Comparing Different Vehicle Architectures Based On Attack Path Analysis

Emilija Kastratović
1052407

Bachelor Thesis
VS-2019-B18

Examined by
Prof. Dr. rer. nat. Frank Kargl

Supervised by
M.Sc. Michael Wolf

Institute of Distributed Systems
Faculty of Engineering, Computer Science and Psychology
Ulm University

March 18, 2023

Issued: March 18, 2023

I hereby declare that this thesis titled:

Comparing Different Vehicle Architectures Based On Attack Path Analysis

is the product of my own independent work and that I have used no sources or materials other than those specified. The passages taken from other works, either verbatim or paraphrased in the spirit of the original quote, are identified in each individual case by indicating the source.
I further declare that all my academic work was written in line with the principles of proper academic research according to the official "Satzung der Universität Ulm zur Sicherung guter wissenschaftlicher Praxis" (University Statute for the Safeguarding of Proper Academic Practice).

Ulm, March 18, 2023

Emilija Kastratović, student number 1052407

ABSTRACT

The increased use of technology in modern vehicles has made cybersecurity a crucial part of the development process of modern vehicles. Cybersecurity plays an increased role in the safety and security of the vehicle and the privacy and personal data of drivers and passengers.

Most security testing, such as pentesting, is done at later stages of development, a point in time at which it is more complex and costly to address vulnerabilities. Additionally, due to the nature of security testing, it is carried out manually by experts. These factors result in a stagnant security testing process that cannot maintain pace with the increasing complexity of modern vehicles.

The internal vehicular network of such E/E systems plays a vital role in the overall cybersecurity of a modern vehicle. Attackers might exploit potential attack paths in the network to gain unauthorized access to a vehicle's systems or networks.

In this thesis, we propose a solution by presenting a tool that can automate the evaluation of vehicular network security based on attack path feasibility. This tool can automatically generate attack paths in a given vehicular network, find the most feasible ones and evaluate the network's overall security. The tool will be used to evaluate multiple different vehicular networks and compare their security in terms of attack path feasibility.

CONTENTS

1 INTRODUCTION

1.1 RESEARCH FIELD: CYBERSECURITY OF VEHICULAR NETWORKS

Modern vehicles are becoming increasingly reliant on technology, with a wide range of systems and components being connected to the internet and each other. This includes everything from infotainment systems and navigation to advanced driver assistance systems and autonomous driving features. ISO 26262 describes these so-called "Electronic/Electrical (E/E) Systems" as systems that consist of electrical and electronic elements and components such as Electronic Control Unit (ECU)s, sensors, actuators, connections, and communication systems like Controller Area Network (CAN), Ethernet, and Bluetooth [5]. As these technologies become more important, the need for strong cybersecurity measures becomes increasingly important. Hackers and cybercriminals are constantly finding new ways to exploit vulnerabilities in these systems, which can have serious consequences. This includes their safety, privacy, finances, and operational viability. Ensuring the safety and security of connected vehicles is crucial to the success of the emerging world of connected and autonomous transportation.

The internal vehicular network architecture plays a crucial role in the overall cybersecurity of a modern vehicle because it determines how different vehicle systems and components are connected and communicate. Attack Paths play an important role in vehicle networks and security because they help companies understand the specific routes or methods that a malicious actor might use to attack a vehicle's systems or networks. For example, companies can implement appropriate security measures to prevent these attacks by understanding the attack paths that might be used to gain unauthorized access to a vehicle's systems. These include encryption, authentication protocols, and firewall systems to protect against cyber threats. A well-designed internal vehicular network architecture can help minimize cyberattack risk. As the number of systems and components that are connected to the internet and each other increases, so too does the complexity of the internal vehicular network architecture. This can make it more challenging to design and implement effective cybersecurity measures, as more potential points of vulnerability need to be addressed. Therefore, companies developing connected and autonomous vehicles need to prioritize cybersecurity in designing their internal vehicular network architecture, which can help to ensure the safety and security of the vehicle, as well as protect the privacy and personal data of drivers and passengers,

Methods for security testing, like penetration testing, are often carried out in the late stages of development, which can lead to the discovery of vulnerabilities at a time when it is more difficult and costly to address. Additionally, pentesting is considered to be a skill-based activity that is still carried out manually. It requires a high level of expertise and experience with other cybersecurity tools and techniques. A Threat Analysis and Risk Assessment (TARA) is a crucial element for security assessment. Companies perform a TARA during the development process to identify and prioritize potential risks and to implement controls or

countermeasures to reduce or mitigate those risks to an acceptable level. The increased complexity of modern vehicles and the arduous nature of the state-of-the-art security testing methods make it more unfeasible for companies to conduct security assessment testing as is done now. Thus, a need for an automated tool that can help resolve this issue and couple to the TARA process is apparent.

