Probabilistic modeling and analysis of sequential cyber-attacks

Qisi Liu | Liudong Xing | Chencheng Zhou

Department of Electrical and Computer Engineering, University of Massachusetts, Dartmouth, Massachusetts

Correspondence
Liudong Xing, Department of Electrical and Computer Engineering, University of Massachusetts, Dartmouth, MA 02747. Email: lxing@umassd.edu

Security is one of the major challenges for promoting the computer industry. Existing models for assessing security have mostly assumed that different hazards causing the security breach are independent of each other. Dependencies however can exist among different hazardous actions and they may affect the system security attribute greatly. This paper advances the state of the art in quantitative security risk assessment by modeling one such dependency, where multiple sequence-dependent hazardous actions are performed to launch a successful security cyber-attack. Continuous-time Markov chain and semi-Markov process–based methods are proposed to estimate the occurrence probability of a security risk for systems undergoing the sequential cyber-attacks. While the CTMC method is limited to the exponential state transition time, the proposed semi-Markov process–based approach is applicable to analyzing attacks with any arbitrary types of transition time distributions. Both methods are illustrated using case studies where Trojan attacks in the banking application are modeled and analyzed.

KEYWORDS
attack tree, continuous-time Markov chain (CTMC), quantitative assessment, security risk, semi-Markov process (SMP), sequential dependence, Trojan attack

1 | INTRODUCTION

Diverse types of cyber-attacks have caused increasing security threats to contemporary computing and networking systems.¹ These threats pose huge potential security risks to individuals, societies, and enterprises.²,³ For instance, massive hack attacks to Sony pictures caused the theft and online exposure of about 40 gigabytes of sensitive data (including pertinent scripts of unreleased films, private information of Sony employees, etc).⁴ For another instance, as one of the largest security breaches in the computer network history, one billion Yahoo email accounts were breached from attacks utilizing fake Internet cookies.⁵ Therefore, it is crucial to assess security risks in a quantitative manner, providing effective guidance on secure design and operation of critical systems and networks.

In general, the risk is referred to as the potential for damage, loss, or destruction of an asset due to some threat exploiting system vulnerabilities.⁶ Vulnerabilities associated with computer-based systems are the main threats to the network security.⁷,⁸ With a proper quantitative analysis of the security, the system survivability may be effectively enhanced, thereby promoting the response to unexpected security attacks to complex networks and systems.

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2019 The Authors. Engineering Reports published by John Wiley & Sons Ltd.
The soaring development of information technology in the last few decades has produced over 200 risk assessment methods. These risk assessment methods can be categorized into three types: qualitative assessment, quantitative assessment, and hybrid (semiquantitative) assessment methods. Different methods not only have different aims, advantages, and weaknesses but also differ in the severity level, complexity to use, and applicability to different-sized organization models.

Qualitative assessment methods involve identifying, characterizing, and ranking unwanted events primarily based on the assessor's experience, knowledge, strategies, and exceptional cases on information systems. A qualitative assessment requires specific expectations rather than exact data. It can make more general and sound conclusions compared to other assessment tools. However, the qualitative assessment usually takes more time (not suitable for dynamic risk assessments that require efficient assessment and decision) and is harder to make an objective assessment. According to studies of Shameli-Sendi et al. and Bolczak et al., the typical qualitative assessment methods include the factor analysis, game theory, fuzzy set theory, historical comparison, and Delphi method.

Quantitative assessment approaches use mathematical calculations, probability theory, and statistics to analyze the level of the risk of an organization and produce number indicators. They typically use monetary values, probabilities, or percentages to present assessment results in a scientific and formal manner. More specifically, a quantitative assessment approach involves evaluating the risk probability and hazardous level characterized by the expected losses of assets and potential impacts to the organization. For example, as the traditional risk assessment method, the information technology-security risk assessment is based on the likelihood of occurrence of a hazardous event and potential consequence caused by the event. Contemporary approaches often focus on requirements of confidentiality, integrity, and availability (CIA) and are mostly model or system-based. The typical quantitative assessment methods include the Markov analysis, statistical parameter analysis, Bayesian network models, and clustering methods. Quantitative methods aim to estimate the loss of assets, vulnerabilities of organization systems, frequency of threats, and cost of the risk. The disadvantages of the quantitative methods include the detailed data needed for assessments could be costly, and the calculation could be time-consuming.

A typical example of quantitative risk assessment methods is CORAS (a model-based approach for conducting security risk analysis). This model is mainly based on the multiplication operation without any formal support. The risk assessment methodology in CORAS integrates classic analysis methods such as the failure mode and effect analysis. Markov analysis, fault tree analysis, and HAZOP analysis. The method can deal with all types of potential threats with different CIA properties and accountability.

In summary, most research on risk assessment are qualitative analysis with subjectivity that limits the model to only specific systems. On the other hand, quantitative risk assessment methods are typically based on certain risk assessment standards. Accuracy of these standard-based methods, however, is dependent on numerous historical data with long investment cycles. In addition, the existing quantitative risk assessment methods mostly focused on the amount or frequency of different and independent system vulnerabilities or hazardous events. In practice, however, different hazardous events may take place in a dependent manner, i.e., the occurrence of one hazardous event impacts the occurrence of another hazardous event happening to the same system. Dependencies or interactions between different attack events or outcomes have received considerable research attentions from the cybersecurity community in the past several years (see, e.g., other works). Cyber-attacks have become a major threat to many modern systems and networks. For example, industrial control systems have been targeted by cyber-attacks based on vulnerabilities in these systems and their environments or based on the equipment degradation. It is a challenging task to address dependence in cybersecurity models.

In this work, we focus on security risks from cyber-attacks subject to sequence dependence, where the occurrence order of hazardous events matters to the system status. Specifically, we address the problem of modeling and assessing the occurrence probability of a security risk from cyber-attacks launched though multiple sequence-dependent hazardous actions. The sequential attack behavior is modeled using an attack tree. The probability of a successful attack (i.e., the occurrence probability of security risk) is evaluated using Markov-based methods. Specifically, a continuous-time Markov chain (CTMC) is applied to determine the time-dependent solution and a semi-Markov process (SMP) is utilized to find the steady-state solution for systems undergoing the sequential cyber-attack. Trojan attacks launched to a bank application are modeled and analyzed to demonstrate the type of attacks considered in this work and the proposed approaches. Effects of different attack model parameters on the system security are also demonstrated through examples.

Note that there exists research on sequential attacks in literature. However, the existing models are mostly limited to physical sequential attacks in areas such as physics, military, and smart grids. Despite the growing literature on addressing dependencies in cyber-attacks (as briefed above), little work has focused on the sequence dependence. In
particular, a security threat with a sequence of small attacks on applications of reinforcement learning in deep neural networks was investigated using simulations in the OpenAI Gym.\textsuperscript{50} To the best of the authors’ knowledge, the work presented in this paper is the first that models and evaluates security risks from sequential cyber-attacks using the analytical modeling methods (CTMC and SMP).

The remainder of this paper is arranged as follows. Section 2 describes the sequential threat model considered in this work, and the attack tree modeling. Section 3 focuses on the CTMC-based time-dependent solution. Section 4 focuses on the SMP-based steady-state solution. Section 5 concludes this work and points out directions of future research.

2 | THREAT MODEL AND ATTACK TREE

This work focuses on one type of security risks from Trojan attacks that were designed to commit bank fraud crimes (stealing identity of bank customers and further their money through mobile devices like smartphones).\textsuperscript{51,52} As illustrated in Figure 1, a hacker sends a message to a mobile banking user, which contains link information with Trojan virus. If the user does not open the link, the malware stays in the mobile device without causing any harm. However, if the user clicks the link, the Trojan virus is triggered to be downloaded and installed on the device. At this time, the device is in an infection state. During the infected state, the Trojan malware is able to simulate the victim's online-banking operations and transmit data to the hacker.

