EMILIJA KASTRATOVIĆ

COMPARING DIFFERENT VEHICLE ARCHITECTURES BASED ON ATTACK PATH ANALYSIS

COMPUTER NETWORKS AND IT SECURITY
PROJECT PROPOSAL

Supervisor: Michael Wolf

Institut für Verteilte Systeme
Institute of Distributed Systems

University of Ulm
uulm.de/in/vs
January 12, 2023

ABSTRACT

The increasing reliance of modern vehicles on technology and connectivity has made the cybersecurity of vehicular networks a critical research field. Ensuring the 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

In this bachelor thesis, we propose a tool to automate the evaluation of the attack path feasibility of multiple vehicular network architectures. This tool would involve generating attack paths automatically, then evaluating the network's security based on the attack paths. Multiple different network architectures will be created and evaluated, and the results will be compared.

Emilija Kastratović: *Comparing different vehicle architectures based on attack path analysis,* Computer Networks and IT Security
Project Proposal, © January 12, 2023.

WEBSITE:
uulm.de/in/vs

E-MAIL:
emilija.kastratovic@uni-ulm.de

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 "E/E Systems" as systems that consist of electrical and electronic elements and components such as ECUs, sensors, actuators, connections, and communication systems like CAN, Ethernet, and Bluetooth [1].

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. This is because it determines how different vehicle systems and components are connected and communicated. 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. This 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 TARA, a Threat Analysis, and Risk Assessment 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:

- proposes an execution of functional testing and specifies engineering requirements for cybersecurity risk management regarding the concept, product development, production, operation, maintenance, and decommissioning of electrical and electronic E/E architecture systems in road vehicles, including their components and interfaces [2].
- provided a guide on vehicle cybersecurity and was created based on existing practices being implemented or reported in industry, government, and conference papers. The best practices are intended to be flexible, pragmatic, and adaptable in their further application to the vehicle industry and other cyber-physical vehicle systems [3].
- AUTOSAR is a standard for the development of software for electronic control units (ECUs) in the automotive industry [4].

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:

- Usually, a TARA (Threat and Risk Assessment) [5] is performed to identify the threats and vulnerabilities of the system. A TARA typically involves using various tools and techniques, such as risk assessment methods, threat modeling, vulnerability assessments, and security testing.
- An important framework is HEAVENS, which performs risk assessments of general IT systems and models explicitly built for automotive systems. HEAVENS framework uses threat and impact levels to calculate ris [6].
- Another framework is the 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 [7].

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.

- F. Sommer et al. introduce the concept of Model-Based Security Testing using an EFSM (Extended Finite State Machine) model in their paper "Model-Based Security Testing of Vehicle Networks" [8]. The Automotive Security Model

section describes the E-E Architecture, security measures and further development artifacts to protect vehicles against attacks, and the characteristics of attacks, including violated security property, exploited vulnerability, and attacker privileges. The model is based on the EFSM, with model elements of Attacker Privileges and transitions of 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. In the Discussion section, the paper notes that the identification of attack paths is similar to performing a TARA (Threat Assessment and Risk Analysis) and that this approach considers security requirements or measures unlike TARA. The potential to couple TARA is also mentioned, as well as the need for prioritization due to the large number of vehicular components. 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.

- J. Dürrwang et al. further describe the concept mentioned in "Model-Based Security Testing of Vehicle Networks" and "Attack Path Generation Based on Attack and Penetration Testing Knowledge" in their paper "Automation in Automotive Security by Using Attacker Privileges" [9]. 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". The passage notes that channels that are not protected by security measures can be immediately accessed by an attacker, but interpretation is needed in other cases. The example given is an attacker connecting to the vehicle via the OBD (On-Board Diagnostics) port, which is connected to the central gateway via CAN (Controller Area Network), and then using the central gateway to gain access to the internal vehicle network. It also mentioned that the attacker needs to reach one of these privileges to access further attached communication systems and components.

