Predictive model for multistage cyber-attack simulation

Ravdeep Kour¹ · Adithya Thaduri¹ · Ramin Karim¹

Received: 30 August 2019 / Revised: 30 August 2019 / Published online: 3 February 2020
© The Author(s) 2020

Abstract Adoption of information and communication technologies (ICT) in railway has improved the reliability, maintainability, operational efficiency, capacity as well as the comfort of passengers. This adoption introduces new vulnerabilities and entry points for hackers to launch attacks. Advanced cybersecurity threats with automated capabilities are increasing in such sectors as finance, health, grid, retail, government, telecommunications, transportation, etc. These cyber threats are also increasing in railways and, therefore, it needs for cybersecurity measures to predict, detect and respond these threats. The cyber kill chain (CKC) model is a widely used model to detect cyber-attacks and it consists of seven stages/chains; breaking the chain at an early stage will help the defender stop the adversary's malicious actions. Due to lack of real cybersecurity data, this research simulates cyber-attacks to calculate the attack penetration probabilities at each stage of the cyber kill chain model. The objective of this research is to predict cyber-attack penetrations by implementing various security controls using modeling and simulation. This research is an extension of developed railway defender kill chain which provides security controls at each stage of CKC for railway organizations to minimize the risk of cyber threats.

Keywords Cyber-attack · Cyber kill chain · Security control · Predict · Simulation

1 Introduction

Railway is one of the important critical infrastructures on which most of the common people rely on travelling and is also one of the major contributors towards the growth of the economy of a country. On one hand, the use of new advanced technologies (like Internet of Things, smart sensors, etc.) have brought significant benefits in reliability, operational efficiency, capacity as well as improved passenger experience. But on the other hand, it also increases the vulnerability of railway system towards cyber threats. Attacker may launch an attack remotely which can lead to denial of control, malfunction of alarms, manipulation of sensors or actuators to adversely affect the physical system, resulting in catastrophic consequences (Karnouskos 2011). Hackers' already targeted rail companies in Belgium, China, Denmark, Germany, Russia, South Korea, Sweden, Switzerland, the UK, and the US (Kour et al. 2019). Thus, the safety and well-being of passengers, employees, and public in general, including nearby traffic and pedestrians, must be the first priority of rail operators. However, this safety is on risk due to cybersecurity incidents, which are increasing over the last years. There are two types of cybersecurity risks in railway organizations: business risks and societal risks (Thaduri et al. 2019a, b). The impact of cybersecurity business risks include loss of revenue, impact on reputation/loss of trust, non-compliance with regulations on data protection, risks to hardware and software, reliance on invalid information, and lack of security of dependencies (Thaduri et al. 2019a, b). The impact of cybersecurity societal risks include risk to public health

✉ Ravdeep Kour
ravdeep.kour@ltu.se

Adithya Thaduri
adithya.thaduri@ltu.se

Ramin Karim
ramin.karim@ltu.se

¹ Division of Operation and Maintenance Engineering, Luleå University of Technology, 97187 Luleå, Sweden

and safety, unavailability of the railway service, societal financial losses, environmental impact due to increased energy consumption, and risk to the confidentiality and privacy of citizens (Thaduri et al. 2019a, b). Therefore, there is a need to build or establish strong cybersecurity measures to safeguard railway infrastructure against cyber-attack penetrations. However, there is a lack of real cybersecurity data and, therefore, this research will use simulation to predict cyber-attack penetration probabilities at each stage of cyber kill chain by assuming various security controls to defend against these attacks. Security controls are defined as “The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system, its components, processes, and data” (Stouffer et al. 2014). There are three general classes of security controls i.e., management, operational, and technical (Ross et al. 2007). Management and operational controls involve contingency planning controls, incident response controls, security awareness and training controls, personnel security controls, physical security controls, etc. Technical controls involve logical access control, user authentication, antivirus softwares, firewalls, penetration testing, etc.

To carry out this research, cyber kill chain (CKC) model has been used which is one of the most widely used framework to detect cyber-attack based on the kill chain tactic of the US military’s F2T2EA (find, fix, track, target, engage and assess) (Martin 2014). This model consists of seven stages and describes a logic that an attacker follows during cyber-attack within the system. Henceforth, this research will simulate cyber-attack penetrations within each stage of this model.

