Question 1/17 – Security standardization strategy and coordination

(Continuation of Question 1/17)

1 Motivation

Security threats to telecommunication, and Information and Communication Technologies (ICTs) and infrastructure remain increasingly complex. Efforts over the years to secure the infrastructure have been somewhat fragmented and reactionary, and so far have not produced the desired level of protection against threats in a timely manner. The economic impact of such attacks and threats has been huge, resulting in several financial and organizational losses to governments and entities. Intensive, continuous and focused efforts are essential to combat these threats.

This effort is complex and requires the participation of a large number of organizations working on various aspects of security, each within their area of expertise and mandate. This requires coordination, collaboration and cooperation among the various stakeholders, which is a difficult and challenging task.

The subject of security is vast in scope. Security can be applied to almost every aspect of ICTs and networks. There are various approaches to addressing security requirements. These include:

– A bottom-up approach in which experts devise security measures to strengthen and protect a particular domain of the network using specific countermeasures and techniques such as biometrics and cryptography. While fairly common, this is a fragmented approach that often results in uneven determination and application of security measures.

– A top-down approach, which is a high-level and strategic way of addressing security. This approach requires knowledge of the overall picture. It is generally a more difficult approach because it is harder to find experts with comprehensive knowledge of every part of the network and its security requirements than it is to find experts with detailed knowledge of one or two specific areas.

– A combination of bottom-up and top-down approaches, with coordination effort to bring the different pieces together. This has often proved to be extremely challenging when dealing with varying interests and agendas.

This Question produces many deliverables that ITU-T considers as fundamental in promoting its work and deliverables. They also provide valuable resources to the ITU and external organizations. Examples include the ICT Security Standards Roadmap, the Security Manual, the Security Compendia, and the Successful Use of Security Standards. This Question will develop a vision and propose the organizational architecture of SG17. This Question will continue to focus on the coordination and organization of the entire range of telecommunication/ICT security activities within ITU-T and will continue to develop and maintain documentation to support coordination and outreach activities. A top-down approach to security will be used in collaboration and coordination with other study groups and standards development organizations (SDOs). This activity is directed at achieving a more focused effort at the projects and strategic level both internal and external to SG17. This Question supports SG17 activities to ensure that they reflect an efficient process capable of developing high quality, timely, market-driven telecommunication/ICT standards. This Question also addresses the needs of developing countries and Regional Study Groups through the implementation of WTSA Resolution 44 on Bridging the standardization gap.

The security standardization strategy is one of the most important topics across all Questions in SG17. SG17 needs to consider how security standardization architecture and design can improve the development of current and future security work items.

SG17 work on security considers WTSA Resolutions 2, 7, 11, 18, 32, 40, 44, 50, 52, 54, 58, 64, 65, 67, 73, 75, 76, 77, 78, 80, 84, 86, 89, 90, 92, 93, 94, 96, 97 and 98; PP Resolutions 101, 123, 130, 136, 174, 177, 178, 179, 181; 188, 189, 197, 199, 200, 201, 204, 205 and 206; and WTDC Resolutions 30, 34, 43, 45, 47, 63, 67, 69, 79, 80, and 84.

SG17 also supports WSIS action line C5 "Building confidence and security in the use of ICTs" and Objective 2 of the Buenos Aires Action Plan adopted at the 2017 World Telecommunication Development Conference on "Modern and secure telecommunication/ICT infrastructure: Foster the development of infrastructure and services, including building confidence and security in the use of telecommunications/ICTs."

Technical Reports under responsibility of this Question as of 7 January 2022: TR.sec-manual, TR.Suss.

Texts under development as of 7 January 2022: X.arch-design.

