Security Analysis of Intelligent Vehicles: Challenges and Scope

Madhusudan Singh
Yonsei Institute of Convergence Technology,
Yonsei University,
Songdo, South Korea
msingh@yonsei.ac.kr

Shiho Kim
Yonsei Institute of Convergence Technology,
Yonsei University,
Songdo, South Korea
shiho@yonsei.ac.kr

***Abstract*— Intelligent Vehicle means vehicles communication with everything such as, in-vehicle, vehicle-to-device, vehicle to vehicle communication, vehicle to roadside unit (RSU), etc. In short, we can say that intelligent vehicle is a system that provides communication environment between vehicles to everything (objects). Due to everything communicating to vehicles, it generates a large amount of data. Data generation is fine with this technology but we need to make sure that these data are safely and securely communicated with their designated destination (right device or users). Privacy of users is another big challenge in intelligent vehicle system. In this article, we discuss the challenges of automotive security in hardware and software, and propose a security architecture for automotive security and also mention future research challenges in automotive cyber security. This paper presents a discussion on Internet oriented application specific secure automotive technology, services, visual aspect and challenges for intelligent vehicles in both academic and industry.**

Keywords—Intelligent Vehicles; Security; Hardware Security; Software Security;

I. Introduction

A. Security Challenges In Intelligent Vehicles

Intelligent Vehicles specially communicate with or with in vehicles in three manners such as In-vehicles communication, vehicle to infrastructure (anything) [1] and vehicle-to-vehicle [2]. Fig. 1 shows security issues in the all three methods of communication viz In-Vehicle (Intelligent Vehicles communications within vehicles), V2X and V2V (Intelligent Vehicles communications with Infrastructure and Vehicles respectively) [3].

Intelligent Vehicle based Automotive Technology has advanced network connectivity in vehicles [4]. The industry has already started manufacturing these advanced vehicles. These are referred to as cyber physical systems [5]. These type of vehicle needs to collect the data from physical environments and cyber systems (Intelligent Vehicle), make decision and execute within physical environment, few examples are Advanced Driver Assistant Systems (ADAS) [6], Advanced Fleet Management, Smart Transportations, Autonomous driving etc [7].

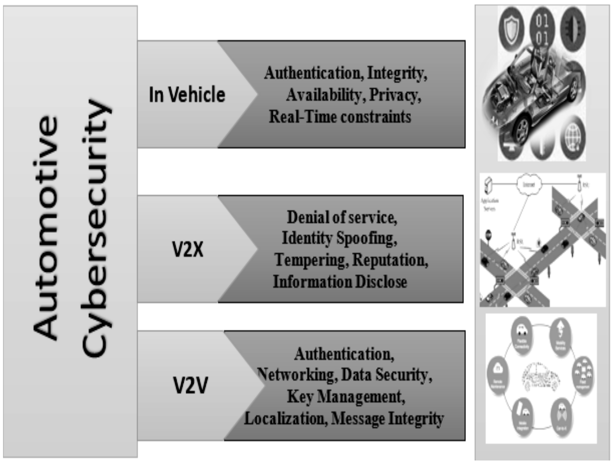
Automotive Cybersecurity
In Vehicle
Authentication, Integrity, Availability, Privacy, Real-Time constraints
V2X
Denial of service, Identity Spoofing, Tempering, Reputation, Information Disclose
V2V
Authentication, Networking, Data Security, Key Management, Localization, Message Integrity

Fig. 1. Security issues in all three automotive communication models

II. Proposed Intelligent Vehicles Security Framework.

Automotive computer security is a collaborative approach to detect, protect, and correct malicious attacks. Intelligent cars have mainly 3 types of security features, first, in-vehicle hardware/ software protection for the electronic control units (ECUs) and control area network (CAN), second, V2V software-based defenses, network monitoring and communication inside and outside of the vehicle, and third, V2X security, which is for the security of data integrity and privacy. In fig. 2, we show the basic security requirement areas in an Intelligent Vehicles.

Intelligent Vehicles security is based on specially two layers, hardware and software security services. Hardware security protects the interior of the vehicles from attackers and ascertain that vehicles hardware such as ECU, CAN etc. are secured from external vulnerability. It also provides fast encryption decryption with cryptographic performance such as immutable device identification, message authentication, and execution isolation. Hardware security is also responsible for secure booting process, secure key data storage and providing trusted execution environment.

Software security increases the security at high level of the hardware such as operating system, firewalls, malware detection, network communication, cryptography activity.

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2017-0-00560, Development of a Blockchain based Secure Decentralized Trust network for intelligent vehicles)

978-1-5386-2285-8/17/$31.00 ©2017 IEEE

Fig.3. illustrates the hardware and software based automotive security architecture.

