Automotive Cybersecurity: Challenges and Methodology

Yao Lu, Aaron Benedek, David M. Uze

Trillium Incorporated
3-21-2 Ebisu, Shibuya-ku, Tokyo, Japan, 150-0013

Abstract

Driverless vehicles have gradually become a reality. Security is a major concern in the process. In this white paper, the challenges of automotive cybersecurity are discussed, and security methodology is proposed to meet these challenges.

Keywords: Automotive cybersecurity, HSM, Cryptographic technology, IPS/IDS, OTA

1 Introduction

Nowadays more and more modern vehicles are wirelessly connected to the Internet. Automotive cybersecurity is not just a vague idea but a real threat, to personal and public safety - numerous automotive hacks have been widely published [1,2].

2 Automotive Cybersecurity Challenges

The importance of functional safety cannot be emphasized enough for a vehicle. After years of effort by the automotive community, safety guidelines (such as ISO 26262) are already well established and well supported. Security shares lots of similarities with safety. However, it has its unique aspects. For example, security risks are dynamic by nature, this means the attack strategy will evolve variably with the time available and the development of the attackers capabilities. Safety-related risks are more static. This leads to the conclusion that a completely different principle is required to address security issues. Therefore, there exist many challenges for the automotive industry to overcome.

- **Connectivity Security:** There exist many wired and wireless communication interfaces in a vehicle such as Infotainment, OBD-II, Bluetooth, et al. These interfaces expose the traditionally closed vehicular system, including security vulnerabilities in the vehicle. Hence automotive cybersecurity architectural design must consider the issues of how to isolate, deploy and manage these connectivity interfaces in a secure way.
- **In-Vehicle Network Architecture:** There are 70 electronic control units (ECUs) inside an average a modern vehicle and over 100 ECUs in high-end vehicles. The large majority of ECUs are internally connected by Controller Area Network (CAN). CAN was initially designed for closed vehicular systems. Security was not a consideration in the specification of CAN protocol topology. In past attacks [3], the attackers have successfully controlled the vehicles utilizing the security weaknesses of CAN. Therefore, security mechanisms must be added on to CAN protocol, including careful design for isolation between the safety-critical ECUs and non-safety-critical ECUs, deployment of intrusion detection/protection systems, authentication/encryption of the network traffic, et al.
- **Data Privacy:** With the advances in autonomous vehicle technology, more and more personal information (such as ID, position, biometric information) will be recorded in the vehicle and uploaded to the cloud. It is a challenging task to protect the integrity and confidentiality throughout the data transmission to prevent data from being intercepted or accessed by an unauthorized entity.

3 Automotive Cybersecurity Methodology

Automotive cybersecurity architectural design should be a defense-in-depth system (consensus by many companies [4–6]) that consists of multi-layers: hardware security module (HSM), security software suites and security as a service. Hardware security modules act as roots of trust that protect cryptographic infrastructure. Security software suites run on the top of HSM and security as a service operates between cloud and vehicle. These two software layers form a feedback loop creating a dynamic protection mechanism.

Email addresses: yao.lu@trillium.co.jp (Yao Lu), aaron.benedek@trillium.co.jp (Aaron Benedek), david.uze@trillium.co.jp (David M. Uze).

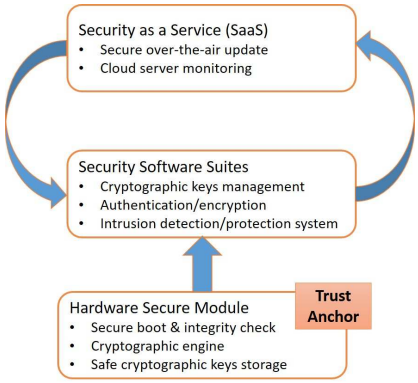

Fig. 1. Multi-layer defense architecture

- **Hardware Security Module (HSM):** HSM provides a hardware-protected security anchor for software layer through hardware encapsulated key generation, key storage, processing of security-critical material and provision of basic security functions. These include:
  - **Secure boot & Integrity check:** Validate the critical OS files by verifying their digital signature and product keys, guarantee the code image is trusted.
  - **Cryptographic engine:** Provide a symmetric cryptographic engine or an asymmetric cryptographic engine depending on the different HSM classes. Fast cryptographic performance in hardware.
  - **Safe cryptographic key storage:** Specifically designed for the protection of the crypto key lifecycle. Store cryptographic keys inside a hardened, tamper-resistant hardware memory.
- **Security Software Suites:** Security software suites are built on top of HSM. They provide a flexible, multi-function and multi-layer solution to secure in-vehicle communication and connected interfaces. Especially considering that there exist many ECUs with different hardware configurations (light HSE/medium HSE/full HSE), a software-based solution is needed to manage the security features of all ECUs. Security software suites include:
  - **Cryptographic keys management:** Including key generation, distribution, storage and revocation. Provide a method to establish the shared key among all the ECUs and the session key generation mechanism.
  - **Authentication/encryption:** Use authentication to verify the integrity and validation of the message, and use encryption to ensure the confidentiality of the message. Provide a secure approach to exchange the messages inside the vehicle.
  - **Intrusion detection/protection system:** Detect for transmission pattern anomalies by checking the behavior (pattern, rule, and destination) of the messages, block inappropriate messages, and alert the system regarding the malicious attempts. Also provides feedback loop for cybersecurity enhancement and updates.
- **Security as a Service (SaaS)** The most difficult part of cybersecurity is that the threats are fluid, evolving as the motivations and capabilities of the attackers change. It is impossible to solve all security issues with a single silver-bullet. Therefore, it is critical to identify and deliver a timely security liberary update to address new vulnerabilities throughout the vehicles entire lifecycle. This suite includes:
  - **Secure over-the-air update:** Secure over-the-air updates to fix vulnerabilities in software components and patch hardware security elements; including the confidentiality of the updates over wireless communication, the verification of the certified source and the integrity of the actual updates.
  - **Cloud server monitoring:** Real-time monitoring, detection and analysis of malicious intrusion of the vehicles without invasion of privacy. Dynamically update the IPS/IDS rule engine based on the big data analysis. Provide secure communication between cloud server and vehicle.

4 Summary

Automotive cybersecurity needs an in-depth, multi-layer solution that should be considered early in both the overall vehicular network architectural and individual ECU design phases.

References

[1] *Hackers Remotely Kill a Jeep on the Highway-With Me in it.* WIRED, July 21, 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[2] *Hackers Take Control of a Moving Teslas Brakes.* WIRED, September 24, 2016. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[3] C. Miller and C. Valasek. *Remote Exploitation of an Unaltered Passenger Vehicle.* August 10, 2015. http://illmatics.com/Remote%20Car%20Hacking.pdf

[4] *White Paper: Automotive Security Best Practices.* Intel Corp. 2016. https://www.mcafee.com/jp/resources/white-papers/wp-automotive-security.pdf

[5] A. Birnie and T. V. Roermund. *White Paper: A Multi-Layer Vehicle Security Framework.* NXP Semiconductors. 2016. http://www.nxp.com/assets/documents/data/en/white-papers/MULTI-LAYER-VEHICLE-SECURITY-WP.pdf

[6] *White Paper: Building Comprehensive Security Into Cars.* Symantec Corp. 2016. https://www.symantec.com/content/en/us/enterprise/other_resources/building-security-into-cars-iot_en-us.pdf