose of the SPAWAR risk management document is to define a process that will assist project managers to develop and execute a plan to identify project risks as early as possible and to periodically reassess and manage those risks (Cobb, 2007).

The first step in the DoN risk assessment process is identifying risks. A peer group is created for assessing risks against criticality. This group includes developer staff, government oversight, certification authority, and validation personnel. The peer group reviews system concept of operations, system requirements, schedules, and cost documents. After review, this team identifies the risks associated with developing, administrating, deploying, and maintaining the system being evaluated. With the risks of the programme identified, the next step is a deeper analysis of the identified risks. Peer group members amplify risks noting programme area, affected phases, risk area, and control source. The peer group reaches a consensus on each risk and assigns a person responsibility for the mitigation of risk (Cobb, 2007).

The next process step is to prioritise the risks into probability, impact, and impact time frames for each risk. This task is accomplished with use of SPAWAR's risk allocation software, Risk Radar. A Risk Radar report is generated which is analysed and adjusted by the system's risk group members. With risks prioritised, the risk board can research process improvement possibilities for the system and begin the next step in the risk assessment process, which is defining risk avoidance alternatives. Peer group meetings are held to determine what actions or decisions could be made that reduce the probability and/or severity of impact of key risks. Residual risk, which could not be avoided, is analysed to determine what risks are candidates for the development of a mitigation strategy. While all risks are discussed, risks with medium and high exposure ratings are the serious candidates for development of mitigation strategies. Mitigation strategies include possible delays in development, extra cost, and possible loss of features or overall system performance. The next step in the process is developing disaster recovery plan or SCP for identified medium and high risks.

3.3 Disaster recovery plans

The DoN recognises that risks and vulnerabilities have a likelihood of being exploited. In many cases, the last line of defence is the Navy disaster recovery plan. The *Disaster Recovery Journal* defines a DRP as, "management approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort (*Disaster Recovery Journal*, 2009). A review of standard DoN DRP will reveal insight into whether these plans perform their desired functions effectively.

3.4 System contingency plans (SCP)

The DoN, which views disaster recovery of ISs as a vital role to mission success, develops their DRPs as SCP. The SCP is developed in accordance with Navy directives OPNAVINST 5239.1C and SECNAVINST 5239.3 and primarily directed towards all DoN systems. The contingency plan satisfies the requirements of DoDI 8500.2 IA Control CODP-3 Disaster and Recovery Planning, which states that a disaster plan exists that provides for the smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity. Disaster recovery procedures include business recovery plans, SCP, facility disaster recovery plans, and plan acceptance.

In addition to the SCP, commands often reference the system operational sequencing system (SOSS) for contingency planning of non-security related casualties. This document defines procedures for systems equipment initialisation and restoration. It is used as a response to system casualties including equipment failure and power loss. Contingency plans are tested monthly and quarterly in respect to their critically to ensure that AIS controls are effective and function reliably during service interruptions. SCPs address plausible situations/conditions that must be recognised and understood by the commands to ensure DoN system integrity is never compromised. SCP recommends a course of action to be taken when dealing with events that could interfere with normal DoN enterprise operations. It discusses actions required to rapidly restore mechanisms soon after their functionality is interrupted. Actions within the SCP are recommendations only and are always subordinate to approved command procedures/policies. DoN enterprise users/maintainers are encouraged to identify additional scenarios and recovery actions, and include them in local command contingency planning and training activities.

3.5 SCP scope

The SCP is applicable to all DoN enterprises equipped surface ships and shore installations. The plan provides the DoN team and security administrators with information that will assist them in the maintenance of information processed by the enterprise in case of emergency. The security contingency plan is a supplement to and subordinate to the ship's existing contingency plan. The SCP assumes that installation sites have approved site contingency plan prepared in accordance with prevailing requirements. The shipboard plans explain the procedures to be followed in case of emergencies that could be encountered by a naval combat vessel. The shipboard contingency plan serves to inform users of overall emergency procedures. The assets referred within the SCP are treated as critical processes. The SCP uses responsibilities, strategies, and situations that may be encountered to breakdown key elements within

contingency process. The situations are based on risk resulting from possible unresolved threats from the site and system's business impact analysis and risk assessment.

3.6 SCP responsibilities

Secure and safe operation of the DoN enterprise system is the primary responsibility of the operators. The operators are required to notify the system administrator when suspected events arise which can compromise system functionality. The security administrator has the responsibility to assure that all classified aspects of the system are protected from compromise including the loading of unauthorised information to the system. This responsibility extends to occasions when normal system operation is interrupted. Assistance from the essential personnel is identified, as often other administrators are required because of the additional system operational capabilities possessed by this individual.

3.7 SCP strategy/methodology

The first responsibility of the DoN during execution of the SCP is the safety of the personnel. To that end, the SCP is subordinated to the shipboard contingency (or emergency) plan. However, the individuals responsible for control of classified material are also responsible for the prevention of the compromise of that material. That responsibility encompasses various DoN systems because they store classified information in the form of storage media such as removable hard disk drives. The primary strategy to protect the classified assets of the DoN enterprise is the use of physical protection. This is accomplished by providing a secure environment for housing the system. Access is limited to individuals with the proper security clearance or under escort by properly cleared individuals and is controlled at the door.

3.8 Action plan

Action plans lays out procedures for revival of systems after an outage has occurred. The action plan in five main categories:

- Category 1: physical damage. This section refers to risks associated to the physical protection and availability of systems. Recovery actions include supplemental locking mechanism or stationing of an appropriately cleared individual in the area.
- Category 2: system failure. System failures may be as simple as loss of a component or as drastic as the failure of the main processors or the loss of power to the system. Failures could affect or degrade the capabilities of the system as well as interfering with the mission.
- Category 3: security violations. Security violations can occur from a number of different circumstances, such as an administrators' misuse of privileges or an unauthorised user attempting to gain access.
- Category 4: backup operations. Backup operations as applied to this contingency plan represents maintaining copies of specific data and system information that can be used in the event the system must be reinstalled.

- Category 5: Restoration of lost services is only one step of the response process used by the DoN. Investigation into how the event occurred, the assailant mission, the source and the attack used are needed to ensure future attempts using the same signature are unsuccessful.

The ease of committing crimes using computers has prompted the DoN to develop procedures for the investigation and prosecution of computer crime against the US Navy. Traditional law enforcement practices are not adequate to handle the capture and prosecution of these electronic criminals.

The DoN networks hold classified information about our country's offensive and defensive weapons systems and other information critical to national security. This makes DoN networks a high value target for hackers and cyber terrorists. Once an attempt to penetrate a DoN network or system has occurred, a set of practices and procedures is needed to acquire the evidence needed to prosecute these offenders, forensics is this practice. Judy Robbins defines forensics as,

> "The application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud." (Robbins, 2006)

The DoN benefits from their internal investigative unit, the Naval Criminal Investigative Service (NCIS). NCIS created a special investigative division named Computer Crime Investigation Group (CCIG) to resolve investigations involving computer hardware and/or software. The CCIG has merged, as all Defense Criminal Investigative Organizations (DCIOs) have, with the DoD Cyber Crime Center (DC3). The DC3, in conjunction with the CCIG, has responsibility for investigating computer misdeeds for the DoN. To perform this intense investigation, it is important for the DoN as well as the DC3 to employ qualified personnel and keep these employees abreast of the newest evidence gathering and investigative procedures.

The DoN utilises vulnerability assessments as the foundation for developing security programmes for new and current systems deployed within its enterprise. A vulnerability assessment is the first step needed for system certification under DIACAP. The purpose of the DIACAP is for the DoD to certify and accredit ISs through an enterprise process for identifying, implementing, and managing IA capabilities and services. IA capabilities and services are expressed as IA controls. IA controls are maintained through a DoD-wide configuration control and management (CCM) process that considers the architecture and risk assessments that are conducted at DoD-wide, mission area (MA), DoD component, and IS levels (DoD, 2007). Once the vulnerability assessments are completed, the DoN commands deploy security assets to defend and/or mitigate identified vulnerabilities. One of the weapons deployed in the security battlefront is the intrusion detection system (IDS). An examination of the methodology used by the DoN for their assessments and how IDSs play a vital role in this organisation's network defense will expose their effectiveness in ensuring solid IA.

3.9 IA vulnerability assessment and methodology

The DoN's methodology for vulnerability assessment was created in a joint effort from the Defense Information Systems Agency and the Department of Energy. Vulnerability

assessments are authorised by local commands developing new systems or current systems which are in need of recertification under DIACAP rules. Systems under development are required to be certified within year of deployment and, upon certification, are required to hold yearly assessments to address new threats. The DoN methodology describes 10 elements or area of concerns during the assessment (Department of Energy, 2002):

1 Network architecture: This element provides an analysis of the IA features of the information network(s) associated with the organisation's critical ISs. Information examined should include network topology and connectivity (including subnets), principal information assets, interface and communication protocols, function and linkage of major software and hardware components (especially those associated with information security such as intrusion detectors), and policies and procedures that govern security features of the network.

2 Threat environment: This element includes a characterisation of threats, identification of trends in these threats, and ways in which vulnerabilities are exploited. To the extent possible, characterisation of the threat environment should be localised, that is, within the organisation's service area.

3 Penetration testing: The purpose of network penetration testing is to utilise active scanning and penetration tools to identify vulnerabilities that a determined adversary could easily exploit. Penetration testing can be customised to meet the specific needs and concerns of the command.

4 Physical security: The purpose of physical security assessment is to examine and evaluate the systems in place (or being planned) and to identify potential improvements in this area for the sites evaluated. This includes access controls, barriers, locks and keys, badges and passes.

5 Physical asset analysis: The purpose of the physical asset analysis is to examine the systems and physical operational assets to ascertain whether vulnerabilities exist.

6 Operations security: The OPSEC assessment reviews the processes and practices employed for denying adversary access to sensitive and non-sensitive information that might inappropriately aid or abet an individual's or organisation's disproportionate influence over system operation.

7 Policies and procedures: The objective of the policies and procedures assessment task is to develop a comprehensive understanding of how a facility protects its critical assets through the development and implementation of those documents.

8 Impact analysis: The purpose of the impact analysis is to help estimate the impact that outages could have on a command. Outages in electric power, natural gas, and oil can have significant financial and external consequences to a command.

9 Infrastructure interdependencies: The purpose of the infrastructure interdependencies assessment is to examine and evaluate the infrastructures (internal and external) that support critical facility functions, along with their associated interdependencies and vulnerabilities.

10 Risk characterisation: Risk characterisation provides a framework for prioritising recommendations across all task areas. The recommendations for each task area are judged against a set of criteria to help prioritise the recommendations and assist the organisation in determining the appropriate course of action. It provides a framework for assessing vulnerabilities, threats, and potential impacts.

These ten elements combine to give the DoN a complete analysis of their security vulnerabilities and priority of mitigation. One of the steps of mitigation will include the deployment of security resources to combat threats identified during the assessment. One of the main tools used by the DoN is IDSs.

3.10 IA enabled product review: intrusion detection systems (IDSs)

An IDS monitors' network traffic, monitors for suspicious activity, and alerts the system or network administrator. IDS respond to malicious traffic by taking action such as blocking the user or source IP address from accessing the network or notifying network management for further action. The DoN deploys mostly Network IDSs, which scan all inbound and outbound traffic from strategic perimeter points on the network. For critical systems, Host IDS (HIDS) are installed. HIDS run on individual hosts or devices on the network. They monitor the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected. DoN IDSs are administrated locally and monitored by the Navy's Network Information Operations Command (NIOC), which gathers the DoN security information to predict the Navy's overall security posture. Attacks against the US military have dramatically increased within the past few years. With country's now using cyber warfare to conduct information theft, espionage, and denial of service attacks, the DoN must stay ahead of its adversaries by deploying the latest technology to fight new challenges on the road ahead.

4 Results and demographic breakdown

RQ1 Is there a common theme amongst the certification and accreditation (C&A) processes?

After review of common processes in the various C&A process the following themes were revealed:

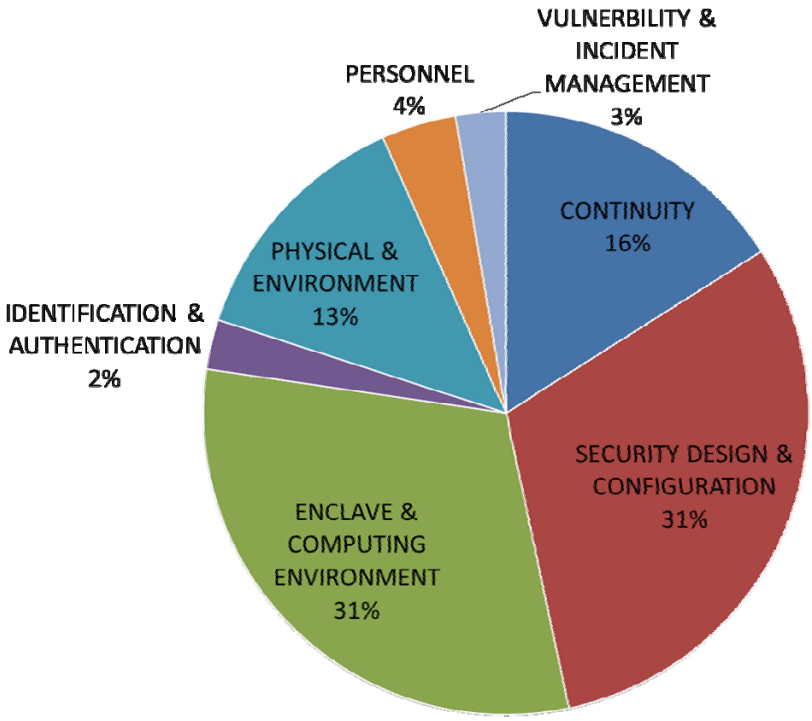
- product/system definition
- identification of applicable IA controls
- extensive documentation of product/system architecture
- initial C&A review
- external testing/evaluation for product/system accreditation
- recertification.

RQ2 Are there IA controls that are applicable to IA enabled products and systems?

A review of the Appendix C: DIACAP Scorecard totalled 75 IA controls. These controls are broken down in the following; 12 IA controls for continuity, 23 IA controls for

security design and configuration, 23 IA controls for enclave and computing environment, 2 IA controls for identification and authentication, 10 IA controls for physical and environment, 3 IA controls for personnel, and 2 IA controls for vulnerability and incident management. Figure 3 displays a graphical breakout of DIACAP IA controls.

Figure 3 DIACAP IA control breakdown for MAC III public (see online version for colours)



Note: Percentage is based upon a total of 75 IA controls.

To determine the percentage of controls that were necessary all 75 were measured against two criteria. The first criterion was against requirements for products and the second criterion was against requirements for systems. The first criterion, which was Criteria A, determined if the DIACAP IA control was necessary for development and fielding of the product. The second criterion, which was Criteria B, determined if the DIACAP IA control was necessary for development and fielding of the product. This part of the study was conducted utilising (U) documents available that was used during C&A events within the last five years. Additionally 40 active experts in the field of IA were used to select the appropriate IA controls that mapped. This data is available upon request. Table 1 displays the only the items that were applicable not applicable to both products or systems.

The result of this study was that 84% of the total DIACAP IA requirements were applicable to both products and systems. The expected result was 24% higher than expected. For further information see Appendix F: DIACAP IA Mapping of Products vs. Systems which contains the results of this portion of the research study.

Table 1 IA controls that were only applicable to product or systems

IA control number	*IA control name*
COAS-1	Alternate site designation
CODP-1	Disaster and recovery planning
COED-1	Scheduled exercises and drills
PEEL-1	Emergency lighting
PEFD-1	Fire detection
PEFI-1	Fire inspection
PEFS-1	Fire suppression system
PEHC-1	Humidity controls
PEMS-1	Master power switch
PETC-1	Temperature controls
PETN-1	Environmental control training
PRMP-1	Maintenance personnel

4.1 Interesting findings

The interesting findings revolved around C&A similarities between difference C&A processes. The process for certifying products and systems were similar to include the IA controls. After reviewing Appendix C: DIACAP Scorecard it was evident that there were IA controls that directly applied to the product itself. The IA controls found within Appendix C: DIACAP Scorecard reference CC and other applicable C&A processes for IA enabled products. The only IA controls not applicable were those that were levied upon the facility and maintenance personnel. Thus it is possible for the development of one C&A process that incorporates systems and products for multiple organisations.

4.2 Importance of research

The importance of this research is provide practitioners and researchers an in depth understanding of the government C&A process that can be applied to government and commercial based systems. This research allows those unfamiliar with the government's process for securing systems to gain insight into the complicated process. Also it is essential for those who play a role within the DoD to take this data and apply it to both their systems and products,

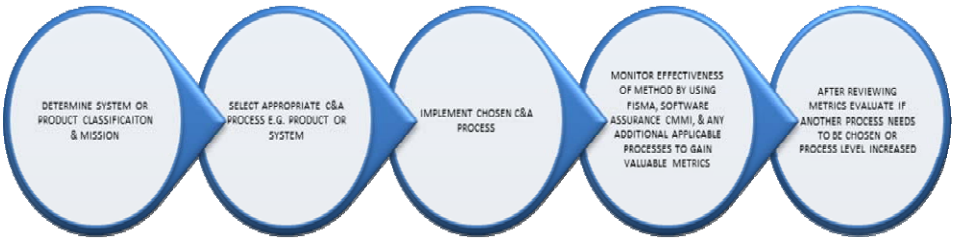
4.3 Recommendations

This research uncovers common themes between a few of the C&A processes utilised by the government. However as only the DoN was reviewed other organisations not under the DoD should be reviewed as well to see if there is truly a correlation between all the various C&A processes. This will show if there is significant redundancy between the organisations and the processes they utilise which could result in more robust C&A process.

4.4 Future research

Future research will incorporate taking the DoD IA controls and applying them appropriately to commercial systems. This will be of importance as commercial-based organisations should utilise these standards as a starting point or a method for measuring their IA posture. Organisations could significantly reduce and mitigate risks utilising proven standards for managing systems. The aim of this future research study shall provide applicable processes and standards to include providing a method for selecting necessary government models for systems development. The output of this research study will be an automated tool that allows the application of government IA controls to be applied to commercial systems based off the availability, integrity, and confidentiality (AIC) of a system. Additionally a process similar to the ones described in this research shall be developed that allows commercial entities to C&A their systems. As Figure 4 displays a method in which these C&A processes can be evaluated in the future. This process should be researched to evaluate its effectiveness over multiple products and systems.

Figure 4 C&A evaluation process (see online version for colours)



5 Conclusions

This research has allowed for the mapping of product and system IA controls. This mapping can be utilised to ensure that products and systems are built with similar controls which would reduce overall costs to major defence programmes. Additionally, this research has found common themes found with the major C&A processes that could be utilised to develop a joint process. These findings should serve as the start of allowing DoD products and systems undergo a joint C&A process at the MAC III (U) level.

References

Brock, J. (1999) 'Information security risk assessment practices of leading organizations', Director, USGAO [online] http://www.gao.gov/special.pubs/ai00033.pdf (accessed 20 March 2009).

Cobb, S. (2006) 'Risks and response: issues and attitudes' [online] https://norwich.angellearning.com/AngelUploads/Content/MSIA_LOR/_assoc/msia_s4/msia_s4_w02_2_comm/msia_s4_w02_cobb_lecture.pdf (accessed 1 June 2012).

Cobb, S. (2007) 'Risk analysis example' [online] https://norwich.angellearning.com/AngelUploads/Content/MSIA_LOR/_assoc/msia_s4/msia_s4_w02_2_comm/msia_s4_w02_cobb_lecture.pdf (accessed 20 March 2009).

Common Criteria Evaluation and Validation Scheme (CCEVS) (2008) 'Common criteria evaluation and validation scheme -- organization, management, and concept of operations (Version 2.0)', National Security Agency, National Information Assurance Partnership website [online] http://www.niap-ccevs.org/policy/ccevs/scheme-pub-1.pdf (accessed 20 March 2012).

Department of Defense (DoD) (2007) 'Dod information assurance certification and accreditation process (DIACAP) (DoDI 8510.01)', Assistant Secretary of Defense for Networks and Information Integration, Department of Defense Chief Information Officer [online] http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf (accessed 18 April 2012).

Department of Energy (2002) 'Vulnerability assessment methodology' [online] http://www.esisac.com/publicdocs/assessment_methods/VA.pdf (accessed 1 June 2012).

Department of the Navy (2005) 'Department of the Navy information assurance program (SECNAV M-5239.1)', The Department of Navy Chief Information Officer, Department of Navy [online] http://doni.daps.dla.mil/secnav manuals1/5239.1.pdf (accessed 20 March 2012).

Disaster Recovery Journal (2009) *Glossary* [online] http://www.drj.com/index.php?option=com_glossary&func=display&letter=All&Itemid=297&catid=35&page=1 (accessed 2 April 2009)

Dodson-Edgars, D. (2002) 'Due care in security management' [online] http://www.bizforum.org/whitepapers/dodson-edgars-2.htm (accessed 1 June 2012).

Robbins, J. (2006) 'An explanation of computer forensics' [online] http://www.computerforensics.net/forensics.htm (accessed 1 June 2012).

SPAWAR (2002) 'Risk management process', Systems Engineering Process Office [online] http://sepo.spawar.navy.mil/Risk_Management_Process.doc (accessed 1 June 2012).

Appendix A

Key definitions

- *Confidentiality:* Assurance that information is not disclosed to unauthorised individuals, processes, or devices.
- *Integrity:* Quality of an IS reflecting the logical correctness and reliability of the OS; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorised modification or destruction of information.
- *Availability:* Timely, reliable access to data and information services for authorised users.
- *Authentication:* Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorisation to receive specific categories of information.
- *Non-repudiation*: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Appendix B

Plan of action and milestones (POA&M) (see online version for colours)

[SYSTEM ACRONYM]
Quarter [Insert Current Quarter (A (Oct-Dec), B (Jan-Mar), C (Apr-Jun), D (Jul-Sep)]
Current FY (i.e. 2012)
Ongoing 3 Completed 0 Delayed 3

System Name	System Critically as defined by FIPS	Confidentiality	Availability	Integrity	If no weakness, provide a reason
"System SSA"	"HIGH, MED or LOW"	"HIGH, MED or LOW"	"HIGH, MED or LOW"	"HIGH, MED or LOW"	

Exhibit 300	Project ID (300)	Project Name	Exhibit 53	Project ID (53)	Security Costs	Accreditation Date (Actual or Scheduled YYYY-MM-DD)
"YES NO"	Required if Exhibit 300	SAMPLE SYSTEMS A	YES	Required For All Systems	"Enter $; required field"	"Enter C&A date"

ID	Weakness	POC	Resources Required	Scheduled Completion Date	Milestones With Completion Dates	Changes to Milestones	Identified in CFO Audit or other review?	Completion Date	Status	Comments	Risk Level	Weakness Severity
"SYSTEM ACRONYM_QTR_YYYY_WEAKNESS #"	"Selected Risk Description from final RMW"	"System Steward Name, Office Org"	"manhours or costs; indicate resource requirement i.e. new, reallocated or current."	"field cannot be changed once negotiated and agreed upon"	"include expected completion date with each milestone"	"When a corrective action is not completed as originally scheduled indicate new date."	"Identify the source of the audit, i.e. CFO, FISMA, RMW, etc. and include the date weakness was first identified; e.g., RMW dated 04-15-2005"	"MM DD YY 'Completed' means weakness has been fully resolved and tested"	"Completed, Delayed or Ongoing"	"Add additional detail for any previous entries"	"High, Medium, Low"	"Weakness, Significant Deficiency or Reportable Condition" - All will be reported as "Weakness" unless otherwise stated by the CISO
*SYS_A_2012_1	(CP-3 (2)) BCP training has not been conducted.	John Doe - CISO	(48 Total Manhours) 40 manhours - current	6/30/2005 (This should ONLY contain a date - no additional information)	(CP-3 (2)) Employ automated mechanisms to provide a more thorough and realistic training environment. (06/15/2005) (Ensure you put the completion date just as shown above for EACH milestone)		RMW dated 06/24/2012	8/30/2011	Completed		High	Weakness
*SYS_A_2012_2	(CP-7 (2)(3)(4)) Controls for the alternate processing site are not in compliance with NIST SP 800-53 requirements.	John Doe - CISO	80 Manhours		(CP-7 (2)) Identify potential accessibility problems at the alternate processing site. (06/15/2005)		RMW dated 06/24/2012	8/30/2011	Completed		Medium	Weakness

Appendix C

DIACAP scorecard

System Name	System Owner		IS Type
<Insert System Name Here>			
Designated Accrediting Authority (DAA)	Accreditation Status	Period Covered Accreditation Date ATD	Last Update
Certifying Authority (CA)	Certification Date	Mission Assurance Category (MAC) **MAC III**	Confidentiality Level (CL) **Public**

☐ MAC I, Classified ☐ MAC II, Classified ☐ MAC III, Classified
☐ MAC I, Sensitive ☐ MAC II, Sensitive ☐ MAC III, Sensitive
☐ MAC I, Public ☐ MAC II, Public ☒ MAC III, Public

IA Control Subject Area	IA Control Number	IA Control Name	Inherited?	C/NC/NA	Impact Code	Last Update
Continuity	COAS-1	Alternate Site Designation			Medium	
Continuity	COBR-1	Protection of Backup and Restoration Assets			High	
Continuity	CODB-1	Data Backup Procedures			Low	
Continuity	CODP-1	Disaster and Recovery Planning			Low	
Continuity	COEB-1	Enclave Boundary Defense			Medium	
Continuity	COED-1	Scheduled Exercises and Drills			Low	
Continuity	COEF-1	Identification of Essential Functions			Low	
Continuity	COMS-1	Maintenance Support			Low	
Continuity	COPS-1	Power Supply			Low	
Continuity	COSP-1	Spares and Parts			Low	
Continuity	COSW-1	Backup Copies of Critical Software			High	
Continuity	COTR-1	Trusted Recovery			High	
Security Design and Configuration	DCAR-1	Procedural Review			Medium	
Security Design and Configuration	DCAS-1	Acquisition Standards			High	
Security Design and Configuration	DCBP-1	Best Security Practices			Medium	
Security Design and Configuration	DCCB-1	Control Board			Low	
Security Design and Configuration	DCCS-1	Configuration Specifications			High	
Security Design and Configuration	DCCT-1	Compliance Testing			Medium	
Security Design and Configuration	DCDS-1	Dedicated IA Services			Medium	
Security Design and Configuration	DCFA-1	Functional Architecture for AIS Applications			Medium	
Security Design and Configuration	DCHW-1	HW Baseline			High	
Security Design and Configuration	DCID-1	Interconnection Documentation			High	
Security Design and Configuration	DCII-1	IA Impact Assessment			Medium	
Security Design and Configuration	DCIT-1	IA for IT Services			High	
Security Design and Configuration	DCMC-1	Mobile Code			Medium	
Security Design and Configuration	DCNR-1	Non-repudiation			Medium	
Security Design and Configuration	DCPD-1	Public Domain Software Controls			Medium	
Security Design and Configuration	DCPP-1	Ports, Protocols, and Services			Medium	
Security Design and Configuration	DCPR-1	CM Process			High	
Security Design and Configuration	DCSD-1	IA Documentation			High	
Security Design and Configuration	DCSL-1	System Library Management Controls			Medium	
Security Design and Configuration	DCSQ-1	Software Quality			Medium	
Security Design and Configuration	DCSR-1	Specified Robustness - Basic			High	
Security Design and Configuration	DCSS-1	System State Changes			High	
Security Design and Configuration	DCSW-1	SW Baseline			High	
Enclave and Computing Environment	EBBD-1	Boundary Defense			Low	
Enclave and Computing Environment	EBCR-1	Connection Rules			Medium	
Enclave and Computing Environment	EBPW-1	Public WAN Connection			High	
Enclave and Computing Environment	EBVC-1	VPN Controls			Medium	
Enclave and Computing Environment	ECAR-1	Audit Record Content			Low	
Enclave and Computing Environment	ECAT-1	Audit Trail, Monitoring, Analysis and Reporting			Low	
Enclave and Computing Environment	ECCD-1	Changes to Data			Medium	
Enclave and Computing Environment	ECIM-1	Instant Messaging			Medium	
Enclave and Computing Environment	ECLP-1	Least Privilege			High	
Enclave and Computing Environment	ECMT-1	Conformance Monitoring and Testing			Low	
Enclave and Computing Environment	ECND-1	Network Device Controls			Low	
Enclave and Computing Environment	ECPA-1	Privileged Account Control			High	
Enclave and Computing Environment	ECPC-1	Production Code Change Controls			Medium	
Enclave and Computing Environment	ECRG-1	Audit Reduction and Report Generation			Low	
Enclave and Computing Environment	ECRR-1	Audit Record Retention			Medium	
Enclave and Computing Environment	ECSC-1	Security Configuration Compliance			High	
Enclave and Computing Environment	ECSD-1	Software Development Change Controls			Medium	
Enclave and Computing Environment	ECTM-1	Transmission Integrity Controls			Medium	
Enclave and Computing Environment	ECTP-1	Audit Trail Protection			Medium	
Enclave and Computing Environment	ECVI-1	Voice over IP			Medium	
Enclave and Computing Environment	ECVP-1	Virus Protection			High	
Enclave and Computing Environment	ECWM-1	Warning Message			Low	
Enclave and Computing Environment	ECWN-1	Wireless Computing and Networking			High	
Identification and Authentication	IAKM-1	Key Management			Medium	
Identification and Authentication	IATS-1	Token and Certificate Standards			Medium	
Physical and Environmental	PEEL-1	Emergency Lighting			Low	
Physical and Environmental	PEFD-1	Fire Detection			High	
Physical and Environmental	PEFI-1	Fire Inspection			Medium	
Physical and Environmental	PEFS-1	Fire Suppression System			Medium	
Physical and Environmental	PEHC-1	Humidity Controls			Medium	
Physical and Environmental	PEMS-1	Master Power Switch			High	
Physical and Environmental	PESL-1	Screen Lock			Medium	
Physical and Environmental	PETC-1	Temperature Controls			Low	
Physical and Environmental	PETN-1	Environmental Control Training			Low	
Physical and Environmental	PEVR-1	Voltage Regulators			High	
Personnel	PRMP-1	Maintenance Personnel			High	
Personnel	PRNK-1	Access to Need-to-Know Information			High	
Personnel	PRRB-1	Security Rules of Behavior or Acceptable Use Policy			High	
Vulnerability and Incident Management	VIIR-1	Incident Response Planning			Medium	
Vulnerability and Incident Management	VIVM-1	Vulnerability Management			Medium	