- F. Sommer et al. further propose a model-based approach to automate penetration testing of vehicles by using a database of successful vehicular penetration tests. The approach is based on the Model-Based Security Testing of Vehicle Networks with EFSM (Extended Finite State Machine) as the foundation. The problem with current security testing methods is that they are carried out in the late stages of development and penetration testing is done manually, which is considered difficult to automate due to the high complexity of modern vehicles. The solution proposed is to automate penetration testing with the help of a database containing successful penetration testing and automatically generating attack paths. The approach and modeling process involve penetration testing and creating a security model based on E-E Architecture, which takes into account the entities that have an impact on the cyber security of a vehicle, and introducing the concept of attacker privileges. The attack path generation process involves using an attack database that is built based on EFSM. The database describes which vulnerabilities and exploits 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. The discussion section highlights that this approach is similar to TARA and can be coupled with it. 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. [10].

- In contrast, D. Zelle et al. introduce a concrete approach that can be used in a TARA called "ThreatSurf" [11]. They show the feasibility of their approach using an algorithm for automated generation and rating of attack paths using the attack building blocks and attack feasibility.

3 PROBLEM STATEMENT

3.1 PROJECT TYPE

My bachelor thesis segues into the problems described in 1.1 by proposing the idea of a tool that can be used to automate the evaluation of vehicular network security. This bachelor thesis is done in cooperation with Mercedes-Benz Tech Innovation.

I will conduct attack path analyses on different internal vehicle network architectures and then compare based on which provides more security regarding attack paths.

First, I will create multiple architecture diagrams with different topologies (A1 4.2).
Second, I will write a script-based program, which automizes the evaluation of the different topologies (F1 4.2) (F2 4.2) (F3 4.2) (F4 4.2) (F5 4.2). Finally, I will decide on a criteria (A2 4.2), how to rate the different topologies, and compare them to conclude which architecture offers the most security (A3 4.2).

The thesis will be both exploratory and implementory in nature, with a focus on the latter.

3.2 THESIS QUESTIONS

The main question of this thesis is:

- How secure is the given vehicular network architecture?

However, other questions might be, but are not limited to:

- What architectural approach makes a network safer than others?
- How do small changes in network positioning affect the network security overall?
- How do simple and more branched out networks compare in terms of security?
- How can different architectures be rated based on attack paths?

4 TOOL DESIGN AND IMPLEMENTATION

4.1 PURPOSE

The tool's purpose is to help security architects quickly evaluate the attack path feasibility of a given vehicular network architecture.

4.2 (FUNCTIONAL) REQUIREMENTS

(Functional) Requirements include but are not limited to:

General:

- A1 Multiple different vehicular network architecture diagrams as files of a certain datatype
- A2 A criteria to evalute the architectures
- A3 Compare architectures with one another and conclude which architecture offers the most security

Tool:

- F1: The tool will take a file as input. This file contains the network diagram of the vehicle, which was created beforehand. The network diagram consists of ECUs (nodes) and bus systems (edges) connecting the ECUs. The file content will be parsed to a convenient datatype.
- F2: Each ECU and each bus system will have an attack feasibility rating, or "difficulty," that can be changed in the script.
- F3: ECUs can then be marked as entry points or target points.
- F4: Next, an algorithm (potentially as mentioned in ThreatSurf [11]) will find the most feasible attack path from each entry to each target based on the ratings. However, the algorithm can also be changed in the script.
- F5: The results are then output to a table, where the overall security of the network architecture is evaluated based on a criteria (see 4.2).

