Security Test Platform for Autonomous Driving

Daniel Zelle, Roland Rieke, Christoph Krauß
firstname.lastname@sit.fraunhofer.de
Fraunhofer Institute for Secure Information Technology
Darmstadt, Germany

CCS CONCEPTS

• **Security and privacy → Embedded systems security**; *Intrusion detection systems*; *Security protocols*; Key management; Trusted computing; • **Hardware →** *Sensors and actuators*; Buses and high-speed links.

KEYWORDS

automotive security, evaluation platform, autonomous driving, testing

ACM Reference Format:
Daniel Zelle, Roland Rieke, Christoph Krauß. 2019. Security Test Platform for Autonomous Driving. In *Proceedings of 3. ACM COMPUTER SCIENCE IN CARS SYMPOSIUM (CSCS 2019).* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Research in the field of automotive security faces several challenges. Vehicles are expensive, closed source, require special test equipment, and changes (either by developing new techniques or by attacking the vehicle) may result in physical damage. Moreover, vehicles are a source of physical hazards, e.g., high voltage, or airbag explosives. Thus, security researchers mostly use theoretical models and estimations. Even if researchers use real vehicles, it is often not possible to execute real attacks or implement security solutions since the vehicles may not (yet) support required

Thus, a test and evaluation environment is required, which resembles real or near-future autonomous vehicles. Such a platform can be used for evaluating new developed security mechanisms, e.g., hardware security solutions, security protocols, or mechanisms such as intrusion detection and prevention systems (IDPS).

In this extended abstract, we introduce the design of our security test platform for autonomous driving, which is integrated in a model car with the scale of 1:5. It includes and implements typical components and protocols, which are used in modern and upcoming autonomous vehicles. This includes, for example, electronic control units (ECUs) for charging electric vehicles using ISO 15118, advanced driver assistance systems (ADAS), or Vehicle2X (V2X) connectivity but also modern communication technologies such as automotive ethernet. Newly developed security mechanisms can be easily integrated and evaluated in a realistic environment without any safety risks for the researcher. In addition, the security of automotive protocols or architecture designs can be evaluated.

CSCS 2019, October 8, 2019, Kaiserslautern, Germany

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

The abstract is organized as follows: First, we give a brief overview on related work. Then, we describe the requirements for the test platform and the architecture itself. This includes some envisioned protocols to be analyzed and a concept for evaluating IDPS.

2 RELATED WORK

In the field of autonomous driving, researches often extended vehicles with sensors and actors for autonomous driving, e.g., in [10] or [14]. These projects extend the cars with lidar sensors and cameras as well as control units for steering wheel, gas and brake paddle. We consider the use of a real car as too dangerous in particular when attacking the system to evaluate for example IDPS solutions. Some researchers have already developed model cars to evaluate their autonomous driving algorithms, for example, in competitions like the Carolo-Cup. [6] shows one of these cars that has one main computational component that is directly connected to all sensors like ultrasonic sensors and cameras. [12] gives an overview of technology used in the Carolo-Cup. The teams often uses automotive data- and time-triggered framework or robot operating system as development frameworks. These are mostly used for prototyping but none of them is used in real vehicles.

A first evaluation platform for cyber security purposes has been proposed in [5]. However, it is limited to a remote controlled car with one central component and it does not address complex in-vehicle networks or even autonomous vehicles. [15] introduced an architecture for autonomous driving cars combining classic automotive bus systems like controller area network (CAN) and FlexRay as well as modern ethernet communication.

3 REQUIREMENTS

The test platform enables easy and realistic tests and evaluations of automotive security concepts in a safe laboratory environment. To achieve this, our model car must integrate realistic components, communication technologies, and protocols used in modern and autonomous vehicles and the implementation of basic autonomous driving functions and external connectivity services. Different E/E architectures for autonomous driving must be supported. These architectures include both automotive hardware (ECUs, sensors, actors, gateways, bus networks like CAN, LIN(local interconnect network), and automotive ethernet) and software (middleware like AUTOSAR or protocols like DoIP). Modularity is a requirement for the architecture for enabling the analysis of security concepts in different architectures. For example, the effectiveness of an IDPS may depend on the E/E architecture and the placement of the IDPS. In addition, the platform must be easily configurable and extendable, e.g., using open source software projects. A further requirement is the ability to evaluate the impact of attacks and how mitigation strategies could operate.

4 ARCHITECTURE

Our evaluation platform is integrated in a model car and provides a basic set of components, communication technologies, and protocols, which can be implemented in different E/E architectures. For example, gateways group several ECUs into domains.