Appendix D

Systems identification plan (SIP) (see online version for colours)

<Insert System Name Here>

1	System Identification:	
2	System Owner:	
3	Governing DoD Component IA Program:	
4	System Name:	
5	Acronym:	
6	System Version or Release Number:	
7	System Description:	
8	DIACAP Activity:	
9	System Life Cycle Phase:	
10	System Acquisition Phase:	
11	IA Record Type:	
12	Mission Criticality:	
13	Accreditation Vehicle:	
14	Additional Accreditation Requirements:	
15	ACAT Category:	
16	Governing Mission Area:	
17	Software Category:	
18	MAC Level:	
19	Confidentiality Level:	
20	Accreditation Status:	
21	Certification Date:	
22	Accreditation Documentation:	
23	Accreditation Date:	
24	Authorization Termination Date:	
25	DIACAP Team Roles, Member Names, and Contact Information:	See Table Below.
26	Privacy Impact Assessment Required:	
27	Privacy Act System of Records Notice Required:	
28	E-Authentication Risk Assessment Required:	
29	Annual Security Date of Annual Security Review:	
30	System Operation:	
31	Contingency Plan Required:	
32	Contingency Plan Tested:	

DIACAP Team Roles, Member Names and Contact Information			
	Name	Phone	Email
PM/SM:			
IAM:			
User Representative:			
CA:			
DAA:			
SIAO:			
CIO:			
SME:			

Appendix E

DIACAP implementation plan (DIP)

System Name	Mission Assurance Category (MAC)	Confidentiality Level (CL)
<Insert System Name Here>	**MAC III**	**Public**

☐ MAC I, Classified ☐ MAC II, Classified ☐ MAC III, Classified
☐ MAC I, Sensitive ☐ MAC II, Sensitive ☐ MAC III, Sensitive
☐ MAC I, Public ☐ MAC II, Public ☉ MAC III, Public

Assigned IA Control	Implementation Status				Responsible Entities	Resources	Estimated Completion Date	Comments
	N/A	Inherited	Implemented	Planned				
COAS-1								
COBR-1								
CODB-1								
CODP-1								
COEB-1								
COED-1								
COEF-1								
COMS-1								
COPS-1								
COSP-1								
COSW-1								
COTR-1								
DCAR-1								
DCAS-1								
DCBP-1								
DCCB-1								
DCCS-1								
DCCT-1								
DCDS-1								
DCFA-1								
DCHW-1								
DCID-1								
DCII-1								
DCIT-1								
DCMC-1								
DCNR-1								
DCPD-1								
DCPP-1								
DCPR-1								
DCSD-1								
DCSL-1								
DCSQ-1								
DCSR-1								
DCSS-1								
DCSW-1								
EBBD-1								
EBCR-1								
EBPW-1								
EBVC-1								
ECAR-1								
ECAT-1								
ECCD-1								
ECIM-1								
ECLP-1								
ECMT-1								
ECND-1								
ECPA-1								
ECPC-1								
ECRG-1								
ECRR-1								
ECSC-1								
ECSD-1								
ECTM-1								
ECTP-1								
ECVI-1								
ECVP-1								
ECWM-1								
ECWN-1								
IAKM-1								
IATS-1								
PEEL-1								
PEFD-1								
PEFI-1								
PEFS-1								
PEHC-1								
PEMS-1								
PESL-1								
PETC-1								
PETN-1								
PEVR-1								
PRMP-1								
PRNK-1								
PRRB-1								
VIIR-1								
VIVM-1								

Appendix F

DIACAP IA mapping of products vs. systems (see online version for colours)

IA Control Subject Area	IA Control Number	IA Control Name	CRITERIA A [PRODUCTS]	CRITERIA B [SYSTEMS]	Impact Code
Continuity	COAS-1	Alternate Site Designation			Medium
Continuity	COBR-1	Protection of Backup and Restoration Assets			High
Continuity	CODB-1	Data Backup Procedures			Low
Continuity	CODP-1	Disaster and Recovery Planning			Low
Continuity	COEB-1	Enclave Boundary Defense			Medium
Continuity	COED-1	Scheduled Exercises and Drills			Low
Continuity	COEF-1	Identification of Essential Functions			Low
Continuity	COMS-1	Maintenance Support			Low
Continuity	COPS-1	Power Supply			Low
Continuity	COSP-1	Spares and Parts			Low
Continuity	COSW-1	Backup Copies of Critical Software			High
Continuity	COTR-1	Trusted Recovery			High
Security Design and Configuration	DCAR-1	Procedural Review			Medium
Security Design and Configuration	DCAS-1	Acquisition Standards			High
Security Design and Configuration	DCBP-1	Best Security Practices			Medium
Security Design and Configuration	DCCB-1	Control Board			Low
Security Design and Configuration	DCCS-1	Configuration Specifications			High
Security Design and Configuration	DCCT-1	Compliance Testing			Medium
Security Design and Configuration	DCDS-1	Dedicated IA Services			Medium
Security Design and Configuration	DCFA-1	Functional Architecture for AIS Applications			Medium
Security Design and Configuration	DCHW-1	HW Baseline			High
Security Design and Configuration	DCID-1	Interconnection Documentation			High
Security Design and Configuration	DCII-1	IA Impact Assessment			Medium
Security Design and Configuration	DCIT-1	IA for IT Services			High
Security Design and Configuration	DCMC-1	Mobile Code			Medium
Security Design and Configuration	DCNR-1	Non-repudiation			Medium
Security Design and Configuration	DCPD-1	Public Domain Software Controls			Medium
Security Design and Configuration	DCPP-1	Ports, Protocols, and Services			Medium
Security Design and Configuration	DCPR-1	CM Process			High
Security Design and Configuration	DCSD-1	IA Documentation			High
Security Design and Configuration	DCSL-1	System Library Management Controls			Medium
Security Design and Configuration	DCSQ-1	Software Quality			Medium
Security Design and Configuration	DCSR-1	Specified Robustness - Basic			High
Security Design and Configuration	DCSS-1	System State Changes			High
Security Design and Configuration	DCSW-1	SW Baseline			High
Enclave and Computing Environment	EBBD-1	Boundary Defense			Low
Enclave and Computing Environment	EBCR-1	Connection Rules			Medium
Enclave and Computing Environment	EBPW-1	Public WAN Connection			High
Enclave and Computing Environment	EBVC-1	VPN Controls			Medium
Enclave and Computing Environment	ECAR-1	Audit Record Content			Low
Enclave and Computing Environment	ECAT-1	Audit Trail, Monitoring, Analysis and Reporting			Low
Enclave and Computing Environment	ECCD-1	Changes to Data			Medium
Enclave and Computing Environment	ECIM-1	Instant Messaging			Medium
Enclave and Computing Environment	ECLP-1	Least Privilege			High
Enclave and Computing Environment	ECMT-1	Conformance Monitoring and Testing			Low
Enclave and Computing Environment	ECND-1	Network Device Controls			Low
Enclave and Computing Environment	ECPA-1	Privileged Account Control			High
Enclave and Computing Environment	ECPC-1	Production Code Change Controls			Medium
Enclave and Computing Environment	ECRG-1	Audit Reduction and Report Generation			Low
Enclave and Computing Environment	ECRR-1	Audit Record Retention			Medium
Enclave and Computing Environment	ECSC-1	Security Configuration Compliance			High
Enclave and Computing Environment	ECSD-1	Software Development Change Controls			Medium
Enclave and Computing Environment	ECTM-1	Transmission Integrity Controls			Medium
Enclave and Computing Environment	ECTP-1	Audit Trail Protection			Medium
Enclave and Computing Environment	ECVI-1	Voice over IP			Medium
Enclave and Computing Environment	ECVP-1	Virus Protection			High
Enclave and Computing Environment	ECWM-1	Warning Message			Low
Enclave and Computing Environment	ECWN-1	Wireless Computing and Networking			High
Identification and Authentication	IAKM-1	Key Management			Medium
Identification and Authentication	IATS-1	Token and Certificate Standards			Medium
Physical and Environmental	PEEL-1	Emergency Lighting			Low
Physical and Environmental	PEFD-1	Fire Detection			High
Physical and Environmental	PEFI-1	Fire Inspection			Medium
Physical and Environmental	PEFS-1	Fire Suppression System			Medium
Physical and Environmental	PEHC-1	Humidity Controls			Medium
Physical and Environmental	PEMS-1	Master Power Switch			High
Physical and Environmental	PESL-1	Screen Lock			Medium
Physical and Environmental	PETC-1	Temperature Controls			Low
Physical and Environmental	PETN-1	Environmental Control Training			Low
Physical and Environmental	PEVR-1	Voltage Regulators			High
Personnel	PRMP-1	Maintenance Personnel			High
Personnel	PRNK-1	Access to Need-to-Know Information			High
Personnel	PRRB-1	Security Rules of Behavior or Acceptable Use Policy			High
Vulnerability and Incident Management	VIIR-1	Incident Response Planning			Medium
Vulnerability and Incident Management	VIVM-1	Vulnerability Management			Medium

Cutting-edge Technologies in Higher Education

Emerald Book Chapter: Use of Open Source Software and Virtualization in Academia to Enhance Higher Education Everywhere

Maurice Eugene Dawson, Imad Al Saeed

USE OF OPEN SOURCE SOFTWARE AND VIRTUALIZATION IN ACADEMIA TO ENHANCE HIGHER EDUCATION EVERYWHERE

Maurice Eugene Dawson Jr. and Imad Al Saeed

ABSTRACT

As costs around the world continue to rise for education, institutions must become innovative in the ways they teach and grow students. To do this effectively, professors and administrative staff should push toward the utilization of Open Source Software (OSS) and virtual tools to enhance or supplement currently available tools. In developing countries, OSS applications would allow students the ability to learn critical technological skills for success at small fraction of the cost. OSS also provides faculty members the ability to dissect source code and prepare students for low-level software development. It is critical that all institutions look at alternatives in providing training and delivering educational material regardless of limitations going forward as the world continues to be more global due to the increased use of technologies everywhere. Doing this could provide a means of shortening the education gap in many countries. Through reviewing the available technology, possible

Increasing Student Engagement and Retention using Immersive Interfaces: Virtual Worlds, Gaming, and Simulation
Cutting-edge Technologies in Higher Education, Volume 6C, 283–313

ISSN: 2044-9968/doi:10.1108/S2044-9968(2012)000006C013

implementations of these technologies, and the application of these items in graduate coursework could provide a starting point in integrating these tools into academia. When administrators or faculty debate the possibilities of OSS, gaming, and simulation tools, this applied research provides a guide for changing the ability to develop students that will be competitive on a global level.

INTRODUCTION

This book chapter will cover the utilization of virtualization, Open Source Software (OSS), and simulation tools that are also OSS. OSS can be defined as software that is made available in source code form. This is important as this source code may fall under the General Public License (GPL) which is a widely used free software license that is managed under the GNU Not Linux (GNU) Project (GNU, 2007). Virtualization is important as this is an effective method to reproduce system learning environments as a virtual instance reducing the overall hardware footprint and need to for a massive lab. This chapter will also cover two simulation tools to include correlating published research on how these items were integrated into graduate systems engineering coursework.

VIRTUALIZATION

In terms of virtualization, there are available tools to create a virtual version of a system. In terms of educational resources this provides a method for institutions to train on virtual machines (VMs). This allows a university to teach students complex techniques to computer science, engineering, or information technology (IT) such as networking, programming, system administration, and Information Assurance (IA). There are multiple types of virtualization such as hardware, desktop, memory, storage, data, and network. In Fig. 1 displayed is a screenshot of Ubuntu 11.10 running in a VM on the Windows 7 desktop.

For institutions that would like the opportunity to provide a cloud-like environment, tools such as Oracle Virtual Box and Vmware Player provide that ability. However, it should be noted that new Linux distributions running that require GNOME 3 will have issues running on older hardware. With older hardware as a constrain, there are bare minimal Linux

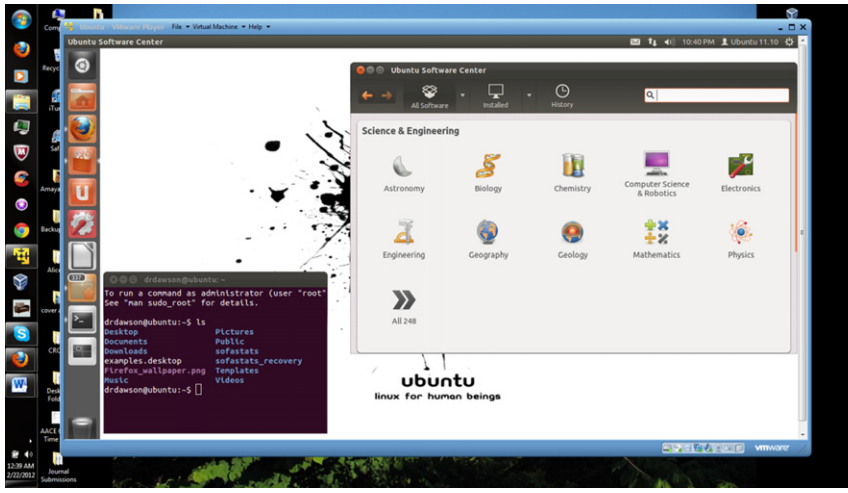


Fig. 1. Screenshot of Ubuntu VMware VM Running on Windows 7 Desktop.

distributions such as Puppy Linux and Damn Small Linux (DSL). VMs provide the ability for a student to experiment with hundreds of Operating Systems (OSs) without installing uninstalling the base OS.

Additionally, this allows for the creation of baseline OS images for classes. For example, a marketing course would have an OS created with all the software, case studies, etc. preloaded. This baseline OS for marketing would have statistics software, graphic design software, social marketing tools, case studies, eBooks, links to online course management tool, etc. This would allow an institution to have image ready for every class to ensure consistency, and that the students have all required tools needed. In the case for a more technical course such as software engineering, the students would have a baseline OS image with all the programming software, the integrated development environment (IDE), quality testing tools, etc. preloaded.

For professors, this virtualized environment would allow for the monitoring, distribution, and quicker deployment of available tools. This environment would be a cloud computing solution. Cloud computing is based on concepts of virtualization, distributed computing, and networking and is underpinned in the latest web and software technologies (Vouk, 2008). A useful definition of cloud computing is that it is a way of delivering applications as services over the Internet as well as a way of providing for the hardware and system software that act as platforms for these

applications and services (Armbrust et al., 2009). Cloud is also used to refer to a network of computers that are linked together and distribute processing capacity and applications to different systems (Johnson, Levine, & Smith, 2009). Cloud computing lets organizations add on to their IT and computing capacity without having to invest in new architecture, software, or hardware or in training and developing personnel (Glotzbach, Mordkovich, & Radwan, 2008). A cloud environment could prove to be a cost-effective implementation of which would allow for scalability if these right tools are utilized.

ADDING AND EXPANDING CAPABILITIES WITH LINUX

In terms of virtualization, the most cost-effective method is with the use of Linux as the OS. As institutions around the world look to provide their students and faculty with the ability to work in highly technical or large demand fields, it is imperative that all institutions have the ability to provide a simulated environment to teach the necessary concepts such as program management, design, and engineering. However, to do this at a fraction of the cost, Linux and other OSS are vital for implementation.

Why We Need to Consider Linux Essential in Higher Education

Linux is a Unix like OS that is built on the Linux kernel developed by Linus Torvalds with thousands of software engineers. As of 2012, there are over 200 active Linux distributions. The majority of the kernel and associated packages are free and OSS. This type of software provides a license that allows users the right to use, copy, study, change, and improve the software as the source code is made available. Providing source code allows developers or engineers to understand the inner workings of development. Imagine being able to study Mac or Windows by viewing all the source code to replicate similar developments. This exercise would be great for a developer to learn low-level coding techniques, design, integration, and implementation.

In terms of associated cost the majority of Linux distributions are free. However, some distributions require a cost for updates or assistance that related to specific needs such as OS modifications for server hosting. In software, there is a packet management system that automates the process

of installing, configuring, upgrading, and removing software packages from an OS. In the Linux OS builds, the most common packet management systems are Debian, Red Hat Package Manager (RPM), Knoppix, and netpkg. Below are a list of some Linux distribution and potential uses in education (Table 1).

Other countries are supporting the OSS movement as well. In China, Red Flag Linux commands over 30 percent of the market (Pan & Bonk, 2007). China is actively looking for an OS to combat Windows OS, thus the momentum for OSS continues to grow. In Russia, Linux may become a national OS by 2015 as they are as well looking for lower cost solutions in all levels of education. The Edubuntu OS, which has roots in South Africa, is being utilized by the Republic of Macedonia in all K-12 schools. With software packages such as LibreOffice students and faculty have the ability to perform similar functions as those found in the Microsoft Office suite without having to spend any money to obtain the software (Fig. 2).

Since the early 2000, there has been significant encouragement for the use of Linux in the Spanish public school system (Munoz et al., 2012). This use has been at the K12 level; however, the university level has yet to fully integrate this technology into the classroom. However, in a survey conducted by Accenture over 300 large blue chip organizations utilize OSS (Accenture, 2010). This indicates that there is a growing need for organizations to have employees familiar with OSS tools for development to include those for management.

OSS to Assist with the Development of Project Management Concepts and Tools

The need and presence of project management knowledge has developed to become a necessity in many organizational industries, while project management methods, processes, and certifications have become accepted standards in many industries (PMI, 2010). In 2008, *Global Knowledge* and *Fortune Magazine* listed project management in their top 10 career of choice, while in a recent salary survey conducted by ZDNET's Tech Republic organization, the PMP (Project Management Professional) certification was listed as the highest paying certification to have in the technology industry, while other project management certifications governed by the International Project Management Association (CPD, CPM) and Office of Government Commerce (PRINCE2) are highly sought after in European industries.

Table 1. Linux Distributions and Potential Uses.

Linux Distributions	Description and Potential Use	Packet Management System
Ubuntu	One of the most popular Linux OS developed to be a complete OS that can be an easily replaced for other comparable OSs	Debian-based
Edubuntu	OS targeted for grades K12. Contained in OS are tons of software applications that are useful to those who are education majors	Debian-based
Damn Small Linux	This OS is designed as a small OS to be utilized on older hardware. This OS is great for institutions that have old computers and want to revitalize them for use. OS is also great for VMs as DSL requires a low amount of memory	Knoppix-based
BackTrack	OS based on Ubuntu for digital forensics and penetration testing. Great tool for students majoring in technology fields. As cyber security is becoming a hot topic around the world, this tool provides students the ability to learn from over 30 software applications that aid in penetration testing and more	Debian-based
Fedora	This OS is supported by the Fedora Project and sponsored by Red Hat. This OS provides a great resource for learning Red Hat Enterprise Language (RHEL). As there are thousands of jobs requiring expertise specifically with Red Hat, this OS is a great tool to prepare students for employment in IT. Fedora has over six Fedora Spins such as Design-suite, Scientific-KDE, Robotics, Electronic-lab, Games, and more	RPM-based
CentOS	This OS is derived entirely from RHEL. The source code is developed from Red Hat, which allows a student to learn RHEL with a small number of differences. CentOS can be used for teaching IT students on how to set up, administer, and secure a server	RPM-based
Ubuntu Studio	This OS is derived from Ubuntu. This OS is developed specifically for multimedia production such as audio, video, and graphics. Departments for multimedia could use this OS for multimedia instruction and the development of projects. As many of the tools for multimedia production are expensive, this alleviates large license costs for institutions	Debian-based

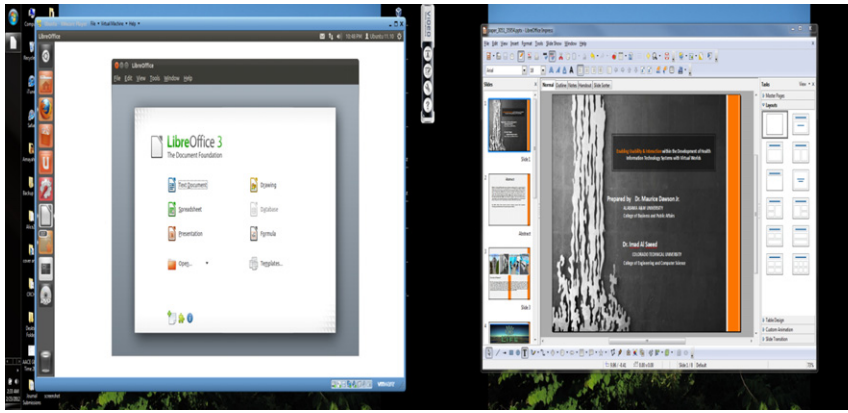


Fig. 2. LibreOffice Running in VMware Virtual Machine.

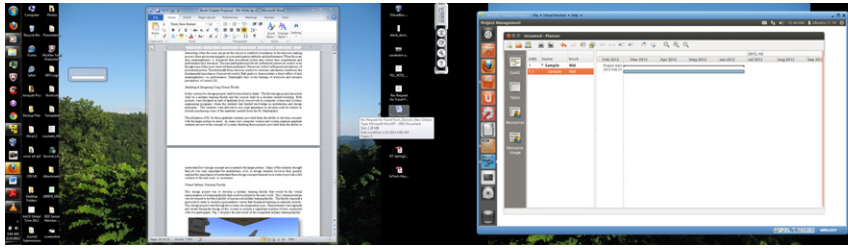


Fig. 3. OSS Project Management Tool Project Planner.

Communication and IT has also developed rapidly within this decade. With the enhanced role of IT, project managers must also prepare themselves to face the challenges of the future, both in the industry of project management as a whole and in the IT sector in particular. The increasingly important role of IT is undoubtedly the effect of rapid globalization that requires companies to have a larger capacity, timelier and more accurate information management within their decision-making system.

In project management part of a project manager's toolkit is the Microsoft Office Project software suite. One of the many available OSS is Project Planner which allows the creation of Gant Charts, ability to manage resources, and ability to track tasks created. Using Linux-based software allows institutions and organizations to teach this critical skillset at a fraction of the cost (Fig. 3).

Additional OSS tools that are present can be found on websites such as Open Source as Alternative (OSALT), which provides open source alternatives for items such as Microsoft Windows Suite, Araxis Merge, Bea Weblogic Server, and more (OSALT, n.d.).

DESIGN COLLABORATION WITH LINUX

In many graduate and undergraduate programs, institutions teach techniques for collaboration and system processes such as the Capability Maturity Model Index (CMMI). In teaching these techniques, OSS is the perfect platform as one of the key pillars for development is essentially coloration. With websites such as SourceForge, there are over 3.4 million developers participating in the development of over 324,000 projects. With these projects there is a group of developers that develop, deploy, and maintain these projects. For institutions this provides a method for students to understand the Software Development Life Cycle (SDLC) first hand.

Teaching and Understanding SDLC with the Aid of OSS Tools

The success of OSS demonstrates the alternative form of software and systems development processes. Software development is undergoing a major change from being a fully closed software development process toward a more community driven OSS development process (Deshpande & Richle, 2008). As a significant number of the information system (IS), computer science, or systems engineering students worldwide need to understand the SDLC, the OSS environment provides a great opportunity to learn all facets of the lifecycle (ACM, 2008). The SDLC known as the Waterfall Method (Fig. 4) is composed of six key phases that entail completing one phase and moving to the next without going back to the previous phase in the development cycle. The first phase is the requirements phase. During this phase of developments requirements are gathered for development. This allows developers and customers to capture requirements such as software functionality to user authentication requirements. The second phase of the SDLC is the design phase. In this phase the requirements become design specifications and developers develop the system. In the third phase, which is implementation, systems and subsystems are integrated to

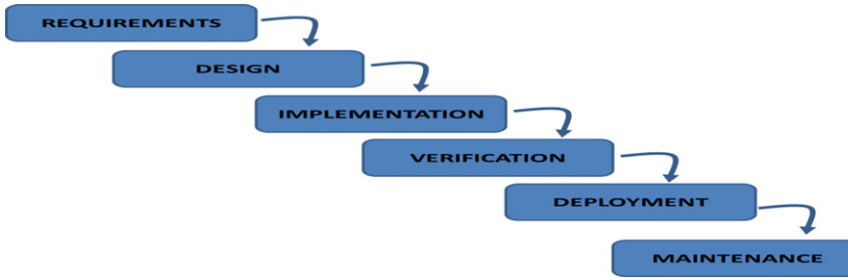


Fig. 4. SDLC Process.

function as an entire system. For example, a software application may be composed of multiple subsystems developed independently. At this phase they are integrated together for a final implementation of the system. In the four-phase verification, a final test of the software or system is conducted before the final release. In the fifth-state deployment the software application is installed after it has passed a rigorous check in the fourth stage. The last state is maintenance which consists of maintaining the software or system. It is important to also note that in this stage the decision to retire a software application or system is also made.

THE OPEN SOURCE LEARNING MANAGEMENT SYSTEM

Many studies suggest the traditional way of teaching, through books and static figures, appears to be inadequate in bringing across the complicated ideas of scientific concepts (Guimaraes & Murray, 2006). The current emerging media technology revolution supplemented the traditional face-to-face learning process with various e-learning communities as one of the fastest moving trends in today's education to assist in preparing the students for more in-depth in interactive instructional environments could lead to enhance their learning opportunities in both online and on ground mixed-learning courses (Cole & Foster, 2007; Ko & Rossen, 2004; Rice, 2007; Waterhouse, 2005). Institutions around the world used various commercial teaching and learning applications such as Blackboard (http://www.blackboard.com) and WebCT to provide 24/7 communications

between instructors and their learners. Those commercial applications could be very costly to buy their licensing.

In 2005, Munoz and Van Duzer mentioned that Humboldt State University paid approximately $8,600 for Blackboard license and they also pointed out that California State University system paid approximately 1 million dollars for licensing all the universities in the system. That could be huge amount of money for many institutes to licensing such educational systems. The best solution for such cost problem may lie in OSS (Wheeler, 2007). There are many open source programs available which are designed to solve numerous problems, but the most robust open source program is called Moodle.

Moodle is one of the most famous emerging media tools and widely known learning management systems (LMSs) in the U.S. universities, and other educational organizations (Martin-Blas & Serrano-Fernandez, 2009) used to develop a professional and more interactive educational (e-learning) environment especially for the higher education. Nowadays, Moodle comes as a first answer to the academic voracious demands for a professional and inexpensive tool for creating professional educational environment particularly by higher education and further education.

Moodle Overview

Moodle is one of the most user-friendly and flexible open source programs for electronic or e-learning (CoSN, 2010), identified as LMS, online interactive environment (OIE), and virtual learning environment (VLE) (Martin-Blas & Serrano-Fernandez, 2009), which has a large social framework of education support, and competitive alternative to many commercial applications. The word Moodle stands for "Modular Object-Oriented Dynamic Learning Environment, which is mostly useful to computer programmers".

Moodle was developed from the ground zero by Martin Dougiamas who has great experience in both education and computer science (Cole & Foster, 2007) as an innovative e-learning tool designed to assist educators to easy build and share their courses online. Moodle was developed as an alternative approach to costly systems available in the market. It has variety of features and a relatively quick learning curve make it very popular tool among U.S. universities for creating online dynamic web-based teaching, and learning environment could be used as a stand-alone online

teaching and learning environment or as a supplement tool to their face-to-face traditional courses.

Dougiamas made the decision to make Moodle a copyrighted open source model to allow users to use, modify, add features, and distribute software package without modifying or removing the original license and copyrights (Melton, 2008). Originally, Moodle was developed for Linux OS but currently it is compatible with various OSs such as Windows and Mac. The first version of Moodle (Ver 1.0) was released on August 20, 2002. After the first release, there were many programmers all over the world starting exploring and examining the Moodle code, adding and removing features, and fixing the possible bugs if available.

Currently, there are many universities all over the world that adopted Moodle to build custom educational environments for their courses. Table 2 shows the list of top 10 countries prepared from registered sites in 223 countries.

Within academic environments, instructors can build their course specifying their course settings including the course format, course title, starting date, finish date, etc. Instructors can use Moodle to create stand-alone online courses by managing web-based content for their courses including course segments, lessons, focused technology, and so on. Additionally, they can use it to complement their traditional courses to facilitate complex courses' concepts with limited face-to-face interaction, or they can use it to augment their traditional courses.

