Question 6/17 – Security for telecommunication services and Internet of Things (IoT)

(Continuation of Question 6/17)

1 Motivation

Recommendation ITU-T X.1101 provides the security requirements and framework for multicast communication. Recommendations ITU-T X.1111, X.1112, X.1113 and X.1114 describe the security framework for home network including the device certificate profile, authentication mechanism, and authorization framework. Recommendations ITU-T X.1121, X.1122, X.1123, X.1124, and X.1125 provide a comprehensive specification on security for mobile network. Recommendations ITU-T X.1171, X.1311, and X.1312 specify the privacy framework for mobile NID services, the security framework for USN (ubiquitous sensor network), USN middleware security guideline and security requirements for wireless sensor network routing, respectively. Recommendations ITU-T X.1191, X.1192, X.1193, X.1194, X.1195, X.1196, X.1197 and X.1198 describe a comprehensive set of requirements, mechanisms, and framework for security of IPTV services. Supplements ITU-T X.Suppl.19 and X.Suppl.24 provide security aspects of mobile phones. Recommendation ITU-T X.1331, X.1332 and Supplement ITU-T X.Suppl.26 describes the security aspects of smart grid. Recommendation ITU-T X.1361, X.1362, X.1363, X.1364 and X.1365 provide IoT related security requirements, mechanisms, and frameworks. A continued effort to maintain and enhance these security Recommendations and Supplements to satisfy the needs of new technologies and services is required.

The telecommunication services, networks and IoT refer to the service that allows anyone to access to any desired information in a user-friendly way, anytime and anywhere using any types of device. The telecommunications industry has been experiencing an exponential growth in the area of mobile technology-based telecommunication services. Specifically, security of domain-specific telecommunication services and networks among heterogeneous devices for the application-level technologies such as IoT and smart cities (including Machine to Machine (M2M), RFID, Near Field Communication (NFC) and sensor network), home network, industrial control systems(ex. smart factory), smart grid, embedded subscriber identity module (eSIM), smartphones, and IPTV networks, etc., are crucial for the further development of the industry, network operators and service providers.

Standardization of the best comprehensive security solutions is vital for network operators and service providers that operate in a multi-vendor international telecommunication environment. Due to some specific characteristics of IoT environment (e.g., limited computing power and memory size of the small mobile devices, long lifecycle, customized operating systems and software), providing security and personally identifiable information (PII) protection is an especially challenging task that deserves special attentions and study.

Recommendations and Supplements under responsibility of this Question as of 7 January 2022: X.1101, X.1111, X.1112, X.1113, X.1114, X.1121, X.1122, X.1123, X.1124, X.1125, X.1126, X.1127, X.1171, X.1191, X.1192, X.1193, X.1194, X.1195, X.1196, X.1197, X.1198, X.1311, X.1312, X.1313, X.1314, X.1331, X.1332, X.1333, X.1361, X.1362, X.1363, X.1364, X.1365, X.1366, X.1367, X.1368, X.1369, X.1453, and Supplements X.Suppl.19, X.Suppl.24 and X.Suppl.26.

Texts under development as of 7 January 2022: X.iotsec-4, X.ra-iot, X.sc-iot, X.ztd-iot, and TR.ibc-cd.

2 Question

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

a) How should security aspects of telecommunication services and IoT be identified and defined in mobile telecommunication?

b) How should threats behind telecommunication services and IoT be identified and handled?

c) What are the security technologies for supporting telecommunication services and IoT?

d) How should secure interconnectivity in telecommunication services and IoT be kept and maintained?

e) How should security technologies using AI/ML based technologies be studied and developed for telecommunication services and IoT?

f) What security techniques, mechanisms and protocols are needed for new telecommunication services and IoT, especially for new digital content protection services?

g) What are the global security solutions for telecommunication services and IoT (e.g. including services for smart cities, smart grid and ICS (ex. smart factory) which are based on telecommunication/ICT networks)?

h) What are the best practices or guidelines for secure telecommunication services and IoT?

i) What enhancements to existing Recommendations under review or new Recommendations under development should be adopted to reduce impact on climate changes (e.g., energy savings, reduction of greenhouse gas emissions, implementation of monitoring systems) either directly or indirectly in telecommunication/ICT or in other industries?

j) What PII (Personally Identifiable Information) protection and management mechanisms are needed for secure telecommunication services and IoT?

3 Tasks

Tasks include, but are not limited to:

a) In collaboration with other ITU-T study groups and standards development organizations, especially with IETF, ISO/IEC JTC 1/SCs 6, 25, 27, 31 and 41, produce a set of Recommendations for providing comprehensive security solutions for secure telecommunication services and IoT.

b) Review existing Recommendations/Standards of ITU-T, ISO/IEC and other standardization bodies in the area of home network, smart grid, smartphone security, IoT and ubiquitous sensor network to identify secure telecommunication services.

c) Study further to define security aspects of telecommunication services and IoT for a multi-vendor international telecommunication environment, and for new services (e.g., those for smart cities, smart grid and ICS (ex. smart factory) which are based on telecommunication/ICT networks).

d) Study and identify security issues and threats in secure telecommunication services and IoT.

e) Study and develop security mechanisms for secure telecommunication services and IoT.

f) Study and develop interconnectivity mechanisms for secure telecommunication services and IoT in a single or multi-vendor telecommunication environment.

g) Study and identify PII protection issues and threats in secure telecommunication services and IoT.

h) Study and develop PII protection and management mechanisms for secure telecommunication services and IoT.

i) Study and develop security technologies utilizing AI/ML based technologies for the secure telecommunication services and IoT.

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, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 and 15/17

Study Groups:

– ITU-R; ITU-T SGs 9, 11, 13, 15, 16 and 20, JCA-IoT and SC&C

Standardization bodies:

– Internet Engineering Task Force (IETF); IEC SEG 6 (Micro Grid), IEC SMB WG3, IEC TCs 57 and 65; ISO/IEC JTC 1/SCs 6, 25, 27, 31 and 41; Open Mobile Alliance (OMA); Third Generation Partnership Project (3GPP); Third Generation Partnership Project 2 (3GPP2)

Other bodies:

– Alliance for Telecommunications Industry Solutions (ATIS); China Communications Standards Association (CCSA); European Telecommunications Standards Institute (ETSI); GSM Association (GSMA); M2M Alliance; NFC Forum; National Institute of Standards and Technology (NIST); oneM2M; Telecommunication Technology Committee (TTC); Telecommunications Technology Association (TTA); Universal Plug and Play (UPnP)