EMILIJA KASTRATOVIC

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
December 29, 2022

ABSTRACT

A short summary of topic, main research questions, central methods and overall goal of the project as detailed in the proposal.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Emilija Kastratovic: *Comparing different vehicle architectures based on attack path analysis,* Computer Networks and IT Security
Project Proposal, © December 29, 2022.

WEBSITE:
uulm.de/in/vs

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

CONTENTS

1 INTRODUCTION

1.1 RESEARCH FIELD

introduction into the coarse research field of the project
scope of this project: define what will be included and what not

This bachelor thesis is done in cooperation with Mercedes-Benz Tech Innovation. The company proposed the idea for a tool which can be used to automize the evaluation of the security of vehicular networks. To give this project a more scietific background, I will do the following:

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

First, I will be creating multiple different architecture diagrams.
Second, I will write a program, which automizes the evaluation of the different topologies.
Finally, I will decide on a criteria how to rate the different topologies and compare them with it.

1.2 PROJECT TYPE

type of the project. this may be implementation centric, exploratory/analytic or constructive/synthetic:

1.2.1 implementation centric

practical transfer of a theoretical concept, e. g. software

1.2.2 exploratory/analytic

define, categorize and evaluate an idea, concept or situation not addressed before in the same dimension as is proposed by this project

example

a new type of attack/exploit; transfer of a typical IT strategy to a new domain like automotive or embedded systems

1.2.3 constructive/synthetic

put together existing implementations of parts or concepts in a novel way or with an unexplored purpose

example

design and composition of a laboratory environment

The bachelor thesis is both implementation centric as well as exploratory/analytic.

The main focus of the project will be to compare different internal vehicle network architectures based on which provides more security with regard to attack paths.

I will create ten different vehicular network architecture diagrams.

2 PROJECT IDEA

detailed discussion of the project's topic, the initial idea and the motivation for pursuing the project

As a computer science student with a passion for cybersecurity and a focus on cyber security in my studies, I was excited to join the CarTT Security team at Mercedes-Benz Tech Innovation a year ago as a working student. When the opportunity arose to complete my bachelor's thesis at the company, I was eager to take on the challenge and contribute to the team's efforts.

My supervisor and colleague proposed the topic of automated vehicular network evaluation as a way to address the need for a tool to more efficiently assess the security of these systems.

One common issue in the field of information security is that security testing is 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 them. Additionally, traditional penetration testing approaches, which rely on manual, experience-based, and explorative techniques, are considered difficult to automate due to the high complexity of modern systems.

To address these issues, there is a growing interest in model-based security testing and automating penetration testing with the help of a database containing successful penetration testing techniques. 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. By leveraging these advanced techniques, it is possible to better identify and mitigate potential vulnerabilities early on in the development process. Doing so ultimately improves the overall flexibility and costs of security testing.

3 STATE OF THE ART

enumerate and discuss related work and practical solutions that form the state of the art

argue how this state of the art supports the project and where current solutions have shortcomings this project ventures to overcome

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. Examples include the ISO 21434 standard for automotive cybersecurity[1], the SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems[2], and the AUTOSAR (AUTomotive Open System ARchitecture) standard for automotive software architecture[3].

Usually, a TARA (Threat and Risk Assessment)[4] 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. It may also involve the use of specialized software or services to automate or streamline the process.

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 the complexity of modern vehicular networks makes it difficult to automate the process.

Further literature aims to improve or couple to already existing appproaches like performing a TARA.
F. Sommer, R. Kriesten, and F. Karg propose a model-based method for security testing of vehicle networks[5] 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.
J. Dürrwang, F.Sommer and R. Kriesten describe this concept of using EFSMs in "Automation in Automotive Security by Using Attacker Privileges"[6].
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[7].

Overall, the testing of automotive cybersecurity is a complex and evolving field, and it involves the use of a variety of tools and techniques to ensure that automotive systems and networks are secure and reliable.

4 REQUIREMENTS ANALYSIS

goal of this project, approach

give a detailed definition of the initial problem that requires a solution, respectively the challenges of transferring or synthesizing a concept into a construction or realization

define use cases and the deduced requirements for the implementation or construction

***just implementation and constructive projects**, remove this chapter if your project is of any other type.*

In this thesis you have to make attack path analyses on different internal vehicle network architectures and compare them based on which provides more security with regards attack paths. The first step would be creating multiple different architecture diagrams. Then you have to write a program, which reads files of a vehicle network topology, maps this to a list of entry point and target ECUs, and generates a list of all possible attack paths. To get a quick and early result, this list should be sorted by the number of hops over each gateway. The next step would be giving each entry point, gateway and connection a rating on how big the attack feasibility for this element is. Then, attack paths can be calculated - e.g. with the formula of the paper ”ThreatSurf A method for automated Threat Surface assessment”. At last, you have to decide on a criteria on how to rate the different topologies and compare them with it.

