Development of an Attack Case Generation Model Based on the Characteristics of Digital Assets of Nuclear Power Plants

Minseok Hur[1*][0009-0008-8889-7516], Eunji Lee[2*], Sooyon Seo[1][0009-0002-5595-6627], Jaeho Hwang[1][0009-0005-6761-2428], Dongmin Kim[3][0009-0009-7948-5947], Moohong Min[4**][0000-0001-8979-1344], and Aram Kim[5**][0000-0003-1030-3534]

[1] Department of Immersive Media Engineering, Sungkyunkwan University, Humanities and Social Sciences Campus, 25-2, Sungkyunkwan-ro, Jongno-gu, 03063 Seoul, South Korea alexhur3535@skku.edu sooyon1119@g.skku.edu ashiereki@g.skku.edu

[2] Department of Forensic Sciences, Sungkyunkwan University, Humanities and Social Sciences Campus, 25-2, Sungkyunkwan-ro, Jongno-gu, 03063 Seoul, South Korea jamemanionda@g.skku.edu

[3] School of Convergence Data Science Convergence Major, Sungkyunkwan University, Humanities and Social Sciences Campus, 25-2, Sungkyunkwan-ro, Jongno-gu, 03063 Seoul, South Korea ehdals5744@g.skku.edu

[4] Department of Computer Education/Social Innovation Convergence Program, Sungkyunkwan University, Humanities and Social Sciences Campus, 25-2, Sungkyunkwan-ro, Jongno-gu, 03063 Seoul, South Korea iceo@skku.edu

[5] Department of Information Security, University of Suwon, 17, Wauan-gil, Bongdam-eup, Hwaseong-si, Gyeonggi-do, South Korea aramkim@suwon.ac.kr

[*] These authors equally contributed to this paper

[**] Corresponding Author: Moohong Min, Aram Kim

Abstract. As cyberthreat technologies develop, threats to critical industrial facilities are increasing. To prepare for these threats, Industrial Control System (ICS) facilities are developing risk management methodologies such as risk assessment models. Various attack scenarios are required to validate risk assessment methodologies. To construct these attack scenarios, attack paths and digital assets must be identified and analyzed. While a considerable amount of research has been done on digital assets, a very small number of research has been conducted on creating attack cases. Even though the data and the framework regarding the security of ICS facilities have been defined, industrial facilities are not practically utilizing them for security. This study proposes a model that can generate attack cases using asset characteristics, pathways, vulnerabilities, and attack methods. NEI 13-10, MITRE ATT&CK, Technical Assessment Methodology (TAM), Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE) are applied to each element. The proposed method is implemented on the web, allowing attack cases to be generated simply by manually adding data.

Keywords: Attack Case Generation, Asset, Attack Pathway, Vulnerability, Nuclear Power Plant.

1 Introduction

“Assets” encompass various elements, including information, hardware, software, facilities, and intangible assets, which an organization must protect [1]. In specific, “digital assets” refer to digitally based devices, systems, and networks such as computers, information systems, and network systems. The digital assets of nuclear facilities are exposed to various threats, and the attack techniques to threaten cyberspace, such as Stuxnet [2], are becoming increasingly sophisticated and advanced.

To mitigate vulnerabilities, nations operating nuclear power plants, such as South Korea, the United States, Canada, and the United Arab Emirates, require nuclear operators to establish and implement cybersecurity programs by providing regulatory guides [3-6]. Regulatory Guide (RG) 5.71 requires risk assessment activities and therefore, nuclear power plant operators should apply effective risk assessment and attack case generation methods to assess risks [7, 8].

Attack cases have not been studied much considering Industrial Control Systems (ICS). Manually writing and utilizing attack cases are not only inefficient in terms of time and cost but also do not guarantee that all possible scenarios are generated. To overcome the limitations of existing attack generation method, this paper develops an attack case generation model using asset, threat, and vulnerability information as standardized inputs for efficient risk assessment.

The contributions of this paper are as follows.

