Propose a new In-Vehicle CAN attack using analog signals for CAN bus fuzzings

Kyungrok Park, Samuel Woo, and Taekyoung Youn*

Dankook University, Yongin-si, Gyeonggi-do, South Korea
{dbqlrnswn, samuelwoo, taekyoung }@dankook.ac.kr

Abstract

With advancements in modern vehicle technology, the number of Electronic Control Units(ECUs) inside a vehicle has increased and various networks in the vehicle control these ECUs. Among them, CAN is used the most [1]. However, security techniques, such as using a rack of message authentication, unsegmented networks, and unencrypted messages, have not been applied to the CAN [2]. Therefore, the Controller Area Network(CAN) is currently the target of most malicious attacks and abuses in vehicles and various cybersecurity activities are being introduced in automobiles to prevent this. For example, vulnerability analysis, which is a cybersecurity activity, was performed to address the vulnerabilities of the CAN. Through the fuzz test, defects and collisions inside the CAN were inspected [3] [4]. The existing CAN bus fuzzing tool analyzes and evaluates Denial of Service , replay, and impersonation attacks using digital signals and software vulnerabilities. In this study, we present new attack methods using the characteristics of CAN analog signal, in addition to previously known attack methods for various fuzzing Tools.

Keywords: Automotive, CAN Bus, In-vehicle Network, CAN analog Signal, Fuzzing **Acknowledgement:** This work was supported by the Technology Innovation Program (P0023522, HRD Program for Industrial Innovation) funded By the Ministry of Trade, Industry & Energy(MOTIE, Korea)

References

[1] Seung-Han Kim, Suk-Hyun Seo, Jin-Ho Kim, Tae-Moon Moon, Chang-Wan Son, Sung-Ho Hwang, and Jae Wook Jeon. A gateway system for an automotive system: Lin, can, and flexray. In *2008 6th IEEE International Conference on Industrial Informatics*, pages 967–972. IEEE, 2008.

[2] Clinton Young, Joseph Zambreno, Habeeb Olufowobi, and Gedare Bloom. Survey of automotive controller area network intrusion detection systems. *IEEE Design & Test*, 36(6):48–55, 2019.

[3] Daniel S Fowler, Jeremy Bryans, Siraj Ahmed Shaikh, and Paul Wooderson. Fuzz testing for automotive cyber-security. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pages 239–246. IEEE, 2018.

[4] Daniel S Fowler, Jeremy Bryans, Madeline Cheah, Paul Wooderson, and Siraj A Shaikh. A method for constructing automotive cybersecurity tests, a can fuzz testing example. In *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 1–8. IEEE, 2019.

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No.P-14

*Corresponding author: Department of Industrial Security, Dankook University, Giheung-gu, Yongin-si (16891) 655, Korea, Email: taekyoung@dankook.ac.kr