5 FUNCTIONAL SPECIFICATION

***just implementation and constructive projects**, remove this chapter if your project is of any other type.*

specification of technical requirements, entities, interfaces, protocols and procedures that will be employed to meet the identified requirements,

interdependencies of technical, human or environmental entities

6 PROBLEM STATEMENT

goal of this project, approach

give a detailed definition of the initial problem that requires a solution, especially the challenges of exploring the field and how they are addressed. This explicitly includes the analysis of the lack of information on the topic, like difficulties in gathering information or resources and reasons why the topic was not pursued before. This has to point out that the project is worthwhile and realistic to complete and on what ground this is assumed.

questions that are to be answered, general tasks that can be identified to achieve the goal

***just exploratory projects**, remove this chapter if your project is of any other type.*

Etiam pede massa, dapibus vitae, rhoncus in, placerat posuere, odio. Vestibulum luctus commodo lacus. Morbi lacus dui, tempor sed, euismod eget, condimentum at, tortor. Phasellus aliquet odio ac lacus tempor faucibus. Praesent sed sem. Praesent iaculis. Cras rhoncus tellus sed justo ullamcorper sagittis. Donec quis orci. Sed ut tortor quis tellus euismod tincidunt. Suspendisse congue nisl eu elit. Aliquam tortor diam, tempus id, tristique eget, sodales vel, nulla. Praesent tellus mi, condimentum sed, viverra at, consectetuer quis, lectus. In auctor vehicula orci. Sed pede sapien, euismod in, suscipit in, pharetra placerat, metus. Vivamus commodo dui non odio. Donec et felis.

Etiam suscipit aliquam arcu. Aliquam sit amet est ac purus bibendum congue. Sed in eros. Morbi non orci. Pellentesque mattis lacinia elit. Fusce molestie velit in ligula. Nullam et orci vitae nibh vulputate auctor. Aliquam eget purus. Nulla auctor wisi sed ipsum. Morbi porttitor tellus ac enim. Fusce ornare. Proin ipsum enim, tincidunt in, ornare venenatis, molestie a, augue. Donec vel pede in lacus sagittis porta. Sed hendrerit ipsum quis nisl. Suspendisse quis massa ac nibh pretium cursus. Sed sodales. Nam eu neque quis pede dignissim ornare. Maecenas eu purus ac urna tincidunt congue.

Donec et nisl id sapien blandit mattis. Aenean dictum odio sit amet risus. Morbi purus. Nulla a est sit amet purus venenatis iaculis. Vivamus viverra purus vel magna. Donec in justo sed odio malesuada dapibus. Nunc ultrices aliquam nunc. Vivamus facilisis pellentesque velit. Nulla nunc velit, vulputate dapibus, vulputate id, mattis ac, justo. Nam mattis elit dapibus purus. Quisque enim risus, congue non, elementum ut, mattis quis, sem. Quisque elit.

Maecenas non massa. Vestibulum pharetra nulla at lorem. Duis quis quam id lacus dapibus interdum. Nulla lorem. Donec ut ante quis dolor bibendum condimentum. Etiam egestas tortor vitae lacus. Praesent cursus. Mauris bibendum pede at elit. Morbi et felis a lectus interdum facilisis. Sed suscipit gravida turpis. Nulla at lectus. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Praesent nonummy luctus nibh. Proin turpis nunc, congue eu, egestas ut, fringilla at, tellus. In hac habitasse platea dictumst.

