Impact of False Positives and False Negatives on Security Risks in Transactions under Threat*

Doncho Donchev[1], Vassil Vassilev[2,1], and Demir Tonchev[1]

[1] Sofia University "St. Kliment Ohridski" - GATE Institute, Sofia, Bulgaria
{doncho.donchev,demir.tonchev}@gate-ai.eu
http://gate-ai.eu/en/home/
[2] London Metropolitan University - Cyber Security Research Centre, London, UK
v.vassilev@londonmet.ac.uk
https://www.londonmet.ac.uk/profiles/staff/vassil-vassilev/

Abstract. This paper presents a theoretical model, algorithms, and quantitative assessment of the impact of false positives and false negatives on the security risks during transaction processing. These two factors play an important role in the decisions to counteract potential threats. The assessment of their impact on the risks during transaction processing is based on analysis of the effect of varying the parameters of the optimal strategy, modeled as a Partially Observable Markov Decision Process. Such an analysis is an important element of any cybersecurity framework, which considers planning of active countermeasures for mitigating the risks and although developed primarily for controlling financial transactions, it is applicable to a wider range of problems in which the asynchronous events during the execution are caused by human errors, malfunctioning or external interventions.

Keywords: Transactional Models · Secure process integration and management · Intrusion detection and information filtering · Security, privacy and trust in real-time Internet e-Services · Risk assessment · Markov Decision Process.

1 Introduction

Contemporary Intrusion Detection Systems (IDS) are widely used in network management and cybersecurity frameworks for detecting and classifying potential security threats of unauthorised intrusions [1–3]. The unauthorized intrusions during transaction processing are particularly dangerous because they can lead to significant financial losses. Tampering with ATM machines, stealing credentials, diverting transactions and complete hijacking - the adversaries never sleep. There are a number of security measures which can be used to counteract, but

* Partially funded by EU Horizon 2020 under WIDESPREAD Big Data for Smart Society (GATE) Project and by Innovate UK under CyberASAP Vulnerability Analysis and Risk Assessment Project.

the success of their use depends on the precision of the detection and the time. In both network-based IDS, which use signature information [8], and host-based IDS, which use behavioral information [9] the data analysis utilizes a variety of methods for Machine Learning (ML). In more advanced frameworks the IDS are often complemented with Intrusion Prevention Systems (IPS) [4, 5]. Such systems typically combine logical analysis of security policies, AI Planning and data analytics based on ML, leading to hybrid AI architectures[16, 16].

The terms *false positives* and *false negatives* in data science and ML denote errors in the change detection, identification, classification or prediction of data patterns as a result of the analysis. Similarly, *true positives* and *true negatives* denote correctness. In this paper we will present the results of a quantitative assessment of the impact of false negatives and false positives on the security risks, calculated on the base of the optimal strategy for control of the transactions under security threats, modelled as Partially Observable Markov Decision Processes (POMDP) [18].

2 False Positives and False Negatives in Data Science and in Cyber Security

In data science the false positives and false negatives measure the quality of the data analytics in general and the detection in particular [6]. Basic statistic analysis of the false positives/false negatives in different methods of ML can be found in abundance in the literature [10]. There is some research on how to reduce the false negatives in specific methods for ML [11] and the false positive rates [12], but surprisingly, a little investigation of their impact on the security risks. In [13] the risks caused by threats are modelled using Markov chain but the analysis looks for predication of attacks rather than for preventing them by executing counteractions. Relatively detailed analysis of the security risks as dependent on the counteractions is given in [14]. By accounting of the prior classification of the various malicious activities there it would become possible to analyse their impact in more details, but because of the use of historical data produced by Monte-Carlo simulation the estimation is less suitable for real-time analytics.

It is unfortunate that the impact of false negatives and false positives on security risks has not been researched more extensively because they play crucial role in the decision making during offline scheduling or real–time planning of security countermeasures. Part of the reason is the lack of formal models which would allow to conduct a credible investigation of the risks. Most of the efforts to mitigate the risks caused by security threats are adopting the *best-practice* approach. By using POMDP our model of the transactions under threat distinguishes between unpredictable, but partially observable security events, and predictable, but uncontrollable effects of the malicious actions. Using this model the assessment of the impact is produced by analyzing the dependencies between the prior probabilities for detecting threats, which is a characteristics of the ML algorithms applicable to the specific data, and the risks of diverting the transactions from their normal execution under the influence of security threats, which can be neutralized by the available countermeasures. This makes our approach more suitable for real-time analytics.

