Question 13/17 – Intelligent transport system (ITS) security

(Continuation of Question 13/17)

1 Motivation

Intelligent Transport System (ITS) including autonomous driving system provides various types of applications in order to increase road safety, decrease the environmental footprint of transport, enhance traffic management and maximize the transport sector's benefits to public and commercial users.

ITS includes various types of communications in vehicles (e.g., vehicle-to-nomadic device), between vehicles (e.g., vehicle-to-vehicle (V2V)), and between vehicles and fixed locations (e.g., vehicle-to-infrastructure (V2I)), i.e., vehicle-to-everything (V2X) communications. Information and communication technologies (ICT) are used to implement ITS including road transport, rail, water and air transport, including navigation systems.

An automated and assisted driving system consists of various components of systems where perception, decision making, and operation of the automobile are performed by electronics and machinery instead of a human driver, and as introduction of automation into road traffic.

In the ITS including autonomous and assisted driving system environment, vulnerabilities of a vehicle can be propagated to other vehicles since the vehicles are connected to each other. Thus, vulnerabilities of V2X communication systems in a vehicle should be managed and handled in order not to influence a lot of other vehicles.

Electric devices inside a vehicle such as electronic control units (ECUs) and electric toll collection (ETC) devices are becoming more sophisticated. As a result, software modules inside those entities need to be appropriately updated for performance and security improvements.

Recommendation ITU-T X.1373 approved in March 2017 provides the secure software update capability for ITS communication devices. X.1373 is currently under revision.

Standardization of the best comprehensive security solutions is vital for ITS environment. Due to some specific characteristics of the vehicular communications, providing security becomes especially challenging tasks that deserve study.

Recommendations under responsibility of this Question as of 7 January 2022: X.1371, X.1372, X.1373, X.1374, X.1375, X.1376.

Texts under development as of 7 January 2022: X.1373rev, X.edrsec, X.eivnsec, X.evtol-sec, X.fstiscv, X.idse, X.ipscv, X.itssec-5, X.rsu-sec and X.srcd.

2 Question

Study items to be considered include, but are not limited to:

a) How should security aspects (e.g., security architecture and subsystems) be identified and defined in an ITS and autonomous and assisted driving system environment?

b) How should threats and vulnerabilities in ITS and autonomous and assisted driving system services and networks be identified and handled?

c) What are the security requirements (e.g., those for identification and authentication) for mitigating the threats in an ITS and autonomous and assisted driving system environment?

d) What are security technologies to support ITS services and networks?

e) How should secure interconnectivity between entities in an ITS and autonomous and assisted driving system environment be kept and maintained?

f) What security techniques, mechanisms and protocols are needed for ITS and autonomous and assisted driving system services and networks?

g) What are globally agreeable security solutions for ITS and autonomous and assisted driving system services and networks, which are based on telecommunication/ICT networks?

h) What are best practices or guidelines for ITS and autonomous and assisted driving system security?

i) How AI/ML technologies can be used to provide security and confidence of the ITS and autonomous and assisted driving system?

j) What personally identifiable information (PII) protection and management mechanisms are needed for ITS services?

3 Tasks

Tasks include, but are not limited to:

a) Produce a set of Recommendations providing comprehensive security solutions for ITS and autonomous and assisted driving system.

b) Study further to define security aspects of ITS and autonomous and assisted driving system services and networks, which are based on telecommunication/ICT networks.

c) Study and identify security issues and threats in ITS and autonomous and assisted driving system.

d) Study and identify requirements and use cases for specific ITS and autonomous and assisted driving system services and applications.

e) Study and develop security mechanisms, protocols, and technologies for ITS and autonomous and assisted driving system.

f) Study and develop security profiling, hierarchical scheme for authentication and mechanism for specific ITS and autonomous and assisted driving system services and applications.

g) Study and develop applications of efficient encryption and decryption algorithms for fast moving network nodes and dynamically changing network topologies.

h) Study and develop the event data recording technologies in context of ITS and autonomous and assisted driving system.

i) Study and develop secure interconnectivity mechanisms for ITS and autonomous and assisted driving system in a telecommunication environment.

j) Study and identify PII protection issues and threats in ITS and autonomous and assisted driving system.

k) Study and develop PII protection and management mechanisms for ITS and autonomous and assisted driving system.

l) Study and develop secure ITS and autonomous and assisted driving system based on AI/ML technologies.

m) Study and develop an existing draft Recommendation X.1373rev, X.itssec-5, X.srcd, X.edrsec, X.eivnsec, X.fstiscv, X.ipscv, X.rsu-sec, X.evtol-sec.

n) Collaborate with the related SDOs to jointly develop Recommendations.

An up-to-date status of work under this Question is contained in the SG 17 work programme at https://www.itu.int/ITU-T/workprog/wp_search.aspx?sp=17&sg=17.

4 Relationships

WSIS Action Lines:

– C5

Sustainable Development Goals:

- 8 (Decent Work and Economic Growth)
- 9 (Industry, Innovation and Infrastructure)
- 11 (Sustainable Cities and Communities)

Recommendations:

- X-series and others related to security

Questions:

- ITU-T Qs 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17 and 15/17

Study Groups and Focus Groups:

- ITU-T SGs 11, 13, 16 and 20; ITU-R WP5A; Collaboration on ITS Communication Standards (CITS); ITU-T FG-VM (Vehicular Multimedia)

Standardization bodies:

- ISO TCs 22 and 204; ISO/IEC JTC 1/SCs 6 and 27; IETF WG ITS; IEEE 802.11 WG and 1609 WG; SAE International (e.g., Vehicle Cybersecurity Systems Engineering Committee, Connected Vehicles Steering Committee, and DSRC Technical Standard Committee); ETSI TC ITS; W3C Automotive WG

Other bodies:

- GSMA; ATIS; CCSA; TIA; TTA; TTC; UNECE (UN Economic Commission for Europe) Working Party 29 and subsidiary bodies (e.g., Taskforce on cyber security (TFCS)); AGL (Automotive Grade Linux)