1.2 BACKGROUND AND MOTIVATION

As a computer science student with a passion for cybersecurity and a focus on cybersecurity in my studies, I joined the CarIT Security team at Mercedes-Benz Tech Innovation (MBTI) a year ago as a working student. I worked with automotive protocols such as CAN, CAN FD, FlexRay, and Ethernet, used software like CANoe, DTS, and proprietary tools for pentesting, performed scans, and created architecture diagrams of vehicular networks. Through my work there, I got to know the field of vehicular cybersecurity.

As already described, the internal vehicular network architecture plays a crucial role in the overall cybersecurity of a modern vehicle. MBTI is facing the same challenges mentioned in 1.1 and is looking for a solution to this problem. My supervisor and colleague proposed the topic of automated vehicular network evaluation as a way to solve the need for a tool to assess the security of these systems more efficiently. This approach automatically generates attack paths, which can be used to simulate and assess the security of a system in a more efficient and comprehensive manner. By doing so, it is possible to better identify and mitigate potential vulnerabilities early on in the development process, improving the overall flexibility and costs of security testing.

2 STATE OF THE ART

There are various approaches to assessing the security of vehicular networks. Cybersecurity standards and frameworks give guidance and best practices for designing, implementing, and testing the cybersecurity of automotive systems and networks. The following standards are mentioned in virtually every piece of literature; thus, they are the most important ones to consider:

ISO 26262 is an international standard for functional safety of E/E systems in vehicles that provides a framework for the development of safety-related systems, and lays out the safety requirements, safety goals, and safety measures to be considered during the whole lifecycle of a vehicle, including the design, development, production, and operation phases. ISO 26262 is divided into several parts, each of which addresses a specific aspect of functional safety. ISO 26262 is designed to help organizations manage the functional safety of their systems and ensure that the systems meet a defined level of safety and helps them to identify and mitigate potential hazards, and to demonstrate that the systems are safe for their intended use. This standard helps to ensure the safety of the vehicles by providing a systematic approach to identify and evaluate the risks associated with the safety-related systems and to implement appropriate measures to eliminate or reduce those risks to an acceptable level [5].

ISO 21434 is an international standard for the execution of functional testing and specifies engineering requirements for cybersecurity risk management regarding the lifecycle of electrical and electronic E/E architecture systems in road vehicles, including their components and interfaces [4]. ISO 21434 outlines the security requirements, goals, and measures to consider throughout the entire lifecycle of a vehicle, including design, development, production, and operation. It aims to assist organizations in managing the security of their vehicles and ensuring they meet a defined level of security by providing a systematic approach to identifying and evaluating security-related risks and implementing measures to reduce them to an acceptable level. The standard is intended to be used in conjunction with ISO 26262, which focuses on functional safety, to provide a comprehensive approach to ensuring the safety and security of vehicles. It also explains how to integrate security into the functional safety process, helping organizations manage security risks similarly to how they manage functional safety risks.

SAE J3061 is a guide for cybersecurity best practices for the automotive industry and was created based on existing methods. The guide provides a comprehensive set of best practices for securing automotive systems and vehicles from cyber threats and covers various aspects of cybersecurity, including threat modeling, risk management, security testing, incident response, and security management. They are intended to be flexible, pragmatic, and adaptable in their further application to the vehicle industry and other cyber-physical vehicle systems. It provides a framework for organizations to incorporate cybersecurity into the lifecycle of vehicle systems, information on standard tools and methods used in designing and verifying systems, basic principles for cybersecurity, and a foundation for further standards development. SAE J3061 is intended to be used in conjunction with other standards and guidelines, such as those mentioned

above [8].

AUTomotive Open System ARchitecture (AUTOSAR) is a standard for the development of software for ECUs in the automotive industry [1]. The goal of AUTOSAR is to create and establish an open and standardized software architecture for automotive ECUs that is scalable to different vehicle and platform variants, transferable of software, considering availability and safety requirements, collaboration between various partners, sustainable use of natural resources, and maintainable during the product lifecycle. This improves the efficiency of development, enables the integration, exchange, re-use, and transfer of functions within a vehicle network, and helps manage the growing complexity of technology and economics in automotive software development.

