Chapter 8
In-Vehicle Cyber Security

Madhusudan Singh

Abstract Recently, the utilization of electronic control units (ECUs) from the well-being of vehicles to infotainment has been incredibly expanded. Thus, vehicles are progressively advancing as smart vehicles or associated vehicles in the basic mechanical system and self-driving vehicles are relied upon to develop sooner rather than later. This presentation will introduce the in-vehicle review and their security challenges and furthermore conceivable solutions.

Keywords V2V communication · Electronic control unit · In-vehicle cyber security · Information security

8.1 Introduction

The evolution of such a car increases the dependence on information sharing among in-vehicle ECUs, communication within the vehicle, and increases the connection with the outside, resulting in the opening of a new attack surface [1]. In order to defend against this, a strong security solution is required in some form.

C. Miller and C. Valasek recently identified 20 categories of vehicles launched in 2014 and 2015 and identified seven categories of Remote Attack Surface, recognizing the severity of vehicle hacking. The success of vehicle hacking depends on three main categories: Remote Attack Surface, Cyber physical Features, and In-Vehicle Network Architecture [2].

According to Intel, "Security of complex systems such as smart cars requires a collaborative, holistic approach with participation of the supply chain and a wide range of ecosystems, and effective security cannot be achieved by responding to the threats or attacks of individual components, unlike traditional computer systems, it makes it more difficult to protect vehicle systems because they can attack vehicles in both the cyber world and the physical world." From this point of view, security for

M. Singh (✉)
School of Technology Studies, Endicott College of International Studies, Woosong University, Daejeon, Republic of Korea
e-mail: msingh@wsu.ac.kr

M. Singh, *Information Security of Intelligent Vehicles Communication*,
Studies in Computational Intelligence 978,
https://doi.org/10.1007/978-981-16-2217-5_8

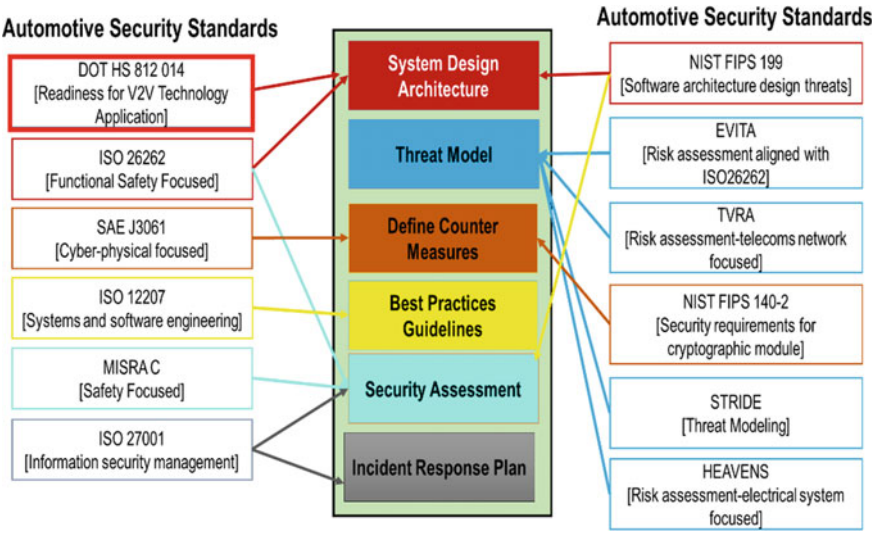

Fig. 8.1 Six Common cyber security practices for automotive technology

vehicle systems needs to refer to the Framework * 1 for the Cyber-Physical System defined by National Institute of Standards and Technology (NIST).

The rest of the chapter is organized as follows. Section 8.2 provides an overview of automotive cyber security practices; Sect. 8.3 introduces requirements of security in-vehicle. Section 8.4 in-vehicle network security. Section 8.5 summarize the in-vehicle security and future research directions.

8.2 Automotive Cyber Security Practices

We have presented in Fig. 8.1. Six common practices related to vehicular cyber security, these practices are defined and described in detail by specific automotive security standards. In Fig. 8.4 has indicated, which standards correlate to what practices. To understand better the existing practices, one must familiarize himself with the standards that guide them [3, 4].

