Title: Securing V2X communication exchanges for automated telematic control unit

Keywords: V2X Communication, Security,

Context

Connected and Automated Vehicles (CAV) have become a prominent technology for the future of passenger & 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 the design of an approach to secure CAV nodes and the end-to-end interactions between the TCU and the V2X application services. To this end, we rely on bio-inspired techniques.

Bio-inspired techniques are inspired by biological phenomena such as biological evolution, biological immune system, neural networks, and swarm intelligence. Bio-inspired cybersecurity approaches are initially motivated by the successful adaptive defense process of insects against threats where they can ramp up their defense rapidly [2][3]. Bio-inspired cybersecurity have been largely studied and applied in numerous use cases [4]. Bitam et al. [2] proposed a generic bio-inspired machine-learning model called Swarm Intelligence for WSN Cybersecurity (SIWC) to enhance the security of Wireless Sensor Networks (WSN). SIWC is a neural network system trained by swarm intelligence optimization to automatically and efficiently determine the optimal critical parameters used to detect cyber-attacks.

In the same context of WSN, Shamshirband et al. [3] proposed an artificial immune system to mitigate WSN DoS attacks. It is a modular-based defense system that consists of a set of agents working together to calculate the abnormality of sensor behavior or to detect the attackers.

In the context of 5G networks, Saleem et al. [4] proposed an approach called Bio-Inspired Secure IPv6 Communication Protocol. This approach improves routing protocols for low-power and lossy networks with classification algorithms supported by an artificial immune system, which classifies the node as self or non-self-based on the behavior using a correlation coefficient algorithm and according to the given threshold. Node energy, link throughput, latency, and quality are used as metrics to detect misbehavior.

Korczynski et al. [5] proposed a distributed, self-organized, honeybee-inspired algorithm for early anomaly detection in a connected system over a wireless network. The algorithm is derived by observing the colonies of honeybees and imitates the way that honeybees use to forage efficiently. The foraging methods may be mapped to computer system networks in order to detect and mitigate distributed attacks in an automated fashion. The proposed approach uses a distributed coordination framework to dynamically and automatically detect distributed attacks using a feedback mechanism.

Unfortunately, very few works focused on the application of bio-inspired techniques to enhance the cybersecurity of vehicular networks.

Zhang et al. [6] introduced an anti-attack trust management scheme. They calculate local trust and global trust, which indicate the local and global trust relationships among vehicles. First, Bayesian inference is adopted to calculate local trust of vehicles based on historical interactions. Then a selection of a small set of seed vehicles according to local trust and some social factors. Once they identify the reputable seed vehicles, they use the local trust link structure of vehicles to evaluate the global trust of all vehicles.

Ayrault et al. [7] presented a game-theoretic model that can be used to compute an optimal Moving Target Defense for a critical embedded system that is facing several attackers with different objectives. However, this approach focused only on CAN communication and the embedded system behavior.

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. For this end we will rely on Neural networks and Artificial Immune Systems.

3. The proposal of a resiliency by design approach for the CAVs. Hence, we propose the use of a moving target defense which consists in modifying the configuration of a CAV's system in such a way to make deterministic attacks impractical. This pattern of defense can be seen in many biological viruses e.g., as HIV, which constantly modify surface proteins exposed to the outside world in such a way as to evade attack by the immune system. In this thesis, we would like to investigate the potential of architectural reconfigurations of the networking setup as a mobile defense against cyber-attacks in CAVs.

Thesis supervision:

Supervisor: Didier Verna (EPITA)
Co-Supervisors: Badis HAMMI (Telecom SudParis), Ghada Gharbi (EPITA)

Plan

1- Year 1:
- State of the art (3 months)
- A survey paper (3 months)
- Proof-of-concept (PoC) of the thesis goal
- Iteration 1: core of scientific contribution (6 months)
    - Rewrite core research question, rewrite thesis subject.
    - Formalize scientific contribution, develop PoC of the contribution.
    - Conference paper.

2- Year 2:
- Iteration 2: refine/extend scientific contribution (6 months)
    - Research question.
    - Formalize scientific contribution, develop PoC of the contribution.
    - Use simulation to validate the results obtained.
    - Conference paper.
- Journal paper (6 months)

3- Year 3:
- Iteration 3: refine/extend again (6 months)
    - Research question.
    - Formalize scientific contribution, develop PoC of the contribution.
    - Use of real implementation.
    - Conference paper.
    - Journal paper.
- Redaction (6 months)
    - Finalize thesis outline.
    - Write (4 months).

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:

Pierre Parrend (pierre.parrend@epita.fr)

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.