The outline of the paper is as follows. After introduction, state-of-the-art is provided and then seven stages of the cyber kill chain model are explained; followed by research methodology. Then, it explains the overview of developed model. Next, simulation cases are discussed. Finally, results and discussions are presented followed by conclusions and future research directions.

2 State-of-the-art

2.1 Generalized modeling tools

There are various modeling tools (both proprietary and open), such as optimized network engineering tools and network simulators to analyze the impact of cyber-attacks on the modeled network (NS-3 2019; OPNET 2019). Literature study shows that researcher are active in the area of simulating cyber-attacks in critical infrastructures and used network simulator i.e. NS2 to predict the impact of denial

of service, malware propagation, and man-in-the-middle attacks on supervisory control and data acquisition systems (SCADA) (Ciancamerla et al. 2013). An agent-based modeling and simulation approach was used in facilitating the assessment of critical infrastructure entities under cyber-attack (Rybnicek et al. 2014). A generalized simulation model of cyber-attacks in IT network was also developed (Shourabi 2015). Researchers are also active in the area of game theory to model the behaviors of complex multistage cyber-attacks. He (2017) has developed an application-oriented cyber threat assessment framework in order to address the risk posed by multistage cyber-attacks in smart grids. Intelligent transportation systems (ITS) have also developed game-theory models to secure against the fatal cyber-attacks (Alpcan and Buchegger 2010; Bahamou et al. 2016; Mejri et al. 2016; Sanjab et al. 2017; Sedjelmaci et al. 2016). In addition to this, a combined simulation of interconnected railway network, ICT network and energy grid using OpenTrack, SINCAL, and NS3 respectively has been achieved in European Union Project (Ciprnet 2013).

2.2 Railway specific simulators

A Survey of existing railway simulators show that most of them were designed for planning and operational purposes (eTrax 2016; Grube et al. 2011; OpenPowerNet Version, 1. 8. 1. 2019; OpenTrack 1990; Yao et al. 2013). The limitations of these simulators are that they lack to support cyber-attack analysis and are very costly to adopt in railway cybersecurity research. To overcome these limitations there was introduction of another simulator called SecureRails; an open source simulator for analyzing cyber-physical attacks in railway (Teo et al. 2016). This simulator is restricted to only two subsystems; the mechanical system (involving the train’s motion) and the electrical system (traction power system). In addition to this, literature does not provide simulation tools to predict cyber-attack penetration probabilities in multiple stages of an attack. Thus, this research provides an easy model using MATLAB to simulate cyber-attack penetration probabilities at various stages of the cyber kill chain model.

The objective of this research is to analyze and simulate cyber-attacks to predict cyber-attack penetration probabilities. The scope of this research is that it does not go into the detail on the various kill chain models. Rather, it applies a simple cyber kill chain model to the railway as an initial step. The limitation of this research is scarcity of real cybersecurity data.

3 Attack propagation in seven stages of cyber kill chain model

An initial CKC model was developed by Lockheed Martin (2009). The seven stages of this model are:

- *Reconnaissance* It is the planning stage of the cyber-attack. The adversary searches for and gathers information about the target through social sites, conferences, blogs, mailing lists and other network tracing tools.
- *Weaponize* The second stage of the model is the operation preparation stage. This stage involves the coupling of a remote access Trojan (RAT) with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer).
- *Delivery* The third stage of the model is the operation launch stage where a weapon is transmitted to the targeted environment.
- *Exploitation* At this stage, exploit is triggered to silently install/execute the delivered payload. The most frequent exploits are operating system, network and application/software level vulnerabilities.
- *Installation* This stage involves the installation of back door remote access Trojans (RATs) and the maintenance of persistence inside the targeted environment.
- *Command and control (C2)* After the successful installation of a back door, the adversary tries to open a two-way communication channel to enable the attacker to control the targeted environment remotely. Once the C2 channel is established, the adversary has “hands on the keyboard” access inside the targeted environment.
- *Act on objective* In the last stage of the model, the adversary achieves the desired attack goals. These goals can be loss of confidentiality, integrity or availability of an asset.

