INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2021, VOL. 67, NO. 1, PP. 35-41
Manuscript received May 3, 2020; revised January, 2021. DOI: 10.24425/ijet.2021.135941

Markov Model of Cyber Attack Life Cycle Triggered by Software Vulnerability

Romuald Hoffmann

***Abstract*— Software vulnerability life cycles illustrate changes in detection processes of software vulnerabilities during using computer systems. Unfortunately, the detection can be made by cyber-adversaries and a discovered software vulnerability may be consequently exploited for their own purpose. The vulnerability may be exploited by cyber-criminals at any time while it is not patched. Cyber-attacks on organizations by exploring vulnerabilities are usually conducted through the processes divided into many stages. These cyber-attack processes in literature are called cyber-attack live cycles or cyber kill chains. The both type of cycles have their research reflection in literature but so far, they have been separately considered and modeled. This work addresses this deficiency by proposing a Markov model which combine a cyber-attack life cycle with an idea of software vulnerability life cycles. For modeling is applied homogeneous continuous time Markov chain theory.**

***Keywords*—Markov model, cyber-attack, vulnerability, life cycle, homogenous continuous time Markov chain**

I. INTRODUCTION

A. Cyber Attack Life Cycle

A CYBER-ATTACK process which is divided into phases can be named a cyber-attack life cycle or a cyber kill chain. In cyber security papers, the cyber kill chain is a very popular conceptual model generally describing processes of targeted cyber-attacks. In research literature cyber-attack life cycles and their phases are variously named, defined and described. For instance, according to [1] the cycle consists of five stages: reconnaissance, scanning, system access, malicious activity and exploitation. In [2] the cyber-attack process is named as the intrusion kill chain and defined as the sequence of seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), action. This chain is also described by researchers in [3,4]. Other researchers [5] point out six stages: reconnaissance, weaponization, delivery, exploitation, installation, C2, objective achievement. These authors indicate that an attack on critical infrastructure should be considered as a sequence of six phases: reconnaissance, weaponization, delivery, cyber execution, control perturbation, physical objective realization. In all available approaches to description of cyber-attack life cycles there are not specified an initiation and a termination stage. So, a generalized cyber-attack life cycle has recently been proposed which includes two additional phases [6]. The first stage is an identification of the attacker's needs. The last stage of the cyber-attack is a termination of the attack combined with removing traces of attackers' activities.

Despite of the fact that in its nature the cyber-attack processes are stochastic a few models of the cyber-attack life cycles using the theory of stochastic processes have been proposed so far [6-8].

B. Software Vulnerability Life Cycle

The life cycle of a software vulnerability can be generally divided into several phases that start or end with events: birth, creation, discovery, exploit, disclosure, software patch release, patch installation. In information security research papers, some definitions of software vulnerability life cycles have been proposed [9-13]. In [9], one of the first papers, the software vulnerability life cycle was defined with following stages:

- birth - the introduction of a vulnerability at the software development stage,
- discovery - somebody discovered the vulnerability,
- disclosure - internal dissemination of information in circle of people who protect the systems,
- correction - a patch released,
- publicity - public disclosure of the vulnerability,
- scripting - an exploit is available and can be used by cyber-attackers,
- death - the vulnerability identified with the installation of the patch.

Despite the fact that the life cycle of a vulnerability is similarly described in the literature, but there are significant differences can be found, e.g. in the work [10] an issue and an installation of patches are treated alternatively, and both these events close the life cycle of the vulnerability.

In last decade, as a result of research on stochastic nature of life cycles of software vulnerabilities, several probabilistic models of vulnerability life cycles have been proposed [13-16]. Published models are based on Markov processes with continuous or discrete time and finite numbers of states.

B. Aim of Article

This paper aim is to provide theoretical and analytical stochastic model combining both life cycles of a cyber-attack and a vulnerability. The proposed model is based on homogeneous continues-times Markov chain theory. The vulnerability part of the joint life cycle considered in this paper generally bases on the idea presented in [9]. For purpose of simplicity, stages of the cyber-attack life cycle used here are understood as in [1]. It is also assumed that any current phase of

Romuald Hoffmann is with Institute of Computer and Information Systems, Faculty of Cybernetics, Military University of Technology, Warsaw, Poland. ORCID: 0000-0001-5999-1986 (e-mail: romuald.hoffmann@wat.edu.pl)

a cyber-attack may be abandoned by aggressors or stopped by cyber defense systems at any time. Then a new iteration of the cyber-attack may begin as long as the vulnerable software is not patched.

II. Preliminary Assumptions of the Model

In the presented model of cyberattack life cycle targeted on exploiting a vulnerability, in the part related to the vulnerability, the model is based on the idea of a vulnerability life cycle described in [9]. The stages of a cyber-attack are basically understood as in [1].

For purpose of this paper, we assume that behavior of both cyber-attack life cycle describing a cyber-attack targeted on a vulnerability and vulnerability life cycle fulfill Markov property. So, the stochastic model of a cyber-attack life cycle triggered by a software vulnerability is a continues-time Markov chain (CTMC) with a finite number of states. The states of the stochastic process are relevant stages of the vulnerability and cyber-attack life cycle as follows:

- (S_0) Birth – a vulnerability is introduced at the software development stage.
- (S_1) Discovered – somebody discovers the vulnerability and then internal dissemination of information in circle. If the discoverer is someone who protects a system, then a patching design process starts.
- (S_2) Disclosed – refers to public disclosure of the vulnerability.
- (S_3) Patched – corresponds to the installation of a patch or patches.
- (S_4) Reconnaissance – refers to acquiring information about targets, targeting process, eventually starting weaponization process.
- (S_5) Scanning – scanning a targeted system for obtaining specific information about the system's devices, services, users, etc. A zero-day vulnerability is identified in targeted software if it is available. Cyber weapon design is finished.
- (S_6) System access – once the strategy of cyber-attack is finally worked out and a set of cyber weapons is prepared the system access step begins. Access to the targeted system can be done by e.g. using social techniques, direct re-mote access to the system, etc. During this stage an initial installation of malicious boot code can be done.
- (S_7) Malicious activity – a dynamic command and control loop is established with the attackers and additional compromising malicious software can be downloaded and installed. A feedback about quality and performance of a weaponry malicious code is sent back to the attacker's developers for improvements. More information about the attacked system is sent back to the hostile environment.
- (S_8) Exploitation – final stage of the cyber-attack. More malicious activities are conducted to achieve the required objectives, e.g. copying and stealing information, deleting or changing data, damaging operational systems, etc. In this stage from infected system the cyber-attacker can launch an attack on other systems, remotely or locally.

