Analysis on Attack Scenarios and Countermeasures for Self-driving Car and Its Infrastructures

Dohyun Lim[1], Kitaek Park[1], Dongjun Choi[1], Jungtaek Seo[1] *
1 Department of Information Security Engineering, Soonchunhyang University, Korea
lingdoz@gmail.com, ir0nykt@gmail.com, zzczzc123@naver.com,
sjtgood7@gmail.com

Abstract. Autonomous vehicles collect and process information required for driving autonomously and apply the processed result for vehicle driving thereby driving vehicles automatically by identifying road situations without additional control of brakes, handling, and acceleration pedal by drivers. Since self-driving cars collect information from various sensors and communication is done between various sensors and devices over the infrastructure, they are vulnerable to unexpected accidents due to malicious hacking attacks if self-driving cars are commercialized without ensuring security technologies and establishment of security systems. In particular, securing safety is highly emphasized due to automobile technology that is directly related to human lives and safety. In the present paper, security threats against self-driving cars and infrastructures are analyzed and possible attack scenarios are developed to predict the impact. Furthermore, the current status on research and development of security technology is analyzed and items of technology development to ensure cyber security of self-driving cars and infrastructures as well as R&D strategies are presented for future research.

1 Introduction

The automobile industry has been evolved rapidly into self-driving cars where the state of the art technologies are concentrated. According to Navigant Research, a market scale of self-driving car system in the world will reach $189 billion by 2020 and $1,152 billion by 2035, which indicates that the era of self-driving car and technology are emerging [1]. To keep pace with the global interest, South Korea disclosed a goal of commercialization of self-driving cars at Level 3 by 2020 [2]. The number of deaths by vehicle accidents around the world amounts to 1,240,000 annually and 90% of the deaths are due to driver's faults such as driving while drowsy or drinking driving, which emphasizes the importance of autonomous driving technology positively more and more [1]. However, much attention has also been paid to risk of accidents due to malicious hacking attacks in contrast with the positive prospect on self-driving cars. If autonomous driving technology is commercialized

L. Barolli et al. (eds.), *Advances on Broad-Band Wireless Computing, Communication and Applications*, Lecture Notes on Data Engineering and Communications Technologies 2, DOI 10.1007/978-3-319-49106-6_42

without ensuring establishing security systems and techniques, unpredictable accidents due to malicious hacking attacks can occur and enormous disruption on the network can occur during cyber-attacks on V2X. Autonomous driving needs mutual information collection through sensors in order to support V2X (InV: In Vehicle, V2V: Vehicle to Vehicle, V2I: Vehicle to Infrastructure) communication and Advanced Driver Assistance Systems (ADAS). First, it is important to collect correct information through sensors and communicate collected information securely between Electronic Control Units (ECU) over the InV communication environment. If sensors that support the ADAS do not collect correct information or if fabrication and modification of collected information occurs during communication between ECUs to employ the collected information, normal operation of autonomous driving systems cannot be achieved [3]. Second, since V2V and V2I communication environments are Wireless Local Area Network (WLAN) environments that use Wireless Access in Vehicle Environments(WAVE), the communication environments are vulnerable to attacks such as spoofing, Denial of Services (DoS), and Man In The Middle Attack (MITM). Thus, it is essential to secure the security of communication in V2V and V2I, as well as a gateway to server. Accordingly, vulnerability of V2X and autonomous driving technologies and factors of security threat are needed to be analyzed clearly and it is necessary to ensure cyber security over the autonomous driving system in preparation of malicious hacking attacks against autonomous driving systems in the future [4]. To provide a countermeasure, it is essential to analyze possible attack scenarios and impact effect on autonomous driving technology. Thus, this paper investigates the current status of technological development on self-driving cars and infrastructure in Section 2 and presents security threats against autonomous driving technology in Section 3. In Section 4, development and analysis on the countermeasure technology are presented focusing on possible attack scenarios and impact. In Section 5, the current status of development on national and international countermeasure technologies against related attacks is discussed. In Section 6, items of technological development and R&D strategies are presented to secure self-driving cars and cyber security over the infrastructure of self-driving cars in the future and in Section 7, conclusions of the present paper including future research are presented.

