Standardization Issues on Secure Vehicular Communication

SANG-WOO LEE, HYUK-CHAN KWON, JUNG-CHAN NA
Information Security Department
Electronics and Telecommunications Research Institute
218 Gajeongno Yuseong-gu Daejeon
SOUTH KOREA
ttomlee@etri.re.kr, hckwon@etri.re.kr, njc@etri.re.kr

Abstract: - Connected vehicles are considered as the key enabling technology in Intelligent Transportation System (ITS) environment. However, connected vehicles without security function can make ITS applications vulnerable to various security threats. Recently, many standard organizations are working on making international standard related with vehicular communication security. This paper presents state of the art of standardization on ITS security and issues being considered by standard development organizations. In particular, this paper elaborates standardization activity and security consideration in ITU-T Security Group.

Key-Words: Vehicular communication security, ITS security, Standardization, V2X communication security

1 Introduction

Significant developments have taken place over the past few years in the area of autonomous driving technology. Autonomous driving technology can consist of sensor technology such as radar, artificial intelligence to control the vehicle itself, and vehicular communication technology. In particular, in order to overcome limitation of sensors, vehicular communication technology is necessarily required. In addition, vehicular communication allows the vehicle to understand the status of neighboring vehicles and to receive useful traffic information from infrastructure including Road-Side Units (RSUs). However, security function should be guaranteed in order to utilize vehicular communication since the vulnerability of the vehicle is directly related to life of a driver and a pedestrian. Furthermore, the vulnerability of a vehicle can be propagated to the other vehicles since the vehicular communication is an ad-hoc type network.

Nowadays, many standard organizations are working on developing international standard related with vehicular communication security. This paper presents current standardization issues on vehicular communication security being considered by standard development organizations (SDOs).

2 Vehicular Communication Security Standardization

ITS security standardization is being progressed in several SDOs such as IEEE, ETSI, ISO and ITU [1, 2, 3, 4, and 5]. ISO has specified ITS standard in terms of Communications access for land mobiles (CALM) [3]. In particular, this paper reviews the standardization issues at IEEE and ITU-T SG17.

2.1 IEEE 1609

5.9 GHz Dedicated Short Range Communications for Wireless Access in Vehicular Environments (WAVE) has been specified by the IEEE P1609 working group. This communication technology enables vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. WAVE provides a communication protocol stack that is suitable for the vehicular environment as shown in Figure 1. WAVE supports both IP and non–IP based data transfers. Non–IP-based data transfers are supported through the WAVE Short Message Protocol (WSMP) specified in IEEE Std 1609.3. WAVE uses IEEE 801.11p as a PHY layer. Medium access control (MAC), WAVE Management Entity (WME) and corresponding network services are specified in IEEE Std 1609.3. WAVE Security Services are specified in IEEE Std 1609.2.

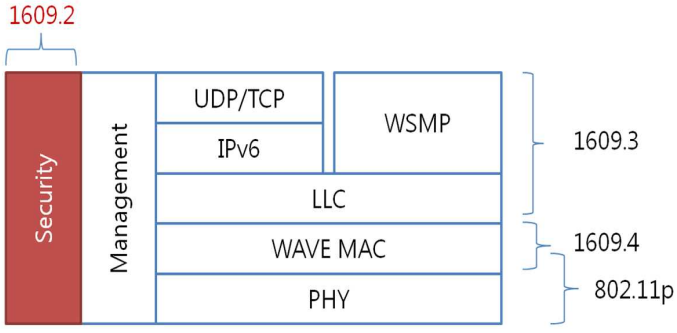

Fig. 1. WAVE reference model.

Table 1. WAVE specifications.

Title	Spec.	Status
IEEE 1609.0-2013	Guide for WAVE - Architecture	Ver.1, 2014
IEEE 1609.2-2013	Security Services for Applications and Management Messages	Ver. 3, 2016
IEEE 1609.3-2016	Networking Services	Ver. 3, 2016
IEEE 1609.4-2016	Multi-Channel Operation	Ver. 3, 2016
IEEE 1609.6	Remote Management Service	Under development
IEEE 1609.11-2010	Over- the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS)	Ver. 1, 2011
IEEE 1609.12-2016	Identifier Allocations	Ver. 2, 2016

In comparison with conventional wireless LAN, IEEE 802.11p specifies narrow channel bandwidth (10MHz) and high RF output, which is maximum 44.8dBm, in order to be suitable for vehicular communication.