We assume that transition rates between the states of the stochastic process are finite and unchanging over time, and the generator matrix is known. Thus, basis on the above assumption made, the cyber-attack chain are modeled with using homogenous continues-time Markov chains.

III. Homogenous Continuous-Time Markov Chain

A continuous-time Markov chain is a stochastic process in which the process moves among states and its sojourn time spent in each state to visit the next state is independent and distributed exponentially [17]. In other words, the property of the stochastic process which the conditional probabilities of the transitions to the future states depend only on the present state and are independent of the history, is called a Markov property. The stochastic processes with Markov property at any time are Markov processes.

Let's consider a continuous-time stochastic process $\{X(t), t \geq 0\}$ with a finite state set $\boldsymbol{S} = \{S_0, S_1, \dots, S_N\}$ and note that the event $\{X(t) = S_k, t \geq 0\}$ represents that the process is in the state S_k $(k = 1, 2, \dots, N)$ at time $t \geq 0$. We want to know in which state the process $X(t)$ is at time $t \geq 0$ and the process converges as $t \to +\infty$.

If we suppose that the probabilities $P\{X(t) = S_k \mid X(t0) = S_0, X(t_1) = S_1, \dots, X(t_n) = S_n\} = P\{X(t) = S_k \mid X(t_n) = S_n\}$ for all $S_0, S_1, \dots, S_n \in \boldsymbol{S}$ and $0 \leq t_0 \leq t_1 \leq \dots \leq t_n \leq t$ then the process $\{X(t), t \geq 0\}$ is said to be a continuous-time Markov chain.

If the probability of $X(t + \Delta t)$ being in the state S_k, given that $X(t)$ is in the state S_j, is independent of $t \geq 0$, i.e. $P\{X(t + \Delta t) = S_k \mid X(t) = S_j\} = P_{jk}(\Delta t)$, then the process $\{X(t), t \geq 0\}$ has a stationary or homogeneous transition probability that depends only on the time difference Δt. The process which has this property is said to be a homogeneous continuous-time Markov chain.

Homogeneous continuous-time Markov chains can be analyzed by forming and solving Kolmogorov differential equations:

$$\frac{d}{\mathrm{dt}}\boldsymbol{P}(t) = \boldsymbol{P}(t) \cdot \boldsymbol{Q} \tag{1}$$

with the initial condition $\boldsymbol{P}(0) = [P_0(0^+), P_1(0^+), \dots, P_N(0^+)]$, where $\boldsymbol{P}(t) = [P_0(t), P_1(t), \dots, P_N(t)]$, $P_k(t) = P\{X(t) = S_k, t \geq 0\}$ $(k = 0, 1, \dots, N)$, $\boldsymbol{Q}$ is the generator matrix which has entries that are the rates at which the process $X(t)$ jumps from state to state. These entries are defined by $\lambda_{jk} = \lim_{\Delta t \to 0} \frac{P\{X(t+\Delta t)=k \mid X(t)=j\}}{\Delta t}$ for all $k \neq j$, and $\lambda_{jj} = -\sum_{\substack{k=1 \\ k \neq j}}^{N} \lambda_{jk}$.

IV. Markov Model of the Life Cycle

The Markov model of a cyber-attack life cycle triggered by a software vulnerability (a joint cyber-attack and software vulnerability life cycle), is illustrated in Fig.1 as a directed graph, i.e. as a Markov graph [17].

In the model, in order to finalize a cyber-attack successfully, the attack process should pass sequentially through the stages from S_4 "reconnaissance" to S_8 "exploitation" without any

possibilities of skipping intermediate stages (see Fig.1). Returning to the previous ones are possible. We assume that cyber-attacks may be stopped or ended during any stage at any time because of a patch installation done. Transition from state S_2 to state S_3 means that once discovering a vulnerability e.g. by a software producer, a patch or patches are developed and installed. This transition finalizes the life cycle.

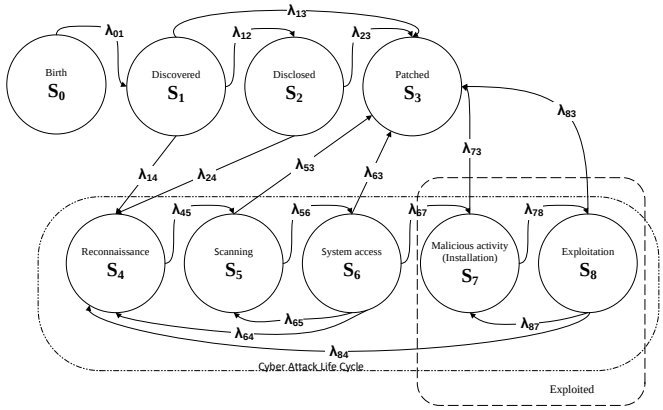

Fig. 1. Markov graph of the proposed cyber-attack life cycle model

The stochastic model is the homogeneous continues-time Markov chain $\{X(t), 0 \le t < +\infty\}$ with the state space $\boldsymbol{S} = \{S_0, S_1, \dots, S_8\}$. Let λ_{kj} be the transition rate from S_k to S_j $(k, j = 0, 2, \dots, 8)$. Then the infinitesimal generator of the CTMC for the life cycle is given by matrix $\boldsymbol{Q}$:

$$\mathbf{Q} = \begin{bmatrix} -\lambda_{01} & \lambda_{01} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\lambda_{11} & \lambda_{12} & \lambda_{13} & \lambda_{14} & 0 & 0 & 0 & 0 \\ 0 & 0 & -\lambda_{22} & \lambda_{23} & \lambda_{24} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\lambda_{45} & \lambda_{45} & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_{53} & 0 & -\lambda_{55} & \lambda_{56} & 0 & 0 \\ 0 & 0 & 0 & \lambda_{63} & \lambda_{64} & \lambda_{65} & -\lambda_{66} & \lambda_{67} & 0 \\ 0 & 0 & 0 & \lambda_{73} & 0 & 0 & 0 & -\lambda_{77} & \lambda_{78} \\ 0 & 0 & 0 & \lambda_{83} & \lambda_{84} & 0 & 0 & \lambda_{87} & -\lambda_{88} \end{bmatrix} \quad (2)$$

where $\lambda_{11} = \lambda_{12} + \lambda_{13} + \lambda_{13}$, $\lambda_{22} = \lambda_{23} + \lambda_{24}$, $\lambda_{55} = \lambda_{53} + \lambda_{56}$, $\lambda_{66} = \lambda_{63} + \lambda_{64} + \lambda_{65} + \lambda_{67}$, $\lambda_{77} = \lambda_{73} + \lambda_{78}$, $\lambda_{88} = \lambda_{83} + \lambda_{84} + \lambda_{87}$.