3 Security Countermeasures and Security Risks in Transactions under Threat

Our method for risk assessment using POMDP model was introduced in [18], where we were discussing its use for integration of decision making with stochastic planning in digital banking. In order to make the paper self-contained here we will provide a brief description of the POMDP model and its use for assessing the security risks by computing the optimal strategy for decision making.

3.1 Applying security countermeasures during transaction execution

The decisions to execute diagnostic actions and to apply counteractions is essential part of any cybersecurity framework. In our framework for controlling the transactions under threats the natural criteria for decision making is the security risk. The empirical description of the data analytics and ML methods provides sufficient ground for developing of a formal model of the decision making process. Due to the presence of asynchronous events, which can be either unpredictable, but anticipated – like many malicious interventions, or unexpected, but predictable – such as human or technical errors, we must model the transaction processing under threats as POMDP, rather than Markov Decision Process (MDP) which assumes full information about all possible actions. Our model has the following elements:

1. **State space** $S = \{safe, danger, deadend\}$ – corresponds to the different types of situations from the point of view of the risk they pose:
   (a) $safe$ Situations along the transactions in absence of any threats;
   (b) *danger* Situations in which the system is under the influence of security threats but still able to recover and
   (c) *deadend* Situations in which the system experiences severity and crashes completely under the security threats.
2. **Control space** $C = \{noact, respond\}$ – corresponds to the two types of actions from risk perspective:
   (a) *noact* – no control intervention, the system goes straight to the next situation according to the recommended action and continues the normal track of execution of the current transaction, and
   (b) *respond* – counteraction, which brings the system back to a safe situation after malicious action deviating the transaction from its normal course.
3. **Observation space** $Z = \{nothreat, threat, crash\}$ – corresponds to the different types of events from risk viewpoint:
   (a) *nothreat* – asynchronous event, which is non-threatening and does not require counteraction;
   (b) *threat* – detection of malicious intervention which requires counteraction, and
   (c) *crash* – losing control of the system without chance for recovery.

4. **Transition kernel** $q(s_{n+1}|s_n, c_{n+1})$ – probability of the transition from situation s_n to situation s_{n+1} under control c_{n+1}, calculated as follows:
   - $q(safe|safe) = p$, p is the probability for absence of threats after transition from a safe situation;
   - $q(danger|safe) = 1 - p$, $1 - p$ is the probability for presence of threats after transition to from safe situation;
   - $q(safe|danger, respond) = 1$ because the counteraction in dangerous situation eliminates the threat;
   - $q(deadend|danger, noact) = 1$ because the absence of counteraction in dangerous situation leads to inevitable crash of the system, and
   - $q(deadend|deadend) = 1$ since there is no way out of the crash.
5. **Occurrence kernel** $t(z_n|s_n)$ – probability of the occurrence of event z_n in situation s_n, calculated as follows:
   - $t(nothreat|safe) = p_{11}$ – probability of not observing threat occurrence in a safe state (*true negative*);
   - $t(nothreat|danger) = p_{12}$ – probability of not observing threat occurence in a dangerous stage (*false negative*);
   - $t(threat|safe) = p_{21}$ – probability of observing threat occurrence in a safe state (`false positive`);
   - $t(threat|danger) = p_{22}$ – probability of observing threat occurrence in a dangerous state (*true positive*), and
   - $t(crash|deadend) = 1$ – probability of observing the system crash under threat.

   If we denote the matrix with entries $p_{ij}, i, j = 1, 2$ by P its transpose P^T is a stochastic matrix since

   $$p_{11} + p_{21} = p_{12} + p_{22} = 1.$$

6. **Costs** – quantitative measures of the costs of taking actions which can be interpreted differently, depending on the needs; we are considering it to be the delay caused by the additional counteractions to neutralize the detected threats:
   (a) Current cost $r(c)$ calculated as follows: $r(noact) = 0$, $r(respond) = -c$ where $c > 0$ is the cost for executing counteraction *respond*;
   (b) Final cost $R(s)$ calculated as follows: $R(safe) = R(danger) = 1$ if either the transaction terminates normally or the threat occurs after finalizing it, and $R(deadend) = 0$ if the crash occurs during the transaction.
7. **Horizon** N – length of the transaction, measured by the number of safe situations along the transaction.

The main difference between an MDP and POMDP is the introduction of the **Observation Space** and the **Occurrence Kernel**. These two components of the model reflect the non-predictability of the asynchronous events, which can happen in different situations at arbitrary times during the transactions. Although they make the POMDP models more complex, as we will show its complexity can be reduced by statistical methods.