Figure 2 presents an attack tree model, which describes the cause of a successful banking Trojan attack (denoted by the top event of the tree) and dependent relationship among basic events A (Trojan virus link received), B (virus installed and infected), and C (online-banking activity). The gates connecting the basic events in Figure 2 are priority-AND (PAND) gates from the dynamic fault tree analysis.\textsuperscript{53} Each PAND gate is logically equivalent to a logic AND gate with extra condition that the left input event must take place before the right input event to fire the gate. The two cascading PAND gates in Figure 2 model a successful Trojan attack (ie, the top event occurring), which is caused by A happening before B, which happens before C. In other words, any violation to this occurrence sequence of events A, B, and C fails the attack.

Based on the attack tree model in Figure 2, the Markov-based methods are developed in Sections 3 and 4 to quantify the occurrence probability of a security risk in systems subject to the sequential cyber-attack. In general, the Markov models are constructed based on system states, and transitions between the states (caused by the occurrence of a particular event).\textsuperscript{53} For systems undergoing the sequential Trojan attack, four states are defined, ie, 0 (clean), 1 (acquisition), 2 (infection), and 3 (fraud complete). Two scenarios of transitions are considered, ie, no recovery transition is possible from the fraud complete state (Section 3) and a recovery is possible from the fraud complete state (Section 4).
This section presents the CTMC-based time-dependent solution to address the sequential cyber-attack. Effects of different model parameters on the attack success probability are also examined.

### 3.1 Continuous-time Markov chain–based solution

Figure 3 illustrates the state transition diagram in the CTMC-based solution. In the initial clean state 0, the security attribute of the system (e.g., confidentiality) can be guaranteed. Because of event A (e.g., the user receiving the virus link), the system transits to the acquisition state 1, where the maliciousness exists but the system still functions. The system can go back to the clean state 0 from the acquisition state 1 with performing the deletion of suspicious, hazardous files. However, if the user clicks the malicious link (i.e., event B takes place), the Trojan virus is triggered and the system transits from the acquisition state 1 to the infection state 2. In state 2, once the user conducts any online banking operations, e.g., making online payment (i.e., event C takes place), the hacker could steal personal banking information and accomplish the banking fraud. That is, due to the occurrence of event C, the system transits to the final fraud complete state 3. In the infection state 2, the system can also be restored to the acquisition state 1 if the user takes some timely and appropriate quarantine action, or even be restored to the clean state 0 through virus clean-up operations. All the transitions are characterized by certain rates. The transition rates $\lambda_A$, $\lambda_B$, and $\lambda_C$ are, respectively, occurrence rates of events A, B, and C. The transition rates $\mu_d$, $\mu_q$, $\mu_c$, respectively, denote deletion, quarantine, and clean-up rates.

Based on the state transition diagram in Figure 3, the state equations in the matrix form is given in (1), where the left-most matrix is the transition rate matrix of the CTMC, $P_j(t)$ represents the probability of the system being in state $j$ ($j = 0, 1, 2, 3$), and $\dot{P}_j(t)$ represents the derivative of the state $j$ probability. Equation (1) can also be detailed using differential equations (2) to (5)

$$
\begin{bmatrix}
-\lambda_A & \mu_d & \mu_c & 0 \\
\lambda_A - (\mu_d + \lambda_B) & -\mu_d & \mu_q & 0 \\
0 & \lambda_B - (\mu_c + \mu_q + \lambda_C) & -\mu_q & 0 \\
0 & 0 & \lambda_C & -\mu_c
\end{bmatrix}
\begin{bmatrix}
P_0(t) \\
P_1(t) \\
P_2(t) \\
P_3(t)
\end{bmatrix}
=
\begin{bmatrix}
\dot{P}_0(t) \\
\dot{P}_1(t) \\
\dot{P}_2(t) \\
\dot{P}_3(t)
\end{bmatrix} \tag{1}
$$

$$
\dot{P}_0(t) = -\lambda_A P_0(t) + \mu_d P_1(t) + \mu_c P_2(t) \tag{2}
$$

$$
\dot{P}_1(t) = \lambda_A P_0(t) - (\mu_d + \lambda_B) P_1(t) + \mu_q P_2(t) \tag{3}
$$

$$
\dot{P}_2(t) = \lambda_B P_1(t) - (\mu_c + \mu_q + \lambda_C) P_2(t) \tag{4}
$$

$$
\dot{P}_3(t) = \lambda_C P_2(t) \tag{5}
$$

Applying the Laplace transform-based method to solve (2)-(5) (using the initial state probability $P_0(0) = 1$), the Laplace transform of those state probabilities is obtained as $P^*_j(s) = \frac{\lambda_A(1+s)}{(1+s)(1+\mu_d+\mu_q+\lambda_B)}$ where $a = \mu_c + \mu_q + \lambda_C$; $P^*_0(s) = \frac{P^*_3(s) \lambda_c}{s + \mu_c + \mu_q + \lambda_C}$; $P^*_3(s) = \frac{P^*_3(s) \lambda_c}{s + \mu_c + \mu_q + \lambda_C}$; $P^*_0(s) = \frac{1}{s} - P^*_1(s) - P^*_2(s) - P^*_3(s)$. Applying the inverse Laplace transform of $P^*_j(s)$, the system state probabilities in the time domain $P_j(t)$ ($j = 0, 1, 2, 3$) can be derived, which is carried out by MATLAB in this work.

### 3.2 Analysis results

Table 1 lists five sets of parameters designed based on statistics and data from. The CTMC in Figure 3 is analyzed using these parameter sets to study effects of different model parameters on the attack success probability. Particularly,
Effects of user parameter $\lambda$

The occurrence rate of the malicious event dominates (other two cases due to the largest transition rate $\lambda_c$ (a cautious user), while this probability under set $c$ is the worst and declines more quickly with time as compared to the other two cases due to the largest transition rate $\lambda_B$ used (a careless user).

As observed from Figure 5, the acquisition state probability under the three parameter sets $P_{1-a}$, $P_{1-b}$, and $P_{1-c}$ ascends quickly at the beginning due to the occurrence of event $A$, reaching a peak value, and then falling gradually due to interactions of effects from the attack and recovery events. Again, the acquisition state probability under set $a$ is the best among the three cases. In particular, $P_{1-a}$ stays the highest all the time with the zenith 0.2156 at 2 k hours; $P_{1-c}$ keeps the lowest over the considered mission time reaching its bottom around 0 after $t = 12$ k hours.

As observed from Figure 6, the infection state probability reaches a peak quickly at the beginning and then declines gradually with a different pace under each different parameter set. The infection state probability under set $c$ declines

### Table 1: Model parameters (per hour)

| Parameter | Set a | Set b | Set c | Set d | Set e |
|-----------|-------|-------|-------|-------|-------|
| $\mu_d$  | 0.1   | 0.1   | 0.1   | 0.482 | 0.0125 |
| $\mu_q$  | 0.2   | 0.2   | 0.2   | 0.527 | 0.098 |
| $\mu_c$  | 0.15  | 0.15  | 0.15  | 0.39  | 0.0067 |
| $\lambda_A$ | 0.034 | 0.034 | 0.034 | 0.034 | 0.034 |
| $\lambda_B$ | 0.024 | 0.106 | 0.47  | 0.106 | 0.106 |
| $\lambda_C$ | 0.0023 | 0.0023 | 0.0023 | 0.0023 | 0.0023 |

### Table 2: System state probabilities under set a

| State | t (hrs) | 2k | 4k | 8k | 16k | 20k |
|-------|---------|----|----|----|-----|-----|
| $P_{0-a}$ | 0.699890 | 0.650841 | 0.562814 | 0.420866 | 0.363943 |
| $P_{1-a}$ | 0.215668 | 0.200554 | 0.173428 | 0.129688 | 0.112147 |
| $P_{2-a}$ | 0.014694 | 0.013664 | 0.011816 | 0.008836 | 0.007641 |
| $P_{3-a}$ | 0.069748 | 0.134941 | 0.251942 | 0.440610 | 0.516269 |

### Table 3: System state probabilities under set b

| State | t (hrs) | 2k | 4k | 8k | 16k | 20k |
|-------|---------|----|----|----|-----|-----|
| $P_{0-b}$ | 0.599336 | 0.467757 | 0.284918 | 0.105711 | 0.064390 |
| $P_{1-b}$ | 0.139879 | 0.109170 | 0.066497 | 0.024672 | 0.015028 |
| $P_{2-b}$ | 0.042102 | 0.032859 | 0.020015 | 0.007426 | 0.004523 |
| $P_{3-b}$ | 0.218684 | 0.390215 | 0.628570 | 0.862191 | 0.916058 |