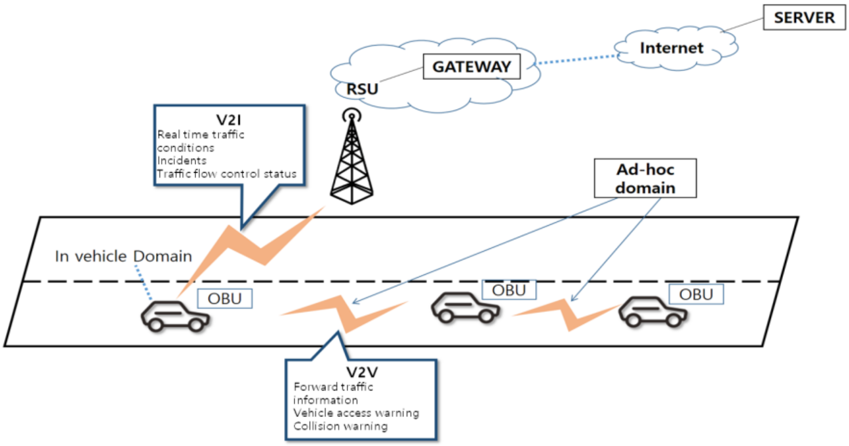

Fig. 1. Conceptual diagram of the self-driving its Infrastrucrue

2 Current status of self-driving cars and infrastructure

2.1 Current status of technological development in South Korea

2.1.1 Current status of technological development in self-driving cars

Hyundai and Kia Motors in South Korea demonstrated the first self-driving car called "Tucson IX" in 2010. Tucson IX demonstrated autonomous driving over nine missions consisting of paved and non-paved roads of 4 km including checkpoints, cross-road and accident-prone location successfully and "Genesis Smart Sense (GSS)", which was a Highway Driving Assist (HDA) system, was launched in the name of Genesis EQ900 in December 2015. The GSS can detect accident occurrence in advance through driving assist technology to help drivers to drive safely and comfortably. Based on the above technologies, the GSS acquired license of autonomous driving in the highway in Nevada State in the USA and accelerated the commercialization of self-driving cars [5].

2.1.2 Cooperative driving technology

As Cooperative Adaptive Cruise Control (CACC) and Automated Queue Assistance (AQA) technologies are developed around the world, the standardization has been underway in South Korea as well. The Telecommunications Technology Association in Korea proposed TTAK.KO-06.0379, which was a message standard at the application level for formation and separation of vehicle platooning during automated queue assist driving. The message standard was made basically by referring the J2735 BSM message proposed by the Federation Internationale de l'Automobile in the USA.

2.2 Current status of technological development in the USA

Vehicles of Ford Motor Company have been equipped with lane keeping system and active park assist in addition to semi-self-driving cars, which are currently commercialized by the CES and research is underway to provide traffic jam assist function for reduction in traffic jam by adjusting a distance between vehicles automatically. Furthermore, the company is now developing universal service including infotainment and vehicle theft prevention system in collaboration with Intel Company [7].

The USA has also started Intelligent Transport System (ITS) related projects as a measure to resolve traffic delay and congestion as well as traffic accidents such as deviation from the lane. Starting from Vehicle Infrastructure Integration (VII) in 2003, the USA changed the VII project into Connected Vehicle project in 2011 to achieve commercialization of Cooperative-ITS(C-ITS) and accelerated R&D on the effect and issue of the connected vehicle technology and commercialization. In the "Safety Pilot" among the project tasks, road tests about various C-ITS services were conducted including interconnection technology test between vehicles over the real driving environment [8].

2.3 Current status of technological development in Europe

The research in Europe has focused on core technology, road safety, and road operation. First, it developed Cooperative Vehicle-Infrastructure Systems (CVIS) from the management viewpoint such as traffic management in cities and open standard-based communication between V2V and V2I for the purpose of traffic stability and efficiency. Second, it developed the safety system (SAFESPOT) that can detect dangerous situations in the road in advance. Finally, it conducted a project for efficient road operation by providing real-time information of specific regions through implementation of two-way wireless communication environment [9].

