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

Effects of the Sampling Technique on Sender Identification Systems for the Controller Area Network

Marcel Kneib[1], Oleg Schell[2]

Abstract: The connectivity of modern vehicles, as well as the associated amount of interfaces, is constantly increasing. This trend does not only allow additional comfort functionalities and complex driver assistance systems, but also offers additional possibilities to attack a vehicle and its functions. Evidence that this is not only a theoretical threat was demonstrated by the attack of Miller and Valasek [MV13; MV15], as well as the latest research of the Tencent Keen Security Lab [Ca19; Te18; Te19]. Due to the absence of authenticity in the Controller Area Network (CAN), which is still the most commonly used bus technology in the automotive domain, an Electronic Control Unit (ECU) cannot check whether a received message was sent by a legitimate sender. This enables the forgery of messages, i.e. the execution of impersonation attacks. However, the use of cryptographic methods is limited due to the constrained resources of the platforms used in vehicles and the low payload and bandwidth of CAN. As an alternative or in combination with attack detection, methods have been presented in the past which provide sender identification on the basis of analog signals [Kn20]. Due to the static configuration of the internal vehicle communication, such systems allow to verify whether a message was sent by a valid ECU. For identification, however, the signals of CAN messages must first be recorded, for which the mentioned approaches suggest different procedures. While some methods capture the entire signal in order to extract the signal characteristics [Ch18; KH18], others concentrate on specific parts [Fo19] or individual points of a frame to determine the sender [KSH20]. The signal recording procedure has a corresponding effect on various properties, such as hardware requirements, costs, complexity and signal quality. In addition, the requirements and architecture of the actual system also have a major influence on the type of recording. For example, it can be an advantage to use additional hardware resources if this accelerates the recording of the relevant signal part, thus enabling the parallel observation of several bus segments. This paper presents the different recording approaches and analyzes the associated effects on the relevant properties of sender identification systems for CAN. In addition, the associated performance is analyzed using the example of the recently presented work Edge-based Sender Identification (EASI) [KSH20] utilizing data from a series production vehicle. Furthermore, this work presents the individual application possibilities of the different sampling techniques, so that the reader is able to assess the optimal methodology with corresponding effects and constraints according to the respective requirements.

[1] Robert Bosch GmbH, Mittlerer Pfad 9, 70499 Stuttgart, Germany, marcel.kneib@de.bosch.com
[2] Bosch Engineering GmbH, Robert-Bosch-Allee 1, 74232 Abstatt, Germany, oleg.schell@de.bosch.com

CC BY NC SA

References

[Ca19] Cai, Z.; Wang, A.; Zhang, W.; Gruffke, M.; Schweppe, H.: 0-days & Mitigations: Roadways to Exploit and Secure Connected BMW Cars. Black Hat USA 2019/, p. 39, 2019.

[Ch18] Choi, W.; Joo, K.; Jo, H. J.; Park, M. C.; Lee, D. H.: VoltageIDS: Low-Level Communication Characteristics for Automotive Intrusion Detection System. IEEE Transactions on Information Forensics and Security 13/8, pp. 2114–2129, Aug. 2018, ISSN: 1556-6013.

[Fo19] Foruhandeh, M.; Man, Y.; Gerdes, R.; Li, M.; Chantem, T.: SIMPLE: Single-Frame Based Physical Layer Identification for Intrusion Detection and Prevention on in-Vehicle Networks. In: Proceedings of the 35th Annual Computer Security Applications Conference. ACSAC '19, Association for Computing Machinery, San Juan, Puerto Rico, pp. 229–244, 2019, ISBN: 978-1-4503-7628-0, URL: https://doi.org/10.1145/3359789.3359834.

[KH18] Kneib, M.; Huth, C.: Scission: Signal Characteristic-Based Sender Identification and Intrusion Detection in Automotive Networks. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. CCS '18, ACM, New York, NY, USA, pp. 787–800, 2018, ISBN: 978-1-4503-5693-0, URL: http://doi.acm.org/10.1145/3243734.3243751.

[Kn20] Kneib, M.: A Survey on Sender Identification Methodologies for the Controller Area Network. In (Reinhardt, D.; Langweg, H.; Witt, B. C.; Fischer, M., eds.): SICHERHEIT 2020. Gesellschaft für Informatik e.V., Bonn, pp. 91–103, 2020.

[KSH20] Kneib, M.; Schell, O.; Huth, C.: EASI: Edge-Based Sender Identification on Resource-Constrained Platforms for Automotive Networks. In: Proceedings of the 27th Network and Distributed System Security Symposium. 2020.

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

[MV15] Miller, C.; Valasek, C.: Remote exploitation of an unaltered passenger vehicle. Black Hat USA 2015/, p. 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. 2019.