Determining the Probability of Cyberattacks

Pavel Yermalovich
Ph.D. student, Faculté des Sciences et de Génie, Université Laval, Quebec City, Canada

Mohamed Mejri
PhD, Professeur titulaire, Département d'informatique et de génie logiciel, Faculté des Sciences et de Génie, Université Laval, Canada

Abstract

The use of information is inextricably linked with its security. The presence of vulnerabilities enables a third party to breach the security of information. Threat modeling helps to identify those infrastructures, which would be most likely exposed to cyberattacks. In some cases, however, threat modeling can not be classified as sufficient method of protection. This paper entitled "Determining the probability of cyberattacks" presents an analysis of different techniques with an attempt to identify the most informative parameters and cyberattack prediction markers, which would lay the foundation for the development of cyberattack probability functions. Next, it would be relevant to design such cyberattack probability functions, which would be used upon the initial identification of a cyberattack. The findings of this research could be applied during the future assessment of risk levels of information systems to ensure more effective information security management.

Keywords: Probability of cyberattacks, information security, cyber security, risk management, risk prediction.

1. Introduction

1.1. Motivation

The information systems are currently monitored by various systems. Such checks (audits) help to obtain various system characteristics within the perimeter of the information system security. On the basis of such verification or data monitoring it is possible to assess a risk level of cyberattack within the protected perimeter (infrastructure, system). The risk assessment is limited to the calculation of its level of risk at a certain time point, such as a freeze frame in a movie. The full risk analysis encompasses several stages. The implementation of each stage takes time. One or several indicators might be radically modified in the process of calculation of values in the end of one or more stages of a risk level analysis. Hypothetically, the risk indicator can be altered significantly as a result of this process and it may even exceed the maximum allowed level. This deviation can not be promptly tracked, while the analysis takes much time. For example, the conduct of risk assessment with MEHARI (MEthod for Harmonized Analysis of RIsk) Expert tool [18] may take more than six months [12]. From this it follows that in the context of such a risk assessment model, there are periods that remain uncontrolled.

The system threat modelling allows to obtain a probabilistic image of a cyberattack plan. At the same time, we can not predict the period of a cyberattack initiation. The periodic scanning of information system for known vulnerabilities helps to identify a list of the system vulnerabilities. However, this list can not ensure an accurate risk assessment in case of all these established vulnerabilities. Thus, for SIEM (Security Information and Event Management), it is important to ensure an obtainment of such a list arranged according to the importance of primary actions and reactions. Additionally, it is important to ensure proper classification of primary responses based on the analysis of the data from this list. First, it would be necessary to use the results of vulnerability assessment covering the most important assets in order to ensure their protection against identified critical vulnerabilities.

To date, there are training developments for Artificial Intelligence (AI) that are formed through the analysis of traffic logs to identify outliers. With this approach, it is possible to identify a cyberattack with a certain probability in a real time. The

difference between Intrusion Detection System (IDS) and AI is that the AI learns without analyzing deeply the cyberattack signature.

This research aims at developing a cyberattack prediction system based on various system parameters. Today it is impossible to determine precisely the time point at which the planned cyberattack will be committed and which vector will be chosen. This confirms the relevance of "prediction of cyberattacks" to be able to identify the levels prone to risks at every moment. Thus, it is proposed to extend risk prediction to all the existing data (risk indicators history).

1.2. Our Contributions

Identification of probability of an attack on information system S between t and t+Δt;

Development of attack forecasting function entitled "Oracle".

For example, the system configuration change, system modification allocation of funds for the system protection or creation of a working schedule.

Prior to applying X-parameters, it is suggested to check:

External threats:

Threats in social networks messages or sent emails;

Text in backlinks;

Text in backlinks to the attack target.

Trapping:

Fail2ban[1], IPS, etc.;

Pages of nonexistent administrators (as reconnaissance component);

One has also to consider the creation of markers that can influence the attack probability.

Experience, knowledge, tactics of the attacker side.

2. Literature review

A number of systems, such as Intrusion Detection System, can detect attacks [3] in real time. The detection of attacks is based on the application of rules (attack signatures) and work statistics under normal conditions (without attacks). The attack detection platforms applying machine learning methodology are based on the following three components:

Statistical analysis;

Attack signature analysis, covering the existing or new signatures created by an information security analyst and based on various sources. This analysis enables the identification of known behaviors or known attacks;

Machine learning to identify outliers.

The PatternEX (Threat Prediction Platform) [19] is an example of a system based on the automatic learning method [4]. The artificial Intelligence combines analysts' intuition with machine learning to mimic a security analyst to predict real-time and large-scale threats. To ensure an application of Artifiial Intelligence in InfoSec, PatternEx has developed a patent-pending technology entitled Active Contextual Modeling[2], or ACM. This technology continually identifies new and evolving (active) threats with the help of (contextual) analyst, and, once identified, synthesizes new models (modeling) that can distinguish between malicious and benign models. Another way to recognize threats is heuristic scanning[3], which is a method used by antivirus software to detect new viruses, as well as new variants of the already known viruses.

[1] http://bit.ly/2XblTyu
[2] http://bit.ly/2P6JOwd
[3] http://bit.ly/2X9nJ2U

Heuristic analysis is a method based on the supposed behavior of a program to determine whether the program is a virus or not. This method differs from statistical analysis, which is based on comparisons of the program with known viruses referenced in an anti-virus software library. The heuristic method can be used to detect DDoS attacks [11], Predictive Blacklisting, Phishing Attacks [9] and Malicious Web Pages [10]. As can be seen from the examination of attack prediction systems, this direction of research is a new one, and as it usually happens with new systems, it should be improved and refined to ensure good results.

3. Formal consideration

3.1. Problem

This research is an attempt to propose a risk level forecasting method. The Formula for establishing a risk value is

$$R = P \cdot I \tag{1}$$

where R is the risk value, P is the probability of an attack event and I is the impact (a likely consequence) of an attack event.

To determine the risk, we can predict only the probability P, while the impact I is considered by us as a constant value. However, the valuation of assets also plays a significant role in determining the future impact, due to changes in asset prices.

Given:

parameters of information system S:

set of business processes;

set of assets;

set of protection techniques applied to ensure the safety of assets;

security policy;

set of of this system log files;

risk assessment methodology;

attack forecasting time frame (t;t+Δt).

Find:

probability that an attack take place on information system S between t and t+Δt;

future risk level allowing to assess and identify the budget required to maintain an acceptable risk level.

The idea of the research aimed at the development of this field could be summarized as follows:

Development of attack forecasting function entitled "Oracle". Determination of parameters for attack forecasting function 2 "Oracle":

$$Oracle: X \to [0,1] \tag{2}$$

Let us consider the research project's general scheme in Figure 1.