4.1 Components

All components of autonomous vehicles are shown in Fig. 1. Their core component are sensor and actor components enabling the surveillance and reaction to the environment.

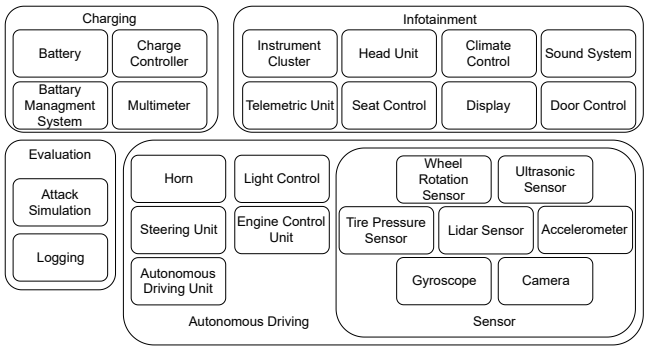

Figure 1: Component architecture

Actors control the steering (steering unit), the speed (engine control unit) and the lights (light unit). The autonomous driving domains is completed with a set of sensors. We decided to use ultrasonic and lidar distance sensors completed with cameras to observe the surrounding. The vehicle can get information about its own conditions with a gyroscope, an accelerometer and a sensor measuring the wheel rotations.

Furthermore, the vehicle is powered by a battery that is controlled with a battery management system and a charge controller is responsible for the communication during charging process. A multimeter allows the battery management system and the charge controller to get the state of the battery.

The infotainment domain is the last of the regular domains of the vehicle. First, it has the instrument cluster and the head unit with a display allowing the driver to get information about the vehicle and control vehicle functions like the climate control or the radio. A sound system allows to play music and the telemetric unit allows communication of the car with a backend, other cars or mobile terminals (e.g. smart phones). Additionally, this domain includes the control over door locks.

The evaluation domain contains components connected to every network in the vehicle. A logger allows to store all communication and sensor values to reproduce test results or gather information for the training of an IDPS. The domain also contains an attack simulation. The attacker has connections to every network in the evaluation platform. The basic features of the attacker are: Denial of service, message manipulation, message removal, message delay, and message misdirect. Various other kinds of targeted attacks can be defined and simulated with the aim to analyze how these attacks and variations thereof could be detected and their impact mitigated.

4.2 Communication Technologies

As main in-vehicle communication technology, our platform supports automotive ethernet since it is expected to be the predominant technology in autonomous vehicles. In addition, it integrates CAN and CAN FD to be able to integrate legacy devices. For external communication, we integrate Wifi, Bluetooth, and cellular communication. In addition, we integrate power line communication to support charging communication via ISO 15118 to a charge point.

4.3 Communication Protocols

Vehicles make use of multiple communication protocols. For our implementation we focus on publicly available protocols, e.g., AUTOSAR. AUTOSAR published the protocol diagnostics over iternet protocol [1] for error diagnose of vehicles, as well as SOME/IP [3] and SOME/IP-SD [2], which allows to offer and consume services for in vehicle communication. The audio video bridging protocol [4] allows the transfer of audio and video date with real time constrains, which is also used in vehicle networks. The connected car features are implemented using the remote vehicle interaction protocol [9] published by Jaguar Land Rover. Vehcile to vehicle communication uses the vehicular ad hoc network via IEEE 802.11p. Charging of the battery uses ISO 15118 for authentication and payment.

5 CONCLUSION AND FUTURE WORK

Regarding the challenges presented in the introduction, we aimed at a platform, which (1) enables easy and realistic tests and evaluations of automotive security concepts in a lab and (2) helps to improve mitigation techniques against cyber-attacks on autonomous vehicles.

Our first objective is addressed by the development of the platform, which enables the test and evaluation of security concepts for autonomous vehicles as well as possible impacts of successful attacks on cyber-physical systems of the vehicle or the environment. The evaluation platform is not limited to specific E/E architectures of a specific car manufacturer and can be easily modified or extended. It consists of hardware (e.g., ECUs, sensors, and actors) - and software components (e.g., implementations of operating systems, automotive middlewares, and automotive protocols). The architectural design and software components will be made publicly available to enable the automotive industry and other researchers to use the platform.

The second important objective is the improvement of mitigation strategies against cyber-attacks on vehicles. So far, the best strategy to deal with a running attack in a vehicle is not clear. The evaluation platform enables the analysis of the physical impacts of different mitigation strategies. These impacts, for example, are extended stopping distances or changed steering behavior. The analysis results in mitigation strategies for different scenarios of autonomous driving and different kinds of attacks.