3.2 Risk assessment based on optimal strategy for transaction control

The problem for controlling the transactions under threats formulated as POMDP can be reduced to a problem for a fully observed MDP [18]. In this section we will sketch the reduction procedure which enables the analysis of the impact of false negatives and false positives rates on the security risks.

Definition *Security decision* $\phi(s)$ is a function, which on each step of the transaction s chooses either *noact* or *respond*.

The security decisions may modify the transactions by enforcing *respond* actions at some steps. Therefore, they can extend the transaction path. If the security decisions are wrong it might even happen that the transaction can end in a *deadend* situation. To maximize the chances to make the right decisions we will account all information available at the time of decision making, which will turn the security decision into a stochastic function of the parameters of the POMDP model.

Definition *Decision policy* $\pi = (\phi(1), \phi(2), ..., \phi(N))$ is a collection of security decision functions such that on each step n of the transaction, $\phi(n)$ depends only on the past history till time n, and the prior probabilities of the states at time 0, that is before the transaction has begun. We assume that the prior probability of state *deadend* is 0, since otherwise any policy makes no sense. Therefore, the sum of the prior probabilities of the other two states is equal to 1, and the prior distribution of the states at time 0 is determined by the prior probability x of state $safe$. So, we are now looking for a decision policy π which maximizes the total reward

$$v^{\pi}(x) = E^{\pi}_{x}(R(state_N) - cK),$$

where E^{π}_{x} is the expectation, corresponding to the policy π and the prior probability x, and K is the number of times when we apply the action *respond*. In the above expression $R(state_N)$ is the final income which we get in the last step of the transaction.

Definition *Value function* of the POMDP model is the function

$$v(x) = \max_{\pi} v^{\pi}(x)$$

Definition The policy π such that $v(x) = v^{\pi}(x)$ is an *optimal policy.*

The optimal policy plays a central role in our framework, since it is linked to the risks. It certainly exists, since there are only a finite number 2^N of possible policies. It is worth noting that $0 < v(x) < 1$, since $R(x) \leq 1,\ c > 0$, and the policy which does not recommend using the action *respond* at all yields a positive income, equal to the probability to avoid observing *crash* during the transaction. This fact motivates us to define the risk, corresponding to the prior probability x as $1-v(x)$. This way, we can find both the value function $v(x)$ (resp. the risk $1-v(x)$) and the optimal policy π, following the standard steps of the dynamic programming algorithm. Let us set

$$\Gamma^1(x,y)=\frac{p_{21}x}{p_{21}x+p_{22}y},\ \Gamma^2(x,y)=\frac{p_{11}x}{p_{11}x+p_{12}y},$$

and $V_N(x)=1$. For $0\leq n<N$ we can recursively find the functions

$$\begin{aligned} V_n'(x) &= -c+(pp_{21}+(1-p)p_{22})V_{n+1}(\Gamma^1(p,1-p)) \\ &\quad +(pp_{11}+(1-p)p_{12})V_{n+1}(\Gamma^2(p,1-p)), \\ V_n''(x) &= (pxp_{21}+(1-p)xp_{22})V_{n+1}(\Gamma^1(px,(1-p)x)) \\ &\quad +(pxp_{11}+(1-p)xp_{12})V_{n+1}(\Gamma^2(px,(1-p)x)), \\ V_n(x) &= \max(V_n'(x),V_n''(x)), \end{aligned}$$

and the set $A_n=\{x\in(0,1):\ V_n(x)=V_n'(x)\}$. If $n=N-1$ we get

$$\begin{aligned} &V_{N-1}'(x)=1-c,\ V_{N-1}''(x)=x, \\ &V_{N-1}(x)=\max(1-c,x),\ A_{N-1}=(0,1-c). \end{aligned}$$

We observe that the set A_{N-1} is a single interval, determined by the threshold $y_{N-1}=1-c$. The same holds for all $n<N-1$. The corresponding thresholds we denote by y_n $n=0,1,...N-1$. The remaining iterations until reaching the beginning of the transaction can be performed recursively, taking the previously calculated solution as terminal.