### Table 4: System state probabilities under set c

| State | t (hrs) | 2k | 4k | 8k | 16k | 20k |
|-------|---------|----|----|----|-----|-----|
| $P_{0-c}$ | 0.459564 | 0.266076 | 0.089192 | 0.010022 | 0.003360 |
| $P_{1-c}$ | 0.051619 | 0.029886 | 0.001008 | 0.001126 | 0.000377 |
| $P_{2-c}$ | 0.068918 | 0.039902 | 0.013376 | 0.001503 | 0.000504 |
| $P_{3-c}$ | 0.419898 | 0.664136 | 0.887414 | 0.987349 | 0.995759 |

### 3.2.1 Effects of user parameter $\lambda_B$

Among the three sets $a$, $b$, and $c$ in Table 1, $\lambda_B$ in set $a$ corresponds to a cautious user (who would seldom open suspicious files containing virus), $\lambda_B$ in set $c$ corresponds to a relatively careless user (who is more likely to click malicious links or files infecting the device), and $\lambda_B$ in set $b$ corresponds to an intermediate case between the former two. Moreover, set $a$ corresponds to a case where the recovery capability dominates ($\lambda_B < \mu_q$), while set $c$ corresponds to a case where the occurrence rate of the malicious event dominates ($\lambda_B > \mu_q$).
more quickly and eventually becomes the lowest due to an increase in the corresponding fraud complete state probability (refer to Figure 7).

Figure 7 shows an upward trend of the fraud complete state probability as time proceeds. In particular, $P_{3-a}$ with the low transition rate $\lambda_B$ stays below 0.6 during the entire considered mission time with a steady ascending pace. In contrast, $P_{3-b}$ and $P_{3-c}$ increase more substantially over the time, especially in the case of the careless user $P_{3-c}$, it jumps in the fastest pace and keeps rising to the roof 1 around 16 k hours. It supports the intuition that the fraud complete state probability is the lowest under set $a$ (having the smallest $\lambda_B$), and is the largest under set $c$ with the highest $\lambda_B$. 

**FIGURE 4**  The clean state probability for different types of users

**FIGURE 5**  The acquisition state probability for different types of users

**FIGURE 6**  The infection state probability for different types of users
3.2.2 Effects of recovery rates $\mu_d$, $\mu_q$, and $\mu_c$

Effects of recovery rates $\mu_d$, $\mu_q$, and $\mu_c$ on the system security are investigated through parameter sets $d$, $b$, and $e$ in Table 1. These three sets share same transition rates $\lambda_A$, $\lambda_B$, and $\lambda_C$ but have different values of $\mu_d$, $\mu_q$, and $\mu_c$. Specifically, set $d$ models a strong recovery capability (system used by an experienced user who protects the device with adequate antivirus/attack measures), set $e$ models a weak recovery capability (system used by an amateur user), and set $b$ models a case in-between the former two. The state probabilities under set $b$ are presented in Table 3. Tables 5 and 6 show the system state probabilities under sets $d$ and $e$, respectively.

In Figures 8 to 11, we illustrate each system state probability under parameter sets ($d$, $b$, $e$) graphically. As shown in Figure 8, under set $d$ having the largest recovery rates (ie, strong/effective antihacking measure), the clean state probability appears the best (largest) among the three cases compared, and declines the slowest over the time; under set $e$ having the smallest recovery rates (ie, weak antihacking measures), the clean state probability appears the smallest all the time, and it declines the most quickly.
As observed from Figure 9, the acquisition state probability ascends quickly at the beginning due to the occurrence of event A, reaching a peak value, and then descending due to interacting effects from the attack and recovery events. In particular, $P_{1,b}$ first ascends to the highest point at 0.14, then drops quickly, and becomes less than $P_{1,d}$ at around 10 k hours; $P_{1,d}$ (with the strongest recovery capability among the three cases) has a steady fall from 0.058 to 0.044 after the initial ascending to the peak; $P_{1,e}$ falls suddenly and stays around a very low value for the rest of time after the initial ascending to the peak. In the long run, the acquisition state probability is the best (largest) under set $d$ and the lowest under set $e$.

As observed from Figure 10, the infection state probability reaches a peak quickly at the beginning and then declines gradually; this probability under set $e$ is the highest at the beginning due to the lowest recovery rates (among the three parameter sets compared), then drops more quickly, and becomes the lowest due to an increase in the corresponding fraud complete state probability (Figure 11).
Figure 11 demonstrates the growing probabilities of the fraud complete state under different levels of antiattack measures. This figure illustrates the intuitive result that the fraud complete state probability under set $d$ (having the largest recovery rates) is the lowest due to the effective recovery actions, and is the largest under set $e$ (having the smallest recovery rates). In particular, $P_{3-d}$ rises slowly to 0.273 at the end of the considered mission time; $P_{3-e}$ soars up to 0.8 by $t = 2k$ hours, and then rises to 1 around 6 k hours.

4 SEMI-MARKOV PROCESS–BASED STEADY-STATE SOLUTION AND ANALYSIS

The CTMC-based time-dependent solution in Section 3 is limited to exponentially distributed transition time between different system states (i.e., all the transition rates in Figure 3 are constant). However, in many applications, the Weibull distribution is a more desirable choice due to its additional shape parameter signifying the trend in the transition rate. In this section, we present the SMP-based steady-state solution to systems subject to the sequential cyber-attack, which relaxes the limitation of the exponential transition time. Effects of different model parameters on the attack success probability are also investigated.

4.1 SEMI-MARKOV PROCESS–BASED SOLUTION

To illustrate the SMP-based steady-state solution, we consider a scenario where the banking fraud protection service is available to cancel any suspicious payments. Specifically, in the case of suspicious payments, e.g., purchase for overpriced items, or credit card payments happening in a totally different area, the subjective bank would send the customer a message (via phone or email) to confirm the activity; the payment would be canceled if no positive confirmation is received. This fraud protection service can possibly bring the system back to the infection state from the fraud complete state, as shown in Figure 12. All the other transitions are similar to those in Figure 3.

Different from the model in Figure 3 having constant transition rates, the SMP model presented in Figure 4 is capable of handling nonexponential distributions such as the Weibull distribution or Gamma distribution, represented using the cumulative distribution function (CDF) $F_{ij}(t; \alpha_{ij}, \beta_{ij})$. In particular, $F_{ij}$ denotes the CDF of the transition time from state $i$ to state $j$ ($i, j = 0, 1, 2, 3$). We choose the Weibull distribution with scale and shape parameters ($\alpha_{ij}, \beta_{ij}$) in the following study due to its flexibility in modeling different failure rate behaviors and its wide application in system dependability.

The CDF of the Weibull distribution is $F_{ij}(t; \alpha_{ij}, \beta_{ij}) = 1 - e^{-(t/\alpha_{ij})^{\beta_{ij}}}$. The exponential distribution appears as a special case of the Weibull distribution when $\beta_{ij} = 1$. The Rayleigh distribution is also a special case of the Weibull distribution when $\beta_{ij} = 2$.

According to other works, the hierarchical analytical approach for steady-state analysis of SMP contains two stages. Stage 1 deals with the evaluation of the one-step transition probability matrix of the embedded Markov chain (EMC) of the SMP using equations in the appendix (A1 to A3) of the work of Kumar et al. Stage 2 evaluates the sojourn time in each system state. The steady-state probability $P_i$ of each state is further obtained using (6):

$$P_i = \frac{v_i T_i}{\sum_{j\in\{0,1,2,3\}} v_j T_j}, \quad i \in \{0, 1, 2, 3\},$$

where $v_i$ means the steady-state probability of state $i \in \{0, 1, 2, 3\}$ in the EMC, and $T_i$ means the sojourn time at state $i \in \{0, 1, 2, 3\}$ for the SMP.