Moodle has many features including:

- easily managed courses;
- real-time collaboration and communication environment;

Table 2. Top 10 Countries Using Moodle (Moodle.com).

Country	Registrations
United States	12,710
Spain	6,558
Brazil	5,384
United Kingdom	4,199
Germany	3,011
Mexico	3,007
Portugal	2,259
Colombia	2,154
Australia	1,808
Italy	1,758

- simple integrated quizzes and easy grade books;
- unlimited class size;
- unlimited enrollments;
- unlimited number of courses per school; and
- unlimited number of courses per teacher in particular.

In addition, Moodle provides many benefits such as

- 24/7 access from anywhere in the world to its learning environment;
- Upload and download course material including audio, video, .doc, .docx, PDF, image, and so on;
- Link to resources anywhere on the Internet;
- Easily create rich courses without need to learn HTML knowledge;
- Access files/papers/resources by a computer;
- Provide the ownership to the course content;
- Manage course content from year to year and never lose any work;
- Handle secure payments through using PayPal.

System Requirements and Obtaining Moodle

In particular, Moodle needs the most recent version of PHP, web application (one programming language), and SQL database such as MySQL or PostgreSQL. These tools could be found in one open source OS called LAMP. LAMP stands for the Linux OS, the Apache web server, MyQSL, and PHP. In addition, Moodle should run an automated Cron process every 5 minutes or so (Melton, 2008). The host of the Moodle should include one. It is good to note that the Moodle website (http://docs.moodle.org/en/Install) has detailed information and complete instruction about how to install Moodle for the first time.

There are two options to obtain Moodle; the first option is that Moodle need to be downloaded and installed on a local installation on a personal server as part of a local network at the institution. This option could require highest maintenance. The second option is a remote hosting by a commercial web server. A user can contact one of the Moodle companies listed as a hosting at the Moodle services website (http://moodle.com). This process includes buying a domain name, and install Moodle software application on one of their servers (Melton, 2008). Those companies offered easy used tools for installing, upgrading, and maintenance. In this way, users will not have a highest amount of maintenance instead they will

have a mid of low-level amount of maintenance, but those companies will charge a fee for doing that.

Moodle Organization

Moodle could be set up according to its needs to deliver the information to the audience. For example, it could be used either as a networking environment or for handling course purposes. Instructors need to choose the format of the course by having only one screen that either contains the course material or consists of semester, term, or even year. In addition, the right and left sides of the main central course content could be arranged to include upcoming events, open forums, course members, latest news, search, recent and upcoming activities, etc. (Fig. 5). Moodle organization's layout could be edited by administrators who have skills with Hyper Text Markup Language or HTML code and cascading style sheet or CSS. In 2008, Melton explained Moodle setup items as follows.

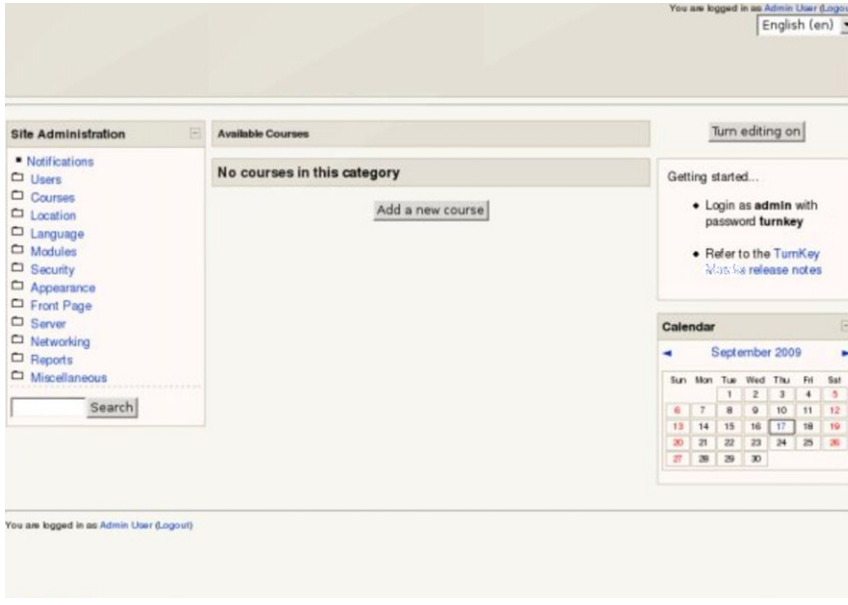


Fig. 5. Screenshot of Moodle Course Page.

Moodle organization's layout can be edited by administrators who have skills with HTML code and CSS. In 2008, Melton explained Moodle setup items as follows:

1. Forum: It is asynchronous module. Instructor can set up four types of forums such as standard forum, a question and answer forum, a forum for each member, and a forum for just one discussion. Instructor can use these entire forums to generate discussions, set for grading, assigning deadlines, attachment files, block attachment, email, and more.
2. Group: Instructor can make team tasks by combining a certain number of students to do a certain project(s) or any other course work. Instructor can hide the group work from other group and make it visible for the other group members by the end of the course. This allows students to learn how to work in virtual groups which according to a survey by Wainhouse, 72 percent of the respondents are more interested in alternatives to travel since the September 11, 2011 event (Wainhouse, 2002).
3. Grading: The latest version of Moodle allowed educators to assign grades for students and export the grades in different formats. These tool can be utilized to allow the student and the instructor to track progress throughout the course.
4. Assignment: Instructor can use this area to organize his course assignments in different ways and assign a specific deadline for submitting each assignment. Moodle allows students to submit their assignment in different formats such as text file, PDF file, Word document, and PowerPoint presentation, Excel sheet, pictures with various formats, etc.
5. Quiz: Instructor can set up their quizzes for each student individually or in groups. Instructor can open and close each quiz in specific day and time, send a customize feedback for each student, and so on. Quizzes can also be developed from a random test bank to minimize cheating.
6. Chat: It is a synchronous module for communication allowing the instructor to announce chat times, groups, and session logs. Student can use chat for real-time communication with or without their instructor for specific discussion issues. These chats can also be archived to be viewed at a later time to review the communication to ensure the message was understood or relayed appropriately.
7. Message: It provides both synchronous and asynchronous benefits. For example, a message window will pop up when the student change his web page during sending the message process. On the other hand,

a user will receive an email message in this registered email addresses when he is not online. Also, the user will see a pop-up message at the time he or she log in to the Moodle course.

8. Blog: A communication modules located on a user's profile. User can use their blogs for personal publications, read and write current entries' purpose, and access popular topics easily. The publications appear in reverse order, so the most recent post appears first.
9. Wiki: A communication module could be used in a different ways. Normally users use Wiki to collaborate with each other on coursework and projects. They can use it as a brainstorming session to exchange their thoughts about ascertaining subject. Wikis can also be exported to reside on a student's or professor's desktop. Wikis can serve a living document which can be updated at any time to include serving as configuration management systems for manuals or books.
10. Lesson: Instructor can use this module to prepare lessons in multimedia or PDF file forms. Also, the instructor can add questions to the content to check his or her understanding to the subject.
11. Glossary: This is very important module that can help the instructor to explain the difficult vocabulary word to the students and add new concept to the content to facilitate the concept of the course content.
12. Gathering feedback and data: Instructors can use this module to gather student's feedback and/or other types of data in three different ways: database, survey, and choice. This module can be exported for a review or to provide a synopsis of issues to administration.
13. Administration issues: Site administration panel contains many tools that allow the instructor to create and organize his course(s) with respect to the privacy and security issues. For example, they can create new courses and share them with the others and store them if necessary. In addition, they can make a manual or automatic backup for their courses including course data and student data (Melton, 2008).

Moodle has associated weakness. Moodle does not have the ability to reorganize courses into functional groups for each user. It only has a few related organizations by the topic of the current and previous courses and weekly course descriptions. The user would be blind and does not have the ability to see his courses' organization and could miss his opportunity to reorganize his courses.

Moodle does not have any link for advanced conferencing features such as a whiteboard conferencing feature. Sometimes chatting with the professors alone does not have the ability to convey the exact meanings like

visual information always do. So this facility allows the professor to visually share information in real time and allow the other students to watch the professor's movement and discuss with him.

Summary

The Moodle is great online learning software or course management system used by a wide variety of users and allows professors and students to conduct and participate in an electronic classroom. Students have the ability to post their discussion items, submit their assignments, and post journals and resources as attachments.

Moodle has a simple interface, uses a minimum of words, and includes simple icons with the words to aid users and show them the direction to where he can find the information they looking for.

REVIEW OF VIRTUAL WORLDS IN THE CLASSROOM

Emerging technologies offer exciting new teaching options for teachers and new learning options for students (Al Saeed, 2011a). For example, open source as one of the emerging media popular tools offered free innovative base to develop new teaching tools for instructors and new learning environment for students. In 2011, Dawson argued, "Simulation-based training provides many benefits to education, commercial, and military industries, allowing trainees to test and hone their skills in a safe virtual environment"(Dawson, 2011).

Financing could be the main driving forces behind utilizing open-source software development especially for the institutions of higher education (Miro International Pty Ltd, 2006; Wang, 2004; Rooij, 2007). Open-source virtual simulator software applications such as Second Life (SL) and Open Simulator (OpenSim) as one of the most popular virtual world environments might be considered as a potential solution to eliminate financial restrictions could face any higher education institution (Pan & Bonk, 2007). Al Saeed argues that "SL and Open Simulator (OpenSim) provide an opportunity to create innovation space educational simulations and allow students to become immersed in the learning process and help in convert them from passive to more active learners to become hand-on operators in more interactive environment. In other words, simulation

environment could be designed using emerging virtual technology for educational purpose such as space education purposes. It may turn students to be active leaners by engaging them in an immersive virtual environment" (Al Saeed, 2011a). University can easily access to source code, modify it, save the license fees could be chard by the vendor to develop and provide the institution with the flexible and cost efficient learning environments (Pavlicek, 2000; Weber, 2004; Williams, 2002).

Virtual world such as SL is a public utility for digital media that includes many features such as 3D graphics and simulation technology, text chat, voice chat (VOIP), and advance digital media for online collaborative courses and classrooms' environment.

Based on the emerging global distribution for web and computerized technologies, all types of virtual worlds were designed on the existing web standards to create a global virtual social network for socializing, messaging, media delivery, storage, and processing. It is an open and extensible platform that enables of Immersive education and distance for a wide range of variety students.

SL as one of the most popular virtual world provides a unique and secure teaching and learning environment for instructors and students. This learning environment could be designed to be private for a specific school where each avatar assigned to a unique name could include the name of the university, collage, or any other educational institution that the individual belongs to.

Many advances are incorporated into the design of such educational environment using virtual world such as SL. For example, the universities that host their own servers have complete control over who

1. Has access to their educational virtual worlds and has the ability to restrict access to those worlds at their discretion. For example, there were no anonymous access allowed for virtual worlds hosted on the Education Grid. Universities can also provide student rosters, and teacher rosters, from which authenticated avatars may be provisioned.
2. Has the ability to keep their virtual worlds for education private, or make them available to some other learners.
3. Has the ability to make separate copies of a virtual world simultaneously available for few levels of learners, where appropriate security measures are applied to enable students and teachers to work together in safe and secure learning environments.
4. Has to ability to have a single virtual world be utilized, simultaneously by multiple universities. Additionally each school can be provided with

Fig. 6. The Virtual Campus for Colorado Technical University.

its own private audio channel, which prevents lectures and discussions from being heard by anyone outside of that particular class.

Higher education technologists especially for those in the doctoral/research institutions utilized the efficiencies of open source. Colorado technical university is one of the first universities who realized the importance of using virtual worlds in teaching. They designed their own virtual campus as new teaching and learning environment in SL (Fig. 6). Additionally this institution has developed new degree programs at the graduate levels to teach emerging media and technology (Al Saeed, 2011b).

SL OSS Educational Competitor

One of the virtual world education grid competitors is OpenSim. OpenSim is an open source multi-user 3D application server designed by taking the advantage and make a reverse-engineering to the published application programming interface (API) functions and specific Linden Lab open source parts of the SL code. One of the strength for creating any virtual environment is making it accessible by a variety of users through using various protocols. OpenSim offers a great opportunity for the virtual world developers to create customized virtual worlds easily extensible through using the technologies that fit with their needs.

One of the weaknesses is that this kind of virtual worlds are susceptible to attacks by regular web clients. It is actually easier to copy assets with a

web-based client. The weakness is that asset servers are connected to the public Internet, and the protocol for interacting with them is public.

The Virtual World Education Grid will result in an improvement over the OpenSim because it has a great potential in language learning and teaching, projects turn out to be motivating both for the students and instructors, task-based activities are favored over other methodologies. On the other hand, OpenSim is high technological requirements and hard user interface compared to the virtual world grid.

Virtual World Educational Grid

Demand for online or non-traditional classes is increasing day after day. Technology is providing more tools in which schools can enhance performance of their learning model. The Virtual World Educational Grid is considered a free environment developed upon existing web standards in order to emerge a unique environment for virtual world delivery.

Virtual World Educational Grid has many powerful features including interactive and collaborative 3D graphics, game technology, audio, video, simulation technology, VoIP, text chatting, web cameras, and so forth with collaborative online course environments. The educators and students will fell themselves are physically attending a class session even that is not possible and that will cut any cost associated with attending class sessions in real world. Students from all over the world can communicate with each other in a way they can enhance their learning experience process. It will engage the instructors, educators, and students with the teaching and learning process in the same way they can collaborate within the traditional teaching and learning process. Virtual World Educational Grid supports individual-based learning process as well as group-based learning environments where the interactive lessons could inject into larger bodies of course material in order to enhance the education learning and teaching experience.

Identified Baseline Requirements

1. Accessible: The Virtual World Educational Grid should be designed in a way to be accessible to all users and institutes thought to previously set up a specific procedure and open usage policy, but also preserve the right to make the server private for events.

2. Open Application Programmer Interface functions and a portion of the code: The Virtual World Educational Grid should be flexible and extensible for virtual world developer to make customized virtual environments, and that would be possible by publishing open API functions, protocols, and a portion of Virtual World Education Grid code.
3. Open and interoperable file formats: Software configuration and files should be transferable to other environments and platforms with respect to the minimum hardware needed.
4. Open hosting with conformance and compatibility: The Virtual World Educational Grid should be designed with the relevant educational and operational standards to achieve the conformance and compatibility standards.
5. Support multiple content formats: The Virtual World Educational Grid should support 3D content in addition to other content formats such as gaming, audio, video, text, etc.
6. Quality control: The Virtual World Educational Grid content should be reviewed and categorized by using metadata in order to meet the standard and be accepted into the Virtual World Educational Grid. That includes qualitative analysis, rating, and tagging by educators, students, and expert people of the subject matter.
7. Security and privacy of the learning environments: Developing Virtual World Educational Grid requires variety levels of protection. Learning environments could be created with some levels of security and access procedures for those only who are authorized in order to provide safe and private learning environment for the learners.

UTILIZATION OF VIRTUAL WORLDS IN ACADEMIA

Currently, virtual worlds are widely used for training and education purposes to facilitate trainees' learning activities (de Freitas, 2008; Dobson et al. 2001; Granlund 2001; Robert et al. 1996). Virtual worlds allow users to create their own avatars, which are referred to their residents and offer them the platform they need to interact with each other easily. Virtual world is a playground for imagination and expands the boundaries of users' creativity in exploring, defining, creating, designing, modeling real environments, building, coding, document sharing and recording facilities, performing, and collaboration (Chen et al., 2008). Virtual worlds can be very effective and cost-efficient

environment that can provide a new methodological framework that supports training purposes to include serving as a tool for collaboration. Virtual worlds are a playground to simulate real-world applications for training purposes, but there is a chance it may not be able to simulate overall scenarios with small details that could be involved in real system because of the limitation boundaries of virtual worlds (Stolk et al., 2001). This chapter lays out the strategic use of virtual worlds for training purpose and provides a framework based on existing methodologies could be employed to facilitate modeling and testing process.

SL is an associated free client program known as the viewer which allows the users, known as residents, to interact with other individuals through avatars. Students created avatars which were representative of their personality and how they best felt to interact with other residents. This environment can be described as environments created by technology that have incorporated virtual representations of elements found in the real world (Kock, 2008). This course allowed students to develop virtual objects with limited knowledge of the Linden Scripting Language. As the Linden Scripting Language has syntax familiar with the C programming language, the students were able to jump right into developing scripts. Fig. 7 is an example of the Linden Scripting Language that would be utilized to have an object display text when they are five meters near the object. In terms of SL the most common method to gather information is through blogs and special journals as this knowledge base is constantly growing (Kern, 2009).

OpenSim is an OSS application that can be utilized to simulate virtual environments. This would allow architects and designers the freedom to develop their own virtual representation of an environment. However, an architect would need to have knowledge of the .net framework and programming in order to develop or modify items without any support. Furthermore, this competition not only developed a health care facility, but also created an entirely new vernacular by approaching this with SL virtual design capabilities. The introduction of a new form of instant communication beyond words and diagrams but in a full on demonstration of ideas creates a platform for creative designs. The implication of SL into competitions will provide user with a clear path to think creatively. The ideas can then overflow into a multi-faceted direct source, instead of just using one or two types of devices to demonstrate ones ideas, such as through email, telephones, video, or webcasting. The impact the SL has had will grow into a more influential design world.

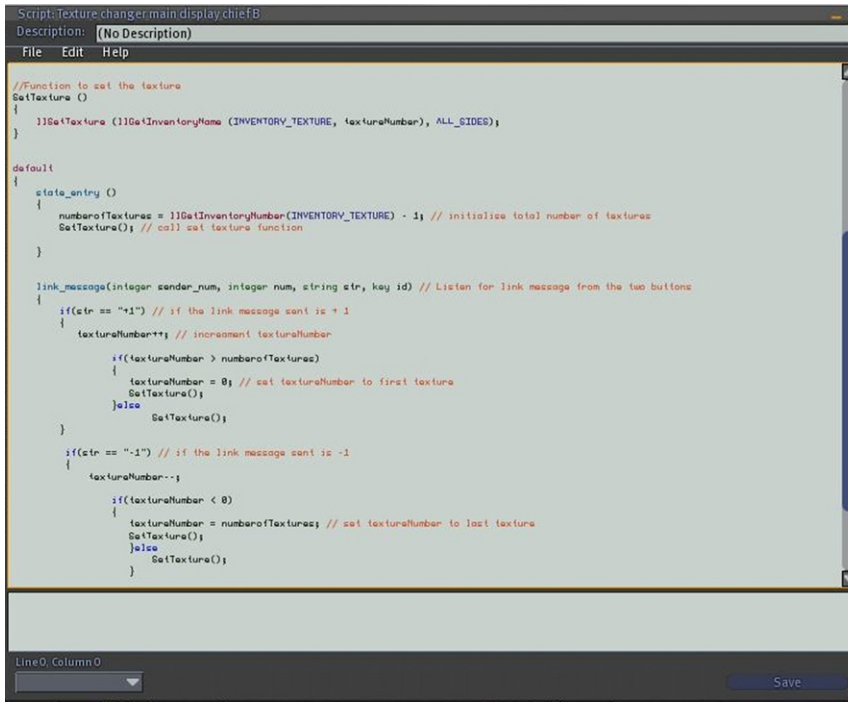


Fig. 7. Example of Second Life Linden Script.

University Graduate Projects Using Virtual Worlds

The introduction to Advanced Systems Engineering course at Morgan State University's School of Engineering graduate students participated in a group project that consisted of creating a virtual education center using SL, a virtual world developed by Linden Lab (Dawson, Burrell, & Emanuel, 2011). This project permitted students to apply their systems engineering concepts and skills learned as a result of the provided course materials (Dawson, Burrell, & Emanuel, 2011). The initiation of this course project was through a Request for Proposal (RFP) provided by the course professor who acted as the end customer. Displayed in Fig. 8 is a screenshot taken of the IEGR 501 SL Class during a live session in a virtual world during the Fall 2010 semester.

The goal of the virtual education center was to foster learning allowing for the development of engineering capabilities, and to hold large

Fig. 8. IEGR SL Class.

conferences of approximately 100 researchers. The land consisted of multiple regions. The first portion of the land was required to provide a large conference center that allowed authentication to occur for all entering personnel. The second portion of the island was to act as an engineering development ground. This development ground was to consist of objects available for testing. Also, in the engineering, development ground was a rapid prototyping center for developing many applications related to the present world. The third portion was to be a classroom environment for

three classes to be held simultaneously without hearing the other classroom during the lecture.

Throughout the semester, every student worked diligently to adhere and produce to the list of requirements proposed by the professor. Small groups were developed within the team to formulate a list of items needed and their pricing. The necessary items ranged from land to office equipment. After all of this preliminary research has taken place, the professor chose the most feasible items presented from each group, purchased them, and put together this virtual education center using SL.

Systems Modeling Using Virtual Worlds

Beginning from the initial problem definition and users' requirements, a High Level Systems Analysis (HLSA) was proposed resulting into graphically modeling the system with high-level and low-level system diagrams. This allowed the developers to capture the main important entities within this project.

Once analyzing the problem and system, a plan for design was implemented into Enterprise Architect (EA) using the SDLC OOAD methodology. The idea then leads to purchasing objects from the SL market to use as prototypes within the environment of SL. Difficulties aroused while using the software SL, such as programming objects as well as receiving objects from the market; some objects were unable to be modified and required to purchase other objects that would cooperate with the proposed system and environment.

The overall experience was interesting in learning to plan a development of a graphical user interface (GUI). Future work will be to present the development process of the research project as well as further enhance knowledge within SL to use an effective tool in simulation work.

Optimizing Student Participation in the Design Process

A widely held principle in the field of systems engineering is that the success of a system is directly proportional to the extent of user participation in developing the system. The results of this are that when an end user has a higher level of perceived meaningfulness task this would positively impact subjects' attitude and performance. The other result is that when the user has a perception of control and procedural justice then the user's outcome is satisfaction and their performance increases for the subjects as one increase the

user's mode of participation. Perception of user control with procedural justice yields an outcome that increases the performance of a project as the user is given more opportunity to voice their opinion. It is interesting that when the users are given the choice to establish boundaries in the decision-making process there are increasing gains in user participation attitudes and performance. When the user's meaningfulness task is increased then procedural justice and control task commitment and performance also increase. The user participation positively influence perceived control even though none of the users received their preference. Perceived control influence perceptions of procedural justice. The direct path from decision control to outcome satisfaction reinforces the fundamental importance of perceived control. Path analysis demonstrates a direct effect of task meaningfulness on performance. Meaningful task evokes feelings of inclusion and increase perceptions of control.

Modeling and Designing Using Virtual Worlds

In this section, two design projects shall be described in detail. The first design project shall be a military training facility and the second shall be a modern student building. Both projects were designed as part of graduate level coursework in computer science and systems engineering programs where the students had limited knowledge on architecture and design principles. The students were allowed to use script generators to develop code for objects to include purchasing some of the materials needed from the SL marketplace.

The utilization of SL for these graduate students provided them the ability to develop concepts with the larger picture in mind. As many new computer science and system engineer graduate students are new to the concept of systems thinking, these projects provided them the ability to understand how design concepts are essential to the larger picture. Many of the students thought that job was only important for architecture, civil, or design students; however, they quickly realized the importance of understanding these design concepts themselves in order to provide a full solution to the end users or customers.

Virtual Military Training Facility

This design project was to develop a military training facility that would be the virtual representation of a training facility that could be utilized in

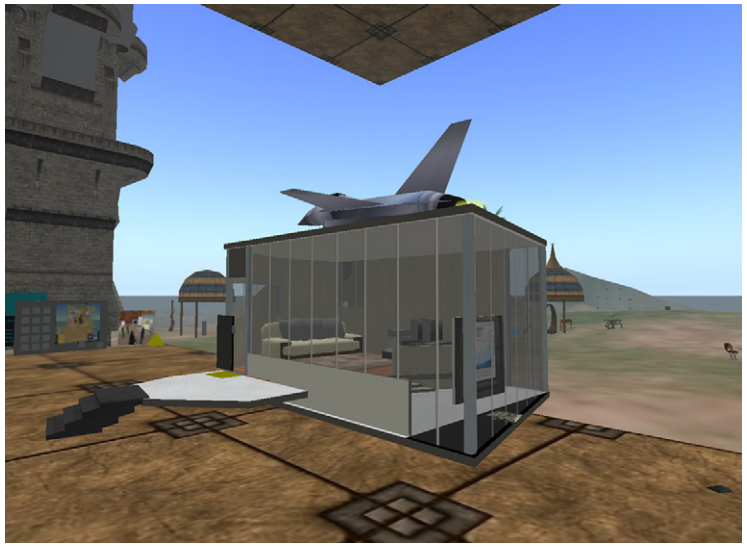


Fig. 9. Virtual Military Training Facility.

the real world (Dawson, 2011). This virtual prototype was developed to test the usability of a proposed military training facility. The facility required a passcode to enter to include a presentation viewer that displayed training on national security. This design project went through the systems development process. Requirements were captured and tested during the design of this system to include a significant number of tests conducted with live participants. Fig. 9 displays the end result of the completed military training facility.

This design project proved that SL was a viable place for designing military training facilities. SL also proved to be a cost-efficient tool for testing the system's design concepts and usability with end users to include stakeholders.

Modern Student Building Project

The main objective of the modern student building project was to research and clearly understand the requirements of an automated teller machine (ATM) system, as well as understand the application model requirements for integration with an ATM system simulation. The goal of this research

design project was to discuss the planning, analyzing, designing, implementing, testing, and evaluating phases of the development of a GUI of an ATM machine model using the software SL; virtual world (Davis & Dawson, 2012).

To accomplish this design project the researchers had to plan the path in which a developer will take to follow for production. This meant properly analyzing requirements and literature review to understand the entities within the system. The use of Object Oriented Analysis & Design (OOAD) to graphically model users, use cases and scenarios, data and flow diagrams was implemented.

The Object Oriented (OO) model was implemented into SL by constructing an environment in which the system will possibly be able to operate in (Davis & Dawson, 2012). Programmed objects to function when virtual users wants to perform a task. Fig. 10 displays the system modelling done for the project.

Beginning from the initial problem definition and users' requirements, a High Level Systems Analysis (HLSA) was proposed resulting into graphically modeling the system with high level and low level systems diagrams. This allowed the developers to capture the main important entities within this project.

Once the program was analyzed and system a plan for design was implemented into Enterprise Architect (EA) using the SDLC OOAD methodology. The idea then leads to purchasing objects from the SL Market to use as prototypes within the environment of SL. Difficulties aroused while

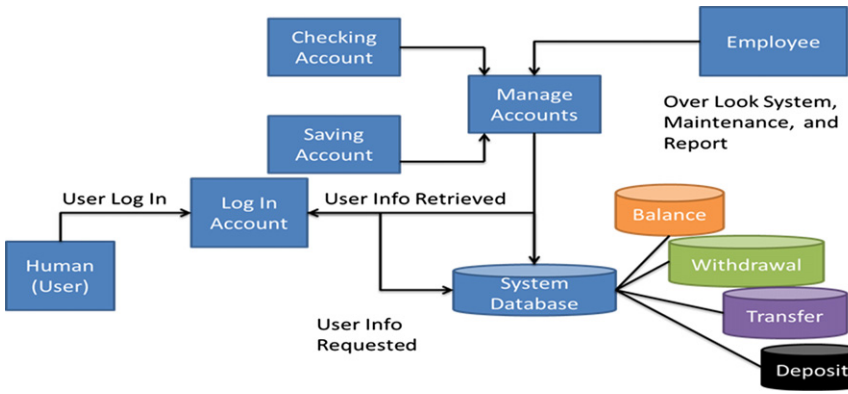


Fig. 10. Low Level Systems Diagram.

Fig. 11. Virtual Modeling of Modern Student Building with ATM.

using the software SL. Difficulties such as programming objects as well as receiving objects from the market; some objects were unable to be modified and required to purchase other objects that would cooperate with the proposed system and environment.

The overall experience was interesting in learning to plan a development of a GUI. Future work will be to present the development process of the research project as well as further enhance knowledge within SL to use an effective tool in simulation work. Fig. 11 displays the finished design project in which live participants utilized the system to capture valuable data to test the hypothesis.

FINAL REMARKS

This chapter discussed the utilization of Linux, OSS, and virtualization tools that are currently available. Also discussed was how OSS virtual tools have been applied at the university level in graduate course projects to teach SDLC. We have described the benefits and challenges of OSS implementation to include how some countries are currently using OSS.

It is important that we as educators utilize these tools to allow students everywhere the opportunity for creativity and learning. As we realize that every institution worldwide does not receive the same level of funding, it is imperative that these tools become part of a technological arsenal to raise educational experiences with minimal impacts to funding.

ACKNOWLEDGMENTS

We would like to recognize Dr. Cynthia Calongne who is a Professor and Chair of Emerging Media in the Doctor of Computer Science and Doctor of Management degree programs at Colorado Technical University who provided great mentorship in the development of virtual worlds. We would also like to recognize the system engineering graduate students at Morgan State University and faculty member Dr. LeeRoy Bronner. Lastly, we would like to thank our families for having patience during the completion of this submission.

REFERENCES

Accenture. (2010). *Investment in open source software set to rise, Accenture Survey Finds*. Retreived from http://newsroom.accenture.com/article_display.cfm?article_id = 5045. Accessed on May 1, 2012.

ACM (2008). *Computer science curriculum 2008: An interim revision of CS 2001*. Retrieved from http://www.acm.org//education/curricula/ComputerScience2008.pdf. Accessed on May 1, 2012.