- Instead of the conventional method that requires individual consideration of attack scenarios, attack scenarios are derived with minimized effort.
- By categorizing cyberattacks, attack confrontation plans for each digital asset can be built.
- Experts can work more efficiently by building a scalable attack case model.

2 Related Work

2.1 Literature Review

Cybersecurity of Nuclear Power Plants. Research on the security of nuclear power plants has been conducted on the assessment of assets and risks, and on the generation of attack scenario generation. Critical Digital Assets (CDAs) were organized into detailed characteristics for applying security measures in a phased approach [9]. A method using software to automatically identify and testing CDAs through a network model for a real nuclear reactor was proposed in [10]. A model based on the CNN algorithm to detect attacks in industrial control systems was proposed in [11]. A CNN model trained on offline assets achieved a 97% accuracy score.

Risk Assessment Models. Vulnerability risk assessment model composed of a vulnerability section (reconnaissance and delivery), and a risk assessment section (installation, command and control, purpose achievement, and final risk assessment) for the

web was conducted in [12]. The model was evaluated by calculating the risk level in each section. In [13], unknown attacks were predicted through similar attack scenarios using clustering in ICS. The authors of [14] constructed a multidimensional threat assessment method by calculating the probability of an attack and quantified the consequences of the attack. An analysis of the results of applying security controls and assessing risk using Nuclear Energy Institute (NEI) 13-10 and Technical Assessment Methodology (TAM) was done in [15].

Attack Scenario Generation Model. Attack scenarios have been studied in general cyber environments using a diamond model consisting of adversary, capability, infrastructure, victim kill chain modeling, and attack graphs [16]. A method proposed in [17] identified attack paths by representing the asset and vulnerability databases as a graph and by deleting nodes according to the conditions of the attacker and propagation length. In [18], the authors divided entities into devices, vulnerabilities, components, domains, and Tactic&Tech. Then they generated various attack scenarios by classifying them into a list of vulnerabilities and affected components for each device.

Most studies did not have specific asset analysis or did not use existing data such as MITRE ATT&CK or TAM.

2.2 Theoretical Background

Asset Characterization Methodology: NEI 13-10. NEI 13-10 is a document issued by Nuclear Energy Institute (NEI) to the Nuclear Regulatory Commission (NRC) to apply security controls. Risk assessment is conducted to protect digital assets from cyber threats in nuclear power plants. According to the importance, the asset is divided into Safety-Related or Important-to-Safety. Cybersecurity measure evaluation is based on classifying the class and determining the degree of impact. Classes are divided into hardware and software, and subclasses are divided into attributes such as Human-Machine Interface (HMI) and communication. Asset characteristics are organized based on a study that extracted characteristics by analyzing NEI 13-10 [19]. The attribute extraction allowed us to represent the main classification in a sequence diagram as shown in Fig. 1.

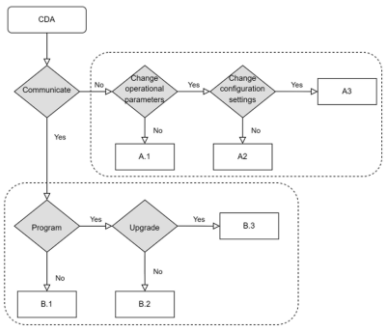

Fig. 1. Attribute classification according to NEI 13-10.

Vulnerability Characterization Methodology: CVE. Common Vulnerabilities and Exposures (CVE) is a unique notation that identifies and defines publicly known cybersecurity vulnerabilities which are flaws or holes in software or hardware that can be exploited by a security attack. CVE was officially launched by the National Cybersecurity FFRDC, which is operated by the MITRE Corporation.

Threat Characterization Methodology: MITRE ATT&CK for ICS. MITRE, a non-profit research and development organization, developed the MITRE ATT&CK framework based on actual attack cases[1]. The framework formats an attack process into tactics, techniques, procedures, and attack software. The MITRE ATT&CK Matrix provides information on attack behaviors which is categorized into Enterprise, Mobile, and ICS. MITRE ATT&CK for ICS targets industrial system control environments, which are similar to nuclear power plant critical assets.