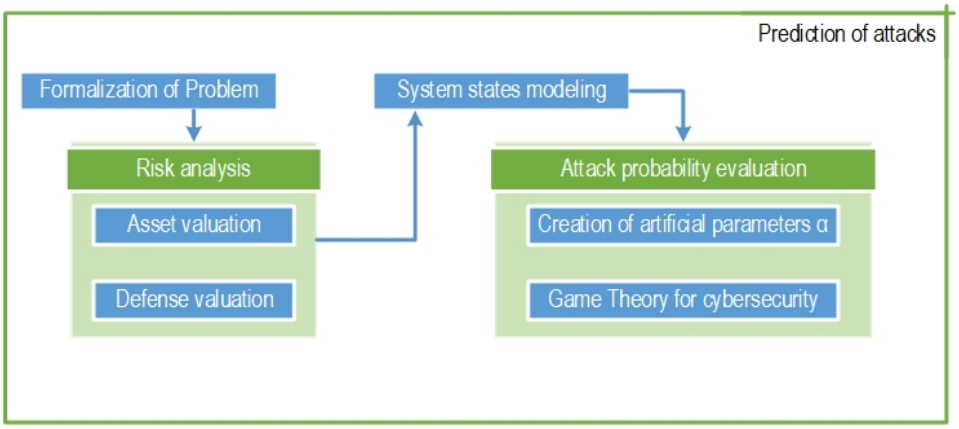

Figure 1: General scheme of the research project.

3.2. Formalization

The following should be noted for proper consideration of this formalization:

Calligraphic letter stands for a domain, for example $\mathcal{A}$;

Capital letter - denotes a subset, for example A;

Small letter stands for - a subset element, for example a.

Based on the above system input parameters, we can represent the initial state of the system S=(A,D). In the output stage we get the modified system state S'=(A,D'), which satisfies the following requirements:

RM(A,D') represents acceptable risk level for our system.

$D' = \min_{x \varepsilon D} Cost(D, Conf, x)$ stands for the selection of a configuration of a minimum cost that meets the requirements for an acceptable risk level.

Based on the input data, we are proceeding to formalizing an attack forecasting function in "Oracle" 3.

$$Oracle: BP, A, D, LOG, SP_r, RM, (t; t + \Delta t) \rightarrow [0,1] \quad (3)$$

Where

Attack - denotes an actual occurrence of an adverse event.

$[0,1]$ is the probability value of the event (attack).

BP: represents a set of business processes. The sequence of $bp_0, bp_1, \ldots$ comprises a set of meta-variables applied by us through the entire BP. Each business process encompasses a lot of assets. For example, content management (bp_0) using assets A comprises a set of assets: Application data (data bases) (a_0), Electronic mail (E-mail) (a_1), Local Area Network services (LAN services) (a_{10}), Web editing Service (a_{27}): $bp_0 = \{a_0, a_1, a_{10}, a_{27}\}$.

A: represents a set of assets. The sequence of $a_0, a_1, \ldots$ describes a set of meta-variables used by us, which are ultimately comprising A. The examples of assets include the Application data (data bases), Electronic mail (E-mail), Local Area Network services (LAN services), Web editing Service, Digital accounting control, etc.

D: describes the defense techniques applied to ensure the safety of assets A. The sequence of $d_0, d_1, \ldots$ describes meta-variables applied through the range D. In our example, the following techniques were used to ensure protection of the operating computer: a firewall, an antivirus and logging. Each security measure could be classified based on its configuration ($Conf$) - the configuration affecting the system system functioning and performance.

LOG is classified as a sequence of lines, where each line represents an event with unique information.

SP: stands for the security policy. The security policy comprises a set of instructions (the sequence of $sp_0, sp_1, \ldots$ describes meta-variables used by us through the range SP) for implementing business processes. The security policy can be accepted and formalized "on paper" as a set of safety rules. However, there are times when the actual security policy is different from what is on paper. Therefore, we will consider two types of security policies, Real (SP_r) and Theoretical (SP_t). For example, the proper use of security measures D to ensure the safety of an acceptable level for collection of assets A. or setting minimum requirements for the configuration of the protection system. The security policy describes which ports should be open to the firewall, antivirus updates frequency, timeframes for the system antivirus scan, logging detailing and the determination of location of the undertaken security measures (firewall at the entrance, antivirus and logging inside the system).

The adopted risk assessment methodology (MEHARI, CobiT, etc.) RM is represented as a function of $RM: A \times D \times SP \rightarrow R$, that returns the level of risk R of loss of assets A when using protection components D and, consequently, disruption of business processes BP.

$(t; t + \Delta t)$ time frame for attack forecasting.

To clarify this formalization we propose to refer to the following article: *Formalization of attack prediction problem* [13].

4. Risk analysis

In order to ensure an adequate protection level, each time we need to identify what should be protected and from whom. For this, it is necessary to identify the assets and obtain the information about them. The above mentioned statement could be illustrated by the following example:

Analysis of business activities or processes:

Determining the ownership of an asset in a business process.

Asset analysis (assessing the degree of importance, the level of loss when the asset is lost, of each value).

Given: List of business activities.

Find: Intrinsic Impact table.

Audit of the protection techniques applied to ensure the safety of assets:

Defense system analysis.

Risk analysis.

Given: List of protection techniques applied to ensure the safety of assetss.

Find: Attack scenarios, risk per asset type, risk per event type.

4.1. Analysis of business activities or processes

Proceeding from the above-mentioned, it is possible to conclude that the obtainment of information about them plays a crucial role. Asset valuation is a very important step in ensuring a proper system security. Thus, we need to know which assets should be protected to maintain their confidentiality, integrity and availability. *MEHARI Expert* [17] uses the following classification of the data, classification of services and classification of compliance with laws and regulations relating.

Sometimes, it is difficult to assign monetary value to assets. This is why each of these classification elements evaluates the classification level in terms of the maximum damage.

There are different methods of risk analysis. Each approach uses its own technique for the interpretation of asset values. It is necessary to represent the valuation of assets to be able to connect and use the results of asset analysis obtained applying different methodology. For that, we could quantify the categories. This will allow us to treat them as generalized attributes.

For example, MEHARI makes assessments based on 4 points scale (from 1 (Weak) to 4 (Unbearable)). As initial approach for this research project we could apply MEHARI only. In this case, the classification level must be determined before initiating risk analysis by MEHARI Expert. This should correspond to the maximum negative consequences of malfunctioning affecting this criterion of the asset evaluation process. It's really easier to determine the assets value in the event of their loss assessing each of the following security principles: availability, integrity, confidentiality. These are three principles for evaluating the Impact of loss asset.

We can represent the Formula 1 for establishing the risk value as follows:

$$R = \sum_{i=0}^{m} (P_{availability}(asset_i) \cdot I_{availability}(asset_i) + \\ + P_{integrity}(asset_i) \cdot I_{integrity}(asset_i) + \\ + P_{confidentiality}(asset_i) \cdot I_{confidentiality}(asset_i)) \quad (4)$$

where R stands for the risk value, $P_{availability}(a_i)$ is the probability of loss availability of asset a_i due to an attack event and $I_{availability}(a_i)$ stands for the impact (a likely consequence) of an attack event due to loss availability of asset a_i, and m stands for the amount of assets. the same for integrity and confidentiality for all the asset. The same relates to the integrity and confidentiality of all assets.