Figure 1 represents the propagation of cyber-attack penetrations at each stage of the cyber kill chain model. P_{attack} is the probability of initiation of cyber-attack and $S1$ – $S7$ are the seven stages of cyber kill chain model.

$Pc11$, $Pc12$, $Pc13$, $Pc14$... $Pc73$, $Pc74$ are the 28 security controls implemented by the defender to minimize the risk of cyber-attacks.

$P\eta1$ to $P\eta7$ are the probabilities of propagation of cyber-attack penetrations from $S1$ – $S7$.

Table 1 shows example of these security controls to be implemented by the defender at each stage of the CKC model. $Pc1$ – $Pc7$ are the probabilities of at least one security control will defend at each of the stage of CKC model.

4 Research methodology

Due to lack of real cybersecurity data, this research is conducted by using simulation in MATLAB. Figure 2 shows flowchart of the research methodology. This research started with generating relevant cybersecurity data from the perspective of both defender and attacker. At the defender side, this research has implemented four security controls at each stage of CKC model. Next, it calculated the probability that out of four security controls at least one will work at each stage of the CKC model. At the attacker side, cyber-attacks were launched using poisson probability density function. After all the simulated cybersecurity data has been generated, the next step of the research methodology is data analysis. During data analysis, this research defined four cases, which are explained at Sect. 6 of this research paper. In the last, cyber-attack penetration probabilities have been visualized and important decisions can be taken in order to minimize the risk of these attacks.

5 Overview of the model

5.1 Notations

The notations used in this research work are as follows:

5.1.1 Intrusion/cyber-attack rates

P_{attack} It is the probability of initiation of cyber-attack. It can be modeled as a random process of arrival with a Poisson Probability Density Function (PDF) (Eq. 1). This

Fig. 1 Seven stages of cyber kill chain

Table 1 Example of security controls at each stage of CKC model

Stage	Example of security control
Reconnaissance	Cyber hygienic workforce of railway Scan the railway network internally and externally using vulnerability-scanning tools Securely dispose of sensitive and confidential railway data Perform proactive penetration testing
Weaponize	Conduct cybersecurity education and improve awareness of railway workforce Conduct detailed analysis of possible attack types to proactively identify indicators of adversaries' actions Share and utilize threat intelligence to learn about adversaries' tactics and techniques Identify weaponization attributes to prevent attacks reaching later stages
Delivery	Use email filtering services Detect anomalous commands not stemming from the normal remote control center Use role-based access control (RBAC) to limit who has access to the railway enterprise network, SCADA system (supervisory control and data acquisition system) or European Train Control System (ETCS) system Require approved cryptographic algorithms for authentication and message integrity on the railway signalling network
Exploitation	Perform patching Use network intrusion detection system Remove remote administration capabilities from Web platforms Use security toolkits to prevent exploits
Installation	Implement firewalls Authenticate users so that physical access to railway assets does not automatically grant logical access Require multi-factor authentication to gain access to sensitive railway information Generate alerts on who has made software additions or modifications
Command and control (C2)	Block communication to the external C2 server Automatically isolate infected devices Perform internal reconnaissance to detect and block the attacker Use DNS blackholing
Act on objective	Use data loss prevention technology Configure email systems and web proxies to prevent sensitive and confidential railway data from being sent Implement internal intrusion detection system, intrusion prevention system and other controls within the railway network to detect and mitigate unauthorized lateral movement Use data-at-rest encryption schemes

function is commonly used for a variety of arrival applications including cyber-attacks (Shourabi 2015). The probability of k occurrences of cyber-attack during any specified interval of time can be expressed as:

$$P(k \text{ events in interval}) = \lambda^k e^{-\lambda} / k! \quad (1)$$

where λ is the average number of events per interval and k takes values 0, 1, 2, 3,

5.1.2 Model parameters

- S : It is the finite set of stages $S = \{S1, S2, S3, S4, S5, S6, S7\}$ with $S7$ as the last stage where data get compromised.
- Pfi : It is the probability of pre-filtering (intrusion detection system) at each stage of CKC.

