SECURITY RESEARCH ON CONNECTED CARS

Sebastian Renner, Prof. Dr. Rudolf Hackenberg
sebastian.renner@st.oth-regensburg.de,
rudolf.hackenberg@oth-regensburg.de

OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

LaS³ Laboratory for Safe and Secure Systems — a discipline of software engineering

MAPRby

Introduction

The networking and digitalisation of commonplace devices is currently increasing. These topics invade all regions of daily life. Automation and digitalisation pervade branches like production technology and also the automotive industry. This growing technification offers lots of new opportunities, on the other hand big challenges regarding the information security are presented to the industry.
The topic is especially relevant in the area of networked vehicles, because in this discipline an attack on the information infrastructure can not only lead to economic damage, also the safety of the passengers can be endangered. The research project, managed by Prof. Dr. Hackenberg wants to investigate the influence of information security to the safe state of the vehicle, additionally other mutual interactions of the two aspects – safety and security – are analysed.

Impacts of security on safety

Today the topic information security is present in nearly all of our connected devices. And even if security breaches in for example mobile phone operating systems or business networks are critical, the safe state of the system in a vehicle has an even higher relevance. This is because an attack on the car can possibly result in immediate danger for the passengers' safety. That's why it's a special issue to investigate the mutual influences of security and safety in the modern and future car. Especially the continuously increasing driving intelligence of the car, as well as the field of autonomous driving are ongoing topics, that emphasize the correlation between safety and security in that context [1].

Some areas, where safety and security interact in connected cars are:

- Steering systems
- Car access functions
- Connected services
- Airbag controls
- Navigation/GPS
- Assistence systems

Example: On-Board Diagnostics (OBD)

On-board diagnostic systems as we know them today, were introduced first in the USA in 1996. From that point on every vehicle that was authorized for US traffic had to be equipped with a standardized OBD-II connector. That rule was also brought to Europe in the following years, so almost every vehicle which is on the streets nowadays has an OBD-II plug installed somewhere inside the vehicle – preferably in the area of the driver's seat. The connector is meant to be used by repair shops. With special equipment it is for example possible to mine more data like error codes by connecting to OBD-II, which should help the mechanic to find reasons why some parts of the vehicle don't work properly.
However, one can not only read data while being connected to the car via OBD-II, also writing data to critical sections – which can also concern safety functions – is specified in the standardized diagnosis protocol. Therefor the OBD-II interface constitutes an attack vector that should be put under investigation. For that one should first focus on studying the corresponding standards, that were developed for the OBD communication. Furthermore looking at the pinout of the OBD-II connector reveals that data is send via the Control Area Network (CAN) bus, which is very common in the vehicle's network architecture. From that point one could inform himself about the structure of these CAN messages or try to sniff in-vehicle communication to see how the communication works exactly. An example of the request/response data structure of the diagnosis protocol can be seen in figure 1. After getting to know the protocol itself, the vulnerability analysis of the implementation should be started. One approach in this case is to try sending data via OBD-II and see how the car reacts to it. Also sending malformed messages is a good technique to determine the robustness of the protocol (fuzzing).

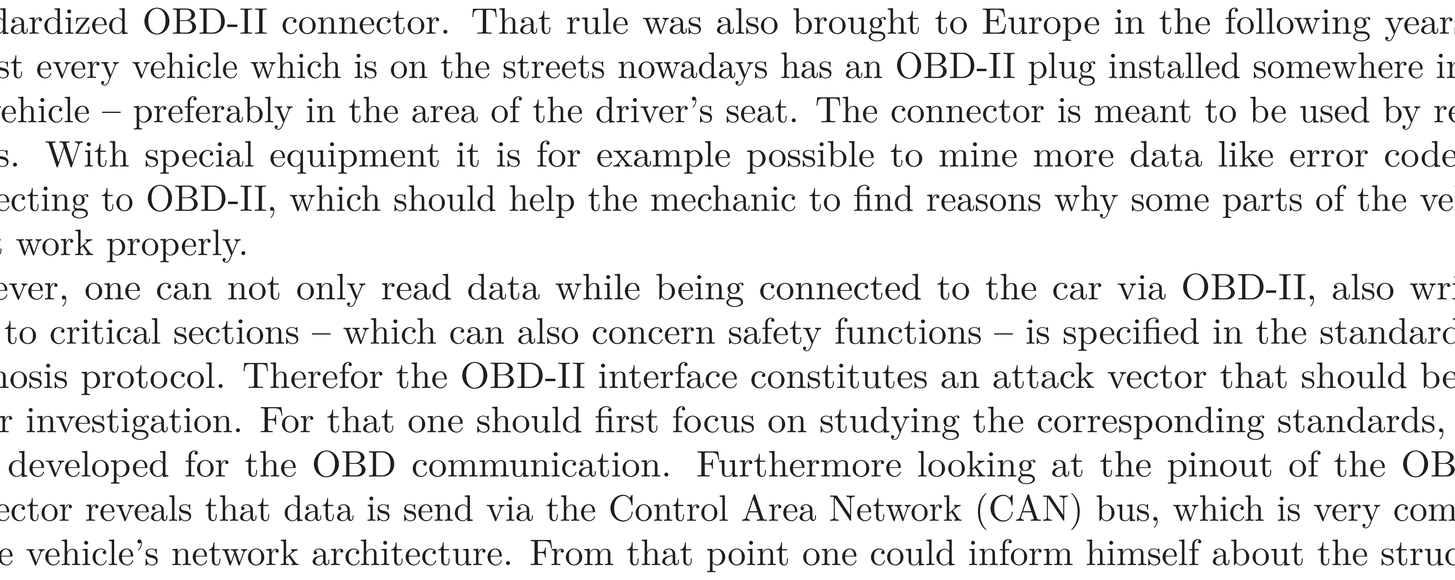

Figure 1: Request/Response frame structure [2]

Methodology

The investigation of a specific aspect in the field of automotive security usually starts with the process of deeply understanding the topic itself. In this first step it's important to develop knowledge on how the system under test works before the actual security analysis gets started. Therefor it is needed to investigate possibly used protocols or software, as well as hardware, depending on the analysed object. The manual analysis is mostly supported by certain tools, that help an engineer by for example presenting data in a more readable format. Sometimes it's also possible to use existing software to solve a part of the analysis puzzle and extend or fit it to new and more specific needs. After this part it is also an important step to search for and choose helpful software to get assistance in the further research process. One should also develop a toolset of programs that can be reused for multiple occasions to avoid doing the work of setting up the same toolchain over and over. Some widely used tools in the field of security research are shown in figure 2.

Figure 2: Selection of commonly used software

After digging into the topic and selecting a valid toolchain, the actual testcase for penetrating the security architecture of the system under test is being developed. A part of this also includes the suspicion of vulnerabilities, generating and executing tests to validate the assumptions. During the whole test process it is a principle to keep track of the actions performed by documenting every step. This is necessary to reproduce the process later and to build a solid base of information about the findings. In the last fraction of the analysing process one wants to feed the new information to the software development cycle of the tested software.

Goals

By investigating the implications of security issues on safety some proposed goals are:

- Testing the security of the software architecture in the vehicle
- Gain more information about the correlation between safety and security
- Integrate the obtained knowledge in the software development lifecycle

References

[1] D. J. Fagnant and K. Kockelman, "Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations," *Transportation Research Part A: Policy and Practice*, vol. 77, no. C, pp. 167–181, 2015.

[2] Werner Zimmermann, Ralf Schmidgall, *Bussysteme in der Fahrzeugtechnik*, 5th ed. Wiesbaden: Springer Fachmedien, 2014.