Title: Securing V2X communication exchanges for automated telematic control unit

Keywords: **Intelligent Transportation System, V2X Communication, Security, Intrusion detection**

Context

Connected and Automated Vehicles (CAV) have become a prominent technology for the future of passenger and freight mobility. As the number of connected vehicles is almost 200 million in 2023 and is expected to reach 367 million by 2027, the need for resilient and secured communication infrastructures is crucial. By exploiting various communication links such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), usually clustered under the term V2X (Vehicle-to-Everything), connected vehicles offer multiple services and applications for a safer, more efficient, and more comfortable mobility.

Connected vehicles interact with V2X applications deployed in cloud or edge servers for multiple functionalities such as data offloading, remote monitoring and diagnostics, software updates, and so on. To support these functionalities, they are equipped with a Telematic Control Unit (TCU) which represents the main vehicle gateway between the in-vehicle network and external entities. Current TCUs integrate multiple radio technologies such as cellular network (4G/5G), C-V2X, Wi-Fi and can be extended with other bearers such as satellite communication.

Being the main component from which data packets are going in and out from the vehicle, it is important to ensure that the TCU can keep a safe and secured behaviour against potential attacks from external entities. Among potential attacks, we can denote GNSS jamming and spoofing, network flooding, data messages corruption.

Problem statement

In this work, we focus on securing the information exchange between vehicular TCU and backend servers from the Original Equipment Manufacturer (OEM) and the service providers. Given the vulnerabilities of technologies used for V2X communication, it is very likely that a TCU can be attacked, potentially resulting into severe consequences on the on-board vehicle equipment if timely detection and countermeasures are not implemented.

Motivation

Securing on-board components of a connected vehicle is a key priority for OEMs as security issues can lead to dangerous situations for vehicle's passengers and important costs for automotive companies in case, they need to recall millions of cars.

On the one hand, securing in-vehicle communication has been extensively studied, and due to the on-board system's ability to function as a closed network, it becomes considerably complex to target it with an attack. On the other hand, V2X communications involve interactions with external entities that need to be trusted. Such communications also involve networks which are operated by other operators, have their own security or even unoperated, secured with neutral entities.

Goal

The goal of this thesis is threefold:

1. A risk assessment performance to identify main vulnerabilities of multi-technology TCU.

2. The proposal of an intrusion detection approach for the security of the end-to-end communication between the CAV and the V2X applications.
3. The proposal of a resilience by design approach for the CAVs.

Thesis supervision

Supervisor: Joaquin Garcia-Alfaro (Institut Mines-Telecom, Telecom SudParis)
Co-Supervisors: Pierre Merdrignac (Vedecom), Badis HAMMI (Institut Mines-Telecom, Telecom SudParis), Ghada Gharbi (EPITA).

Required profile

Applicants must hold a master's degree or an equivalent degree (e.g., engineering degree) in Computer Science, Telecommunications Engineering, or Applied Sciences. A strong foundation in either cybersecurity, networks, mathematics for data science, and performance evaluation is essential, along with skills in programming languages, such as Python and C/C++. Practical experience in machine learning will be highly appreciated. A good English level is a required, while French language skills are not mandatory but highly appreciated.

How to apply

Candidates must provide:

- A curriculum vitae
- Diplomas and transcripts of grades
- A motivation letter

Applications should be sent to:

Badis HAMMI (badis.hammi@epita.fr), Pierre Merdrignac (pierre.merdrignac@vedecom.fr), Ghada Gharbi (ghada.gharbi@epita.fr)

Application deadline*:* 30 Septembre 2023

References

[1] Alan Weissberger (2023). Juniper Research: 5G connectivity opportunity for the connected car market. IEEE ComSoc Technology Blog.

[2] Parrend, P., Guigou, F., Navarro, J., Deruyver, A., & Collet, P. (2018). Artificial Immune Ecosystems: the role of expert-based learning in artificial cognition. Journal of Robotics, Networking and Artificial Life, 4(4), 303-307.

[3] Bitam, S., Zeadally, S., & Mellouk, A. (2016). Bio-inspired cybersecurity for wireless sensor networks. IEEE Communications Magazine, 54(6), 68-74.

[4] P. Parrend, Immune-based defense and resiliency, Nature-inspired Cyber Security and Resilience: Fundamentals, Technology and Applications, El-Sayed M. El-Alfy, Mohamed Eltoweissy, Errin Fulp, Wojciech Mazurczyk (Eds.), IET, mars 2019

[5] Shamshirband, S., Anuar, N. B., Kiah, M. L. M., Rohani, V. A., Petković, D., Misra, S., & Khan, A. N. (2014). Co-FAIS: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks. Journal of Network and Computer Applications, 42, 102-117.

[6] Saleem, K., Chaudhry, J., Orgun, M. A., & Al-Muhtadi, J. (2017, December). A bio-inspired secure IPv6 communication protocol for Internet of Things. In 2017 Eleventh International Conference on Sensing Technology (ICST) (pp. 1-6). IEEE.

[7] Korczynski, M., Hamieh, A., Huh, J. H., Holm, H., Rajagopalan, S. R., & Fefferman, N. H. (2016). Hive oversight for network intrusion early warning using DIAMoND: a bee-inspired method for fully distributed cyber defense. IEEE Communications Magazine, 54(6), 60-67.

[8] Zhang, J., Zheng, K., Zhang, D., & Yan, B. (2020). AATMS: An anti-attack trust management scheme in VANET. IEEE Access, 8, 21077-21090.

[9] Ayrault, M., Kühne, U., & Borde, É. (2022). Finding Optimal Moving Target Defense Strategies: A Resilience Booster for Connected Cars. Information, 13(5), 242.