Study of the Correlation Methodology between Common Vulnerabilities and Sequential Attack Technique

Doyeon Kim*, Seongsu Yoon, Joonseok Kim, Kakyung Kim and Ieckchae Euom

Chonnam National University,
{ehdus928, skymoonight}@jnu.ac.kr, jss8707@naver.com, kakyung98@gmail.com, iceuom@jnu.ac.kr

Abstract

Given the characteristics of the operational technology, prioritizing availability necessitates proactive vulnerability management. Utilizing security verification techniques to understand the intent of attackers is a crucial aspect of mitigating risks and enhancing responses to cyberattacks. However, a significant issue is the difficulty of providing meaningful proactive management due to the lack of consideration for the sequence of attack techniques. Therefore, this study analyzes a methodology for the correlation of sequential attack techniques based on textual descriptions of vulnerabilities. This provides insights into prioritizing vulnerability patches in the operational technology.

Keyword: CVE, ATT&CK Framework, Vulnerability Management, Attack Identification

1 Introduction

In the context of vulnerability management, it is essential to have technologies that identify and verify the intent of attackers for risk mitigation and response. The conventional methods of vulnerability management, as shown in 'existing' in [Figure 1], utilize attack information like CAPEC to reflect dynamic characteristics. However, this approach often lacks a connection with common vulnerability information, which poses a problem.

To address this, this study intends to consider the dynamic characteristics of each vulnerability by utilizing the ATT&CK framework from MITRE corporation, which reflects the attacker's intent, considering the purpose and method of the attacker.

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan Article No. W-6

*Corresponding author: Department of Convergence Security Engineering, Chonnam National University, Gwangju, 611864, Republic of Korea, Tel: + 82-62-530-5791

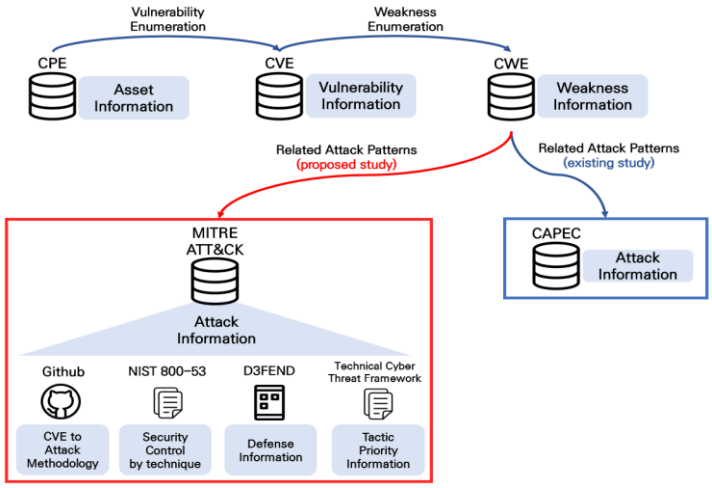

Figure 1: Common Vulnerability and Related Attack Information Association Diagram

However, applying this to operational environment processes is not suitable. Operational environments that prioritize availability cannot implement immediate patches, hence the importance of proactive vulnerability management before an attack occurs. Existing methods of understanding the attacker's intent do not consider the sequence of attack techniques[1], thereby failing to yield meaningful results in proactive management. In response, this study aims to analyze the interconnectivity between common vulnerabilities and attack techniques by utilizing the CVE to Attack methodology provided by CTID, employing the ATT&CK framework to derive sequential attack techniques.

2 Related Work

In this chapter, we discuss the issues with existing research that utilizes the dynamic characteristics of vulnerabilities and common attack pattern information and propose the necessity of vulnerability linkage analysis using TTPs information from MITRE ATT&CK as a solution.

2.1 Analysis of Previous Research on the Correlation between Common Vulnerabilities and Common Attack Pattern Information

In previous research, CAPEC has been utilized to derive attack information, proceeding in a manner as depicted in [Figure 2], where vulnerability information about assets is used to understand attack information about each vulnerability's weaknesses.

