Standardization Trends in Security Technologies for Connected Cars at ITU-T

Koji Nakao
Former Vice-chairman, ITU-T SG17
National Institute of Information Communications Technology

1. The significance and necessity of security standardization for connected vehicles

As vehicles become more autonomous and connect to networks such as the Internet, ensuring the security of their on-board systems has become a top priority for the car industry. In recent years, the deployment of new connection services and autonomous driving functions in vehicles has also made them potential targets for malicious hackers. Furthermore, it is envisaged that large numbers of ECUs (electronic control units) incorporated into modern vehicles will be connected via diverse external networks such as Wi-Fi, mobile phone networks, and the Internet. Ensuring the security of complex systems provided by vehicles is therefore an urgent issue.

Various standards organizations have already begun to take steps towards achieving international standardization with regard to the above issues from the viewpoint of ensuring security in the connected car era. By drawing up standardized international technical specifications such as security frameworks for connected cars, threat analysis and security countermeasures, these efforts have resulted in a useful common reference for many stakeholders with an interest in international standards, and can be expected to provide materials such as international certification rules. This article outlines the trends in connected car security standardization in ITU-T SG17 (Security).

2. Standardization activities at SG17

(1) ITS Security: Question 13

ITU-T SG17 is a study group aimed at security standardization in general. One of its assigned tasks is to work on Question 13, which relates to Intelligent Transport System (ITS) security. This is a new Question that was established in the fall of 2017. It builds on the assumption of a connected car environment, and covers a wide range of topics including the formulation of security frameworks and guidelines, and the technical issues associated with connected cars.

(2) Current status of work on ITS security recommendations

ITU-T SG17 Question 13 is currently working on the Recommendations shown in the table.

Details of Recommendations that are of particular interest in this table are outlined below.

A) Revision of Recommendation X.1373 (Secure software update capability for intelligent transportation system communication devices)

Overview: Recommendation X.1373 was issued in March 2017. This Recommendation describes a secure procedure for updating software and firmware that runs on ECUs (electronic control units) installed in cars. It includes provisions regarding the use of electronic signatures to confirm the completion of updates (scope: see Figure 1). We are currently

Table: Recommendations being worked on by ITU-T SG17 Question 13

Recommendation	Title	Date of finalization
X.1373rev	Secure software update capability for intelligent transportation system communication devices	Sep-21
X.itssec-2	Security guidelines for V2X communication systems	Sep-19
X.itssec-3	Security requirements for vehicle accessible external devices	Mar-20
X.itssec-4	Methodologies for intrusion detection system on in-vehicle systems	Mar-20
X.itssec-5	Security guidelines for vehicular edge computing	Sep-21
X.edrsec	Security guidelines for cloud-based event data recorders in automotive environment	Sep-21
X.eivnsec	Security guidelines for the Ethernet-based in-vehicle networks	Sep-21
X.fstiscv	Framework of security threat information sharing for connected vehicles	Sep-21
X.mdcv	Security-related mis-behavior detection mechanism based on big data analysis for connected vehicles	Dec-20
X.srcd	Security requirements for categorized data in V2X communication	Dec-20
X.stcv	Security threats in connected vehicles	Sep-19

Figure 1: Scope of the former Recommendation X.1373 (this scope is expanded in the current revision)