Al Saeed, I. (2011a). Important of emerging technology in society for futuring and innovation. *Journal of Applied Global Research*, *4*(11), 12–22.

Al Saeed, I. (2011b). Emerging technology as a degree option. *Proceedings of Intellectbase Conference*, *18*, 421.

Armbust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., … Zaharia, M. (2009). Above the clouds: A Berkeley view of cloud computing. October 10, 2009. Retrieved from http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf. Accessed on October 11, 2010.

Chen, Y-F., Rebolledo-Mendez, G., Liarokapis, F., de Freitas, S., & Parker, E. (2008). *The use of virtual world platforms for supporting an emergency response training exercise*. In *Proceedings of the 13th international conference on computer games: AI, animation, mobile, interactive multimedia, educational & serious games*. Wolverhampton, UK, November 3−5 (pp. 47−55). ISBN: 978-0-9549016-6-0.

Cole, J., & Foster, H. (2007). *Using moodle: Teaching with the popular open source course management system* (2nd ed.). Sebastopol, CA: O'Reilly.

Davis, L., & Dawson, M. (2012). Systems modeling a graphic user interface with using virtual worlds. *Academy of Information and Management Sciences Proceedings*, *16*, 1–6. Available at http://sbaer.uca.edu/research/allied/2012-new%20orleans/AIMS%20Proceedings%20Spring%202012.pdf.

Dawson, M. (2011). Applicability of web 2.0: Training for tactical military applications. In *Proceedings of global TIME 2011* (pp. 395–398). AACE.

Dawson, M., Burrell, D. & Emanuel, W. (2011). Utilization of e-learning tools, virtual machines, & open source software to enhance graduate systems engineering Programs. In S. Barton, et al. (Eds.), *Proceedings of global learn Asia Pacific 2011* (pp. 2088–2091). AACE.

de Freitas, S. (2008). *Serious virtual worlds: Scoping study*. Bristol: Joint Information Systems Committee.

Deshpande, A & Richle, D. (2008). The total growth of open source. In *Proceedings of the fourth conference on Open Source Systems (OSS 2008)* (pp. 197–209). Milan, Italy: Springer Verlag.

Dobson, M., Pengelly, M., Sime, J., Albaladejo, S., Garcia, E., Gonzales, F., & Maseda, J. (2001). Situated learning with cooperative agents simulations in team training. *Computers in Human Behavior*, *17*, 543–557.

Glotzbach, R., Mordkovich, D., & Radwan, J. (2008). Syndicated RSS feeds for course information distribution. *Journal of Information Technology Education*, *7*. Retrieved from http://informingscience.org/jite/documents/Vol7/JITEv7p163-183Glotzbach293.pdf. Accessed on October 11, 2010.

GNU. (2007). *GNU general public license*. Retrieved from http://www.gnu.org/copyleft/gpl.html. Accessed on April 25, 2012.

Granlund, R. (2001). Web-based micro-world simulation for emergnecy management training. *Future Generation Computer Systems*, *17*, 561–572.

Johnson, L., Levine, A., & Smith, R. (2009). *The 2009 Horizon report. One year or less: Cloud computing*. Austin, TX: The New Media.

Kern, N. (2009). Starting a second ife. *English Teaching Professional*, *61*, 57–59.

Ko, S., & Rossen, S. (2004). *Teaching online: A practical guide*. Boston, MA: Houghton Mifflin.

Kock, N. (2008). E-collaboration and e-commerce in virtual worlds: The potential of Second Life and world of warcraft. *International Journal of e-Collaboration*, *4*(3), 1–13.

Martin-Blas, T., & Serrano-Fernandez, A. (2009). The role of new technologies in the learning process: Moodle as a teaching tool in physics. *Computers & Education*, *52*, 35–44.

Melton, J. (2008). Need an LMS? Try the open source package moodle. *Journal of Instruction Delivery System*, *22*(1), 18–21.

Miro International Pty Ltd. (2006). *Application of open-source software in chinese schools. OS School*. Retrieved from: http://www.osschool.org/index.php? option = com_content&task = view&id = 1&Itemid = 1. Accessed on February 1, 2006.

Munoz, J. V., Nofuentes, G., Garcia-Domingo, B., & Torres, M. (2012) Customizing distrobutions based on linux. A new software tool to stimulate and design integrated circuits. *INTED2012 Proceedings*, 3209–3214

Murray, M. C. & Guimaraes, M. (2006). A review of the first phase of a project to develop and utilize animated database courseware. In *Proceedings of the 2006 Southern Association for Information Systems conference* (pp. 259–264). Jacksonville, FL USA: Southern Association for Information Systems. Available at http://sais.aisnet.org/2006/Murray-SAIS2006-paper.pdf.

OSALT (n.d.). *Development*. Retrieved from http://osalt.com/development#. Accessed on April 16, 2012.

Pan, G., & Bonk, C. (2007). The emergence of open-source software in North America. *The International Review of Research in Open and Distance Learning*, *8*(3), 1492–3831.

Pavlicek, R. G. (2000). *Embracing insanity: Open source software development*. Indianapolis, IN: SAMS.

PMI. (2010). *Handbook of accreditation of degree programs in project management* (3rd ed.). Newton Square, PA: Project Management Institute. Retrieved from http://www.pmi.org/~/media/PDF/Professional-Development/GAC_handbook_2010.ashx

Rice, W. H., IV. (2007). *Moodle teaching techniques*. Birmingham: Packt.

Rooij, S. (2007). Perceptions of open source versus commercial software: Is higher education still on the fence? *Journal of Research on Technology in Education*, *35X4*, 433–453.

Robert, B., Gamelin, C., Hausler, R., & Jarry., V. (1996). Training concept for environmental emergency measures structuring knowledge. *Journal of Contingencies and Crisis Management*, *4*(3), 175–183.

Stolk, D., Alexandrian, D., Gros, B., & Paggio, R. (2001). Gaming and multimedia applications for environmental crisis management training. *Computers in Human Behavior*, *17*(5), 627–642.

The Consortium for School Networking (CoSN). (2010). *CoSN K12 open technologies implementation study #3 Moodle: An open learning content management system for schools*. Washington, DC: CoSN K12 Open Technologies Implementation Study.

Vouk, M. A. (2008). Cloud Computing – issues, research and implementations. *Journal of Computing and Information Technology*, *16*(4), 235–246.

Wainhouse. (2002). *Survey results: Usage trends of collaboration technology by business travelers*. Duxbury, MA: Wainhouse Research.

Wang, G. (2004) The role of Linux in the development of campus network. *Red flag linux*. Retrieved from: http://www.redflag-linux.com/upfiles/solution/aa.doc. Accessed on February 1, 2006.

Waterhouse, S. (2005). *The power of elearning: The essential guide for teaching in the digital age*. Boston, MA: Pearson.

Weber, S. (2004). *The success of open source*. Cambridge, MA: Harvard University Press.

Wheeler, B. (2007). Open source 2010: Reflections on 2007. *EDUCAUSE Review*, *42*(1), 48–67.

Williams, S. (2002). *Free as in freedom: Richard stallman's crusade for free software*. Sebastopol, GA: O'Reilly.

Transitional leadership in the defence and aerospace industry: a critical analysis for recruiting and developing talent

Maurice Dawson*

Strayer University,
9220 Franklin Square Drive,
Nottingham, MD 21236, USA
E-mail: dr.mauricedawson@yahoo.com
*Corresponding author

Emad Rahim

Walden University,
155 5th Avenue South,
Minneapolis, MN 55401-2511, USA
E-mail: emad.rahim@waldenu.edu

Abstract: This article proposes a framework to create effective transitional leadership in the defence and aerospace industry. The proposed framework identifies and maps traits and skills of military personnel in a manner that can be tested and validated in accordance with principles of human resource management. Applying this framework would assist hiring managers in their selection of program or project managers from the military in transition to a defence contractor support organisation. Employing a research approach embracing a mix of both quantitative and quantitative strategies, the study examined more than 50 respondents to a 34-question survey, focusing on 14 respondents who submitted fully completed surveys. The conceptual framework for this study is derived from investigations conducted by project management practitioners and scholars who have built upon the research of previous research, which studied project development models within various industries.

Keywords: program management; project management; transitional leadership; Department of Defense; DoD; aerospace industry; recruitment; talent; human resource.

Reference to this paper should be made as follows: Dawson, M. and Rahim, E. (2011) 'Transitional leadership in the defence and aerospace industry: a critical analysis for recruiting and developing talent', *Int. J. Project Organisation and Management*, Vol. 3, No. 2, pp.164–183.

Biographical notes: Maurice Eugene Dawson Jr. is currently employed as an Information Assurance (IA) and Networking Product Line Manager at Textron Systems' AAI Division. Responsibilities include overseeing the efforts of a network engineering, software assurance, and IA engineering staff to design, develop, engineer and implement solutions to network and security requirements. He is also a Senior Researcher with Morgan State University. He has over a decade of project management experience working in cross-functional organisations, managing government, military and private

contracts. He has published widely on the topics of project management, information security, DoD, higher education, engineering and organisational development. He received a DCS with a concentration in Enterprise Information Systems from IAS at Colorado Technical University, an MBA and MSM in Information Security from Colorado Technical University and earned several internationally recognised IT certifications (CSSLP, CGEIT, ISP).

Emad Abdul Rahim is a Core Faculty at Walden University, where he teaches in the DBA degree program. He is also an Assistant Professor for Venture Connect at Morrisville State College. He is the Principal Consultant at Global i365, a management consulting organisation specialising in e-learning solutions and thought leadership and diversity training. He has published widely on the topics of diversity management, project management, Islam, organisational development, leadership, entrepreneurship and organisational behaviour. He obtained his Doctorate in Management from the Institute for Advance Studies at Colorado Technical University, two graduate degrees in Business Management and Project Management from Colorado Technical University and earned four internationally recognised management certifications (PMP, CM, CPM). He is a Certified FastTrac Facilitator through the Kauffman Foundation.

1 Introduction

As numerous acquisition program managers (APMs) leave the military, companies are working hard to hire them to lead their government-funded programs, as indicated through the military human resources commands. With this influx of personnel to the civilian workforce, human resources departments must adapt to select the best individual for the job, as indicated by the Rockwell Collins Human Resources and Diversity Advisory Council (DAC). These former-military PMs bring tactical and strategic knowledge from their commands, including program management utilising the acquisition lifecycle, direct end-user experience on the battlefield, and understanding of military operations in relation to the war fighter. Each of these PMs will become the leader, manager, facilitator, and voice to communicate with both upper management and the executing team in the company, as indicated by the federal and defence acquisition communities.

2 Research design

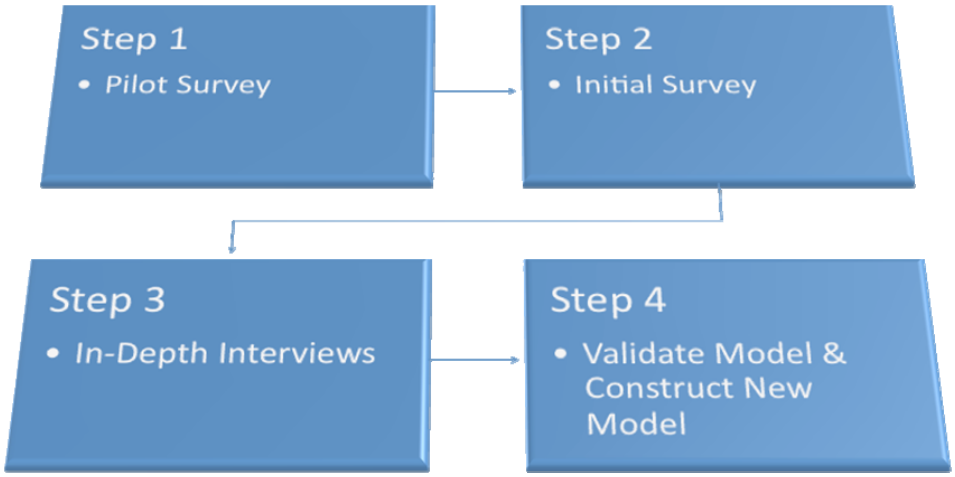
Inquiry can consist of quantitative, qualitative, or mixed methods as a form of gathering information. Figure 1 is an extraction from Creswell's table found in *research design: qualitative, quantitative, and mixed methods approaches* (Creswell, 2003). This figure displays the three methods utilised for gathering information to include the common uses of these various methods and illustrates the strategy of inquiry utilised in the research; its impact was that a mixed-methods approach should be taken in order to perform a complete analysis with the data types presented in the paper (Creswell, 2003).

Figure 1 Alternate strategies of inquiry (see online version for colours)

The purpose for using a mixed-methods approach was that using only one did not allow the researcher to have the desired control, given the subject matter and manner of research. However, the use of both methods allowed the researcher to reach a more focused audience to develop a base and then select a smaller audience to build a sound theory. Through this particular method, the researcher was able to create a sequential model for constructing the model for effective transitional leadership (Creech, 2004).

The study, a four-step process displayed in Figure 2 is detailed as follows: Step 1 involved presenting a pilot survey to selected military service personnel with acquisition experience. Upon completion of this pilot survey, the requested responses were received and then incorporated to an initial survey.

Figure 2 Stages of research approach (see online version for colours)



Step 2 was built upon Step 1's pilot survey. This allowed for the development of the initial survey, which was directed toward a smaller group with more focused questions regarding items taken from the literature review. Step 3 pertained to in-depth interviews of five non-acquisition PMs, all former service personnel. Each interview was a tape-recorded conversation consisting not only of direct questions but also probing questions to gain more information needed for research. Step 4 consisted of validating and constructing a model that represented transitional leadership after doing a detailed analysis of all findings.

The research was conducted using the stages described in Figure 2. The hypothesis is that a system that identifies and maps the traits and skills of military personnel transitioning to non-military positions can be developed, tested, and validated under the principles of human resource management. The hypothesis that will be validated is the assertion that there is a common thread of trait and skill sets allowing for individuals to transition successfully from the military into the Department of Defense (DoD) associated civilian sector, specifically into the defence and aerospace market.

3 Target population

The target population consisted of former service members and project managers from the DoD. The preference was to target individuals in the initial pilot study who had received their training from the Defense Acquisition University (DAU), which requires the minimum of a bachelor's degree with at least 24 semester hours from an array of subjects, including accounting, business finance, law, contracts, purchasing, economics, industrial management, marketing, quantitative methods, and organisational management. Other target population considerations included years of overall experience and years within that specific role for which the certification is being required. For example, if an individual wanted to do contracts, he or she would take all required DAU coursework and must perform for a length of time in that position. This was the additional training that the above individuals (targeted in the pilot study) had received that played a part in their success in the military and commercial sectors.

4 Sample size

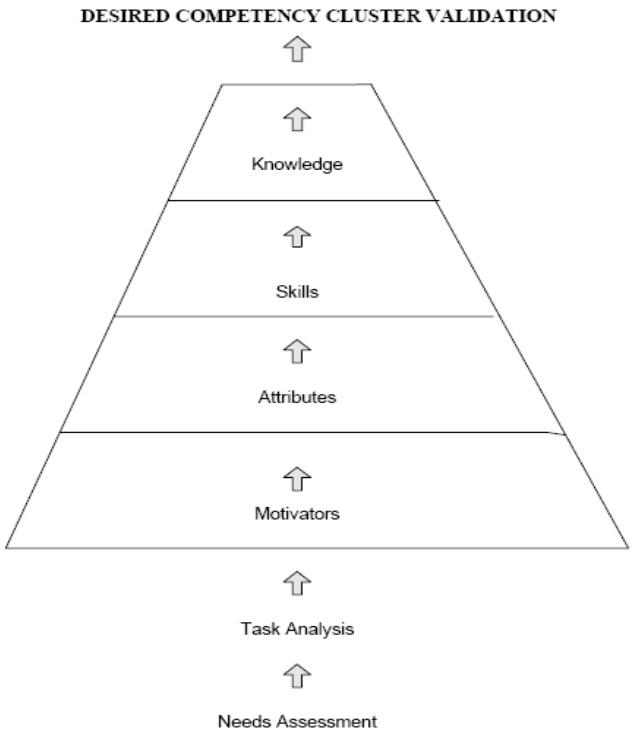
The sample size for the initial study was approximately 50 respondents. The researcher anticipated between 25–50 responses. The reason for acquiring the number of respondents in this survey was that only completed surveys were utilised. By using the anonymous survey instrument, versus a purposive sampling strategy and personal interviews for the initial survey, the researcher hoped to remove any investigator bias. Participants of these surveys were current professionals in the defence and aerospace sectors.

5 Study design

The customised questionnaire was the primary data collection tool; it was strengthened using the desired competency cluster validation. The validity for the desired competency

cluster validation tool was reestablished by Stevens (2003) in his dissertation. The questionnaire was designed to require that key personnel identify and solidify key roles, traits and responsibilities as a project manager. The assessment model is measured by a five-point Likert scale, where a score of 1 shows a low rate of competence and 5 shows a high rate of competence. Participants rated themselves on each criterion. The instrument design, displayed as Figure 3. Desired competency cluster validation, was of particular note pertaining to the study's hypothesis.

Figure 3 Desired competency cluster validation



The instrument had to be designed and modified in such a way that the respondents could freely disclose the level, if any, of their implementation of the competency cluster validation. The questionnaire consisted of 34 questions that focused on the level and implementation of competency cluster validation processes. The demographics were detailed only to the appropriate level needed to meet the hypothesis contained within this study.

6 Ethical issues

Ethical issues in qualitative research are more subtle, and less visible, than issues in survey or experimental research. The issues are related to the characteristics of qualitative methodologies, such as the researching author's long-term involvement, personal relationships, and interviewing. This tends to create potential for variances in field research due to the human interaction component; hence, the research for this study was

prone to a biased outcome due to interaction with the interviewees. However, the quantitative component of the research was limited to the data that was collected and the way data was interpreted since it was numerically based without any emotions involved; thus, it may be concluded that the quantitative findings are unbiased. In performing this study, the author complied with the Colorado Technical University Institutional Review Board's standard for the review of all requests for conducting research using human or animal subjects. The primary purpose of this standard is to ensure ethical treatment and protection of all human and animal participants.

7 Validity issues and reliability

Validity issues rest upon the quality of interview questions and the selection of interviewees. Since the data set is composed of interviews of four individuals, the quality of the emergent theory and insight will be delimited by the depth and breadth of the interview questions. While the individuals chosen for the interviews comprise various military backgrounds, they all have experienced similar leadership training and hold leadership positions within the same company; as such, results are case-specific.

In an effort to validate the instrumentation tool prior to its distribution, a pilot study was administered to members of the acquisition workforce. This workforce had multiple locations: Cedar Rapids, IA; Huntsville, AL; Washington, D.C.; Colorado Springs, CO; and Heidelberg, Germany. Multiple respondents completed a pilot study questionnaire put forth by the researcher. Together, the responses and comments recorded in the pilot study served as a valuable asset in adjusting some questions while eliminating others. Further, an advantage was achieved through this learning process of developing an instrument that would elicit the desired information pertaining to the developed model for transitional leadership.

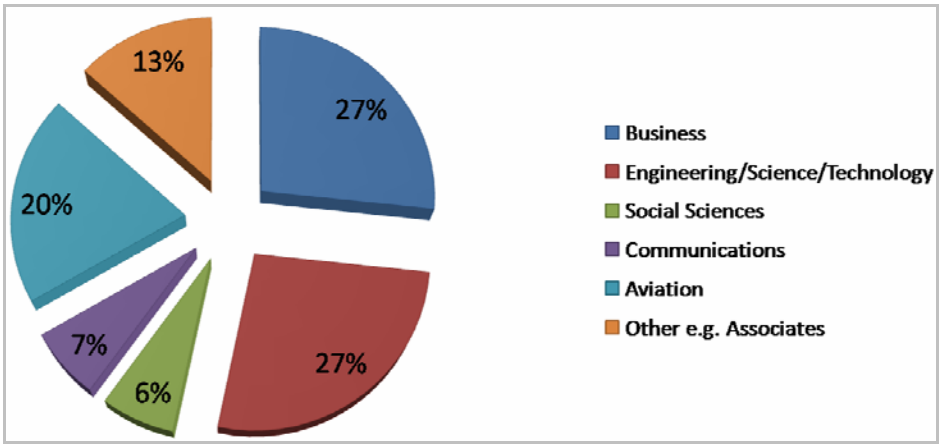
8 Results and demographic breakdown

The completed responses were examined; the partially completed surveys were discarded and were not included in the analysis. Reasons given for not fully completing surveys were time constraints, lack of knowledge pertaining to questions, or ability and willingness to answer the question(s). The demographic information collected included undergraduate education, graduate education, military education, motivations, roles in the service, and answers to 34questions. Background information relating to leadership and managerial roles was also considered. Over 50 respondents replied to the pilot survey; however, only 14 submitted fully completed surveys. The respondents came from all over the USA, with 57% from the southern region, 29% from the western region, and the remaining 14% from the eastern region. The breakdown included 64% commissioned officers and 36% non-commissioned officers (NCOs). Of the 14 respondents, all were middle-level managers, senior managers, or executive-level managers/officers.

Regarding education level, all had attained at least an associate degree. Pertaining to prior undergraduate-level studies, 27% were business majors, 27% were engineering/science/technology majors, 20% were aviation majors, 13% were educated at an associate's level only, 7% were communications majors, and 6% had an educational background in the social sciences. In counting the educational background, some of the

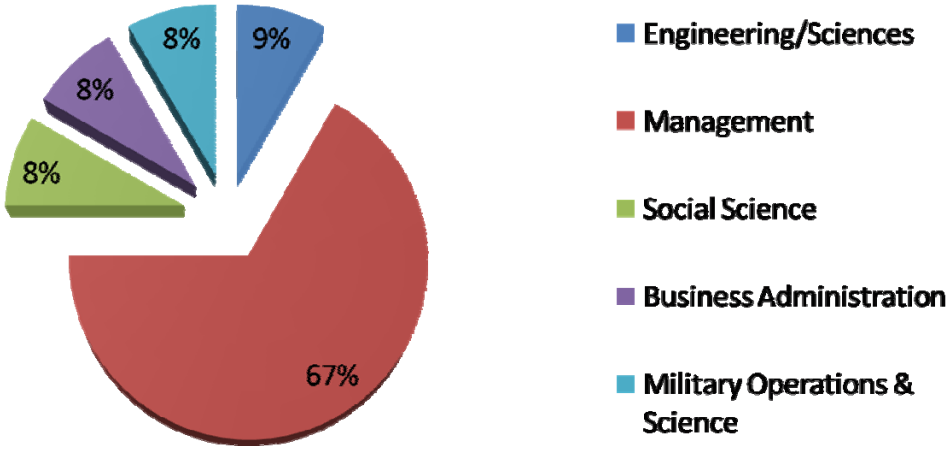
respondents had more than one degree and thus, were counted individually when performing the statistical analysis of this survey. Figure 4 displays the graphical representation for education percentages at the bachelor and associate level.

Figure 4 Pilot study undergraduate education breakout (see online version for colours)



Out of all the respondents, 78.5% had one or more advanced degrees. The breakout of the types of graduate-level degrees displays 67% in business administration [Masters of Business Administration (MBA)], 9% as engineering/science majors, 8% in social sciences, and 8% in management. The percentages are captured in Figure 5. All respondents' educational degrees were attained from regionally accredited institutions located within the US In looking at all data, 74% of all respondents' undergraduate educational experiences related to business and engineering/technology/sciences, whereas at the graduate level, 84% had degrees relating to business, management, and engineering/science. It appears that at the undergraduate level, the main drivers were engineering and business-related programs; meanwhile, at the graduate level, more than 75% had degrees pertaining to management and business.

Figure 5 Pilot study graduate education background (see online version for colours)

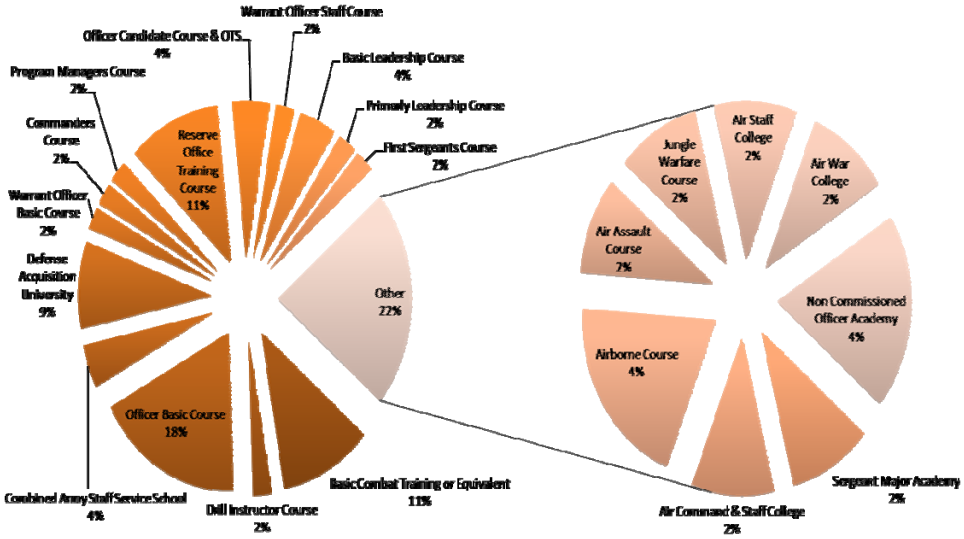


In total, regardless of military service and gender, 100% of the respondents reported being in management and leadership roles. Only 7% were female, but 93% of the total respondents were included in the pilot survey. All individuals had a role within the acquisition process; however, only 50% were acquisition project or program managers to include being branched as part of the Acquisition Corps. Of the total respondents, all managed projects or programs in excess of $1,000,000; however, only 21.4% had profit and loss (P&L) responsibility for $100,000,000 or more. Only 28.5% had projects or programs in excess of $50,000,000, and 64.2% were responsible for projects over $15,000,000.

9 Preliminary findings

To date, preliminary analysis of the data has enabled identification of a number of characteristics among the interviewees' military backgrounds. None of the individuals interviewed went through a direct commission program, which means they had to undergo rigorous officer training: They became commissioned leaders through either Reserve Officer Training Corps (ROTC), which required two to four years of leadership development, or Officer Candidate School (OCS), which included an intensive 14-week leadership course in Fort Benning, GA. Other individuals interviewed went through BCT and Warrant Officer Basic Course (WOBC), which is an intensive five-week course in Fort Rucker, AL. All enlisted soldiers went through advanced management courses that allowed them to continue their career as NCOs. All of these training courses teach the Army values, known as "LDRSHIP: loyalty, duty, respect, selfless service, honour, integrity, and personal courage"; this reflects the values instilled in them since becoming part of the USA military and that prepares them for the stress of performing in an intensive combat zone. Below in Figure 6, specific percentages concerning military education are broken out.

Figure 6 Pilot study military education (see online version for colours)



All participants engaged in a variety of a formal college studies from business to aviation. However, 100% of the interviewees had at least an associate-level degree. Out of the individuals selected from the entire group for specific correlation to study, all had at least a bachelor-level education. A majority of them pursued graduate degrees and completed certifications/courses within the Acquisition Corps. The researcher expected the comparative analysis to reveal more common characteristics of leadership traits and skills.

10 Research questions

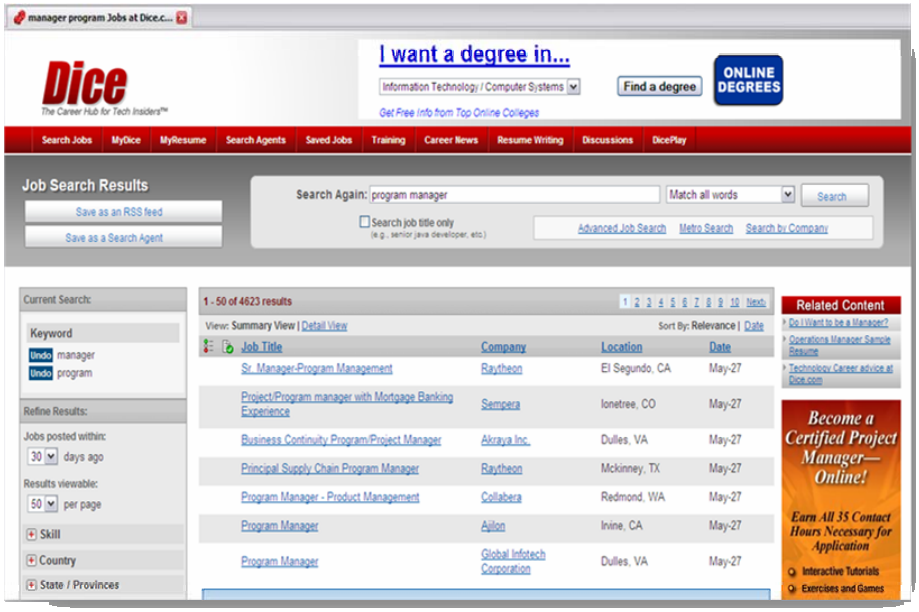
RQ1 Is there a need for acquisition program management personnel to work as contractors on government-funded programs?

