Trends in Security Standardization at ITU-T SG17

Kan Yasuda

Abstract

The International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) Study Group (SG) 17 is a de jure organization that deals with security. Another such organization is the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) 1/Subcommittee (SC) 27. This article introduces the efforts of ITU-T SG17 and outlines trends in security standardization by comparing them with JTC 1/SC 27.

Keywords: security standardization, ITU-T SG17, ISO/IEC JTC 1/SC 27

1. ITU-T SG17 (Security)

The International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) Study Group (SG) 17 deals with general security issues. While other SGs handle security issues specific to their respective fields, SG17 is responsible for the overall security study of ITU-T.

ITU-T SG17 has a long history of dealing not only with security but also with fundamental technologies for security, including directories, object identifiers, and technical languages. One of the classic recommendations of ITU-T SG17 is X.509, which defines a standard format for digital certificates. Also well known are the Abstract Syntax Notation One (ASN.1) and object identifiers.

As of July 2023, ITU-T SG17 has five Working Parties (WPs) and twelve Questions (Qs). Each Q belongs to one of the WPs. The composition of these WPs and Qs is dynamic. Qs are added and merged as discussions evolve and technology advances. (That is why they are numbered in skips.) The scope of a particular Q may be expanded. WPs and Qs may be reconfigured at regular intervals. Next year marks a milestone, and a major reorganization may take place. The current structure of WPs and Qs is shown in **Fig. 1**.

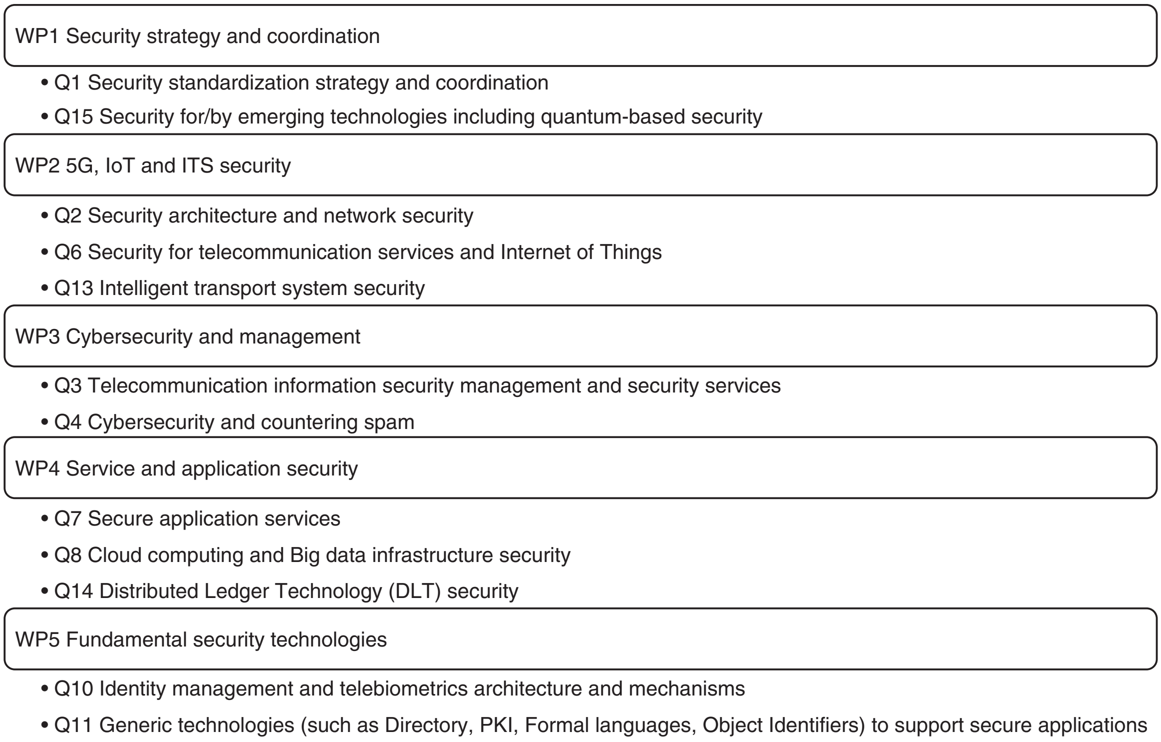
2. JTC 1/SC 27 (Information security, cybersecurity and privacy protection)