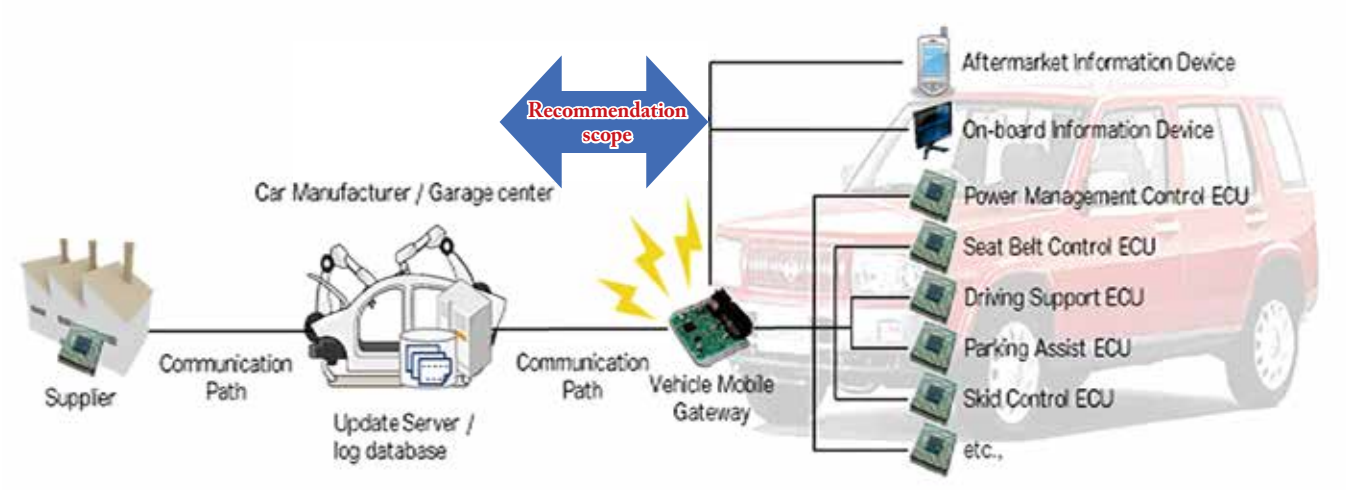
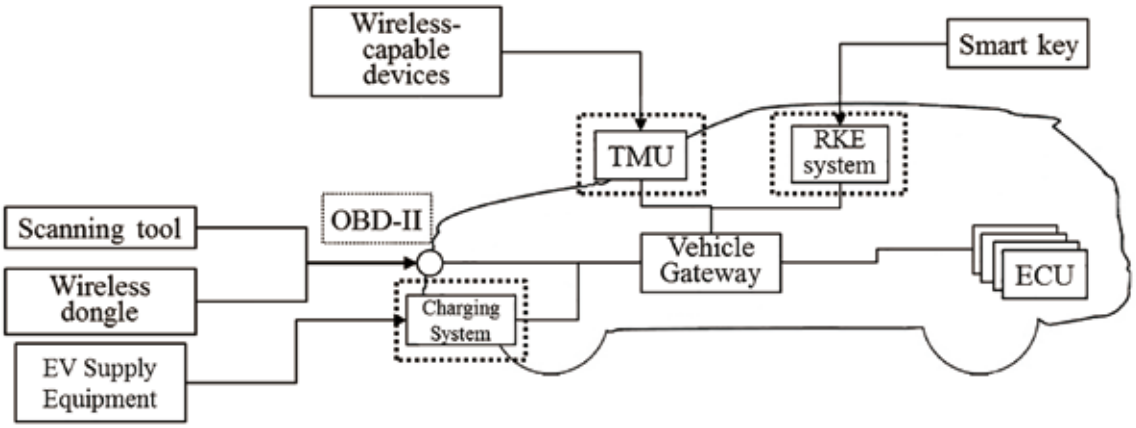


Figure 2: Expected interfaces and external equipment



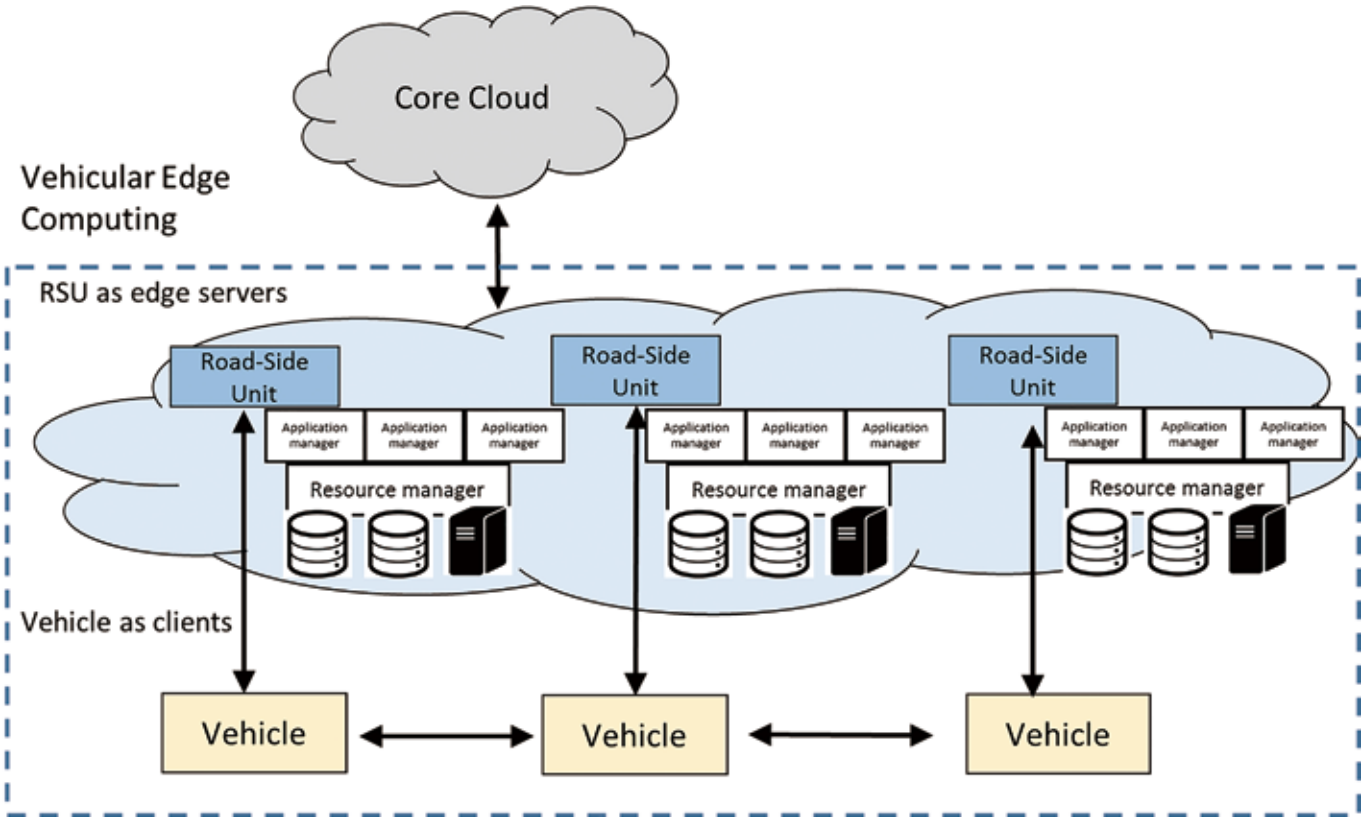
making revisions to this Recommendation, and are expanding its scope to reflect the requirements of OEM vendors around the world.