To determine a risk, we can predict only the probability P, while the impact I is considered by us a constant value for the time window $(t; t + \Delta t)$.

The probability of losing an asset is the probability of attacks on a given asset. Similarly, for security purposes, the likelihood of loss of availability / integrity / confidentiality for an asset P_{asset} corresponds to the likelihood of attacks $P(A)$ on the availability / integrity / confidentiality of the asset : $P_{asset} = P(A)$

In Section 5.1. "Cyberattack probability evaluation in each of the states", we take a closer look at the decomposition of the Formula for the probability of an asset attack.

The principle of reasonable sufficiency [8] states that it is fundamentally impossible [7] to create an absolutely insurmountable security system. It is important to choose the appropriate protection level for which the costs, risks and possible damages would be acceptable. Each of these steps takes time. The intervals between modifications can reach several months.

Formula 1 is still applied in MEHARI [17]. It allows to verify an average risk, but does not reflect the risk level in real time. There is a need to know the level of a probabilistic risk to track the risk levels over the specific time period.

The risk level can be calculated separately for each of the assets. The security context (security system) is created for each asset separately. Each security system consists of many components. In this way, we can design a chain of all security components (security barriers) for each asset separately. Each asset in the information system is valued differently in the event of total loss. We can rely on the indicator I (impact) which remains constant throughout time.

The elements of this table need to be expanded to take into account the different levels of probabilities of attacks and impacts. Lets assume that the average risk level for the whole company is ranked as 2 in compliance with MEHARI. This is a "Tolerated" level. However, another department of this company can be assigned an "Unbearable" risk level (4 of 4). Reasoning with the average value does not make it possible to spend the security budget properly. Thus, we want to have a dynamic system that adapts all the time, which can cost on average 25k$ per year, even if the forecast for next month is only around 500$. This can significantly change the value of a risk indicator and even allow to get out of the maximum allowed level (by MEHARI it is level 3 "Unacceptable"). This difference can not anticipated within very strict deadlines, while the analysis takes time. By doing this, as part of this risk assessment model, we will explore the so-called unchecked periods. An example of such case is shown in Figure 2. In this graph, the red line represents the limit of acceptable risk. The blue bars represent the true value of the risk and the black dots stand for the calculated risk values (calculations are carried out every four time units).

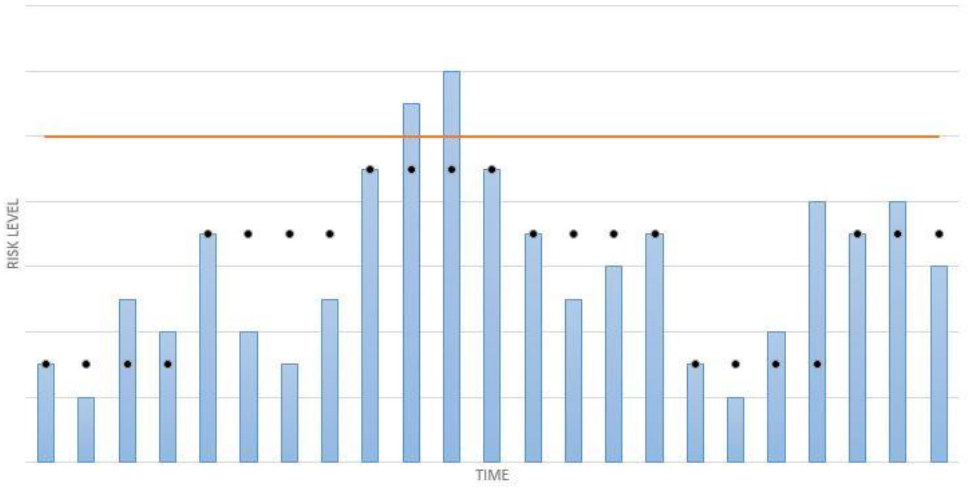

Figure 2: Graphical representation of the periods when risks take the passed calculated value.

In order to be able to represent the risk level at any time, it is suggested to analyze the already existing data sets and associated risks. For that we need to have an estimate of the appropriate level as a function of time, that is, a probability.

4.2. Audit of the protection techniques applied to ensure the assets safety

The system safety assessment approach through a security system audit is structured as questionnaire (yes / no) designed to analyze each security category (according to MEHARI Expert).

It is worth to undertake an analysis of protection measures D for assets A involved in business processes BP for the initial configuration of the system $Conf_h$, where $h = 0$ stands for the initial configuration.

$$D = (Conf, v), \tag{5}$$

where v - vulnerabilities and exposures.

The following Formula 6 is used by us to determine the level of risk for business processes:

$$RM: BP \times A \times D \rightarrow [1..4] \tag{6}$$

MEHARI uses charts containing audit results collected after the provision of "yes" or "no" answers to the questions used to collect the information enabling an analysis of the existing security systems. This analysis takes place within the time interval Δt. The risk level assessment in the time period $t_0 + \Delta t$ takes place with an application of the chosen risk assessment methodology RM. This analysis assesses the existing measures to protect the assets entering the business processes. After completing all the charts relating to the organisation's audit, the MEHARI risk analysis methodology forms a panorama of risks for each asset type (information, services, management processes). The asset protection system needs to be improved to change the risk level. It could be strengthened after the system configuration change i. e. $Conf_{(h-1)} \rightarrow Conf_h$ (where $Conf_h$ stands for the system configuration ensuring lesser risk for business processes). Each of $h \in R^+$ configurations has its own price by function $Cost: (d_{firewall}, Conf_{firewall}) \rightarrow p$, where $p \in R^+$. The task of the defense side is to minimize the risk level R to an acceptable level, with minimal costs $Cost(D, Conf_d)$.

$$\begin{cases} RM(BP \times A \times D') \rightarrow \text{acceptable level of risk} \\ D' = \min\limits_{x \varepsilon D} Cost(D, Conf, x) \end{cases} \tag{7}$$

It is suggested to use a cycle consisting of 1) analysis, 2) modeling, 3) selection and 4) application of the configuration in case of the system configuration change. The cycle is presented in Figure 3.

