Question 15/17 – Security for/by emerging technologies including quantum-based security

(Continuation of Question 15/17)

1 Motivation

SG17 recognizes the dynamic nature of security studies which heavily depend on the both the attacker/defenders' arms race and the ripple effect from innovations being leveraged by both sides. This results in a cadence of emerging security technologies from which some require global standardization.

As by nature, it is impossible to anticipate what and when, SG17 proactively established and runs an incubation mechanism (TP.inno) which offers controlled agility in studying emerging security areas in order to secure new emerging telecommunication/ICT based services and applications.

This incubation mechanism enables SG17 to introduce new work items in an efficient manner in the emerging areas and encourages non-normative texts (Technical Papers and Technical Reports) as a proven best practice to allow SG17 community time to familiarize itself with these new emerging areas and newcomers to familiarize themselves with SG17 and ITU-T procedures and environment. In the development of the new work items, sometimes, the nature of the emerging security technology reveals it is closer to an existing Question and this work item can be transferred to maximize the coherency, efficiency and quality of SG17 work.

As well, this incubation mechanism allows the identification of trends in emerging security technologies which are being developed in this Question. Some emerging technologies come from

– the nature of the topic itself is nascent, for example quantum-based security, secure multi-party computation, homomorphism, or potentially identifiable security for robotics, etc.
– the topic is not nascent, but it is the first time they enter global standardization, e.g. malware analysis, data loss prevention, etc.
– operational security architecture gaps that do not fit in any question e.g. security product themselves, heavy integration and composition issues showing emerging new cross-topic solutions, security data schemas, etc.

One of emerging areas identified during incubation mechanism is quantum-based security. The advent of large-scale quantum computers offers potential significant disruptions on conventional telecommunication systems based on ICT as well as, poses significant risks to security.

Indeed, the current cryptography security relies on computationally difficult problems: a discrete logarithmic problem and an integer-factorization problem. They are considered to be difficult to solve in a reasonable time, given the current architectures of current computers available today and in the medium term. Yet, public key cryptography using asymmetric keys is a cornerstone of authentication over public networks. As, by its nature, quantum computers can solve integer-factoring and discrete-logarithm problems in a reasonably fast time, they are, by ripple effect, able to break the foundations on which cryptography is currently built on, threatening an existential corner stone of todays' cyber life and digitalization.

Quantum key distribution (QKD) enables two parties to produce a shared random secret key known only to them which can be used to encrypt and decrypt messages using conventional cryptographic algorithms. QKD had two limits that create network topological and integration issues: a) it is point-to-point (p-t-p) and can only be applied to tow parties, A and B and b) it has distance limitations on terrestrial networks. To overcome these two limitations, the concept of QKD networks has been introduced in the industry consisting of (1) an ensemble of nodes that are linked together through QKD systems working in p-t-p, and (2) a management system that is shared between and embedded in each of the QKD nodes. The purpose of this management system is to distribute secret keys between two or more nodes within the same QKD network that might not be directly linked. Currently, commercial QKD systems are stable and mature enough to start planning for large scale

QKD networks. There are several initiatives by companies/institutions to develop QKD networks, however, there is no widely accepted standard for what constitutes a QKD system.

Additionally, random numbers are a fundamental key element in engineering with important applications in cryptography. The inherent randomness at the core of quantum mechanics makes quantum systems a perfect source of entropy. Quantum random number generation is one of the most mature quantum technologies with many alternative generation methods.

In summary, a quantum-based security ensures communication that is not vulnerable to attacks by quantum computers. Implementation of quantum-based security requires several key elements including quantum key distribution and quantum random number generator (QRNG). In addition, the interoperability in the key elements and functionalities for the QKD and the QRNG are important to be widely used in real telecommunication networks.

In turn, there is a strong need for SG17 to study quantum-based security that are resistant to quantum attacks.

Recommendations and Technical Papers/Reports under responsibility of this Question as of 7 January 2022: X.1702, X.1710, X.1712, X.1714, and X.1770, and Technical Papers TP.inno, TP.sgstruct, and TR.sec-qkd.

Texts under development as of 7 January 2022: X.1712 Corrigendum, X.icd-schemas, X.sec_QKDN_AA, X.sec_QKDN_CM, X.sec_QKDN_intrq, , X.sec-QKDN-tn, TR.hybsec-qkdn, TR.sec-ai, and TR.sgfdm.

2 Question

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

a) What are the new emerging security technologies?

b) What are the categories of new emerging security technologies?

c) How to safely develop emerging security technologies?

d) What are the most effective mechanisms for implementing incubation mechanism?

e) What are the impacts and challenges of conventional communications from advent of largescale quantum computers?

f) What are the key elements for building quantum-based security?

g) What is transition strategy for building quantum-based security?

h) How should threats and vulnerabilities in quantum-based security be handled?

i) What are the security requirements for mitigating threats in quantum-based security?

j) What are the security technologies to support quantum-based security?

k) How should secure interconnectivity between entities in quantum-based security be kept and maintained?

l) What security requirements, techniques, mechanisms and protocols are needed for quantum-based security?

m) What are globally agreeable security solutions for quantum-based security, which are based on telecommunication/ICT communications?

n) What are best practices or guidelines of security for quantum-based security?

3 Tasks

Tasks include, but are not limited to:

a) Identify new emerging security technologies.

b) Identify new categories of emerging security technologies to firm up Question M strategy.

c) Potentially reallocate NWI to other question should their development makes it clearer the match to an existing Question.

d) Incorporate incubation mechanism to address the new emerging areas in ITU-T SG17.

e) Produce a set of technical Recommendations providing comprehensive security solutions to establish quantum-based security.

f) Study to define security aspects of quantum-based security, which is based on telecommunication/ICT infrastructure.

g) Study and identify security issues and threats in quantum-based security.

h) Study and develop security requirements, mechanisms, protocols, and technologies for quantum-based security.

i) Study and develop secure interconnectivity mechanisms for quantum-based security.

j) Study and develop information management system for entities providing quantum-based security.

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, 13/17, and 14/17

Study Groups:

– ITU-T SGs 2, 3, 5, 9, 11, 12, 13, 15, 16, and 20

Standardization bodies:

– ETSI TC Cyber, ISG-QKD; ISO/IEC JTC 1/SC 27; OASIS; IETF

Other bodies:

– GSMA; ATIS; CCSA; TIA; TTA; TTC