3 Security threats against self-driving cars and infrastructure

3.1 Security threats against self-driving cars

3.1.1 Physical vulnerability

The Communication Control Unit (CCU) is a unit that can manage multimedia systems inside vehicles by enabling communication with external devices via cellular networks. Since the CCU is not directly connected to the Control Area Network (CAN) bus and an air gap is present between connection and physical parts, communication can be done with other connected components if V850 controller is used thereby being able to control the CAN bus by sending commands through reprogramming.

3.1.2 Encryption and authentication

Since the CAN protocol is suitable to networks for vehicles where real-time property is important, it has been used as a standard for most vehicles among various vehicle control protocols. It is implemented via internal network of various types of vehicles. It does not provide encryption and authentication features although it is a broadcasting communication protocol. In 2010, a research team led by K. Koscher attempted a hacking test using real vehicles and pointed out the problem of internal network in vehicles to show that vehicles can be controlled via replay attack of messages [10].

3.1.3 Access control

The ODB-II port is used to diagnose failure of engines and maintenance of vehicles. Attackers can access the CAN bus by connecting to the ODB-II port and replay attack or DoS attack can be done through packet analysis.

3.2 Security threats against self-driving car infrastructure

3.2.1 Network scale

When vehicles with different specifications and vehicle purpose are driving in the same road in the same region, interference between sensors mounted at different vehicle models, electromagnetic interference occurred at vehicles, and disruption of networks for vehicles can occur.

3.2.2 Operation of devices and systems

A path where attackers can penetrate into infrastructures of self-driving cars can be found due to inappropriate security setup, use of unauthorized mobile storage media, and inappropriate security audit in terms of operation and management of devices and system.

3.2.3 Denial of Service

Attackers can execute an attack of DoS against networks such as the Road Side Unit (RSU) via generation of a large amount of traffic, attempts of multiple accesses, and vulnerabilities to paralyze the traffic control center.

4 Possible attack scenarios and analysis on the impact

4.1 Intrusion scenarios through networks

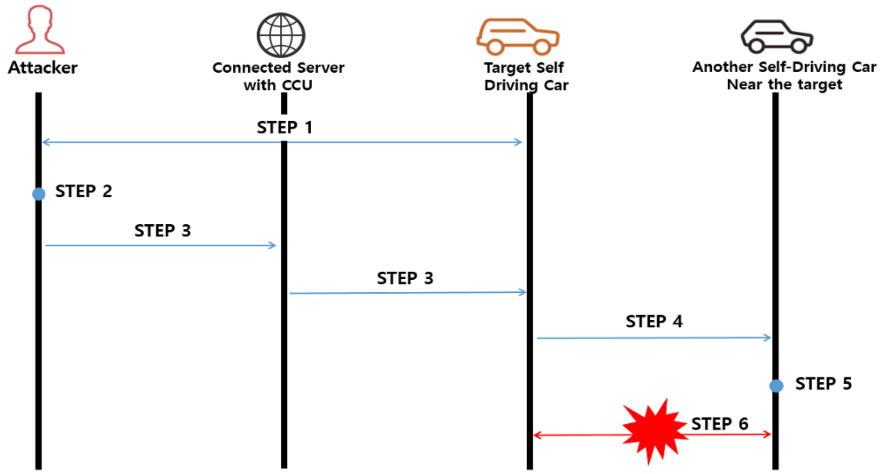

Fig. 2. Attacks on internal communication basis of vehicles

*Precondition 1: Encryption communication is not done in the inside of the CAN bus.
*Precondition 2: There is a vulnerability inside the CCU communication server.

Step 1. Attacker choose a target self-driving car and secures the IP information of the CCU system connected to the Internet through cellular networks.
Step 2. Security vulnerabilities are identified through Internet scanning and remote executable code is developed.
Step 3. The CAN bus communication is analyzed and then manipulation packets related to vehicle driving information is fabricated thereby sending the information through remote executable code.
Step 4. The target self-driving car recognizes the current car speed and acceleration as modified values, and sends Vehicle Safety Communications (VSC) message
Step 5. Another self-driving car that received the VSC message from the infected vehicle recognizes speed and acceleration of the infected self-driving car as modified values.
Step 6. Car collision is induced through re-adjustment of vehicle distance based on the modified value.