Let $P_k(t)$ (k = 0, 1, …, 8) be the probability of the event $\{X(t) = S_k\}$ i.e. the probability of that the process $X(t)$ is in the state S_k at time $t \ge 0$. Thus, the row vector $\boldsymbol{P}(t) = [P_0(t), P_1(t), \dots, P_8(t)]$ is the probability distribution of the process X(t) at time $t \ge 0$. For purpose of this paper we assume that process $X(t)$ at $t = 0^+$ starts from state S_1 "Discovered".

In order to calculate the probability distribution $\boldsymbol{P}(t), t \ge 0$, the Kolmogorov differential equations of the process $X(t)$ should be solved. Laplace transformation particularly is a helpful tool to do it. The transformation is also useful to calculate some stochastic characteristics of stochastic processes [17], e.g. an expected value of total time which process $X(t)$ spends in a state.

Let the Laplace transformation of the probability $P_k(t), t \ge 0$, denote by

$$P_k^*(s) = \mathcal{L}[P_k(t); s] \stackrel{\text{def}}{=} \int_0^\infty P_k(t) \mathrm{e}^{-st} dt.$$

Thus, by the Laplace transformation of the vector $\boldsymbol{P}(t)$ we have $\mathcal{L}[\boldsymbol{P}(t); s] = \boldsymbol{P}^*(s) = [P_0^*(s), P_1^*(s), \dots, P_8^*(s)]$.

For the given generating matrix $\boldsymbol{Q}$ (see (2)), a Laplace transformation of the system of Kolmogorov differential equations (1) is:

$$s \cdot \boldsymbol{P}^*(s) - \boldsymbol{P}(0^+) = \boldsymbol{P}^*(s) \cdot \boldsymbol{Q} \quad (3)$$

with the initial condition $\boldsymbol{P}(0^+) = [P_0(0^+), P_1(0^+), \dots, P_8(0^+)] = [0,1,0,0,0,0,0,0,0]$.

Solving the equations (3), we get the transform of $\boldsymbol{P}(t)$:

$$\boldsymbol{P}^*(s) = \boldsymbol{P}(0) \cdot [s \cdot \boldsymbol{I} - \boldsymbol{Q}]^{-1} \quad (4)$$

The solution of equations (4) is collected in Table I, where

$$\det[s \cdot \boldsymbol{I} - \boldsymbol{Q}] = s(s + \lambda_{01})(s + \lambda_{12} + \lambda_{13} + \lambda_{14})(s + \lambda_{23} + \lambda_{24})((\lambda_{56}(-\lambda_{45}\lambda_{64} - s\lambda_{65} - \lambda_{45}\lambda_{65}) + (s + \lambda_{45})(s + \lambda_{53} + \lambda_{56})(s + \lambda_{63} + \lambda_{64} + \lambda_{65} + \lambda_{67}))(s + \lambda_{73} + \lambda_{78})(s + \lambda_{83} + \lambda_{84} + \lambda_{87}) + \lambda_{78}(-\lambda_{45}\lambda_{56}\lambda_{67}\lambda_{84} - (\lambda_{56}(-\lambda_{45}\lambda_{64} - s\lambda_{65} - \lambda_{45}\lambda_{65}) + (s + \lambda_{45})(s + \lambda_{53} + \lambda_{56})(s + \lambda_{63} + \lambda_{64} + \lambda_{65} + \lambda_{67}))\lambda_{87})) .$$

TABLE I
SOLUTION OF KOLMOGOROV EQUATIONS (3)

$\boldsymbol{P}^*(s)$	if $\boldsymbol{P}(0^+)$=[0,1,0,0,0,0,0,0,0]
$P_0^*(s)$	0
$P_1^*(s)$	$(s + \lambda_{12} + \lambda_{13} + \lambda_{14})^{-1}$
$P_2^*(s)$	$\lambda_{12}[(s + \lambda_{12} + \lambda_{13} + \lambda_{14})(s + \lambda_{23} + \lambda_{24})]^{-1}$
$P_3^*(s)$	$\frac{1}{s} - \sum_{k=0, k\neq 3}^{8} P_k^*(s)$
$P_4^*(s)$	$(det[s \cdot \boldsymbol{I} - \boldsymbol{Q}])^{-1} s(s + \lambda_{01})(\lambda_{12}\lambda_{24} + \lambda_{14}(s + \lambda_{23} + \lambda_{24}))(-\lambda_{56}\lambda_{65} + (s + \lambda_{53} + \lambda_{56})(s + \lambda_{63} + \lambda_{64} + \lambda_{65} + \lambda_{67}))(-\lambda_{78}\lambda_{87} + (s + \lambda_{73} + \lambda_{78})(s + \lambda_{83} + \lambda_{84} + \lambda_{87}))$
$P_5^*(s)$	$(det[s \cdot \boldsymbol{I} - \boldsymbol{Q}])^{-1} s(s + \lambda_{01})(\lambda_{12}\lambda_{24} + \lambda_{14}(s + \lambda_{23} + \lambda_{24}))\lambda_{45}(s + \lambda_{63} + \lambda_{64} + \lambda_{65} + \lambda_{67})(\lambda_{78}(s + \lambda_{83} + \lambda_{84}) + s(s + \lambda_{83} + \lambda_{84} + \lambda_{87}) + \lambda_{73}(s + \lambda_{83} + \lambda_{84} + \lambda_{87}))$
$P_6^*(s)$	$(det[s \cdot \boldsymbol{I} - \boldsymbol{Q}])^{-1} s(s + \lambda_{01})(\lambda_{12}\lambda_{24} + \lambda_{14}(s + \lambda_{23} + \lambda_{24}))\lambda_{45}\lambda_{56}(\lambda_{78}(s + \lambda_{83} + \lambda_{84}) + s(s + \lambda_{83} + \lambda_{84} + \lambda_{87}) + \lambda_{73}(s + \lambda_{83} + \lambda_{84} + \lambda_{87}))$
$P_7^*(s)$	$(det[s \cdot \boldsymbol{I} - \boldsymbol{Q}])^{-1} s(s + \lambda_{01})(\lambda_{12}\lambda_{24} + \lambda_{14}(s + \lambda_{23} + \lambda_{24}))\lambda_{45}\lambda_{56}\lambda_{67}(s + \lambda_{83} + \lambda_{84} + \lambda_{87})$
$P_8^*(s)$	$(det[s \cdot \boldsymbol{I} - \boldsymbol{Q}])^{-1} s(s + \lambda_{01})(\lambda_{12}\lambda_{24} + \lambda_{14}(s + \lambda_{23} + \lambda_{24}))\lambda_{45}\lambda_{56}\lambda_{67}\lambda_{78}$

The probabilities $\boldsymbol{P}(t), t \ge 0$ can be obtained by performing the inverse Laplace transform $\boldsymbol{P}(t) = \mathcal{L}^{-1}[\boldsymbol{P}^*(s); t]$ (e.g. see section VI).

