Threat Intelligence approach for mapping CVE to MITRE ATT&CK for better vulnerability management in Automotive Security

COMP-4800 Selected Topics in Software Engineering

Monday, February 28, 2022

Keerthana Madhavan

“I confirm that I will keep the content of this assignment confidential. I confirm that I have not received any unauthorized assistance in preparing for or writing this assignment. I acknowledge that a mark of 0 may be assigned for copied work.”

Threat Intelligence approach for mapping CVE to MITRE ATT&CK for better vulnerability management in Automotive Security

***Abstract*— Due to the current development in the Automotive industry and the move towards a connected and autonomous vehicle, there is a need for more rigorous cyber security-based approaches in automobile software. Several research projects have confirmed that existing or new vulnerabilities attacked vehicles. However, research also suggests that there aren't any methods to identify in-depth autonomous-related vulnerabilities and patch them based on tactics and techniques. We need to leverage threat intelligence and machine learning research to provide better patching mechanisms for the vulnerability management team and secure software developers. The challenge in Automotive Security is the need for Continuous cybersecurity monitoring. The automotive industry has traditionally not had defined processes for cybersecurity monitoring to actively monitor for threats, vulnerabilities, and attacks on their vehicles. In this report, I show that we can solve this problem by leveraging existing research in security and utilizing the mapping of CVE to the MITRE ATT&CK framework. This will give an in-depth perspective on automotive-related threat actors and their evolving tactics and techniques behind the scenes to target new flaws in the software systems. The need for new approaches in automotive vulnerabilities management is discussed in the report.**

Keywords—Threat Intelligence, MITRE ATT&CK, Vulnerability Management, NIST CVE, vulnerabilities

I. INTRODUCTION

Since 2010, the automotive industry has been gradually introducing the notion of connected and autonomous vehicles, and there exists the need for proactive vulnerability management. Nowadays, most advanced cars rely on external entities, third-party libraries, and software-based driving systems.

As more software exists in vehicles, there is a risk of raising software bugs and vulnerabilities that could potentially have catastrophic consequences on the vehicles' safety, privacy, and operation if abused by malicious adversaries. The volume of software in the automotive industry is an ever-increasing important topic considered seriously. Cybersecurity monitoring services or tools that alert new vulnerabilities should exist proactively to provide automotive vulnerability management teams input to mitigate software threats. About sixty-two percent say that a malicious or proof-concept attack against the automotive technologies or systems developed by their organizations is likely or very likely in the next 12 months. [1] However, 61% of the organizations face a technical challenge in addressing critical security vulnerabilities promptly through a software update delivery model. Oka in [1] suggests that we need to regarding open source software, mainly focusing on known vulnerabilities in such software used in automotive systems that attackers can exploit. It is necessary to assess which software versions are affected by the identified vulnerability and the exploitability and impact. So by considering the CVE of different exposures and mapping it to MITRE tactics and techniques for a better and faster vulnerability management process.

Once the developed software for the automotive system is more or less functional, organizations can perform vulnerability scanning using known attacks and attack patterns to identify vulnerabilities in the software. We also need to use CVE mapping to find better approaches for immediate software patches. Oka in [2] discusses an example of how security teams can actively search for newly identified vulnerabilities published online and actively monitor and process information gathered from deployed vehicles to detect attack patterns. However, AUTO ISAC (Automotive Information Sharing and Analysis Center) platform is only available for private or limited members, so there is also a need for shared threat intelligence across the automotive industry. [3] In March 2018, within just five months after the released software package, three critical vulnerabilities in curl had been CVE-2017-8817, CVE-2017-8817, CVE-2018-1000120.

The automotive software companies should have a proper continuous cybersecurity monitoring process that is not in place; an automotive organization would not be aware of any critical vulnerabilities shortly found after the software is released. [3]

Vulnerability Management involves identifying how critical a particular threat or vulnerability is regarding the specific products. Along with it, we need more Threat Intelligence approaches to solve this problem, like leveraging CVE - MITRE ATT&CK mapping for efficient vulnerability management across all industries, especially the automotive industry.

The rest of the report is organized as follows: what is threat intelligence, what is vulnerability management, what is NIST CVE, What are MITRE ATT&CK, the need for mapping CVEs to MITRE ATT&CK, and conclusions.