I now discuss the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) 1/Subcommittee (SC) 27 as a comparison. This de jure organization also deals with general security issues, particularly methods, techniques and guidelines related to information security, cybersecurity, and privacy protection. Although its role is similar to that of ITU-T SG17 in that it is also responsible for security that affects the entire JTC 1, it does not deal with standardization of underlying technologies such as directories or technical languages. (It does make use of them, though.)

Within JTC 1/SC 27, there are five working groups (WGs), each of which is responsible for a different topic. An overview is given in **Fig. 2**. Although the WGs in JTC 1/SC 27 have been added or renamed, they are basically static and the scope of their work has not changed significantly.

3. Comparison of the two organizations

Corresponding to the respective organizational structures of ITU-T SG17 and JTC 1/SC 27, the Japanese domestic committees have different structures. The domestic committee corresponding to ITU-T



WP1 Security strategy and coordination

- Q1 Security standardization strategy and coordination
- Q15 Security for/by emerging technologies including quantum-based security

WP2 5G, IoT and ITS security

- Q2 Security architecture and network security
- Q6 Security for telecommunication services and Internet of Things
- Q13 Intelligent transport system security

WP3 Cybersecurity and management

- Q3 Telecommunication information security management and security services
- Q4 Cybersecurity and countering spam

WP4 Service and application security

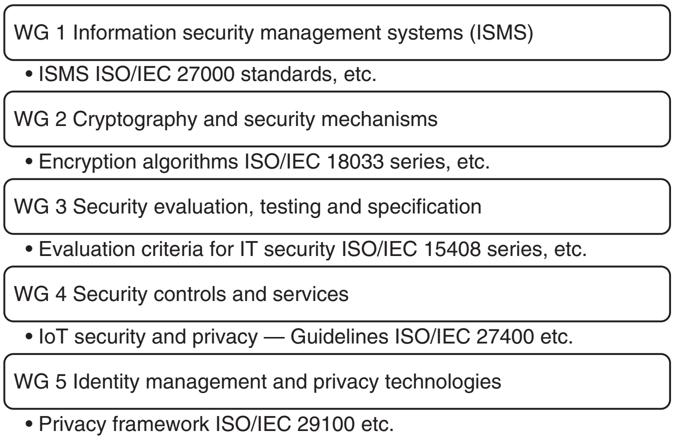
- Q7 Secure application services
- Q8 Cloud computing and Big data infrastructure security
- Q14 Distributed Ledger Technology (DLT) security

WP5 Fundamental security technologies

- Q10 Identity management and telebiometrics architecture and mechanisms
- Q11 Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications

5G: fifth-generation mobile communications network
IoT: Internet of Things
ITS: intelligent transport system
PKI: public key infrastructure

Fig. 1. Composition of WPs and Qs in ITU-T SG17 (as of writing).



WG 1 Information security management systems (ISMS)

- ISMS ISO/IEC 27000 standards, etc.

WG 2 Cryptography and security mechanisms

- Encryption algorithms ISO/IEC 18033 series, etc.

WG 3 Security evaluation, testing and specification

- Evaluation criteria for IT security ISO/IEC 15408 series, etc.

WG 4 Security controls and services

- IoT security and privacy — Guidelines ISO/IEC 27400 etc.

WG 5 Identity management and privacy technologies

- Privacy framework ISO/IEC 29100 etc.

Fig. 2. Areas of responsibility and representative standards of WGs in JTC 1/SC 27.