To assess the losses generated by cyber criminals exploiting the vulnerability over a long period of time, it is necessary to calculate the total average time spent by attackers at each stage of the life cycle of the cyberattack. The calculation can be done with using Laplace transform $\boldsymbol{P}^*(s)$.

Let T_k be a mean stay time of the life cycle in the stage S_k i.e. a mean cumulative time while the process $\{X(t), t \geq 0\}$ stay in the state S_k. Let $\boldsymbol{T}_S = [T_0, T_1, \ldots, T_8]$ be a vector of mean stay times in the life cycle stages. To obtain $\boldsymbol{T}_s$ we need only to calculate the limit

$$T_k = \lim_{s\to 0} P_k^*(s) = \lim_{s\to 0} \int_0^\infty P_k(t)\mathrm{e}^{-st}dt$$

for $k = 0, 1, \ldots, 8$.

In other words, $\boldsymbol{T}_S = \lim_{s\to 0} \boldsymbol{P}^*(s)$. The solution of $\boldsymbol{T}_S$ is shown in Table II.

TABLE II
MEAN CUMULATIVE TIME $\boldsymbol{T}_S$

$\boldsymbol{T}_s$	if $\boldsymbol{P}(0^+)$=[0,1,0,0,0,0,0,0,0]
T_0	0
T_1	$(\lambda_{12} + \lambda_{13} + \lambda_{14})^{-1}$
T_2	$\lambda_{12} \cdot [(\lambda_{12} + \lambda_{13} + \lambda_{14})(\lambda_{23} + \lambda_{24})]^{-1}$
T_3	$+\infty$
T_4	$\big(\lambda_{12}\lambda_{24} + \lambda_{14}(\lambda_{23} + \lambda_{24})\big)\big(\lambda_{56}(\lambda_{63} + \lambda_{64} + \lambda_{67}) + \lambda_{53}(\lambda_{63} + \lambda_{64} + \lambda_{65} + \lambda_{67})\big)\big(\lambda_{78}(\lambda_{83} + \lambda_{84}) + \lambda_{73}(\lambda_{83} + \lambda_{84} + \lambda_{87})\big) / \lambda_{45} \cdot M_T$
T_5	$(\lambda_{12}\lambda_{24} + \lambda_{14}(\lambda_{23} + \lambda_{24}))(\lambda_{63} + \lambda_{64} + \lambda_{65} + \lambda_{67})(\lambda_{78}(\lambda_{83} + \lambda_{84}) + \lambda_{73}(\lambda_{83} + \lambda_{84} + \lambda_{87})) / M_T$
T_6	$(\lambda_{12}\lambda_{24} + \lambda_{14}(\lambda_{23} + \lambda_{24}))\lambda_{56}(\lambda_{78}(\lambda_{83} + \lambda_{84}) + \lambda_{73}(\lambda_{83} + \lambda_{84} + \lambda_{87})) / M_T$
T_7	$(\lambda_{12}\lambda_{24} + \lambda_{14}(\lambda_{23} + \lambda_{24}))\lambda_{56}\lambda_{67}(\lambda_{83} + \lambda_{84} + \lambda_{87}) / M_T$
T_8	$\lambda_{56}\lambda_{67}\lambda_{78}(\lambda_{12}\lambda_{24} + \lambda_{14}(\lambda_{23} + \lambda_{24})) / M_T$
$M_T = (\lambda_{12} + \lambda_{13} + \lambda_{14})(\lambda_{23} + \lambda_{24})\Big(\big(\lambda_{56}(\lambda_{63} + \lambda_{67}) + \lambda_{53}(\lambda_{63} + \lambda_{64} + \lambda_{65} + \lambda_{67})\big)(\lambda_{73} + \lambda_{78})(\lambda_{83} + \lambda_{84} + \lambda_{87}) + \lambda_{78}\Big(-\lambda_{53}(\lambda_{63} + \lambda_{64} + \lambda_{65} + \lambda_{67})\lambda_{87} - \lambda_{56}\big(\lambda_{63}\lambda_{87} + \lambda_{67}(\lambda_{84} + \lambda_{87})\big)\Big)\Big)$	

V. EXAMPLE ON APPLICATION OF THE MODEL: PROBABILISTIC RISK ASSESSMENT

Traditional risk assessment quantifies risk as the product of the probability of an undesirable event leading to specific consequences and a measure of the negative impact on the organization due to this undesirable event (probabilistic risk assessment) [18] or as a triplet of threat, vulnerability, and consequences [19].

In this section we use probabilistic risk assessment to quantify cyber risks. To do this, we should first calculate the probability of each phase of the cyber-attack life cycle, which can be determined using the proposed model (for examples see section VII).

We can calculate "risk" traditionally as a product of likelihood of threats and their impacts on the assets of an organization. To illustrate our approach simply assume that $\boldsymbol{A} = [A_0, \ldots A_3, A_4 \ldots, A_8]$, where $A_0 = \cdots = A_3 = 0$ and $A_4 \ldots, A_8 \geq 0$, is a vector of monetary losses of an organization's key assets calculated at each stage of the cyber-attack life cycle. Then, "total risk score" at time $t \geq 0$ represented as a real value function $R(t)$ can be calculated using the following equation:

$$R(t) = \boldsymbol{P}(t) \cdot \boldsymbol{A}^T$$

where $\boldsymbol{P}(t) = [P_0(t), \ldots, P_8(t)]$, $P_n(t) = P\{X(t) = n\}$ $(n = 0, \ldots, 8)$.