Through the literature review and participation with the DAC companies at a company with its headquarters in the Midwest, it has been revealed that the need and presence of project management have developed to become necessities in many industries (Rahim and Dawson, 2009). In 2008, the two magazines *Global Knowledge* and *Fortune* named 'project management' in their top ten careers of choice. This means it is a popular career, yet many personnel are needed to fill the ranks of this profession. Relating to the professional certification and credentials, the Project Management Professional (PMP) certification was listed as the highest paying certification to have in the technology industry, with the Certified Associate in Project Management (CAPM) falling into second place. This survey was conducted by ZDNET's Tech Republic organisation, and further helps prove that this profession is in demand across all industries. The DoD, in cooperation with DAU, has specifically created a career path and military designation relating directly to project management to include methods for retention of these personnel, so as to ensure that the military has appropriate personnel to ensure the successful management of government programs. Even the Department of Homeland Security (DHS) has developed an Acquisition Corps with the United States Coast Guard (USCG) to better manage government programs. The increasing attention on project management has increased the need to educate and further develop project managers and staff in order to provide better services, especially in the defence and aerospace sectors.

Multiple postings through http://www.Dice.com, http://www.Careerbuilder.com, and http://www.Securityclearancejobs.com are seeking project managers to supervise their projects with very specific skill sets, military experience, and educational credentials. The screenshot below from http://www.Dice.com has revealed 4,623 job postings that were displayed within a 30-day job period. When the word 'clearance' was typed in addition to the basic search, approximately 1,000 job results appeared.

Another job search using the words 'project manager' and 'security' displayed approximately 1,900 jobs in the results field. What the http://www.dice.com search has shown is that there is a need for program or project managers with security clearances; however, a larger need exists in general for individuals who know how to the manage time, scope, and schedule of a project.

Figure 7 Dice jobs screen shot (see online version for colours)



RQ2 What is the common thread of traits and skills amongst individuals in the acquisition community?

Through the conducted research it was revealed that a remarkable portion of the discussions lead into more of a qualitative analysis. Various topics were addressed during the in-person interviews conducted with former service personnel at a defence and aerospace company headquartered in the Midwest. This particular company has brand aircraft electronics installed in the cockpits of nearly every airline in the world, and its airborne and ground-based communication systems transmit nearly 70% of all US and allied military airborne communication.

Professional relationships have been built with nearly all individuals chosen to study; to include the majority of them, the researcher has worked directly with a military program. The preliminary interviews and questions have been completed as a result of an earlier study which was not appropriately constructed. However, the result has allowed the researcher to have a large repository of information that shall assist in this research moving forward. Each of the military personnel interviewed:

1 has a different military background and has served a minimum of four years within the USA armed forces

2 is currently in a leadership role within an organisation that supports the military in either developing a product or providing a service

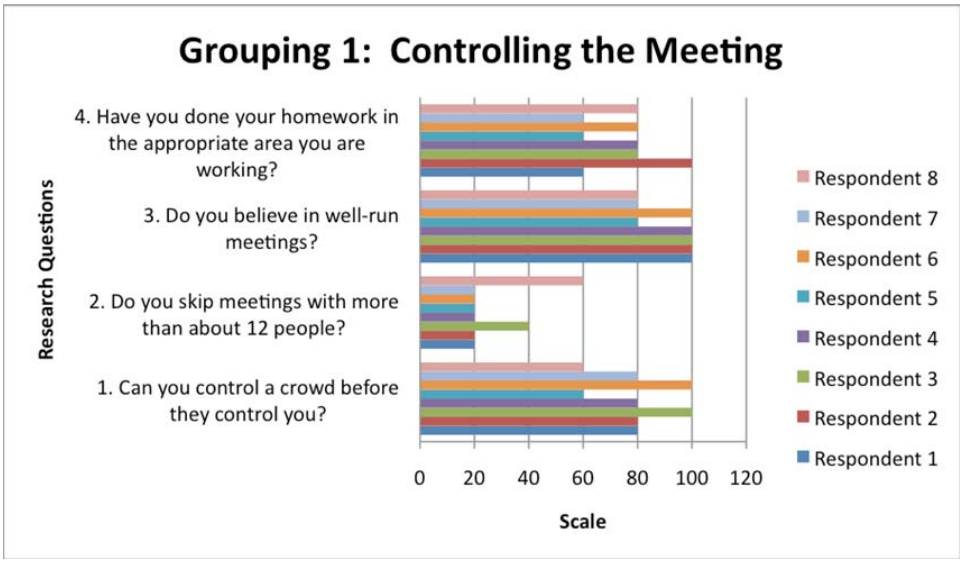
3 was interviewed separately through an intensive note-taking session for later analysis as well as for constructing themes and checking evolving concepts

4 was compared to the summarised results of all individuals to include some items found in the work completed earlier in the literature study.

The groupings were questions relating to management, values, ethics, leadership, business development, and technical competency. Many of the individuals interviewed had been in some form of leadership role since childhood. That leadership role varied from a position within the church to academic or athletic teams where they said they learned multiple things such as teamwork, leadership, dedication, determination, integrity, and motivation. Additionally, the probe questions revealed that many had a positive role model whose guidance they followed. All of the interviewees come from various social classes; however, of importance are the above traits they have in common. Even the education aspect presents wide variance, from prestigious university alumni to state university alumni. It appeared that neither race, colour, creed, religion, nor social class was common across the board. However, many did admit that due to social class, they did not have as many opportunities but rather made the best out of what they had out of the ambition to better themselves. All the individuals' studies showed they sought continuous growth and learning, for both educational and professional benefit.

The information gathered was utilised to further define the research questions by understanding how to develop follow-up questions and narrow down the information with the interviewee. Some of the items learned were how to properly form a follow-up question, understand the differences in responses that may not be complete or accurate, and decomposing and categorising results.

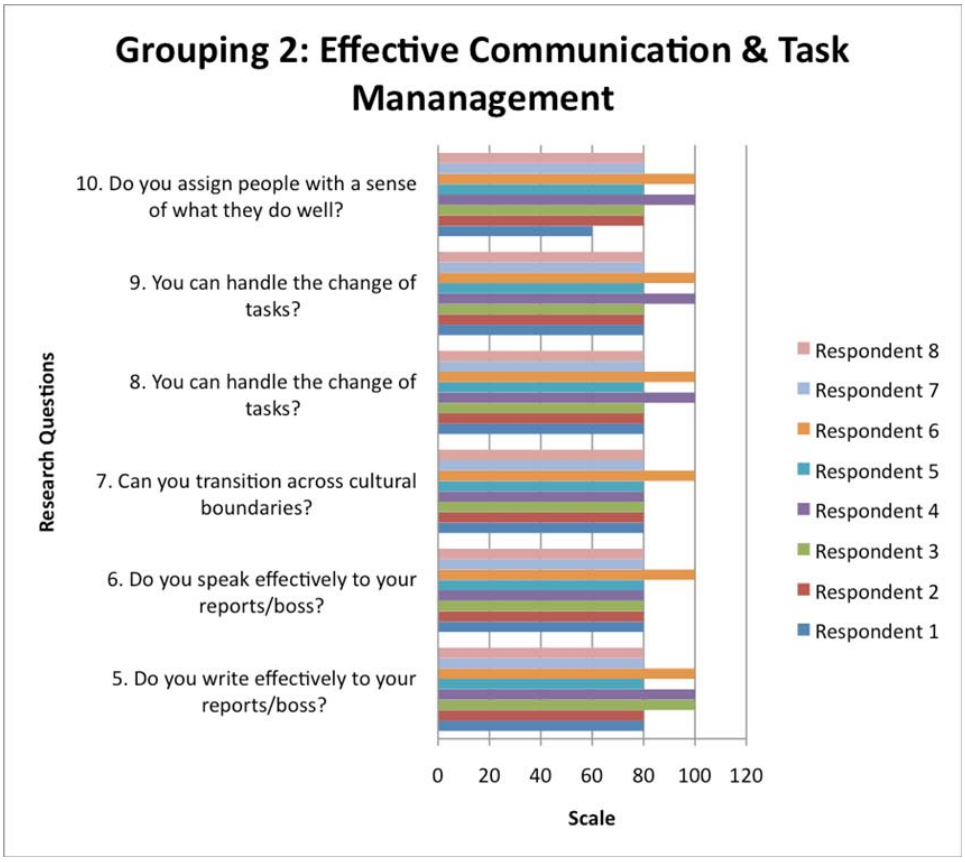
Figure 8 Grouping 1 (see online version for colours)



As displayed in Figure 8, according to the survey respondents, the vast majority stated that they could control a meeting as it relates to the questions asked in Grouping 1: controlling the meeting. The only response that had a large variation was a question regarding to skipping meetings with more than about 12 people. Otherwise, the rest answered 'almost never,' with one person responding with 'sometimes'.

In Figure 9, according to the survey respondents, the vast majority stated that they could effectively communicate and manage a task as it relates to the questions asked in Grouping 2: effective communication and task management. In this particular grouping the variations were not large. At any one time, no less than 62.5% felt that they performed or conducted a particular task 'almost always.' Thus, all of these items should be considered key skills in terms of program management. Questions 8 and 9 were the same to ensure the integrity of the survey process was maintained; noted in Figure 9, both questions have the same answers by the same respondents.

Figure 9 Grouping 2 (see online version for colours)



According to survey respondents in Figure 10, the vast majority responded similarly in Grouping 3: managing personnel. Here, the variations were noticeable on question 15, which probes the belief that a good employee sometimes may not fit into the corporate culture. With this question, 50% felt they believe this 'somewhat,' while the remaining 50% were divided in between variations of 'never' and 'always'. As a whole, the majority did not feel strongly toward one or the other. This question was divided in multiple ways, but for the most part, the respondents felt that they could judge between 'great' and 'no good'. In all other items, the respondents felt as if they could handle and make the appropriate choices as they saw fit.

Figure 10 Grouping 3 (see online version for colours)

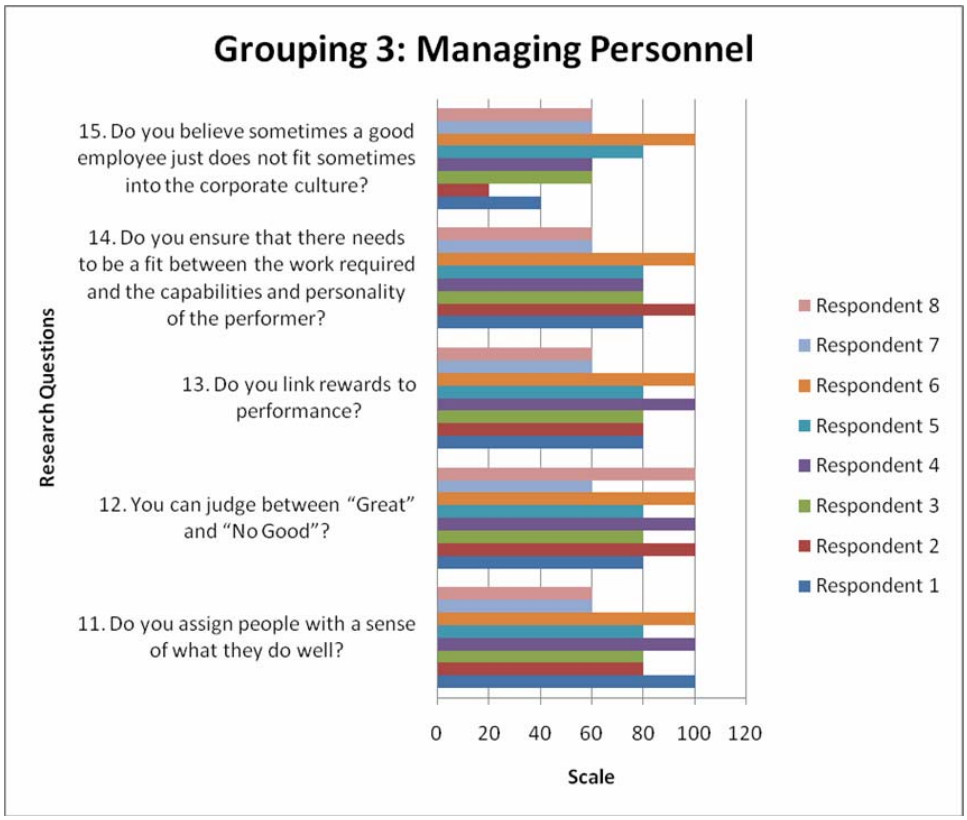
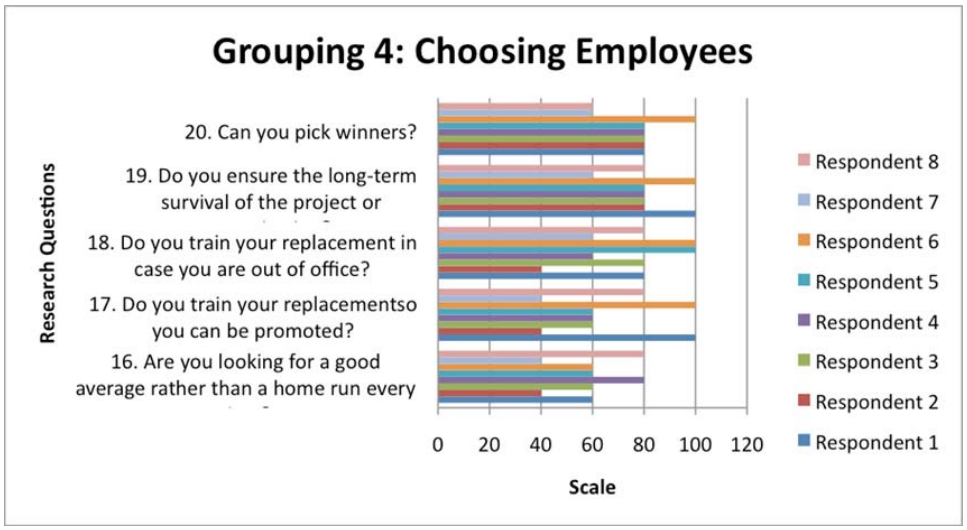
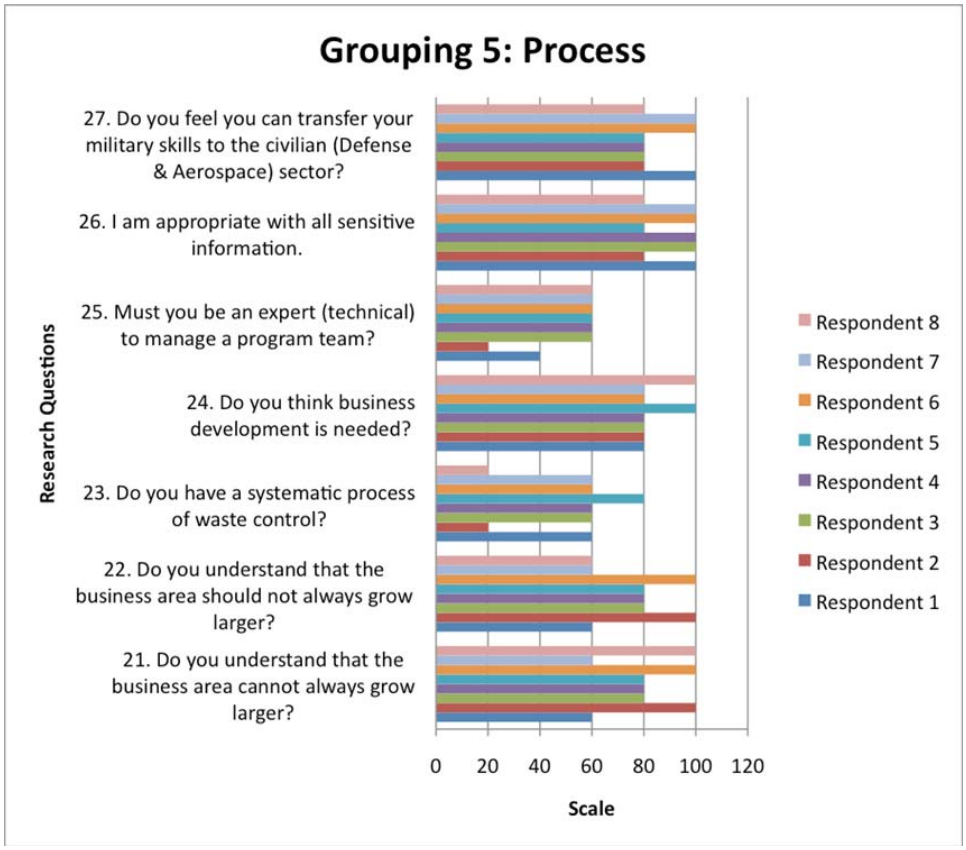


Figure 11 Grouping 4 (see online version for colours)



According to the survey respondents portrayed in Figure 11, a good percentage did not train employees as replacements; nevertheless, they felt they could pick winners, ensure long-term survival of the project or organisation, and look for a average employee rather than one who excels. Further clarifying on the last point, 'a good average' refers to an employee who comes in, does the job, and performs it as expected. Someone who hits the home run is far from expected, but 25% were indeed looking for that superstar employee. In this particular grouping, the variations occurred in questions 16, 17, and 18.

Figure 12 Grouping 5 (see online version for colours)

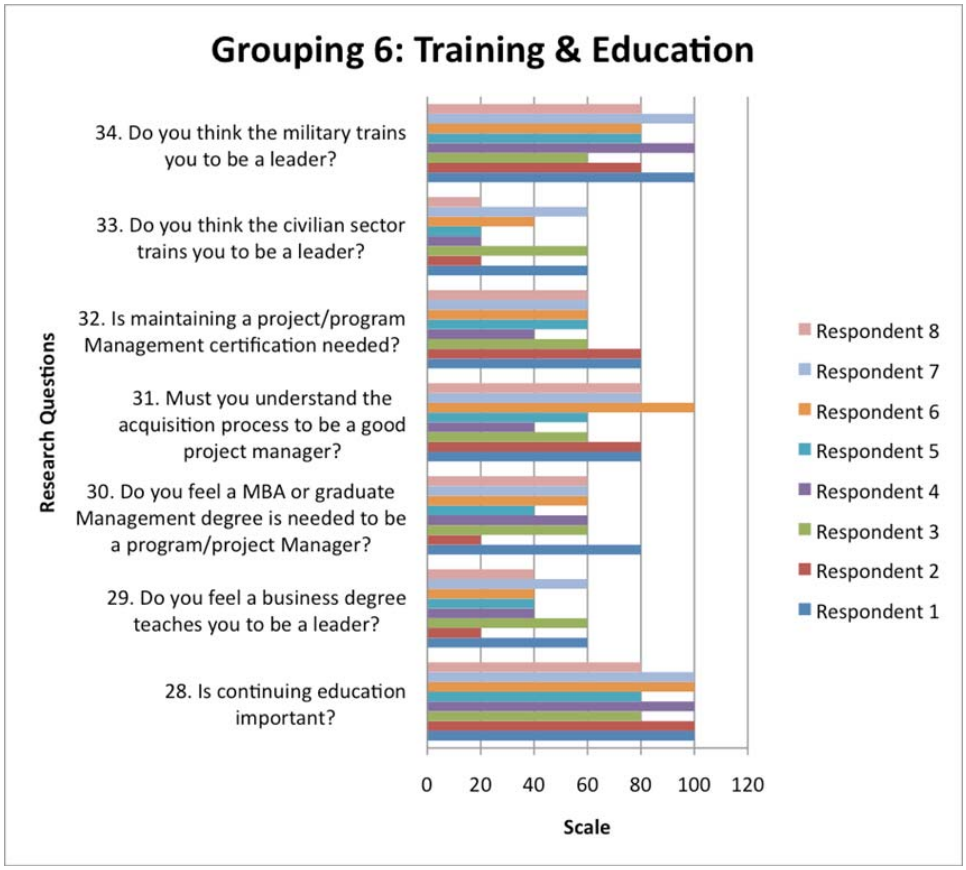


As Figure 12 displays, according to survey respondents, the vast majority indicated that they could transfer their military skills to the civilian sector in Grouping 5: process and transfer. Process is pivotal, as the goal is to create a framework that allows for this to occur. The response received for question 25 was that approximately 75% of the respondents did not have a strong answer regarding whether an individual should be a technical expert to manage the program. Nonetheless, it does appear that one must have knowledge of the business market if seeking growth. Also included is that an organisation cannot always expand beyond a certain size.

As shown in Figure 13, the vast majority of survey respondents acknowledged that continuing education is important, and 87.5% of the respondents felt that the military trained them for leadership. Another important finding within Grouping 6: training and

education is the consensus that having either an MBA or a business degree was not of high importance. It appears the majority felt that the degree overall, as it relates to business or management, is unimportant. In the earlier survey, it was brought to light that a large percentage had business undergraduate and graduate degrees, albeit there seemed to be mixed messages regarding civilian sector leadership training and one's understanding of the acquisition process.

Figure 13 Grouping 6 (see online version for colours)



RQ3 Can random non-acquisition personnel in program management fit in the model or be a rejection of the model?

By conducting qualitative in-depth interviews, the final results revealed that the individuals did not possess all traits necessary to be an Acquisition Program Manager. Interviewees had very specific skill sets within their domain, such as information assurance (IA), systems engineering, contract management, and test. It should be noted that they did not possess all these skills, but there was a large variation amongst all interviewees: some of the individuals lacked experience in program management and did not understand the acquisition process at all. Many of the interviewees admitted that they may not be good for a program management experience, while others stated that they

could be successful starting off at a small program. One of the interviewees appeared to dodge the questions completely; outside the interview in private discussion, it was apparent that many of the needed skill sets and qualities were not present. In comparing the answers captured in the initial survey and according to how they were answered, they proved inadequate as program managers.

RQ4 What would a framework look like that could be utilised by the Human Resources group for selecting personnel?

The framework that could be utilised for selecting personnel should encompass a two-step process. The first step is similar to the original framework created, although this framework is based on the demographics and results taken from the pilot and initial survey. This model would select individuals with the all following properties:

1 leadership roles within military

2 P&L responsibility of at least $15 million

3 undergraduate education in business, engineering, or aviation

4 graduate education in management.

The second step is to take the individuals who have the required credentials and experiences that relate and measure them once again, but against more criteria. These criteria should be base on the initial survey. The individuals shall be measured against the six groupings as follows:

1 controlling the meeting

2 effective communication and task management

3 managing personnel

4 choosing employees

5 process

6 training and education.

Grouping 1 shall provide information on how they control a meeting, including meeting preparation. Grouping 2 shall provide how well an individual can communicate to the team and handle task management. For a program manager, task management is essential as detailed by PMI (2004). With the global nature of work in business, one must also be able to transition across cultural boundaries internally in the workplace as well as externally to customers. As a project manager, it is essential to communicate upward to senior leadership and downward to the project team. Grouping 3 shall provide information on personnel management. This shall give insight on judgments, assignment of tasks, and rewards for performance. Grouping 4 provides information on choosing employees, training replacements, and ensuring long-term survival of project or organisation. This grouping shows the traits and skills needed essentially for choosing key players and displaying aspects of 360-degree leadership (Yukl, 2001). Grouping 5

shall provide information relating to the knowledge of processes and transfer. Specifically, this grouping point to skills of various systematic processes of waste elimination and business development, as well as validates self-view of skill transfer. Grouping 6 shall provide information relating to training and education, which will allow the variety of items ranging from continuing education to importance of an education to be evaluated. This new two-step process is created from the majority answers given during each grouping. These answers serve as the standard against which individuals will be evaluated.

11 Interesting findings

The interesting findings revolved around the variety of leadership experiences and the ways in which some individuals were shaped into their current role. The entire process for conducting this research led the researcher to discover additional developmental facets behind leadership qualities. Acquiring these details facilitated the insertion of more frequent, probing questions for gaining more information that is related to the research topic. Many interviewees that participated in the research were open and honest in disclosing their strengths and weaknesses. This enhanced the capturing of questions for building the pilot survey. During the pilot survey, many provided critical feedback, particularly via contacting the originator of the survey/questionnaire if there were items that were misunderstood.

A key factor that influences the acceptance of organisational decisions is trust in the leadership. When trust is high, an organisation's internal atmosphere is positive, which increases the potential for positive outcomes. Likewise, the opposite is true; a low level of trust generates a negative internal environment that impedes organisational success. To create an effective leadership transition plan for program managers, it is recommended that the defence and aerospace industry evaluate their recruitment practices and organisational culture and examine its blind spots and to create best practices. Hurley (2006) proposes a model to develop trust for leaders and for decisions made, and suggestions for practical ways to manage trust, which influences recruitment practices and success for the DoD sector, specifically in the defence and aerospace.

12 Future research

The finalised process selecting program managers shall encompass two steps. The first step is similar to the original transitional leadership framework created however this framework is based off the demographics and results taken from the pilot and initial survey. This model would select program managers who have the minimum of all following numbered items below:

1 leadership roles within military

2 P&L responsibility of at least $15 million

3 undergraduate education in business, engineering, or aviation

4 graduate education in management.

The next step within this newly created process is to take the selected program manager have acquired the common credentials and experience. These criteria shall be based of the initial survey. The individuals shall be measured against the six groupings which are the following:

1 controlling the meeting

2 effective communication and task management

3 managing personnel

4 choosing employees

5 process

6 training and education.

13 Importance of research

The importance of this research is that the process utilised can be applied to multiple disciplines such as PM, enterprise information systems (EIS), human resources, and knowledge management (KM). This research has touched multiple disciplines in a manner that can ultimately shape the way organisations select employees. For example, a Chief Executive Officer (CEO) must select their organisation thus, they could utilise this selection process for employment. This process could be applied to healthcare, education, non-profit organisations and even political groups. This research allows multiple groups to truly interface and experience the systems development life cycle (SDLC) from start to end. For example, the human resource team must map out the personnel traits and the EIS team would develop a system that would interpret the information. The management team would use this developed system to select and/or manage employees. The SDLC would also require testing of the system, requirement development, fielding of the systems, and maintenance that would continuously engage all parities throughout. This research could be utilised to properly profile terrorists and criminals eliminating issues today that are widely known to the greater public.

14 Recommendations

This research has answered four questions but reveals opportunities for other interesting research into the further development of human resource decision support systems (DSS) and selecting future APMs. Because the literature indicates that individual factors are strongly correlated to education, ethics, leadership, this study did not consider many demographic factors. However, if a future revised model were to be developed for transitional leadership, other individual factors must be considered. A limitation of this study is that the vast majority of these interviewees in the sample did not communicate with international offices. Though the organisations varied in size and industry, a commonality among all but one of the organisations was that work with international program offices was very limited. Through the interviewees it has been demonstrated that the military had a significant part in the development as a leader, and manager. Though the results of the present study showed no statistical relationship between working with

program managers with military experience and managers from the commercial sector, further research could explore this potential correlation with a different sample of program management workers.

15 Areas of potential research

There are many ways that this research can be utilised for near and long term areas of future research. For areas of near term research it would be beneficial to the program management community to compare program managers with military program experience with those who have only commercial experience As the surveys were distributed to individuals who have served in the multiple branches representing the majority of the participating organisations in this study, many of the participants expressed their thoughts of leadership, management, and other related items pertaining to program management verbally to the researcher. The similarities in atmospheres and military leadership training were often similar. However a quantitative or qualitative study examining the differences and correlations between the program managers of military and non-military experience backgrounds might also be conducted to ensure that program managers of military background provide the organisation the best value. For areas of long-term research it would be beneficial to all communities to understand key traits across all disciplines. This would allow the proper selection of employees in multiple areas to be properly selected thus, reducing the overall program risk. Other areas would be in KM by utilising the DSS to act as a key decision maker on the program. Essentially the selected PM would be emulated by the DSS to make key decisions or act as a mentor to younger managers. Another area of future research is to understand how this knowledge could be utilised for executive training and knowledge transfer.

16 Conclusions

The findings of this study implicate organisational politics as a correlate of the building blocks of program management and transitional leadership. If human resource managers or corporate level managers are concerned about recruiting the best and brightest from the military sector preparing to leave they might want to consider a model for selection with steps built into place to weed out the low potential employees.

The findings of this study also strongly implicate the problem of not having selected the proper individual for the task of managing program significant. Nearly all of the respondents felt that education was unimportant. Workers may be interrupted with tasks they deem menial and then receive conflicting or ambiguous messages about what work is has highest priority or how they should be spending their time at work, and this uncertainty and feelings of inefficacy could certainly lead to emotional exhaustion. To avoid incorrectly placing, practitioners must be diligent in prioritising the weights for the tasks and qualities that become the foundation for the model of transitional leadership. This research is beneficial to multiple communities as this can ultimately affect the way all organisations select all employees and develop KM systems to transfer key skills/traits.

References

Creech, G.W.L. (2004) 'Organizational and leadership principles for senior leaders', *AU-24 Concepts for Air Force Leadership*.

Creswell, J.W. (2003) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Sage, Thousand Oaks, CA.

Hurley, R.F. (2006) 'The Decision to Trust', *Harvard Business Review*, Vol. 84, No. 9, pp.55–62.

PMI (2004) *A Guide to the Project Management Body of Knowledge*, Project Management Institute, Newton Square, PA.

Rahim, E. and Dawson, M. (2009) 'Emerging trends: IT project management in a global market', *Journal of Information Systems Technology and Planning*.

Stevens, J.A. (2003) *The Motivations-Attributes-Skills-Knowledge Competency Cluster Validation Model: An Empirical Study*, August, Doctoral dissertation, Texas A&M University, available electronically at http://handle.tamu.edu/1969.1/339.

Yukl, G. (2001) *Leadership in Organizations*, Prentice Hall, Jersey City, NJ.