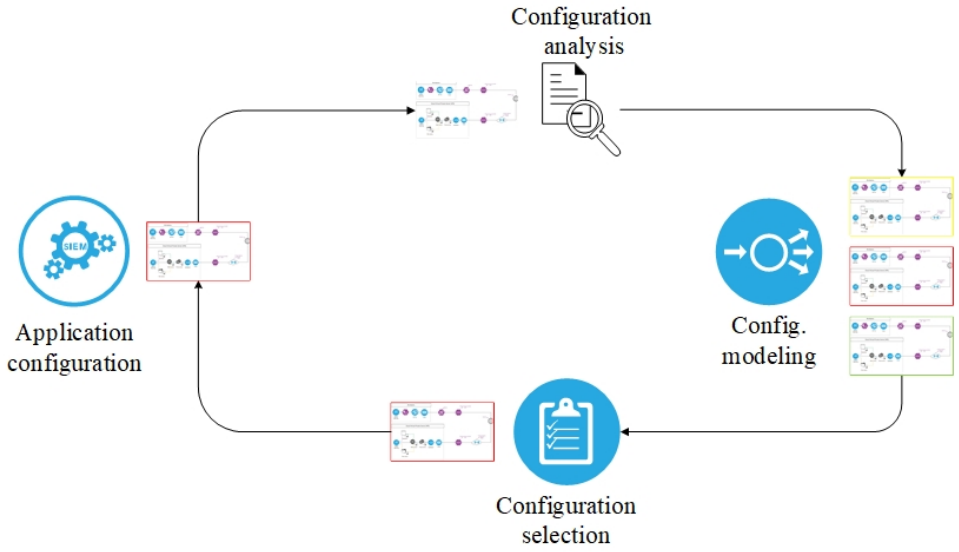

Figure 3: System configuration change cycle.

5. System states modeling

It is necessary to determine and model states of the system applying a formal method, meaning that we should decompose the system into simple components or variables (host, port, service, service version, availability, etc.). Each variable should be determined for the initial time instant. Later, system will affect the change of variables, i.e. removal and addition of variables describing the state of the system at each time point.

The system state change takes place upon the change of its configuration, switching or connection of any component aimed at ensuring its protection.

security configuration change $D[Conf_h/Conf_{h+1}]$;

disabling the system protection component D^-;

connecting system security component D^+.

The system is modelled by a probabilistic attack graph G, which is tuple,

$G = (S; \tau; \pi; L)$ consisting of

initial or start state $s_0 \in S$;

all of the states S;

transition relationship $\tau \subseteq S \times S$;

probabilistic transition $\pi: S \to S$;

labelling of states $L: S \times S$.

The function π specifies probabilities of transitions from probabilistic states, that applies to all transitions, meaning $s_1 \to s_2 \in \tau$ such that $s_1 \in S$, thus we have $P(s_1 \to s_2) = \pi(s_1)(s_2) > 0$. In that context $\pi(s)$ can be viewed as probability distribution on next states. Intuitively, when the system is in a deterministic state s_0, we have information about the relative probabilistic state s_1. Next it will choose the next state according to probability distribution $\pi(s)$.

In the context of this work it was suggested to apply MEHARI methodology. Consequently, we have four risk levels (identified by different colors, higher intensity corresponds to the maximum risk level). An approximate draft of the system is displayed below in Figure 4.

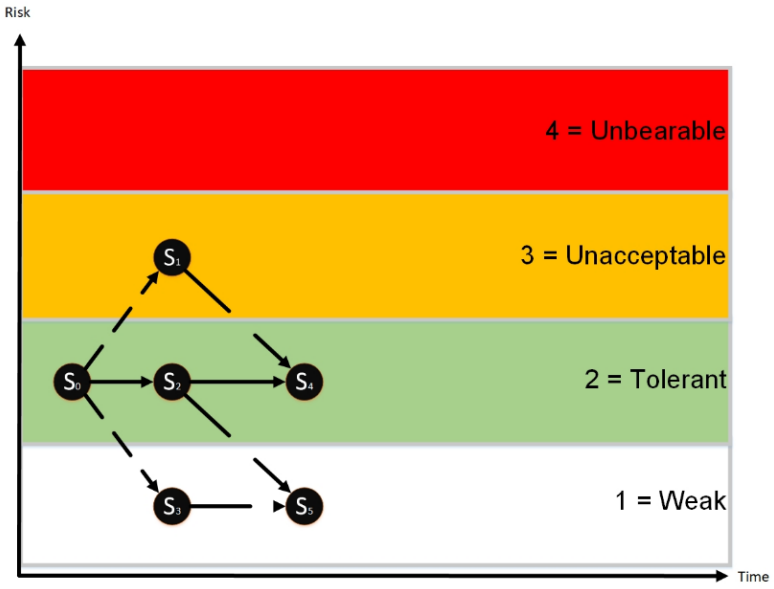

Figure 4: Graphical representation of states and risk levels.

5.1. Cyberattack probability evaluation in each of the states

We introduced Formula 1 for establishing the risk value of an asset. Let us rewrite this Formula considering the probability of losing an asset as a result of possible attack on one of the assets:

$$R_{asset}(Attacks) = \sum_{i=0}^{k} (P_{availability}(attack_i) \cdot I_{availability}(attack_i) + P_{integrity}(attack_i) \cdot I_{integrity}(attack_i) + P_{confidentiality}(attack_i) \cdot I_{confidentiality}(attack_i)) \quad (8)$$

where $R_{asset}(Attacks)$ is a risk value due to attack events, $P_{availability}(attack_i)$ is the probability of loss availability of asset $attack_i$ due to attack events and $I_{availability}(attack_i)$ is the impact (a likely consequence) of an attack event of loss availability of asset $attack_i$, and the same for integrity and confidentiality for the asset due to attack events. The number of attacks is expressed by k.

Each attack is based on exploiting the existing vulnerability using an attack vector. Attack vector [1] - is a path or route used by the intruder to gain access to the target (asset). Vulnerability [5] - is a weakness in design, implementation, operation or internal control of a process that could expose the system to adverse threats at the time of threat events.

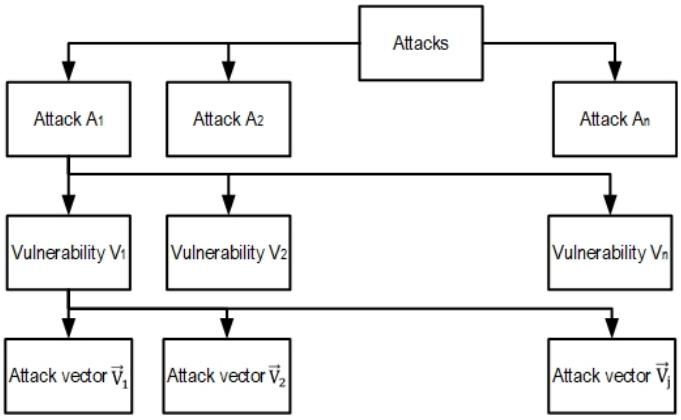

Figure 5: Attack consists of exploiting an existing vulnerability using an attack vector.

We can rewrite the likelihood of an attack (a_i) of all the attacks A on one of asset for each of security principle (availability, integrity or confidentiality) as follows: $P_{availability|integrity|confidentiality}(a_i) = P_{(c,[t;t+\Delta t])}(a_i|s)$.

Where

c - situation context within the time window $[t; t + \Delta t]$;

s - system state in the time window $[t; t + \Delta t]$.

Visual representation[1] of an attack on an asset is displayed in Figure 6.