![FIGURE 12 Semi-Markov process model of the Trojan attack](image-url)
Specifically, in stage 1, the SMP model is illustrated by its kernel matrix $\mathbf{K}(t)$, whose elements $k_{ij}(t)$ are the probabilities that the SMP has just entered state $i$, the next transition occurs within time $t$ and the next state is $j$. $^{62}$ The matrix $\mathbf{K}(t)$ for the SMP model in Figure 12 is given in (7).

$$\mathbf{K}(t) = \begin{bmatrix} 0 & k_{01} & 0 & 0 \\ k_{10} & 0 & k_{12} & 0 \\ k_{20} & k_{21} & 0 & k_{23} \\ 0 & 0 & k_{32} & 0 \end{bmatrix}$$ (7)

Assuming the Weibull state transition time, the nonzero elements of $\mathbf{K}(t)$ are given in (8) to (14). $^{62}$ Wolfram mathematics and MATLAB are used to calculate the complex integrals involved.

$$k_{01}(t) = F_{01}(t) = 1 - e^{-\left(\frac{t}{\alpha_{01}}\right)^{\beta_{01}}}$$ (8)

$$k_{32}(t) = F_{32}(t) = 1 - e^{-\left(\frac{t}{\alpha_{32}}\right)^{\beta_{32}}}$$ (9)

$$k_{10}(t) = \int_{0}^{t} F_{12}(x) \, dF_{10}(x) = \frac{\beta_{10}}{\alpha_{10}^{\beta_{10}}} \int_{0}^{t} x^{\beta_{10}-1} e^{-\left[\left(\frac{x}{\alpha_{10}}\right)^{\beta_{10}} + \left(\frac{x}{\alpha_{11}}\right)^{\beta_{11}}\right]} \, dx$$ (10)

$$k_{12}(t) = \int_{0}^{t} F_{10}(x) \, dF_{12}(x) = \frac{\beta_{12}}{\alpha_{12}^{\beta_{12}}} \int_{0}^{t} x^{\beta_{12}-1} e^{-\left[\left(\frac{x}{\alpha_{10}}\right)^{\beta_{10}} + \left(\frac{x}{\alpha_{11}}\right)^{\beta_{11}}\right]} \, dx$$ (11)

$$k_{20}(t) = \int_{0}^{t} F_{21}(x) \, F_{23}(x) \, dF_{20}(x) = \frac{\beta_{20}}{\alpha_{20}^{\beta_{20}}} \int_{0}^{t} x^{\beta_{20}-1} e^{-\left[\left(\frac{x}{\alpha_{21}}\right)^{\beta_{21}} + \left(\frac{x}{\alpha_{23}}\right)^{\beta_{23}} + \left(\frac{x}{\alpha_{20}}\right)^{\beta_{20}}\right]} \, dx$$ (12)

$$k_{21}(t) = \int_{0}^{t} F_{20}(x) \, F_{23}(x) \, dF_{21}(x) = \frac{\beta_{21}}{\alpha_{21}^{\beta_{21}}} \int_{0}^{t} x^{\beta_{21}-1} e^{-\left[\left(\frac{x}{\alpha_{21}}\right)^{\beta_{21}} + \left(\frac{x}{\alpha_{23}}\right)^{\beta_{23}} + \left(\frac{x}{\alpha_{20}}\right)^{\beta_{20}}\right]} \, dx$$ (13)

$$k_{23}(t) = \int_{0}^{t} F_{20}(x) \, F_{21}(x) \, dF_{23}(x) = \frac{\beta_{23}}{\alpha_{23}^{\beta_{23}}} \int_{0}^{t} x^{\beta_{23}-1} e^{-\left[\left(\frac{x}{\alpha_{21}}\right)^{\beta_{21}} + \left(\frac{x}{\alpha_{23}}\right)^{\beta_{23}} + \left(\frac{x}{\alpha_{20}}\right)^{\beta_{20}}\right]} \, dx.$$ (14)

For the SMP steady-state analysis, $^{64}$ the one-step transition probability matrix of the EMC is evaluated as $\mathbf{K}(\infty)$ ($t$ approaches infinity) as shown in (15), with condition that the sum of elements on the same row of $\mathbf{K}(\infty)$ is always 1. Thus, $k_{01}(\infty)$ and $k_{32}(\infty)$ should be equal to 1 as they are the only element in row 1 and row 4, respectively.

$$\mathbf{K}(\infty) = \begin{bmatrix} 0 & k_{01}(\infty) & 0 & 0 \\ k_{10}(\infty) & 0 & k_{12}(\infty) & 0 \\ k_{20}(\infty) & k_{21}(\infty) & 0 & k_{23}(\infty) \\ 0 & 0 & k_{32}(\infty) & 0 \end{bmatrix}$$ (15)

Solving the EMC steady-state equations $\mathbf{v} = \mathbf{v} \cdot \mathbf{K}(\infty)$ and $\mathbf{v} \cdot \mathbf{e}^T = 1$, where row vectors $\mathbf{v} = [v_1 \ v_2 \ v_3 \ v_4]$ and $\mathbf{e} = [1 \ 1 \ 1 \ 1]$, we obtain the steady-state probabilities of the EMC for the SMP. The set of equations is solved by Wolfram mathematics in this work to find values of $v_i$ used in (6).

In stage 2, sojourn time $T_1$ used in (6) is evaluated using (16) to (19) according to the work of Kumar et al. $^{62}$

$$T_0 = \int_{0}^{\infty} F_{01}(t) \, dt = \int_{0}^{\infty} e^{-\left(\frac{t}{\alpha_{01}}\right)^{\beta_{01}}} \, dt$$ (16)

$$T_1 = \int_{0}^{\infty} F_{10} F_{12} \, dt = \int_{0}^{\infty} e^{-\left[\left(\frac{x}{\alpha_{10}}\right)^{\beta_{10}} + \left(\frac{x}{\alpha_{11}}\right)^{\beta_{11}}\right]} \, dt$$ (17)

$$T_2 = \int_{0}^{\infty} F_{20} F_{21} F_{23} \, dt = \int_{0}^{\infty} e^{-\left[\left(\frac{x}{\alpha_{21}}\right)^{\beta_{21}} + \left(\frac{x}{\alpha_{23}}\right)^{\beta_{23}} + \left(\frac{x}{\alpha_{20}}\right)^{\beta_{20}}\right]} \, dt$$ (18)

$$T_3 = \int_{0}^{\infty} F_{32}(t) \, dt.$$ (19)
Finally, according to (6), the steady-state probabilities $P_i (i = 0, 1, 2, 3)$ for the SMP model in Figure 12 are determined. The attack success probability is given as $P_3$, and the system security is equal to $1 - P_3 = P_0 + P_1 + P_2$.

### 4.2 Analysis results

Table 7 shows some baseline values of model parameters for the example system based on statistics and data of other works.\(^{52,65-67}\)

While in Section 3, the system security performance is investigated from the perspective of user’s protection awareness and recovery capability, in this section, we study effects of different transition time distribution parameters on the system security. Particularly, we choose to vary the Weibull distribution parameter ($\alpha$ or $\beta$) of a single attack transition $F_{12}$ (case 1), or a single recovery transition $F_{10}$ (case 2), or all attack transitions ($F_{01}, F_{12}, F_{23}$) (case 3), or all recovery transitions ($F_{10}, F_{20}, F_{21}, F_{32}$) (case 4) to illustrate their effects on the system security performance.

#### 4.2.1 Effects of scale parameter $\alpha$

We vary the value of scale parameter $\alpha$ from 1 second to 1 month and collect the system state probabilities and the final security (evaluated as $P_0 + P_1 + P_2$) in Tables 8 to 11 under four cases with changing $\alpha_{12}$ (mean time to infection), changing $\alpha_{10}$ (mean time to delete malicious files or links), changing ($\alpha_{01}, \alpha_{12}, \alpha_{23}$) (mean time from a better state to a worse state), and changing ($\alpha_{10}, \alpha_{20}, \alpha_{21}, \alpha_{32}$) (mean time from a worse state to a better state), respectively. All other unchanging parameters remain the same as those in Table 7. Figures 13 to 16 show the results graphically.