Attacker secures the IP address by which the CCU system is connected to the external cellular network and then security vulnerability is investigated through port scanning on the corresponding IP. Based on the identified vulnerability, attacker configures a backdoor to send remote executable command to the CAN bus and produce a manipulation packet related to vehicle driving information in order to send the modified packet through the backdoor. The modified packet is broadcasted through the CAN bus thereby letting the target vehicle recognize the modified driving information as normal value. Here, the modified driving information is included in the VSC that is sent between self-driving cars in real time prior to broadcasting and adjacent self-driving car receives the corresponding information. The adjacent self-driving car performs re-adjustment of vehicle distance via the modified received information, which can be followed by collision or multiple car crashes.

4.2 Intrusion scenarios through physical access

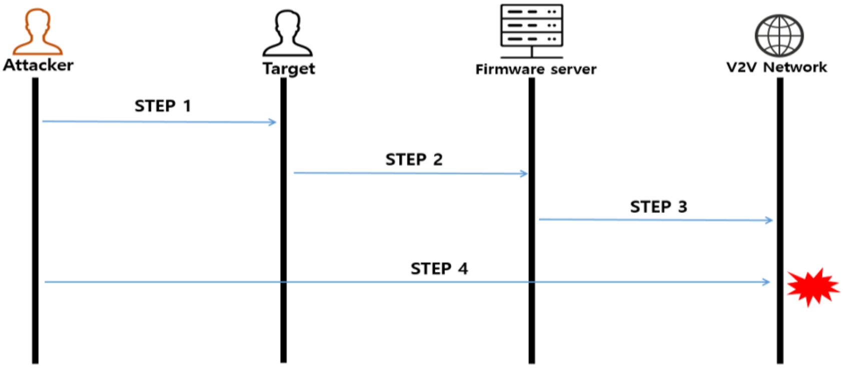

Fig. 3. Attack through firmware update

*Precondition: Penetration process into local networks is not considered.

Step 1. Malicious code is infected through spear phishing or USB thereby inducing malicious behavior desired by attacker.
Step 2. Firmware server manager opens emails or inserts infected USB thereby infecting the firmware server with malicious code.
Step 3. Attacker overwrites the correct firmware with malicious firmware and vehicles updated with malicious firmware are all infected.
Step 4. Vehicles can experience damage due to out-of-control and chain collision according to the command by attacker.

Attacker performs Advanced Persistent Threat (APT) against firmware server in the infrastructure thereby overwriting the update server with malicious firmware. When vehicles update firmware from the update server, those vehicles are infected with malicious code thereby experiencing out of control or vehicle accidents resulting in a large scale of casualties.

4.3 IoT control attack scenario in the home network using V2I communication spoofing

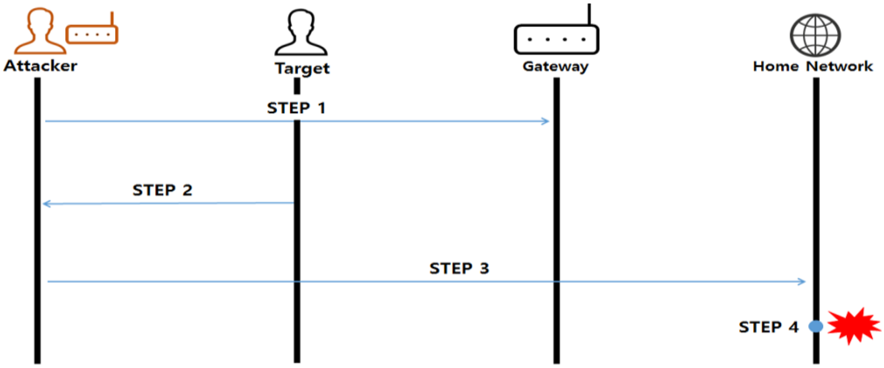

Fig. 4. IoT control in the home network using V2I communication spoofing

*Precondition: Internal authentication and connection of Internet of Things (IoT) in the home network can be done through vehicle and gateway communication data.