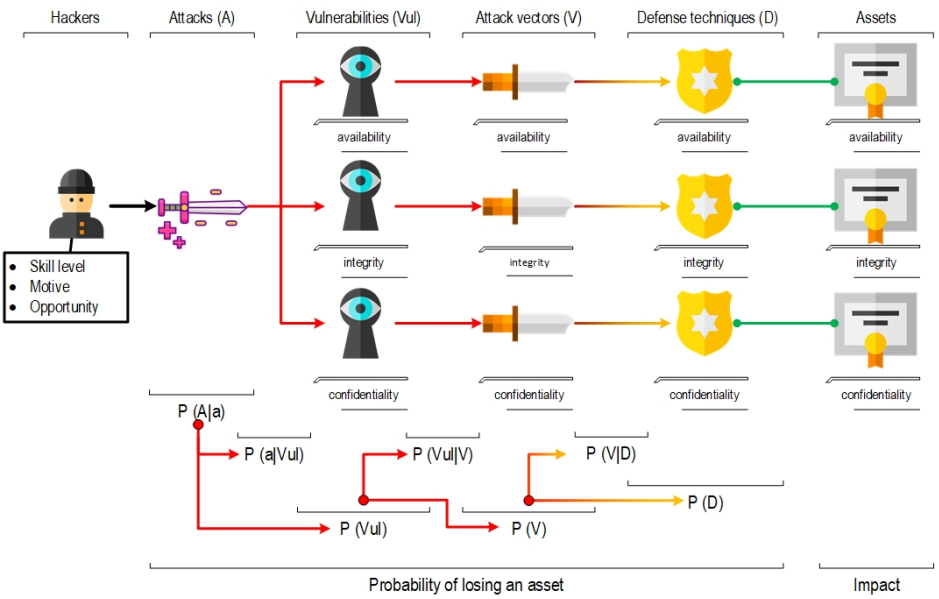

Figure 6: Visualized decomposition of an attack on an asset.

[1] Full size picture of decomposition of an attack on an asset http://bit.ly/2PnSI8I

Since we cannot rely on average risk values, it is necessary to establish the probability of an attack a_i within the time window $[t; t + \Delta t]$ inside the context c (system parameters and LOGs), denoted by $P_{(c,[t;t+\Delta t])}(a_i|s)$:

$$P_{(c,[t;t+\Delta t])}(a_i|s) \quad = \sum_{i=0}^{k} \left(P_{(c,[t;t+\Delta t])}(A|a_i) \cdot P_{(c,[t;t+\Delta t])}(a_i)\right) \tag{9}$$

Where

k - stands for a number of all system states S;

$(P_{(c,[t;t+\Delta t])}(A|a_i)$ - denotes probability of attack a_i from various attacks (frequency of using this attack a_i), statistical data;

$P_{(c,[t;t+\Delta t])}(a_i)$ - stands for probability of occurrence of an attack a_i. This event is predetermined by total probability of exploiting all vulnerabilities $|Vul|$ during the time interval $[t; t + \Delta t]$. Let us consider this decomposition in more detail in the Formula 10.

$$P_{(c,[t;t+\Delta t])}(a_i) = \sum_{j=0}^{|Vul|} P_{(c,[t;t+\Delta t])}(a_i|vul_j) \cdot P_{(c,[t;t+\Delta t])}(vul_j) \tag{10}$$

Where

$|Vul|$ - number of vulnerabilities enabling commitment of an attack a_i;

$P_{(c,[t;t+\Delta t])}(a_i|vul_j)$ - probability that precisely this vulnerability vul_j among among others vulnerabilities of attack a_i (frequency of using this vulnerabilities vul_j), statistical data.

The probability of occurrence of a vulnerability vul_j event depends on total probability of exploitation of attacks vector $\overleftarrow{V}$ during the time interval $[t; t + \Delta t]$ presented in Formula 11.

$$P_{(c,[t;t+\Delta t])}(vul_j) = \sum_{i=0}^{|\overleftarrow{V}|} P_{(c,[t;t+\Delta t])}(vul_j|\overleftarrow{v_i}) \cdot P_{(c,[t;t+\Delta t])}(\overleftarrow{v_i}) \tag{11}$$

Where

$|\overleftarrow{V}|$ - identifies the number of vulnerability attack vul_j;

$P_{(c,[t;t+\Delta t])}(vul_j|\overleftarrow{v_i})$ - probability of using attack vector $\overleftarrow{v_i}$ from among various attacks vectors for the vulnerability vul_j (frequency of using this attack vector $\overleftarrow{v_i}$), statistical data.

More detailed representation of the attack vector probability can be tracked by analyzing Formula 12.

$$P_{(c,[t;t+\Delta t])}(\overleftarrow{v_i}) = \sum_{j=0}^{|D|} P_{(c,[t;t+\Delta t])}(\overleftarrow{v_i}|d_j) \cdot P_{(c,[t;t+\Delta t])}(d_j) \tag{12}$$

Where

$|D|$ - number of protective measures against the attack vector v_i;

$P_{(c,[t;t+\Delta t])}(\overleftarrow{v_i}|d_j)$ - harm caused by an attack vector $\overleftarrow{v_i}$ with a valid protection measures d_j (return value of quality of defense against attack vector), statistical data;

$P_{(c,[t;t+\Delta t])}(d_j)$ - probability of using this protection measure (yes or no).

When calculating values in one or more stages of the risk level analysis, some parameters of P (Formula 13) might be changed. Each attack vector has different parameters α_1 (information flow on the computer network), α_2 (number of backlinks), ..., α_n, which affect the probability of an attack.

The detection of anomalies for parameter α_i serves as one of the ways to determine the intrusion through IDS. For example, IDS / IPS analyze the data to detect the following intrusions:

Anomaly detection;

Signatures and Heuristic Detections.

For each probability $P_{(c,[t;t+\Delta t])}(\overleftarrow{v_i}|d_j)$ of attack within context c, attack vector $\overleftarrow{v_i}$ and protection measure d_j we can define the function $f(\alpha_1, \dots, \alpha_n)$:

$$P_{(c,[t;t+\Delta t])}(\overleftarrow{v_i}|d_j) = f(\alpha_1, \dots, \alpha_n) \quad (13)$$

The improved prediction of probability of attacks could be achieved through the creation of artificial parameters. Consider such countermeasures to increase the prediction chances. Some countermeasures assume the application of parameters α that increase the predicting probability. The examples of attacks and countermeasures are presented below:

Copy a site using HTTrack software or similar programs [16]. In this case, it would be necessary to perform a real-time speed analysis and check the order of web pages asking. Consider an option of script-markers adding upon finding a complete copy of the website (JavaScript for the website's pages). The downloaded pages will automatically contain these built-in scripts. This will allow to determine whether these pages were opened from a different address or not. When opened, the address of the opened page will not match the original (canonical) address. The script for these markers sends information to the attack prediction system with the note "view the saved pages of the site" ($\alpha_{view-saved-pages-site}$) in case you view the downloaded pages on your website. In this case, it is desirable to send the maximum complete information from the computer which was used to open the registered copy of a website. This will help to obtain the information about the potential attacker, which will change the system risk level.