Full Article Available Online at: Intellectbase and EBSCOhost | JISTP is indexed with Cabell's, JournalSeek, etc.

JOURNAL OF INFORMATION SYSTEMS TECHNOLOGY & PLANNING

Journal Homepage: www.intellectbase.org/journals | ©2010 Published by Intellectbase International Consortium, USA

INTEGRATING SOFTWARE ASSURANCE INTO THE SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC)

Maurice Dawson[1,2], Darrell Norman Burrell[3,4], Emad Rahim[5,6] and Stephen Brewster[7]

[1]Morgan State University, USA, [2]Colorado Technical University, USA, [3]A. T. Still University, USA, [4]Virginia International University, USA, [5]Morrisville State College, USA, [6]Walden University, USA and [7]Capitol College, USA

ABSTRACT

This article examines the integration of secure coding practices into the overall Software Development Life Cycle (SDLC). Also detailed is a proposed methodology for integrating software assurance into the Department of Defense Information Assurance Certification & Accreditation Process (DIACAP). This method for integrating software assurance helps in properly securing the application layer as that is where more than half of the vulnerabilities lie in a system.

Keywords: *Secure Coding; Software Assurance; Secure Software Development Lifecycle.*

INTRODUCTION

In the past software product stakeholders did not view software security has high priority. It was believed that a secure network infrastructure would provide the level of protection needed against malicious attacks. In recent history network security alone has proved inadequate against such attacks. Users have been successful in penetrating valid channels of authentication through techniques such as cross site scripting, Structured Query Language (SQL) Injection, and Buffer Overflow exploitation. In such cases system assets were compromised and both data and organizational integrity were damaged. The Gartner Group reports that more than 70 percent of current business security vulnerabilities are found within software applications rather than the network boundaries (Aras, Barbara, & Jeffrey, 2008). A focus of application security emerged in order to reduce the risk of poor software development, integration, and deployment. Through this need software assurance quickly became an Information Assurance (IA) focus area in the financial, government, and manufacturing sectors to reduce the risk of unsecure code.

MEETING DEPARTMENT OF DEFENSE (DOD) DEMANDS

The United States Army is the primary customer may defense contractors. The Army is managed and ran by the Department of Defense (DoD). The primary objective of the DoD is to provide military forces in an effort to deter war and to protect the security of the United States of America. The Department of Defense (DoD) has addressed security through governance issued under the Office of Management and Budget (OMB) Circular A-130. The focus of Information Technology security was further derived by DoD Directive 8500.2. It specifically states that all IA and IA-enabled IT products incorporated into DoD

information systems shall be configured in accordance with DoD-approved security configuration guidelines. On April 26, 2010, the DoD released the third version of the Application Security and Development Security Technical Implementation Guide (STIG) provided by the Defense Information Systems Agency (DISA). This document provides DoD guidelines and requirements for integrating security throughout the software development lifecycle. As a leader in the development and fielding of unmanned aerial vehicles, it is our responsibility to meet the needs and demands of our customer to the best of our ability. Therefore we must adhere to the integration of security throughout our SDLC in an effort to meet the requirements of our customer.

COMMON INDUSTRY STANDARDS FOR SOFTWARE DEVELOPMENT

Software engineering is the process of developing and implementing algorithms. Software Assurance is the level of confidence that software algorithms function as specified free of intentional and unintentional vulnerabilities. Generally an organization's software development life cycle is based upon the waterfall model. There are five phases to the Software Development Life Cycle (SDLC). The figure below details a process flow diagram of the waterfall SDLC.

Figure 2: *Common Defense & Aerospace SDLC*

An allocated baseline is created during the Requirements and Analysis phase. This baseline contains all of the requirements for a specific system allocated across four different functional areas. Once each functional area lead identifies its allocated requirements as correct, the allocated baseline becomes a verified baseline. Software is one of the four functional areas in which system requirements are allocated. These requirements are then used to design code, integrate and test a completed software configuration item within the system. The IA security controls for the system are identified during the requirements and analysis phase. They are provided by customer and implemented through the Defense Information Assurance Certification and Accreditation Process (DIACAP) in compliance with DoD Instruction (DoDI) 8510.01. The respective Program Management Office of the DoD for provides an organization's IA department with a list of IA requirements that are to be met. These requirements serve as the DIACAP Implementation Plan (DIP), which must be executed in order to reduce the security risk of the system to an acceptable level and receive an Authority To Operate (ATO). The ATO is needed in order for our systems to be fielded within the DoD network. However, the execution of the DIP occurs during the CSCI Test phase of the SDLC. Therefore any and all vulnerabilities are being identified and mitigated after the software has been designed, developed, unit tested, and submitted for computer software configuration item testing.

PROCESS TO SECURE SOFTWARE CODE

In the event of a vulnerability finding, the software code may require redesign and implementation. This iterative cycle is costly in time and resources. To truly understand security threats to a system, security must be addressed beginning with the initiation phase of the development process. For an organization this means they must allow the IA controls and requirements to drive design and influence the software requirements. Therefore, any identified security threats found during the requirements and analysis phase will drive design requirements and implementation. Security defects discovered can then be addressed at a component level before implementation. The cost of discovery and mitigation can be absorbed within the review, analysis and quality check performed during the design, and implementation of our SDLC. The resultant product is one with security built in rather than security retrofitted. A study was performed by the IBM System Science Institute in order determine the relative cost in order to fix defects within the SDLC. Figure 2 displays their findings.

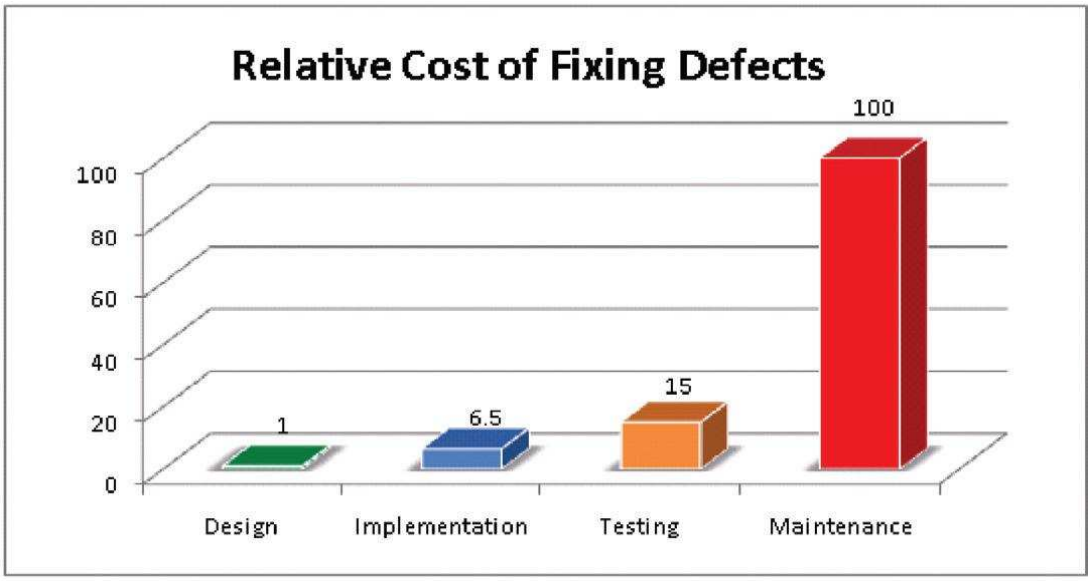


Figure 3: *IBM System Science Institute Relative Cost of Fixing Defects*

Defects found in testing were 15 times more costly than if they were found during the design phase and 2 times more than if found during implementation.

SECURE SDLC

DoDI 8500.2, IA Implementation, states that the Information Systems Security Engineer (ISSE) must work with the system architects, engineers, and developers to ensure that IA controls are designed and implemented into the system throughout the development process. Though this requirement is for government entities, it serves as a guide into how an organization could also integrate security into software development. The software development process which an organization should have should serve as the baseline process in which the integration of security controls and activities must take place. The objectives are as follows for secure development:

- Reduce cost of fixing vulnerabilities.
- Increase the integrity, availability, and confidentiality of our software.

- Conform to DoD standards of secure software development

The security activities involved should seamlessly interface with existing activities found with the organization's SDLC. In order to achieve such a unified process we must first examine the activities required within a Secure SDLC. The International Information Systems Security Certification Consortium, Inc (ISC)2, a global leader in the creation of security certification standards, has published best practices for integrating security into the system development life cycle. The security activities suggested by (ISC)2 should be further derived into the secure SDLC using existing SDLC phase definitions. The following diagram depicts the activities within the Secure SDLC with the Department:

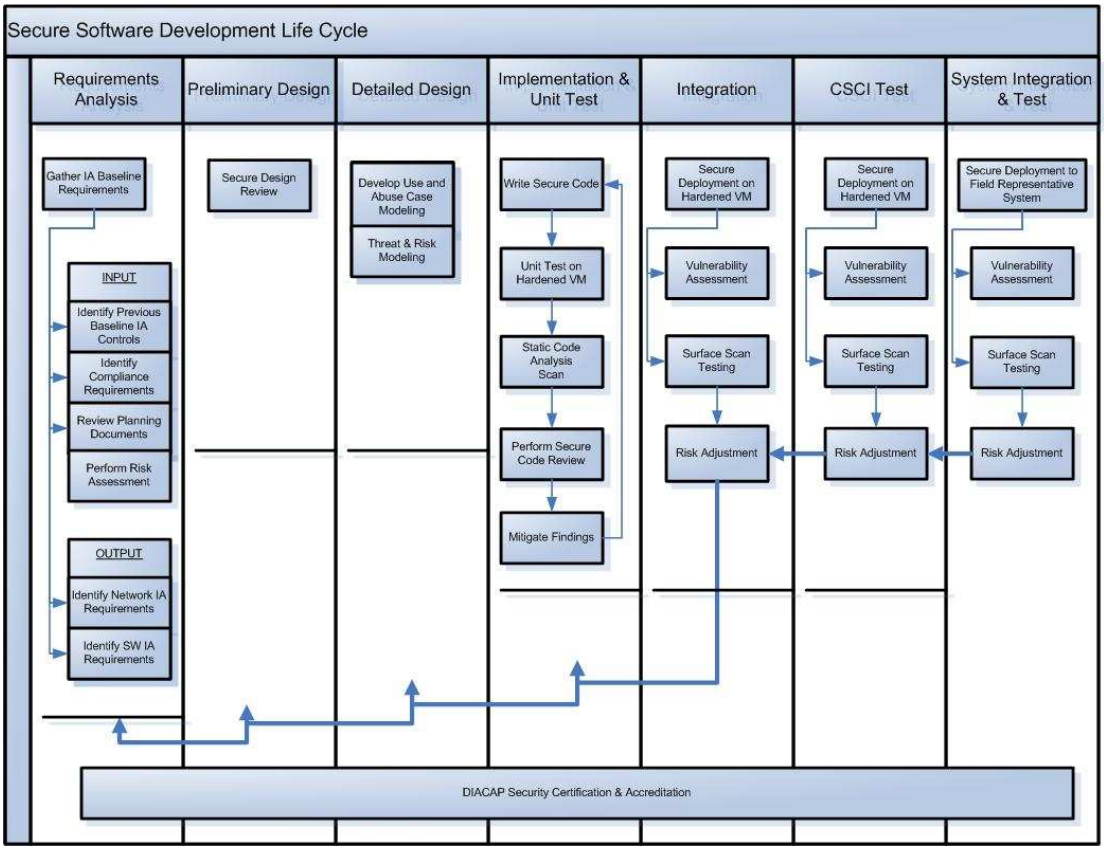


Figure 4: *Industry Standard Secure Software Development Life Cycle Activities*

Using this outlined Secure SDLC, security can be addressed over the course of the software's development life cycle. DIACAP artifacts can now be gathered during each phase and compiled in order to deliver a more complete system profile. Installation and deployment activities will incorporate security controls in order to maintain the security posture of the system from implementation through integration and test. Threat analysis, system modeling, and security design review will provide the opportunity to identify system exploitable attributes before any code is written. Vulnerability assessments using static code scan tool and surface scan tools will provide output for determining if the software was developed to specifications identified during the security design review. The end product will be both hacker resistant and security hardened.

SUMMARY

The Secure SDLC has as its base components all of the activities and security controls needed to develop DoD compliant and industry best practices hardened software. A knowledgeable staff as well as secure software policies and controls is required in order to truly prevent, identify, and mitigate exploitable vulnerabilities within developed systems. Not meeting the least of these activities found within the secure SDLC provides an opportunity for misuse of system assets from both insider and outsider threats. Security is not simply a network requirement, it is now an Information Technology requirement which includes the development of all software for the intent to distribute, store, and manipulate information. Therefore, as a developer in the defense industry contractors must implement the highest standards of development in order to insure the highest quality of products for its customers and the lives which they protect.

REFERENCES

Aras, O, Barbara, C, & Jeffrey, L. (2008). Secure software development-the role of it audit. *Information Systems Control Journal*, *4*.

Defense Information Systems Agency, DISA Field Security Operations. (2006). *Application services security technical implementation guide,* Washington, DC: Defense Information Systems Agency. Retrieved from http://iase.disa.mil/stigs/stig/application-services-stig-v1r1.pdf

Defense Information Systems Agency, DISA Field Security Operations. (2010). *Application services security technical implementation guide,* Washington, DC: Defense Information Systems Agency. Retrieved from http://iase.disa.mil/stigs/stig/

Paul, M. (2008). *The need for software security*. Retrieved from https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/Certification_Programs/CSSLP/CSSLP_WhitePaper.pdf

Dowd, M, McDonald, J, & Schuh, J. (2007). *The art of software security assessment*. Boston, MA: Pearson Education, Inc.

Maxon, R. (2008). *Software assurance best practices for air force weapon and information technology systems – are we bleeding?.* Published manuscript, Department of Systems and Engineering Management, Air Force Institute of Technology, Wright-Patterson Air Force Base, OH. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA480286&Location=U2&doc=GetTRDoc.pdf

Full Article Available Online at: Intellectbase and EBSCOhost | JISTP is indexed with Cabell's, JournalSeek, etc.

JOURNAL OF INFORMATION SYSTEMS TECHNOLOGY & PLANNING

Journal Homepage: www.intellectbase.org/journals | ©2010 Published by Intellectbase International Consortium, USA

EXAMINING THE ROLE OF THE CHIEF INFORMATION SECURITY OFFICER (CISO) & SECURITY PLAN

Maurice Dawson[1,2], Darrell Norman Burrell[3,4], Emad Rahim[5,6] and Stephen Brewster[7]

[1]Morgan State University, USA, [2]Colorado Technical University, USA, [3]A. T. Still University, USA, [4]Virginia International University, USA, [5]Morrisville State College, USA, [6]Walden University, USA and [7]Capitol College, USA

ABSTRACT

The Chief Information Security Officer (CISO) is an emerging role in many organizations as cyber security continues to be on the minds of many executives. As the number of vulnerabilities and attacks on large enterprise systems continue to rise there must be an identified key leader with full responsibility. Thus understanding the role and need of the CISO is essential to all organizations that have any technological footprint. One of the most important artifacts from a CISO is the security plan which provides an organization its direction in terms of providing availability, integrity, confidentiality, non repudiation, and authentication.

Keywords: *Cyber Security; Leadership; Executive Management.*

PURPOSE

The purpose of this submission is to present an argument and discussion on the subject concerning the roles and responsibilities of the Chief Information Security Officer (CISO). Five steps to an effective strategic plan is also included. The paper shall discuss the author's view as written and the view from the Defense and Aerospace Industry to include further discussion as to how to properly implement information security.

A key component to every good security team is the Chief Security Officer. This administrative role is primarily responsible for all information security within the organization. The security directives, policy, and responsibilities are strictly managed under the CISO position. The CISO's three most primary objectives are:

- Ensure business continuity and disaster recovery (Barr, 2007)
- Enforcing security policy (Barr, 2007)
- Aligning security strategy with business goals (Barr, 2007)

The CISO must engage the C-Suite Colleagues, such as the Chief Executive Officer (CEO), in order to gain support of security objectives within the company. The CISO must procure security funds for training and technologies though communications with the CEO. The CEO ensures that proper funding

is allocated for training, personnel, and technology. The CISO must motivate and lead teams and bring about a security aware culture within the organization. CISOs are constantly testing and evaluating the effectiveness of company security policies, procedures, and practices. This allows for the CISO to divert procured funds to resolve high priority risk. In order for the CISO to reduce security administration costs, the CEO must provide solutions to business barriers which prevent the merge of security functions. Likewise, in order for the CEO to maintain a level security funding the CISO must present performance metrics.

The CISO and the Chief Privacy Officer (CPO) also work closely together to define and meet organizational security needs. In an effort to enforce security policies within the company the CISO must dictate the security regulations and guidelines through security awareness training. At the same time, the CPO must monitor access controls, authorization, data transmission, and network logging.

The CISO maintains a set of skills in which lie the foundation of his/her performance. These skill sets include budgeting, team building, crisis management, and vendor management. Often times CISOs are required to obtain their Masters in Business Administration in order to better integrate organizational business goals with security objectives (Barr, 2007). The budget is critical to any security plan. The CISO must use budgeting skills to reflect a positive return on security investments. "Approximately 42 percent of organizations polled in the 2007 Computer Security Institute Computer Crime and Security Survey said they used Return On Investment (ROI) to measure their information security investments" (Fitzgerald, 2008). There has been a 39 percent increase from the previous year. However, this increase is 55 percent less than reported in 2004. The Internal Rate of Return (IRR) measures were reportedly used by 21 percent of the respondents, and Net Present Value was reported by 19 percent of the respondents (Fitzgerald, 2008).

The CISO must develop security policy analysis of Commercial Off The Shelf (COTS) technology, and personnel that provide the CEO with multiple financial options. The CISO is responsible for developing a security team. The CISO has to see beyond the documented skill sets of potential team candidates and assess the interoperability of the potential employee (Barr, 2009). The CISO must manage and periodically review risk to company assets from probable threats and vulnerabilities. However, risks are never alleviated, only reduced. Thus, in a time of crisis a CISO must remain calm, decisive, and authoritative as not to tarry. Vendor management allows for the CISO to produce project management metrics such as earned value management information (Barr, 2009). Also, the CISO must negotiate all customer Service Level Agreements (SLA) between their current organization and outsourced companies.

The role of the CISO is both rewarding and complex. The CISO must perform as an administrator, yet also put forth efforts managing the implementation and development of security controls. This role is critical in order to align the business objectives of an organization with that of the security objectives. Financial, personnel, vendor, security, and company direction are all influenced by the CISO. Organizational culture is implemented from top down, from C-Suite Colleagues to the workstation employee. Therefore the culture of any organization can only obtain security practice standards through the effective leadership of the CISO.

A key artifact that the CISO is responsible for is the security plan. This plan encompasses all facets of security whether technical or physical. Through research it has been indicated that there are steps to

developing a proper plan. In the next section of this submission we shall further discuss the complete steps needed to create a security plan.

INTEGRATED STEPS TO DEVELOPING A SECURITY PLAN

Presented by Sarah Scarlet is a paper detailing the five steps to an effective strategic plan as it relates to Information Assurance (IA) or Information Systems (IS) security. The first item is to begin with the business's big picture plan (Scarlet, 2005). What this means is to start out what is overall goal for the business. What is the intended function of the organization so one can develop a plan that is aligned with this particular function. With this stated think of business plan that be aligned and changed as original plans morph themselves. In the creation of this business plan the functional leaders from business need to be involved from the beginning to ensure that support is obtained. This allows insight to budgets which directly affect what the IA department may be able to due to in planning for future requirements. Knowing what the budget is shall help prioritize mission capabilities over a three year cycle. However once the budget is known for the three year cycle is best to look at this budget quarterly to track progress and see if the budget has changed.

The second step is to perform risk assessment as it relates to potential threats to the system. Below is a diagram specifying the displaying potential threats, threat agents, and areas of potential harm as they relate to systems. These items will be protected through the technical security requirements.

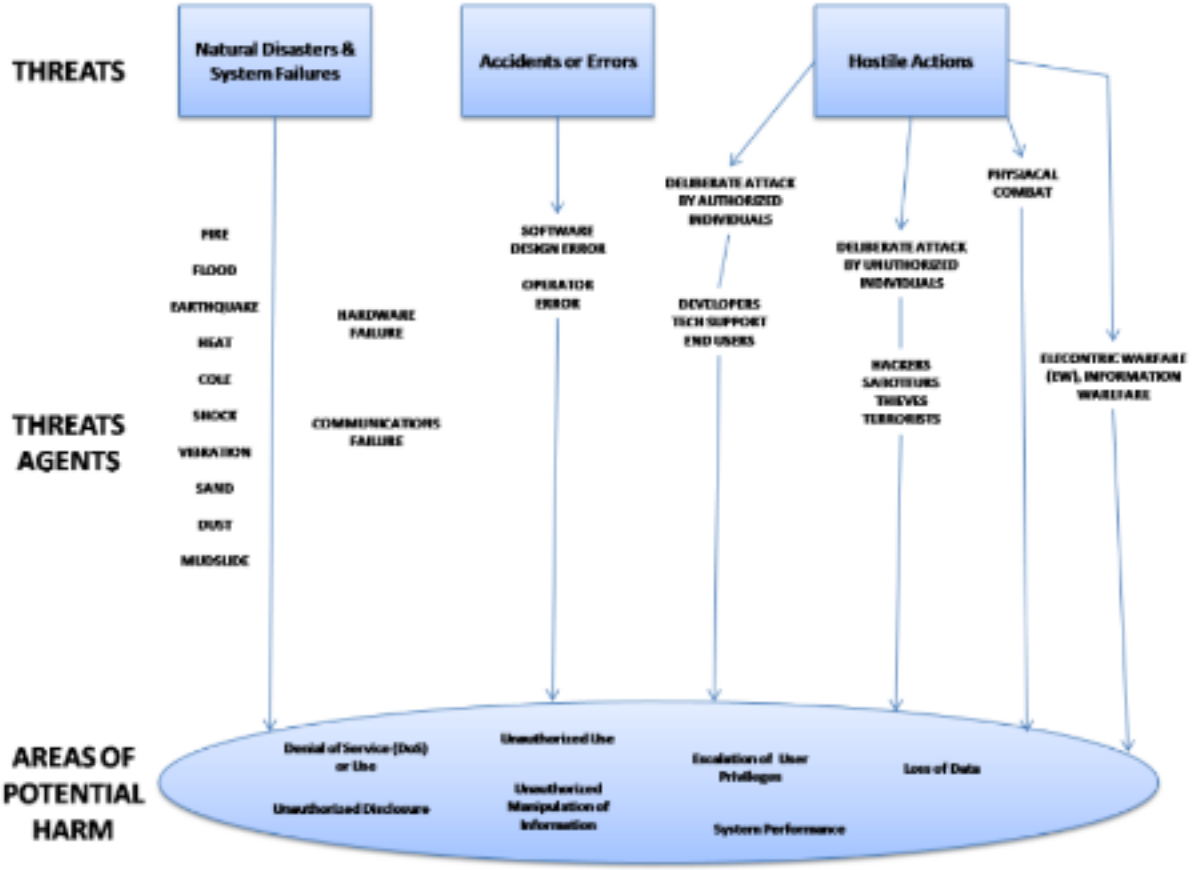


Figure 1: Threat Model

An approach to protecting these threats is to utilize a Defense-In-Depth approach. This is the proposition that multiple layers of security are better than a single protection mechanism. This method is an important part of an IA layered defense. Defense-In-Depth describes the actions taken within the Department of Defense (DoD) to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks. The three core components of Defense in Depth are people, technology, and operations. Specific ways to protect however not limited to uses of cryptography, cryptographic protocols, manageable lines of source code, active anti tamper, passive anti tamper, antivirus software, guards, and TEMPEST protection mechanisms.

The third step is to set measurable goals (Scarlet, 2005). Goals are useless if one cannot properly measure their effectiveness. There needs to be a strategic plan which is the long term objective and a tactical plan which covers the short term objectives. A short term plan could detail software patches. A key item is to find metrics than can measure how well you can meet those objectives over time (Scarlet, 2005).

The fourth step is to recognize there is no correct time frame (Scarlet, 2005) Scarlet discusses this in relation to non military government organizations however many military organizations are usually bound by budgets set forth by Congress which have strict timelines for program funding. In the government there is a cycle for major funding which all goals and objectives must be stated and categorized according to mission need. From this point is when the allocation is found and from here various milestones are created from previous stated mission needs, goals, and or objectives.

The last step is to stay flexible as it is more important to know what is truly flexible than how far your plan stretches out (Scarlet, 2005). With this stated this is very true and applicable in the military setting as one may have to prioritize goals. When prioritization of goals occur in military programs some items may be pushed out further and other brought in. This is generally up to the Program Manager (PM) to make this item occur as they are generally the ones responsible for managing the program.

IMPLEMENTING ADEQUATE SECURITY

First provide a complete high-level description of the system architecture, including diagrams or drawings to amplify the description highlighting the information security features of the system. Describe all components of the system. The description should include all critical elements required for the mission need. Clearly define the functions or capabilities expected in the fully accredited system and the mission for which it will be used. Include functional diagrams of the system. Provide the intended flows of data into the system, data manipulation, and product output. Define the system criticality and the acceptable risk for the system in meeting the mission responsibilities. System criticality should consider the impact if the system were not operational. Define the system user's security clearances, their access to specific categories of information processed, and the actual information that the system is required to process. If the system's authorized users include contractor personnel, indicate how proprietary information will be protected. Define the system life cycle and where the system is in relationship to its life cycle.

Second address the operating environment by providing an overview of the operating environment. Include a description of the facility, physical security, administrative procedures, personnel, maintenance procedures, and training plans that provide security to the system. Describe the physical environment in which the system will operate including floor plans, equipment placement, electrical and plumbing outlets, telephone outlets, air conditioning vents, sprinkler systems, fences, and extension of

walls from true floor to true ceiling. The physical security of a system will depend on the complexity and organizational requirements. The goal is to describe security that will be in place throughout the system's life cycle. Identify the procedures needed to counter potential threats that may come from inside or outside the organization. Identify the routine office security practices that ensure unauthorized access to protected resources is prohibited. The physical security description should also consider safety procedures for personnel operating the equipment. Identify the administrative security procedures including the manual operations that counter threats. For example, separation of duties is an administrative activity that provides internal controls designed to make fraud, abuse, or espionage difficult without collusion. Identify the number and type of personnel required to operate and maintain the system. Identify routine maintenance procedures and the number of personnel required to maintain the system. Certain categories of information may mandate special maintenance procedures to ensure physical security protection against unauthorized access to the information or system resources.

Third identify the training for individuals associated with the system's operation and determine if the training is appropriate to their level and area of responsibility. Describe the training requirements, types of training, who is ultimately responsible for preparing and conducting the training, equipment that will be required to conduct training, and training devices that must be developed to accomplish training. Another item to address is the cycle of this training and what further training is needed to handle more responsibility on the equipment.

The last step is to properly define the potential threats and single points of failure that can affect the confidentiality, integrity, and availability of the system. Clearly state the nature of the threat that is expected and where possible, the expected frequency of occurrence. Unintentional human error, system design weaknesses, and intentional actions on the part of authorized as well as unauthorized users can cause these events. Most systems have common threats, such as penetration attempts by hackers, damage or misuse by disgruntled or dishonest employees, and misuse by careless or inadequately trained employees. Generic threat information is available but it must be adapted to clearly state the threats expected to be encountered by the system or perceived threat.

REFERENCES

Barr, J. (2009). Essential CSO Skills. *Faulkner information services*. Retrieved January 26, 2010, fromhttp://wf2dnvr6.webfeat.org/

Barr, J. (2007). Profile: Today's CSO. *Faulkner information services*. Retrieved January 25, 2010, fromhttp://wf2dnvr6.webfeat.org/

Benson, R. J., Bugnitz, T., and Walton, B. (2004). *From Business Strategy to IT Action: Right Decisions for a Better Bottom Line*. Wiley.

Fitzgerald, M. (2008, June 23). Security and business: financial basics [Web log message]. Retrieved fromhttp://www.csoonline.com/article/394963/security-and-business-financial-basics?page=1

Security Solutions for Hyperconnectivity and the Internet of Things

Maurice Dawson
University of Missouri-St. Louis, USA

Mohamed Eltayeb
Colorado Technical University, USA

Marwan Omar
Saint Leo University, USA

A volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

IGI GLOBAL
DISSEMINATOR OF KNOWLEDGE
www.igi-global.com

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Dawson, Maurice, 1982- editor. | Eltayeb, Mohamed, 1978- editor. | Omar, Marwan, 1982- editor.
Title: Security solutions for hyperconnectivity and the Internet of things / Maurice Dawson, Mohamed Eltayeb, and Marwan Omar, editors.
Description: Hershey, PA : Information Science Reference, [2017] | Series: Advances in information security, privacy, and ethics | Includes bibliographical references and index.
Identifiers: LCCN 2016023423| ISBN 9781522507413 (hardcover) | ISBN 9781522507420 (ebook)
Subjects: LCSH: Cyberterrorism--Prevention. | Computer crimes--Prevention. | Internet of things. | Computer security. | Data protection.
Classification: LCC HV6773.15.C97 S43 2017 | DDC 005.8--dc23 LC record available at https://lccn.loc.gov/2016023423

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 10
Tails Linux Operating System:
The Amnesiac Incognito System in Times of High Surveillance, Its Security Flaws, Limitations, and Strengths in the Fight for Democracy

Jose Antonio Cardenas-Haro
University of Missouri – St. Louis, USA

Maurice Dawson
University of Missouri – St. Louis, USA

ABSTRACT

After the information released by Edward Snowden, the world realized about the security risks of high surveillance from governments to citizens or among governments, and how it can affect the freedom, democracy and/or peace. Research has been carried out for the creation of the necessary tools for the countermeasures to all this surveillance. One of the more powerful tools is the Tails system as a complement of The Onion Router (TOR). Even though there are limitations and flaws, the progress has been significant and we are moving in the right direction.