Threat Analysis and Risk Assessment Model: TAM.
Technical Assessment Methodology (TAM) is a cybersecurity assessment and action methodology for power and power generation control systems published by the Electric Power Research Institute (EPRI) [19]. It identifies the exploit sequence that exists in each asset, sets the minimum-security level that can mitigate it, and ensures that all security measures applied to the asset are at or above the minimum-security level. It also evaluates the performance of cybersecurity measures by quantifying the effectiveness and appropriateness of the identified cybersecurity measures. Fig. 2 depicts the overall process of TAM.

The proposed model utilizes Step 1 of the three steps. After specifying the assessment scope of the asset, it identifies the characteristics of the attack area of the asset and derives the exploit sequence.

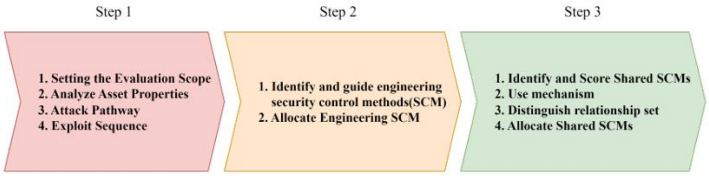

Fig. 2. The overall process of TAM.

3 Attack Case Generation Model Development

3.1 Design of the Attack Case Generation Model

The attack case generation model refers to the Exploit Sequence of the TAM. The model is divided into 4 steps as shown in Fig. 3. The input for each step is standardized and designed as a variable structure so that they can be updated periodically or be

[1] MITRE ATT&CK. https://attack.mitre.org/

applied to other general IT elements. The sequence of the model is comprised of 4 steps. In step 1, asset characteristics are defined from the Asset. In step 2, Attack Pathways derive possible attack points for each characteristic element. The attack points and vulnerabilities are combined in step 3. Finally, an attack case is generated in step 4.

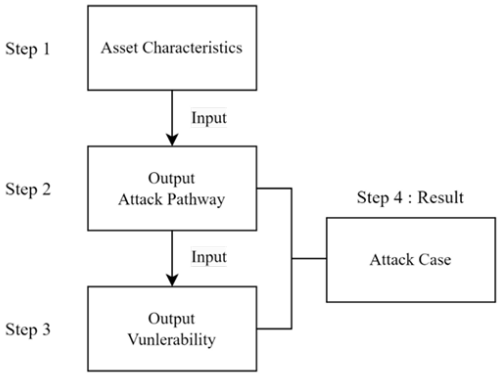

Fig. 3. Sequence of the proposed model.

3.2 Standard Input Shape

Step 1: Asset Attributes as an Input. In this step, asset attributes are categorized based on the functional classification of NEI 13-10 and prior research on CDA [20]. NEI 13-10 provides classification criteria for CDA but covers only 0-2 levels, which are inappropriate to accommodate various digital assets. Therefore, in addition to Classes A.1-B.3 of NEI 13-10, we also defined Class C which includes IT assets as shown in Fig. 4. To include the 3-5 levels of the Purdue model and IT assets that are not covered by NEI 13-10, we used NIST's IT Asset Management to divide the assets into security, network, and other devices. We excluded items related to servers as they are not suitable for nuclear power plant asset classification. The combination of the attributes determines the value of the next step.

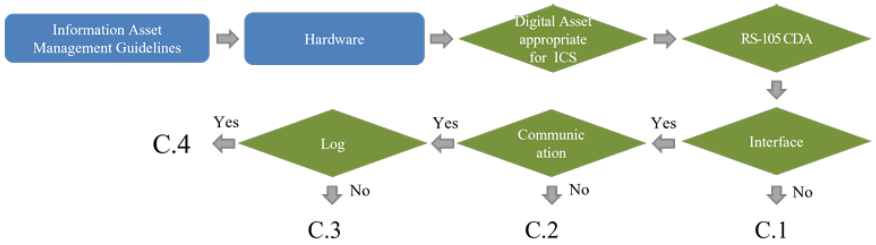

Fig. 4. Classification of C Class asset attributes.