The following frameworks also, are mentioned frequently in literature and offer a base for the development of a tool to assess the security of vehicular networks:

TARA is an important process for ensuring the cybersecurity of systems and networks, especially in the automotive industry. In the context of automotive systems, TARA can be used to identify and evaluate potential threats and vulnerabilities to the electronic and electrical (E/E) architecture of vehicles. This includes identifying assets such as connected systems and networks and evaluating the likelihood and potential impact of threats such as cyber-attacks, hacking, and software vulnerabilities. TARA can help prioritize these threats and vulnerabilities based on their potential impact on the safety, financial, operational, privacy, and aspects. Then, it can be used to determine appropriate controls or countermeasures to mitigate these risks, such as implementing security protocols, software updates, and network segmentation. TARA process can be used to ensure compliance with industry standards such as ISO 26262 or ISO 21434. Additionally, TARA can be integrated with other frameworks, such as the HEAVENS security model, which also focuses on identifying security requirements in the context of the automotive E/E architecture systems. Regularly reviewing and updating the TARA process is crucial to keep up with the evolving threats and vulnerabilities in the automotive industry, which is constantly evolving with the integration of new technologies such as connected cars, autonomous driving, and V2X communication. By identifying and mitigating potential risks through the TARA process, automotive systems can be made more secure and reliable, protecting the assets, and the safety of the passengers, and the data they hold [7].

An important framework is HEAling Vulnerabilities to Enhance Software, Security, and Safety (HEAVENS), which performs risk assessments of general IT systems and models explicitly built for automotive systems. The HEAVENS framework uses threat and impact levels to calculate risks [3]. The primary objective of the framework is to identify security requirements and vulnerabilities in automotive systems and to provide countermeasures to minimize the risks associated with these vulnerabilities. It uses the Microsoft STRIDE model for threat modeling and aligns its impact level estimation parameters with established industry standards such as ISO 26262. It is a great candidate as a framework for automotive risk assessments over traditional IT risk assessment models.

Another framework is the E-safety vehicle intrusion protected applications (EVITA) framework, which essentially performs the same things as HEAVENS, but also considers the potential of attacks to impact the privacy of vehicle passengers, financial losses, and the operational capabilities of the vehicles systems

and functions [6].

Many of these approaches aim to standardize the process of assessing the security of vehicular networks. However, most of them are based on manual penetration testing and manual vulnerability assessment today. This is because penetration testing is an experienced-based and explorative skill that is difficult to automate. Further research aims to improve or couple existing approaches like performing a TARA, as well as automate and accelerate the process of security testing.

F. Sommer et al. introduce the concept of Model-Based Security Testing using an Extended Finite State Machine (EFSM) model in their paper "Model-Based Security Testing of Vehicle Networks" [10]. The Automotive Security Model section describes an E/E Architecture, security measures, and further development artifacts to protect vehicles against attacks. The model is based on the EFSM, with nodes representing attacker privileges and transitions representing a vulnerability. The Proof of Concept section of the paper demonstrates how the model can be used to identify different Attack Paths, analyze the model for attack paths, and execute the attack paths on a real vehicle. The incremental approach allows for the redefinition of attack paths, making it useful at different stages during development. The paper concludes that this approach can be useful in identifying attack paths and potential vulnerabilities in automotive systems, thus helping to improve the security of vehicles.

F. Sommer et al. further expand on the same model-based approach by using a database of successful vehicular penetration tests in their paper "Attack Path Generation Based on Attack and Penetration Testing Knowledge." The attack path generation process involves using an attack database, which describes vulnerabilities and exploits that can be used, including attack taxonomy and classification, attack steps, requirements, restrictions, components, and interfaces. The database can also be used to find new attack paths by permuting existing attack steps. Additionally, the process of creating the database can be done iteratively over several penetration tests and can be transferred to test scripts. However, there is a risk that the attack path generated may not be transferable, which can be circumvented by permuting previous attacks. The authors also suggest that further testing activities, such as black-box testing, should be carried out. Despite its limitations, this approach can be used as a useful tool to automate the process of penetration testing and improve the efficiency of security testing in the automotive industry. [9].

J. Dürrwang et al. further describe the concept of attacker privileges mentioned in the papers above in "Automation in Automotive Security by Using Attacker Privileges" [2]. It defines several types of privileges that an attacker may seek to gain access to a vehicle's communication system and components, such as "Read/Write," "Execute," "Read," "Write," and "Full Control.". They note that channels that are not protected by security measures can be immediately accessed by an attacker, but interpretation is needed in other cases. It also mentioned that the attacker needs to reach one of these privileges to access further attached communication systems and components. The authors applied their privilege model to real-world automotive security attacks to demonstrate its practical use, in which an attacker is connecting to the vehicle via the On-board diagnostics (OBD) port, which is connected to the central gateway via CAN, and then uses the central gateway to gain access to the internal vehicle network. They also

showed the automatic generation of attack trees using a model checker in a custom software tool and an application of their privileges in security testing by describing attack paths. In future work, the authors plan to formalize the security testing approach to allow for early testing during development and to evaluate the TARA and security testing approach in a case study.