In addition, IEEE 802.11p specifies compact initialization procedure which means that it removes initial authentication procedure in order to fast connection.

- IEEE 1609.0-2013 describes WAVE architecture and services necessary for multi-channel devices to communicate in a vehicular environment.
- IEEE 1609.2-2016 specifies secure message formats, the processing of those secure messages, and methods for securing WAVE management messages and application messages.
- IEEE 1609.3-2016 describes transport layer which supports addressing and routing mechanism. It also defines WAVE Short Message Protocol.
- IEEE 1609.4-2016 defines MAC layer which supports multi-channel operation and interoperable remote management of WAVE devices.
- IEEE 1609.11-2010 specifies an application service layer and profile for payment and identity authentication, and payment data transfer for WAVE. In addition, this standard specifies a basic level of technical interoperability for electronic payment equipment using DSRC.
- IEEE 1609.12-2016 specifies allocations of WAVE identifiers.

In particular, 1609.2 version 2 in 2016 includes anonymous certificates for privacy. Furthermore, it specifies WAVE security service which consists of internal security services and high layer security services. The internal security services define secure massage exchange mechanism including certification management. The high layer security services define the function of certificate revocation mechanism and peer-to-peer certificate distribution mechanism which is specified in version 3 for the first time.

2.2 ITU-T SG17

ITU-T Study Group 17 (SG17) has standardized on ITS security since 2014. Standardization on ITS security has been processed in several SDOs such ISO and ETSI. However, those standard activities are part of the communication technology standardization. Therefore, it is worthy of note that security-specialized SDO such as ITU-T SG17 has started to work on ITS security recently.

There are two work items on ITS security in ITU-T SG17. One is focused on a specific area in ITS security (X.itssec-1) [4]. The other handles the overview of the ITS security (X.itssec-2) [5].

X.itssec-1, Software Update Capability for ITS Communications Devices, defines secure update procedure. X.itssec-1 is in the procedure of determination in SG17 March 2017 meeting. Since electric devices inside a vehicle such as electronic control units (ECUs), and electric toll collections (ETCs) and car navigation systems are becoming more sophisticated. As a result, software modules inside those electric devices need to be appropriately updated for the purpose of bug fixing, performance improvements, and security enhancements in order to avoid crucial accidents. Based on the above requirement, X.itssec-1 provides secure software update procedures between software update server and vehicles with appropriate security controls.

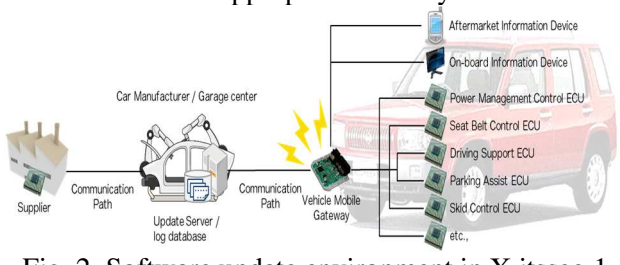

Fig. 2. Software update environment in X.itssec-1

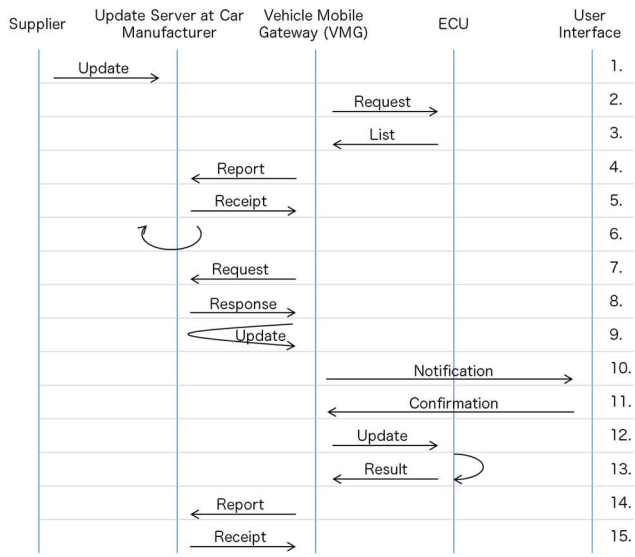

Fig. 3. Software update procedure.