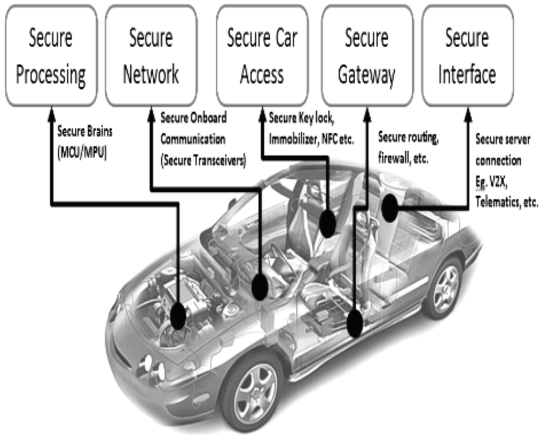
Secure Processing
Secure Network
Secure Car Access
Secure Gateway
Secure Interface
Secure Brains (MCU/MPU)
Secure Onboard Communication (Secure Transceivers)
Secure Key lock, Immobilizer, NFC etc.
Secure routing, firewall, etc.
Secure server connection Eg. V2X, Telematics, etc.

Fig. 2. Basic Security need in Vehicles.

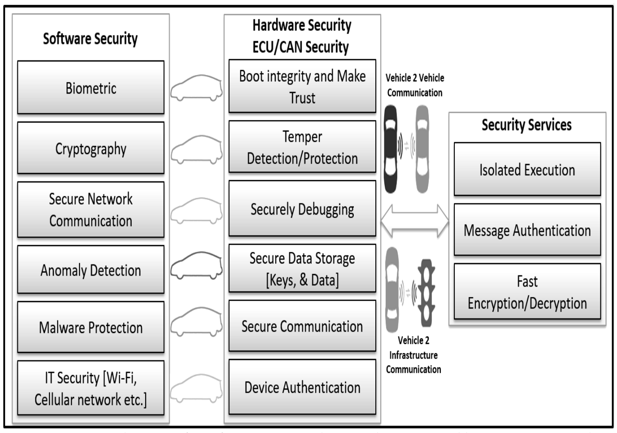
Software Security
Biometric
Cryptography
Secure Network Communication
Anomaly Detection
Malware Protection
IT Security [Wi-Fi, Cellular network etc.]
Hardware Security ECU/CAN Security
Boot integrity and Make Trust
Temper Detection/Protection
Securely Debugging
Secure Data Storage [Keys, & Data]
Secure Communication
Device Authentication
Vehicle 2 Vehicle Communication
Vehicle 2 Infrastructure Communication
Security Services
Isolated Execution
Message Authentication
Fast Encryption/Decryption

Fig. 3. Hardware/Software based intelligent Vehicles Security Architecture

III. Research Challenges and Opportunities

In this article, we consider security issues for intelligent vehicles. We concentrate our topic near hardware and software security issues in vehicles and mention the basic security architecture for intelligent vehicles hardware and software points. Still, intelligent vehicles have various issues, which are not discussed in this paper. Below, we have defined possible future security issues related to intelligent vehicles.

- Providing security in every small sensor.
- Providing security between ECU to ECU.
- Providing secure data.
- Provide security for communication (Routing) betweenV2V, V2X etc.
- Provide secure user information.
- Provide security for data integrity, safety and security during communication between V2V or V2X or In-Vehicle.

There are many others research challenges available in intelligent vehicle security. In future, cars will be equipped with much more advanced technology so security challenges will always be there according to their updation.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2017-0-00560, Development of a Blockchain based Secure Decentralized Trust network for intelligent vehicles)

References

[1] White Paper, “The Internet of Things: Reduce Security Risks with Automated Policies”, Cisco, 2015.

[2] White Paper, “Automotive Security Best Practices Recommendations for Security and Privacy in the era of the next-generation Car”, McAfee Part of Intel Security. 2015.

[3] Singh, Irish, et al. "A novel privacy and security framework for the cloud network services,” 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), IEEE, 2015, pp.301-305.

[4] Su-Hyun Kim and Im-Yeong Lee, “A Secure and Efficient Vehicle-to-Vehicle Communication Scheme using Bloom Filter in VANETs”, International Journal of Security and Its Applications Vol.8, No.2 (2014), pp.9-24.

[5] Vinh Hoa LA, Ana Cavalli, “Security Attacks and Solutions, in Vehicular Ad-hoc, Networks: A Survey”, International Journal on Ad-Hoc Networking Systems (IJANS) Vol. 4, No. 2, pp. 1-20, April 2014.

[6] Technical White Paper, “Automotive Cyber Security: An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles”, The Institution of Engineering and technology (IET), June 2015.

[7] Qi Jing, Athanasios V. V., Jiafu Wan, Jingwei Lu, Dechao Qiu, “Security of the Internet of Things: perspectives and challenges”, Wireless Networks, Springer , june 2014.