Step 1. Self-driving car is camouflaged as gateway through spoofing in the ad-hoc network. The ad-hoc network is characterized by no Access Point (AP) so if communication is needed externally inside the Network Address Translation (NAT), a single node is used as AP to communicate externally.
Here, ARP spoofing is conducted by attacker to be disguised as if attacker were a gateway.
Step 2. Attacker collects information about victim vehicle while being disguised as a gateway. Data by which home network can be connected are extracted from data transferred from victim vehicle to gateway.
Step 3. Through the collected information, home network is connected. Through the collected information, home network is connected and electronic appliances such as gas range, lights, air-conditioning, and personal computer can be controlled.

Step 4. Through the control of electronic appliances, financial damage, privacy information leakage, excessive electric bill charge and fire due to overheating, privacy information leakage through remote connection to PC can occur.

The communication between self-driving car and infrastructure can be done via the Vehicle Ad-hoc Network (VANET). If attacker is within the same network, he/she scans neighbor IPs and selects a victim vehicle thereby spoofing security message containing location, acceleration, and current speed that are transferred to the gateway by victim vehicle after sending its own MAC address. By ARP spoofing the gateway connected to the self-driving car, attacker becomes a gateway and extracts data by which home network can be connected through data sent by victim vehicle. Later, attacker is connected to home network through information extracted by connecting to the external Internet network and controls electronic appliances at home remotely.

4.4 V2V communication paralysis through OCSP server attack at infrastructure data transmission and reception environments

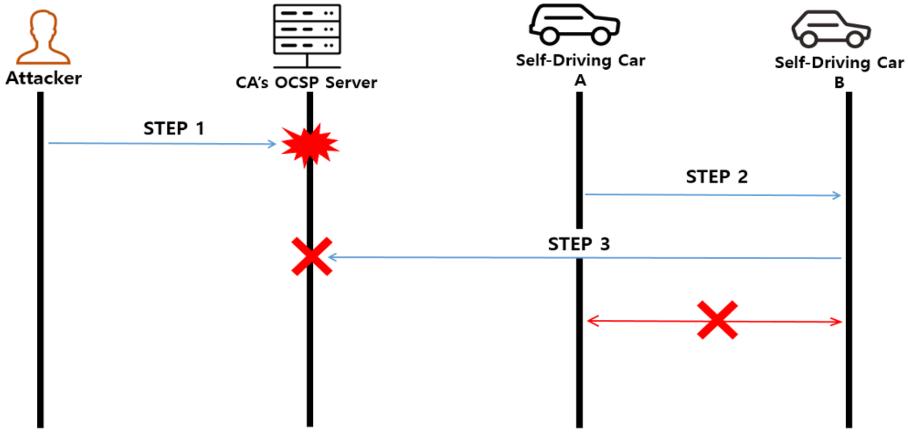

Fig. 5. OCSP server attack over infrastructure data transmission and reception environment

*Precondition 1: Certificate-based authentication environment is already constructed.
*Precondition 2: Attacker has information about Online Certificate Status Protocol (OCSP) server and access path was already acquired.

Step 1. Attacker disables services of OCSP server via various attacks.
Step 2. Self-driving car A signs in data that are transmitted to self-driving car B with private key included in the certificate embedded at the time of manufacture or issued via the Certificate Authority (CA) previously prior to transmission of data.
Step 3. In order to verify data signature received from self-driving car A, a request of validity verification is sent to the OCSP server.
Step 4. Since the OCSP server becomes disabled service status in ***Step 1,*** validity verification cannot be done.

Attacker attempts Distributed Denial of Service (D-DoS) attack through infection of OCSP client application services via malicious code or infection of USB of administrator through spear phishing against OCSP manager to infect OCSP server during maintenance resulting in making services disabled. Accordingly, it is impossible to verify signatures included in data such as accident information during driving and location information that are transferred via V2V communication. Furthermore, certificate is applied not only to self-driving car but also to the RSU thereby making authentication impossible at overall self-driving car environments. Since authentication is not possible, road traffic paralysis or human casualties upon attacking during driving could occur.