To calculate the sum of the total risk score $R(t)$ in a period $[0, \tau]$ we should calculate the integral $\int_0^\tau R(t)dt$. If $\tau \to +\infty$ we can obtain the limit total risk score

$$R_{tot} = \lim_{\tau\to+\infty} \int_0^\tau R(t)dt = \int_0^{+\infty} R(t)dt.$$

It is easy to show that for calculation of the total risk score R_{tot} there can be applied the Laplace transformation $R^*(s) = \mathcal{L}[R(t); s]$. If we calculate the limit, $\lim_{s\to 0} R^*(s)$ then we yield:

$$R_{\mathrm{tot}} = \boldsymbol{T_s} \cdot \boldsymbol{A}^T$$

where the vector $\boldsymbol{T_s} = [T_0, T_1, \ldots, T_8]$ is given in Table II.

Of course the proposed model allows us to determine the magnitude of the risk of losses at each stage of an cyber-attack triggered by an vulnerability during its life cycle. The risk of the cyber-attack stage k $(k = 4, \ldots, 8)$ at time $t \geq 0$ can be expressed as follows:

$$R_k(t) = A_k \cdot P_k(t)$$

The sum of the risk score $R_k(t)$ in a period $[0, \tau]$ can be calculated as the integral $\int_0^\tau R_k(t)dt$. For $\tau \to +\infty$ we can obtain the limit overall risk score at the stage k of the cyber-attack cycle $R_{k,tot}$ $(k = 4, \ldots, 8)$ as follows:

$$R_{k,tot} = \lim_{\tau\to+\infty} \int_0^\tau R_k(t)dt = \int_0^{+\infty} R_k(t)dt = A_k \cdot T_k$$

In order to calculate risks at each stage of the cyber-attack cycle the stochastic model has to be parameterized. To estimate the stationary probabilities, it is necessary and enough to know the expected values $1/\lambda_{kj}$. The most popular and straightforward solution is:

- to ask experts in cyber security domain to assess the values $1/\lambda_{kj}$ and to base on their opinion, or
- to analyze existed empirical data, or
- a combination of both.

The process of assessing the expected values is crucial, but it is not the primary focus of this article.

VI. Numerical Examples: Probabilities and Risk Score

A. Example 1

In order to illustrate the solution in Table I, simply suppose that the transition rates are $\lambda_{kj} = \lambda$ for $j,k = 0,1,\dots,8$ and $j \neq k$. Bases on this assumption, Table III contains the solution of (4) and Table IV contains probability distribution $\boldsymbol{P}(t) = [P_0(t), P_1(t), \dots, P_8(t)]$ obtained by performing the inverse Laplace transformation $\boldsymbol{P}(t) = \mathcal{L}^{-1}[\boldsymbol{P}^*(s); t]$ of the functions from Table III.

Table III
Solution of Kolmogorov equations (2) when $\lambda_{kj} = \lambda$

$\boldsymbol{P}^*$(s)	if $\boldsymbol{P}(0^+)$=[0,1,0,0,0,0,0,0,0]
$P_0^*(s)$	0
$P_1^*(s)$	$\frac{1}{s+3\lambda}$
$P_2^*(s)$	$\frac{\lambda}{s^2+5s\lambda+6\lambda^2}$
$P_3^*(s)$	$\frac{\lambda(s^5+12s^4\lambda+54s^3\lambda^2+116s^2\lambda^3+126s\lambda^4+58\lambda^5)}{s(s^6+14s^5\lambda+77s^4\lambda^2+212s^3\lambda^3+307s^2\lambda^4+219s\lambda^5+58\lambda^6)}$
$P_4^*(s)$	$\frac{\lambda(s^4+11s^3\lambda+42s^2\lambda^2+65s\lambda^3+35\lambda^4)}{s^6+14s^5\lambda+77s^4\lambda^2+212s^3\lambda^3+307s^2\lambda^4+219s\lambda^5+58\lambda^6}$
$P_5^*(s)$	$\frac{\lambda^2(s^3+9s^2\lambda+25s\lambda^2+20\lambda^3)}{s^6+14s^5\lambda+77s^4\lambda^2+212s^3\lambda^3+307s^2\lambda^4+219s\lambda^5+58\lambda^6}$
$P_6^*(s)$	$\frac{\lambda^3(s^2+5s\lambda+5\lambda^2)}{s^6+14s^5\lambda+77s^4\lambda^2+212s^3\lambda^3+307s^2\lambda^4+219s\lambda^5+58\lambda^6}$
$P_7^*(s)$	$\frac{\lambda^4(s+3\lambda)}{s^6+14s^5\lambda+77s^4\lambda^2+212s^3\lambda^3+307s^2\lambda^4+219s\lambda^5+58\lambda^6}$
$P_8^*(s)$	$\frac{\lambda^5}{s^6+14s^5\lambda+77s^4\lambda^2+212s^3\lambda^3+307s^2\lambda^4+219s\lambda^5+58\lambda^6}$

Bases on results from Table II or Table III the vector $\boldsymbol{T_s} = [T_0, T_1, \dots, T_8]$ is as follows:

$$\boldsymbol{T_s} = \left[0, \frac{1}{3\lambda}, \frac{1}{6\lambda}, \infty, \frac{35}{58\lambda}, \frac{10}{29\lambda}, \frac{5}{58\lambda}, \frac{3}{58\lambda}, \frac{1}{58\lambda}\right]$$

The vector of the risks scores $R_{k,tot}$, $k = 4,\dots,8$ is as follows:

$$\left[R_{4,tot}, \dots., R_{8,tot}\right] = \left[\frac{35\cdot \mathrm{A}_4}{58\lambda}, \frac{10\cdot \mathrm{A}_5}{29\lambda}, \frac{5\cdot \mathrm{A}_6}{58\lambda}, \frac{3\cdot \mathrm{A}_7}{58\lambda}, \frac{\mathrm{A}_8}{58\lambda}\right]$$