4.3 OTHER REQUIREMENTS

other requirements such as hardware, software or non-funcitonal requirements include, but are not limited to:

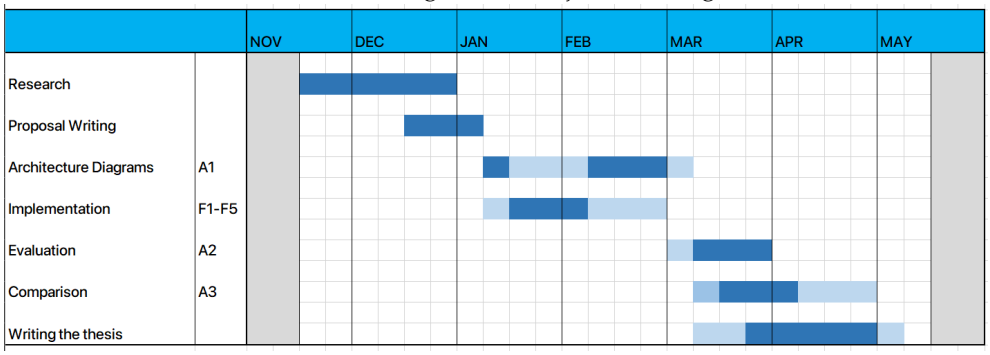
- N1: The tool must be script based
- N2: The programming language is Python (version not yet specified)

- N3: A virtual machine with a Linux distribution (distribution not yet specified)
- N4: Appropriate libraries for the tool
- N5: An IDE like PyCharm (recommended) or a text editor to change the script
- N6: A Git repository where the code and thesis will be stored

5 PROJECT SCHEDULE

5.1 THESIS TIMELINE

The coarse schedule looks as following and is subject to change:



5.2 CONTINGENCY PLANS

The project is subject to change.
New insights gained during the project might affect some aspects of tool implementation (4) or diagrams (4.2) This may inclue implementation problems, such as library or datatype incompatibilities, that might arise while working on the tool. It can be addressed using other libraries, datatypes, or by changing the implementation.

BIBLIOGRAPHY

[1] International Organization for Standardization, *Road vehicles – functional safety*, Geneva, Switzerland: International Organization for Standardization, 2018. [Online]. Available: https://www.iso.org/standard/64539.html.

[2] International Organization for Standardization, *Road vehicles – cybersecurity engineering – guideline and general aspects*, Geneva, Switzerland: International Organization for Standardization, 2020. [Online]. Available: https://www.iso.org/standard/73547.html.

[3] SAE International, *Cybersecurity guidebook for cyber-physical vehicle systems (sae j3061)*, Warrendale, Pennsylvania, USA: SAE International, 2018. [Online]. Available: https://www.sae.org/standards/content/j3061_201801/.

[4] AUTOSAR Development Partnership, *Autosar 4.2.2 specification*, Munich, Germany: AUTOSAR Development Partnership, 2019. [Online]. Available: https://www.autosar.org/standards/standard-downloads/.

[5] National Institute of Standards and Technology, *Threat analysis risk assessment (tara)*, Gaithersburg, Maryland, USA: National Institute of Standards and Technology, 2011. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[6] 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. [Online]. Available: https://cordis.europa.eu/project/id/866041.

[7] National Institute of Standards and Technology, *Evaluating the vulnerability of information technology assets (evita)*, Gaithersburg, Maryland, USA: National Institute of Standards and Technology, 2003. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

[8] F. Sommer, R. Kriesten, and F. 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.

[9] J. Dürrwang, F. Sommer, and R. Kriesten, "Automation in automotive security by using attacker privileges," 2021. [Online]. Available: https://hss-opus.ub.ruhr-uni-bochum.de/opus4/frontdoor/index/index/year/2021/docId/8357.

[10] F. Sommer and R. Kriesten, "Attack path generation based on attack and penetration testing knowledge," 2022.

[11] D. Zelle, C. Plappert, R. Rieke, D. Scheuermann, and C. Krauß, "Threatsurf: A method for automated threat surface assessment in automotive cybersecurity engineering," *Microprocessors and Microsystems*, vol. 90, p. 104461, 2022, ISSN: 0141-9331. DOI: https://doi.org/10.1016/j.micpro.2022.104461. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0141933122000321.