Create false or incorrect metadata for txt, docx, xlcx, pptx, etc. In this case, it is necessary to consider the creation of fake characters (first and last name). The search is done in the search engines that provide erroneous information to the potential attacker. Relying on this collection of information, it is necessary to transmit to the attacker the fake web page where it is necessary to obtain the most complete information on the potential attacks during the transmission and, consequently, a notification is sent to the attack forecasting system with a note "display false pages with the transmission of the search system" ($\alpha_{display-false-pages}$).

Fill in the robots.txt file with additional false information and try to confuse the attacker who is interested in this file. Add links to this file, which would provoke the attacker's interest, such as links that include words like "admin", "login", etc. Establish link tracking transitions in the same way as in step 2. All calls to the robots.txt file by agents that are not search engine robots must be logged to inform the system prediction attacks through the note "display of the robots.txt file is from intruder" ($\alpha_{display-robots.txt-by-intruder}$).

In the html code of the page, it is necessary to provide comments where fake addresses of system administrators and/or developers are found. Applying scanning programs, like The Harvester [15], the attacker will get "an interesting target for an attack" that will be an excellent marker for predicting attack system ($\alpha_{display-target-for-an-attack}$).

In case of our example, shown in Figure 7, it is possible to embed script-markers for the attack prediction system on Cloud VPS. With built-in scripts-markers, the $S_{scripts-markers}$ system parameter $\alpha_{scripts-markers}$ will be added to the list of indirect parameters affecting the probability of attack.

It is possible to add false metadata, including a fake author of some files (docx, pdf, etc.). One has to create a page with contacts of this fake author who created these files (docx, pdf, etc.) on the website. Relying on the site's viewing statistics, we can track visits to the pages of the fake author's files. Viewing this page is a consequence of studying method documents for the purpose of *footprinting and reconnaissance*. It means that someone is interested in the created fake pages, then the probability of the parameter $\alpha_{metadata-fake-search}$, will change the state of the system to the state $S_{metadata-faike-search}$.

For a variety of attack vectors one must identify parameters $\alpha_1, \dots, \alpha_n$ to produce the probability function of various attacks. These parameters, indicating a certain type of attack, must be "sieved" using the BigData method. It is necessary to eliminate noise from the results of the study. Following the BigData methodology, the most informative parameters will be highlighted.

To estimate the probabilistic law of our reference parameters $\alpha_1, \dots, \alpha_n$ we should choose different learning techniques, for example, the artificial neural network. This could help us find the exact function of $f(\alpha_1, \dots, \alpha_n)$ for each probability $P_{c_{[t;t+\Delta t]}}(a_i)$ of attack.

6. Example of simplified website administration on a cloud dedicated server

In this section we will attempt to clarify the application of our approach by referring to a simplified example. Figure 7 illustrates an example of simplified website administration on a cloud dedicated server (system S).

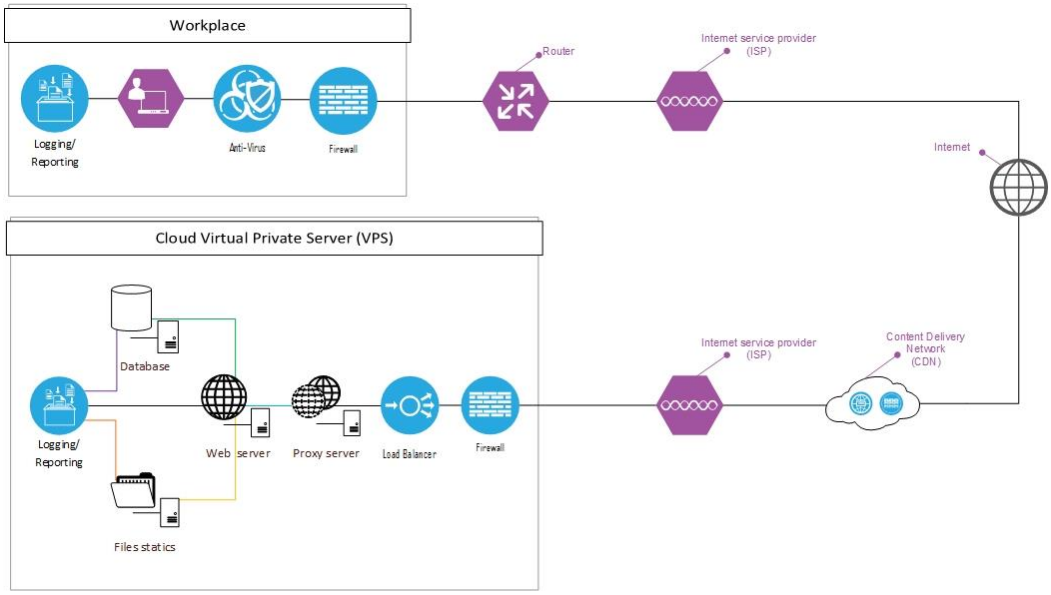

Figure 7: Website administration on a cloud dedicated server.

The list below contains a general set of website administration components on a dedicated server:

Workplace:

Firewall;

Anti-virus;

Logging/reporting by operating system (OS) and by anti-virus.

Router (for connection to the Internet Service Provider (ISP));

Content Delivery Network (CDN);

Cloud Virtual Private Server (VPS):

Firewall;

Load balancer (e.g. Gobetween, Nginx, etc.);

Proxy server (e.g. Squid, Varnish, etc.);

Web server (e.g. Apache, IIS, etc.);

Statics files (e.g. images, CSS, JS, etc.);

Database (e.g. MySQL, MSSQL, etc.);

Logging/reporting by OS.

The administrator has root access via SSH to the server through one-step authentication via a Certificate for Authentication, while a hacker wants to obtain a database dump. This is a simplified model consisting of two sides: administrator and hacker. We will refer to this example later to clarify different steps within the framework of our approach.

6.1. Example of assets analysis

Let us analyze the system description in more detail. The initial stage encompasses the consideration of assets. They are falling under definition of business processes that use assets (application data, data bases, personal office data, local area network services, common services, working environment, digital accounting control, etc.) $A: a_0 \dots a_n$, where $n \in N$.

Each asset class comprises the following components avl - Availability, int - Integrity, cnf - Confidentiality:

$$a = (Asset_0, avl, int, cnf) \quad (14)$$

An estimate is made of their value $(Val_{avl}, Val_{int}, Val_{cnf})$. This evaluation occurs by assigning each asset a certain criticality level when the asset is completely lost. Thus, the damage is taken into account after the asset's complete loss. The asset valuation is carried out in compliance with the selected methodology (MEHARI, CobiT, etc.). The system S performs an analysis in compliance with the chosen risk assessment methodology RM. This means that the value of the used assets is determined in case of each business process.

A: represents a set of assets. The sequence of $a_0, a_1, \dots$ describes a set of meta-variables used by us, which are ultimately comprising A. For this example of assets: a_0 =Application data (data bases).