Step 2: Attack Pathway Standard as an Input. The Exploit Sequence-Pathway of TAM is referred to generate an attack pathway. A standard input form is generated by analyzing the characteristics of the asset and the initiation path of the threat as described in the MITRE ATT&CK for ICS. Vulnerable elements are categorized into Access, Wired Network, Portable Media, Supply Chain, and Software. Resources and capabilities are added as minor categories. Asset attributes are compared with these categories, and according to the elements, the Vulnerability is determined. The code of the Attack Pathway is an abbreviation of the type of name (e.g., Physical Access – PS) for a large classification, followed by the abbreviation of the subcategory (e.g., Mechanical Access – PS/M).

Step 3: Vulnerability Standard as an Input. This step utilizes the vulnerability analysis results of open-source CVEs, a list of vulnerability expressions, and Common Weakness Enumerations (CWE), a list consisting of security weaknesses in software and hardware that can cause security problems for data input. A list corresponding to the resource characteristics of the system is then created. The value from the previous step is linked to the corresponding vulnerability and multiple vulnerability values can be generated for each attack pathway element.

Step 4: Creation of the Attack Case. Asset, Attack Pathways, and Vulnerability is linked to create an Attack Case as shown in Table 1. When the result value of the Vulnerability is determined through the Asset attribute value, the Attack Case value is generated. Attack case codes can be presented in the form of [Asset Class]-[Attack Pathways Code]-[Vulnerability Code].

Table 1. Example of Attack Cases. AP stands for Attack Pathways code.

Attack Cases			
Code	AP	Vul.	Description
A1-001	SCWN	V001	Specially crafted packets sent to a port could cause denial-of-service of the affected device. Unexpected restart or shutdown of control system devices.
A1-002	PM	V001	Code execution, memory corruption, or unauthorized access. Transmitting manipulated configuration values.
A1-004	PS	V003	Error in changing configuration setting, operational parameter.

3.3 Development of the Attack Case Model and the Database

The base model was created using Excel. The model was applied to 6 assets to show that the inputs can be used to derive threats and vulnerabilities associated with the assets. Based on this model, a database was designed using object-oriented modeling and class diagrams. To use the model, the details of the Asset, Attack Pathway, and Vulnerability are added. Then, classes and descriptions are defined. Finally, the Attack Case is predicted from the interaction of Assets, Attack Pathways, and Vulnera-

bilities and is saved into the database. Fig. 5 depicts the overview diagram of the Attack Case generation.

We deployed a Node js-based attack scenario generation web application according to the design (https://anonymous.4open.science/r/AttackCaseGenerationTool/).

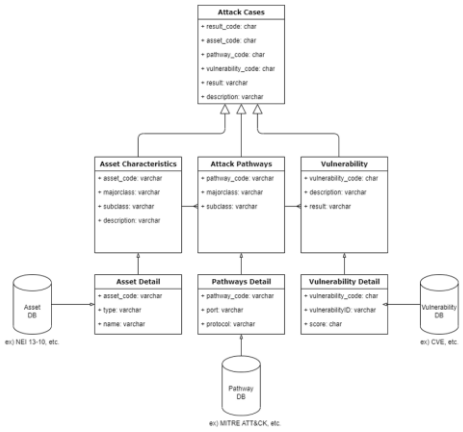

Fig. 5. The overview diagram of the Attack Case generation.

4 Conclusion

In this study, a model that predicts an attack case from the interaction of Assets, Attack Pathways, and Vulnerabilities is presented. The Exploit Sequence referred from TAM was utilized and a standard input form was created in a variable structure for regular updates and applications in other fields. Based on NIST 800-30, we utilized NEI 13-10 for asset characteristics, MITRE ATT&CK for threat characteristics, and Common Vulnerabilities and Exposures (CVE) for vulnerabilities. We also derived a new criterion for Class C IT assets, which were difficult to classify in NEI 13-10. We also developed a web application framework according to the proposed model.

