Question 7/17 – Secure application services

(Continuation of Question 7/17)

1 Motivation

Recommendations ITU-T X.1141, X.1142, X.1143, X.1144, X.1145, X.1146, X.1147 provide a set of Recommendations on security tokens for authentication/authorization and security architectures for message of network services. Recommendations ITU-T X.1151, X.1152, X.1153, X.1154, X.1155, X.1156, X.1157, X.1158, X.1159 specify guidelines on secure password-based authentication with key exchange and various Trusted Third Party (TTP) services. Recommendations ITU-T X.1161, X.1162, X.1163, and X.1164 specify a comprehensive framework and mechanisms for the security of P2P services. A continued effort to maintain and enhance these security Recommendations to satisfy the needs of emerging technologies and services is required.

The telecommunications industry has been experiencing an exponential growth in TTP (Trusted Third Party) services. Security of telecommunication-based application service including social network service, P2P and TTP service is crucial for the further development of the industry. Secure application protocols play a very critical role for providing secure application service. Standardization of the best comprehensive security solutions is vital for the industry and network operators that operate in a multi-vendor international environment. It is also required to study and develop other types of secure platform, application services such as time stamping services, secure notary services, secure FinTech (open banking, peer-to-peer lending, remittance, mobile wallet, insurance) services, secure OTT (Over The Top) services, and digital twin; use of security assertions as a replacement to the use of certificates in PKI based protocols and PKI application services, etc. Security technologies such as security assertion and access control assertion become very critical in communication networks.

As telecommunication and ICT are developing application services, they are facing two new horizons which need to be studied: applications are generating and processing more and more data, and to support it, artificial intelligence is now required. Secure application services need to be extended to cover the extensive research and market required to study the spectrum of operational and technical aspects of data protection which builds on the existing work on data analytics services.

Regarding Artificial Intelligence, service providers are facing several challenges in particular the selection, onboarding and integration of dozens, if not hundreds, of AI components from open source and industry that they need to package in various form factors (integrated AI applications, AI as more generic platforms, AI as platform as a service, etc.) on various infrastructures (on premise, private cloud, hybrid cloud, public cloud). As when Big Data started, this creates new security interoperability issues, let alone ensuring the confidentiality, integrity, and availability issues for input training data to AI and AI output data. All of this forms a new attack surface for Artificial Intelligence that needs to be studied and developed. Again, it can build on the initial existing work on data analytics services.

Recommendations and Supplements under responsibility of this Question as of 7 January 2022: X.1141, X.1142, X.1143, X.1144, X.1145, X.1146, X.1147, X.1148, X.1149, X.1151, X.1152, X.1153, X.1154, X.1155, X.1156, X.1157, X.1158, X.1159, X.1161, X.1162, X.1163, X.1164, X.1450, X.1451, X.1452, X.1470, and Supplements X.Suppl.17, X.Suppl.21 and X.Suppl.22.

Texts under development as of 7 January 2022: X.1144rev, X.guide-cdd, X.rdda, X.saf-dfs, X.scpa, X.sec-grp-mov, X.sg-dtn, X,sles, X.smdtsc, X.smsrc, X.vide, X.websec-7 and TR.cta.

2 Question

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

a) How should threats behind secure application services be identified and handled?

b) What are the security technologies for providing secure application services?

c) How should secure interconnectivity between application services be kept and maintained?

d) What security techniques or protocols are needed for secure application services?

e) What security techniques or protocols are needed for emerging secure application services, including service platform, FinTech services, OTT services?

f) What are the global security solutions for secure application services and their applications?

g) How to define a strategy for operational and technical data protection for application services?

h) How to define a strategy for protecting Artificial Intelligence attack surface?

3 Tasks

Tasks include, but are not limited to:

a) In collaboration with other ITU-T Study Groups and Standards Development Organizations, especially with ISO/IEC JTC 1/SC 27, produce a comprehensive set of Recommendations for providing comprehensive security solutions for application communication services.

b) Review existing Recommendations/Standards of ITU-T and ISO/IEC in the area of secure application services.

c) Study further to define security aspects of secure application services and for emerging new services such as FinTech Services and OTT services.

d) Study and develop security issues and threats in secure application services.

e) Study and develop security mechanisms for secure application services.

f) Study and develop strategies and Recommendations for operational and technical aspects of data protection for application services.

g) Study and develop strategies and Recommendations for protecting Artificial Intelligence attack surface.

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.800 series and others related to security

Questions:

– ITU-T Qs 1/17, 2/17, 3/17, 4/17, 6/17, 8/17, 10/17, 11/17, 14/17, 15/17, 7/13 and 13/17

Study Groups:

– ITU-T SGs 2, 9, 11, 13, 16, and 20

Standardization bodies:

- Internet Engineering Task Force (IETF); European Telecommunications Standards Institute (ETSI); GSM Association (GSMA); ISO/IEC JTC 1/SC 27, ISO/IEC JTC 1/SC 42, ISO/TC 68, ISO/TC 307; Kantara Initiative; Organization for the Advancement of Structured Information Standards (OASIS); Open Mobile Alliance (OMA); World Wide Web Consortium (W3C)

Other bodies:

- Council of Europe (COE); European Network and Information Security Agency (ENISA); Fast Identity Online (FIDO) Alliance; International Multilateral Partnership Against Cyber Threats (IMPACT)