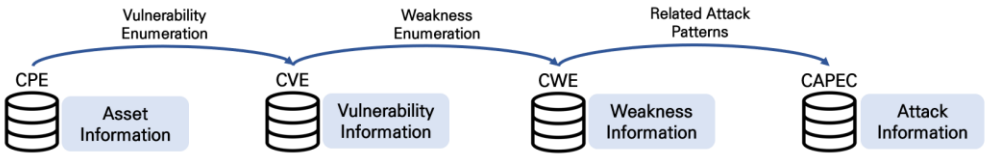

Figure 2: Common Vulnerability and Related Attack Pattern Association Diagram

McLean[2] employs CAPEC to extract cyberattack patterns and, through text-based analysis of CAPEC data itself or its interaction with CWE information, produces visualization results. This provides information on what software weaknesses can be exploited in specific attack scenarios.

Kenta[3] analyzes the similarity of CVE descriptions to link CVE_ID and CAPEC_ID. Utilizing TF-IDF provided by Scikit-learn and Doc2Vec from Gensim, a similarity test is performed for each CVE_ID against all CAPEC_IDs, and the CAPEC_ID with the highest similarity is derived.

Piraeus[4] connects CAPEC by analyzing each CVE description information based on the CVE-CWE, CWE-CAPEC relationship combination. Here, CVE description information is pre-processed using NLTK, and subsequently, the spaCy model provided by the Python library is used to connect to CAPEC_ID through the derived similarity.

The flow of connecting vulnerability and attack pattern information (CAPEC) in the manner described above results in papers as shown in [Table 1].

	Utilized method	Connection Relationship	Result
[2]	Manual	CWE – CAPEC	Mapping number between CWE and CAPEC
[3]	TF-IDF, Doc2Vec	CVE – CWE - CAPEC	Similarity between CVE and CAPEC
[4]	NLTK, spaCy	CVE – CWE - CAPEC	Similarity between CVE and CAPEC

Table 1: Comparative analysis of prior research about correlation between Common Vulnerabilities and Common Attack Pattern Information

A general limitation of existing research is the insufficiency of attack pattern information for common vulnerabilities, resulting in some vulnerabilities not being matched with attack patterns. Therefore, this paper proposes utilizing MITRE ATT&CK, as mentioned in Section 2.2, to identify attack pattern information that maps at a minimum of a 1:1 ratio.

2.2 Attack Technique Information (MITRE ATT&CK)

MITRE ATT&CK serves as a threat intelligence resource, consolidating various cyberattack instances globally, and encompasses a myriad of attack TTPs (Tactics, Techniques, and Procedures) that attackers execute or could potentially employ, as well as attack groups, software, and methods to detect and mitigate each attack technique, including the data sources and data components utilized there in[5].

From 2020 onwards, MITRE ATT&CK undergoes two major updates annually, which are executed across its three versions: Enterprise, ICS, and Mobile. During the update process, tasks such as the addition of new technique entities, modification and deletion of existing entities, and discontinuation of support are performed. Adapting to the dynamic characteristics of the evolving threat environment, the current version 13 of MITRE ATT&CK encompasses 14 tactics, 196 techniques, 138 groups, 22 campaigns, and 740 software[6].

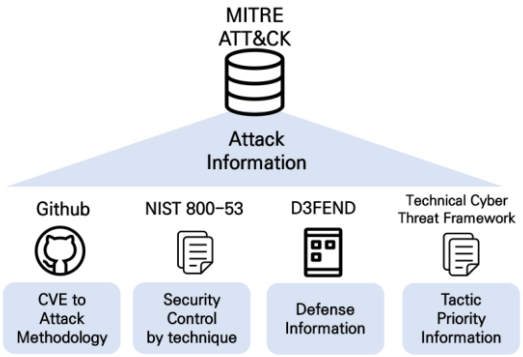

Figure 3: MITRE ATT&CK-Based Documents and Projects

Additionally, there exist documents and projects related to ATT&CK, as depicted in [Figure 3]. Initially, there exists a CVE to Attack methodology[7] in Github format to link each vulnerability with attack techniques, providing Technique and Tactic information for vulnerabilities. Subsequently, the Technique Cyber Threat Framework[8], released by the United States National Security Agency, exists to determine the mitigation priority for attacks, providing priority for the 14 Tactics through the document.

