CS 12 computer science 12

Fachprojekt

Simulating Security Attacks on Embedded Systems

Lea Schönberger, M. Sc.
Junjie Shi, M. Sc.
Prof. Dr. Jian-Jia Chen

April 28, 2020

In the automotive sector, Controller Area Network (CAN) is the status quo for in-vehicle networks connecting multiple electronic control units (ECUs), which allows each participant to send and receive data such as the vehicle speed, motor temperature, and brake pressure. Since a non-negligible number of the transmitted messages contain safety-critical information, it is of utmost importance to ensure the reliability of the system under any circumstances.

However, due to the increasing usage of vehicle-to-vehicle and vehicle-to-everything communication, security attacks on vehicles and their communication infrastructure become more and more frequent and can have a serious impact not only on the functioning of the vehicle, but also on the driver's health. Against this background, this project aims to investigate the impact different security attacks on the in-vehicle network have on the vehicle behavior.

In this project, the students are expected to set up a simple CAN network using the OMNeT++ network simulator[1] and to connect it to a simple Gazebo[2] model. In this setup, the students are expected to simulate different security attacks and to exemplary evaluate their impact. Please note that it is not necessary to use a vehicle model, but that also simpler models, e.g., an inverted pendulum, can be used.

Required Skills:

- basic knowledge of C++

Acquired Skills after the Project:

- knowledge about controller area network
- familiarity with OMNeT++ and Gazebo
- knowledge about security threats to embedded and automotive systems

[1] https://omnetpp.org/
[2] http://gazebosim.org/