Novel CAN Bus Fuzzing Framework for Finding Vulnerabilities in Automotive Systems

Manu Jo Varghese, Adnan Anwar, Frank Jiang, Robin Doss

Centre for Cyber Resilience and Trust, Deakin University, Geelong, Australia

mvarghese@deakin.edu.au

***Abstract*—Modern vehicles, increasingly becoming interconnected digital ecosystems, rely on sophisticated networks for operations and safety. This study introduces a novel fuzzing framework aimed at identifying vulnerabilities within automotive systems, specifically focusing on the Controller Area Network (CAN) bus. By employing "Automated Reverse Engineering-Guided Fuzzing," our framework evaluates the security resilience of these networks against sophisticated attacks. Modified data packets are disseminated within the CAN framework, and ECU reactions are monitored, uncovering potential vulnerabilities. This comprehensive approach not only identifies weaknesses but also enhances the understanding of operational characteristics, setting a new benchmark for automotive cybersecurity.**

***Index Terms*—CAN bus, automotive systems, cybersecurity, fuzzing, vulnerability detection, ECU, automated reverse engineering**

I. Introduction

In the realm of modern automotive engineering, the advent of complex sensor and computational networks has brought forth unprecedented enhancements in vehicle functionality, including autonomous driving and real-time navigation (Giannaros et al., 2023) [1]. Yet, this sophistication introduces significant cybersecurity risks, particularly within the Controller Area Network (CAN) bus, which is vital for ECU communication but inherently vulnerable to cyber-attacks. This paper presents a specialized fuzzing framework aimed at proactively identifying and mitigating such vulnerabilities, employing a blend of automated testing and reverse engineering to scrutinize the CAN bus's security landscape (Cremer et al., 2022) [2].

Our research's cornerstone is an innovative fuzzing methodology that feeds the system with aberrant data to expose potential security loopholes. Simulated cyber-attacks probe the resilience of ECUs, revealing both existing weaknesses and operational patterns susceptible to exploitation. By systematically analyzing attack outcomes, we propose not just a diagnostic tool, but a strategic blueprint for fortifying automotive cybersecurity. This work endeavors to safeguard the burgeoning connectivity intrinsic to modern vehicles, setting a trajectory for heightened security in automotive technology.

II. Motivation

In the contemporary landscape of automotive engineering, vehicles have evolved into intricate networks brimming with digital intelligence. Central to this evolution is the Controller Area Network (CAN) bus system, which, while being the linchpin of vehicular communication, has emerged as a potential playground for cyber adversaries due to its inherent lack of robust security protocols. As the automotive industry propels toward an increasingly interconnected future, the urgency to fortify these vehicular networks against cyber threats becomes not just a priority, but a critical imperative [3].

The motivation behind our novel fuzzing framework stems from the imperative to bridge the security lacunae inherent in the CAN bus systems of modern vehicles. Traditional security solutions [13] fall short in addressing the dynamic and complex nature of cyber-physical automotive systems, rendering them vulnerable to sophisticated cyber-attacks that could lead to catastrophic safety and privacy breaches. Previous studies have explored various techniques for reverse engineering and fuzzing the CAN bus to uncover vulnerabilities [4], [5], [6]. Yet, these investigations often isolate reverse engineering and fuzzing as distinct methodologies, lacking a cohesive strategy that leverages the strengths of both to systematically identify and mitigate automotive cybersecurity threats. This disjointed approach may not fully capitalize on the potential insights reverse engineering offers for more targeted and effective fuzzing. Our research bridges this gap by integrating reverse engineering with fuzzing into a comprehensive framework specifically tailored for the automotive CAN bus. This unified method not only streamlines the process of vulnerability detection but also facilitates the development of precise mitigation strategies Our framework introduces an innovative, holistic approach, employing Automated Reverse Engineering-Guided Fuzzing to systematically simulate and analyze potential cyber-attacks, enabling the detection and fortification against security vulnerabilities.