Moreover, research specifying defensive techniques, such as D3FEND[9], also exists, not only concerning attack techniques. This is a catalog regarding the relationship between defensive cyber security techniques and attack techniques, created by MITRE Corporation using over 500 samples from the United States Patent and Trademark

Office. Also, for security measures against attacks, MITRE provides a CSV file[10] that is publicly available, which links TTPs and NIST 800-53.

In this vein, numerous documents and projects based on MITRE ATT&CK are being conducted. Particularly, research utilizing artificial intelligence, not merely employing methodologies for the linkage analysis between vulnerabilities and TTPs, is also being performed, which will be mentioned in Section 2.3 of this paper."

2.3 Prior Study Analysis on the Vulnerability–Attack Technique Correlation

To comprehend the dynamic characteristics of each vulnerability, MITRE ATT&CK TTPs are utilized as depicted in [Figure 4]. According to existing research, analyses linking vulnerabilities and TTPs have been conducted not only by utilizing methodologies provided on Github but also through studies involving artificial intelligence learning based on the contextual information of CVE descriptions.

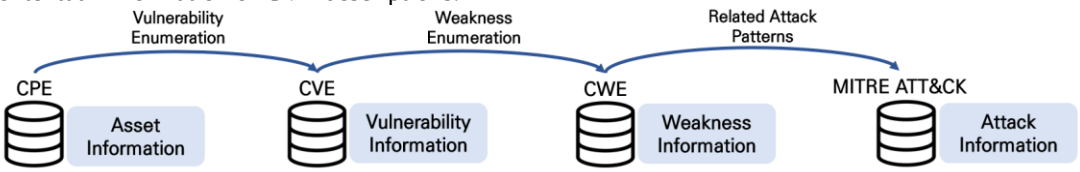

Figure 4: Common Vulnerability and Attack Technique Association Diagram

Yosra[11] employs CVE description information as input, providing tactical information of MITRE ATT&CK by blending a multi-label classification method and an ensemble-based machine learning algorithm, demonstrating a high accuracy of 0.9963.

Octavian[12] uses a data augmentation approach to overcome the limitations of existing data and employs BERT, a natural language processing model, to understand contextual information, subsequently providing pertinent attack technique information. This method offers a figure of 0.4784 in terms of the F1-score.

Otgonpurev[13] provides attack technique information using a machine learning algorithm based on a multi-label classification method, offering a figure of 0.7432 in terms of accuracy.

	Utilized method	**Classification on Vulnerability type**	**Consideration of attack procedures**
[11]	Binary Relevance, Random Forest	Unclassified	Not considered
[12]	BERT	Unclassified	Not considered
[13]	Binary Relevance	Unclassified	Not considered

Table 2 : Comparative analysis of prior research

As shown in [Table 2], previous studies, unlike this paper, conducted automated learning but derived attack techniques without considering the type of each vulnerability, subsequent impacts, and other procedures, presenting a limitation. Consequently, this paper intends to derive attack techniques by considering subsequent impacts and attack technique procedures, based on the methodology suggested by MITRE engenuity.