ACKNOWLEDGMENTS

This research work has been funded by the German Federal Ministery of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity.

REFERENCES

[1] AUTOSAR. 2018. *Specification of Diagnostic over IP - Classic Platform 4.4.0.* https://www.autosar.org/fileadmin/user_upload/standards/classic/4-3/AUTOSAR_SWS_DiagnosticOverIP.pdf

[2] AUTOSAR. 2018. *Specification of Service Discovery - Classic Platform 4.4.0.* https://www.autosar.org/fileadmin/Releases_TEMP/Classic_Platform_4.4.0/Communication.zip

[3] AUTOSAR. 2018. *Specification on SOME/IP Transport Protocol - Classic Platform 4.4.0.* https://www.autosar.org/fileadmin/Releases_TEMP/Classic_Platform_4.4.0/Communication.zip

[4] AVnu Automotive Technical Working Group. 2016. *Automotive Ethernet AVB Functional and Interoperability Specification Revision 1.5.* https://avnu.org/wp-content/uploads/2014/05/Automotive-Ethernet-AVB-Func-Interop-Spec-v1.5-Public.pdf

[5] Jakob Axelsson, Avenir Kobetski, Ze Ni, Shuzhou Zhang, and Eilert Johansson. 2014. Moped: A mobile open platform for experimental design of cyber-physical systems. In *2014 40th EUROMICRO Conference on Software Engineering and Advanced Applications*. IEEE, 423–430.

[6] F. Bormann, E. Braune, and M. Spitzner. 2010. The C2000 autonomous model car. In *4th European Education and Research Conference (EDERC 2010)*. 200–204.

[7] Wonsuk Choi, Kyungho Joo, Hyo Jin Jo, Moon Chan Park, and Dong Hoon Lee. 2018. VoltageIDS: Low-Level Communication Characteristics for Automotive Intrusion Detection System. *IEEE Transactions on Information Forensics and Security* (3 3 2018). https://doi.org/10.1109/TIFS.2018.2812149

[8] Daimler, Aptiv, Audi, Baidu, BMW, Continental, Fiat Chrysler Automobiles, HERE, Infineon, Intel, and Volkswagen. 2019. *Safety First for Automated Driving.* https://www.daimler.com/dokumente/innovation/sonstiges/safety-first-for-automated-driving.pdf

[9] Jaguar Land Rover. 2014. *REMOTE VEHICLE INTERACTION (RVI).* https://github.com/GENIVI/rvi_core

[10] J. Levinson, J. Askeland, J. Becker, J. Dolson, D. Held, S. Kammel, J. Z. Kolter, D. Langer, O. Pink, V. Pratt, M. Sokolsky, G. Stanek, D. Stavens, A. Teichman, M. Werling, and S. Thrun. 2011. Towards fully autonomous driving: Systems and algorithms. In *2011 IEEE Intelligent Vehicles Symposium (IV)*. 163–168. https://doi.org/10.1109/IVS.2011.5940562

[11] Michael Müter, André Groll, and Felix C. Freiling. 2010. A structured approach to anomaly detection for in-vehicle networks. *2010 Sixth International Conference on Information Assurance and Security* (2010), 92–98.

[12] Marcus Nolte, Thomas Form, Susanne Ernst, Robert Graubohm, and Markus Maurer. 2018. The Carolo-Cup Student Competition: Involving Students with Automated Driving. In *12th European Workshop on Microelectronics Education, EWME 2018, Braunschweig, Germany, September 24-26, 2018*. 95–99. https://doi.org/10.1109/EWME.2018.8629462

[13] Loreto Pescosolido, Marco Conti, and Andrea Passarella. 2018. Performance Analysis of a Device-to-Device Offloading Scheme in a Vehicular Network Environment. *CoRR* abs/1801.09082 (2018). arXiv:1801.09082 http://arxiv.org/abs/1801.09082

[14] Junqing Wei, Jarrod M. Snider, Junsung Kim, John M. Dolan, Raj Rajkumar, and Bakhtiar Litkouhi. 2013. Towards a Viable Autonomous Driving Research Platform. *Proceedings of the 2013 IEEE Intelligent Vehicles Symposium, pp. 763-770* (June 2013), 763–770.

[15] B. Zheng, H. Liang, Q. Zhu, H. Yu, and C. Lin. 2016. Next Generation Automotive Architecture Modeling and Exploration for Autonomous Driving. In *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. 53–58. https://doi.org/10.1109/ISVLSI.2016.126