III. Proposed Framework and Methodology

In addressing the critical need for automotive cybersecurity, we have devised a novel fuzzing framework that employs Automated Reverse Engineering-Guided Fuzzing (ARE-GF) to interrogate the Controller Area Network (CAN) bus. This methodical approach, which harnesses a unique blend of reverse engineering and sophisticated fuzzing techniques, is meticulously designed to detect vulnerabilities by simulating a spectrum of cyber-attacks.

2833-292X/24/$31.00 ©2024 IEEE
DOI 10.1109/DSN-S60304.2024.00024

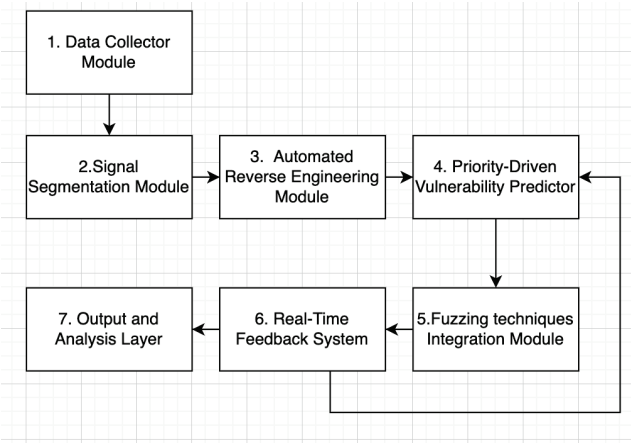

Fig. 1: Proposed Fuzzing Framework

Figure 1 illustrates the key components of our proposed fuzzing framework. The Proposed framework employs a segmentation process that begins with an algorithm that constructs signals from the data frames collected by the Data Collector Module. Starting from the first bit, it incrementally appends bits, hypothesizing the formation of complete signals. Once a potential signal is formed, it undergoes a strict validation process to assess its viability. Decision points in the process include either expanding the signal by adding more bits for reevaluation or confirming the signal's completion and moving to the next set of bits. This iterative method continues until every bit in the frame is evaluated, ensuring each signal is thoroughly examined and correctly interpreted.

For each frame in the 'candump', the algorithm examines all possible signal lengths starting from the first bit. It extracts a potential signal and checks if adding another bit changes its value. If it does, the signal is committed as complete, and the process moves to the next bit. This step-by-step procedure is critical in identifying and separating meaningful data from the CAN bus traffic, enabling further analysis of ECU-originated data and uncovering common data types and boundaries. These foundational steps set the stage for the subsequent phase of vulnerability prediction and refinement of fuzzing techniques, which are pivotal for enhancing the CAN bus's security against cyber threats.

IV. Evaluation and Findings

The assessments elucidate the proposed framework's capabilities in enhancing automotive cybersecurity, particularly through its nuanced approach to fuzzing and vulnerability analysis. The framework has a pass rate of 94% which is superior to other competitive frameworks and it is possible by the Automated Revere Engineering guided fuzzing process.

TABLE I: Comparison of frameworks in addressing identified vulnerabilities and their pass rate.

Framework	Extended CAN IDs	DoS Vulnerability	Pass Rate
Q. Li [7].	×	×	70%
Shirvani [8].	Unknown	×	80%
Schönhärl [9].	×	Unknown	75%
S. Li [10]	Unknown	✓	67%
F. Luo [11].	✓	✓	72%
K. He [12].	×	×	76%
Proposed Framework	✓	✓	94%

To benchmark the performance of our proposed framework, we conducted a comparative analysis against six existing frameworks, as shown in Table 1. The proposed fuzzing framework was rigorously evaluated through a comprehensive testing regime designed to assess its effectiveness in identifying vulnerabilities within the CAN bus system of modern automotive architectures. The evaluation process involved the simulation of various attack scenarios that the CAN bus network might encounter, including but not limited to, spoofing attacks, denial-of-service (DoS) attacks, and message replay attacks. This section outlines the methodology employed in the evaluation process, the testing environment, and a detailed analysis of the findings obtained from the experimental simulations.