3 Common Vulnerabilities – Attack Techniques Correlation Methodology Study

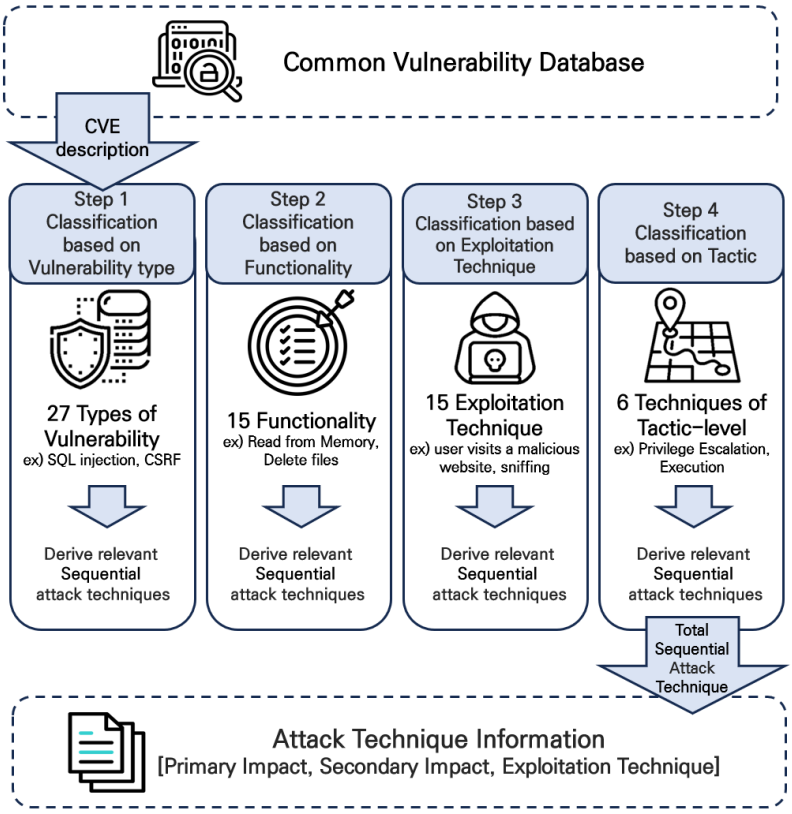

Figure 5: Common Vulnerability – Attack Technique Correlation Process

The overall process of this methodology is shown in [Figure 5]. This study analyzes the methodology for deriving sequential attack techniques.

3.1 Analyze classification based on vulnerability type

The initial step in this methodology involves identifying vulnerability types based on the description of the vulnerability and analyzing the associated attack technique information. Vulnerabilities of the same type generally share the same attack stages and impacts. Through this, the derivation of first and second-order effects as well as attack technologies used in exploitation techniques illustrated in [Table 3].

Vulnerability Type	Primary Impact	Secondary Impact	Exploitation Technique
General Improper Access Control	(Refer to the functionality section)	(Refer to the functionality section)	N/A
Authentication Bypass by Capture-replay	T1190 (Exploit Public-Facing Application)	N/A	T1040 (Network Sniffing)
Overly Restrictive Account Lockout Mechanism	Mobile - T1446 (Device Lockout) Others – T1531 (Account Access Removal)	N/A	T1110 (Brute Force)
Cross-site Request Forgery (CSRF)	T1068 (Exploitation for Privilege Escalation)	(Refer to the functionality section)	T1204.001 (User Execution: Malicious Link)
Session Fixation	T1563 (Remote Service Session Hijacking)	N/A	N/A
Server-Side Request Forgery (SSRF)	T1090 (Proxy)	T1135 (Network Share Discovery) T1005 (Data from Local System)	T1133 (External Remote Service)

Table 3: Part of Classification based on vulnerability type

In this context, the criteria for classifying vulnerability types utilize the high-level categories of vulnerability types determined through the Common Weakness Enumeration (CWE) system, specifically referencing CWE-699 (Software Development) and CWE-1000 (Research Concepts).

In linking attack techniques, more than one type of vulnerability can be mapped, and the primary and secondary impacts, as well as exploitation techniques associated with a vulnerability type, are common attack techniques found in that type. When advised to refer to the technology-based classification, it implies the extraction and application of technical information based on vulnerability text information due to the variety of attack techniques associated with the impacts of a vulnerability type. Additionally, the presence of 'N/A' signifies that there are no precise attack techniques that can be derived from the CVE description information.