Figure 2 provides remote software update reference model in the ITS communication environment. There are several entities include information devices, ECUs, and vehicle mobile gateway on a vehicle, update server and log database of car manufacturer and supplier. The Vehicle Mobile Gateway (VMG) is a module which communicates with a software update server in order for the vehicle to conduct software-update. The VMG can be a conceptual entity which is practically implemented with a set of multiple components. The update server is located at car manufacturers or garage centers in Fig. 2. It gathers status information of software modules from vehicles and distributes software update modules to the vehicles.

Figure 3 describes a secure software update procedure. The step 2, 3, 10, 11, 12, and 13, which are related with an in-vehicle communication, are only informative procedures for this recommendation. The detailed steps for the update procedure are described as follows:

1. An update module is provided by an automotive component supplier, which occurs asynchronously with the following steps.
2. As the initiation of the update procedure starts, a VMG requests ECUs to submit their software list.
3. An ECU checks its software status, generates a list of software modules and reports it to VMG.
4. The VMG submits the collected list to the update server to check whether any update for the vehicle exists.
5. The update server sends back a receipt of the submitted list to the VMG.
6. According to the list, the update server inspects the status of the installed software of the vehicle and determines the necessary software updates for the ECUs.
7. Since this inspection may take a long time, the VMG periodically checks the necessity of the updates for the vehicle.
8. If there is any update, the update server sends an access uniform resource locators (URLs) for the updates; otherwise, it sends back only an acknowledgement message.
9. If there is any update for the vehicle, the VMG connects to the update server to download the update modules for the vehicle.
10. Before applying the updates to ECUs, the VMG notifies the driver to confirm the application of the updates.
11. The driver confirms and accepts to apply the updates.
12. The VMG delivers the update files to the corresponding ECUs and requests them to apply the updates.
13. Each ECU applies the update and reports the application result to the vehicle mobile gateway.
14. The vehicle mobile gateway submits a report of application results to the update server.
15. Finally the update server sends back a receipt of the update information. If the application of the update has failed or some remaining update is found, the update server retries the procedure from step 6 to 14 until the application has succeeded.

X.itssec-1 also provides each message format and its XML example.

X.itssec-2, Security Guidelines for V2X Communication Systems, provides an overarching security consideration for V2X communication systems. V2X means V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure) and/or V2N (Vehicle-to-Nomadic Devices). X.itssec-2 provides analysis of threat and the security requirements for V2X communication systems. X.itssec-2 defines several attacks in terms of vehicle and RSU authentication, message integrity, message confidentiality, privacy, nonrepudiation, availability, and misbehavior of on-board unit (OBU) and vehicle sensors. It also presents some examples of attacks such as impersonation attack, Sybil attack, and DDoS attack in vehicular communication environment. Based on the analysis of the threats, it defines security requirements of V2X communication systems.

- Authentication of vehicle and RSU
  An entity such as OBU and RSU should prove to be an authorized owner of legitimate ID. This requirement is called as entity authentication. In case of group communication, the vehicle does not need to prove the ID. The vehicle should prove that he is a right member of the group. This requirement is called attribute authentication.
- Message integrity
  Messages sent to or from a vehicle and a RSU should be protected against unauthorized modification and deletion
- Confidentiality
  It should not be possible for an unauthorized entity to reveal the messages between vehicles and vehicles and between vehicles and infrastructure.
- Privacy protection
  It should not be possible for an unauthorized entity to analyse identification of a person and personally-identifiable information such as location or driving route of a particular person using communication messages.
- Non-repudiation
  It should not be possible for an entity to deny that it has already sent a message. This requirement can be implemented using digital signatures.
- Availability
  It should be possible for an entity to send and receive messages in appropriate latency. For example, forward collision warning message should be transmitted to an incoming vehicle before the vehicle arrives at the accident point. If the warning message cannot deliver to the incoming vehicle because of jamming attack, V2V/V2I safety application would be useless.
- Misbehaviour check (detection / prevention)
  It should be possible for an entity to detect and/or prevent any misbehaviour of OBU or vehicle sensors by checking its data.

Table 2. Security requirement for V2V/V2I communication in X.itssec-2

	V2V warning propagation	V2V platooning	V2V beaconing	V2I warning	V2V/V2I Information exchange
Authentication of vehicle and RSU	○	▲	○	○	○
Message integrity	○	○	○	○	○
Confidentiality	-	○	-	-	○
Privacy protection	○	○	○	▲	○
Non-repudiation	○	○	○	○	○
Availability	○	○	○	○	○
Misbehaviour check	○	○	○	○	○

O: Required, -: Not required, ▲: partially required

X.itssec-2 clarifies four different type of communications in V2V/V2I and it describes security requirements for each communication types shown in Table 2.