B) Draft Recommendation X.itssec-2 (Security guidelines for V2X communication systems)
Overview: Assuming communication takes place over connections between vehicles, between vehicles and the roadside (infrastructure), between vehicles and nomadic devices (e.g., smartphones), and between vehicles and people, we are extracting use cases and threat models that can be assumed for each type of connection, and are deriving security guidelines for each type of connection.

C) Draft Recommendation X.itssec-3 (Security requirements for vehicle accessible external devices)
Overview: By focusing on interfaces that are deployed in cars to facilitate external access, such as OBD-II, telematic management units (TMUs), remote keyless entry (RKE) systems, and charging systems, we are identifying threats and security requirements for access from external devices (scanning tools, wireless dongles, smart keys, etc.) and are summarizing them as standardized documents. Figure 2 shows the interfaces and external equipment assumed in this draft Recommendation.

D) Draft Recommendation X.itssec-4 (Methodologies for

Figure 3: The concept of edge computing for vehicles



intrusion detection system on in-vehicle systems)
Overview: This draft Recommendation focuses on methods of detecting intrusions into Controller Area Networks (CANs) that have a direct impact on ECUs, and presents a summary of lightweight intrusion detection methods that can be assumed to be installed in vehicles, including signature-based, entropy-based and self-similarity-based detection methods.

E) Draft Recommendation X.itssec-5 (Security guidelines for vehicular edge computing)
Overview: This draft Recommendation assumes the vehicular edge computing environment shown in Figure 3, analyzes the threats and vulnerabilities inherent in this environment, and summarizes its security requirements based on use cases provided as reference.

F) Draft Recommendation X.stcv (Security threats in connected vehicles)
Overview: In the Cyber Security Recommendation formulated by WP29 (World Forum for Harmonization of Vehicle Regulations) of UNECE (United Nations World Forum for Harmonization of Vehicle Regulations), based on the security threats summarized in the agreements between OEM vendors of each country, we are promoting a Recommendation for security threat information in Question 13 with the aim of using it as common threat information in ITU-T SG17. (Due to be finalized in September 2019)

3. Conclusion

This article has presented an overview of the ongoing Recommendation work under ITU-T SG17 Question 13. Most of these activities are based on proposals from Korea (principally, Hyundai Motor) and China (security vendors in cooperation with Chinese OEMs). Japan also recognizes the need for active participation in important draft Recommendations, including assessing the feasibility of questions and examining their details. As a new work item, a group comprising Chinese communications carriers and 20 Chinese OEM providers submitted a proposal at the ITU-T SG17 meeting held in January 2019, regarding security guidelines for network-based driving assistance in autonomous vehicles. This proposal was put on hold because it was too soon for a new work item, but we will continue to monitor and study future relevant developments.