Question 2/17 – Security architecture and network security

(Continuation of Question 2/17)

1 Motivation

Recommendations ITU-T X.800, X.802 and X.803 describe security within the context of open systems. The security architecture for systems providing end-to-end communications is provided in Recommendation ITU-T X.805. A comprehensive set of detailed security frameworks covering aspects of security such as authentication, access control, non-repudiation, confidentiality, integrity, and security audit and alarms has been established (X.810, X.811, X.812, X.813, X.814, X.815 and X.816). To provide Generic Upper Layers Security (GULS), Recommendations ITU-T X.830, X.831, X.832, X.833, X.834 and X.835 have been developed. In cooperation with ISO/IEC JTC 1/SC 27, Recommendations ITU-T X.841, X.842 and X.843 on security information objects and trusted third party services have been established.

A continued effort to maintain and enhance these security Recommendations to satisfy the needs of emerging technologies (e.g., next generation networks (NGN), security aspects of software-defined networking (SDN)/network function virtualization (NFV), network slicing (NS), service function chain (SFC), multi-access edge computing (MEC),long term evolution/system architecture evolution (LTE/SAE), IMT-2020/5G network and beyond, common security framework and architecture for services/applications, the foundations of artificial intelligence (AI) / machine learning (ML) in supporting the building of confidence and security in the use of ICTs, technical implementation guidance for systems providing end-to-end communications and Internet protocol based networks) and services is required. This effort is reflected by X.1035 and X.1036 that show details of password-authenticated key exchange protocols and policy distribution and enforcement, X.1037 that provides IPv6 security guidelines, X.1038, X.1042, X.1043 and X.1044 that provide security requirements etc. on software-defined networking (SDN) and network function virtualization (NFV), X.1045 that provides customized security services based on service function chain (SFC).

Due to convergence and mobility, telecommunications carrier networks and the associated information systems are exposed to new classes of security threats. The attackers have a deeper reach into networks and require less skill levels with a higher damage propensity. Viruses, hacking and denial of service attacks have become pervasive and they adversely impact network elements and support systems alike.

The telecommunications and information technology industries are seeking cost-effective comprehensive security solutions that are technology agnostic and protect a wide spectrum of networks, services and applications. To achieve such solutions in multi-vendor environment, network security should be designed and optimized around the standard security architectures and standard security technologies. Taking into account the security threats to the telecommunication environment and the current advancement of security countermeasures against the threats, new security requirements and solutions should be investigated. New Recommendations that show how to combine the technology standards and security frameworks are needed to implement comprehensive security for the emerging networks, services and applications.

Recommendations and Supplements under responsibility of this Question as of 7 January 2022: X.800, X.802, X.803, X.805, X.810, X.811, X.812, X.813, X.814, X.815, X.816, X.830, X.831, X.832, X.833, X.834, X.835, X.841, X.842, X.843, X.1011, X.1031, X.1032, X.1033, X.1034, X.1035, X.1036, X.1037, X.1038, X.1039, X.1040, X.1041, X.1042, X.1043, X.1044, X.1045, X.1046, X.1047, X.1811, and Supplements X.Suppl.2, X.Suppl.3, X.Suppl.15, X.Suppl.16, X.Suppl.23 and X.Suppl.30.

Texts under development as of 7 January 2022: X.5GSec-ecs, X.5GSec-guide, X.5Gsec-message, X.5Gsec-netec, X.5Gsec-ssl, X.5Gsec-t (X.1812), X.5Gsec-vs, TR.zt-acp, and XSTP-5Gsec-RM.

2 Question

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

a) How should a comprehensive, coherent telecommunications security solution be defined?

b) What is the architecture for a comprehensive, coherent telecommunications security solution?

c) What is the framework for applying the security architecture in order to establish a new security solution?

d) What is the framework for applying the security architecture in order to assess (and consequently improve) an existing security solution?

e) What are the architectural underpinnings for security?

   i) What is the architecture for end-to-end security?

   ii) What is the open systems security architecture?

   iii) What is the security architecture for the mobile environment?

   iv) What is the security architecture for evolving networks?

   v) What is the security architecture for application services in collaboration with Q7/17?

f) What new security architecture and framework Recommendations are required for providing security solutions in the changing environment?

g) How should architectural standards be structured with respect to existing Recommendations on security?

h) How should architectural standards be structured with respect to the existing advanced security technologies?

i) How should the security framework Recommendations be modified to adapt them to emerging technologies and what new framework Recommendations are required?

j) How are security services applied to provide security solutions?

k) How is telecommunication/ICT infrastructure monitoring applied to provide security solutions?

l) What are the foundations of artificial intelligence / machine learning (AI/ML) in supporting the building of confidence and security in the use of ICT?

m) What are the new security threats and challenges introduced by the emerging network technologies (e.g., SDN, NFV, network slicing, SFC, MEC, LTE/SAE, IMT-2020/5G network and beyond, etc.)?

n) What are the security requirements of IMT-2020/5G network and beyond, and how SG17 can address them?

o) What are common security mechanisms for the emerging networks technologies?

3 Tasks

Tasks include, but are not limited to:

a) Development of a comprehensive set of security architecture and framework Recommendations for providing standard security solutions for telecommunications in collaboration with other standards development organizations and ITU-T study groups.

b) Studies and development of Recommendations on a trusted telecommunication network architecture that integrates advanced security technologies.

c) Studies and development of Recommendations on the foundations of AI/ML in supporting the building of confidence and security in the use of ICT.

d) Maintenance and enhancements of Recommendations and Supplements in the X.800-series and X.103x-series.

e) Studies and development of Recommendations on common network security.

f) Study the security requirements of IMT-2020/5G network and beyond, coordinate the related work in various Questions of SG17, be the single point of contact for the security aspect of IMT-2020/5G network and beyond in SG17, and lead the research and development of standards on Security aspects of IMT-2020/5G network and beyond.

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, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 and 15/17

Study Groups:

– ITU-D SG2; ITU-R WP6B; ITU-T SGs 2, 9, 11, 13, 15, 16 and JCA-IMT2020

Standardization bodies:

– Alliance for Telecommunications Industry Solutions (ATIS); European Telecommunications Standards Institute (ETSI); GSM Association (GSMA); Forum for International Irregular Network Access (FIINA); ISO/IEC JTC 1/SC 27 and SC 37; IEC TC 25; ISO TC 12; Internet Engineering Task Force (IETF); Third Generation Partnership Project (3GPP)