8.3 In-Vehicle Security Requirements

In this part, we are going to discuss about the In-vehicle cyber security requirements. In-vehicle cyber security requirements are based on vehicles connectivity, access, Electronic Control Unit (ECU), Control Area Network (CAN) data platform and communication environment [5]. The security requirements are described in Fig. 8.2.

Fig. 8.2 The security requirements for in-vehicles

8.4 Vehicle Security Requirements Projects

The security for the vehicle system includes Secure Processing for in-vehicle ECU, Secure Network for in-vehicle network, Secure Car Access and Secure Gateway and Secure Interface are required [6]. In Fig. 8.3 has shown the position of security requirements in a vehicle.

Various Vehicle Information Security projects such as Secure Hardware Encryption (SHE), Hardware Security Modules (HSM), E-safety Vehicle Intrusion protected Application (EVITA) are supported by European Transportation Association (ETA) and currently they are active on these projects. These projects focus on eliciting security requirements and security objectives for In-Vehicle Security. The elementary security objective is to meet the in-vehicle security specified goals and objectives

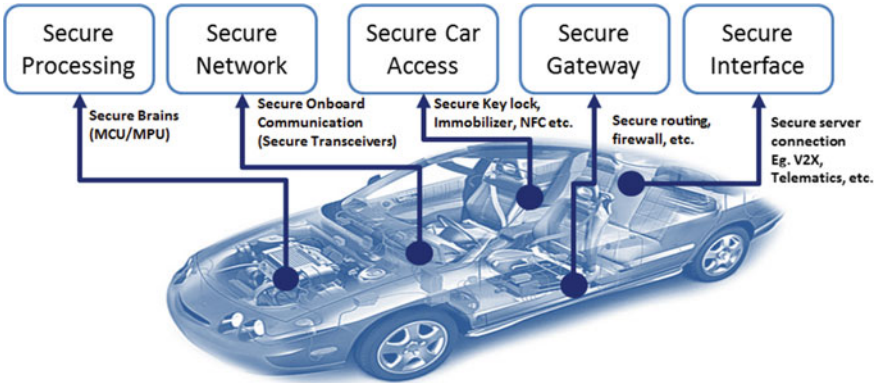

Fig. 8.3 In-vehicle security model

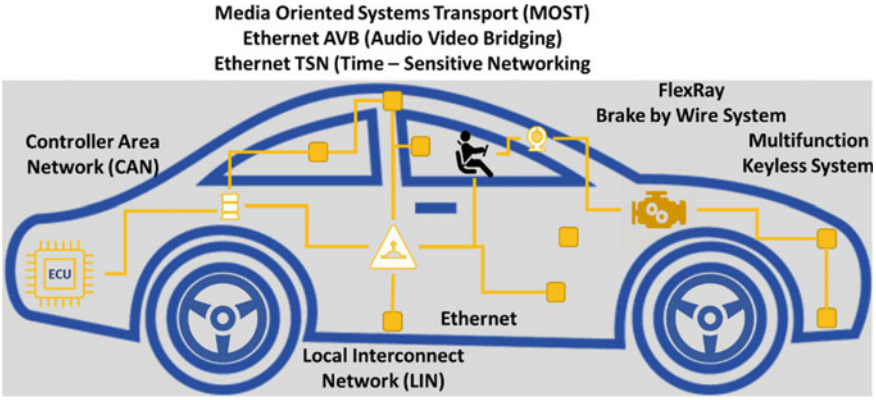

Fig. 8.4 In-vehicle security

while sustaining the functional performance of vehicles development and vehicle's security services.

The key objective of the EVITA projects is to prevent unauthorized access inside the car from adversaries during vehicle communication in the network. It is primary concern to protect any illegitimate modification of the Vehicle application. During vehicle communication, vehicles must disclose the information of operation. In-vehicle security also comprises of protection of intellectual property rights of the vehicle parts, the suppliers, and the developers.

8.5 Isolation and Virtualization

Although various encryption and authentication technologies are used as a defense method for vehicle security, the most basic method is to prevent the internal system and the network from being exposed to the outside. This requires the utilization of a different network between vehicle ECUs that share data, for example, the utilization of a passage that isolates the vehicle's distributed internal system network all things considered. It is likewise important to virtualize the vehicle data so as to forestall direct access to the vehicle ECU for gaining vehicle data from the external network and to forestall change of the vehicle data.