Table IV
Probability distribution $P(t)$ for $\lambda_{kj} = \lambda$

$\boldsymbol{P}$(t)	if $\boldsymbol{P}(0^+)$=[0,1,0,0,0,0,0,0,0]
$P_0(t)$	0
$P_1(t)$	$e^{-3\lambda t}$
$P_2(t)$	$e^{-2\lambda t} - e^{-3\lambda t}$
$P_3(t)$	$\lambda t - \lambda^2 t^2 + \frac{5\lambda^3 t^3}{6} - \frac{\lambda^4 t^4}{2} + \frac{13\lambda^5 t^5}{60} - \frac{47\lambda^6 t^6}{720} + \frac{\lambda^7 t^7}{112} + O(t^8)$
$P_4(t)$	$\lambda t - \frac{3\lambda^2 t^2}{2} + \frac{7\lambda^3 t^3}{6} - \frac{7\lambda^4 t^4}{12} + \frac{7\lambda^5 t^5}{40} + \frac{\lambda^6 t^6}{360} - \frac{227\lambda^7 t^7}{5040} + O(t^8)$
$P_5(t)$	$\frac{\lambda^2 t^2}{2} - \frac{5\lambda^3 t^3}{6} + \frac{3\lambda^4 t^4}{4} - \frac{59\lambda^5 t^5}{120} + \frac{193\lambda^6 t^6}{720} - \frac{659\lambda^7 t^7}{5040} + O(t^8)$
$P_6(t)$	$\frac{\lambda^3 t^3}{6} - \frac{3\lambda^4 t^4}{8} + \frac{9\lambda^5 t^5}{20} - \frac{55\lambda^6 t^6}{144} + \frac{431\lambda^7 t^7}{1680} - \frac{833\lambda^8 t^8}{5760} + O(t^9)$
$P_7(t)$	$\frac{\lambda^4 t^4}{24} - \frac{11\lambda^5 t^5}{120} + \frac{77\lambda^6 t^6}{720} - \frac{443\lambda^7 t^7}{5040} + \frac{383\lambda^8 t^8}{6720} + O(t^9)$
$P_8(t)$	$\frac{\lambda^5 t^5}{120} - \frac{7\lambda^6 t^6}{360} + \frac{17\lambda^7 t^7}{720} - \frac{5\lambda^8 t^8}{252} + O(t^9)$

Thus the total risk score R_{tot} is as follows:

$$R_{tot} = \frac{35\cdot \mathrm{A}_4}{58\lambda} + \frac{10\cdot \mathrm{A}_5}{29\lambda} + \frac{5\cdot \mathrm{A}_6}{58\lambda} + \frac{3\cdot \mathrm{A}_7}{58\lambda} + \frac{\mathrm{A}_8}{58\lambda}$$

In order to calculate the risk scores $R(t)$ and $R_k(t)$ at time $t \geq 0$ the vector of probabilities $\boldsymbol{P}(t), t \geq 0$, should be calculated. The probabilities $\boldsymbol{P}(t)$ are obtained by performing an inverse Laplace transformation $\boldsymbol{P}(t) = \mathcal{L}^{-1}[\boldsymbol{P}^*(s); t]$. All probabilities $P_k(t), k = 0,1,\dots,8$ are presented in Table IV.

B. Example 2

In this example let us consider the cyber-attack with no internal iterations (see Fig. 2). In order to illustrate the solution (Table I) simply suppose that the transition rates are: $\lambda_{01} = \lambda$, $\lambda_{12} = 2\lambda$, $\lambda_{13} = \lambda$, $\lambda_{23} = 2\lambda$, $\lambda_{14} = \lambda$, $\lambda_{24} = 6\lambda$, $\lambda_{53} = \lambda_{63} = \lambda_{73} = \lambda_{83} = \lambda$, $\lambda_{45} = 2\lambda$, $\lambda_{56} = 4\lambda$, $\lambda_{67} = 8\lambda$, $\lambda_{78} = 10\lambda$ and $\lambda_{64} = \lambda_{65} = \lambda_{84} = \lambda_{87} = 0$.

Fig. 2. illustrates the model when the returning transitions between stages $S_8 \rightarrow S_7, S_4$ and $S_6 \rightarrow S_5, S_4$ are equal to zero, i.e. $\lambda_{64} = \lambda_{65} = \lambda_{84} = \lambda_{87} = 0$.

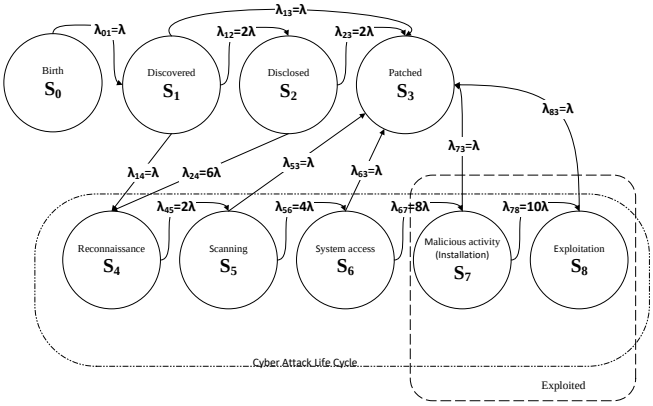

Fig. 2. Markov graph for the life cycle for example 2

Table V contains the solution of (4) that is the vector of $\boldsymbol{P}^*(s) = \mathcal{L}[\boldsymbol{P}(t); s]$ the Laplace transformation of the probability distribution $\boldsymbol{P}(t) = [P_0(t), P_1(t), \dots, P_8(t)]$ (see Table VI)

Bases on results from Table V (or Table II) the vector $\boldsymbol{T_s} = [T_0, T_1, \dots, T_8]$ is as follows:

$$\boldsymbol{T_s} = \left[0, \frac{1}{4\lambda}, \frac{1}{16\lambda}, \infty, \frac{5}{16\lambda}, \frac{1}{8\lambda}, \frac{1}{18\lambda}, \frac{4}{99\lambda}, \frac{40}{99\lambda}\right]$$

The vector of the risks scores $R_{k,tot}$, $k = 4,\dots,8$ is as follows:

$$\left[R_{4,tot}, \dots., R_{8,tot}\right] = \left[\frac{5\cdot \mathrm{A}_4}{16\lambda}, \frac{\mathrm{A}_5}{8\lambda}, \frac{\mathrm{A}_6}{18\lambda}, \frac{4\cdot \mathrm{A}_7}{99\lambda}, \frac{40\cdot \mathrm{A}_8}{99\lambda}\right]$$

The total risk score R_{tot} is as follows:

$$R_{tot} = \frac{5 \cdot A_4}{16\lambda} + \frac{A_5}{8\lambda} + \frac{A_6}{18\lambda} + \frac{4 \cdot A_7}{99\lambda} + \frac{40 \cdot A_8}{99\lambda}$$

In order to calculate the risk scores $R(t)$ and $R_k(t)$ at time $t \geq 0$ the vector of probabilities $\boldsymbol{P}(t), t \geq 0$ should be calculated. The probabilities $\boldsymbol{P}(t)$ are obtained by performing an inverse Laplace transformation $\boldsymbol{P}(t) = \mathcal{L}^{-1}[\boldsymbol{P}^*(s); t]$. Probabilities $P_k(t), k = 0,1, \ldots, 8$ are presented in Table VI.