3 Security Consideration on ITS Security Standardization in ITU-T

With regard to X.itssec-1, several security considerations have been discussed. Step 15 in Fig. 3 expects that the system retries the procedure from the Step 6 to 14 until the application is succeeded. The Retry-until-success makes the VMG vulnerable to malfunction. Since it is possible that the procedure will never succeed or may take a long time to do in some cases, the recommendation to retry-until-success can cause the VMG to retry an unbounded number of times. Furthermore, X.itssec-1 specified the possibility that stream updating procedures will be needed in cases where ECUs do not have sufficient memory for a full update module. In spite of the VMG may have larger memory resources than the ECU, the VMG is also generally has the resource constraints of finite memory. Upon the mentioned security consideration, the recommendation has been modified to make limitation of the number of retries in order to remove this vulnerability.

The VMG and the update server can be connected using public network. If they are connected in public network, the exchanging messages between the VMG and the update server are required to be confidential. Also, those messages are required to be not modified. Therefore, X.itssec-1 additionally mentioned that the confidentiality mechanism is out of scope. It also specified that the confidentiality can be provided by lower layer protocols (e.g. hypertext transfer protocol secure (HTTPS) and secure tunneling protocol, etc.).

With regard to X.itssec-2, it defines threats and security requirements on V2V and V2I. Analysis of threat and security requirements on V2N communication should be considered in terms of message confidentiality, message integrity, entity authentication, privacy and availability. In addition, a lot of studies have considered Long Term Evolution - Vehicle (LTE-V) as the V2X technology recently. LTE-V is currently in the process of being standardized in 3GPP [6]. Since LTE infrastructure has already been deployed, the low cost of the deployment makes the LTE-V as a promising candidate for V2X communication. Thus, X.itssec-2 should also consider security aspects of LTE-V.

4 Conclusion

Connected vehicles are considered as the key enabling technology in ITS environment which includes autonomous driving technology. However, connected vehicles without security function can make ITS applications vulnerable to various security threats. Based on this requirement, many standard organizations are working on making international standard related with vehicular communication security.

This paper reviewed the standardization issues on ITS security especially in ITU-T SG17. X.itssec-1, Software Update Capability for ITS Communications Devices, is in the final determination procedure. X.itssec-2, Security Guidelines for V2X Communication Systems, is still in on-going standardization. Contributions on X.itssec-2 are encouraged to improve the recommendation.

In particular, automotive industry such as Hyundai Motor Group became a member of ITU [9]. It means that standardization on ITS security is essential not only for IT security industry but also for automotive industry. Furthermore, privacy issues in vehicular environment should be considered and developed in SDOs.

5 Acknowledgement

This work is conducted under international technology R&D collaboration program which is supported by the Ministry of Trade, Industry & Energy (MOTIE) and Korea Institute for Advancement of Technology (KIAT) (N0001710).

References:

[1] IEEE Std 1609.2, *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Security Services for Applications and* Management Messages, 2016.

[2] ETSI TS 102 731 V1.1.1, *Intelligent Transport Systems (ITS); Security; Security Services and Architecture*, 2010.

[3] ISO 21217:2014, *Intelligent transport systems -- Communications access for land mobiles (CALM) – Architecture,* 2014

[4] ITU-T SG17 draft Recommendation, *X.itssec-1*, *Software update capability for ITS communications devices,* Sep. 2016.

[5] ITU-T SG17 draft Recommendation, *X.itssec-2*, *Security Guidelines for V2X communication Systems*, Sep. 2016.

[6] 3GPP TR 22.885*, Study on LTE support for Vehicle to Everything (V2X) services*, 2015.

[7] E. Hamida, H. Noura, and W. Znaidi, *Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures*, Electronics, vol. 4, no. 3, pp. 380–423, 2015.

[8] Torsten Schütze, *Automotive security: Cryptography for car2x communication*, Embedded World Conference 2011.

[9] ITU Press release, *Hyundai becomes an ITU member to influence international standards for connected cars,* Nov. 2016

[10] PRESERVE (PREparing SEecure Vehicle-to-X Communication Systems), *Security Requirements of Vehicle Security Architecture*, 2011.