After all thresholds have been found, the optimal policy recommends the following optimal behavior:

1. At the beginning of transaction ($n=0$), depending on whether we detect a threat or not, we calculate the posterior probability x_0 of the state $safe$ by the formula

$$x_0=\begin{cases}\Gamma^1(x,1-x), \text{ if } z_0=treath \\ \Gamma^2(x,1-x), \text{ if } z_0=notreath\end{cases}.$$

   If x_0 is greater than the threshold y_0, then we do not apply the corrective action, x_0 remains unchanged, and with probability $1-x_0$ we fall into a state *deadend*. Otherwise, we use *respond* after paying the cost c, and the posterior probability becomes 1 since we certainly know that we are $safe$;
2. On the next step we start with a prior probability equal to the just found posterior probability (x_0 or 1), multiplied by p, observe again if there is detection of a threat, calculate the posterior probability x_1, compare it with the threshold y_1, and so on till the end of the transaction;
3. Finally, the connection between the value functions in both POMDP and MDP models is given by the formula

$$\begin{aligned} v(x) &= (xp_{21}+(1-x)p_{22})V_0(\Gamma^1(x,1-x)) \\ &\quad +(xp_{11}+(1-x)p_{12})V_0(\Gamma^2(x,1-x)). \end{aligned}$$

The above equations form the algorithmic foundation for assessment of the security risks in transaction processing under threats. In the next section we will use it for analysis of the impact of the false negatives and the false positives on the security risks.

4 Measuring False Positives and False Negatives

In security analytics *false positives* and *false negatives* characterize the methods used to detect the threats. *False negatives* is particularly in the focus of interest in ML literature, because wrong detection, identification, classification or prediction of the security threats can lead to breaches in security with serious consequences. On the other hand, *false positives* affect the performance since they may lead to unnecessary actions to mitigate risks which are too small or even do not exist at all.

4.1 Confusion matrix

Popular measure of the precision of detection algorithms ACC is typically given by the following formula:

$$ACC = \frac{p_{11} + p_{22}}{p_{11} + p_{12} + p_{21} + p_{22}} = \frac{1}{2}(p_{11} + p_{22}),$$

where the prior probabilities p_{ij} measure the true and false positives and negatives of the algorithms and form a *confusion matrix* [15]. These measures may characterize the quality of the algorithms but they do not account the impact of the false negatives and false positives on the security risks in particular scenarios, such as the execution of transactions under threats. As we will show bellow the precision of the algorithms should not be a sole factor which determines the choice of countermeasures.

4.2 The cost of false positives and false negatives

In the POMDP model *false negatives* and *false positives* are represented by the prior probabilities p_{12} and p_{21}, respectively. They depend only on the method for detection of the potential threats and, as such, are input parameters for our analysis. The *horizon* N depends on the particular transaction and it is another input parameter for the analysis. The last parameter of the model, which may have an impact on the risk, is the *cost* for using mitigating counteractions, c. At first glance it looks like another input parameter, which needs to be known in advance, but as we will show here it can be calculated on the base of the other input parameters by estimating its boundary values using purely analytical methods, so it is not an input parameter as such.

If we assume that the cost c as a parameter of the model is independent on the other parameters we can face the following extremes:

- **Case 1:** c is too small. Then the optimal policy may recommend applying mitigating action *respond* permanently, without taking into consideration any observations;
- **Case 2:** c is too large. Then we would not be able to neutralize all threats even if we know exactly when they occur, i.e., when both the false positives and the false negatives are equal to 0. This could happen because the total cost of the mitigating actions may exceed 1, which is the maximum reward we can get for successful end of the transaction.

In order to avoid such extremes we will make c dependant on both p-s and N.

Let M be the maximum number when the action *respond* can be used. Then, we have $Mc < 1$ and $(M+1)c > 1$ and therefore,

$$\frac{1}{M+1} < c < \frac{1}{M}. \tag{1}$$

On the other hand, the number of potential threats during the transaction is a random variable which has a binomial distribution with parameters $1-p$ and $N-1$. Taking M to be an $1-\alpha$–quantile of this distribution, for α small enough, we guarantee that we can face Case 2 only with probability less than α. In view of (1), $1/(M+1)$ is a lower bound for c which mitigates the risks more than M times by executing *respond*. Thus, Case 1 will not take place either.

The costs can be discounted by introducing a weight for repeating the same counteractions in subsequent situations, but due to the relatively short horizon of the transactions this is unnecessary and for the sake of simplicity we will use fixed costs.

5 Impact of False Positives and False Negatives on Security Risks

In this section we will provide experimental results about the impact of the false negatives and false positive rates on the security risks, based on the optimal strategy for control of the transactions under threats using the method of dynamic programming. In the calculations we vary the values of the input parameters to cover the typical precision of the detection algorithms.