A^N: describes a set of attribute names of A. Availability (avl), Integrity (int), Confidentiality (cnf), Efficiency (eff) are attribute names applied by us to specify a security class of an asset a. For example, efficiency of the management process in order to comply to the legal, regulatory or contractual requirements, domain laws and regulations.

A^V: represents a set of attribute values of N_{att}. We are proposing to use 4 point scale (1 = Low, 2 = Acceptable, 3 = Inadmissible, 4 = Intolerable) for any asset's attribute name (avl, int, cnf, eff) while assessing the degree of importance (the level of loss when the asset is lost) of each value.

Val: represents a function 15 of assets valuation.

$$Val: A \times A^N \to A^V \quad (15)$$

In the example, provided by us, it is defined as $Val_{a_0} = (3,3,4)$ (Application data) and established for the following three attribute's components (Availability $a_0[0] = 3$, Integrity $a_0[1] = 3$, Confidentiality $a_0[2] = 4$).

For a_0 = Application data (data bases)

$Val_{a_0[0]} = 3$ (Availability = Intolerable);

$Val_{a_0[1]} = 3$ (Integrity = Inadmissible);

$Val_{a_0[2]} = 4$ (Confidentiality = Inadmissible);

6.2. Example of protection measures analysis

It is worth to undertake an analysis of protection measures D for assets A involved in business processes BP for the initial configuration of the system $Conf_h$, where $h = 0$ stands for the initial configuration.

$$D = (Conf, v), \quad (16)$$

where v stands for vulnerabilities and exposures.

The following protection measures are ensured in case of our system:

Cloud Virtual Private Server (VPS);

Firewall;

Logging/reporting by OS.

The following Formula 17 is used by us to determine the risk for business processes:

$$RM: BP \times A \times D \rightarrow 2\text{"Tolerant"} \tag{17}$$

The risk level is assessed for the applied system configuration $Conf_i$, and it corresponds to the undertaken security measures. The network audit is carried out applying the chosen risk assessment methodology RM. At configuration modeling stage, the system configuration variants are created to match the acceptable risk levels.

6.3. Example of system states modeling

Consider the example of a network shown in Figure 7. In our example, a hacker would undertake an attempt to download the entire database dump. Here we are speaking about SQL injection[1]. In that context we would need to use the following Formula 18 as a first step:

$$R_{database}(\text{SQLinjection}) = \sum_{i=0}^{1} (P_{availability}(\text{SQLinj.}) \cdot 3 + P_{integrity}(\text{SQLinj.}) \cdot 3 + \\ + P_{confidentiality}(\text{SQLinj.}) \cdot 4) \tag{18}$$

Relying on OWASP it is possible to conclude that $P_{confidentiality}$ is one of the most widespread types of attack[2].

$$P_{(c,[\text{month}])}(\text{SQLinj.}|s) = \sum_{i=0}^{1} (1 \cdot P_{(c,[\text{month}])}(\text{SQLinj.})) \tag{19}$$

For illustrative purposes let us consider only the following vulnerability CVE-2019-8429 [14] applying Formula 10:

$$P_{(c,[\text{month}])}(\text{SQLinj.}) = \sum_{j=0}^{1} P_{(c,[\text{month}])}(\text{SQLinj.}|\text{CVE} - 2019 - 8429) \cdot \\ \cdot P_{(c,[\text{month}])}(\text{CVE} - 2019 - 8429) \tag{20}$$

Only one attack vector (Network) is identified for this vulnerability, therefore, Formula 11 will look as follows:

$$P_{(c,[\text{month}])}(\text{CVE} - 2019 - 8429) = \sum_{i=0}^{1} 1 \cdot P_{(c,[\text{month}])}(\overleftarrow{v_i}) \tag{21}$$

Taking into account the applied protection measures (firewall and logging), we may represent Formula 12 as follows:

$$P_{(c,[\text{month}])}(\overleftarrow{v}) = \sum_{i=0}^{1} (P_{(c,[\text{month}])}(\overleftarrow{v}|\text{firewall}) \cdot 1) \tag{22}$$

In our case, the firewall does not protect against SQL-injection. The success rate of this attack corresponds to 1. Accordingly, the level of risk remains "Unacceptable" in one month : $S_0 \rightarrow S_1$ (Figure 4). To maintain the level of risk, it is necessary to reconfigure the system $S_0 \rightarrow S_2$ (Figure 4). For possible attack scenarios, it is necessary to select such α parameters (markers) that will indicate a planned attack. In our case, a log analysis can show how often hackers are attempting to identify vulnerabilities. For our example, the period of one month is based on the logs analysis. Thus, we can predict the level of risk for the future. This will allow us to prepare for an attack in advance.

7. Future Work

One of the possible directions of the scientific work is the Theory of Games. This theory enables the prediction of behavior patterns of attacking and defending sides. Let us briefly consider this option.

Today, it is possible to draw an analogy between an Intruder (or a group of cybercriminals) and an information security specialist (a group of information security experts). Both could be compared with two gamers (teams) playing against

[1] OWASP SQL Injection http://bit.ly/2vmHNTD
[2] Top 10-2017 A1-Injection http://bit.ly/2VVAopZ

each other in real time. This game environment creates a realistic situation when both teams must take rapid decions, which might have serious consequences.

The teams are lacking time and have rather limited amount of information while making such decisions. In such a game, the defending party may incur maximum financial losses, while the attacking party can be prosecuted. The stakes in such a game are raised much higher, in the case the attacking party is represented by a special governmental department acting nationwide.

The mechanism of this game is shown in Figure 8.