Specifically, Figure 13 illustrates the graphical results when $\alpha_{12}$ (mean time to infection) varies from 1 second to 1 month. As $\alpha_{12}$ increases, the attack success probability ($P_1$) reduces or the system security ($P_0 + P_1 + P_2 = 1 - P_3$) increases.

| CDF   | Distribution | Parameter values |
|-------|--------------|------------------|
| $F_{01}$ | Weibull      | $\alpha_{01} = 1/0.034$, $\beta_{01} = 0.54$ |
| $F_{10}$ | Weibull      | $\alpha_{10} = 1/0.0125$, $\beta_{10} = 0.86$ |
| $F_{12}$ | Rayleigh     | $\alpha_{12} = 1/0.106$, $\beta_{12} = 2$ |
| $F_{20}$ | Exponential  | $\alpha_{20} = 1/0.15$, $\beta_{20} = 1$ |
| $F_{21}$ | Exponential  | $\alpha_{21} = 1/0.2$, $\beta_{21} = 1$ |
| $F_{23}$ | Weibull      | $\alpha_{23} = 1/0.0023$, $\beta_{23} = 0.072$ |
| $F_{32}$ | Exponential  | $\alpha_{32} = 1/0.39$, $\beta_{32} = 1$ |

**Abbreviations:** CDF, cumulative distribution function.

| $\alpha_{12}$ | 1 second | 1 minute | 15 minutes | 1 hour | 1 day | 1 month |
|---------------|----------|----------|------------|--------|-------|---------|
| $P_0$         | 0.1208621826 | 0.788977963 | 0.63387133 | 0.488176056 | 0.374639318 | 0.373586817 |
| $P_1$         | 0.000538558 | 0.030412079 | 0.266976239 | 0.474171663 | 0.625044861 | 0.626412820 |
| $P_2$         | 0.104155888 | 0.09737860 | 0.053507887 | 0.020300786 | 0.000173191 | 0.000000196 |
| $P_3$         | 0.098023728 | 0.083231357 | 0.045734142 | 0.017354195 | 0.00014803 | 0.000000167 |
| Security      | 0.910976272 | 0.916758643 | 0.954265858 | 0.982648505 | 0.99985197 | 0.99999833 |

| $\alpha_{10}$ | 1 second | 1 minute | 15 minutes | 1 hour | 1 day |
|---------------|----------|----------|------------|--------|-------|
| $P_0$         | 0.9996499143 | 0.977106103 | 0.796930798 | 0.693465 | 0.62368873 |
| $P_1$         | 0.00003492017 | 0.0200080196 | 0.133502566 | 0.191962 | 0.23067525 |
| $P_2$         | 0.0000004766 | 0.001517049 | 0.037507911 | 0.061774 | 0.07852195 |
| $P_3$         | 0.0000004074 | 0.001296651 | 0.032058725 | 0.052799 | 0.06711408 |
| Security      | 0.999995926 | 0.998703349 | 0.967941275 | 0.947200793 | 0.932885922 |

| $\alpha_{01} = \alpha_{12} = \alpha_{23}$ | 1 second | 1 minute | 15 minutes | 1 hour | 1 day |
|------------------------------------------|----------|----------|------------|--------|-------|
| $P_0$                                   | 0.001364646 | 0.08564646 | 0.456367754 | 0.65885505982257 | 0.96703022772433 |
| $P_1$                                   | 0.001395198 | 0.097118889 | 0.376945508 | 0.31370215501020 | 0.03295369510430 |
| $P_2$                                   | 0.269827571 | 0.310973599 | 0.075547948 | 0.01343059373942 | 0.00000913099143 |
| $P_3$                                   | 0.727412567 | 0.50624305 | 0.091138791 | 0.01401219142781 | 0.00000694617794 |
| Security                                | 0.272357433 | 0.49376595 | 0.90861209 | 0.9859870857219 | 0.9999930582006 |

**Tables 7 to 10:**

- **Table 7** Baseline values of model parameters
- **Table 8** System state probabilities and security with changing $\alpha_{12}$
- **Table 9** System state probabilities and security with changing $\alpha_{10}$
- **Table 10** System state probabilities and security with changing $\alpha_{01}, \alpha_{12}, \alpha_{23}$
TABLE 11 System state probabilities and security with changing $\alpha_{10}$, $\alpha_{20}$, $\alpha_{21}$, $\alpha_{32}$

| $\alpha_{10} = \alpha_{20} = \alpha_{21} = \alpha_{32}$ | 1 second | 1 minute | 15 minutes | 1 hour | 1 day | 1 month |
|------------------------------------------------|----------|----------|-------------|--------|-------|---------|
| $P_0$                                              | 0.999650794 | 0.97923659 | 0.658469824 | 0.243042517 | 0.00821834 | 0.000195167 |
| $P_1$                                              | 0.000349203 | 0.002083527 | 0.010400927 | 0.0060351934 | 0.002615381 | 6.34860E-05  |
| $P_2$                                              | 1.39029E-09 | 0.000265528 | 0.076701042 | 0.203923282 | 0.224349785 | 0.16339693   |
| $P_3$                                              | 1.53633E-09 | 0.000427285 | 0.160828208 | 0.492682267 | 0.764816494 | 0.836344418  |
| Security                                           | 0.99999999846 | 0.999573   | 0.839172    | 0.507318   | 0.235184 | 0.16365558 |

FIGURE 13 Steady-state probabilities with changing $\alpha_{12}$

FIGURE 14 Steady-state probabilities with changing $\alpha_{10}$

FIGURE 15 Steady-state probabilities with changing $\alpha_{01} = \alpha_{12} = \alpha_{23}$
In particular, the steady-state probability for the clean state $P_0$ decreases quickly, but for the acquisition state, $P_1$ grows fast; their combined effects contribute to the increasing trend of the entire system security (last row of Table 8).

Figure 14 illustrates the graphical results when $\alpha_{10}$ (mean time to delete hazardous file) varies from 1 second to 1 month. As $\alpha_{10}$ increases, the time of the system being in the acquisition state becomes longer, making it more likely to be infected. Thus, the attack success probability increases or the system security decreases.

Figure 15 illustrates the graphical results when $\alpha_{01} = \alpha_{12} = \alpha_{23}$ vary simultaneously from 1 second to 1 month. The similar but more prominent decreasing trend than that in Figure 13 for the attack success probability can be observed. Figure 16 illustrates the graphical results when $\alpha_{10} = \alpha_{20} = \alpha_{21} = \alpha_{32}$ vary simultaneously from 1 second to 1 month. The similar but more prominent increasing trend than that in Figure 14 for the attack success probability can be observed. Namely, it is notable that trends for the system security ($1-P_3$) when transition rate parameters change together have a much wider range (0.16 to 0.999) than cases with only one variant transition rate with range (0.91 to 0.99). All these results support the intuition that, as the time toward the fraud complete state takes longer (increasing $\alpha_{01}$, $\alpha_{12}$, $\alpha_{23}$), the attack success probability $P_3$ becomes lower (ie, the system security increases); as the recovery time toward the clean state takes longer (increasing $\alpha_{10}$, $\alpha_{20}$, $\alpha_{21}$, $\alpha_{32}$), the attack success probability $P_3$ becomes higher (ie, the system security decreases). These studies clearly show that the steady-state probabilities and the system security are highly dependent on the scale parameters of the Weibull distributions modeling the transition time between different states.