- C : It is the finite set of 28 security controls $C = (Pc11, Pc12, Pc13, Pc14, Pc21, Pc22, Pc23, Pc24, Pc31, Pc32, Pc33, Pc34, Pc41, Pc42, Pc43, Pc44, Pc51, Pc52, Pc53, Pc54, Pc61, Pc62, Pc63, Pc64, Pc71, Pc72, Pc73, Pc74)$ with four controls at each stage to defend against the cyber-attack (Eq. 2).

$$\underbrace{\sum_{i=1}^{i=4} Pcji}_{\text{Stage } j=1} \underbrace{\sum_{i=1}^{i=4} Pcji}_{\text{Stage } j=2} \dots \underbrace{\sum_{i=1}^{i=4} Pcji}_{\text{Stage } j=7} \quad (2)$$

These security controls include Intrusion Detection and Prevention System, HoneyPot, Web Analytics, Threat Intelligence, Video Surveillance, Vulnerability Scanning, Penetration Testing, Firewall, Proxy Filter, Anti-virus, and most of them were listed in the previous work (Kour et al. 2020).

Fig. 2 Flowchart of research methodology

- P_{ci} : It is the probability of at least one security control will work at stage S_i of CKC, $i = 1, 2, \dots, 7$.
- $P_{\eta 1}$: It is the probability of attack penetration at stage S_1 .
- $P_{\eta i}$: It is the probability of attack penetration at stage S_i , $i = 2, 3, \dots, 7$.
- $Loss$: It is the malicious cyber activity cost in Euro. Around 30% of Swedes were exposed to cybercrime, resulting in total financial losses of 3.14 billion Euros in 2018 (Ahlstrom 2019).
- $Risk$: Risk is related to three elements: Threat, Vulnerability, and Asset (ISO/IEC 27005:2011). In this model, risk is a function of probability of cyber-attack, probability that defensive mechanism can exploit the vulnerabilities present and the loss to the asset as consequence.
- Uc : It is the updated security control which will be implemented after assessing cyber-attack for a period of one month.

5.1.3 Model functions

- $f(P_{_attack}, P_{c1})$: It calculates the probability of infiltration at the first stage of CKC.
- $f(P_{\eta(i-1)}, P_{ci})$: It calculates the probability of propagation of cyber-attack to next stage of CKC with i as current stage and $i - 1$ as previous stage, $i = 2, 3, \dots, 7$.
- $f(P_{ci}, P_{fi})$: It calculates the probability of filtering the attack traffic with a detection mechanism. The success of an attack depends upon this detection mechanism to thwart the attack.
- $f(P_{_attack}, f(P_{ci}), loss)$: It calculates the risk of penetration of cyber-attack at each stages of the CKC model.

$$Risk = Threat \times Vulnerability \times Asset \quad (3)$$

- $f(Uc, Pc, P_{\eta}, P_{attack})$: It calculates last stage penetration probabilities with updated controls for each month.

5.2 Assumptions

1. This research assumes the probability of cyber-attack arrival as a Poisson Probability Density Function (PDF) (Shourabi 2015). According to University of Maryland, hackers attack every 39 s (University of Maryland, 2007). In addition to this, Cisco reported that Asia-Pacific companies receive 6 cyber threats every minute (Cisco 2018). McAfee recorded 478 new

cyber threats every minute, 8 every second with an 18% increase in the number of reported security incidents across Europe (McAfee 2019). This research assumed 8 cyber-attacks every second and simulated attack arrival as Poisson PDF.

2. This research assumes four security controls implemented at each stage with at least one security control to work at each stage to defend against the cyber-attacks. But these security controls can be extended further based on the requirements of the defender.
3. This research assumes a prefilter which is cyber-attack detection mechanism at each of the seven stages of CKC. This detection mechanism assumes an exponential pdf for detection (Shourabi 2015).
4. This research assumes three cases of probabilities of security controls at third, fourth and fifth stage of CKC as (20–25%), (26–30%), and (31–35%). In addition to this, the probabilities of security controls for rest four stages (1–2 and 6–7) are 1–5%. The security control probabilities at first two stages are less, because these two stages are bound towards attacker side and from delivery stage actual attack happens. But these probabilities can be extended further based on the requirements of the defender.
5. This research assumed that the Loss due to cyber-attack is 3.14 billion Euros in a year (Ahlstrom 2019).