5.1 Dependence of the security risks from the precision of the detection

The 3D plot of the binomial dependence of the security risks from the rate of false negatives and false positives is shown on Fig. 1 in the Appendix. In order to make it representative and sufficiently informative in the calculations we used several combination of input parameters as follows:

- for the false negatives p_{12} within the interval 0.0–0.3, i.e. detection precision up to 70%, which is more than adequate as an estimation of the precision of a variety of methodsm and
- for false positives p_{21} within the interval 0.0–0.5, i.e. up to 50% miss rate, which is also adequate.

The 3D plot in Fig. 1 is based on the calculations in Tab. 1. It has a regular spatial shape with monotonous dynamics without any extremes or inflection areas. This allows for more convenient analysis of the simultaneous dependence of the risks on both the false positives and false negatives after reducing it to a series of projections on a 2D plane for a fixed second rate within the sampling intervals.

The diagram of the risk dependence on the false negatives under a fixed rate of the false positives is shown on Fig. 2 in the Appendix. As you can see

p12 **p21**	**0.01**	**0.05**	**0.10**	**0.15**	**0.20**	**0.25**	**0.30**	**0.35**	**0.40**
0.01	0.26490	0.34798	0.45190	0.52604	0.55737	0.56926	0.57152	0.57156	0.57039
0.05	0.28062	0.36173	0.46836	0.53355	0.55973	0.57060	0.57085	0.57117	0.57161
0.10	0.30599	0.38422	0.48614	0.53993	0.56390	0.57092	0.57045	0.57117	0.57125
0.15	0.32487	0.40617	0.50181	0.55006	0.56778	0.57117	0.57212	0.57029	0.57326
0.20	0.34341	0.42234	0.51571	0.55538	0.57060	0.57094	0.57067	0.57241	0.57045
0.25	0.36716	0.44334	0.52447	0.56019	0.57128	0.57029	0.57241	0.57060	0.57212
0.30	0.38485	0.45882	0.53555	0.56377	0.56953	0.57153	0.57106	0.57031	0.57067
0.35	0.40217	0.47885	0.54599	0.56730	0.57203	0.57239	0.57170	0.57220	0.56991
0.40	0.41912	0.49361	0.55429	0.56922	0.57060	0.57020	0.57052	0.56953	0.56983

Table 1. Risk threshold in function of the false negatives and false positives

the risk for a very low level of false positives p_{21} increases with the increase of the false negatives p_{12} in a linear order. This means that when the detection captures actual threats the risk depends only on the false negatives detection rate. On the contrary, the risk for false positives p_{21} around and more than 50% is practically constant and does not depend on the rate of false negatives p_{12}. This can be explained by the fact that although the false positives enforce unnecessary responses to non-existing threats they also neutralize some of the undetected threats.

The diagram of the risk dependence on the false positives p_{21} under the fixed rate of the false negatives p_{12} is shown on Fig. 3 in the Appendix. The striking observation from the diagram is, that the risk saturates around 20-25% rate of false positives practically for all false negatives rates (false negatives rate are normally within the range 0-50%). This means that the algorithms for detection which produce more than 25% false positives practically have the same effect on the risk and the quality of detection does not increase when lowering further the false negatives rate. From the differentiation of the curves for different fixed rates of false negatives in the initial rate intervals it is also obvious that the quality of the algorithms which produce a low rate of false positives before the saturation (0-25%) depends nearly proportionally on their rate - the fewer false negatives, the lesser risk.

The results meet further the expectation. The two boundary combinations of false positives/false negatives - high/high and low/low - determine the maximum and minimum risky methods. More interesting are the results for a combination of law false negatives with false positives close to the max. They show that the high rate of false positives completely neutralizes the low false negatives. Once more, this confirms the importance of the false positives for the choice of detection method.

The above analysis shows that the choice of methods for detection needs to consider not just the minimal false negatives and false positives, but also their combined rate. Beyond certain rate of false negatives further minimization does not reduce the risks and beyond certain rate of false positives the risk doesn't depend on the false negatives at all. There is no need to look for minimization of both false negatives and false positives, since the optimum depends on their combination and any further minimization of false negatives or false positives may be too costly without significant effect on the risk reduction.

5.2 Dynamics of the security risks along the transactions

Intuitively, the lower the rates of the false negatives and false positives are the lower the risks are. But this does not account the moment of executing the counteractions in response to the threats. Table 2 contains calculations based on the optimal strategy which helps analyzing this dependence in more details.