II. WHY THREAT INTELLIGENCE?

Threat Intelligence is the data that is "collected, processed, and analyzed to understand a threat actor's motives, techniques, targets, and attack behaviors." [4] The threat intelligence in the automotive industry must provide the context to make informed decisions that vulnerability management analysts can use. Humans cannot process and categorize raw data orders as quickly as machines. On the other hand, humans can do intuitive, big-picture analysis far better than any artificial intelligence - as long as they aren't swamped with large data sets and tiresome study. When paired, people and machines work smarter, saving time and money, reducing human burnout, and improving security overall.

Cyber threats come from all places of all sorts, including third parties, brand attacks, and internal threats, and digital business risk is at an all-time high. We need a comprehensive strategy that requires implementing techniques and technology to reduce risk and stop threats proactively. Today's cybersecurity industry faces various challenges because of "increasingly persistent and devious threat actors; a daily flood of data full of extraneous information and false alarms across multiple systems."[5] The world of Cybersecurity is in short of skilled professionals. According to [5], about 44% of security alerts go uninvestigated, and 66% of companies are

breached at least once. With data, the threat intelligence provides context like who's attacking you, their motivation and capabilities, and what indicators of compromise (IOC'S) in your systems to look for. It helps teams to make informed judgments about companies' security.

Vulnerability management teams can benefit from Threat Intelligence. They need to prioritize the most critical vulnerabilities accurately. Threat Intelligence provides access to external insights and context that helps them to differentiate immediate threats to their specific enterprise from merely potential threats. Threat Intelligence lightens the burden by assisting the analysts in deciding what to prioritize and ignore. The intelligence helps analyze data and information to uncover patterns and stories that inform decision-making. Intelligence is the product of a cycle of identifying the goals of the question, collecting relevant data, processing them, analyzing them, producing actionable intelligence, and distributing them. Threat Intelligence will play a massive role in Cybersecurity in the next decade.

There are two types of threat intelligence: operational and strategic. My paper focuses on Strategic Threat Intelligence. Strategic Threat Intelligence requires much human expertise because it takes time to evaluate and test new tactics, techniques, and procedures against existing security controls. I believe it can be automated because existing research suggests the Mapping of CVE to MITRE ATTA&K, which we will explore later.

III. THREAT INTELLIGENCE FOR VULNERABILITY MANAGEMENT

The process of finding, analyzing, and reporting security vulnerabilities in systems and the software that runs on them is known as vulnerability management.[6] Along with other security measures, frameworks and methods are critical for businesses to prioritize risks and reduce their "attack surface." Data feeds play an essential role in threat intel; they provide the valuable raw material for threat intelligence. The critical success in VM is to shift the thinking of your security teams from trying to patch everything to making risk-based decisions. They can make good risk-based decisions by taking advantage of more sources like threat intelligence. Based on the research from Gartner Inc., there are about 8000 vulnerabilities a year are disclosed.[7]

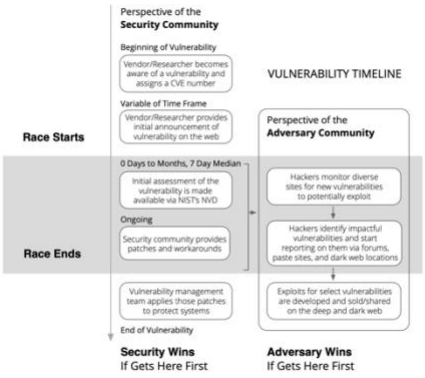
More software, more vulnerabilities, but fewer new vulnerabilities, there are cases of old vulnerabilities appearing in new software is something to be concerned about (bad security coding). A threat intelligence system detects vulnerabilities that pose a risk to your organization and provides insight into their chances of being exploited. [8] Relying solely on vulnerability severity is dangerous, so we need to consider the threat actors exploiting vulnerabilities in the industry now. We should use CVE and MITRE ATT&CK Framework for better vulnerability management.

Figure 1: The race between security professionals and adversaries. [7]

One powerful way is to assess "the risk of a vulnerability is to look at the progress from initial identification to availability," weaponization, commoditization in exploit kits. [6] Also, another reason why we need MITRE attack mapping to CVEs. We need to leverage existing frameworks like MITRE ATTACK because they develop and maintain CVEs. The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework was created to track adversarial behavior over time. It has 11 different tactic categories. Classifying a CVE into its tactics and methods allows security teams to be very granular in describing and tracking the hacking process. It can also be shared between other groups. It is a tedious process, but Machine Learning can significantly help the automotive industry. The need for Threat intelligence.