6 Simulation cases

This research considers following cases for simulating the penetration probabilities:

6.1 Case 1 (detection mechanism)

This case simulates the cyber-attack penetration probabilities at all the seven stages when attack detection mechanism as prefiltering is applied and when no prefiltering mechanism is applied at each of the seven stages (Fig. 3). In Fig. 3a, b, $P_{\eta 1}-P_{\eta 7}$ are the next stage cyber-attack penetration probabilities and $P_{c1}-P_{c7}$ are the security controls which are at least working at each stage of the CKC. In Fig. 3b, $P_{f1}-P_{f7}$ are the prefilters implemented at each stage of CKC. This case will estimate how much of the cyber-attack penetration probability will be reduced by using prefilter in the form of cyber-attack detection mechanism.

6.2 Case 2 (variable controls)

This case simulates the cyber-attack penetration probabilities at all the seven stages when security controls at third,

fourth and fifth stages are having variable probabilities (Fig. 4). The control probabilities at first two stages are less because these two stages are bound towards attacker side and from delivery stage actual attack happens. Further, control probabilities at last two stages are assumed less for simulation in this research but can be extended further based on the requirements of the defender.

This case considers three cases of security control probabilities:

1. Probabilities of four controls at delivery, exploit and install stages are between (20 and 25%).
2. Probabilities of four controls at delivery, exploit and install stages are between (26 and 30%).
3. Probabilities of four controls at delivery, exploit and install stages are between (31 and 35%).

The rest of the four security controls' probabilities are between 1 and 5% for all the three cases. This simulation considers that out of four security controls at least one will work. Therefore, the probability that at least one control is defensive is:

$$P(\text{at least one control is defensive}) = 1 - (\text{None is defensive}) \quad (4)$$

6.3 Case 3 (equalizer)

This case considers that probability of each of the 25 security controls out of 28 is same except the three controls at any one stage (Fig. 5). This case will estimate the impact of changing security controls on the last stage penetration.

These variable controls are implemented at each of the stages in seven iterations to calculate the penetration probability at last stage.

6.4 Case 4 (learning curve)

This case is a feedback learning criterion that simulates the penetration probabilities after assessing the cyber incidents and then improving the security controls for similar types of cyber-attacks in future (Fig. 6).

This research has undertaken this case because it will help the defender to learn from the attack and reconsider the security controls to minimize the risk of similar type of cyber-attacks in future. This simulation considers that every month the cyber-attacks will be assessed, and then security controls were updated based on the attack penetrations. The following expression is used to calculate updated control for each simulated month:

$$Uc = P_{\eta 7}(\text{Previous Month}) * \text{Updated Percentage}/100 + P_{c1}(\text{Previous Month}) \quad (5)$$

Fig. 3 Cyber-attack penetrations without prefilter **a** and with prefilter **b**

Fig. 4 Three cases of security controls

Fig. 5 Changing security controls at each stage of CKC

Equation 5 shows how every month the updated security control probability (U_c) is calculated after assessing cyber-attack for 1 month. The security control will be updated based on the attack's penetration probability at last stage during previous month. After calculating updated security control probability, new penetration probabilities were simulated using following function:

$$\text{function}(U_c, P_c, P_{\eta}, P_{attack}) \quad (6)$$

This function is called for each month to draw penetration probabilities with new updated controls each time.

7 Simulation results and discussion

MATLAB has been used for the simulation of cyber-attack penetration probabilities. All the discussed cases have been simulated in this research.

Case 1 results and discussions Figure 7 shows cyber-attack penetration probabilities at each stage of the cyber kill chain model. Green lines show that there is a prefilter in the form of detection mechanism implemented at each of the stage of CKC. Red line on the other hand, shows that there is no prefilter implemented at any of the stage. Figure 7 clearly indicates that after implementing prefilter at each stage of CKC, the attack penetration probabilities can be reduced. For example, in Fig. 7 five cases of cyber-

Fig. 6 Feedback loop showing security controls enhanced at every next iteration

attacks have been presented that shows how these attacks will penetrate within each of the stages with and without cyber-attack detection mechanism. For instance in Figs. 7 and 8, with the cyber-attack probability of 0.13953, penetration probability at stage 2 is 0.1151 and 0.07865 without and with detection mechanism respectively. More cases of cyber-attack and penetration probabilities at second stage of the CKC are presented in the Fig. 8. These results clearly indicate that after implementing prefilter in the form of detection mechanism at each stage of CKC, the cyber-attack penetration probabilities can be reduced.