Through further research, the attack cases could be automatically derived through the automation of mapping the vulnerabilities, threat paths, and methods according to the input. It should be conducted in the direction of minimizing errors in attack case generation by specifically developing step-by-step process of converting data into an input of the model.

Acknowledgements

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety(KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission(NSSC) of the Republic of Korea. (No. RS-2024-00403596)

References

1. Lee, Joontaik, et al. "A Study on IT Based Risk Management System Development for Business Continuity Management: Centering on Cases at Automobile Manufacturing Industry." Journal of Society for e-Business Studies 18.2 (2013).
2. Langner, Ralph. "Stuxnet: Dissecting a cyberwarfare weapon." IEEE security & privacy 9.3 (2011): 49-51.
3. USNRC. Cybersecurity programs for nuclear facilities: Rg 5.71-2010. Washington, DC: US NRC, pages 4–20 (2010)
4. KINAC. Rs-015. Technical standard on cyber security for computer and information system of nuclear facilities (2014)
5. Canadian Nuclear Safety Commission et al. Dis-21-03, cyber security and the protection of digital information (2021)
6. Federal Authority for Nuclear Regulation. Fanr-rg-011, cyber security at nuclear facilities (2015)
7. Gonzalez-Granadillo, Gustavo, et al. "Dynamic risk management response system to handle cyber threats." Future Generation Computer Systems 83 (2018): 535-552.
8. Tantawy, Ashraf, et al. "Model-based risk assessment for cyber physical systems security." Computers & Security 96 (2020): 101864.
9. Kim, Sangwoo, Ick-Hyun Shin, and Kook Heui Kwon. "Analysing Current state of Identifying Critical digital assets And Cyber security control for Nuclear Facility." Proceedings of the Korean Institute of Information and Communication Sciences Conference. The Korea Institute of Information and Communication Engineering, 2015.
10. West, Jonathan, et al. "Automatic identification of critical digital assets." 2019 2nd International Conference on Data Intelligence and Security (ICDIS). IEEE (2019)
11. Nedeljkovic, Dusan, and Zivana Jakovljevic. "CNN based method for the development of cyber-attacks detection algorithms in industrial control systems." Computers & Security 114 (2022): 102585.
12. Jin, Hui Hun, and Huy Kang Kim. "A study on web vulnerability risk assessment model based on attack results: focused on cyber kill chain." Journal of the Korea Institute of Information Security & Cryptology 31.4 (2021): 779-791.
13. Zhang, Yaofang, et al. "A risk assessment model for similar attack scenarios in industrial control system." The Journal of Supercomputing 79.14 (2023): 15955-15979.
14. Kim, Aram, et al. "Consider the consequences: a risk assessment approach for industrial control systems." Security and Communication Networks 2022.1 (2022): 3455647.
15. Jung, Daun, et al. "Cyber security controls in nuclear power plant by technical assessment methodology." IEEE Access 11 (2023): 15229-15241.
16. Al-Mohannadi, Hamad, et al. "Cyber-attack modeling analysis techniques: An overview." 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW). IEEE (2016)
17. Polatidis, Nikolaos, Michalis Pavlidis, and Haralambos Mouratidis. "Cyber-attack path discovery in a dynamic supply chain maritime risk management system." Computer Standards & Interfaces 56 (2018): 74-82.
18. Wang, Zibo, et al. "An Automatic Planning-Based Attack Path Discovery Approach from IT to OT Networks." Security and Communication Networks 2021.1 (2021): 1444182.
19. EPRI, "Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation, Revision 1", EPRI (2018)
20. Kim, In-kyung, Ye-eun Byun, and Kook-heui Kwon. "Analysis of the application method of cyber security control to develop regulatory requirement for digital assets in NPP." Journal of the Korea Institute of Information Security & Cryptology 29.5 (2019): 1077-1088.