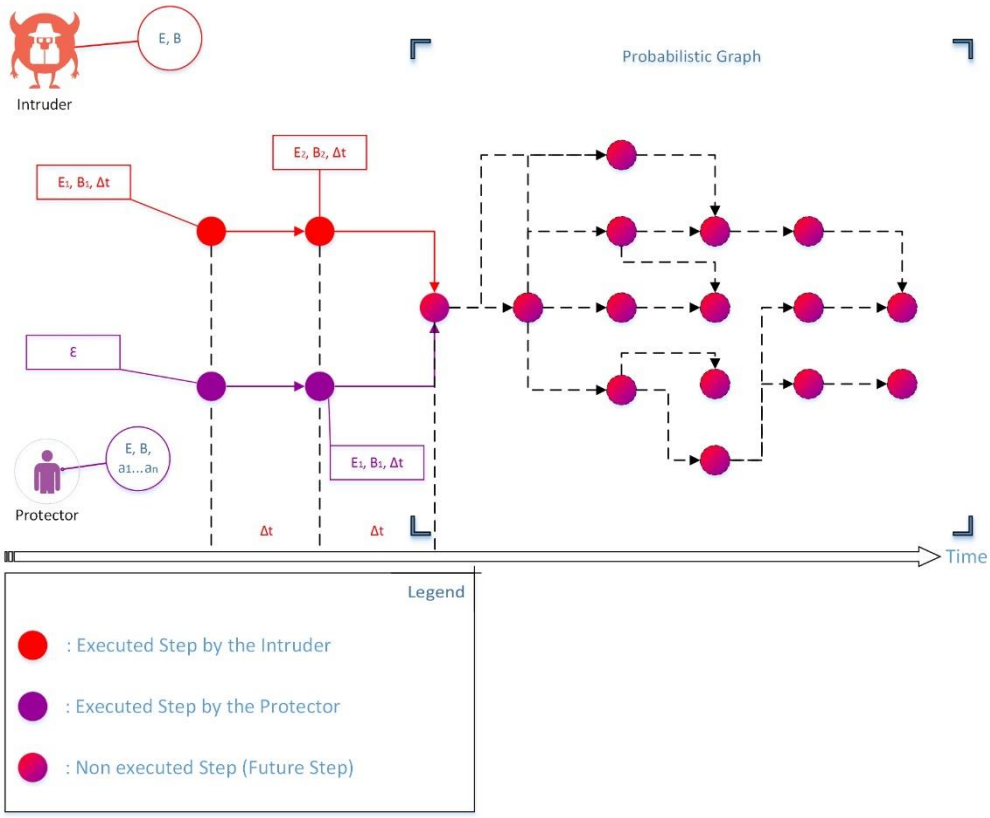

Figure 8: The mechanism of game for cybersecurity.

Consider a formal example of such a game. The attacker - Intruder (I) starts his game by identifying the vulnerabilities in the information security system of the defending party - Protector (P). Protector makes an action plan $a_1 \dots a_n$ to improve the protection of your system in real time. Intruder, in turn, analyses the presence of the vulnerabilities $v_1 \dots v_n$. Afterwords, he/she compiles an attack strategy. Each side has its own characteristics in this case, which include the level of experience E, the budget B, the time limit for the accomplishment of certain actions Δt. Bayesian games could be viewed as another representation of the characteristics describing the game theory. In Bayesian games, the challenge is to identify how a player can assign appropriate initial beliefs to its opponents. Furthermore, it is sometimes interesting to consider a dynamic update of the players' beliefs. The formal definition of the repeated Bayesian game can be expressed applying a 7-tuplet [6]:

$$G = (N, \Theta_k, A_k, H(t_q), \Sigma_k, \mu_k, U_k) \quad (23)$$

where:

N is the set of game players (M stands for a number of players);

Θ_k is the set of possible player types $k \in N$;

A_k is the set of available action types $k \in N$;

$H(t_q)$ is the set of possible $date - t_q$ game histories;

Σ_k is the set of the player's behavior strategies $k \in N$;

μ_k is the player's posterior belief k defined as a conditional probability that its opponents' types are θ_{-k}, given history $h(t_q)\varepsilon H(t_q)$ and type $\theta_k \in \Theta_k$;

U_k is the utility function of a player $k \in N$ until time $t_q, q \geq 0$, given the history $h(t_q)$.

Let us consider as a basis the shortest time for the execution of an attack or countermeasures taken during Δt. Each side has its own budget B and experience corresponding to level E. Anyway, a certain level of experience is required to perform one action, which also results in time expenditures expresses as $n \cdot \Delta t$. In this case, the empty action is taken ε. Upon the accomplishment of several actions, each system state would affect the opponent's subsequent steps. The system states modeling is enabled through the resort to probability graphs.

Conclusion

This research work has practical applications in information security systems. The findings of this work will contribute to the development of prediction of cyberattacks. Thus, it will be possible not only to simulate a threat, but to determine the level of its risk, depending on different configurations of security systems. This will enable more effective information security management. This work will serve as a basis for further research in the area of distribution of funds for the investment in information security [2]. This research work is also an attempt to prove that in the context of system security it will be possible to predict the level of risk of the weakest points based on the analysis of statistical data and hackers' behaviour in different contexts.

References

[1] Common vulnerability scoring system calculator version 3 cve-20198429," http://bit.ly/2XufnCR, accessed: 2019-04-20.
[2] Owasp risk rating calculator, https://bit.ly/2VmPUij, accessed: 201905-07.
[3] Threat prediction platform http://bit.ly/2Zadf4X, accessed: 2018-0331.
[4] Ellis and T. McELwee, "System and method for predicting impending cyber security events using multi channel behavioral analysis in a distributed computing environment," Mar. 21 2017, US Patent 9,602,530.
[5] Seifert, I. Welch, and P. Komisarczuk, "Identification of malicious web pages with static heuristics," in *Telecommunication Networks and Applications Conference, 2008. ATNAC 2008. Australasian*. IEEE, 2008, pp. 91–96.
[6] Siaterlis and B. Maglaris, "Detecting ddos attacks with passive measurement-based heuristics" in *Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on*, vol. 1. IEEE, 2004, pp. 339–344.
[7] Achmadi, Y. Suryanto, and K. Ramli, "On developing information security management system (isms) framework for iso 27001-based data center," in *2018 International Workshop on Big Data and Information Security (IWBIS)*. IEEE, 2018, pp. 149–157.
[8] Fudenberg, "Andj. Tirole, Game Theory," 1991.
[9] J. Farahani, M. H. A. Kachoee, and M. A. A. Kachoee, "Vulnerability assessment of the critical infrastructure against man-made threats," *Industrial Engineering & Management Systems*, vol. 17, no. 1, pp. 136– 145, 2018.
[10] Cavusoglu, B. Mishra, and S. Raghunathan, "A model for evaluating it security investments," *Communications of the ACM*, vol. 47, no. 7, pp. 87–92, 2004.

[11] Debar and A. Wespi, "Aggregation and correlation of intrusiondetection alerts," in *Recent Advances in Intrusion Detection*. Springer, 2001, pp. 85–103.
[12] Mehari expert (2010) tool." http://bit.ly/2uHDFgh, accessed: 201903-31.
[13] N. C. Wael Kanoun, Fredéric Cuppen, in "Evaluation des risques dans une processus de supervision de la securité," in *Ecole Nationale Superieure des Télécommunications.* IFSIC, 2007, pp. 11–12.
[14] N. Minar, K. H. Kramer, and P. Maes, "Cooperating mobile agents for dynamic network routing," in *Software agents for future communication systems*. Springer, 1999, pp. 287–304.
[15] P. Mongsawad *et al*., "The philosophy of the sufficiency economy: a contribution to the theory of development," *Asia Pacific Development Journal*, vol. 17, no. 1, p. 123, 2010.
[16] P. Prakash, M. Kumar, R. R. Kompella, and M. Gupta, "Phishnet: predictive blacklisting to detect phishing attacks," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–5.
[17] P. Yermalovich and M. Mejri, "Formalization of attack prediction problem," in *2018 IEEE International Conference" Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)*. IEEE, 2018, pp. 280–286.
[18] Mehari expert 2010 fr, http://bit.ly/2GlaeaI, accessed: 2018-02-21.
[19] Harvester - osint, http://bit.ly/2KxADGk, accessed: 2018-02-23.
[20] Httrack." http://bit.ly/2VQl6T2, accessed: 2018-02-23.