N	**p12=0.05** **p21=0.05**	**p12=0.30** **p21=0.30**	**p12=0.05** **p21=0.30**	**p12=0.15** **p21=0.15**	**p12=0.30** **p21=0.05**	**cost**
5	0.189638093	0.271971568	0.271838029	0.272796722	0.22716054	0.417
10	0.361736347	0.571060961	0.57085112	0.550062678	0.458826459	0.292
15	0.580335931	0.747278141	0.747077204	0.735406971	0.677226803	0.292
20	0.631718964	0.851101596	0.847870525	0.824268906	0.768704437	0.225
25	0.669172001	0.911364804	0.903965426	0.879386462	0.834110451	0.183
30	0.70195926	0.946130333	0.937595461	0.916204114	0.882486834	0.155

Table 2. Change of security risks as a function of the remaining steps

We have calculated the change of the risks for several representative combinations of p_{12} and p_{21}:

1. Low rates for both false negatives and false positives: $p_{12} = 0.05$ and $p_{21} = 0.05$;
2. Low rate of false negatives but high rate of false positives: $p_{12} = 0.05$ and $p_{21} = 0.30$;
3. Close average rates of both false positives and false negatives: $p_{12} = 0.15$ and $p_{21} = 0.15$;
4. High rate of false negatives but low rate of false positives: $p_{12} = 0.30$ and $p_{21} = 0.05$, and
5. High rates for both false negatives and false positives: $p_{12} = 0.3$ and $p_{21} = 0.3$.

Fig. 4 in the Appendix shows the dynamics of the risks along the path of the transactions for these combinations. All curves are aperiodic, which means that the earlier you counteract, the lower the risks of crashing the transaction are.

5.3 Dependence of the cost from the moment of counteracting

The parameter c, which measures the costs of executing counteractions for neutralizing the threats, depends on the horizon N and can be calculated analytically as discussed earlier. Since the interpretation of this parameter can be done in terms of relative delay of the transaction due to the additional actions which have to be executed to neutralize the threats, the distribution of its estimation for discrete values of the horizon N allows to analyze the relative delays. The diagram of the estimation of the costs for executing counteractions to respond to security threats in function of the remaining situations before reaching the end of the transaction is shown in Fig. 5 in the Appendix. It looks like a step function because it is based on analytical estimation of the interval of possible values rather than on the actual values, but it still shows the linear dependence of the costs - the longer the transaction is, the lower the cost is. This meets precisely the intuition, since the relative delay caused by the extra time needed to execute countermeasures in long transactions decreases towards the end, while the earlier application of countermeasures may require several repetitions.

6 Discussion and Future Development

The estimation of the security risks within the POMDP model is based on the optimal strategy for control of the transactions which minimizes only the integral risks, without accounting any specific information about the transactions. At first glance the experimental results look somewhat trivial, but more importantly, they essentially validate the theoretical model we are using. We can apply the same method for investigation of safety problems in other application domains in which asynchronous events may occur, such as faults, caused by machine failure or human errors in autonomous devices and production lines.

More detailed estimation of the impact of false negatives/false positives can be done if we know in which situation along the transaction the different threats can occur. In such a case the optimal strategy can be tuned according to the transactions to produce more informed security decisions. For this purpose the prior probabilities should be functionally dependent on both the false negatives/false positives rates of the detection algorithms and the situations, in which the malicious activities take place. We are also considering the possibility to use the risk assessment for analyzing the vulnerability of transaction processing systems by identifying dangerous situations. This would allow to validate the security policies and to optimize them. In a more distant future we are also planning to explore the potential of reinforcement learning for increasing the precision of the assessment by additionally analyzing historical data. Since it is difficult to obtain a real transaction data we are considering using Monte Carlo simulations or other statistical methods for generating synthetic data.

Acknowledgments

The research reported here is a result of collaboration between the Cyber Security Research Centre of London Metropolitan University, UK and GATE Institute of Sofia University, Bulgaria. The Cyber Security Research Centre would like to acknowledge the continuing support of Lloyds Banking Group as the driver behind the security framework based on hybrid AI. The opinions and the results presented in this paper are, however, of the authors only and do not reflect the official policies of the bank.

