Herausgeber et al. (Hrsg.): SENSYBLE - Smart Systems for Better Living Environment,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 1

Assessment of Current Intrusion Detection System Concepts for Intra-Vehicle Communication

Oleg Schell[1], Jan Peter Reinhard[2], Marcel Kneib[3], Martin Ring[4]

Abstract: In our current time, vehicles are no longer the self-contained systems they were in their early days. With the advancing digitalization, vehicles began to incorporate numerous electronic components, which enabled the implementation of advanced safety and comfort functionalities [Fl16]. However, the increasing number of electronics also provides a greater surface to intrude into the system and cause severe harm for the driver, its environment or the manufacturer. The potential extent of such attacks has been demonstrated in recent years by different research groups [MV13, MV15, Te18, Te19], which were able to take over crucial vehicular functions like steering or accelerating over wireless interfaces. Therefore, such intrusion attempts on the communication network of a vehicle have to be detected and respective measures taken to prevent threats. In this regard, Intrusion Detection Systems (IDSs) have long been successfully put into utilization to recognize and log malicious behavior in the classical IT domain. Unfortunately, most of these existing detection mechanisms cannot easily be transferred into the automotive sector as different communication architectures and protocols are implemented there. The stringent requirements on the availability and reliability of vehicular functions make the transfer even more difficult. Since with the upcoming UNECE regulations regarding the implementation of cybersecurity mechanisms in the automotive sector [UN20], it is of high importance for both manufacturers and engineers to understand the challenges and possibilities of such a system.

Due to the fact that network monitoring will be required in the future and the transfer of existing systems is a difficult task, the goal of this elaboration is to give an overview of aspects to be considered during the selection and engineering process of such an IDS. For this purpose, the requirements are described first and their importance for the design of an automotive IDS is discussed. For example, with regard to safety requirements, an IDS must not delay the communication of safety relevant data, as this can in turn delay the functionality of live-saving measures. Also requirements for privacy and security are set up which, for instance, predetermine that no user data is disclosed. Furthermore, possible attack types on intra-vehicle communication structures, which can be used to cause severe harm to those affected vehicles, are discussed. Regarding the IDS requirements and the attack types, different concepts are presented which form the basis of current IDSs. The focus is mainly put on existing signature and anomaly-based network realizations, with several approaches being introduced more detailed here. After discussing possibilities on how to react to the detection of a potential intrusion attempt, this overview is concluded with an outlook on what still has to be achieved to successfully integrate the presented systems into a vehicle, as these point to relevant research questions.

[1] Bosch Engineering GmbH, Robert-Bosch-Allee 1, 74232 Abstatt, Germany, oleg.schell@de.bosch.com
[2] Hochschule RheinMain, Kurt-Schumacher-Ring 18, 65197 Wiesbaden, Germany, janpeterreinhard@gmail.com
[3] Robert Bosch GmbH, Mittlerer Pfad 9, 70499 Stuttgart, Germany, marcel.kneib@de.bosch.com
[4] Bosch Engineering GmbH, Robert-Bosch-Allee 1, 74232 Abstatt, Germany, martin.ring@de.bosch.com

References

[Fl16] Flores-Arias, JM; Ortiz-Lopez, M; Quiles-Latorre, Francisco Javier; Pallarés, Víctor; Chen, A: Complete hardware and software bench for the CAN bus. In: 2016 IEEE International Conference on Consumer Electronics (ICCE). IEEE, pp. 211–212, 2016.

[MV13] Miller, Charlie; Valasek, Chris: Adventures in automotive networks and control units. Def Con, 21:260–264, 2013.

[MV15] Miller, Charlie; Valasek, Chris: Remote exploitation of an unaltered passenger vehicle. Black Hat USA, 2015:91, 2015.

[Te18] Tencent Keen Security Lab: Experimental Security Assessment of BMW Cars: A Summary Report. 2018.

[Te19] Tencent Keen Security Lab: Experimental Security Research of Tesla Autopilot. March 2019.

[UN20] UN Task Force on Cyber Security and Over-The-Air issues: Proposal for the 01 series of amendments to the new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of cybersecurity management systems. 2020.