3.2 Analyze classification based on functionality

The subsequent step, as mentioned in section 3.1, involves mapping attack techniques using the functionality of the vulnerability, especially when there are impact details not connected in the vulnerability type-based attack technique mapping. Here, 'vulnerability functionality' refers to the access techniques that an attacker must acquire to exploit the vulnerability. Through this function-specific attack technique mapping, we can discern the attack technique information for the primary and secondary impacts, as illustrated in [Table 4].

Functionality	Primary Impact	Secondary Impact
Modify Configuration	T1632 (Subvert Trust Controls)	N/A
Create Account	T1136 (Create Account)	T1078 (Valid Accounts)
Disable protections	T1562 (Impair Defenses)	N/A
Read files	T1005 (Data from Local System)	T1003.008 (OS Credential Dumping: /etc/passwd and /etc/shadow) T1552.001 (Unsecured Credentials: Credentials in Files)
Memory Read (Memory Buffer Errors, Pointer Issues, Type Errors, etc.)	T1574 (Hijack Execution Flow) T1499.004 (Endpoint Denial of Service: Application or System Exploitation)	T1211 (Exploitation for Defense Evasion), T1212 (Exploitation for Credential Access)
Obtain sensitive information: Other data	T1005 (Data from Local System)	N/A

Table 4: Part of Classification based on functionality type

During this process, attack technique mapping occurs based on the functionality, and if the secondary impact is marked as 'N/A', it indicates that either the attacker cannot undertake additional actions leveraging the primary impact, or there is insufficient information in the vulnerability description to derive substantial details for further actions.

3.3 Analyze classification based on the exploitation technique

Perform this mapping in the event that a mapping of exploitation techniques by vulnerability type has not been established in Section 3.1. In this step, we group the common techniques taken to exploit a vulnerability into phases and map the attack techniques as follows [Table 5].

Main Question	Sub Question	Exploitation Techniques
If the user executes a malicious file?	Where did this file come from?	T1204.002 (User Execution: Malicious File)
		T1204.001 (User Execution: Malicious Link)
		T1566.001 (Phishing: Spearphishing Attachment)
		T1566.003 (Phishing: Spearphishing via Service)
		T1091 (Replication Through Removable Media)
If the user visits a malicious website?		T1189 (Drive-by Compromise)
If the attacker exploits remote system applications?		T1190 (Exploit Public-Facing Application)

Table 5: Part of Classification based on the exploitation technique

This process generates attack technique mappings based on abuse techniques, and it can be utilized independently from the attack technique mappings derived from vulnerability types and features. This method aids in a more detailed analysis and understanding of attack techniques.

3.4 Analyze classification based on tactic

In the event that no attack techniques can be identified through the three classification methods previously described, the final step involves utilizing the tactical information, which pertains to the overarching categories of attack technique, to perform mapping as illustrated in the following [Table 6].

Tactic	Generic Exploitation Technique
Initial Access	T1190 (Exploit Public-Facing Application)
Execution	T1203 (Exploitation of Client Execution)
Privilege Escalation	T1068 (Exploitation for Privilege Escalation)
Defense Evasion	T1211 (Exploitation for Defense Evasion)
Credential Access	T1212 (Exploitation for Credential Access)
Lateral Movement	T1210 (Exploitation of Remote Services)

Table 6: Classification based on tactic

This approach to mapping based on attack tactics serves as the ultimate step; however, it bears the limitation of not providing detailed attack technique information that could be derived through vulnerability types, functionalities, and exploitation techniques discussed in the preceding sections.

4 Case Study

In this study, we present a case study applying a methodology that establishes the correlation between attack technique information based on operational technology vulnerabilities. To facilitate this, we utilized data obtained from ICS-CERT[14], a provider of threat and vulnerability information in the industrial control system sector. Our analysis centered on the common vulnerabilities disclosed in the same period as the CERT information released in 2023, identifying a total of 468 vulnerabilities.

According to a report by CISA[15], attackers are estimated to be able to exploit a vulnerability within an average of 15 days after its discovery. Taking this into consideration, our case study focused on 34 vulnerabilities based on ICS-CERT that occurred within 15 days.