References

1. OWASP Foundation, Inc., “Intrusion Detection”. [Online: https://owasp.org/www-community/controls/Intrusion_Detection; Accessed: 20/01/2021]

2. Cisco, “Cisco and the NIST Cybersecurity Framework”. [Online: https://www.cisco.com/c/dam/en/us/products/collateral/security/nist-cybersecurity.pdf; Accessed: 28/12/2020]
3. Amazon, Inc., “Amazon Detective”. [Online: https://aws.amazon.com/detective; Accessed: 2/01/2021]
4. Palo Alto Networks, ”Palo Alto Networks Approach to Intrusion Prevention”, 2020. [Online: https://www.paloaltonetworks.com/ resources/whitepapers/ips-as-platform; Accessed: 20/01/2021]
5. Darktrace, “Darktrace Cyber AI Analyst” [Online: https://www.darktrace.com/en/resources/wp-cyber-ai-analyst.pdf; Accessed: 28/12/2020]
6. F. Liang, “Evaluating the Performance of Machine Learning Model” [Online: https://towardsdatascience.com/classifying-model-outcomes-true-false-positives-negatives-17c1e702810; Accessed: 20/01/2021]
7. C. Ho, Y. Lai, I. Chen, F. Wang and W. Tai, “Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems”, IEEE Communications Magazine, vol. 50, no. 3, March 2012, pp. 146-154.
8. M. Kulariya, P. Sarafet al., “Performance analysis of network intrusion detection schemes using Apache Spark,” Proc. 2016 Int. Conf. on Communication and Signal Processing (ICCSP), Melmaruvathur, 2016, pp. 1973-1977.
9. J. Parmar, “A classification based approach to create database policy for Intrusion Detection and Respond anomaly requests”, Proc. 2014 Conf. on IT in Business, Industry and Government (CSIBIG), Indore, 2014, pp. 1-7.
10. C. Ho, Y. Lin, Y. Lai, et al., “False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems”, Int. J. of Future Computer and Communication, Vol. 1, No. 2, August 2012, pp. 87-90.
11. N. Chawla, K. Bowyeret al., “SMOTE: Synthetic Minority Over-sampling Technique”, J. of Artificial Intelligence Research, Vol. 16 (2002), pp. 321–357.
12. A. Mezic, “How AI is Solving the False Positives Problem in Network Security”, MixMode, Inc., 2020 [Online: https://mixmode.ai/blog/how-ai-is-solving-the-false-positives-problem-in-network-security; Accessed: 24 Jan 2021]
13. Q. Liu, L. Xing, and C. Zhou, “Probabilistic modeling and analysis of sequential cyber-attacks”, John Wiley, Engineering Reports, March 2019, pp. 1-19.
14. O. Kreidl, “Analysis of a Markov Decision Process Model For Intrusion Tolerance”, Int. Conf. Dependable Syst. and Networks, IEEE Xplore, 2010, pp. 156–161.
15. O. Caelen, “A Bayesian interpretation of the confusion matrix”, Ann. Math. Artif. Intell., 2017, Vol. 81 (3-4), pp. 429–450.
16. V. Vassilev, V. Sowinski-Mydlarz et al., “Intelligence Graphs for Threat Intelligence and Security Policy Validation of Cyber Systems”, in: P. Bansal et al., Eds., Adv. in Int. Sys. and Computing, vol. 1164. Springer, 2020, pp.125–140.
17. K. Bataityte, V. Vassilev and O. Gill, “Ontological Foundations of Modelling Security Policies for Logical Analysis”, in: I. Maglogiannis et al., Eds., IFIP Advances in Inf. and Comm. Technology, vol. 583. Springer, 2020, pp. 368–380.
18. V. Vassilev, D. Donchev and D. Tonchev, ”Risk Assessment in Transactions under Threat as a Partially Observable Markov Decision Process” (to appear).

Appendix: Plots of the analytical calculations

The diagrams in this Appendix are plotted on the base of the calculations shown in Tab. 1 and Tab. 2. They have been produced using Python programs which calculate the optimal strategy using the method of dynamic programming by varying the input parameters of the value function.

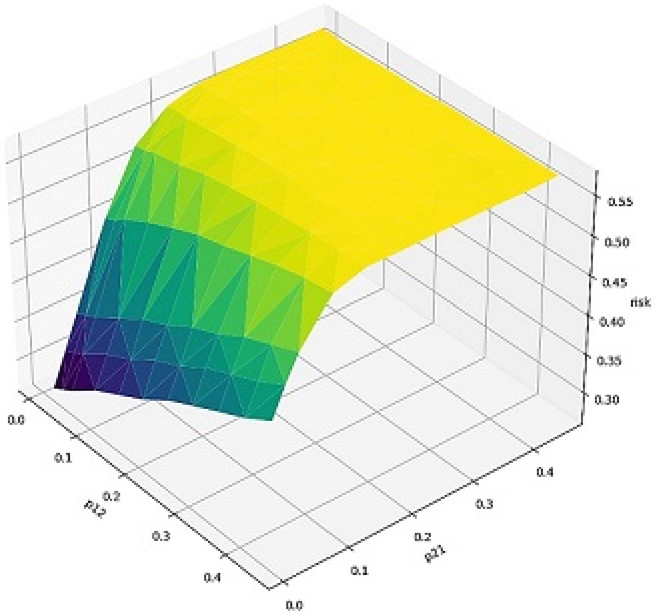

Fig. 1. 3D plot of the risk in function of the false negatives and false positives