IV. THE NEED FOR AUTOMOTIVE CVE?

Common Vulnerabilities and Exposures (CVE) list publicly known cybersecurity vulnerabilities entries. Each entry has an identification number, a description, and at least one public reference. CVE was created in 1999 and has since become the industry standard for addressing interoperability



and different databases and tools. CVE entries, also referred to as CVEs, CVE IDs, and CVE numbers by the community, serve as common reference points for cybersecurity products and services. CVE is an international cybersecurity community endeavor, and CVE Numbering Authorities assign each new CVE entry (CNAs). We have multiple vulnerability systems in the cybersecurity world, such as the NIST's National Vulnerability Database repository (NVD). This database consists of more than 100k CVEs, security checklists, security-related software flaws, misconfigurations, product names, and impact metrics. [9] Common, Vulnerability and Exposures (CVE) is a collection of IT-related vulnerabilities, especially network. NVD was established to provide detailed information related to CVE's vulnerability list. NVD is a database operated by the National Institute of Standards and Technology (NIST). It gives a technical perspective on the vulnerability and a score of standard vulnerability scoring systems (CVSS) and related CWE information.[10] Finding a weakness in the automotive software industry requires a lot of human effort.

It is challenging to determine if the CVE is about Automotive Industry unless there are distinct cybersecurity professionals. In [11], the authors develop an Automotive CVE that shares car-related vulnerabilities and attack cases to overcome the limitations of just CVE, NVD, and CWE and also Auto-ISAC. We should be leveraging these CVEs created by Automotive Cybersecurity Research (AEGIS) organization to map out further diagnosis using MITRE ATT&CK.

V. WHAT IS MITRE ATT&CK FRAMEWORK?

MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a curated knowledge base for cybersecurity for Industry Control Systems (ICS). It is

globally accessible and contains adversary tactics techniques based on real-world observations. This framework is used to develop various threat models and other types of methodologies and tools. The adversary tactics are categorized as per [12]:

Reconnaissance: obtaining information about the target organization to organize future enemy actions

Resource Development: putting in place resources to assist activities, such as command and control infrastructure

Initial Access: spear phishing is an attempt to access your network.

Execution: trying the malicious run code

Persistence: attempting to keep their footing, i.e., switching configurations

Privilege Escalation: Trying to get higher-level permissions, e.g., by exploiting a flaw to gain Access

Defense Evasion: looking to keep away from being detected, i.e., the usage of depended on strategies to cover malware

Credential Access: obtaining accounts names and passwords

Discovery: mapping out the environment

Lateral Movement: getting into the environment and maintaining Access

Collection: stealing data that the hacker needs

Command and Control: maintain Access and have Control

Exfiltration: steal data

Impact: CIA matters

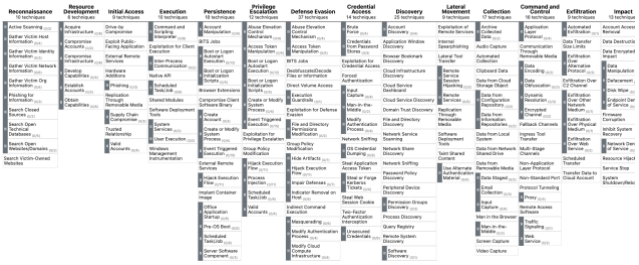


Figure 2: MITRE ATT&CK tactics and techniques from [13].

The above image is a list of all the techniques mapped to the 14 tactics in MITRE ATT&CK.

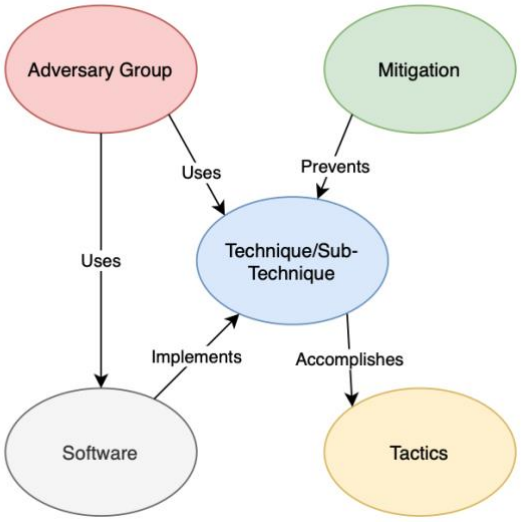


Figure 3: MITRE ATT&CK components and their relationship [13]

This diagram illustrates the need for mapping CVEs to MITRE ATT&CK because it will provide in-depth insights for many cybersecurity teams and better understand the perspective of hackers.