### 4.2.2 Effects of shape parameter $\beta$

In reliability engineering, the value of $\beta$ has a distinct effect on the failure rate. Specifically, $\beta < 1$ corresponds to a failure rate that decreases with time, $\beta = 1$ corresponds to a constant failure rate (ie, exponential distribution), and $\beta > 1$ corresponds to a failure rate that increases with time. According to these characteristics, we choose values of $\beta$ covering all those three categories, specifically, (0.1, 0.5, 1, 1.5, 2, 5). Figure 17 illustrates the CDFs of the Weibull distribution with the chosen values of $\beta$ and $\alpha = 2$. All the CDFs share the same point with $t = \alpha = 2$. Their relative relationships are different before and after this common turning point (eg, the CDF for $\beta = 5$ is the lowest among the six values, but becomes the highest after the point).
TABLE 12  System state probabilities and security with changing $\beta_{12}$

| $\beta_{12}$ | 0.1 | 0.5 | 1 | 1.5 | 2 | 5 |
|-------------|-----|-----|---|-----|---|---|
| $P_0$       | 0.511481883 | 0.626552378 | 0.670986889 | 0.678059137 | 0.679147007 | 0.675238107 |
| $P_1$       | 0.429253434 | 0.271701801 | 0.210858953 | 0.210172168 | 0.199940657 | 0.206433841 |
| $P_2$       | 0.031953538 | 0.054857824 | 0.063868065 | 0.065168748 | 0.065168106 | 0.063798434 |
| $P_3$       | 0.027311145 | 0.046887997 | 0.054582291 | 0.055700847 | 0.055720529 | 0.055429622 |
| Security    | 0.972688555 | 0.953112003 | 0.945417709 | 0.942499153 | 0.94279471 | 0.945470378 |

TABLE 13  System state probabilities and security with changing $\beta_{20}$

| $\beta_{20}$ | 0.1 | 0.5 | 1 | 1.5 | 2 | 3 |
|-------------|-----|-----|---|-----|---|---|
| $P_0$       | 0.85555126 | 0.739535723 | 0.664397574 | 0.635145505 | 0.624383459 | 0.618879551 |
| $P_1$       | 0.900167217 | 0.164022807 | 0.208403553 | 0.224727721 | 0.230515175 | 0.233382059 |
| $P_2$       | 0.029264626 | 0.051997954 | 0.06851306 | 0.07555188 | 0.078233726 | 0.079655517 |
| $P_3$       | 0.025013031 | 0.044443516 | 0.058617568 | 0.064575186 | 0.066867639 | 0.068082872 |
| Security    | 0.974986969 | 0.955556484 | 0.941382432 | 0.935428414 | 0.933132361 | 0.931917128 |

TABLE 14  System state probabilities and security with changing $\beta_{01}$, $\beta_{12}$, $\beta_{23}$

| $\beta_{01} = \beta_{12} = \beta_{23}$ | 0.1 | 0.3 | 0.4 | 0.5 | 0.7 | 1 | 1.5 | 2 |
|---------------------------------------|-----|-----|-----|-----|-----|---|-----|---|
| $P_0$       | 0.999999544 | 0.884889745 | 0.761517234 | 0.684137245 | 0.63896689 | 0.651344125 | 0.624383459 | 0.618879551 |
| $P_1$       | 2.05229E-07  | 0.099628355 | 0.201320749 | 0.259912667 | 0.318078637 | 0.320514408 | 0.326612014 | 0.330787765 |
| $P_2$       | 3.01651E-08  | 0.012955858 | 0.033419363 | 0.052477538 | 0.043032278 | 0.097062677 | 0.105857571 | 0.102230181 |
| $P_3$       | 2.09488E-08  | 0.002526042 | 0.003742654 | 0.003472501 | 0.001992397 | 0.000572464 | 0.07241E-05  | 1.37618E-09 |
| Security    | 0.999999979 | 0.997473958 | 0.996257346 | 0.996527499 | 0.998007603 | 0.999427536 | 0.999932759 | 0.999999999 |

TABLE 15  System state probabilities and security with changing $\beta_{10}$, $\beta_{20}$, $\beta_{21}$, $\beta_{32}$

| $\beta_{10} = \beta_{20} = \beta_{21} = \beta_{32}$ | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 | 1 | 1.5 | 2 |
|--------------------------------------------------|-----|-----|-----|-----|-----|---|-----|---|
| $P_0$       | 2.10477E-05 | 0.242107751 | 0.650125207 | 0.726566069 | 0.664397574 | 0.61770584 | 0.390440571 |
| $P_1$       | 2.13365E-06 | 0.031607815 | 0.103509065 | 0.154197617 | 0.208403553 | 0.23392732 | 0.330153912 |
| $P_2$       | 0.00080784   | 0.046256243 | 0.047072539 | 0.044829966 | 0.06851306 | 0.091125102 | 0.181975245 |
| $P_3$       | 0.999168979 | 0.680028191 | 0.199231188 | 0.074406365 | 0.058617568 | 0.063176993 | 0.097430271 |
| Security    | 0.000831021 | 0.319971809 | 0.800706812 | 0.925593635 | 0.941382432 | 0.936823007 | 0.902569729 |

FIGURE 18  Steady-state probabilities and security with changing $\beta_{12}$

While we vary $\beta$, all other unchanging parameters remain the same as those in Table 7. Tables 12 to 15 summarize the system state probabilities and the final security under the four cases. Figures 18 to 21 show the results graphically. Specifically, Figure 18 illustrates the steady-state probabilities and security when $\beta_{12}$ varies. The attack success probability $P_3$ first increases, then reaches the maximum around $\beta_{12} = 2$, and then drops due to interacting effects between $\beta$ and $\alpha$. This trend can be observed more clearly in the zoomed graph for the system security (right figure), which declines at the beginning, reaches the bottom around 2, and then ascends slowly.
When parameters $\beta_{01}$, $\beta_{12}$, and $\beta_{23}$ vary simultaneously, the nonmonotonic change in the attack success probability or the system security becomes more apparent, as demonstrated in Figure 19. The curve for the system security declines quickly at the beginning, then reaches the bottom around $\beta_{01} = \beta_{12} = \beta_{23} = 0.4$, then starts to increase, and eventually reaches the peak value 1.
Figure 20 illustrates the monotonic decreasing trend of the system security as $\beta_{10}$ increases within the set of considered values. It shows that the shape parameter $\beta$ affects the system security in a way that is different from the scale parameter $\alpha$ (Figure 14 versus Figure 20). The nonmonotonic change in the attack success probability or the system security starts to show when parameters $\beta_{10}$, $\beta_{20}$, $\beta_{21}$, and $\beta_{32}$ vary simultaneously in Figure 21. Specifically, the system security ranges from 0.0008 to 0.9; it reaches the peak quickly at the beginning, and then decreases gradually after $\beta_{10} = \beta_{20} = \beta_{21} = \beta_{32} = 1$.

It is also observed that, for the case with changing $\beta_{10} = \beta_{12} = \beta_{23}$, the system security plot is concave, while for the case with changing $\beta_{10} = \beta_{20} = \beta_{21} = \beta_{32}$, the system security is a convex curve.

The analysis based on the numerical results in this section shows that the system steady-state probabilities and particularly, the system security, are highly dependent on values of the transition time distribution parameters. For the Weibull distribution studied, the scale parameter and the shape parameter affect the system security differently (the former’s impact is more intuitive, while the latter’s impact is more complicated appearing nonmonotonic).

5 | CONCLUSION AND FUTURE WORK

Most of the existing works for security risk assessment have assumed independence among different hazardous events toward a successful malicious attack. In this paper, we have contributed by addressing the sequence dependent cyber-attack in the modeling and analysis of the attack success probability (ie, the security risk occurrence probability). The solution methodology encompasses a CTMC-based method to assess the security risk occurrence probability for any mission time and an SMP-based method to assess the steady-state probabilities for systems subject to sequential cyber-attacks. While the CTMC-based method is limited to exponential state transition time, the SMP-based method is flexible in modeling diverse types of transition time distributions. Effects of different model parameter reflecting users’ protection awareness and recovery capabilities are demonstrated via detailed analyses of Trojan attacks launched to the bank application.

There exist other types of sequential cyber-attacks such as the denial-of-service attack and the buffer overflow attack. The proposed model will be applied to these cases where different Markov models should be generated to represent their sequential attack behaviors and then analyzed to obtain the occurrence probabilities of security risks from those attacks. We are also interested in extending the SMP-based method for time-dependent analysis of systems under sequential cyber-attacks. Another direction is to study other types of dependencies (eg, function dependencies and competitions) in system security modeling and analysis. In addition, we are interested in exploring models and algorithms for addressing both reliability and security of complex systems in a unified manner.