7 AGREEMENT ON DELIVERABLES

***just exploratory projects**, remove this chapter if your project is of any other type.*

which results are expected, especially what kind of results will be produced, this may be a concept and proof thereof, a physical lab or teaching environment, an actual test setup and other tangible or equivalent deliverables

Vivamus eu tellus sed tellus consequat suscipit. Nam orci orci, malesuada id, gravida nec, ultricies vitae, erat. Donec risus turpis, luctus sit amet, interdum quis, porta sed, ipsum. Suspendisse condimentum, tortor at egestas posuere, neque metus tempor orci, et tincidunt urna nunc a purus. Sed facilisis blandit tellus. Nunc risus sem, suscipit nec, eleifend quis, cursus quis, libero. Curabitur et dolor. Sed vitae sem. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Maecenas ante. Duis ullamcorper enim. Donec tristique enim eu leo. Nullam molestie elit eu dolor. Nullam bibendum, turpis vitae tristique gravida, quam sapien tempor lectus, quis pretium tellus purus ac quam. Nulla facilisi.

Duis aliquet dui in est. Donec eget est. Nunc lectus odio, varius at, fermentum in, accumsan non, enim. Aliquam erat volutpat. Proin sit amet nulla ut eros consectetuer cursus. Phasellus dapibus aliquam justo. Nunc laoreet. Donec consequat placerat magna. Duis pretium tincidunt justo. Sed sollicitudin vestibulum quam. Nam quis ligula. Vivamus at metus. Etiam imperdiet imperdiet pede. Aenean turpis. Fusce augue velit, scelerisque sollicitudin, dictum vitae, tempor et, pede. Donec wisi sapien, feugiat in, fermentum ut, sollicitudin adipiscing, metus.

Donec vel nibh ut felis consectetuer laoreet. Donec pede. Sed id quam id wisi laoreet suscipit. Nulla lectus dolor, aliquam ac, fringilla eget, mollis ut, orci. In pellentesque justo in ligula. Maecenas turpis. Donec eleifend leo at felis tincidunt consequat. Aenean turpis metus, malesuada sed, condimentum sit amet, auctor a, wisi. Pellentesque sapien elit, bibendum ac, posuere et, congue eu, felis. Vestibulum mattis libero quis metus scelerisque ultrices. Sed purus.

Donec molestie, magna ut luctus ultrices, tellus arcu nonummy velit, sit amet pulvinar elit justo et mauris. In pede. Maecenas euismod elit eu erat. Aliquam augue wisi, facilisis congue, suscipit in, adipiscing et, ante. In justo. Cras lobortis neque ac ipsum. Nunc fermentum massa at ante. Donec orci tortor, egestas sit amet, ultrices eget, venenatis eget, mi. Maecenas vehicula leo semper est. Mauris vel metus. Aliquam erat volutpat. In rhoncus sapien ac tellus. Pellentesque ligula.

8 (SYSTEM) DESIGN

details on the general approach, solution strategies and implementation methods

specification of the concrete lab, experiment or test setup or the prototype…

OR the architecture and detailed design plan of the implementation…

…that is expected to achieve the goals,

IN PARTICULAR: that answers the identified research questions

OR meets the requirements

identify/partition work packages and their dependencies

Cras dapibus, augue quis scelerisque ultricies, felis dolor placerat sem, id porta velit odio eu elit. Aenean interdum nibh sed wisi. Praesent sollicitudin vulputate dui. Praesent iaculis viverra augue. Quisque in libero. Aenean gravida lorem vitae sem ullamcorper cursus. Nunc adipiscing rutrum ante. Nunc ipsum massa, faucibus sit amet, viverra vel, elementum semper, orci. Cras eros sem, vulputate et, tincidunt id, ultrices eget, magna. Nulla varius ornare odio. Donec accumsan mauris sit amet augue. Sed ligula lacus, laoreet non, aliquam sit amet, iaculis tempor, lorem. Suspendisse eros. Nam porta, leo sed congue tempor, felis est ultrices eros, id mattis velit felis non metus. Curabitur vitae elit non mauris varius pretium. Aenean lacus sem, tincidunt ut, consequat quis, porta vitae, turpis. Nullam laoreet fermentum urna. Proin iaculis lectus.

Sed mattis, erat sit amet gravida malesuada, elit augue egestas diam, tempus scelerisque nunc nisl vitae libero. Sed consequat feugiat massa. Nunc porta, eros in eleifend varius, erat leo rutrum dui, non convallis lectus orci ut nibh. Sed lorem massa, nonummy quis, egestas id, condimentum at, nisl. Maecenas at nibh. Aliquam et augue at nunc pellentesque ullamcorper. Duis nisl nibh, laoreet suscipit, convallis ut, rutrum id, enim. Phasellus odio. Nulla nulla elit, molestie non, scelerisque at, vestibulum eu, nulla. Ut odio nisl, facilisis id, mollis et, scelerisque nec, enim. Aenean sem leo, pellentesque sit amet, scelerisque sit amet, vehicula pellentesque, sapien.