DOI: 10.4018/978-1-5225-0741-3.ch010

INTRODUCTION

The erosion of privacy in the Web has created a movement from the free software advocates, in the search and development of free and proper tools for everybody. The TOR project is the core of this movement, followed by other many tools which are part of The Amnesic Incognito Live System (Tails). In this document is analyzed the importance of Tails and all its tools in the fight for privacy, freedom, and democracy.

THE BIRTH OF PUBLIC TOR

TOR project was set by the government and developed by the Defense Advanced Research Projects Agency (DARPA) as a security measure to avoid national and international surveillance of the classified government operations (Fagoyinbo & Babatunde, 2013). The Onion Routing principle is the use of several layers of encryption to conceal a user's location and ensure private and anonymous communications. Every router in this network only knows the address of the previous router and the address of the following one (Reed, Sylverson & Goldschlag, 1998).

Later the TOR project was released as a free software, and the development continues with funding from diverse sources (Tor: Sponsors, 2010); and these give more confidence to the public about its independence and reliability. So the use of this secure network soon became very popular in all the world propitiating its grow in many users and routers as well. The development of this project is continuous and dynamic; we are now in the second generation of TOR (Dingledine, Mathewson & Syverson, 2011).

This network was made available as a protection of the individuals' privacy (which is a constitutional right in most countries), and to promote and maintain the freedom of confidential communications through the Internet among the public, avoiding or, at least, making very hard the monitoring of them. TOR is an excellent tool not only for the hide of political activists but also for domestic violence survivors to escape abusers (Russell, 2014), or just for regular users to bypass censorship (Gurnow, 2014).

The National Security Agency (NSA) has said that TOR is "the King of high secure, low latency Internet anonymity" (The Guardian, 2013). The TOR project received an award for projects of social benefit from the FSF (Free Software Foundation) in 2010, acknowledging it not only for the privacy and anonymity that it provides, but also for the freedom of access and expression on the Internet granted to millions of people, which has proved to be pivotal in dissident movements around the world (FSF, 2010). The Business Week magazine has described it as one of the most effective means to defeat surveillance around the world (Lawrence, 2014).

HOW IT WORKS

The more people using TOR network, the better. It is easier for a person to be anonymous among many others, it is harder to keep track of someone in a busy unknown and highly tangled network that is frequently changing and mixing up the connections randomly (Edman, Sivrikaya & Yener, 2007). As an analogy, we can say that a chameleon to camouflage effectively needs leaves, branches and trees, the more, the better for the blend. In defeating surveillance, we need to take care of several aspects. Who we talk to and when is just as important as what we said, and to secure these we also need encryption and randomness in the routing as well. The messages from the different anonymous users are shuffled and then sent to the next randomly selected router, shuffled again and so forth until the final destination is reached. So as an observer it is very hard to know which data were coming into the TOR network corresponds to which data coming out of it.

All the data is encrypted, including the origin and destination IP addresses, every time before it is sent to the next relay of the anonymous circuit. Since the TOR is a dynamic network that is constantly evolving, the path that our packets take to change all the time making things harder for the observer (Dingledine, Serjantov & Syverson, 2006). The users can set up a browser, a relay, a hidden service or all of them. Also "bridge relays" can be used to circumvent any blocking to the TOR network.

THE NECESSITY OF ANONYMITY AND CYBER SECURITY

We all need privacy for many diverse reasons, and is not only about the individuals, but also the private companies and even the governmental entities in the world need some anonymity at different levels. Journalists who want to protect their sources, or the law enforcement agencies that require communication with their infiltrated personnel in criminal groups protecting their identity, or the human rights activists in oppressive regimes, or the private companies in avoiding the disclosure of their technological developments for economic reasons, or the governments saving a lot of information for national security.

Surveillance and Espionage have always being an issue; several countermeasures have been developed according to the times, but now is harder than ever. The cell phones can easily be converted into tracking devices and recordings of the phone calls, web pages visited, Internet search history and interactions in social media can create a detailed profile of anyone. The persons can be affected negatively by all these. They could suffer work discrimination because of their political views, or even their physical integrity could be in danger for those who are living in tyrannic regimes, like the recent case of Niloy Neel a Bangladeshi blogger killed in Dhaka

(BBC, 2015). The governments are always looking for ways to have more control and capabilities for surveillance; Linus Torvalds, the creator of the Linux Operating System (OS) and still in control of the development of the Linux kernel, revealed that the NSA asked him to put a backdoor in the OS (Greenwald, 2014).

Furthermore, there is the high risk of a democracy degrading into an authoritarian state if its citizens are surveilled to the degree of losing their privacy. The government can face significant economic risks if sensitive information is leaked, as in the case of the tax accounts hacked in the IRS (Weise, 2015). The use of technology is increasing and spreading quickly in most of the devices used by humans, which represents a new security threat if the owners lose the control of them, as in the case of the car hacked when in the middle of the road (Ward, 2015). For all these and more, the governments and the citizens are always looking for ways to avoid the intrusion in their data and systems.

BIRTH OF TAILS OPERATING SYSTEM

The first version of the operating system The Amnesic Incognito Live System (Tails) was released in mid-2009 as a merge of the Incognito and Amnesia Linux distributions. It was created by a team of anonymous hackers which still are in charge of its development, with support and funding from the TOR project and the Freedom of Press Foundation (FPF) (Finances of Tails., 2015), and also from the Debian and Mozilla projects (Tails report, 2014), and other sources that continue founding it. The Tails project is based on the Debian distribution with the security and anonymity as a core philosophy to give privacy to anyone anywhere. Tails were born as a complement of TOR to enhance the anonymization of their users. The Tails Linux distribution became so famous after being known that is the OS used by Edward Snowden, the whistleblower who leaked information about the PRISM project to The Guardian and The Washington Post newspapers (Finley, 2014). The Tails team created this Linux distribution as a countermeasure of erosion of online privacy. The big companies of the Internet, as well as the governments (especially in totalitarian regimes), want to take away our privacy making our lives more transparent every time.

THE STRENGTHS

The Tails OS is an integrated system consisting of several tools aimed to avoid the detection of the identity of their users. It is designed to boot from a removable live media as a Universal Serial Bus (USB) stick or a Digital Video Disk (DVD), and

the saving of any file in it is deleted after a reboot for security reasons; of course, we can use the hard drive or another USB memory for the saving of the required data. In the case when we really want to delete any document, videos, pictures or any data file, the Tails is equipped with a tool called "Nautilus Wipe" for securely deleting the data; this is necessary since regular operating systems only remove the file name and link from the file system directory, not even the reformatting or overwriting of the hard drive or memory stick is a guarantee that the deleted or previous information is indeed gone. Tails come with visual camouflage that can be activated to give the look and feel of a Microsoft Windows 8 system, the purpose of this is to avoid attracting unwanted attention when working in public places.

All the traffic is handled through the TOR network, using Media Access Control (MAC) spoofing; all these to avoid leaving any digital footprint. It also gives the option to use Invisible Internet Project (I2P) as an alternative to TOR. The I2P is an anonymous overlay network used as an instrument to circumvent surveillance and censorship. This Linux distribution includes several state-of-the-art cryptographic tools to encrypt files, emails and instant messaging. It uses LUKS Linux Unified Key Setup (LUKS) which is an encryption tool for hard drives or USB sticks. All the communications with websites are encrypted automatically using Hypertext Transfer Protocol Secure (HTTPS). In the case of documents and emails, are encoded using Open Pretty Good Privacy (OpenPGP). The chatting or instant messaging is done using Off-the-Record (OTRP messaging which is another tool for encryption which also provides deniable authentication that cannot be achieved with PGP systems (Borisov, Goldberg & Brewer, 2004). It includes the "Shamir's Secret Sharing" program which runs an algorithm used in cryptography where the decryption of a message is only possible with some threshold number of participants (Shamir, 1979).

Tails also come with software to create virtual keyboard as a countermeasure against hardware keyloggers, and even with tools to anonymize metadata in files, to calculate checksums. It includes the "AppArmor" system which is a Linux kernel enhancement to confine programs to a limited set of resources. To prevent the "cold boot" attacks and forensics to the Random Access Memory (RAM), it deletes all the memory at the shutdown.

The updates to patch any security hole are available in a prompt manner as an automatic mechanism to upgrade the USB stick or the Secure Digital (SD) card to the most recent version of Tails. The creators of Tails and TOR support and promote the search for flaws in the system as a way to keep it in a continuous improvement state. This incredible operating has been created using only free software, which is a must in these cases since closed private software cannot be trustable. It is not a coincidence that Tails is the preferred operating system by Edward Snowden (Finley, 2014).

LIMITATIONS AND FLOWS

As is the case with everything, the Tails system has its limitations. This system is the conjunction of many tools, any flaw in any of its tools becomes a flaw for the Tails system. Furthermore, working effectively under this system requires some technical knowledge, most of the tools in Tails are not precisely user-friendly. It is known that the NSA has been able to crack the computers of some TOR users, but not the core security of the TOR network (Ball, Schneier & Greenwald; 2013); this has to do more with errors or carelessness from the users. Tails were created as a complement to the TOR browser, as an integrated system for the improvement of the security and anonymity.

TOR encrypts all inside its network and anonymizes the origin of the traffic, but the communications from the TOR network and the final destinations are like the regular transferring of information on the Internet. So, depending on your data, you might need to use some of the tools provided in Tails for further encryption and authentication. Also, we need to change some of our habits, it is not recommended to enable or install browser plugins, neither to open any document downloaded through TOR while online. The Tails does not protect against compromised pieces of hardware, like a key logger unless you use for this specific case a virtual keyboard "Florence" provided in one of its tools. The Basic Input/Output System (BIOS) or firmware attacks are other forms of compromised hardware.

Another important factor that needs close attention is the metadata in our files. Tails does not clear it for us, but it provides the tools necessary for the removal of information that can help to identify us from the metadata, before sending any of the files. In the case of e-mails even if we encrypt the contents, the subject and other headers remain understandable. Another problem in the case of TOR is that it does not protect us from a global adversary, this means an entity monitoring all or most of the nodes in the TOR network, such entity using statistical data may infer the relations between the users and the connections (Dingledine, Mathewson & Syverson. 2004). Another important habit here is the use of a strong password, and the Tails will not create strong passwords for you. It is not straightforward to hide the fact that you are using Tails, and this in some ways is a disadvantage, a flaw in the anonymity. Users have to be ready to update the Tails system every time that there is a patch available.

TOOL FOR FREEDOM AND DEMOCRACY

As humans, we have the natural right to privacy and in all the democracies that right is granted in the constitutions. Unapproved or unreasonable searches and seizures

go against the human rights. The exchange of information between individuals, corporations or governmental agencies has to be encrypted. It is evident that would be easier for the cops and law enforcement agencies to detect illegal activities if the information were not encrypted, but in the same way it would be easier for the criminals to affect the citizens.

The open source philosophy is a great medium to provide trustable tools to build all the infrastructure that we need to keep the freedom and democracy not only on the Internet but also in our lives. The open source has given birth to the Linux operating system, encryption tools, Wikipedia, Wikileaks, Bitcoin, BitTorrent, social media and many more valuable programs. The General Public License (GPL) is a free software license to guarantee anybody the right and freedom to use, modify and share the programs (Dawson, Leonard, & Rahim, 2015). All these show how humans around the globe can be organized without borders to improve their economies, to build the required products without the need of the private companies or centralized governments with all the toxic and corrupted control that they represent. In other words, out of the master and slave model, or without "baby sitters".

The mistrust of a central authority is common anywhere, as humans, we have the innate desire for freedom in everything. It is important to clarify that while some media and governments have slandered and libeled the DarkNet, the TOR, and the Tail Linux OS saying that these are evil tools used by criminals; all these are also essential tools used by many people for the good, including dissidents, journalists and law enforcement agencies around the world.

There is always the risk of cyber espionage or mass surveillance done by governments around the globe. In the case of US is with the project PRISM developed by the NSA (Ball, 2013). The UK has the project Tempora (Bump, 2013). In Russia is the SORM project (Paganini, 2014) and China has two significant tools for the control of the Internet, the Golden Shield (or Great Firewall) for censorship and surveillance (Randy, 2009); and the Green Dam for Personal Computer (PC) content control (Watts, 2009; Chen, 2009). There are also companies that sell technology for surveillance even to oppressive regimes (Gilbert, 2015), so we can say that all or, at least, most of the states around the world do some kind surveillance that could go worst as the technology improves and evolves. The monitoring between nations can cause tensions and damage in the diplomatic relations or even the loss of them (Smith, 2014; Menn, 2015; Fitsanakis, 2013).

Furthermore, the surveillance does not come only from the states. The private companies also want your data for economic purposes. They want to know what are you more likely to consume, to buy, and this way you could become the target of some specific advertising. Companies like Microsoft, Apple, Facebook, Yahoo, Google or Amazon among others are collecting their user's data is also for psychological manipulation to make you consume some products that other way you might

not buy. They need all the possible information from you to link it with your real life behavior, and these give them some control over you. Your cell phone location, who you share information with, who you talk to, what you buy, etc. The companies usually have arrangements with the government to share this information or they might also be under government surveillance for these data (Branstetter, 2015; Greenwald, MacAskill, Poitras, Ackerman, & Rusche, 2013; Bekker, 2013). The problem is that the more you are surveilled, the less autonomous and free you are. It is not easy to know the level and kind of control that they could exercise over us, but our freewill is indeed affected.

People are saying that they do not care about surveillance because they do not have anything to hide pure ignorance, it is like saying that they do not care about free speech because they do not have anything to say. Thanks to free thinkers and researchers, there are tools, services, protocols and free software available and under continuous development and improvement to avoid surveillance, for an anonymous and private exchange of information; science and technology is fighting back. All these come down to live a free life which is a core human value, and a foundation for any true democracy.

CONCLUSION

As more people express the desire for privacy, the demand will fuel the market as data found publicly can fall prey to those conducting Open Source Intelligence (OSINT) mining and analysis for nefarious reasons. By making the surveillance harder we protect ourselves as individuals, and all the others by making it more expensive to surveillance everyone all the time. At the end encryption and chaos is all about mathematics, and in the quest for more privacy the numbers work in our favor. It is a lot easier the encryption of the data than the decryption of it for intruders. Our universe fundamentally favors privacy. In order of having a free society, we need to have freedom from analysis about behaviors and communications among us. When considering issues about privacy, cyber terrorism, and digital crime (Dawson & Omar, 2015; Dawson, Omar, & Abramson 2015).

REFERENCES

Ball, J. (2013). NSA's Prism surveillance program: how it works and what it can do. *The Guardian*, 8.

Ball, J., Schneier, B., & Greenwald, G. (2013). NSA and GCHQ target Tor network that protects anonymity of web users. *The Guardian*, 4.

BBC. (2015). *Bangladesh blogger Niloy Neel hacked to death in Dhaka*. Retrieved from: http://www.bbc.com/news/world-asia-33819032

Bekker, S. (2013, June 20). *PRISM and Microsoft: What We Know So Far*. Redmond Channel Partner.

Borisov, N., Goldberg, I., & Brewer, E. (2004, October). Off-the-record communication, or, why not to use PGP. In *Proceedings of the 2004 ACM workshop on Privacy in the electronic society* (pp. 77-84). ACM. doi:10.1145/1029179.1029200

Branstetter, B. (2015, August 16). The NSA is asking your favorite apps how to spy on you better. *Business Insider, Daily Dot*.

Bump, P. (2013, June 21). The UK Tempora Program Captures Vast Amounts of Data – and Shares with NSA. *The Atlantic Wire*.

Chen, W. (2009, June 13). Let people decide on Green Dam. *China Daily*.

Dawson, M. (2015). A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism. In M. Dawson & M. Omar (Eds.), *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 1–7). Hershey, PA: Information Science Reference; doi:10.4018/978-1-4666-8345-7.ch001

Dawson, M., Leonard, B., & Rahim, E. (2015). Advances in Technology Project Management: Review of Open Source Software Integration. In M. Wadhwa & A. Harper (Eds.), *Technology, Innovation, and Enterprise Transformation* (pp. 313–324). Hershey, PA: Business Science Reference; doi:10.4018/978-1-4666-6473-9.ch016

Dawson, M., & Omar, M. (2015). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*. Hershey, PA: IGI Global; doi:10.4018/978-1-4666-8345-7.ch001

Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the Methods behind Cyber Terrorism. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology* (3rd ed.; pp. 1539–1549). Hershey, PA: Information Science Reference; doi:10.4018/978-1-4666-5888-2.ch147

Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The second-generation onion router*. Naval Research Lab Washington DC.

Dingledine, R., Serjantov, A., & Syverson, P. (2006, June). Blending different latency traffic with alpha-mixing. In *Privacy Enhancing Technologies* (pp. 245–257). Springer Berlin Heidelberg. doi:10.1007/11957454_14

Edman, M., Sivrikaya, F., & Yener, B. (2007, May). *A Combinatorial Approach to Measuring Anonymity*. ISI.

Fagoyinbo, J. B. (2013). *The Armed Forces: Instrument of Peace, Strength, Development and Prosperity*. AuthorHouse.

Finances of Tails. (2015). Retrieved from: https://tails.boum.org/doc/about/finances/index.en.html

Fitsanakis, J. (2013, June 20). Analysis: PRISM Revelations Harm US Political, Financial Interests. *IntelNews*.

FSF. (2010). *2010 Free Software Awards announced*. Free Software Foundation.

Gilbert, D. (2015). Hacking Team hacked: Spy tools sold to oppressive regimes Sudan, Bahrain and Kazakhstan. *International Business Times Magazine*.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillan.

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., & Rushe, D. (2013). Microsoft handed the NSA access to encrypted messages. *The Guardian,* 12.

Gurnow, M., (2014, July). Seated Between Pablo Escobar and Mahatma Gandhi: The Sticky Ethics of Anonymity Networks. *Dissident Voice*.

Harris, S., & Meyers, M. (2002). *CISSP.* McGraw-Hill/Osborne.

James, R. (2009, May 11). A brief history of Chinese internet censorship. *Time*.

Janczewski, L., & Colarik, A. (2007). *Cyber Warfare and Cyber Terrorism*. Hershey, PA: IGI Global. doi:10.4018/978-1-59140-991-5

Lawrence, D. (2014). *The inside story of Tor, the best Internet anonymity tool the government ever built*. Bloomberg Businessweek.

Levine, Y. (2014). Almost everyone involved in developing Tor was (or is) funded by the US government. *PandoDally*. Retrieved from: http://www.infowars.com/almost-everyone-involved-in-developing-tor-was-or-is-funded-by-the-us-government/

Menn, J. (2015, February 16). *Russian Researchers Expose Breakthrough US Spying Program.* Reuters.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from: https://bitcoin.org/bitcoin.pdf

Paganini, P. (2014). New powers for the Russian surveillance system SORM-2. *Security Affairs*. Retrieved http://securityaffairs.co/wordpress/27611/digital-id/new-powers-sorm-2.html

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Anonymous connections and onion routing. *Selected Areas in Communications*. *IEEE Journal on*, *16*(4), 482–494.

Russell, B., (2014, May). Domestic violence survivors turn to Tor to escape abusers. *The Verge*.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612–613. doi:10.1145/359168.359176

Smith, A. (2014). U.S. Spy Scandal Triggers Outrage, Paranoia in Germany. NBC News. August 2, 2014. "Tails report for May, 2014". *Tails*. Retrieved from: https://tails.boum.org/news/report_2014_05/index.en.html

The Guardian. (2013). *Tor: The king of high-secure, low-latency anonymity*. Tor Project.

Ward, M. (2015). Warning after security experts hack Tesla car. *BBC News*. Retrieved from: http://www.bbc.com/news/technology-33802344

Watts, J. (2009, June 8). China orders PC makers to install blocking software. *The Guardian*.

Weise, E. (2015). IRS Hacked, 100,000 Tax Accounts Breached. *USA Today*. Retrieved from: http://www.usatoday.com/story/tech/2015/05/26/irs-breach-100000-accounts-get-transcript/27980049/

KEY TERMS AND DEFINITIONS

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (Harris, 2002).

Availability: Timely, reliable access to data and information services for authorized users (Harris, 2002).

Bitcoin: Bitcoin is a peer to peer electronic cash system that no one controls and there are not printed currency (Nakamoto, 2008).

Confidentiality: Assurance that information is not disclosed to unauthorized individuals, processes, or devices (Harris, 2002).

Cyber Terrorism: Attacks with the use of the Internet for terrorist activities, including acts of de-liberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses, worms, Trojans, and zombies (Janczewski & Colarik, 2008).

Integrity: Quality of an IS reflecting the logical correctness and reliability of the OS; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (Harris, 2002).

Non-Repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (Harris, 2002).

Open Source Intelligence: Intelligence collected from publicly available sources (Dawson, 2015).

Understanding User's Acceptance of Personal Cloud Computing: Using the Technology Acceptance Model

Mohamed Eltayeb and Maurice Dawson

Abstract Personal Cloud Computing (PCC) is a rapidly growing technology, addressing the market demand of individual users for access to available and reliable resources. But like other new technologies, concerns and issues have surfaced with the adoption of PCC. Users deciding whether to adopt PCC may be concerned about the ease of use, usefulness, or security risks in the cloud. Negative attitudes toward using a technology have been found to negatively impact the success of that technology. The purpose of this study was to understand users' acceptance of PCC. The population sample consisted of individual users within the United States between 18 and 80 years of age. The theoretical framework utilized in this study was based on the technology acceptance model (TAM). A web survey was conducted to assess the measurement and understanding of patterns demonstrated by participants. Our results shows that in spite of the potential benefits of PCC, security and privacy risks are deterring many users from moving towards PCC.

Keywords Personal Cloud Computing · Cloud computing · Technology Acceptance Model

1 Introduction

Recently, cloud computing has been injected with new life from companies such as Google, Microsoft, IBM, Amazon, and others who now offer cloud computing

M. Eltayeb
Colorado Technical University, 4435 N. Chestnut St., Colorado Springs, CO 80907, USA
e-mail: Mohamed.Eltayeb@coloradotech.edu

M. Dawson(✉)
University of Missouri-St. Louis, 1 University Drive, St. Louis, MO 63121, USA
e-mail: Maurice.Dawson@umsl.edu
http://www.umsl.edu/

S. Latifi (ed.), *Information Technology New Generations*,
Advances in Intelligent Systems and Computing 448,
DOI: 10.1007/978-3-319-32467-8_1

services for personal use. In this paper, we refer to PCC as the private and hybrid cloud computing for the individual user's usage. PCC has emerged as a new paradigm model for individual users. It has transformed the user's computer device from being device-centric to information-centric [1-7]. PCC enables individuals to share music, photos, videos, documents, and applications using any computer devices connected to the network. It provides portable access from anywhere in the world to information held centrally.

Though PCC demonstrated great potential in terms of scalability and agility, and is therefore enjoying great popularity and attention, storing data and applications in the cloud is becoming very risky [8]. Many cloud users have become concerned about security and protection of privacy [9], perhaps not surprisingly as the cloud functions to store and share private data [10]. The main challenge and disadvantage users see in the adoption of cloud computing is that they lack full control over the hardware [11]. There are, therefore, several issues related to privacy and security that must be addressed before PCC can be considered reliable.

Very often, data stored in the cloud is seen as valuable to those with malicious intent [12]. Storing data and applications in the cloud is becoming very risky. It is very important for users to take personal precautions in order to secure personal, sensitive information—information they would have stored in their local computer device (laptop, desktop, phone, tablet, etc.), and now store in the cloud. It is critical for users to understand the security measures that the cloud provider has in place [13].

Predicting technology usage and adoption has become a topic of mainstream study [14]. The rapidly growing importance of technologies has led researchers to study user technology acceptance intensively. Negative attitudes toward a technology, its ease of use, and its usefulness may negatively impact the success of that technology. Indeed, several IT scholars considered the user's acceptance of a technology to be the key success factor for the adoption of that technology [15].

The remaining of the paper is organized as follows: in the next section, we present the objectives of the study. Section 2 discusses and articulates our theoretical framework. Section 3 presents the research questions and hypothesis. The population sample information are discussed in section 4. A detailed discussion of the study's data collection and validation are provided in section 5. Section 6 discusses the data analysis of the study.

Section 5 presents methods used for data collections. Section 6 discusses the data analysis. Section 7 discusses our findings; and additional findings are discussed in section 8. Our recommendation and discussion are presented in section 9. Finally, section 10 concludes the paper.

2 Theoretical Framework

This research was deductive in nature. Therefore, a quantitative method was selected to understand user's acceptance of PCC. In particular, a non-experimental quantitative approach was used. The theoretical framework utilized in this study

was based on TAM—a widely recognized model in the field of IT, introduced by Davis in 1986 [16]. Davis [16, 17] recommended TAM as the best model for investigating end user attitudes towards and acceptance or rejection of a technology. According to Gao [18], "TAM can serve the purpose of predicting user acceptance of a technology before the users get heavily involved in the technology and thus is a cost-effective tool in screening potential candidate systems or programs" (p. 3). This theoretical framework was used in this study to examine factors influencing PCC adoption.

TAM proposes two independent variables—perceived ease of use, and perceived usefulness (PU) of a technology—to predict the user's attitude toward adopting a technology [18]. Davis [16, 17] defined PU as the degree to which a user believes that the adoption of a particular technology will improve the performance of his or her job. The perceived ease of use, on the other hand, is the degree to which a user believes that using a particular technology would be effortless [17].

Since the purpose of this study was to understand users' thoughts, experiences, expectations, and security concerns with respect to the adoption of PCC, TAM was found to be the most suitable theoretical approach due to its validity and reliability in exploring and explaining users' attitudes toward using technologies [16]. Cloud computing is a new approach to computing [19], and as new technologies are introduced and are adopted, concerns and challenges emerge [20]. Therefore, this study on PCC technology has a legitimate place in research on user technology acceptance.

This research study extended TAM to include attitude towards using (ATU) as an additional independent variable. This study adapted a survey instrument tested by Davis [16], and validated by Venkatesh [21]. Overall, this study included three independent variables and one dependent variable. The independent variables are perceived ease of use (PEOU), attitude toward using PCC (ATU) and perceived usefulness of PCC (PU). One dependent variable—Intention to Use PCC (ITC)—was used broadly in this study.

3 Research Questions and Hypothesis

3.1 Research Question 1: How Does Perceived Ease of Use Influence the Acceptance of PCC?

$H1_A$: Perceived ease of use positively influences attitude toward the acceptance of PCC.

$H1_0$: Perceived ease of use has no correlation to attitude toward the acceptance of PCC.

The independent variable PEOU determines the degree to which a user believes that using PCC would be effortless. PEOU is measured on a typical scale of seven ordered continuum of response categories: Strongly disagree, Disagree, Slightly disagree, Neutral, Slightly agree, Agree, Strongly agree.

3.2 Research Question 2: How Does Perceived Usefulness of PCC Influence the Acceptance of PCC?

H2A: Perceived usefulness positively influences attitude toward the acceptance of PCC.

H20: Perceived usefulness has no correlation to attitude toward the acceptance of PCC.

The independent variable PU determines the degree to which a user believes that the adoption of PCC would improve the performance of his or her job. PU is measured on a typical scale of seven ordered continuum of response categories: Strongly disagree, Disagree, Slightly disagree, Neutral, Slightly agree, Agree, Strongly agree.

Research Question 3: How does attitude toward using PCC influence acceptance of PCC?

$H3_A$: There will be a correlation between attitude toward using PCC and the user's acceptance of PCC.

$H3_0$: There will be no correlation between attitude toward using PCC and the user's acceptance of PCC.

The independent variable (ATU) determines the degree to which a user's acceptance of PCC relates to that user's attitude toward using PCC. ATU is measured across a typical scale of seven ordered continuum of response categories: Strongly disagree, Disagree, Slightly disagree, Neutral, Slightly agree, Agree, Strongly agree.

4 Population Sample

This study used a simple random sample from Survey Monkey engineering and IT professionals panels. The minimum representative sampling size (n) was estimated to be 384 participants for this study, based on a confidence interval of 5% and a confidence level of 95%. As many participants as possible were included to increase the accuracy of statistical sampling data.

A total of 464 participants were randomly chosen to participate in the study. However, only 399 of the chosen participants fully completed the survey; 20 participants opted out and 45 were disqualified either with unanswered questions or with providing partial data. Only fully completed responses were admitted. There was a 95.69% completion rate of surveys. Thus, the number of completed responses exceeded the estimated, representative minimal sample size of 384. Several items in the survey—gender, age range, education, state, and census region—were included to further describe demographic characteristics of the sample.

5 Data Collection and Validation

This study used a web survey to collect data from participants. The survey was hosted by SurveyMonkey.com, which is considered one of the leading providers of online survey solutions. The identity of participants was kept confidential and anonymous. Participant had the right to withdraw from participation at any time. Participants were required to complete a consent form as soon as they login to the SurveyMonkey.com. The consent form store collected information confidentially. Information collected by the survey included: gender, age range, state of residence, and level of education.