Building on this foundation, we carried out a process to link vulnerabilities with attack technique information according to the methodology, an example of which is illustrated in [Figure 6].

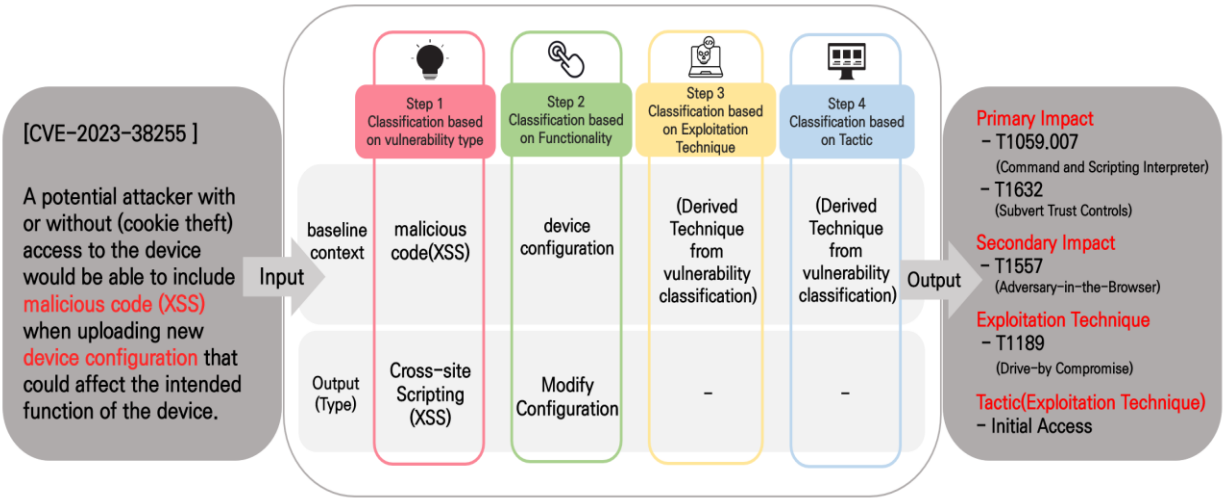

Figure 6: Common Vulnerability – Attack Technique Correlation Example

Through this approach, we were able to identify the interconnectivity between each vulnerability and attack technique, represented in the final results as displayed in [Table 7].

CVE_ID	Vulnerability Type	Functionality	Primary Impact	Secondary Impact	Exploitation
CVE-2023-27373	Improper Restriction of Excessive Authentication Attempts	Modify Configuration	T1078 T1632	N/A	T1110.001
CVE-2023-41032	Code Injection	Write to existing file	T1059 T1565.001	T1059 T1574 T1554	T1203
CVE-2023-40732	Session Fixation	Obtain sensitive information: Other data	T1563 T1005	N/A	T1190
CVE-2023-39446	Cross-site Request Forgery (CSRF)	Obtain sensitive information: Other data	T1068 T1005	N/A	T1204.001
CVE-2023-38582	Cross-site Scripting (XSS)	N/A	T1059.007	T1557	Stored – T1189 Others – T1204.001
CVE-2023-40728	General Cryptographic Issues	- Obtain sensitive information: Other data - Delete files - Write to existing file - Read files - Create/Upload file	T1078 T1557 T1040 T1190 T1565.001 T1485 T1005 T1505.003	T1059 T1574 T1554 T1499.004 T1003.008 T1552.001 T1059	T1110
CVE-2023-0215	N/A	Memory Read (Memory Buffer Errors, Pointer Issues, Type Errors, etc.)	T1005 T1499.004	T1211 T1212	T1190
CVE-2023-3569	XML Entity Expansion (XEE)	N/A	T1499.004	N/A	T1133 T1210
CVE-2023-38433	Hard-coded Credentials	N/A	T1078.001 T1529	N/A	T1078 T1190

Table 7 : Part of interconnection between CVE and MITRE ATT&CK technique

Upon conducting mapping for the 34 cases, we found that 7 cases (approximately 20%) in vulnerability type classification, 10 cases (around 29%) in function classification, and 14 cases (about 41%) in secondary impact classification were identified as unmapped values.