Isolation is formed by grouping vehicle ECUs belonging to the same domain to form a network, connecting the domains to each other through a domain gateway, and connecting the whole network to an external network through a vehicle communication gateway (VCG) [7]. In this regard, it is considered necessary to study the contents necessary for grouping considering the security and function of the vehicle, not the function-oriented domain (chassis domain, body domain, engine domain, etc.). The requirements for security-related functions of the Domain Gateway and the VCG and the criteria for efficiently partitioning each other's roles should also be standardized. For the VCG, ISO TC204 defines the role of the ITS station gateway and the connection between the portable device (Nomadic Device) and ISO TC22 SC31, which deals with the data communication of the road vehicle, in order to establish the VCG standard for sensitive vehicle information access.

Virtualization prevents other devices other than the authorized vehicle ECU from directly accessing specific ECUs and accessing the vehicle information held by the ECUs, and requires a separate secured CPU [8], storage device, and management system for encapsulation Do. Therefore, it is necessary to define the requirements for the definition and management of the virtualized vehicle information architecture, the criteria for classifying the vehicle information to be virtualized, and the communication protocol for the vehicle ECU and the virtualized vehicle information management system need.

8.6 In-Vehicle Network Security

For the in-vehicle Network Security, the data and information are exchanged using the same communication bus. The communication bus utilizes CAN (Controller Area Network), FlexRay, LIN, etc. According to the recent research on Automotive Ethernet, CAN was first developed by BOSCH and later was launched as an international standard for using internal serial communication buses in ISO. CAN message is carried to all the other ECUs linked to the CAN bus in broadcast mode. The ECU is sent in the DATA frame of one message and is authenticated by another message and this authentication is not certified and not supported by an authenticated encryption protocol as there is no DATA field [9] as shown in Fig. 8.4.

8.6.1 Electronic Control Unit [ECU] Protection

Although there are many aspects of vehicle system security requirements, it is necessary to consider safety as a top priority. From this point of view, it is necessary to protect the ECUs inside the vehicle from cyberattacks so that the designed functions and performance can operate properly, we can see in Fig. 8.5.

There are standards for automobile security that incorporate cyber security concepts into existing development processes, standards for vehicle security architecture, and standards for HSM. However, most of them are definitions at higher level, so further research and development is required.

In the case of the current HSM, the built-in encryption and digital signature technologies are suitable modules for current ITS vehicle communication, but the scalability is very weak when the more secure encryption technology is developed in the future. Therefore, it is necessary to develop and standardize the HSM architecture that can be easily updated when security vulnerabilities are detected, considering scalability.

And as more smart cars get smarter, and more connected cars are deployed, cyberattacks on cars will be more exposed to attacks and more vulnerabilities will be discovered. If the existing automobile maintenance procedure is to be countered, it will have a serious effect on the safety of the vehicle. Therefore, it is necessary to develop a method of safely, easily and quickly updating the ECU or the security

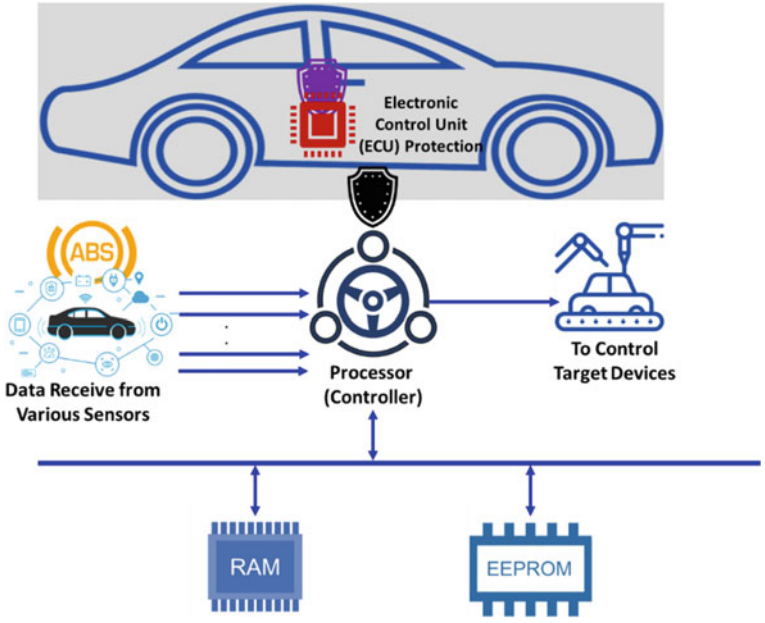

Fig. 8.5 Electronic control unit protection (ECU)

program of the vehicle. OTA (Over the Air) is considered as a solution to this problem. We think that it is necessary to design the ECU architecture that links this with the vehicle security, and to update the security code including the ECU algorithm as well as the ECU firmware.