The survey questions in this study were designed to express a clearly negative or positive opinion and avoided neutral opinions to solicit more definitive responses. The researcher transcribed the data collected through Survey Monkey into digital documents. Data was downloaded by the researcher after the completion of data collection. Only fully completed surveys were employed in this study. Some participants were disqualified either with unanswered questions or with providing partial data. Incomplete responses and partial data were completely discarded. Additionally, Survey data was assessed for multicollinearity, homoscedasticity, linearity, and normality [22].

6 Data Analysis

The multiple regression test was performed as follows: (1) predictors were selected using their semi-partial correlation with the outcome; (2) predictors were entered into the model based on a mathematical method using Statistical Package for the Social Sciences (SPSS) Version 19.0; (3) the selection of predictors was performed in steps [23].

Descriptive statistics, ANOVA, Chi-square, and Multiple regressions were performed to explore the relationship between the continuous dependent variable (ITU) and independent variables (PEOU, PU, and ATU). Several descriptive statistics techniques were used to depict the sample population characteristics. ANOVA was used to analyze both dependent and independent variables. In addition, the multiple regression test was performed to assess the impact of each independent variable (PU, PEOU, and ATU) on the dependent variable (ITU).

7 Findings

TMultiple regressions were performed to explore the relationship between the continuous dependent variable (ITU) and independent variables (PEOU, PU, and ATU). This research study tested the relationship between perceived ease of use, usefulness, attitude toward using PCC, and the acceptance of PCC. The model's adequacy was tested in terms of normality, linearity, and collinearity [24].

7.1 First Regression Model

The first regression was performed to determine the relationship between the independent variable PEOU and the dependent variable ITU. Six predictors of the independent variable PEOU were tested to address the first research question. The relationship between the predictors and the outcome were measured using a stepwise method, so that the unique contribution of each predictor could be assessed to explain variance of the outcome [24]. The following research question and hypothesis were tested at this stage:

How does perceived ease of use influence the acceptance of PCC?

$H1_0$: Perceived ease of use has no correlation to the acceptance of PCC.

The results of the regression analysis demonstrated a positive correlation between PEOU and the acceptance of PCC. It was found that approximately 23.5% of the variance in the acceptance of PCC can be accounted for by PEOU. Therefore, the null hypothesis was rejected and the alternative was supported.

This result is consistent with other studies showing that there is a positive correlation between PEOU and the user's acceptance of a technology. Davis [16] argued that perceived ease of use positively influence attitude toward using a technology. Perceived ease of use plays an important role in determining and predicting the user's intention to use a technology [25]. Ramgovind [26] stated "The success of modern day technologies highly depends on its effectiveness of the world's norms, its ease of use by end users and most importantly its degree of information security and control" (p. 1).

7.2 Second Regression Model

The second regression was performed to determine the relationship between the independent variable PU and the dependent variable ITU. Five predictors of the independent variable PU were tested to address the first research question. A stepwise regression was performed to build the model. The unique contribution of each predictor was measured to explain the variance of the outcome [24]. The following research question and hypothesis were tested at this stage:

How does perceived usefulness of PCC influence the acceptance of PCC?

H20: Perceived usefulness has no correlation to attitude toward the acceptance of PCC.

The results of the regression analysis demonstrated a positive correlation between PU and the acceptance of PCC. It was found that approximately 78.2% of the variance in the acceptance of PCC can be accounted for by PU. Therefore, the null hypothesis was rejected and the alternative was supported. This result is consistent with other studies showing that there is a positive correlation between PU and the user's acceptance of a technology.

7.3 Third Regressions Model

The third regression was performed to determine the relationship between the independent variable ATU and the dependent variable ITU. Four predictors of the independent variable ATU were tested to address the first research question. The relationship between the predictors and the outcome were measured using stepwise regression. The unique contribution of each predictor was measured to explain the variance of the [24]. The unique contribution of each predictor is measured to explain the variance of the outcome. The following research question and hypothesis were tested at this stage:

How does attitude toward using PCC influence user's acceptance of PCC?

$H3_0$: There will be no correlation between attitude toward using PCC and user's acceptance of PCC.

The independent variable ATU was used for determining the degree in which there is a correlation between attitude toward using PCC and users' intention to use. The results of the regression analysis demonstrated a significant correlation between ATU and the acceptance of PCC. It was found that approximately 38.2% of the variance in the acceptance of PCC can be accounted for by ATU. Therefore, the null hypothesis was rejected and the alternative was supported.

8 Additional Findings

Statistically significant differences were found between age group means, as indicated by results of the one-way ANOVA (F (5, 2.801)=2.801, p=.017). The output result of the one-way ANOVA showed that the age group significantly contributed to the variation in the respondent's acceptance of the PCC technology. Because the output result of the one-way ANOVA test demonstrated significant differences between the age groups, a Post Hoc test was conducted to further investigate which means were significantly different from each other. The Post Hoc test result

indicated that the score of the age group 40-49 was much higher than the other age groups. Also, age groups 21-29 and 30-39 appeared to accept PCC more easily compared with age groups 18-20, 50-59, and 60-80.

A chi-square test of independence was performed to examine the relation between independent variables (PU, PEOU, and ATU) and the acceptance of PCC. A significant relationship was found between the independent variables and the frequency of acceptance of PCC at p-value <0.01, and degrees of freedom of 36. Additionally, a chi-square test of independence was performed to examine the relation between age group and acceptance of PCC. No significant relationship was found between age group and the frequency of acceptance of PCC, X2(10, N=399) =17.24, p-value=.069. The acceptance of PCC among the age group was as follows: approximately 66.6% of the age group "18-20;" 75% of the age group of "21-29;" 73% of the age group "30-39;" 80.5% of the age group "40-49;" 69.9% of the age group "50-59;" and 67.3% of the age group "60-80." Overwhelming majority of users that accepted PCC were in the "40-49" age group. On the other hand, the majority of users that did not have intention to use PCC were in the age group "60-80."

9 Discussion and Recommendation

Given the results of the data analysis in this study, it is arguable that PCC is here to stay. However, there are several issues related to security and privacy that must be tackled to increase user's acceptance of PCC. Hardly a day goes by without hearing news about privacy and security concerns of users. The findings of this study demonstrated that users are concerned about the way security and privacy is handled in the cloud. Protecting users' privacy in the cloud is big business for cloud providers. The success of a technology depends greatly on its ease of use but even more crucially its degree of security [26]. According to Koved [27], "When end-users' perceptions of risk are not aligned with those on which the system is based, there is a mismatch in perceived benefit, leading to poor user acceptance of the technology" (p. 1). Thus, users' understanding of privacy and security in the cloud rapidly becomes obsolete as the PCC technology progresses. Privacy and security must be evaluated continuously to achieve information privacy and security objectives and, thereby, user acceptance.

Prior research has shown that perceived privacy and security risks in the cloud negatively influence attitude toward using cloud computing. There are always security risks when moving towards cloud computing [28]. Though computer users would like to use PCC, they are concerned with utilizing a system they do not control. Data stored in the cloud is often seen as valuable to those with malicious intent [12]. It is very important for users to take precautions in order to secure personal, sensitive information—information they would have stored in their local computer device and now store in the cloud. It is critical for users to understand the security measures the cloud provider has in place before moving toward PCC [13].

10 Conclusion

The study's objective was to understand users' acceptance of PCC and a web survey was conducted to assess it. Several key findings emerged from this research study. The results of the data analysis showed that the majority of respondents had a positive view about PCC, but the participants seemed particularly concerned about security, privacy, and data theft in the cloud. User's attitude towards PCC appeared to be the most critical factor among the three suggested determinants of PCC acceptance in this study.

References

1. Ularu, E.G., Puican, F.C., Suciu, G., Vulpe, A., Todoran, G.: Mobile computing and cloud maturity Introducing machine learning for ERP configuration automation. Informatica Economica **17**(1), 40–52 (2013)
2. Onyegbula, F., Dawson, M., Stevens, J.: Understanding the need and importance of the cloud computing environment within the National Institute of Food and Agriculture, an agency of the United States Department of Agriculture. Journal of Information Systems Technology & Planning **4**(8), 17–42 (2011)
3. Dhar, S.: From outsourcing to cloud computing: Evolution of IT services. Management Research Review **35**(8), 664–675 (2012)
4. Okezie, C.C., Chidiebele, U.C., Kennedy, O.C.: Cloud computing: A cost effective approach to enterprise web application implementation (A case for cloud ERP web model). Academic Research International **3**(1), 432–443 (2012)
5. Reavis, D.: Information evaporation: The migration of information to cloud computing platforms. International Journal of Management & Information Systems (Online) **16**(4), 291 (2012)
6. Lin, A., Chen, N.C.: Cloud computing as an innovation: Perception, attitude, and adoption. International Journal of Information Management **32**(6), 533–540 (2012)
7. Tian, Y., Song, B., Huh, E.N.: Towards the development of PCC for mobile thin-clients. In: 2011 International Conference on Information Science and Applications (ICISA). IEEE (2011). doi:10.1109/ICISA.2011.5772368
8. Dutta, A., Peng, G.C.A., Choudhary, A.: Risks in enterprise cloud computing: The perspective of its experts. The Journal of Computer Information Systems **53**(4), 39–48 (2013)
9. Han, Y., Sun, J., Wang, G., Li, H.: A cloud-based BPM architecture with user-end distribution of non-compute-intensive activities and sensitive data. Journal of Computer Science and Technology **25**(6), 1157–1167 (2010)
10. Wang, H.: Privacy-preserving data sharing in cloud computing. Journal of Computer Science and Technology **25**(3), 401–414 (2010)
11. Katzan Jr., H.: On the privacy of cloud computing. International Journal of Management and Information Systems **14**(2), 1–12 (2010)
12. Chakraborty, R., Ramireddy, S., Raghu, T.S., Rao, H.R.: The information assurance practices of cloud computing vendors. IT Professional Magazine **12**(4), 29–37 (2010)
13. Alzain, M.A., Soh, B., Pardede, E.: A new model to ensure security in cloud computing services. Journal of Service Science Research **4**(1), 49–70 (2012)

14. Selamat, Z., Jaffar, N.: IT acceptance: From perspective of Malaysian bankers. International Journal of Business and Management **6**(1), 207–217 (2011)
15. Cocosila, M.: Role of user a priori attitude in the acceptance of mobile health: An empirical investigation. Electronic Markets **23**(1), 15–27 (2013)
16. Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of IT. MIS Quarterly **13**(3), 318–342 (1989)
17. Davis, F.D.: User acceptance of IT: System characteristics, user perceptions and behavioral impacts. International Journal of Man-Machine Studies **38**(3), 475–487 (1993)
18. Gao, Y.: Applying the technology acceptance model (TAM) to educational hypermedia: A field study. Journal of Educational Multimedia and Hypermedia **14**(3), 237–247 (2005)
19. Khan, S., Khan, S., Galibeen, S.: Cloud computing an emerging technology: Changing ways of libraries collaboration. International Research: Journal of Library and Information Science **1**(2), 151–159 (2011)
20. Paquette, S., Jaeger, P., Wilson, S.: Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly **27**, 245–253 (2010)
21. Venkatesh, V.P.: An assessment of security vulnerabilities comprehension of cloud computing environments: a quantitative study using the unified theory of acceptance and use. (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (Order No. 3564324, Capella University) (2013)
22. Vogt, P.: Quantitative research methods for professionals. Pearson Education, Boston (2007)
23. Field, A.: Discovering statistics using SPSS. Sage, Thousand Oaks (2009)
24. Fabozzi, F.J., Focardi, S.M., Rachev, S.T., Arshanapalli, B.G.: Building and testing a multiple linear regression model. In: The Basics of Financial Econometrics: Tools, Concepts, and Asset Management Applications, pp. 81–102. John Wiley & Sons, Hoboken (2014)
25. Hackbarth, G., Grover, V., Yi, M.Y.: Computer playfulness and anxiety: Positive and negative mediators of the system experience effect on perceived ease of use. Information & management **40**(3), 221–232 (2003)
26. Ramgovind, S., Eloff, M. M., Smith, E.: The management of security in cloud computing. In: Information Security for South Africa (ISSA), pp. 1–7. IEEE (2010)
27. Koved, L., Trewin, S., Swart, C., Singh, K., Cheng, P.C., Chari, S.: Perceived security risks in mobile interaction. In: Symposium on Usable Privacy and Security (SOUPS), July 2013. http://cups.cs.cmu.edu/soups/2013/risk/Koved-RP-IT-2013.pdf
28. Aleem, A., Christopher, R.S.: Let me in the cloud: Analysis of the benefit and risk assessment of cloud platform. Journal of Financial Crime **20**(1), 6–24 (2013)

Research in Progress- Defending Android Smartphones from Malware Attacks

Dr.Marwan Omar
Colorado Technical University
Colorado Springs, USA
marwankhan2003@yahoo.com

Dr.Maurice Dawson
Alabama A&M University
Alabama, USA
dr.mauricedawson@yahoo.com

Abstract— **Smartphones are becoming enriched with confidential information due to their powerful computational capabilities and attractive communications features. The Android smartphone is one of the most widely used platforms by businesses and users alike. This is partially because Android smartphones use the free, open-source Linux as the underlying operating system, which allows development of applications by any software developer. This research study aims to explore security risks associated with the use of Android smartphones and the sensitive information they contain; the researcher devised a survey questionnaire to investigate and further understand security threats targeting Android smartphones. The survey also intended to study the scope of malware attacks targeting Android phones and the effectiveness of existing defense measures. The study surveyed the average Android users as the target population to understand how they perceive security and what security controls they use to protect their smartphones.**
Keywords- Malwar; Android Smartphones; Hacker; Anti-Virus; Cyber Threats; Vulnerability

Introduction

Smartphones are becoming a more integrated and prevalent part of people's daily lives due to their highly powerful computational capabilities, such as email applications, online banking, online shopping, and bill paying. With this fast adoption of smartphones, imminent security threats arise while communicating sensitive personally identifiable information (PII), such as bank account numbers and credit card numbers used when handling and performing those advanced tasks [1], [2]. Traditional attacks (worms, viruses, and Trojan horses) caused privacy violations and disruptions of critical software applications (e.g., deleting lists of contact numbers and personal data). Malware attacks on smartphones were generally "proof of concept" attempts to break to the phone's system and cause damage. However, the new generation of smartphone malware attacks has increased in sophistication and is designed to cause severe financial losses (caused by identity theft) and disruption of critical software applications [3]. Because smartphones are becoming more diverse in providing general purpose services (i.e., instant messaging and music), the effect of malware could be extended to include draining batteries, incurring additional charges, and bringing down network capabilities and services [4].

I. THEORETICAL FRAMEWORK

Smartphones are rapidly becoming enriched with confidential and sensitive personal information, such as bank account information and credit card numbers, because of the functionality and powerful computational capabilities built into those mobile devices. Cyber criminals, in turn, launch attacks especially designed to target smartphones, exploiting vulnerabilities and deficiencies in current defense strategies built into smartphones' operating systems. [5] indicated that because of skill and resource constraints, businesses are ill-prepared to combat emerging cyber threats; this claim is true for smartphones as well, given the fact that those mobile devices are even less equipped with necessary protections, such as antivirus and malware protection software. Some services and features, such as Bluetooth and SMS, create attack vectors unique to smartphones, and thus expand the attack surface. For example, in December, 2004, A Trojan horse was disguised in a video game and was intended to be a "proof of concept," which signaled the risks associated with smartphones that could potentially compromise the integrity and confidentiality of personal information contained in smartphones [6]. Attackers can easily take advantage of those services provided by smartphones and subvert their primary purpose because they can use Bluetooth and SMS services to launch attacks by installing software that can disable virus protection and spread via Bluetooth unbeknownst to smartphone users.

With the development of innovative features and services for smartphones, security measures deployed are currently not commensurate because those services and features, such as MMS and Bluetooth, are driven by market and user demands, meaning that companies are more inclined to provide more entertainment features than security solutions. In turn, this further increases vulnerabilities and opens doors for hackers to deploy attacks on smartphones. Furthermore, [7] argue that the operating systems of smartphones allow the installation of third-party software applications, coupled with the increase in processing power as well as the storage capacity. This poses more security challenges because hackers could exploit those vulnerabilities, which are further compounded by users' lack of security awareness. Smartphone attackers are becoming more adept in designing and launching attacks by applying attack techniques already implemented on desktop

978-0-7695-4941-5/13 $26.00 © 2013 IEEE
DOI 10.1109/ACCT.2013.69

and laptop computers; smartphones' enhanced features, such as music players and video games, produce easy-to exploit targets by sending seemingly benign files via music or video game applications to users and lure them into downloading such files. [8] indicated that attackers could exploit such vulnerabilities to spread worms autonomously into smartphones. Therefore, hackers usually use a combination of technical expertise along with some social engineering techniques to trap users into accepting and downloading benign applications, which are used later to execute malicious code and affect critical applications running on smartphones.

II. Research Objectives

The primary goal of this research study is to investigate security risks associated with the use of Android smartphones and then propose to design an effective, real-time, integrated defense framework for Android smartphones. This study will contribute to identifying top security threats facing Android phones and the confidential information they contain. The proposed solution will detect attacks (viruses, worms, and Trojan horses) and prompt users to take actions to prevent breaches; any suspicious activity that may reveal personal information to third parties or unknown entities will be reported to users to prevent potential attacks. Smartphones contain easy-to-exploit vulnerabilities as well as sensitive personal information, which collectively offer appealing motives for attackers to target them to gain financial incentives [9]. A focused review of the literature reveals that there have been many protection strategies offered for securing smartphones and ensuring user privacy; however, most of those endeavors are small-scale and tackle particular areas of protection, such as access control [10] and anomaly detection [11]. This research study is different in that it will leverage previously proposed and implemented defense strategies and present an enhanced protection framework that will address Android's vulnerabilities and risks. Furthermore, this project will extend the existing knowledge about Android smartphones' security and provide in-depth understanding of how to effectively manage emerging threats and fend off attacks, an issue that has long been realized and pointed out by security researchers and required more extensive research [12].

III. The research problem statement

Google's Android is free, open-source software that allows the development and programming of third-party software programs, in addition to being used as a tool to handle e- commerce tasks and perform online banking activities. Android's core components, such as Linux and connectivity media, are vulnerable to attacks through which personal and confidential information is likely to be compromised. Android's threats are further amplified by the fact that users are limited to using their smartphones for basic services and functions, such as email and SMS/MMS. Users lack the programming mind-set to protect their Android smartphones and stay current with the latest security software updates. This gives hackers an edge to target Android smartphones in the hope of gaining unauthorized access to disable core services (email and web browsing), abuse costly services (i.e., sending MMS/SMS and making calls to high-rate numbers), eavesdrop on calls, and most importantly compromise sensitive information to be sold for a price. Android's open-source nature further increases security vulnerabilities because attackers could easily exploit this feature to modify the core applications and install malicious software, which could be used to compromise Android-based smartphones and ultimately cause disruption and monetary loss.

IV. Research Questions

Research Question1: What are the shortcomings of current security practices in Android smartphones?
Research Question 2: Has research fully addressed the importance of protecting sensitive personal data in Android smartphones and recommended defenses and mitigation countermeasures?
Research Question 3: Are the operating systems of Android smartphones able to handle processing power required to implement an integrated security framework to provide real-time security for confidential data?
Research Question 4: What protection mechanisms (i.e., antivirus, access control, intrusion detection, and encryption) have proven to be most robust in protecting confidential data and ensuring user privacy?

Research Question 5: Which attack techniques/vectors (i.e., Bluetooth, Wi-Fi, MMS, video games, music files, and SMS) are most popular among attackers, and what is the extent of their damage?

V. METHODOLOGY

The researcher used a quantitative, descriptive survey design strategy to collect and analyze data from Android smartphone users. Surveys are very commonly used in current research and are considered to best suit quantitative data analysis, in addition to the fact that survey results and findings can be replicated on the same people at different times to further confirm or refute previous findings. A link to the online Android security survey, which was hosted on the popular commercial Survey Monkey website, was sent to 200 Android users, including people from different industries and professions who were randomly chosen as a sample of the population of interest (the population of interest encompassed the average Android users who were of both genders, 18 years old or older, and belonged to a variety of industries and professions). The survey webpage included clear and detailed information about ensuring complete anonymity of research participants as well as maintaining the confidentiality of their identity and the information

provided. Potential respondents were asked to voluntarily take part in the study, and they also had the option of declining to participate or exiting the online survey at any stage during the survey process. The survey was available for five months and ran from August 2012 until December 2012; 45 completed responses were received from the Survey Monkey website.

Also, respondents were required to answer all 25 questions in the questionnaire for their responses to count as complete. The survey questionnaire included 25 questions and was designed to be completed in about 5 minutes to encourage more respondents to take part in the survey and thereby maximize the response rate, which reached about 22%. A response rate of 22% with a sample size of 200 is considered a valid sample size statistically [13]. The researcher ensured that the only data collection method would be to count the responses received from Survey Monkey and that no other responses were counted if they were received in any other form. This data-gathering fashion can guarantee standardization and contribute to the objectivity of research results. A total of 46 people responded to the survey, 45 of whom provided complete answers to all 25 questions. Any incomplete responses were discarded to further validate representativeness of results, as there was only one respondent who did not complete the survey and was listed as an outlier.

The study was conducted anonymously (respondents were unknown to the researcher) to maximize representativeness and minimize potential bias. The researcher did not consider using other forms of data collection, such as sending the survey to potential respondents by first class mail, due to financial concerns and time constraints. Personal interviews were also discarded because respondents are more inclined to express their true experiences anonymously, in addition to the fact that the researcher had decided to conduct this study in a double-blind manner, meaning that potential respondents and the researcher did not know each other. A consent form was attached to the online survey webpage to express anonymity of the research study and ensure respondents' privacy and confidentiality of information collected. The research clearly stated that participation in the survey was voluntary and that all responses would be confidential.

A. About the Pilot Study

The objective of the pilot study was to ensure the appropriateness and adequacy of questions for the sample of interest and incorporate feedback and suggestions from the pilot study participants to enhance the survey and make slight changes on the questions' format and style. For the pilot study, the researcher chose ten respondents who were all Android users and met the criteria for the research population. A link to the online survey was sent via email to ten participants over a period of two weeks. Constructive feedback and valuable insights were received from some participants who suggested a few changes to the way some questions were asked and the choices provided for those answers.

B. Population of Interest and Representativeness of Results

The population of interest was Android users among the general public who were from both genders and over the age of 18; all respondents had at least completed high school and some of them had a college degree. All respondents used Android phones on a daily basis with a vast majority of them downloading apps for a variety of purposes, such as entertainment, financial transactions, and web browsing. A random sample of Android users was chosen from this population where the chances of including any user from any other sample was equal, and therefore, the sample was as representative as possible and the risk of bias was reduced to a minimum. Furthermore, the researcher chose to conduct this study in a double-blind manner where the researcher and respondents did not have any direct communication, nor did they know each other. This method prevented personal prejudices from influencing the results of this study.

C. Data Collection Procedure

A link to the online Android survey hosted by Survey Monkey was distributed to potential respondents, and the researcher created an account with Survey Monkey to save all the responses received. The researcher ensured that the only data collection method would be to count the responses received from Survey Monkey; no other responses were counted if they were received in any other form. This method for gathering data guarantees standardization and contributes to the objectivity of research results. A total of 46 people responded to the survey, 45 of whom provided complete answers to all 25 questions. Any incomplete responses were discarded to further validate representativeness of results, as there was only one respondent who did not complete the survey.

D. Delimitation of The Study

This research study was uniquely designed for smartphones using the Android platform as the underlying

operating system; the research design methodology only encompassed the general public of Android users and advertently excluded participants who would be "tech-savvy" in order to meet the purpose and objectives of the dissertation. Also, the research study did not address any security threats or risks associated with the Android hardware, such as battery life or stealing or losing the phone physically. Furthermore, the results of the study represent what survey participants reported and may not be considered as ideal perspectives. Finally, the findings will not be applicable to other mobile platforms, such as Windows Mobile and Symbian. This study mainly provides insightful solutions for major types of malicious attacks, such as viruses, worms, and Trojan horses; it does not encompass attacks based on exhausting battery power or any other types of attacks outside of the scope of malware attacks.

VI. HYPOTHSES

Hypothesis 1: Current security mechanisms of Android smartphones are ineffective at withstanding well-crafted malware attacks. Authentication measures (i.e., user name and password) and antivirus software are reactive and can only detect known malware. Furthermore, Android, unlike other platforms such as iPhone and Blackberry, does not have any built-in encryption, which in turn makes Android phones attractive and soft targets for malware writers.

Hypothesis 2: The top security risks to Android phones stem from Android apps where hackers can conveniently pass and deliver their malicious apps to the Android Market with no restrictions. The Android Market does not enforce any kind of testing or vetting process to certify apps and filter rogue ones. Moreover, current security mechanisms implemented by the Android platform does not distinguish malicious apps from legitimate ones. Therefore, malicious apps (once installed onto Android phones) can misuse their access to phones' resources and commit unauthorized activity, such as sending users' confidential information to remote servers operated by hackers.

Hypothesis 3: Android devices are exposed to and vulnerable to a variety of threats, which can be exploited by hackers. Examples include threats of rogue and malicious apps, which can abuse their capabilities when accessing the phones' resources and thus send users' private information to remote servers without users' knowledge or consent. Most recently, there was an Android Trojan that was capable of sending SMSs and recording phone calls from victims' smartphones.

Hypothesis 4: Hackers have previously launched attacks on Android smartphones. Therefore, an integrated and effective security solution is required to address vulnerabilities and threats within Android devices.

CONCLUSION

This research will contribute to raising awareness among security experts and the academic community about the impact and consequences of smartphone attacks, which is something that has not yet been fully recognized. This is critically important given the fact that smartphones, if compromised, can be used to cause extensive damage and disruption for individuals and businesses alike. The contribution of this study is further exemplified by extending the body of knowledge for smartphone security and stimulating the need for more extensive research in this area. The contribution will be particularly important because it will present proactive defense strategies and alert the academic community to place more emphasis on making smartphone security a more active area of research. Moreover, those proactive defense techniques will best serve in mitigating risks that are higher than ever before in current mobile environments. This will ultimately contribute to prevention of data loss (which could be sold by hackers for a price), decrease potential lawsuits caused by identity theft, and increase the confidence for smartphone users conducting mobile commerce.

REFERENCES

[1] Wong, L. (2005). *Potential Bluetooth vulnerabilities in smartphones*. Retrieved from http://citeseerx.ist.psu.edu.

[2] Brown, B. (2009). *Beyond Downadup: Security expert worries about smart phone, TinyURL threats: Malware writers just waiting for financial incentive to strike, F-Secure exec warns*. Retrieved from http://business.highbeam.com/409220/article-1G1-214585913/beyond-downadup-security-expert-worries-smart-phone

[3] Bose, A. (2008). *Propagation, detection and containment of mobile malware*. (Doctoral dissertation, University of Michigan). Retrieved from www.phoenix.edu/apololibrary.

[4] Xie, L., Zhang, X., Chaugule, A., Jaeger, T., & Zhu, S. (2009). *Designing system-level defenses against cellphone malware*. Retrieved from www.cse.psu.edu

[5] Bhattacharya, D. (2008) *Leardership styles and information security in small businesses: An empirical investigation* (Doctoral dissertation, University of Phoenix). Retrieved from www.phoenix.edu/apololibrary

[6] Rash, W. (2004). *Latest skulls Trojan foretells risky smartphone future*. Retrieved from www.eweek.com.

[7] Mulliner, C., & Miller, C. (2009). Injecting SMS messages into smartphones for security analysis. *Proceedings of the 3rd USENIX Workshop on Offensive Technologies Montreal, Canada*. Retrieved from www.usenix.org

[8] Becher, M., Freiling, F., & Leider, B. (2007, June) On the effort to create smartphone worms in Windows Mobile. *Proceedings of the 2007 IEEE workshop on Information Assurance. United States Military Academy*. West Point, NY. Retrieved from http://pi1.informatik.uni-mannheim.de/filepool/publications/on-the-effort-to-create-smartphone-worms-in-windows-mobile.pdf. .

[9] Portokalidis, G., Homburg, P., Anagnostakis, K., & Bos, H. (2009). *Paranoid Android: Zero-day protection for*

smartphones using the cloud. Retrieved from www.cs.vu.nl/~herbertb/papers/trpa10.pdf.

[10] Ni,X., Yang, Z, Bai, X., Champion, A., & Xuan, D. (2009). *DiffUser: Differentiated user access control on smartphones*. Retrieved from http://www.cse.ohio-state.edu/~champion/pubs/09_wsns_nybcx.pdf

[11] Schmidt, A-D., Peters, F., Lamour, F., Scgeel, C., Camtepe, S., & Albayrak, S. (2009). Monitoring smartphones for anomaly detection. *Mobile Networks and Applications, 14*(1), 92-106.

[12] Xie, L., Zhang, X., Chaugule, A., Jaeger, T., & Zhu, S. (2009). *Designing system-level defenses against cellphone malware*. Retrieved from www.cse.psu.edu

[13] Salkind, N. J. (2004). Statistics for people who (think they) hate statistics. Retrieved from http://search.barnesandnoble.com/Statistics-for-People-Who/Neil-J-Salkind/e/9781412979597/?cm_mmc=AFFILIATES-_-Linkshare-_-je6NUbpObpQ-_-10:1.