5 Discussion

Through the case study conducted in Chapter 4, we verified that each vulnerability possesses distinct exploitation techniques, and these techniques can be interconnected to the MITRE ATT&CK Tactic. This discovery suggests the potential for each vulnerability to be utilized at various stages of an attack process, encompassing multiple tactics, as illustrated in the subsequent [Table 8].

Tactic	CVE_ID	Number
Initial Access	CVE-2023-38558 / CVE-2023-29463 / CVE-2023-3935 CVE-2023-40725 / CVE-2023-40726 / CVE-2023-40727 CVE-2023-28831 / CVE-2023-0215 / CVE-2023-0286 CVE-2023-38582 / CVE-2023-41965 / CVE-2023-38255 CVE-2023-3526 / CVE-2023-3569 / CVE-2023-38433 CVE-2023-40221	16
Execution	CVE-2023-40731 / CVE-2023-41032 / CVE-2023-41033 CVE-2023-39446 / CVE-2023-38255 / CVE-2023-3526 CVE-2023-38582	7
Persistence	CVE-2023-38558 / CVE-2023-29463 / CVE-2023-3935 CVE-2023-28831 / CVE-2023-3569 / CVE-2023-38433 CVE-2023-40221	7
Privilege Escalation	CVE-2023-38558 / CVE-2023-36497 / CVE-2023-38433	3
Defense Evasion	CVE-2023-38558 / CVE-2023-24932 / CVE-2023-38256 CVE-2023-38433	4
Credential Access	CVE-2023-27373 / CVE-2023-31041 / CVE-2023-40724 CVE-2023-40727 / CVE-2023-40728 / CVE-2023-40729 CVE-2023-40730 / CVE-2023-39903 / CVE-2023-41084 CVE-2023-39452 / CVE-2023-41256	11
Discovery	CVE-2023-39903/ CVE-2023-40730 / CVE-2023-41084 CVE-2023-39452 / CVE-2023-41256	5
Lateral Movement	CVE-2023-29463 / CVE-2023-3935 / CVE-2023-28831 CVE-2023-40221 / CVE-2023-3569	5

Table 8: Tactic connection based on exploitation techniques

The results derived in this study, based on ICS-CERT data, project a prospect of presenting a methodology apt for vulnerability management in operational technology environments. Building upon this, the prioritization among CVEs occurring in a specific asset and among techniques occurring within a CVE, utilizing the Tactic prioritization mentioned in Section 2.2 from the Technical Cyber Threat Framework, is deduced as shown in [Figure 7].

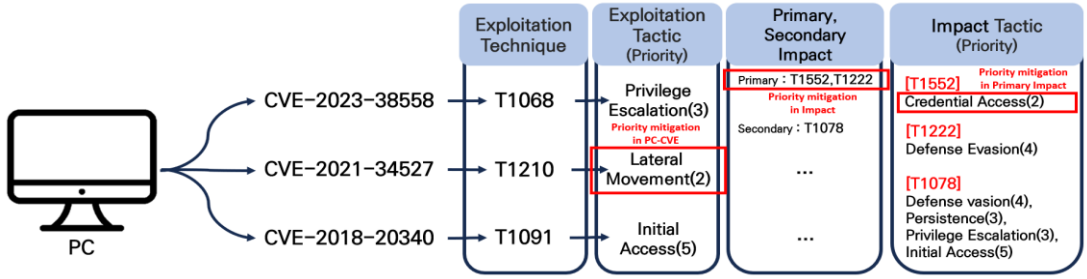

Figure 7: Vulnerability and Related Attack Technique Mitigation Priority

This research did not consider determining priorities when the weights of each tactic are identical. Therefore, future research aims to introduce a scoring system for each attack technique, enabling severity assessment that reflects the dynamic characteristics of vulnerabilities. This, in turn, proposes a method to specify the priority of security measures in a more granular manner.

