Closing remark for Webinar Series- Episode #9: Addressing the Security Risks of Digital Transformation on IoT

6 December 2021

Heung Youl YOUM

Chairman of ITU-T SG17

Professor, Soonchunhyang University

SG17 overview - Mission

- The mandate of SG17 was confirmed by WTSA-16.
- Mission
  - Building confidence and security in the use of information and communication technologies (ICTs) is one of the top priorities of the ITU (PP-Res. 130, WSIS Action Line C5).
  - New emerging technologies such as cloud computing, smart grid, ITS, 5G/Network 2030, SDN, NFV, Big Data analytics, DLT, AI/ML-enabled cybersecurity, QKD, Privacy, and IoT, need technical, organizational, and physical measures to protect assets for the applications and services.
  - New security approaches to adequately address emerging security threats need to be addressed.

SG17 overview - Major topics

SG17

SG17 as lead study group for security

Public key infrastructure

Decentralized Identity

Protection of Personally Identifiable Information (PII)

Operational and technical aspects for data protection

Quantum key distribution

AI/ML security

DLT security

IoT security

Security for 5G/6G

SG17 overview - Questions – LSG – JCAs – Projects

SG17 has 12 Questions announced by January 2021 TSAG meeting.

11 Restructured (of 14 existing) Questions

+

1 new Question, Emerging technologies security

SG17 should be the lead study group responsible for:

Languages and description techniques

IDENTITY MANAGEMENT

JCA-IdM and JCA-COP as well as ASN.1 & OID Projects need to continue given their important contributions.

Regional groups
SG17 regional group for Africa

SG17 regional group for Arab

SG17 Questions

- ❑ Q1/17 Security standardization strategy and coordination
- ❑ Q2/17 Security architecture and network security
- ❑ Q3/17 Telecommunication information security management and security services
- ❑ Q4/17 Cybersecurity and countering spam
- ❑ Q6/17 Security for telecommunication services and Internet of Things
- ❑ Q7/17 Secure application services
- ❑ Q8/17 Cloud computing and Big data infrastructure security
- ❑ Q10/17 Identity management and telebiometrics architecture and mechanisms
- ❑ Q11/17 Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications
- ❑ Q13/17 Intelligent transport system security
- ❑ Q14/17 Distributed Ledger Technology (DLT) security
- ❑ Q15/17 Security for/by emerging technologies including quantum-based security

