CarSec: Security research on connected cars

Autor: Nils Weiss, **Tutor:** Prof. Dr. rer. nat. Rudolf Hackenberg
nils.weiss@st.oth-regensburg.de, rudolf.hackenberg@oth-regensburg.de

Introduction

Automotive and internet technology coalesce. Consumers claim continuously for new connected features and services. Car manufactures discovered the benefit of big data and started collecting data related to their cars and customers. Also the european government is working on a draft law to prescribe a mobile radio module for every new car. All of these new connected features and business cases require some kind of remote interface, usually to the internet. To determine the overall risk for a remote attack on a modern car, the internal vulnerabilities and design faults have to be explored first.

Overview

The communication technology and network architecture in current cars are mainly historical grown. The CAN standard for example was designed over 30 years ago. Decades before the internet and mobile communication had their breakthrough. Various external interfaces are added to modern cars. Every interface can be a target for attacks.

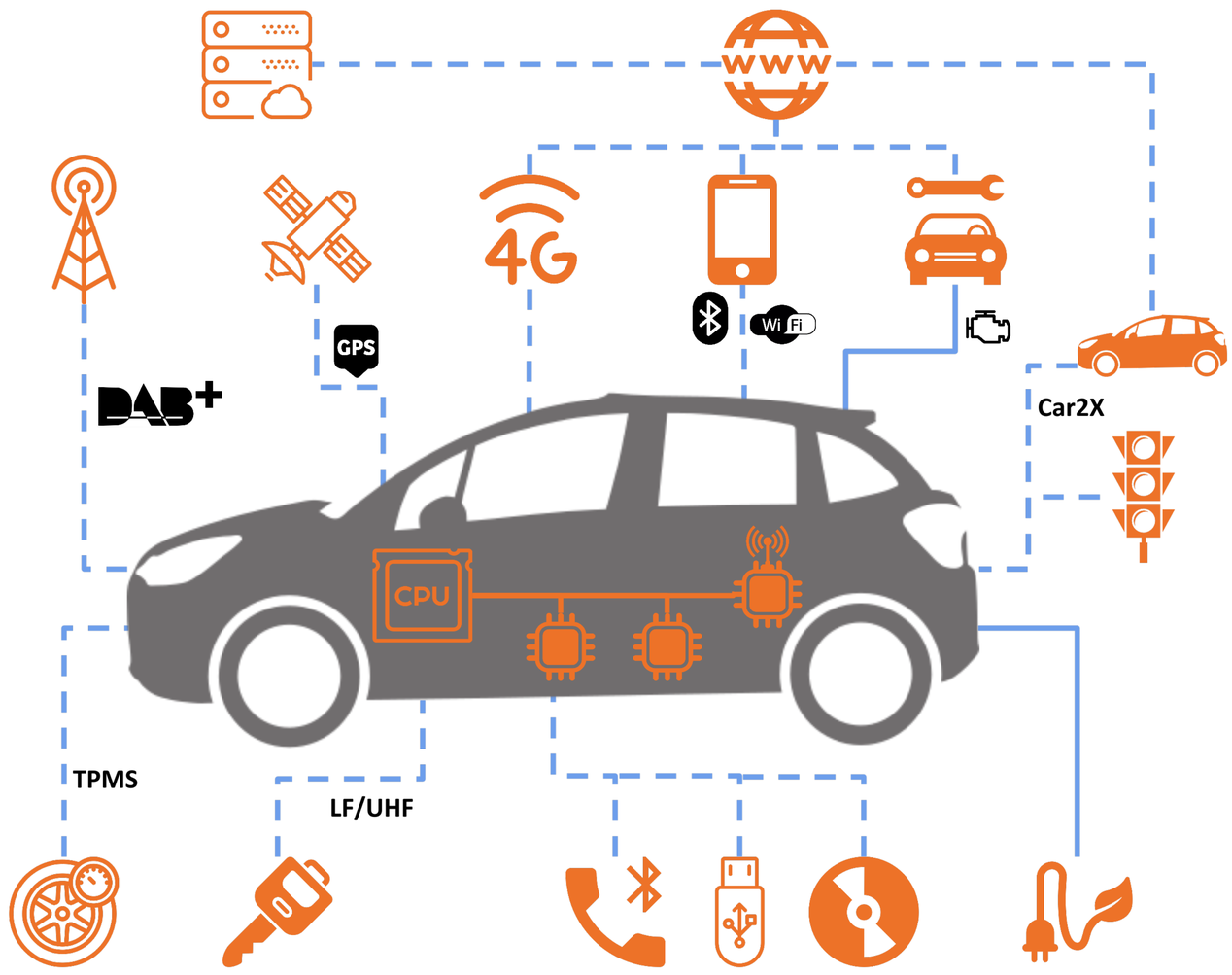

Figure 1: Overview of external interfaces on modern cars

Dive into automotive networks

Automotive communication networks inside a car are a major security risk. CAN and FlexRay are the leading communication technologies inside modern cars. Unfortunately these communication standards are not designed for secured or encrypted communication. If an attacker get access to an ECU he is able to attack other ECUs as well, and he can compromise the complete car. A first step in this research project is to develop a penetration test framework for automotive ECUs. Vulnerabilities in bootloaders or protocols can be found efficiently by automated tests.