4.5 Scenario of communication jamming attack inside V2V environments

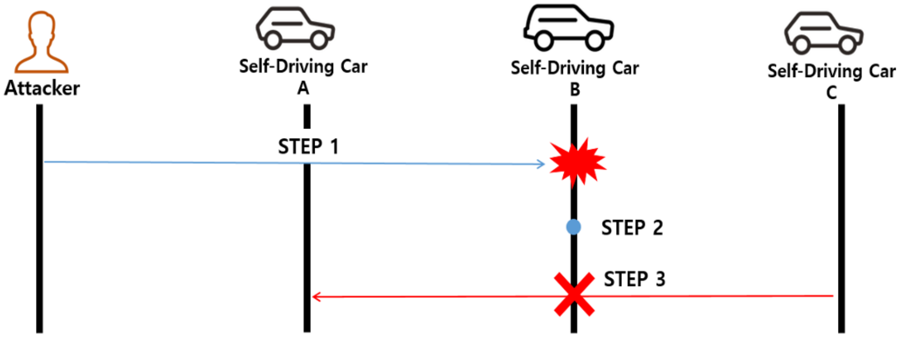

Fig. 6. OCSP server attack over infrastructure data transmission and reception environment

*Precondition: Attacker acquires access right to the CAN network.

Step 1. Attacker gains control of the CAN network inside the target vehicle thereby acquiring access right of the routing table.
Step 2. Attacker changes the routing protocol intentionally.
Step 3. Attacker drops safety message transmitted to surrounding vehicles thereby interrupting the movement to the destination node.

Once attacker gains control of the CAN network inside the target vehicle and acquires access right of the routing table, he/she can control the routing protocol directly. A self-driving car needs control of parameters such as speed by determining situations of surrounding vehicles. Here, messages are exchanged between surrounding vehicles, which are safety messages. If safety message is dropped, it can affect Packet Delivery Rate (PDR) between V2V commun ications and surrounding vehicles can have communication jamming thereby unable to recognize a distance between vehicles at high speed driving situation, resulting in vulnerable human casualties.

4.6 Scenario of vehicle control attack using control App of self-driving car

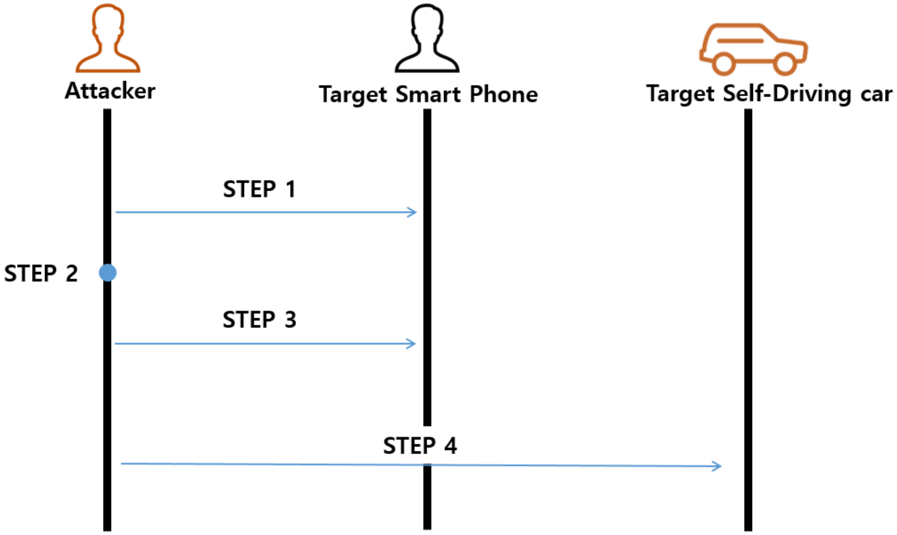

Fig. 7. Vehicle control using control App of self-driving car

*Precondition: Nonce values between message transmission and reception are not applied.

Step 1. A target smartphone is infected by malicious code through SMS phising letters sent by attacker thereby forcing rooting of the smartphone.
Step 2. Attacker acquires root right of the smartphone infected by malicious code thereby installing a rootkit.
Step 3. Attacker monitors control App packet of self-driving car using the rootkit.
Step 4. Based on the acquired information, replay attack is done to steal the vehicle.

A target smartphone is induced to be infected by malicious code through SMS phishing letters sent by attacker. Then, attacker acquires root right and installs a rootkit thereby monitoring control App packets using network packet monitoring tool. After this, attacker retransmits packets through replay attack to steal the vehicle.