VI. VULNERABILITIES IN THE AUTOMOTIVE INDUSTRY

Security Vulnerabilities in connected cars have various vulnerabilities and devastating consequences. The authors in [14] paper use empirical data to understand the needs of security in the automobile industry. With the help of NVD CVE, CVSS database, the authors map 183 reports from Qualcomm and 28 from the rest of the sector on the Automobile industry to develop a better taxonomy. They found that vulnerabilities generally had a high exploitable rate and high impact according to CVSS standards for Automotive related exposures. They found that the most common weaknesses among the major car companies were:

- Protection mechanism failure.
- Information exposure.
- Improper restriction of operations within the bounds of memory buffer.
- Improper input validation.

They suggest that 47% of vulnerabilities were in the infotainment system, and 39% were in the telematics control unit. The connected car has humble beginnings. The first connected car was founded in 1996 with an emergency call system, and the industry has grown ever since.

Numerous automobile attacks have been demonstrated in previous research, where the new connectedness has proven to have a lot of weaknesses. To make meaningful progress in the automobile security industry, we must collect critical data and understand the problems. From their study, the vulnerabilities showed a high alarming trend of high exploitability rate. The automobility industry's ignorance of security is reflected in the exploitability metrics. Even though exposures had low attack complexity, researchers still proved that they could be hacked with no pre-conditions and executed with an average laptop.

Vulnerabilities in such software will naturally be easier to find due to the collective feedback and collaborative development. Employing a coordinated strategy could highly support the connected car industry in the future.

In [15], the author shows that existing taxonomies for the automotive development process are insufficient and do not consider the security aspect. One important part we need is the derivation of security requirements that usually result from a prior threat modeling. A vehicle's attack surface is analyzed for attack possibilities in threat modeling. Existing security taxonomies are not suitable for automotive dev and cannot provide more insights on security incidents. The authors offer a solution to classify schemes to automotive security attacks as a uniform taxonomy. They classify 162 existing attacks and provide a new taxonomy. They focus on security incidents taxonomies in which vulnerability, invasion, and flaw classification can be distinguished. They propose a tailored taxonomy using Threat Analysis, Risk Assessment (TARA), and security approach. Their final work presents a taxonomy to describe automotive security attacks, the classification of attacks using different frameworks that provides a uniform description for security developers. They classified 162 published security incidents and split 413 staged attacks on vehicles. Existing research also suggests that we need more threat intelligence, framework, and analysis for automotive security.

VII. CVE TO MITRE ATT&CK MAPPING

Defenders have a hard time integrating vulnerability and threat data, and they don't have a consistent picture of how adversaries exploit vulnerabilities to achieve their objectives. It's impossible to prioritize vulnerabilities without this information. So, one solution that researchers came up with is to develop a methodology to use MITRE ATT&CK to characterize the impact of CVEs and prove the bigger picture. [16] This approach will be a game-changer for the automotive industry because it will lead to faster and more efficient vulnerability management. CVEs associated with ATT&CK methodologies provide a critical contextual link between vulnerability management, threat modeling, and compensating controls, allowing defenders to analyze better the genuine risk posed by individual vulnerabilities in their environment.[16]

Software vulnerabilities (CVE) play a crucial part in cyber-attacks and are typically categorized into four ATT&CK approaches that encompass the exploitation phase of the attack chain. Vulnerabilities that attackers exploit must be identified, and vulnerability assessments must comprehend how exposure can assist the attacker at each stage of the attack life cycle. The defenders lack a concrete approach to prioritize CVEs based on their role in the attack chain and in the context of rules in place due to the sparse classification of a CVE into the ATT&CK taxonomy, the lack of methods to extract labels from threat reports, and the volume of vulnerabilities disclosed.

In [17], the authors propose a neural network model to automatically map CVEs to ATT&CK Techniques using a novel unsupervised labeling technique.

The authors supplement CVEs with a curated knowledge base of 50 mitigation techniques that aid the model in learning both the attacker and defender perspectives on a given CVE. They compare the method to established baseline models and ablation analysis using a dataset containing CVEs reported in the last ten years. They also mapped 62,000 CVE records to 37 different ATT&CK approaches using the suggested model, demonstrating that the proposed multi-head design functions effectively in the lack of labels in the training dataset. [17] Their model learns attacker and defender view of a CVE by feature enrichment from the knowledge base of attack scenarios and preliminary mitigation steps. We need to apply this approach in the Automotive Sector; mapping out car-related vulnerabilities and CVE would support the vulnerability management team in many ways.

