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 8, 2023

ABSTRACT

The increasing reliance of modern vehicles on technology and connectivity has made the cybersecurity of vehicular networks an important 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, I propose the idea for a tool to automate the evaluation of the security of a vehicular network architecture. This tool would involve generating attack paths automatically, and then evaluating the security of the network based on the attack paths. Multiple different network architectures will be created and evaluated, and the results will be compared to each other. The goal of this project is to improve the overall security testing for Mercedes-Benz Tech Innovation (MBTI) and to better identify and mitigate potential vulnerabilities early on in the development process.

Emilija Kastratović: *Comparing different vehicle architectures based on attack path analysis,* Computer Networks and IT Security
Project Proposal, © January 8, 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 which consists of electrical and electronic elements and components such as ECUs, sensors, actuators, connections and communication systems like CAN, Ethernet, Bluetooth, etc.[1]
As these technologies become more prevalent, 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 for both the safety and privacy of drivers.
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 systems and components within the vehicle are connected and communicate with each other.
Attack paths play an imprtant role in vehicle networks and security because they help companies to understand the specific routes or methods that a malicious actor might use to attack a vehicle's systems or networks. Identifying and understanding attack paths is crucial for protecting the safety and security of connected and autonomous vehicles, as it allows companies to anticipate and prepare for potential threats. For example, by understanding the attack paths that might be used to gain unauthorized access to a vehicle's systems, companies can implement appropriate security measures to prevent these attacks from occurring.
These might include the use of encryption, authentication protocols, and firewall systems to protect against cyber threats. A well-designed internal vehicular network architecture can help to minimize the risk of cyberattacks.

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 difficult to design and implement effective cybersecurity measures, as there are more potential points of vulnerability that need to be addressed.
Therefore, it is important for companies developing connected and autonomous vehicles to prioritize cybersecurity in the design of 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 late stages of develpment, which can lead to the discovery of vulnerabilities at a time when it is more difficult and costly to address them.

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 crucial element for security assessment is a TARA, a Threat Analysis and Risk Assessment. Companies perform a TARA during the development process to identify and prioritize potential risks, a nd to implement controls or countermeasures to reduce or mitigate those risks to an acceptable level.

The increased complexity of modern vehicles and arduous nature of the state-of-the-art security testing methods make it more unfeasibile for companies to conduct security assessment testing as is done right now. Thus, a need for an automated tool which can help resovle 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 cyber security in my studies, I joined the CarTT Security team at Mercedes-Benz Tech Innovation (MBTI) a year ago as a working student. I worked with automotive protocols such as CAN, CANFD, FlexRay, and Ethernet, used software like CANoe, DTS, as well as proprietary tools for pentesting, and 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 as 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 more efficiently assess the security of these systems. This approach involves generating attack paths automatically, which can be used to simulate and assess the security of a system in a more efficient and comprehensive manner. Doing so, it is possible to better identify and mitigate potential vulnerabilities early on in the development process and ultimately improves the overall flexibility and costs of security testing for MBTI.

2 STATE OF THE ART

There a various approaches to assess 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 literature and are also used at MBTI, thus they are the most important ones to consider:

- ISO21434 proposes in particular an execution of functional testing and specifies engineering requirements for cybersecurity risk management regarding 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].
- SAE J3061 provides a guide on vehicle cybersecurity and was created based off of, and expanded on from, existing practices which are 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 as well as to 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. TARA typically involves the use of a variety of tools and techniques, such as risk assessment methods, threat modeling, vulnerability assessments, and security testing. A TARA is used by the security architectures at MBTI, so including it in my thesis is a must It is evaluated using a method called CVSS[6] (Common Vulnerability Scoring System).
- An important framework is HEAVENS, which perform risk assessments of general IT systems and models built specifically for automotive systems. HEAVENS framework uses both a threat level and impact level to calculate risk[7].
- 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 vehicle's systems and functions[8].

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 as of today. This is due to the fact that penetration testing is an experienced-based and explorative skill which is difficult to automate. Further research aims to improve or couple to already existing approaches like performing a TARA.

