Building a Prototyping Platform for Investigating the Impact of Attacks against Automotive Networks

Alexander Stühring*, Günter Ehmen*, Sibylle Fröschle†

*University of Oldenburg, Germany
{stuehring|ehmen}@informatik.uni-oldenburg.de

†OFFIS, Germany
sibylle.froeschle@offis.de

I. Introduction

Depending on their configuration, modern vehicles have up to 70 Electronic Control Units (ECUs), which are communicating over local networks like CAN or FlexRay with each other. Each ECU is designed for one or more applications such as brake assistance or navigation. In view of future automotive applications like Car2X the number of interfaces to other systems as well as the communication between ECUs will increase. Already today a strict separation between the different communication domains of modern vehicles is no longer possible. In view of the growing safety impact of future applications it is getting more and more important to investigate the impact of attacks on critical components and applications.

The goal of the prototyping platform is to investigate and demonstrate different security aspects and scenarios as introduced in [1] within a simulated environment while using standardized hardware and software components.

II. Prototyping Platform

The prototyping platform itself allows the analysis of distributed systems in the automotive domain and was already introduced in [2]. A driver assistance system, mapped on several ECUs which communicate over CAN, was analyzed within an Hardware-in-the-Loop (HIL) simulation using the driving simulation software SILAB (see figure 1). The new setup integrates hardware and software components to enable security investigations. This upgrade is divided into two parts. First, the software of the existing ECUs is updated to be able to investigate aspects of in-vehicle network security based on [3]. Second, hardware and software components were added to support wireless communication standards like IEEE 802.11p for supporting Car2X applications.

A. In-Vehicle Networks

To simulate a compromised ECU we extended the protocol stack of our OSEK operating system to provide the possibility for security investigations without necessarily manipulating the task itself. With this modification we have full control about every incoming and outgoing message. Moreover we are able to send and receive messages on the bus. One advantage of the prototyping platform is, that each ECU is equipped with a Field Programmable Gate Array (FPGA). With this we are able to use modified controller designs to investigate the impact of manipulations on the physical layer, which plays an important role when analyzing the impact of attacks as well as the development of protection techniques. Moreover the prototyping platform is able to measure the execution time of code fragments and tasks. So we are able to to analyze the timing of different tasks while doing manipulations on the bus system like flooding the bus with messages.

This work was supported by the funding initiative *Niedersächsisches Vorab* of the Volkswagen Foundation and the Ministry of Science and Culture of Lower Saxony as part of the *Interdisciplinary Research Center on Critical Systems Engineering for Socio-Technical Systems*.

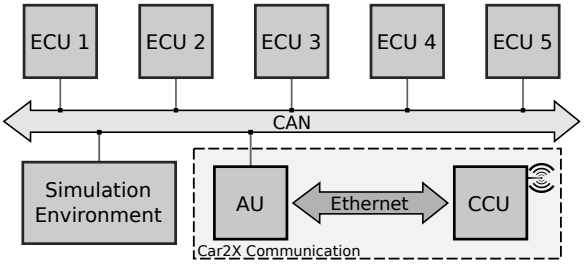

Fig. 1. Setup of the Prototyping Platform

B. Car2X Communication

The aim of the second extension (see figure 1) is to support Car2X applications within the prototyping platform. The extension consists of a Communication and Control Unit (CCU) and an Application Unit (AU).

The CCU connects the car with other wireless networks. To fulfil the requirements of future automotive applications our CCU is able to communicate based on IEEE 802.11p, WiFi, UMTS, LTE and Bluetooth. Moreover the platform itself is highly configurable and upgradable. This will allow us to run our own software as well as open communication standards like ETSI[1]. The AU implements the Car2X applications and creates the connection between the wireless interfaces of the CCU and the in-vehicle networks like CAN or FlexRay.

III. Further Platform Extensions

Hardware Security Modules (HSMs) can be integrated into the prototyping platform as a design on the FPGA or as a commercial off-the-shelf component. This will allow us to investigate techniques like secure boot, secure update, or encrypted communication. Furthermore by equipping the prototyping platform with multiple Car2X components we will be able to simulate Car2X scenarios with more than one car in a controlled environment.

References

[1] S. Fröschle and A. Stühring, "Idea: Security Engineering Principles for Day Two Car2X Applications," in *International Symposium on Engineering Secure Software and Systems (ESSOS)*, 2014.

[2] M. Büker, W. Damm, G. Ehmen, S. Henkler, D. Janssen, I. Stierand, and E. Thaden, "From Specification Models to Distributed Embedded Applications: A Holistic User-Guided Approach," *SAE International Journal of Passenger Cars- Electronic and Electrical Systems*, vol. 6, pp. 194–212, May 2013.

[3] A. Stühring, "Untersuchung der Angriffssicherheit von CAN-Netzwerken im Automobilbereich," Master's thesis, Carl von Ossietzky Universität Oldenburg, Nov. 2012.

[1] European Telecommunications Standards Institute (http://www.etsi.org/)