Case 2 results and discussions This case considers three cases of security controls' probability at third, fourth and fifth stages of the CKC i.e. (20–25%), (26–30%), and (31–35%). In these three cases, it has been indicated that with the increase in security controls, the cyber-attack penetration probabilities will decrease. In Fig. 9 it can be seen that with cyber-attack probability of 0.1241, the cyber-attack penetration at exploitation stage of CKC decreases from 0.0069 to 0.0038 to 0.0012, when security controls' probability is (20–25%), (26–30%), and

(31–35%) respectively at delivery, exploit and install stages (also shown as highlighted value in Fig. 10). Few more simulated results of penetration probability values at exploitation stage are given in Fig. 10, when security controls are (20–25%), (26–30%), and (31–35%).

Thus, with the real cybersecurity data related to cyber-attack and security controls probability, this simulation will help to predict attack penetrations at each stage of the cyber kill chain.

Case 3 results and discussions Figure 11 represents the result of an equalizer, where the probability of each of the 25 security controls out of 28 is same except the three controls at any one stage. The displayed results are for 1, 3, 5 and 7 stages (reconnaissance, delivery, installation, and act on objective) of CKC model. These variable controls are implemented at each of the stages in seven iterations to calculate the penetration probability at last stage. The result shows that when the sum of probabilities of controls is same at any stage, penetration at the last stage will remain same and position of controls does not matter.

Fig. 7 Cyber-attack penetration probabilities at each stage of cyber kill chain model

Fig. 8 Cyber-attack and penetration probabilities at second stage of cyber kill chain

Attack	Second_Stage_Pene_Without_Filter	Second_Stage_Pene_With_Filter
0.0027	0.0022	0.0015
0.0107	0.0089	0.0060
0.0286	0.0236	0.0161
0.0573	0.0472	0.0323
0.0916	0.0755	0.0516
0.1221	0.1007	0.0688
0.1396	0.1151	0.0786
0.1396	0.1151	0.0786
0.1241	0.1023	0.0699
0.0993	0.0819	0.0559
0.0722	0.0595	0.0407
0.0481	0.0397	0.0271
0.0296	0.0244	0.0167

Case 4 results and discussions Figure 12 shows learning curve results; that after detecting cyber-attacks, these attacks were assessed so that future attacks can be minimized. Based on assessment result, security controls are improved (refer Fig. 6) so that penetrations can be reduced.

Figure 12 shows that attack penetrations are decreasing with updating security controls. This simulation considers that after assessing the cyber-attacks, security controls are enhanced or updated with 10% successively for each attack for consecutive 4 months. Thus, it can be seen clearly in

Fig. 12 that last stage penetrations are decreasing with 10% increase in controls each time in four consecutive months for three variable cases of security controls i.e. when security controls lie between (20 and 25%), (26 and 30%), and (31 and 35%).

Other results and discussions Figure 13 shows the risk of cyber-attack penetration per person in Euro at the last stage of the CKC with three cases of security controls at delivery, exploit and install stages as 20–25%, 26–30%, and 31–35%. Risk is related to three elements: Threat,

Fig. 9 Cyber-attack penetration probabilities with varied security controls at 3–5 stages of CKC

Attack	Exploit_Stage_Pene_With_Control_20_and_25	Exploit_Stage_Pene_With_Control_26_and_30	Exploit_Stage_Pene_With_Control_31_and_35
0.0027	1.4953e-04	8.2891e-05	2.5757e-05
0.0107	5.9814e-04	3.3156e-04	1.0303e-04
0.0286	0.0016	8.8417e-04	2.7474e-04
0.0573	0.0032	0.0018	5.4947e-04
0.0916	0.0051	0.0028	8.7916e-04
0.1221	0.0068	0.0038	0.0012
0.1396	0.0078	0.0043	0.0013
0.1396	0.0078	0.0043	0.0013
0.1241	0.0069	0.0038	0.0012
0.0993	0.0055	0.0031	9.5266e-04
0.0722	0.0040	0.0022	6.9284e-04

