CarSec: Security research on connected cars

B. Sc. Nils Weiss
OTH Regensburg (Germany)
nils.weiss@st.oth-regensburg.de

Prof. Dr. rer. nat. Rudolf Hackenberg
OTH Regensburg (Germany)
rudolf.hackenberg@oth-regensburg.de

Abstract

Automotive technology and Internet technology coalesce. Consumers claim continuously for new connected features and services. Car manufactures discovered the benefit of big data and started collecting tons of 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 with the Internet.

The communication technology and network architecture in current cars are mainly historical increased. The CAN standard for example was designed over 30 years ago. Decades before the Internet and mobile communication had their break through. In this time, security was no design criteria for an automotive communication protocol. Therefore most communication protocols in current cars are insecure by design. To fulfill the new needs of customers and law regulations, car manufactures added remote interfaces to their old fashion car communication network. Two American security researchers could already prove that unaltered passenger vehicles with such interfaces were exploited remotely over the Internet.

Modern cars can be hacked by offline attacks as well. Electronic control units are attackable from infected repair shop testers. In this way, attackers can modify invulnerable cars with back doors or malware, when customers doing their regular service check.

In the CarSec research project a small team at the OTH-Regensburg, started to discover attack surfaces of connected cars. In the following years, the team wants to identify state of the art vulnerabilities of connected cars and develop holistic solutions for the cars of tomorrow.

To achieve this goal a lot of interdisciplinary research has to be done. The range of technologies in a connected cars goes from embedded software and low level hardware interfaces up to backbone servers and smart phone applications. Security holes can exist in every link of this chain.

Keywords
Security, Car, Connected Cars, Internet, IoT