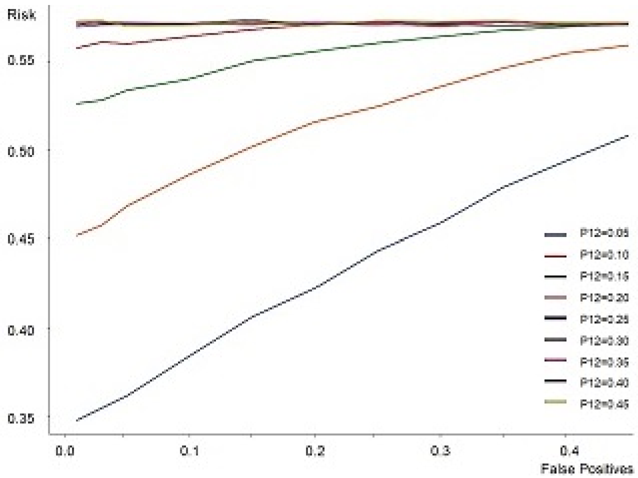

Fig. 2. Risk in function of the false negatives at fixed false positives

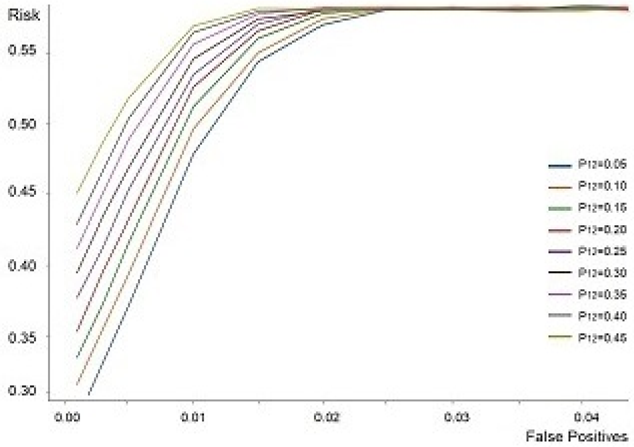

Fig. 3. Risk in function of the false positives at fixed false negatives

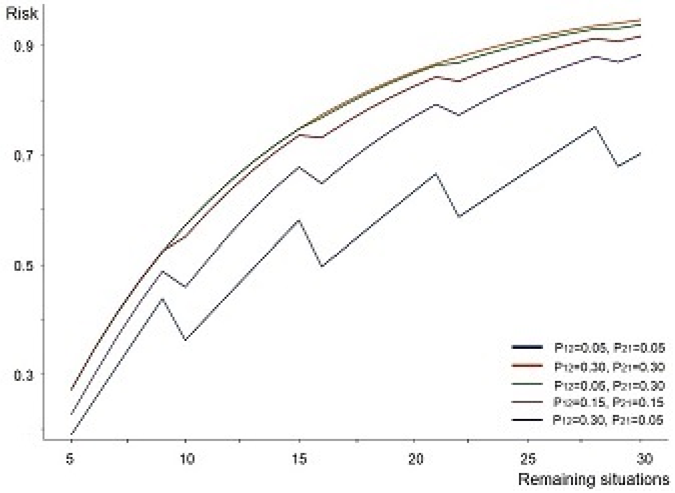

Fig. 4. Risk in function of the remaining situations of the transaction

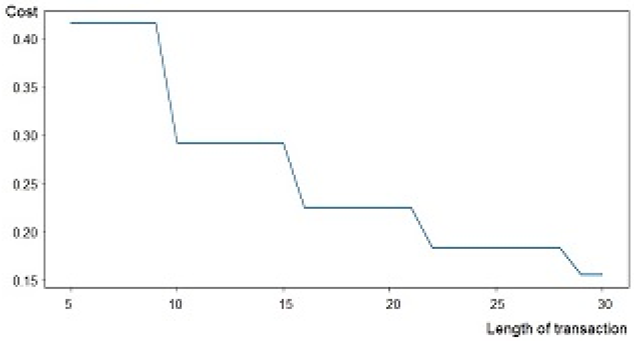

Fig. 5. Estimations of the cost c in function of the horizon N