Fig. 10 Penetration probabilities for exploitation stage when security controls are (20–25%), (26–30%), and (31–35%)

Fig. 11 Penetration probabilities at reconnaissance, delivery, installation, and act on objective stage of CKC

Fig. 12 Last stage penetration probabilities with updated (improved) security controls

Fig. 13 Cyber-attack risk with varying security controls at delivery, exploit, and install stages

Vulnerability, and Asset. In this model, risk is a function of probability of cyber-attack, defensive mechanism that can exploit vulnerabilities present and the loss to the asset as consequence. Loss in this model is the total financial losses of 3.14 billion Euros caused due to malicious cyber activity where around 30% of Swedes were exposed to cybercrime (Ahlstrom 2019). Thus, loss per person due to this cyber-crime is 1152.83 Euro (3.5 Billion/30% of 10.12 Million Swedish population in year 2018). Figure 13 data point shows that risk/person in euro reduces from 3.02 to 2.17 to 1.99 when attack probability is 0.099.

8 Conclusion and future research directions

This research simulates and predicts cyber-attack penetrations in the presence of various security controls. This research concludes following points:

- Cyber-attack detection mechanism in the form of prefilter at each stage of the cyber kill chain will reduce the attack penetrations at each stage.
- These penetrations will further reduce with increase in the probabilities of security controls to defend against these cyber-attacks.
- Next, it was inferred that when the sum of probabilities of controls is same at any stage, penetration at the last stage will remain same and position of controls does not matter.
- In addition to this, simulation results show that after assessing last stage penetrations to improve the security controls will further reduce the future cyber-attack.

In future, this research will consider cyber-attack penetration probabilities in combined extended cyber kill chain and industrial control system (ICS) cyber kill chain.

Acknowledgements Open access funding provided by Luleå University of Technology. The authors would like to thanks Luleå Railway Research Center (JVTC) for sponsoring research work.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Ahlstrom T (2019) Sweden: cyber security. Retrieved from <https://www.export.gov/article?id=Sweden-Cyber-Security>. Accessed 13 Aug 2019
- Alpcan T, Buchegger S (2010) Security games for vehicular networks. *IEEE Trans Mob Comput* 10(2):280–290
- Bahamou S, Ouadghiri E, Driss M, Bonnin J (2016) When game theory meets VANET's security and privacy. Paper presented at the proceedings of the 14th international conference on advances in mobile computing and multi media, pp 292–297
- Ciancamerla E, Minichino M, Palmieri S (2013) Modeling cyber attacks on a critical infrastructure scenario. Paper presented at the IISA 2013, pp 1–6
- Ciprnet (2013) Critical infrastructures preparedness and resilience research network. EU project. Retrieved from <https://www.ciprnet.eu/home.html>. Accessed 13 Aug 2019
- Cisco (2018) Asia pacific security capabilities benchmark study. Retrieved from https://www.cisco.com/c/dam/global/en_au/products/pdfs/executive_summary_cisco_2018_asia_pacific_Security_capabilities_benchmark_study.pdf. Accessed 13 Aug 2019
- eTrax (2016) Railway traction power analysis | rail power system software. Retrieved from <https://etap.com/solutions/railways>. Accessed 13 Aug 2019
- Grube P, Nunez F, Cipriano A (2011) An event-driven simulator for multi-line metro systems and its application to santiago de chile metropolitan rail network. *Simul Model Pract Theory* 19(1):393–405
- He X (2017) Threat assessment for multistage cyber attacks in smart grid communication networks (doctoral dissertation, universität passau). Threat assessment for multistage cyber attacks in smart grid communication networks
- Karnouskos S (2011) Stuxnet worm impact on industrial cyber-physical system security. Paper presented at the IECON 2011-37th annual conference of the IEEE industrial electronics society, pp 4490–4494
- Kour R, Aljumaili M, Karim R, Tretten P (2019) eMaintenance in railways: issues and challenges in cybersecurity. *Proc Inst Mech Eng F J Rail Rapid Transit*. <https://doi.org/10.1177/0954409718822915>
- Kour R, Thaduri A, Karim R (2020) Railway defender kill chain to predict and detect cyber-attacks. *J Cyber Secur Mobil* 9(1):47–90
- Lockheed Martin (2009) Cyber kill chain®. Retrieved from <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>. Accessed 13 Aug 2019
- Martin L (2014) Cyber kill chain®. <http://Cyber.Lockheedmartin.Com/Hubfs/GainingtheAdvantageCyberKillChain.Pdf>. Accessed 13 Aug 2019
- McAfee (2019) McAfee labs reports record. Retrieved from https://www.mcafee.com/enterprise/es-es/about/newsroom/press-releases/press-release.html?news_id=20180311005028. Accessed 13 Aug 2019
- Mejri MN, Achir N, Hamdi M (2016) A new security games based reaction algorithm against DOS attacks in VANETs. Paper presented at the 2016 13th IEEE annual consumer communications and networking conference (CCNC), pp 837–840
- NS-3 (2019) Network simulator. Retrieved from <https://www.nsnam.org/>. Accessed 13 Aug 2019
- OpenPowerNet Version, 1. 8. 1. (2019) Traction power supply and train performance simulation software. Retrieved from <http://www.openpowernet.com/>. Accessed 13 Aug 2019
- OpenTrack. (1990). Simulation of railway networks. Retrieved from http://www.opentrack.ch/opentrack/opentrack_e/opentrack_e.html. Accessed 13 Aug 2019