TABLE V
SOLUTION OF KOLMOGOROV EQUATIONS (2) WHEN $\lambda_{01} = \lambda, \lambda_{64} = \lambda_{65} = \lambda_{84} = \lambda_{87} = 0$ AND OTHERS $\lambda_{kj} \geq \lambda$

$\boldsymbol{P}^*(s)$	if $\boldsymbol{P}(0^+)$=[0,1,0,0,0,0,0,0,0]
$P_0^*(s)$	0
$P_1^*(s)$	$\frac{1}{s+4\lambda}$
$P_2^*(s)$	$\frac{2\lambda}{s^2+12s\lambda+32\lambda^2}$
$P_3^*(s)$	$\frac{\lambda(s^3+15s^2\lambda+40s\lambda^2+64\lambda^3)}{s(s^4+15s^3\lambda+70s^2\lambda^2+120s\lambda^3+64\lambda^4)}$
$P_4^*(s)$	$\frac{\lambda(s+20\lambda)}{s^3+14s^2\lambda+56s\lambda^2+64\lambda^3}$
$P_5^*(s)$	$\frac{2\lambda^2(s+20\lambda)}{s^4+19s^3\lambda+126s^2\lambda^2+344s\lambda^3+320\lambda^4}$
$P_6^*(s)$	$\frac{8\lambda^3(s+20\lambda)}{s^5+28s^4\lambda+297s^3\lambda^2+1478s^2\lambda^3+3416s\lambda^4+2880\lambda}$
$P_7^*(s)$	$\frac{64\lambda^4(s+20\lambda)}{s^6+39s^5\lambda+605s^4\lambda^2+4745s^3\lambda^3+19674s^2\lambda^4+40456s\lambda^5+31680\lambda^6}$
$P_8^*(s)$	$(((640\lambda^5(s+20\lambda))) / ((s^7+40s^6\lambda+644s^5\lambda^2+5350s^4\lambda^3+24419s^3\lambda^4+60130s^2\lambda^5+72136s\lambda^6+31680\lambda^7)))$

TABLE VI
PROBABILITY DISTRIBUTION $P(t)$ FOR $\lambda_{01} = \lambda, \lambda_{64} = \lambda_{65} = \lambda_{84} = \lambda_{87} = 0$ AND OTHERS $\lambda_{kj} \geq \lambda$

$\boldsymbol{P}$(t)	if $\boldsymbol{P}(0^+)$=[0,1,0,0,0,0,0,0,0]
$P_0(t)$	0
$P_1(t)$	$e^{-4\lambda t}$
$P_2(t)$	$\frac{1}{2}e^{-8\lambda t}(e^{4\lambda t}-1)$
$P_3(t)$	$\frac{1}{7}e^{-8\lambda t}-\frac{5}{6}e^{-4\lambda t}+\frac{3}{2}e^{-2\lambda t}-\frac{38e^{\lambda(-t)}}{21}+1$
$P_4(t)$	$\frac{1}{2}e^{-8\lambda t}(-4e^{4\lambda t}+3e^{6\lambda t}+1)$
$P_5(t)$	$-\frac{1}{3}e^{-8\lambda t}+\frac{10}{3}e^{-5\lambda t}-4e^{-4\lambda t}+e^{-2\lambda t}$
$P_6(t)$	$\frac{22}{35}e^{-9\lambda t}-\frac{4}{3}e^{-8\lambda t}+\frac{10}{3}e^{-5\lambda t}-\frac{16}{5}e^{-4\lambda t}+\frac{4}{7}e^{-2\lambda t}$
$P_7(t)$	$\frac{8}{315}e^{-11\lambda t}(e^{\lambda t}-1)^4(-40e^{\lambda t}-e^{2\lambda t}+56e^{3\lambda t}+80e^{4\lambda t}+20e^{5\lambda t}-10)$
$P_8(t)$	$\frac{2}{63}e^{-11\lambda t}(e^{\lambda t}-1)^5(-40e^{\lambda t}-21e^{2\lambda t}+55e^{3\lambda t}+125e^{4\lambda t}+57e^{5\lambda t}-8)$

The probabilities from Table VI are drawn in Fig. 3 – 5 for sample $\lambda = 1/100$.

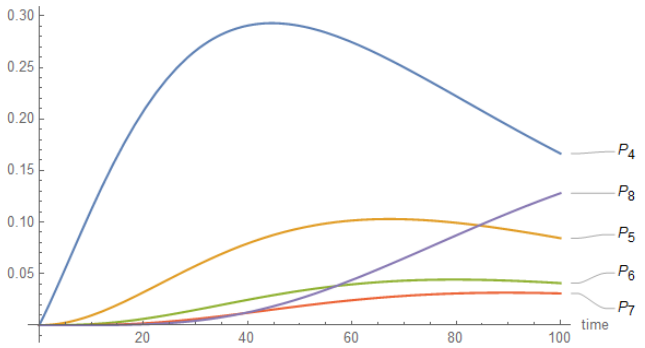

Fig. 3. Example 2. The probabilities $P_k(t)$, $k = 4, \ldots, 8$; $\lambda = 1/100$