SG17 conducts technical discussions on all matters; however, there is no subcommittee corresponding to each international WP. (There is of course an assignment of responsibilities within the domestic committee.) There is also a domestic committee corresponding to JTC 1/SC 27, but this committee does not conduct technical studies. The technical discussions are primarily conducted by their domestic subcommittees, which range from WG 1 to WG 5, corresponding to each of the international WGs. Considering the aforementioned differences, namely the dynamic and static organizational structures of ITU-T SG17 and JTC 1/SC 27, it can be said that how the Japanese domestic committees are organized makes sense.

Regarding technical fields, ITU-T SG17 and JTC 1/SC 27 obviously share many common subjects, but there are also many subjects that complement each other. For example, in the area of public key cryptography, ITU-T SG17 defines the standard format and verification algorithms for the public key infrastructure (PKI), while JTC 1/SC 27 defines the cryptographic algorithms and digital signature schemes used in the PKI. Both are essential for the use of public key cryptography. Of course, there are many deeply related subjects regarding guidelines and frameworks for security management and network security; therefore, ITU-T SG17 and JTC 1/SC 27 have liaisons in both directions and work closely to promote their standardization activities.

4. Trends in security standardization

The larger numbered Qs in ITU-T SG17 are relatively new technologies. Examples include Q14 distributed ledger technology (DLT) and Q15 quantum key distribution (QKD). For DLT, a temporary body called ITU-T FG DLT (Focus Group on Application of Distributed Ledger Technology) was active from 2017 to 2019. The recommendations issued by the body have now been taken over by the respective SGs of ITU-T. JTC 1/SC 27 also discussed DLT for a while, and in 2016 a permanent body called ISO/TC (Technical Committee) 307 (Blockchain and DLTs) was established. This body is currently promoting the standardization of DLTs.

The situation is similar for quantum information technology, where a temporary body, ITU-T FG-QIT4N (Focus Group on Quantum Information Technology for Networks), was active from 2019 to 2021. In JTC 1/SC 27, the standardization of QKD is underway in WG 3, and ISO/IEC 23837 series, which defines implementation security requirements and evaluation methods for QKD, is expected to be published soon. However, quantum information technology covers a wide range of areas, certainly not restricted to QKD, and there is a view that a dedicated body is needed to handle the whole area (e.g., TC 307, which is devoted to handling DLT in general), and it is possible that a new permanent organization should be established within ISO/IEC in the future.

In addition to DLT and quantum information technology, another new technology is artificial intelligence (AI). It is not yet clear how AI security is going to be handled and standardized in these organizations.

Finally, I would like to mention post-quantum cryptography (PQC). It is believed that if a large-scale quantum computer is put into practical use, many current cryptographic algorithms, especially many of the public-key cryptographic algorithms, should become insecure. Therefore, there is an active movement to standardize cryptographic algorithms that can be used securely even if a large-scale quantum computer is put into practical use, i.e., quantum computer resistant cryptography. Technically speaking, we see that PQC is not part of quantum information technology but belongs to the conventional “electronic” information technology. In other words, PQC can be implemented and used on current electronic computers. One might have heard that the National Institute of Standards and Technology is running a competition for the standardization of PQC. Now that a part of the competition is over and the selection of cryptographic algorithms has progressed, WG 2 of JTC 1/SC 27 is accelerating its work on PQC. Rather than creating a new standard, at least initially, they plan to start standardization by amending to existing parts of standards or establishing new parts of existing standards. It is natural to expect that these renewed standards should then affect accordingly those set of ITU-T SG17 recommendations, which are related to public key cryptography.

Kan Yasuda

Principal Research Scientist, Head of Cryptography Research Group, Information Security Technology Project, NTT Social Informatics Laboratories.

He received a Ph.D. in mathematical sciences from the University of Tokyo in 2003. He has been working for NTT and involved in security standardization since 2004. He was the head of Delegate of Japan for JTC 1/SC 27/WG 2 from 2016 through 2020. He has been the vice chair of Japan ITU-T SG17 committee since 2022.