5 Current status of countermeasure technology development

5.1 Privacy protective authentication technology

The Electronics and Telecommunications Research Institute in South Korea (ETRI) utilized zero-knowledge proof and encryption techniques for digital signature generation, validation, signature verification, and connection algorithm design. The privacy protective authentication technology can prevent possibility that can easily track driving information of specific vehicle by attacker if no privacy protective measure is provided in vehicle communication. The techniques can be utilized as advanced information exposure control method because it can prove knowledge, right, and qualification justification only without exposure of detailed identification information of users [11].

5.2 Security technology of V2X service integration for self-driving cars

The government in South Korea started a project called “security technology development for V2X service integration for self-driving cars”, which was launched in early 2016. In the above vehicular project, Public Key Infrastructure (PKI) for vehicle privacy and information protection and reliability guarantee technology of V2V and V2I communication service for infrastructure technology and self-driving cars, V2N security technology for prevention of hacking remotely and introduction of malicious code against vehicles, and development of remote security update technology for vehicles are performed. Furthermore, it also performs international standardization of security technology for self-driving cars and applicability test and verification of security technology at self-driving environments [12].

5.3 ProtectivX technology

ProtectivX which is a platform for self-driving cars and now under development by Intel and BMW is a platform technology to prevent unauthorized accesses to information systems and IoT networks. The development is now underway to monitor all ECUs that have suspicious activities while residing in the CAN bus inside vehicles. It aims to protect the CAN bus from scan and external threats continuously such as ECU infotainment system, vision safety device, cruise control, electronic key, and remote engine starter [13].

5.4 PRESERVE technology

The PRESERVE technology was designed to prevent the abuse and infringement of privacy information during V2X communication as it summarized projects such as SEVECOM, EVITA, OVERSEE, and PRECISA as shown in Fig. 8 and included other security requirements to complete security and universal applicability tests. This technology is now at the pre-distribution stage after strengthening scalability and reducing the cost more than the previous project [14].

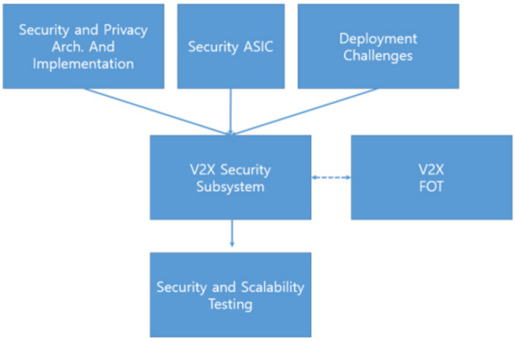
Security and Privacy Arch. And Implementation
Security ASIC
Deployment Challenges
V2X Security Subsystem
V2X FOT
Security and Scalability Testing

Fig. 8. Configuration of PRESERVE

6 Direction and strategy of future technological development

6.1 Implementation of certificate-based certification system

Certification is essential between self-driving car and infrastructure system. For certification between self-driving car and infrastructure, certificate and digital signature issued from the CA can be used. However, identification information is contained in certificate so that moving trajectory and driving time of vehicle can be identified. That is, there is an infringement on privacy information about vehicle location. Thus, it is necessary to have a certification method to protect privacy information that employs anonymous certificates that can replace identification information included in the certificate with non-identifiable anonymous value. Furthermore, it is also necessary to consider a method that requires certification only for a specific section when a vehicle enters that section.

6.2 IDS/IPS embedded with aulighthentication and lightweight encryption algorithm

The CAN bus employs a broadcasting mode that supports data communication in real time inside vehicles but it does not design and implement certification and encryption functions with respect to transmission messages. Thus, it is necessary for the CAN bus to apply certification and lightweight encryption in order to prevent hacking attacks such as packet sniffing or command injection. It is also necessary to apply detection method of white-list mode against hacking attacks that can occur inside vehicles and develop and apply Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) in order to provide real time detection and response by setting a threshold of data value.

6.3 Ultra-lightweight hardware security module for key management and internal encryption operation

The Hardware Security Module (HSM) is not only used in integrity protection of ECU firmware but also in secure flashing, secure boot, run-time tuning detection, and secure debug. However, it requires encryption operation process mandatorily and includes data exchange in real time. Thus, it is necessary for the HSM to include ultra-lightweight and high performance module to provide required functions while maintaining real-time requirements.