2 Question

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

a) What are the deliverables for this Question?

b) What are the processes, work items, work methods and timeline for the Question to achieve the deliverables?

c) What outreach documents (roadmap, security compendia, technical reports, flyers, webpages, etc.) need to be produced and maintained by ITU?

d) What security workshops are needed and how they can be organized?

e) What is needed to build effective relationships with other SDOs in order to advance the work on security?

f) What are the key milestones, success criteria and supporting performance metrics?

g) How can Sector Member and Administration interest in security work be stimulated and how can momentum be sustained?

h) How could telecommunication/ICT security features become more relevant to the marketplace?

i) How can the crucial importance of security and the urgent need to protect global economic interests, which depend on a robust and secure telecommunication/ICT infrastructure, best be promoted to governments and the private sector?

j) What are the security activities under development in other ITU Study Groups and other SDOs?

k) How to address the needs of developing countries and Regional Study Groups in the implementation of WTSA Resolution 44?

l) What is the standardization strategy in support of a comprehensive, coherent telecommunications security solution?

m) How should standardization strategy embrace existing Recommendations on security?

3 Tasks

Tasks include, but are not limited to:

a) Act as primary SG17 contact for telecommunication/ICT security coordination matters.

b) Develop and maintain an organizational architecture roadmap – to provide a vision and a detailed plan that determines the level and scope of the security domain for study. The roadmap shall identify all related components (structure, processes) and their interrelationships, participating organizations and roles. Distinction needs to be made between emerging systems/networks and existing systems/networks.

c) Maintain and update the ICT Security Standards Roadmap.

d) Maintain and update the ITU-T Security Compendia.

e) Assist and provide input to TSB in maintaining the Security Manual published as technical report "Security in telecommunications and information technology".

f) Maintain and update the technical report on the successful use of security standards.

g) Provide guidance on the implementation of telecommunication/ICT security standards.

h) Promote cooperation and collaboration between groups working on telecommunication/ICT security standards development.

i) Review Recommendations and liaisons from other study groups and SDOs as appropriate to assess security coordination implications.

j) Assist in efforts to ensure effective security coordination where necessary.

k) Help direct liaisons from external groups to appropriate study groups in ITU-T.

l) Take ITU-T lead in organizing and planning security workshops and seminars as appropriate.

m) Ensure effective and efficient participation in security coordination efforts with other organizations.

n) Assist in improving the efficiency of SG17 work (e.g., by creating templates, tools, or procedures, performance metrics).

o) Encourage national authorities and operators from developing countries in regions to work together and better contribute to ITU-T SG17 activities in line with the SG17 mandate and in implementing SG17 security Recommendations.

p) Assist SG17 in Bridging Standardization Gap with the aim of supporting WTSA Res. 44, PP Res. 123, and WTDC Res. 47.

q) Achieve effective and efficient participation in security coordination efforts within SG17 to ensure the SG17 work programme reflects the current SG17 security activities and addresses the concerns of the ITU-T membership.

r) Development of a comprehensive set of security standardization strategy documents, including architecture documents, for supporting the standardization of security solutions in collaboration with other standards development organizations and ITU-T study groups.

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)

– 17 (Partnerships to achieve the Goal)

Recommendations:

– X-series and others related to telecommunication/ICT security.

Questions:

– ITU-T Qs 2/17, 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; ITU-R; ITU-T SGs 2, 3, 5, 9, 11, 13, 15, 16 and 20; TSAG, including relevant JCAs and FGs

Standardization bodies:

– Alliance for Telecommunications Industry Solutions (ATIS); Cloud Security Alliance (CSA); European Telecommunications Standards Institute (ETSI); Institute of Electrical and Electronics Engineers (IEEE); Internet Engineering Task Force (IETF); ISO/IEC JTC 1/SCs 6 and SC 27, ISO TC 292, ISO TMB; Organization for the Advancement of Structured Information Standards (OASIS); Third Generation Partnership Project (3GPP); Third Generation Partnership Project 2 (3GPP2); Asia-Pacific Telecommunity Standardization Program (ASTAP)

Other bodies:

– European Network and Information Security Agency (ENISA); National Institute of Standards and Technology (NIST); one M2M; Regional Asia Information Security Exchange (RAISE) Forum