In contrast, D. Zelle et al. introduce a concrete approach, "ThreatSurf" [11], which presents an algorithm for automated generation and rating of attack paths in the automotive industry, using various attack building blocks and assessing attack feasibility. The attack feasibility assessment can be used in a TARA to assess an entire attack path of a threat scenario. It also discusses different methods for calculating attack paths, such as Sum, Average, Maximum, and Hybrid-weighted Sum. The paper describes four different types of threat agents - Thief and Owner, Terrorist, Organized Crime and Mechanic, Hacktivist, and Foreign Government - and their motivations, capabilities, and window of opportunity for performing an attack. The paper provides an example of how the proposed attack feasibility rating concept can be applied to threat scenarios derived from the use cases and also compares it with other rating approaches such as attack-potential based approaches, Common Vulnerability Scoring System (CVSS) based approaches, and attack vector-based approaches. The proposed attack feasibility rating concept is based on the attack-potential approach due to the complex nature of attacks against electric vehicles. Other approaches include the CVSS and attack vectors. They conclude that attack-potential based approaches have high flexibility but high complexity, CVSS-based approaches are easier to handle but have lower flexibility and attack vector-based approaches are simpler but less suited for automotive applications.

3

TOOL

BIBLIOGRAPHY

[1] AUTOSAR Development Partnership. *AUTOSAR 4.2.2 Specification*. Munich, Germany: AUTOSAR Development Partnership, 2019. URL: https://www.autosar.org/standards/standard-downloads/.

[2] Jürgen Dürrwang, Florian Sommer, and Reiner Kriesten. "Automation in Automotive Security by Using Attacker Privileges". In: (2021). URL: https://hss-opus.ub.ruhr-uni-bochum.de/opus4/frontdoor/index/index/year/2021/docId/8357.

[3] European Union's Horizon 2020 research and innovation programme. *HEAVENS: HEAling Vulnerabilities to ENhance Software Security and Safety*. Brussels, Belgium: European Union's Horizon 2020 research and innovation programme, 2019. URL: https://cordis.europa.eu/project/id/866041.

[4] International Organization for Standardization. *Road vehicles – Cybersecurity engineering – Guideline and general aspects*. Geneva, Switzerland: International Organization for Standardization, 2020. URL: https://www.iso.org/standard/73547.html.

[5] International Organization for Standardization. *Road vehicles – Functional safety*. Geneva, Switzerland: International Organization for Standardization, 2018. URL: https://www.iso.org/standard/64539.html.

[6] National Institute of Standards and Technology. *Evaluating the Vulnerability of Information Technology Assets (EVITA)*. Gaithersburg, Maryland, USA: National Institute of Standards and Technology, 2003. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

[7] National Institute of Standards and Technology. *Threat Analysis Risk Assessment (TARA)*. Gaithersburg, Maryland, USA: National Institute of Standards and Technology, 2011. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[8] SAE International. *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (SAE J3061)*. Warrendale, Pennsylvania, USA: SAE International, 2018. URL: https://www.sae.org/standards/content/j3061_201801/.

[9] Florian Sommer and Reiner Kriesten. "Attack Path Generation Based on Attack and Penetration Testing Knowledge". In: (2022).

[10] Florian Sommer, Reiner Kriesten, and Frank Kargl. "Model-Based Security Testing of Vehicle Networks". In: *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*. 2021, pp. 685–691. DOI: 10.1109/CSCI54926.2021.00179.

[11] Daniel Zelle et al. "ThreatSurf: A method for automated Threat Surface assessment in automotive cybersecurity engineering". In: *Microprocessors and Microsystems* 90 (2022), p. 104461. ISSN: 0141-9331. DOI: https://doi.org/10.1016/j.micpro.2022.104461. URL: https://www.sciencedirect.com/science/article/pii/S0141933122000321.

ACRONYMS

AUTOSAR AUTomotive Open System ARchitecture. 4

CAN Controller Area Network. 1, 5

CVSS Common Vulnerability Scoring System. 6

E/E Electronic/Electrical. 1, 3

ECU Electronic Control Unit. 1, 4

EFSM Extended Finite State Machine. 5

EVITA E-safety vehicle intrusion protected applications. 4

HEAVENS HEAling Vulnerabilities to Enhance Software, Security, and Safety. 4

OBD On-board diagnostics. 5

STRIDE Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege. 4

TARA Threat Analysis and Risk Assessment. 1, 4

GLOSSARY

Attack Path As defined in [4], an attack path is a set of deliberate actions that an attacker takes to realize a threat scenario, a potential cause of compromise of cybersecurity properties of one or more assets in order to realize a damage scenario. . 1, 5