SG17 IoT security work - general

SG17

Q6: Security for telecommunication services and Internet of Things

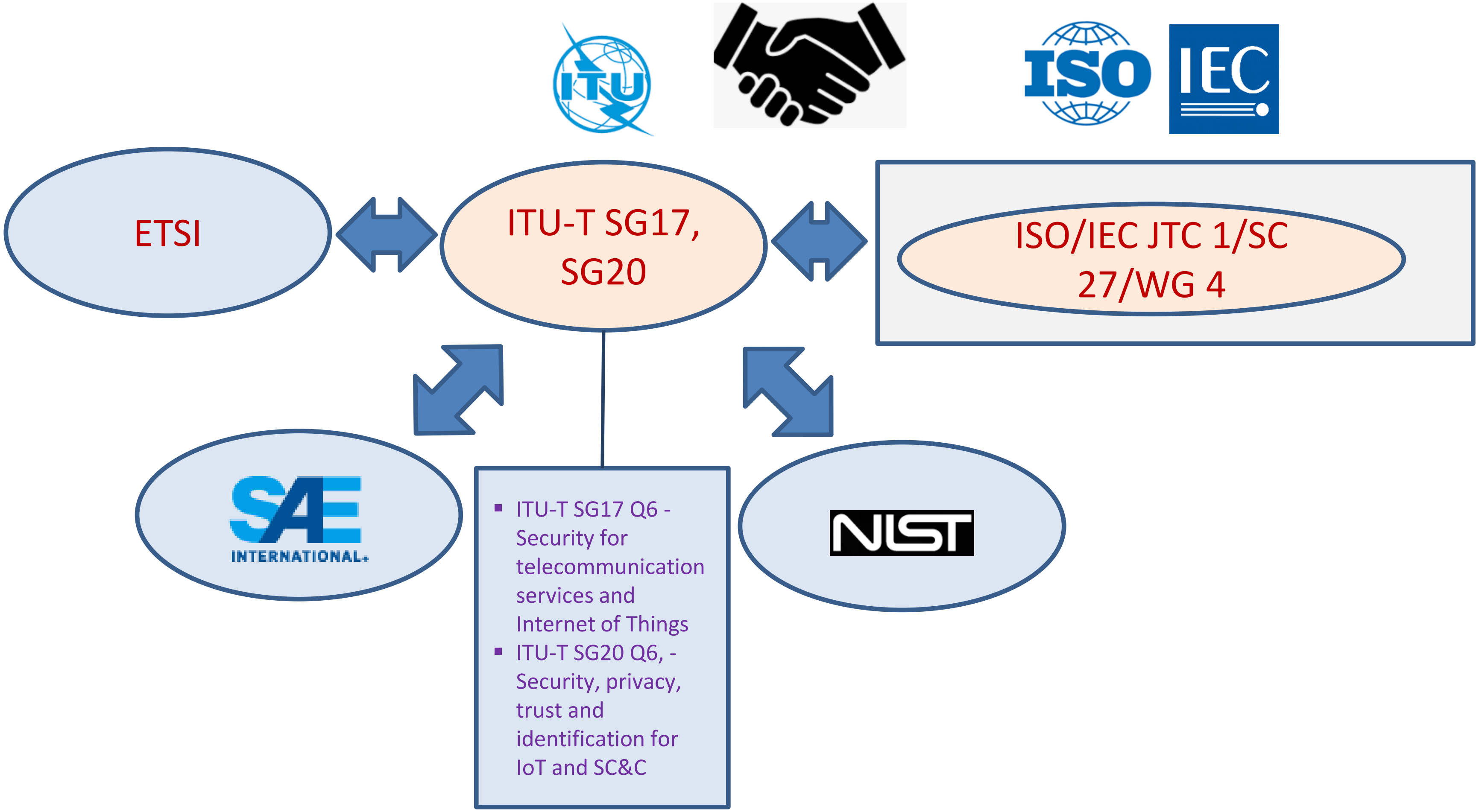
Published eight Recommendations

- X.1361 (ex X.iotsec-2), Security framework for the Internet of things based on the gateway model
- X.1362 (ex X.iotsec-1), Simple encryption procedure for Internet of things (IoT) environments
- X.1363 (ex X.iotsec-3), Technical framework of personally identifiable information (PII) handling system in Internet of things (IoT) environment
- X.1364 (ex X.nb-iot), Security requirements and framework for narrow band Internet of things
- X.1365 (ex X.ibc-iot), Security methodology for use of identity-based cryptography in support of Internet of Things (IoT) services over telecommunication networks
- X.1366 (ex X.amas-iot), Aggregate message authentication scheme for IoT environment
- X.1367 (ex X.elf-iot), Standard format for Internet of things (IoT) error logs for security incident operations
- X.1368 (ex X.secup-iot), Secure firmware/software update for Internet of things (IoT) devices

Texts under development (4)

- X.1369 (X.ssp-iot), Security requirements for IoT service platform
- X.iotsec-4 “Security requirements for IoT devices and gateway”
- X.ra-iot “Security risk analysis framework for IoT devices”
- X.sc-iot “Security controls for Internet of Things (IoT) systems”

SG17 IoT security work – global cooperation



ETSI

ITU-T SG17, SG20

ISO/IEC JTC 1/SC 27/WG 4

- ITU-T SG17 Q6 - Security for telecommunication services and Internet of Things
- ITU-T SG20 Q6, - Security, privacy, trust and identification for IoT and SC&C

Concluding remarks

- ❑ Security standard work should be coordinated across ITU-T SGs with other SDOs.
- ❑ Security by design/privacy by design should be applied for IoT devices, network connected devices.
- ❑ Controls or measures for IoT devices and applications should be defined based on threats and risks using a general risk-based approach.
- ❑ International standards developed by ITU-T should be used when there is a need for security certification for IoT devices and applications.
- ❑ IoT certification should be expanded to include all IoT consumer devices, equipment and systems.
- ❑ Global mutual recognition for IoT certification is needed.

SAFE : Security is Absolutely First Everywhere

Thank you very much

for your attention!