The Need for a Multilayer Cybersecurity Framework for IoV

Mohammad Hamad and Jan Lauinger

July 30, 2021

1 Introduction

During the last decade, significant developments were introduced within the vehicular domain, evolving the vehicles to become a network of many embedded systems distributed throughout the car, known as Electronic Control Units (ECUs). Each of these ECUs runs several software components that collaborate to perform various vehicle functions. In addition, modern vehicles are also equipped with multiple technologies, such as WiFi, 5G, GPS, and Bluetooth, giving them the capability to collaborate and communicate with roadside units to ensure a safe and comfortable journey for drivers and passengers. Adding all these technologies was a double-edged sword. On the one hand, it extends the vehicle's functionalities and capabilities. On the other hand, it opens the door to several cybersecurity threats and makes the car a more attractive target for adversaries [1, 2].

Securing modern vehicles requires a holistic solution that considers security during the whole life cycle of the vehicle development, starting from the secure development of components, continuing to protect them. At the same time, they operate and reacting correctly even when an attack is successful.

2 IOV Secure Multilayer Framework Architecture

In [3], we have proposed a holistic framework (shown in Figure 1) to ensure the security of the vehicular system. This framework consists of multiple layers of mitigation strategies to deal with cybersecurity intrusions and provide a high degree of protection for the IoV ecosystem. We have proposed a framework that is based on the cybersecurity framework proposed by the National Institute of Standards and Technology (NIST) [4]. The NIST framework uses five principal functions, "Identify, Protect, Detect, Respond, and Recover," to build a comprehensive approach to developing layered cybersecurity. Our framework depends on three principles: prevention, detection, and response, covering most of the NIST framework's functions.

- **Prevention**: This is covered by the first two layers. Within the first layer (i.e., layer 0), a comprehensive thread modeling process identifies all

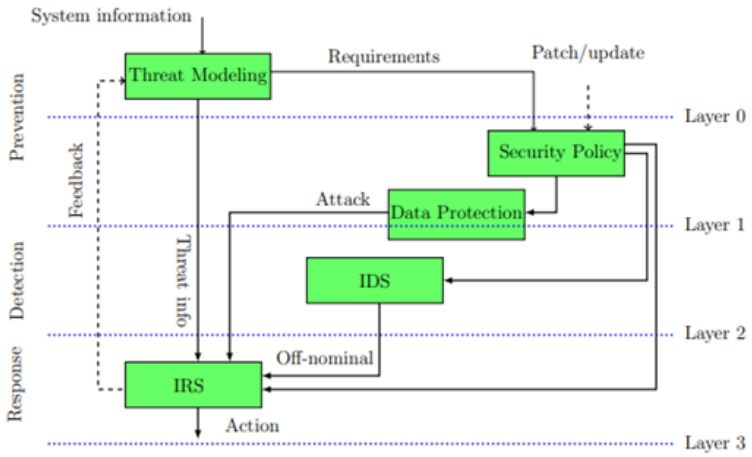

Figure 1: The different layers of the proposed secure framework [3].

possible threats and vulnerabilities which could face the system. One primary outcome of this process is defining the security requirements for the different system assets. These requirements need to be satisfied to prevent attackers from compromising the system. The second layer (i.e., Layer 1) includes developing the security policy that implements each system component's security requirements. The security policy contains security rules which the other layers of the framework will use. Another process within this layer is defining the mechanism used to enforce the security policy and implement a mechanism to ensure the security requirements. This function includes building an access control mechanism to prevent unauthorized parties from accessing the system assets. Also, it adopts crypto mechanisms to ensure data security. Some of these mechanisms, such as a firewall, can be considered detection and prevention tools simultaneously; therefore, they can overlay on to the next layer.

- **Detection** This is covered by layer 2. The core function of this layer is building monitoring mechanisms to detect the occurrence of cyber-attacks that were not prevented by the prevention layers. This layer ensures continuance monitoring as well as the early detection of attacks and suspicious actions. Both anomaly-based and signature-based detection technologies need to be adopted in this layer. Security policy plays a pivotal role in defining the nominal behavior of the system components. This defined behavior is used as a reference to detect any odd behaviors.

- **Response**: This is covered by layer 3. This layer determines the process when a security violation is detected either by layer 1 or layer 2. The main aim of this layer is to protect the vehicle from entering unstable states as a result of the detected attack. The effective design of this layer requires inputs from the above layers, such as the properties of the detected attack or the off-nominal behavior. The security policy is also needed for this layer since it includes possible responses for different attacks. Besides that, the collocated characteristics of attacks (i.e., aim, scenario, severity,

etc.) are needed too [5]. One output of this layer is feedback which can be used to support the next threat modelling process. In addition, it can be used to develop patches or updates for the security policy to mitigate these attacks. This update will be reflected on the underlying layers.

3 nIoVe and Multilayer cybersecurity framework

The main goal of the nIoVe project[1] is to provide multi-layered cybersecurity solutions for the IoV by:

- developing blockchain-based trust management solutions to ensure secure communication among the different components of the IoV ecosystem [6, 7].
- developing Machine-learning based mechanisms for near real-time intrusion detection and threat analysis.
- developing effective response strategies that mitigate complex cyberattacks and ensure the system's successful recovery from any risky situation.

References

[1] Rudolf Hackenberg, Nils Weiss, Sebastian Renner, and Enrico Pozzobon. Extending vehicle attack surface through smart devices. In *The Eleventh International Conference on Emerging Security Information, Systems and Technologies*, pages 131–135, 2017.

[2] Ishtiaq Rouf, Robert D Miller, Hossen A Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In *USENIX Security Symposium*, volume 10, 2010.

[3] Mohammad Hamad. *A multilayer secure framework for vehicular systems*. PhD thesis, Technische Universität Carolo-Wilhelmina zu Braunschweig, 2020.

[4] National Highway Traffic Safety Administration et al. Cybersecurity best practices for modern vehicles. *Report No. DOT HS*, 812(333):17–20, 2016.

[5] Mohammad Hamad, Marinos Tsantekidis, and Vassilis Prevelakis. Redzone: Towards an intrusion response framework for intra-vehicle system. In *VEHITS*, pages 148–158, 2019.

[6] Jan Lauinger, Jens Ernstberger, Emanuel Regnath, Mohammad Hamad, and Sebastian Steinhorst. A-poa: Anonymous proof of authorization for decentralized identity management. In *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–9, 2021.

[1] `https://niove.eu/`

[7] Anastasia Theodouli, Konstantinos Moschou, Konstantinos Votis, Dimitrios Tzovaras, Jan Lauinger, and Sebastian Steinhorst. Towards a blockchain-based identity and trust management framework for the iov ecosystem. In *2020 Global Internet of Things Summit (GIoTS)*, pages 1–6, 2020.