ACKNOWLEDGEMENT

Portion of this work was presented at the 12th International Conference on Reliability Maintainability and Safety. We would like to thank the attendees for their feedback. We are also grateful to the Editor-in-Chief Dr Giampiero Accardo and anonymous reviewers for their helpful comments.

CONFLICT OF INTEREST

The authors have no conflict of interest relevant to this article.

ORCID

Liudong Xing https://orcid.org/0000-0003-1606-1644

REFERENCES

1. Liu S, Liu Y. Network security risk assessment method based on HMM and attack graph model. In: Proceedings of the 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel Distributed Computing (SNPD); 2016; Shanghai, China.
2. Taylor H. Biggest cybersecurity threats in 2016. CNBC. http://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html. Accessed November 2019.
3. Escudero C, Sicard F, Zamai E. Process-aware model based IDSs for industrial control systems cybersecurity: approaches, limits and further research. In: Proceedings of the IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA); 2018; Turin, Italy.
4. Zetter K. Sony got hacked hard: what we know and don’t know so far. https://www.wired.com/2014/12/sony-hack-what-we-know/. Accessed November 2019.

5. Goel V, Perlroth N. Yahoo says 1 billion user accounts were hacked. https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached. Accessed November 2019.

6. Modarres M, Kaminskiy M, Krivtsov V. Reliability Engineering and Risk Analysis: A Practical Guide. 2nd ed. Boca Raton, FL: CRC Press; 2009. ISBN: 978-0-849-39247-4.

7. Cui X, Tan X, Zhang Y, Xi H. A Markov game theory-based risk assessment model for network information system In: Proceedings of the International Conference on Computer Science and Software Engineering; 2008; Hubei, China.

8. George G, Thampi SM. A graph-based decision support model for vulnerability analysis in IoT networks. In: Security in Computing and Communications: 6th International Symposium, SSCC 2018, Bangalore, India, September 19-22, 2018, Revised Selected Papers. Singapore: Springer; 2018:1-23.

9. Matulevičius R, Mayer N, Mouratidis H, Dubois E, Heymans P, Genon N. Adapting secure tropos for security risk management in the early phases of information systems development. In: Advanced Information Systems Engineering: 20th International Conference, CAISE 2008 Montpellier, France. June 16-20, 2008 Proceedings. Berlin, Germany: Springer; 2008:541-555.

10. Lo C-C, Chen W-J. A hybrid information security risk assessment procedure considering interdependences between controls. Expert Syst Appl. 2012;39(1):247-257.

11. Wang L, Wang B, Peng Y. Research the information security risk assessment technique based on Bayesian network. In: Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE); 2010; Chengdu, China.

12. Paintsil E. Taxonomy of security risk assessment approaches for researchers. In: Proceedings of the IEEE 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN); 2012; Sao Carlos, Brazil.

13. Smojver S. Selection of information security risk management method using analytic hierarchy process (AHP). In: Proceedings of the 22nd Central European Conference on Information and Intelligent Systems; 2011; Varaždin, Croatia.

14. Taubenberger S, Jürgens J, Yu Y, Nuseibeh B. Problem analysis of traditional IT-security risk assessment methods – an experience report from the insurance and auditing domain. In: Future Challenges in Security and Privacy for Academia and Industry. Berlin, Germany: Springer; 2011:259-270.

15. Zhang H, Zhang J-H, Liu N, Wu X. Function-oriented information assets identification on substation automation system. In: Proceedings of the IEEE International Conference on Power and Energy Engineering; 2009; Wuhan, China.

16. Shameli-Sendi A, Aghababaei-Barzegar R, Cheriet M. Taxonomy of information security risk assessment (ISRA). Comput Secur. 2016;57:14-30.

17. Bolczak CN, Fong V, Jehlen R. NextGen flight security risk assessment information concept. In: Proceedings of the 2009 IEEE/AIAA 28th Digital Avionics Systems Conference; 2009; Orlando, FL.

18. Letchford J, Vorobeychik Y. Computing optimal security strategies for interdependent assets. In: Proceedings of the 28th Conference on Uncertainty in Artificial Intelligence; 2012; Catalina Island, CA.

19. Samantra C, Datta S, Mahapatra SS. Risk assessment in IT outsourcing using fuzzy decision-making approach: an Indian perspective. Expert Syst Appl. 2012;41(8):4010-4022.

20. Schmidt R, Lyytinen K, Keil M, Cule P. Identifying software project risks: an international Delphi study. J Manag Inf Syst. 2001;17(4):5-36.

21. Hulitt E, Vaughn RB. Information system security compliance to FISMA standard: a quantitative measure. Telecommunication Systems. 2010;45(2-3):139-152.

22. Ekelhart A, Fenz S, Neubauer T. Ontology-based decision support for information security risk management in. In: Proceedings of the 4th International Conference on Systems; 2009; Gósper, Brazil.

23. Farahmand F, Navathe SB, Sharp GP, Enslow PH. A management perspective on risk of security threats to information systems. Inf Technol Manage. 2005;6(2-3):203-225.

24. Guan B-C, Lo C-C, Wang P, Hwang J-S. Evaluation of information security related risks of an organization the application of the multi-criteria decision-making method. In: Proceedings of the 37th IEEE Annual International Carnahan Conference on Security Technology; 2003; Taipei, Taiwan.

25. Lund MS, Solhaug B, Stolen K. Model-Driven Risk Analysis: The CORAS Approach. Berlin, Germany: Springer Science & Business Media; 2010.

26. Winkelvos T, Rudolph C, Repp J. A property based security risk analysis through weighted simulation. In: Proceedings of the 2011 Information Security for South Africa; 2011; Johannesburg, South Africa.

27. Yacoub SM, Ammar HH. A methodology for architecture-level reliability risk analysis. IEEE Trans Softw Eng. 2002;28(6):529-547.

28. Paté-Cornell M-E, Kuypers M, Smith M, Keller P. Cyber risk management for critical infrastructure: a risk analysis model and three case studies. Risk Analysis. 2018;38(2):226-241.

29. Romero M, Haddad H, Molero A. A methodological tool for asset identification in web applications: security risk assessment. In: Proceedings of 4th International Conference on Software Engineering Advances; 2009; Porto, Portugal.

30. Farahmand F, Navathe SB, Enslow PH, Sharp GP. Managing vulnerabilities of information systems to security incidents. In: Proceedings of the 5th International Conference on Electronic Commerce; 2003; Pittsburgh, PA.

31. Den Braber F, Hogganvik I, Lund MS, Stolen K, Vraalsen F. Model-based security analysis in seven steps—a guided tour to the CORAS method. BT Technol J. 2007;25(1):101-117.

32. Stolen K, den Braber F, Dimitrakos T, et al. Model-based risk assessment—the CORAS approach. In: Proceedings of NIK 2002 Informatics Conference; Kongsberg, Norway; 2002.
33. Xing L, Levitin G, Wang C. Dynamic System Reliability: Modeling and Analysis of Dynamic and Dependent Behaviors. Hoboken, NJ: Wiley; 2019. ISBN: 978-1-119-50763-5.

34. Dunjó J, Fthenakis V, Vilchez JA, Arnaldos J. Hazard and operability (HAZOP) analysis. A literature review. J Hazard Mater. 2010;173(1-3):19-32.

35. Lenkala SR, Shetty S, Xiong K. Security risk assessment of cloud carrier. In: Proceedings of the 13th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing; 2013; Delft, The Netherlands.

36. Joh H, Malaiya YK. Defining and assessing quantitative security risk measures using vulnerability lifecycle and CVSS metrics. In: Proceedings of the 11th International Conference on Security and Management; 2011; Las Vegas, NV.

37. Liu S, Wu J, Lu Z, Xiong H. VMRSa: a novel virtual machine risk assessment scheme in the cloud environment. In: Proceedings of the IEEE 10th International Conference on Services Computing; 2013; Santa Clara, CA.

38. Werner C, Bedford T, Quigley J. Sequential refined partitioning for probabilistic dependence assessment. Risk Analysis. 2018;38(12):2683-2702.

39. Hu X, Xu M, Xu S, Zhao P. Multiple cyber attacks against a target with observation errors and dependent outcomes: characterization and optimization. Reliab Eng Syst Saf. 2017;159:119-133.