V. Conclusion and Future Work

In a nutshell, our research combines the power of automated reverse engineering and guided fuzzing which gives a superior pass rate and uncover some potential unknown vulnerabilities. Our Oongoing work focuses on polishing the reverse engineering process by utilising ML techniques and winding the Vehicle models and ECU range to further test the model performance and adapt to the real-world situations.

References

[1] A. Giannaros, A. Karras, L. Theodorakopoulos, C. Karras, P. Kranias, N. Schizas, G. Kalogeratos, and D. Tsolis, "Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 493–543, 2023. [Online]. Available: https://doi.org/10.3390/jcp3030025

[2] F. Cremer, B. Sheehan, M. Fortmann, A. N. Kia, M. Mullins, F. Murphy, and S. Materne, "Cyber risk and cybersecurity: A systematic review of data availability," *The Geneva Papers on Risk and Insurance - Issues and Practice*, vol. 47, no. 3, pp. 698–736, 2022. [Online]. Available: https://doi.org/10.1057/s41288-022-00266-6

[3] Brown, A. (2011). "Connectivity and the mobility industry. SAE International". http://euro.ecom.cmu.edu/resources/elibrary/auto/PT-148.pdf

[4] A. Buscemi, I. Turcanu, G. Castignani, R. Crunelle, and T. Engel, "CANMatch: A fully automated tool for CAN bus reverse engineering based on frame matching," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 12358–12373, 2021. [Online]. Available: https://doi.org/10.1109/TVT.2021.3124550

[5] T. Huybrechts, Y. Vanommeslaeghe, D. Blontrock, G. Van Barel, and P. Hellinckx, "Automatic reverse engineering of CAN bus data using machine learning techniques," in *Advances on P2P, Parallel, Grid, Cloud and Internet Computing*. Springer, 2017, pp. 751–761. [Online]. Available: https://doi.org/10.1007/978-3-319-69835-9_71

[6] A. Frigerio, B. Vermeulen, and K. Goossens, "Component-level ASIL decomposition for automotive architectures," in *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, 2019. [Online]. Available: https://doi.org/10.1109/DSN-W.2019.00021

[7] S. Li, X. Zhang, Y. Zhou, and M. Zhang, “SP-E: Security Evaluation Framework of In-vehicle Infotainment System based on Threat Analyses and Penetration Tests,” J. Phys. Conf. Ser., vol. 2517, p. 012012, 2023.
[8] F. Luo, X. Zhang, and S. Hou, “Research on Cybersecurity Testing for In-vehicle Network,” in Proceedings of the 2021 International Conference on Intelligent Technology and Embedded Systems (ICITES), Chengdu, China, September 2022.
[9] K. He, C. Wang, Y. Han, and X. Fang, “Research on cyber security Technology and Test Method of OTA for Intelligent Connected Vehicle,” in Proceedings of the 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), Virtual Conference, China, July 2022.
[10] Q. Li, J. Zuo, R. Cao, J. Chen, Q. Liu, and J. Wang, “A Security Evaluation Framework for Intelligent Connected Vehicles Based on Attack Chains,” IEEE Network, p. 1, 2023.
[11] S. Shirvani, Y. Baseri, and A. Ghorbani, “Evaluation Framework for Electric Vehicle Security Risk Assessment,” IEEE Trans. Intell. Transp. Syst., pp. 1–24, 2023.
[12] B. Arkin, S. Stender, and G. McGraw, “Software penetration testing,” IEEE Secur. Priv., vol. 3, pp. 84–87, 2005.
[13] T. Hutzelmann, S. Banescu, and A. Pretschner, “A comprehensive attack and defense model for the automotive domain,” *SAE International Journal of Transportation Cybersecurity and Privacy*, vol. 2, no. 1, 2019. [Online]. Available: https://doi.org/10.4271/11-02-01-0001