VIII. CONCLUSION

In conclusion, the automotive industry needs more threat intelligence and exploring different approaches such as mapping CVEs to MITRE ATT&CK. We can start by mapping the automotive-related CVEs crafted by Automotive Cybersecurity Research (AEGIS) organization. This would enable accurate patches for automotive-related vulnerabilities and prevent further damage in this connected world, especially for autonomous vehicles. There is great demand for threat intelligence for any organization entailing advanced cyber-threat and detection capabilities. Since threat intelligence aims to gain rich evidence for decision-making, the automotive industry can highly benefit from it. I plan to extend this study into practically developing a Machine Learning model to create a tailored automotive-related CVE to MITRE ATT&CK mapping for future work. This study also suggests that we need more shared threat intelligence amongst automotive partners for better, proactive, and faster security remediation in ages of threats and cyber-attacks.

REFERENCES

[1] D. K. Oka, “Overview of the Current State of Cybersecurity in the Automotive Industry,” in Building fast cars: Assuring the Automotive Software Development Lifecycle, Hoboken, NJ: Wiley, 2021.

[2] D.K. Oka, “Need for Automated Security Solutions in the Automotive Software Development Lifecycle,” in Building secure cars: Assuring the Automotive Software Development Lifecycle, Hoboken, NJ: Wiley, 2021

[3] Kaya, Koray. "A Study of Vulnerabilities and Weaknesses in Connected Cars." (2019).

[4] “What is Cyber Threat Intelligence? [beginner's guide],” crowdstrike.com, 14-Feb-2022. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/.

[5] Zane Pokorny, “What is Threat Intelligence,” in The Threat Intelligence Handbook: Moving Toward a Security Intelligence Program, Annapolis, MD: CyberEdge Group, LLC, 2019, pp. 3–11.

[6] “Vulnerability Management Processes and Systems,” Rapid7. [Online]. Available: https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/.

[7] Zane Pokorny, “Threat Intelligence for Vulnerability Management,” in The Threat Intelligence Handbook: Moving Toward a Security Intelligence Program, Annapolis, MD: CyberEdge Group, LLC, 2019, pp. 43–53.

[8] “How security intelligence enables risk-prioritized vulnerability management,” Recorded Future, 18-Mar-2020. [Online]. Available: https://www.recordedfuture.com/vulnerability-management-prioritization/.

[9] V. Mavroeidis and S. Bromander, "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence," 2017 European Intelligence and Security Informatics Conference (EISIC), 2017, pp. 91-98, doi: 10.1109/EISIC.2017.20.

[10] *National Vulnerability Database*, Dec. 2019, [online] Available: https://nvd.nist.gov/general.

[11] Y. Lee, S. Woo, Y. Song, J. Lee and D. H. Lee, "Practical Vulnerability-Information-Sharing Architecture for Automotive Security-Risk Analysis," in *IEEE Access*, vol. 8, pp. 120009-120018, 2020, doi: 10.1109/ACCESS.2020.3004661.

[12] "What is the mitre ATT&CK framework?: Get the 101 guide," McAfee. [Online]. Available: https://www.mcafee.com/enterprise/en-ca/security-awareness/cybersecurity/what-is-mitre-attack-framework.html.

[13] Mitre ATT&CK®," MITRE ATT&CK®. [Online]. Available: https://attack.mitre.org/.

[14] Kaya, Koray. "A Study of Vulnerabilities and Weaknesses in Connected Cars." (2019).

[15] Sommer, Florian et al. "Survey and Classification of Automotive Security Attacks." Inf. 10 (2019): 148.

[16] "Mapping ATT&CK to CVE for impact," CTID, 28-Oct-2021. [Online]. Available: https://ctid.mitre-engenuity.org/our-work/attck-to-cve/.

[17] Aditya Kuppa, Lamine Aouad, and Nhien-An Le-Khac. 2021. Linking CVEs to MITRE ATT&CK Techniques. The 16th International Conference on Availability, Reliability and Security (ARES 2021). Association for Computing Machinery, New York, NY, USA, Article 21, 1–12. DOI:https://doi.org/10.1145/3465481.3465758