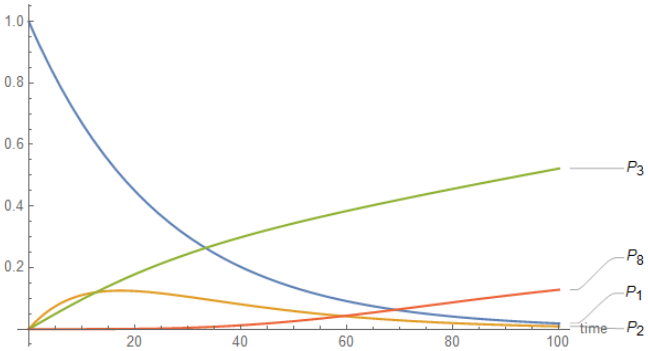

Fig. 4. Example 2. The probabilities $P_k(t)$, $k = 1,2,3,8$; $\lambda = 1/100$

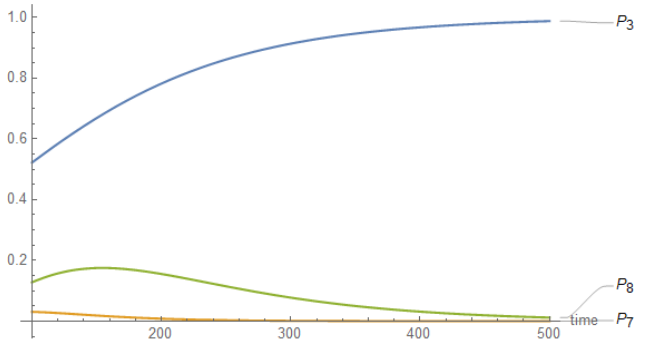

Fig. 5. Example 2. The probabilities $P_k(t)$, $k = 3,7,8$; $\lambda = 1/100$

CONCLUSION

In current literature there can be observed research results of software vulnerability life cycles in which a cyber-attack is reduced to one stage, i.e. a vulnerability was exploited. In fact, exploitation of an vulnerability is a symptomatic result of a running or pending cyber-attack that is not an time short event but is a process. This work addresses this deficiency by proposing the stochastic model of the "specific joint" life cycle of cyber-attack and software vulnerability. The model is distinguished from these published in the literature in principle by combining two approaches which have been researched separately so far. The presented research result in this paper should be treated as an illustration of the proposed approach of considering in one model two correlated phenomena referring to vulnerable software.

It is well known that nowadays cybercrime is a serious problem faced by many organizations both commercial and public (e.g. [20,22]). Since cyber burgles operate by day and night [23] cyber-defenders are obligated to provide firms' management with cyber risk assessment reports. It should be realized that today the cyber risk assessment should be a fundamental element of the risk management system in organizations since during the cyber risk assessment process we obtain the information indispensable to make right decisions concerning the strategy of handling the risk, efficient choice of the risk reduction measures, assessment of the transfer validity, acceptance or avoidance of the risk. In the author's opinion, the cyber risk assessment as a continuous-time process should be built into real-time cyber defense systems in any organization. Stochastic models like this proposed in this paper may be an important part of cyber defense systems. Such models can be also used for building situational awareness of cyber security in organizations.

REFERENCES

[1] K. G. J. Coleman, "Aggression in Cyberspace," in *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, S. Jasper, Ed. Washington, DC: Georgetown University Press, 2012, pp. 105-119.

[2] E. M. Hutchins, M. J. Cloppert, and R.M. Amin: "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in *Leading Issues in Information Warfare and Security Research, vol. 1*, J. Ryan, Ed. Reading, UK: Academic Publishing International Ltd, 2011, pp.78-104.

[3] M. S. Khan, S. Siddiqui, and K. Ferens, "A Cognitive and Concurrent Cyber Kill Chain Model," in *Computer and Network Security Essentials*, K. Daimi, Ed. Cham, Switzerland: Springer, 2018, pp. 585-602.

[4] J. M. Spring, E. Hatleback, "Thinking about intrusion kill chains as mechanisms," *Journal of Cybersecurity*, vol. 3 (3), pp. 185-197, Nov. 2017. DOI: 10.1093/cybsec/tyw012

[5] A. Hahn, R.K. Thomas, I. Lozano, and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 11, pp. 39-50, Dec. 2015.

[6] R. Hoffmann, "The general cyber-attack life cycle and its continuous-time Markov chain model," *Ekonomiczne Problemy Usług*, vol. 2/2018 (131), t.1, pp. 121-130, 2018. DOI: 10.18276/epu.2018.131/1-12

[7] R. Hoffmann, "Markov Models of Cyber Kill Chains with Iterations," in *2019 International Conference on Military Communications and Information Systems (ICMCIS)*, Budva, Montenegro, IEEE, 2019. DOI: 10.1109/ICMCIS.2019.8842810

[8] R. Hoffmann, „The Markov models of cyber-attack life cycles," *Roczniki Kolegium Analiz Ekonomicznych SGH*, vol. 54, pp. 303–317, 2019.

[9] W. A. Arbaugh, W. L. Fithen and J. McHugh, "Windows of vulnerability: a case study analysis," *Computer*, vol. 33, no. 12, pp. 52-59, Dec. 2000.

[10] E. Rescorla, "Is finding security holes a good idea?," in IEEE Security & Privacy, vol. 3, no. 1, pp. 14-19, Jan.-Feb. 2005.

[11] S. Frei, "Security econometrics – the dynamics of (in)security. Dissertation 18197," Zurich: ETH Zurich 2009.

[12] S. Frei, D. Schatzmann, B. Plattner and B. Trammell, "Modeling the Security Ecosystem - The Dynamics of (In)Security," in *Economics of Information Security and Privacy*, T. Moore, D. Pym, C. Ioannidis, Ed. Boston: Springer 2010, pp.79-106.

[13] H. Joh, Y.K. Malaiya, "A Framework for Software Security Risk Evaluation using the Vulnerability Lifecycle and CVSS Metrics," in: *Proceedings of the 2010 International Workshop on Risk and Trust in Extended Enterprises (RTEE'2010)*, USA, San Jose 2010, pp. 430–434.

[14] H. Joh, Y.K. Malaiya, "Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics," in *Proceedings of the 2011 International Conference on Security and Management (SAM'11)*, vol. 1, USA, Las Vegas 2011, pp.10–16.

[15] H. Okamura, M. Tokuzane and T. Dohi, "Security Evaluation for Software System with Vulnerability Life Cycle and User Profiles," in *Proceedings of 2012 Workshop on Dependable Transportation Systems/Recent Advances in Software Dependability (WDTS-RASD 2012)*, Japan, Niigata 2012, pp. 39–44.

[16] S.M. Rajasooriya, Ch.P. Tsokos and P.K. Kaluarachchi, "Stochastic Modelling of Vulnerability Life Cycle and Security Risk Evaluation," *Journal of Information Security*, vol. 7 (4), pp. 269–279, July 2016.

[17] T. Nakagawa, "Stochastic Processes with Applications to Reliability Theory," Springer, London 2011.

[18] W. Keller, M. Modarres, "A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: A tribute to the late Professor Norman Carl Rasmussen," *Reliability Engineering & System Safety*, vol. 89 (3), pp. 271–285, Sep. 2005.

[19] S. Kaplan, B. J. Garrick, "On the quantitative definition of risk," *Risk Analysis*, vol. 1(1), pp. 11–27, Mar. 1981.

[20] ENISA, "ENISA Threat Landscape Report 2018," Jan. 2019 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (2019), last accessed 2019/11/02.

[21] McAfee, "McAfee Labs Threats Report. August 2019," https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf, last accessed 2019/11/01.

[22] https://www.fireeye.com/cyber-map/threat-map.html, last accessed 2020/03/02.

[23] https://threatmap.checkpoint.com, last accessed 2020/03/02.