CANtact-Framework

Eric Evenchick introduced the CANtact framework at the BlackHat Conference Asia in 2015 [2]. CANtact is an open source tool based on linux. To achieve higher datarates and reliability, the open source hardware was redesigned and the firmware improved. CANtact gives access the CAN bus from python or bash scripts and enables wireshark to sniff packets. These software tools allow an efficient penetration test. Also multiple CANtact interfaces can be used to investigate the packet flow over gateways.

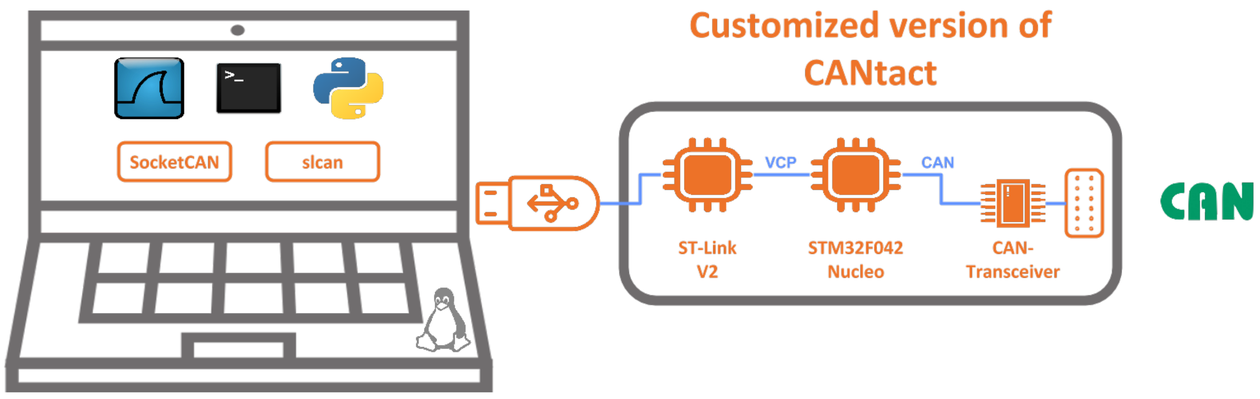

Figure 2: Functional diagram of the CANtact penetration testing framework

Network architecture

The internal network topology is an important factor for the overall security of a car. Two different network topologies are primary used in modern cars.

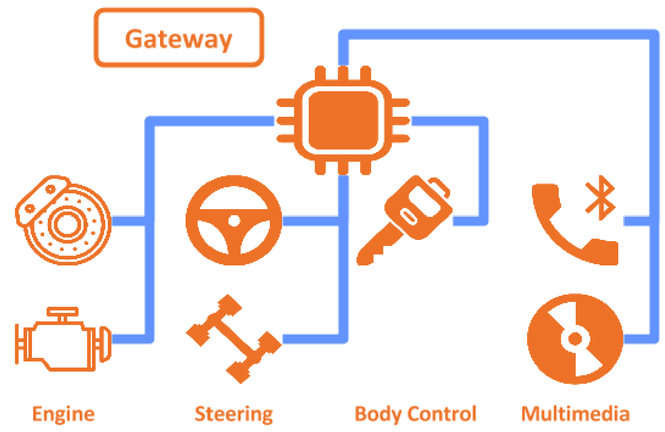

Figure 3: Network topology with central gateway

The central gateway architecture can be found in high-priced cars. ECUs are connected to a domain specific line bus. All domains are connected to a central gateway, which controls the inter domain access. Usually remote interfaces are located in a multimedia domain. If an attacker hijacks an ECU in this domain, he can not immediately send commands to other domains.

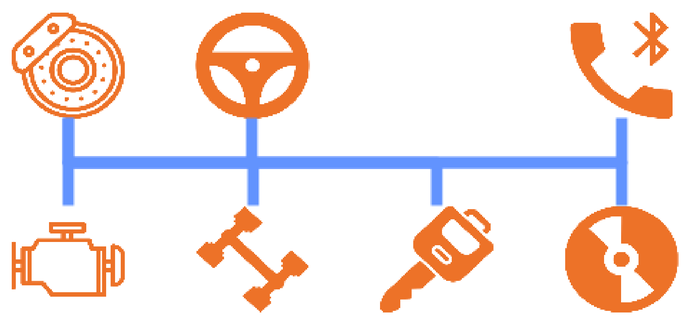

Figure 4: Network topology with single line bus

A simpler network topology with one common bus is mainly used in lower-priced cars. If an attacker gets access to any ECU on this bus, he is immediately able to send commands to other ECUs for example to the break control ECU.

Results

The security of a modern car is mainly dependant on three factors:

- Remote interfaces
- Internal network architecture
- Cyber physical systems

The combination of these three factors gives a value for the vulnerability of modern cars [1]. In the next step of this project, the security of bootloader protocols and the firmware signing mechanisms will be investigated.

References

[1] Dr. Charlie Miller and Chris Valasek. A survey of remote automotive attack surfaces. DEF CON 22 Hacking Conference. Las Vegas, NV: DEF CON, August 2014.

[2] Eric Evenchick. An introduction to the canard toolkit. Black Hat Conference Asia, 2015.

Acknowledgements

Icons: "designed by Freepik"