Such methodology is anticipated to provide crucial information necessary for cybersecurity experts in developing and implementing vulnerability management strategies, thereby contributing to enhancing safety in operational technology environments.

6 Conclusion

In operational technology, the availability of systems is most important, thus making it essential to thoroughly manage vulnerabilities in advance. Recently, as vulnerabilities are continually increasing, attacker-centric security verification methods are being utilized. However, the problem lies in the lack of sequence reflection in these methods, making it difficult to respond immediately to vulnerabilities.

Against this backdrop, this paper presents a method of connecting attack techniques for each vulnerability by analyzing the ATT&CK to CVE methodology proposed by the Center for Threat-Informed Defense. This methodology, considering vulnerability classification and attack procedures overlooked in previous research, proposes a means to create a security framework suitable for vulnerability management.

Future research directions include modifying the mapping method for currently unlinked attack techniques and conducting research to develop an automated solution that automatically maps vulnerabilities and attack techniques using artificial intelligence technology, based on this. Subsequently, as mentioned in the Discussion, research will also be conducted on evaluating the severity score of each vulnerability and managing mitigation priorities between attack techniques through a scoring method for attack techniques. This aims to establish a system that allows security experts to manage vulnerabilities and respond more effectively.

Acknowledgement

"This work was supported by Institute for Information & communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT)(No.2022-0-01203, Regional strategic Industry convergence security core talent training business)

The results of a study on the supported by 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.2106061).

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1G1A1010506).

References

[1] Staves, A. (2023). An Analysis of Adversary-Centric Security Testing within Information and Operational Technology Environments. *Digital Threats: Research and Practice*, *4*(1), 1-29. ACM

[2] Noel, S. (2015). Interactive visualization and text mining for the CAPEC cyber attack catalog. In *Proceedings of the ACM Intelligent User Interfaces Workshop on Visual Text Analytics* (pp. 1-8). ACM

[3] Kanakogi, K.(2021). Tracing capec attack patterns from cve vulnerability information using natural language processing technique. MDPI

[4] Giannakopoulos, T. (2022). Threat categorization on CVE descriptions using text classification (*Master's thesis, Πανεπιστήμιο Πειραιώς*). UniPi

[5] MITRE. *ATT&CK Framework* Retrieved from https://attack.mitre.org/

[6] MITRE. *ATT&CK. Framework Resource updates.* Retrieved from https://attack.mitre.org/resources/updates/updates-april-2023/

[7] Center for Threat-Informed Defense. *cve-to attack methodology.* Retrieved from https://github.com/center-for-threat-informed-defense/attack_to_cve/blob/master/methodology.md

[8] NSA (2018, 11). NSA/CSS Technical Cyber Threat Framework v2. *CYBERSECURITY OPERATIONS THE CYBERSECURITY PRODUCTS AND SHARING DIVISION*

[9] MITRE. *D3FEND* Retrieved from https://d3fend.mitre.org/

[10] MITRE ENFENUITY. *Project Resources* Retrieved from https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/nist-800-53-control-mappings/

[11] Lakhdhar, Y. (2021, May). Machine learning based approach for the automated mapping of discovered vulnerabilities to adversial tactics. In *2021 IEEE Security and Privacy Workshops (SPW)* (pp. 309-317). IEEE.

[12] Grigorescu, O., Nica, A., Dascalu, M., & Rughinis, R. (2022). Cve2att&ck: Bert-based mapping of cves to mitre att&ck techniques. *Algorithms*, *15*(9), 314. MDPI

[13] Otgonpurev, M. (2020). Automatic Mapping of Vulnerability Information to Adversary Techniques *In SECURWARE 2020 : The Fourteenth International Conference on Emerging Security Information, Systems and Technologies.*UPV

[14] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. *Cybersecurity Alerts & Advisories* Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories

[15] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. Remediate Vulnerabilities for Internet-Accessible Systems. *CISA INSIGHTS*