9 HARDWARE REQUIREMENTS AND REQUIRED PURCHASES

RESOURCES: identification, enumeration, prioritization, justification, if applicable prizes and alternatives of:

- hardware
- software and licenses
- special literature
- study participants, cooperation partners, stakeholders, . . .

Donec vel nibh ut felis consectetuer laoreet. Donec pede. Sed id quam id wisi laoreet suscipit. Nulla lectus dolor, aliquam ac, fringilla eget, mollis ut, orci. In pellentesque justo in ligula. Maecenas turpis. Donec eleifend leo at felis tincidunt consequat. Aenean turpis metus, malesuada sed, condimentum sit amet, auctor a, wisi. Pellentesque sapien elit, bibendum ac, posuere et, congue eu, felis. Vestibulum mattis libero quis metus scelerisque ultrices. Sed purus.

Donec molestie, magna ut luctus ultrices, tellus arcu nonummy velit, sit amet pulvinar elit justo et mauris. In pede. Maecenas euismod elit eu erat. Aliquam augue wisi, facilisis congue, suscipit in, adipiscing et, ante. In justo. Cras lobortis neque ac ipsum. Nunc fermentum massa at ante. Donec orci tortor, egestas sit amet, ultrices eget, venenatis eget, mi. Maecenas vehicula leo semper est. Mauris vel metus. Aliquam erat volutpat. In rhoncus sapien ac tellus. Pellentesque ligula.

Cras dapibus, augue quis scelerisque ultricies, felis dolor placerat sem, id porta velit odio eu elit. Aenean interdum nibh sed wisi. Praesent sollicitudin vulputate dui. Praesent iaculis viverra augue. Quisque in libero. Aenean gravida lorem vitae sem ullamcorper cursus. Nunc adipiscing rutrum ante. Nunc ipsum massa, faucibus sit amet, viverra vel, elementum semper, orci. Cras eros sem, vulputate et, tincidunt id, ultrices eget, magna. Nulla varius ornare odio. Donec accumsan mauris sit amet augue. Sed ligula lacus, laoreet non, aliquam sit amet, iaculis tempor, lorem. Suspendisse eros. Nam porta, leo sed congue tempor, felis est ultrices eros, id mattis velit felis non metus. Curabitur vitae elit non mauris varius pretium. Aenean lacus sem, tincidunt ut, consequat quis, porta vitae, turpis. Nullam laoreet fermentum urna. Proin iaculis lectus.

10 PROJECT SCHEDULE

PROJECT PLAN: effort, mapping of work packages to milestones, deadlines, assignment of activities (in hours per task per team member)

Sed mattis, erat sit amet gravida malesuada, elit augue egestas diam, tempus scelerisque nunc nisl vitae libero. Sed consequat feugiat massa. Nunc porta, eros in eleifend varius, erat leo rutrum dui, non convallis lectus orci ut nibh. Sed lorem massa, nonummy quis, egestas id, condimentum at, nisl. Maecenas at nibh. Aliquam et augue at nunc pellentesque ullamcorper. Duis nisl nibh, laoreet suscipit, convallis ut, rutrum id, enim. Phasellus odio. Nulla nulla elit, molestie non, scelerisque at, vestibulum eu, nulla. Ut odio nisl, facilisis id, mollis et, scelerisque nec, enim. Aenean sem leo, pellentesque sit amet, scelerisque sit amet, vehicula pellentesque, sapien.

11 CONCLUSION

complete the discussion on the project, hand over to the implementation step, identify possible dangers and problems that can diminish or demolish the project and alternate courses of action if necessary

revise the proposal to become a whole and integrated document, remember adding the section, revise introduction (Section 1) if necessary

Sed consequat tellus et tortor. Ut tempor laoreet quam. Nullam id wisi a libero tristique semper. Nullam nisl massa, rutrum ut, egestas semper, mollis id, leo. Nulla ac massa eu risus blandit mattis. Mauris ut nunc. In hac habitasse platea dictumst. Aliquam eget tortor. Quisque dapibus pede in erat. Nunc enim. In dui nulla, commodo at, consectetuer nec, malesuada nec, elit. Aliquam ornare tellus eu urna. Sed nec metus. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas.

BIBLIOGRAPHY

[1] 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.

[2] 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/.

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

[4] 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.

[5] 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.

[6] 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.

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