Demo: CAN Security Hands-On Education Platform

Ayaka Matsushita*, Tsuyoshi Toyama*, Hisashi Oguma*, Takeshi Sugawara†
*Toyota Motor Corporation
†The University of Electro-Communications

I. Introduction

While the future connected autonomous vehicles become increasingly more complex, there is a huge demand for the education and training of security engineers with controller area network (CAN). Although software simulators (e.g., ICSim) are a cost-effective education platform, hands-on experience using hardware is still a crucial part in learning CAN security. However, learning by attacking real cars is controversial for ethical and legal concerns. Arduino can be a cheap hardware platform, but it lacks software to simulate the in-car system, including CAN IDs and data formats. Hardware/software-in-the-loop simulators (HILS and SILS) can address the issue, but they are professional tools and expensive for teaching.

Addressing the issue, we developed *PASTA for Education* comprising two hardware ECUs that generate realistic CAN network traffic. PASTA for Education is easily accessible with the simple architecture and open-source software and hardware designs [1]. This demonstration showcases its real-time interaction and analysis capabilities. Furthermore, we show a CTF-style activity based on PASTA for Education that we used for our competitions and our university course. The setup is designed to provide participants with hands-on experience in understanding the security of CAN networks.

II. PASTA for Education

PASTA for Education aims at teaching the basics of the CAN protocol and its security, including reverse engineering, denial of service, and fake message injection. It is made up of two hardware ECUs along with software running on a PC that emulates the dashboard, as shown in Fig. 1.

The first ECU represents the powertrain system, and the other represents the body and chassis systems. CAN IDs and messages transmitted among them are designed with reference to a real-car network. The two junction boxes interconnect the ECUs with patch cables, and a user can sniff and inject any CAN traffic by hooking a USB-CAN adapter to them. The user can also temporarily disconnect the cable from the junction box to reverse engineer the mapping between CAN IDs and ECUs. The hardware and firmware designs of the ECU are distributed as open source[1], allowing users to extend the platform.

The ECUs and the control PC are connected through a USB serial interface, which is used as a control-plane network. The software running on the control PC present users a dashboard interface. User interactions on the software, such as dragging a handle with a mouse, change the car behavior and the underlying CAN messages.

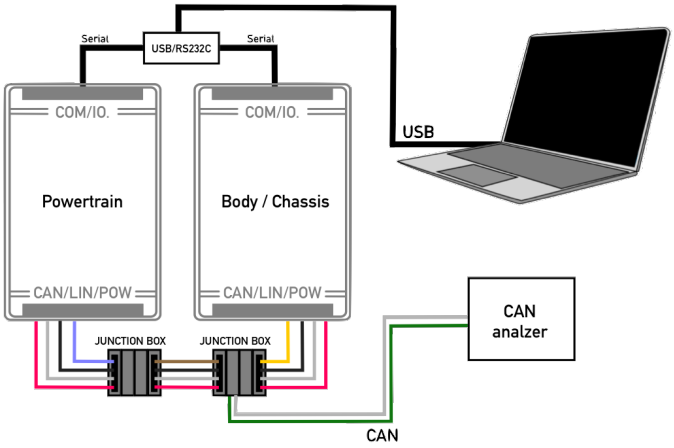

Fig. 1. PASTA for Education composed of two ECUs talks with a PC running a software for emulating the dashboard. Users capture CAN traffic by hooking a USB-CAN adapter to the junction box. The minimum configuration requires a single PC which runs the emulation software and a CAN analyzer.

We used PASTA for Education in the CTF competitions and the university course. The CTF competition in 2022 (resp. 2023) invited the 13 (resp. 11) teams of university students from the United States and Japan. The CTF challenges cover a wide range of CAN security topics, including traffic analysis, injection attacks, OBD-II/UDS analyzes, firmware reprogramming, and reading the PCB marking and schematic diagram. The course comprises a series of lectures, hands-on training, and CTF-style quizzes and was opened to graduate students not familiar with automotive security in 2023.

III. Conclusion

PASTA for Education is designed to efficiently teach automotive security. It is leveraged in the CTF competitions and in the university course for university students in 2022 and 2023. We continuously develop PASTA for Education to contribute to education of automotive security. Current teaching materials are limited to the basics for beginners. Therefore supporting more advanced automotive security topics for engineers is one of future works. We also plan to distribute PASTA for Education's materials further, including teaching materials.

[1] https://github.com/pasta-auto

Symposium on Vehicles Security and Privacy (VehicleSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-7-6
https://dx.doi.org/10.14722/vehiclesec.2024.25003
www.ndss-symposium.org

References

[1] T. Toyama, A. Matsushita, H. Oguma, and T. Matsumoto, "Series of PASTAs to Meet Diverse Needs," Computer Security Symposium, 2021.