8.6.2 Hardware Security Component

The hardware security component is fashioned to hand over optimal level of security, service, and performance. The security and performance requirements of signing message and V2X communication verification are satisfied by its highly effective asymmetric encryption engine. Hardware security component consists of Encryption BB (Building Block) where all cryptographic hardware functions are executed. It consists of an Asymmetric Cryptographic Engine (ECC-256-GF(p)), and an AES based hash function known as WHIRLPOOL. It also consists of AES-128 encryption/decryption engine, a pseudo random number, AES-PRNG, a 64 bit monotonically increasing counter and a logic BB that associates EVITA hardware with the ECU application core. An HSM internal CPU is also present to deal with all logics and non-time-critical cryptographic functionality. Further, the hardware security component consists of a 64 KB RAM, 10 KB ROM, a 32 KB non-volatile memory to store keys, security credentials, and counter values and a secure EVITA hardware interface called as HW-API which is used to access all the security functionalities for the software and application CPU.

8.7 Summary

Security in CAN BUS can be achieved by using several authentication protocols and authentication tags such as Message Authentication Codes (MAC). To improve CAN's limitation on the Automotive Vehicle, Automotive Ethernet is being analyzed as an option to the new Network Architecture and also proposed to develop it as a standard in the in ISO TC22 SC31.

Acknowledgements This research was funded by Woosong University Academic Research in 2021.

References

1. J.H. Kim, S.-H. Seo, N.-T. Hai, B.M. Cheon, Y.S. Lee, J.W. Jeon, Gateway framework for in-vehicle networks based on CAN, FlexRay, and Ethernet. IEEE Trans Vehic Technol 64(10) (2010). https://doi.org/10.1109/TVT.2014.2371470
2. D.A. Brown, G. Cooper, I. Gilvarry, A. Ranjan, A. Totourian, R. Venugopalan, D. Wheelerr, M. Zhao, *Automotive Security Best Practices.* White Paper: McAfee Intel Security, US (2015)
3. M. Cheah, S.A. Shaikh, J. Bryans, P. Wooderson, Building an automotive security assurance case using systematic security evaluations. Comput. Secur. **77**, 360–379 (2018). ISSN 0167-4048. https://doi.org/10.1016/j.cose.2018.04.008
4. V. Rajarajan, K. Nedungadi, B. Bhatia, C. Kiernan, A. Ganesan, J. Johnston, L. Gallagher, K. Hodge, T. Martino, C. Rohwer, A. Hayes, A.B. Hall, A. Zimnicks, M. MacMahon, *User Interface for Managing Multiple Network Resources.* US 7689921B2, US Patent (2000)
5. M.A. Rahman, Q. Duan, E. Al-Shaer, Energy efficient navigation management for hybrid electric vehicles on highways, in *Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems (ICCPS'13)* (ACM, New York, USA, 2013), pp. 21–30. https://doi.org/10.1145/2502524.2502528
6. S. Burnett, S. Paine, *RSA Security's Official Guide to Cryptography* (RSA Press Book, McGraw-Hill Publication, 2001). https://doi.org/10.1036/0072192259. https://www.scribd.com/document/325732034/RSA-Security-Official-Guide-to-Cryptography
7. J. Joy, S. Samuel, V.S. Vinu, *White Paper: Gateway Architecture for Secured Connectivity and in Vehicle Communication* (Tata Elxsi, 2015)
8. C. Bernardini, M.R. Asghar, B. Crispo, Security and privacy in vehicular communications: challenges and opportunities. Vehic. Commun. **10**, 13–28 (2017). ISSN 2214-2096. https://doi.org/10.1016/j.vehcom.2017.10.002
9. A. Muneeswaram, Automotive diagnostics communication protocol analysis KWP2000, CAN and UDS. IOSR J. Electron. Commun. Eng. (IoSR-JECE) **10**(1), 20–31 (2015). e-ISSN: 2278-2834, p-ISSN: 2278-8735