- F. Sommer, R. Kriesten, and F. Kargl propose a model-based method for security testing of vehicle networks[9] using an EFSM (Extended Finite State Machine). The nodes of the EFSM are the attacker privileges and the transitions are the actions or vulnerabilities that can be performed by the attacker. However, this approach yet does not have a practical implementation.

- J. Dürrwang et al. describe this concept of using EFSMs in "Automation in Automotive Security by Using Attacker Privileges"[10]. Also no practical implementation is given.

- They further propose a method where both concepts are used in combination with a database containing successful vehicular penetration tests is proposed to faciliate and automate penetration testing by generating attack paths[11].

- In contrast, D. Zelle et al. introduce concrete approach that can be used in a TARA, called "ThreatSurf"[12]. They show 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 for a tool which can be used to automize the evaluation of the security of vehicular networks. This bachelor thesis is done in cooperation with Mercedes-Benz Tech Innovation. To give this project a more scientific background, I will do the following:

I will conduct attack path analyses on different internal vehicle network architectures. The architectures then I will compare based on which provides more security with regard to attack paths.

First, I will be creating multiple different architecture diagrams, each 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 with each other to conclude which archtiecture offers the most security (A3 4.2).

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

3.2 THESIS QUESTIONS

Since the thesis is based on a tool needed by MBTI, the main question 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?
- Is a shorter attack path more vulnerable than longer attack paths?

4 TOOL DESIGN AND IMPLEMENTATION

4.1 PURPOSE

The purpose of the tool is to help security architects at MBTI to quickly evaluate the security of a given vehicular network architecture.

4.2 (FUNCTIONAL) REQUIREMENTS

(Funcitonal) Requirements include but are not limited to:

General:

- A1 Multiple different vehicular network archtitecure 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: It will take a file as input. This file contains the network diagram of the vehicle, which I have 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. Fortunately, a member of the MBTI team has already implemented a convenient ARXML parser, that might be used in this tool.
- F2: Each ECU and each bus system will have a rating, or "difficulty", that can be changed in the script.
- F3: ECUs can then be marked as entry vectors or target vectors.
- F4: Next, an algorithm (potentially as mentioned in ThreatSurf[12]) will find the most feasibile 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 evaluted based on a criteria.

4.3 OTHER REQUIREMENTS

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

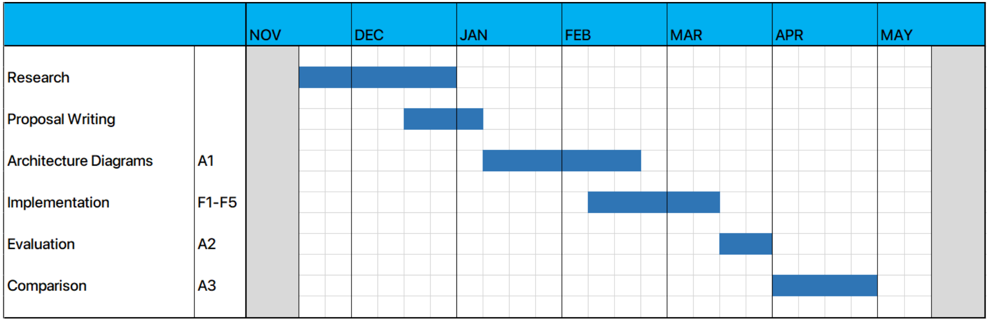
- N1: Tool must be script based

- N2: 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 due to the following reasons:

- Due to other university assignments, I might not be able to follow the timeline as strictly as planned
- New insights gained during the projet might affect some aspects of tool implementation(4), diagrams(4.2), or thesis questions(3.2)
- Implementation problems, such as bugs or library incompatibilities, might arise while working on the tool

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] FIRST, *Common vulnerability scoring system (cvss)*, Bethesda, Maryland, USA: FIRST, 2005. [Online]. Available: https://www.first.org/cvss/.

[7] 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.

[8] 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.

[9] 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.

[10] J. Dürrwang, F. Sommer, and R. Kriesten, "Automation in automotive security by using attacker privileges," 2021. [Online]. Available: https://www.h-ka.de/en/ieem/profile.

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

[12] 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. 104 461, 2022, ISSN: 0141-9331. DOI: https://doi.org/10.1016/j.micpro.2022.104461. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0141933122000321.