40. Ghaeini HR, Antonioli D, Brasser F, Sadeghi A-R, Tippenhauer NO. State-aware anomaly detection for industrial control systems. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing; 2018; Pau, France.

41. Wu B, Tang A, Wu J. Modeling cascading failures in interdependent infrastructures under terrorist attacks. Reliab Eng Syst Saf. 2016;147:1-8.

42. Xu M, Da G, Xu S. Cyber epidemic models with dependences. Internet Mathematics. 2015;11(1):62-92.

43. Franck S, Cédric E, Eric Z, Jean-Marie F. From ICS attacks' analysis to the S.A.F.E. approach: implementation of filters based on behavioral models and critical state distance for ICS cybersecurity. In: Proceedings of 2nd IEEE Networking Conference on Cyber Security (CSNet); 2018; Paris, France.

44. Sicard F, Zamaï E, Flaus J-M. An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems. Reliab Eng Syst Saf. 2019;188:584-603.

45. Xing L, Shrestha A, Dai Y. Exact combinatorial reliability analysis of dynamic systems with sequence-dependent failures. Reliab Eng Syst Saf. 2011;96(10):1375-1385.

46. Curty M, Zhang LL, Lo H-K, Lütkenhaus N. Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states. arXiv preprint quant-ph/0609094. 2006.

47. Song S-J. Probability Models for Assessing the Value of Battle Damage Assessment in the Defense Against Sequential Theater Missile Attacks [master's thesis]. Monterey, CA: Naval Postgraduate School; 1996.

48. Yan J, Tang Y, Zhu Y, He H, Sun Y. Smart grid vulnerability under cascade-based sequential line-switching attacks. In: Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM); 2015; San Diego, CA.

49. Yan J, He H, Zhong X, Tang Y. Q-learning-based vulnerability analysis of smart grid against sequential topology attacks. IEEE Trans Inf Forensics Secur. 2016;12(1):200-210.

50. Tretschk E, Oh SJ, Fritz M. Sequential models on agents for long-term adversarial goals. arXiv preprint arXiv:1805.12487. 2018.

51. Lin Z, Zhang X, Xu D. Reuse-oriented camouflaging trojan: vulnerability detection and attack construction. In: Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN); 2010; Chicago, IL.

52. Deng F-G, Li X-H, Zhou H-Y, Zhang Z. Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys Rev A. 2005;72(4):044302.

53. Trivedi KS. Probability and Statistics With Reliability, Queuing, and Computer Science Applications; vol 13. Englewood Cliffs, NJ: Prentice-Hall; 1982.

54. Widdler DV. Laplace Transform (PMS-6). Princeton, NJ: Princeton University Press; 2015.

55. Seals T. Banking trojans, led by the ever-changing Emotet, dominated the email-borne threat landscape in Q4, according to Proofpoint. https://threatpost.com/banking-trojans-top-threat-email/141814/. Accessed November 2019.

56. Chebyshev V, Sinitsyn F, Parinov D, Larin B, Kupreev O, Lopatin E. IT threat evolution Q2 2019. Statistics. https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/. Accessed November 2019.

57. Yang L-X, Yang X, Zhu Q, Wen L. A computer virus model with graded cure rates. Nonlinear Anal Real World Appl. 2013;14(1):414-422.

58. Tang C, Wu Y. Global exponential stability of nonresident computer virus models. Nonlinear Anal Real World Appl. 2017;34:149-158.

59. Koutras VP, Platis AN. Semi-Markov performance modelling of a redundant system with partial, full and failed rejuvenation. Int J Crit Comput Based Syst. 2010;1(1/2/3):59-85.

60. Limnios N, Oprisan G. Semi-Markov Processes and Applications. New York, NY: Springer Science & Business Media; 2012.

61. Kharoufeh JP, Solo CJ, Ulukus MY. Semi-Markov models for degradation-based reliability. IIE Transactions. 2010;42(8):599-612.

62. Kumar G, Vipul J, Gandhi OP. Availability analysis of repairable mechanical systems using analytical semi-Markov approach. Quality Engineering. 2013;25(2):97-107.

63. Dohi T, Goševa-Popstojanova K, Trivedi K. Estimating software rejuvenation schedules in high-assurance systems. Comput J. 2001;44(6):473-485.

64. Kulkarni VG. Modeling and Analysis of Stochastic Systems. Boca Raton, FL: Chapman and Hall/CRC; 2016.

65. Alexander DC. Application of Monte Carlo simulations to system reliability analysis. In: Proceedings of the 20th International Pump Users Symposium; 2003; Houston, TX.
66. Bailey RL, Dell TR. Quantifying diameter distributions with the Weibull function. Forest Science. 1973;19(2):97-104.
67. Thoman DR, Bain LJ, Antle CE. Inferences on the parameters of the Weibull distribution. Technometrics. 1969;11(3):445-460.
68. Blazek RB, Kim H, Rozovskii B, Tartakovsky A. A novel approach to detection of denial-of-service attacks via adaptive sequential and batch-sequential change-point detection methods. In: Proceedings of the IEEE Systems, Man and Cybernetics Information Assurance Workshop; 2001; West Point, NY.
69. Cameron C, Patsios C, Taylor PC, Pourmirza Z. Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes. IEEE Trans Smart Grid. 2018;10(3):3010-3019.
70. Moran DB. System and method for detecting buffer overflow attacks. US patent 6,826,697. November 30, 2004.
71. Xing L, Amari SV. Binary Decision Diagrams and Extensions for System Reliability Analysis. Salem, MA: Wiley-Scrivener; 2015. ISBN: 978-1-118-54937-7.
72. Liu Q, Xing L, Zhou C, Wang Y. Probabilistic security risk assessment of systems subject to sequential attacks. In: Proceedings of the 12th International Conference on Reliability Maintainability and Safety (ICRMS); 2018; Shanghai, China.

**AUTHOR BIOGRAPHIES**

**Qisi Liu** received her BE degree in Mechanical Engineering from Donghua University, Shanghai, China, in 2012 and the MS degree in Computer Engineering from the University of Massachusetts (UMass), Dartmouth, MA, in 2016. She is currently a PhD candidate at UMass Dartmouth. Her research interest includes probabilistic reliability and security risk assessment.

**Liudong Xing** received her PhD degree in Electrical Engineering from the University of Virginia, Charlottesville, VA, in 2002. She is currently a Professor in the Department of Electrical and Computer Engineering, University of Massachusetts (UMass), Dartmouth, MA. Her current research interests include reliability and resilience modeling, analysis, and optimization of complex systems and networks. She was the recipient of the 2014 Leo M. Sullivan Teacher of the Year Award, the 2010 Scholar of the Year Award, and the 2011 Outstanding Women Award of UMass Dartmouth. She was the recipient of the 2018 IEEE Region 1 Outstanding Teaching in an IEEE Area of Interest (University or College) Award, the 2015 ChangJiang Scholar award by the Ministry of Education of China, and the 2007 IEEE Region 1 Technological Innovation (Academic) Award. She was also a corecipient of the Best (Student) Paper Award at several conferences and journals. She has published two books titled “Binary Decision Diagrams and Extensions for System Reliability Analysis” and “Dynamic System Reliability: Modeling and Analysis of Dynamic and Dependent Behaviors”. She is an Associate Editor or Editorial Board member of multiple journals including Reliability Engineering & System Safety, and International Journal of Systems Science. She is a senior member of IEEE and fellow of The International Society of Engineering Asset Management.

**Chencheng Zhou** received his BE degree in Business English from Tianjin University of Commerce, Tianjin, China, in 2010 and the MS degree in Math Finance from the University of North Carolina at Charlotte, NC, in 2013. He is currently a PhD student at the University of Massachusetts, Dartmouth, MA. His research interest includes reliability analysis of complex systems, data mining, machine learning, and blockchain.

**How to cite this article:** Liu Q, Xing L, Zhou C. Probabilistic modeling and analysis of sequential cyber-attacks. Engineering Reports. 2019;1:e12065. [https://doi.org/10.1002/eng2.12065](https://doi.org/10.1002/eng2.12065)