6.4 Detection and recovery against ECU security threat

The CAN bus does not provide inter-certification between ECUs so it is vulnerable to spoofing attack. Attackers can broadcast forged or modified packets easily through spoofing attack. Therefore, it is necessary for the CAN controller to overwrite an error frame to the message to notice abnormal ECU to monitoring nodes when the CAN controller detects a spoofing message as a monitoring system to validate integrity of packets. In addition, when abnormal messages are detected through monitoring, it is necessary to perform detection and recovery in real time by combining recovery development technology that can restore information state of ECUs stored in the recovery partition back to the “initial information state”.

6.5 Construction of security testbed

It is necessary for self-driving cars to have an environment where real self-driving car and infrastructures are analyzed with respect to impact and effect scope during accident occurrence as well as security compliance verification and validation inspection, and develop tools that can discover vulnerabilities of components of self-driving cars and environments that can verify vulnerability through simulation hacking and analysis on security vulnerability of service infrastructures and devices. Therefore, a testbed shall be constructed to test various security functions and diagnose possible hacking attacks in advance to complement the system.

7 Conclusion and future research

In recent years, technologies of autonomous driving systems have strived for perfection. Most automobile companies aim to commercialize and run self-driving cars on the road by 2020. For commercialization, sensor parts which play a role as eyes in humans have been advanced continuously. Nonetheless, much attention has been paid to hacking issues in self-driving cars so security has become the main subject. Compared to explosive growth in technologies and industries related to self-driving cars, security system and security technology that support self-driving cars have been fallen behind. Accordingly, various technologies such as security technology development, security standardization, privacy protective certification technology development, hardware-based high-speed encryption module development have been applied to V2X communication around the world.

In the present paper, security threats against self-driving cars and infrastructures were analyzed and possible attack scenarios were developed to predict the impact. Furthermore, a method of R&D on security technology was also provided to ensure cyber security.

For the future research, experiments will be conducted with regard to possible attack scenarios and required security technologies will be studied and developed.

Acknowledgments. This research was supported by the Research Program through the National Security Research (NSR) Institute of Korea. (#2016-038)

References

1. Collaboration of Related Ministries, Support Measures for Commercialization Self-driving Cars, Ministry of Land, Infrastructure and Transport (2015)
2. Lee, Jeonghoon; Kim, Hyunyong, Electricity flows in car. The Collaboration, eBEST INVESTMENT SECURITIES Co., Ltd (2015)
3. Korea communications Agency, Current trend of technologies and prospects of security technology for vehicle communication used in intelligent road systems No. 59 (2014)
4. Shin, Younoh, Precision Map, V2X Self-driving car without road infrastructure, Can it be run well? e4ds News (2016)
5. Hyundai Motor Company, Press release of the current trend on technological development of self-driving cars (2016)
6. Oh, Hyunseo, Technological trend of cooperative driving via V2X communication ETRI (2015) 33-36
7. Kim, Sangguk, Autonomous driving functional systems, Industrial Information Analysis Department (2015)
8. Policy Research Center, V2X communication, Rising core technology for intelligent traffic system, Trend Focus (2014) 45-46
9. Ministry of Land, Infrastructure and Transport, Report on the current trend of standardization on ITS in overseas Vol. 2(2014)
10. Lee, Donghoon, Technology fusion of vehicle and ICT and current trend of security technology, TTA Journal. Vol. 153 (2014)
11. Sohn, Gyungho, ETRI Privacy technology, ISO standard adoption, ZDNet Korea (2013)
12. Lee, Yuji, Launching of technology development for V2X integrated security for safe autonomous driving era, BYLINE NETWORK (2016)
13. Idan, E.: ProtectivX Hacker Detection System Helps Reduce the Threat of a Collision Caused by Hackers. PR Newswire (2016)
14. Norbert, B., Sebastian, M., Jonathan P., Mirko, L., Martin, M., Daniel, E., Michel, S., Michael, F., Rim, M., Marcello, L., Frank, K.:V2X Security Architecture V2. Vol. 1. PERSERVE (2014)