Automated Mapping System for Identifying Vulnerable Assets Based on TTP

Bo-Ram Kim, Ye-Eun Kim, and Hwankuk Kim*

SangMyung University, Cheonan-si, South Korea
{yeoun132, yeni0.0king}@gmail.com, rinyfeel@smu.ac.kr

Abstract

The rapid technological advancement has significantly increased cyber threats, emphasizing the need to protect assets within organizations[1]. While experts have manual methods to identify threats, this approach faces challenges such as time constraints and a manpower shortage compared to rising security threats. Recent research shows a growing interest in automating cyber threat analysis using standardized identification systems to mitigate cost-related challenges. Prior studies evaluated vulnerabilities[2, 3] and quantified asset risk[4, 5] using these systems in asset management research. However, earlier studies exhibit limitations, such as their inability to account for emerging threats and inadequacy in presenting effective responses to cyber threats. To address these challenges, we propose a model that utilizes the [1]National Vulnerability Database (NVD) in the United States to identify threats to internal assets using a standardized identification system. This model incorporates real-time Cyber Threat Intelligence (CTI) to reflect external threats. Figure 1 illustrates the structure of the proposed model, which aims to safeguard the organization's assets associated with newly emerging CTI. The model comprises four modules: ① CTI collection and Formalization module, ② CTI-based TTP mapping module, ③ Threat factor identification module, and ④ response strategy derivation module. ① The CTI Collection and Formalization Module gathers emerging CTI and structures relevant vulnerability information into a formalized format. Various methods are used for CTI collection, and the formalization process involves extracting meaningful details(CVE ID, CPE, CVSS, TTP, description, source) and organizing them into a structured format. ② The CTI-Based TTP Mapping Module links CTI to [2]MITRE ATT&CK's TTP, categorizing attack techniques tied to specific vulnerabilities into a unified matrix. This aids in providing helpful response strategies. TTP mapping can be done using rules or machine learning (ML) in our model, [3]utilizing data from NVD (CVE → CWE), STIX-CAPEC (CWE → CAPEC), or MITRE ATT&CK (CAPEC → TTP) at each mapping stage. ③ The threat factor identification module detects threat actors impacting the organization's internal assets through CPE. We assume the organization's internal assets are managed and stored in a database using the common asset identification system, NVD CPE. The presence of threat actors within these assets is established by comparing the CPE in CTI with that in the organization's asset database. If there's a match, threat actors are considered to be present within the organization's internal assets. ④ The response strategy derivation module maps response strategies corresponding to TTP representing attack techniques. Response strategies based on TTP and rules are derived using Mitigations provided by MITRE ATT&CK. Consequently, users of this model can comprehensively review vulnerability information (CVE ID), internal threat actors within the organization (CPE), attack information (TTP), and response strategies (Mitigation ID) related to CTI. The main goal is to categorize Cyber Threat Intelligence (CTI) into an attack-based matrix (Technique-ID) using a standardized identification system and derive suitable response strategies. We evaluate the model's

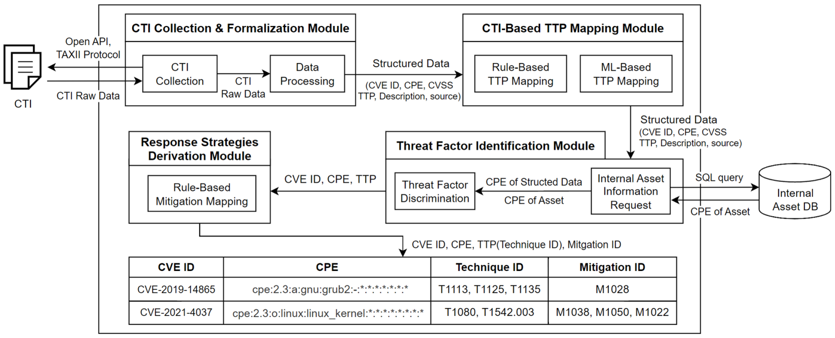
The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No.P-12

*Corresponding author: SangMyung University, Cheonan-si, 03616, South Korea, Email: rinyfeel@smu.ac.kr

[1] https://www.nist.gov/

[2] https://attack.mitre.org/

[3] https://github.com/mitre/cti



CVE ID	CPE	Technique ID	Mitigation ID
CVE-2019-14865	cpe:2.3:a:gnu:grub2:-:*:*:*:*:*:*:*	T1113, T1125, T1135	M1028
CVE-2021-4037	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	T1080, T1542.003	M1038, M1050, M1022

Figure 1: Proposed Model for Threat Identification of Assets

efficiency in accurately classifying CTI into Technique-ID using the Confusion Matrix's accuracy metric. Comparing the algorithm's outcomes for 145,421 CVEs with MITRE ATT&CK data, we found 145,300 matches, achieving an impressive 99.92% accuracy rate. In this study, we propose that security experts utilizing this model can efficiently manage assets exposed to cyber threats in real-time. Additionally, they can comprehensively review information from cyber threats to response strategies, thus enhancing overall work efficiency. In future research, ML-based studies to expand the coverage of TTP (Tactics, Techniques, and Procedures) mapping within the model proposed in this study will be included. Moreover, there are plans to conduct research focusing on asset prioritization. Also, experiments are planned to rigorously evaluate the overall effectiveness of the proposed model.

keywords: Automated Threat Analysis, Cyber Threat Intelligence, MITRE ATT&CK matrix

Acknowledgement: This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea Government (MSIT) (No.2021-0-00358, AI · Big data based Cyber Security Orchestration and Automated Response Technology Development)

References

[1] SCOTT MUSMAN and Andrew J Turner. A game oriented approach to minimizing cybersecurity risk. *Safety and Security Studies*, 27, 2018.

[2] Jackson Wynn, Joseph Whitmore, Geoff Upton, Lindsay Spriggs, Dan McKinnon, Richard McInnes, Richard Graubart, and Lauren Clausen. Threat assessment and remediation analysis (tara). *MITRE Corporation*, 2014.

[3] Roman Ushakov, Elena Doynikova, Evgenia Novikova, and Igor Kotenko. Cpe and cve based technique for software security risk assessment. In *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, volume 1, pages 353–356. IEEE, 2021.

[4] Thomas D Wagner, Khaled Mahbub, Esther Palomar, and Ali E Abdallah. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, 87:101589, 2019.

[5] Jay Jacobs, Sasha Romanosky, Benjamin Edwards, Idris Adjerid, and Michael Roytman. Exploit prediction scoring system (epss). *Digital Threats: Research and Practice*, 2(3):1–17, 2021.