- OPNET. (2019). Opnet is now part of riverbed steelcentral™. Retrieved from <https://www.riverbed.com/se/products/steelcentral/opnet.html>. Accessed 13 Aug 2019
- Ross RS, Katzke SW, Johnson LA, Swanson MM (2007) Recommended security controls for federal information systems | NIST (No. Special Publication (NIST SP)-800-53 rev 2) o title
- Rybníček M, Tjoa S, Poisel R (2014) Simulation-based cyber-attack assessment of critical infrastructures. Paper presented at the Workshop on enterprise and organizational modeling and simulation, pp 135–150
- Sanjab A, Saad W, Başar T (2017) Prospect theory for enhanced cyber-physical security of drone delivery systems: a network interdiction game. Paper presented at the 2017 IEEE international conference on communications (ICC), pp 1–6
- Sedjelmaci H, Senouci SM, Ansari N (2016) Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: a bayesian game-theoretic methodology. *IEEE Trans Intell Transp Syst* 18(5):1143–1153
- Shourabi NB (2015) A model for cyber attack risks in telemetry networks. International Foundation for Telemetering, San Diego
- Stouffer K, Lightman S, Pillitteri V, Abrams M, Hahn A (2014) NIST special publication 800-82, revision 2: guide to industrial control systems (ICS) security. National Institute of Standards and Technology
- Teo Z, Tran BAN, Lakshminarayana S, Temple WG, Chen B, Tan R, Yau DK (2016) SecureRails: towards An open simulation platform for analyzing cyber-physical attacks in railways. Paper presented at the 2016 IEEE region 10 conference (TENCON), pp 95–98
- Thaduri A, Aljumaili M, Kour R, Karim R (2019a) Cybersecurity for eMaintenance in railway infrastructure: risks and consequences. *Int J Syst Assur Eng Manag* 10:149–159
- Thaduri A, Aljumaili M, Kour R, Karim R (2019b) Cybersecurity for eMaintenance in railway infrastructure: risks and consequences. *Int J Syst Assur Eng Manag* 10(2):149–159. <https://doi.org/10.1007/s13198-019-00778-w>
- University of Maryland (2007) Study: hackers Attack every 39 seconds. Retrieved from <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>. Accessed 13 Aug 2019
- Yao X, Zhao P, Qiao K (2013) Simulation and evaluation of urban rail transit network based on multi-agent approach. *J Ind Eng Manag (JIEM)* 6(1):367–379

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.