5G Security in ITU-T SG17

Xiaoya Yang
Counsellor of ITU-T SG17 ‘Security’
@ETSI Security Week 2018
2018.6.13
About ITU

ITU is the United Nations specialized agency for information and communication technologies (ICTs)

Founded in Paris in 1865 as the International Telegraph Union

More than 150 years of experience and innovation
ITU members

193 **Member States** and Regulatory Bodies

700+ **Companies**, Business Associations, NGOs

150+ **Universities** & Research Establishments
Membership sectors

Staff Bureaus
(Each Bureau below consists of ITU Staff and one elected official as a Director)

- BR
- BDT
- TSB

Members

- ITU Radiocommunication Sector (ITU-R)
- ITU Development Sector (ITU-D)
- ITU Standardization Sector (ITU-T)

ITU General Secretariat
(The general secretariat consists of ITU staff and two elected officials as deputy Secretary General and Secretary General)
ITU-T standardization work is carried out by the technical Study Groups (SGs) in which representatives of the ITU-T membership develop consensus based Recommendations (standards) for the various fields of international telecommunications.

- **SG2 - Operational aspects**
- **SG3 - Economic and policy issues**
- **SG5 - Environment and climate change**
- **SG9 - Broadband cable and TV**
- **SG11 - Protocols and test specifications**
- **SG20 - IoT and its applications including smart cities and Communities**
- **SG12 - Performance, QoS and QoE**
- **SG13 - Future networks with a focus on IMT-2020, Cloud & Big Data**
- **SG15 - Transport, Access and Home**
- **SG16 - Multimedia**
- **SG17 - Security**
Strategic Vision for ITU-T SG17 in study period 2017-2020

- A center of security competence with more participation from ITU membership
- Study new emerging areas and produce high quality technical Recommendations
- Increase collaboration/cooperation with other international organizations

ITU-T Study Group 17 is responsible for building confidence and security in the use of information and communication technologies (ICT).
## ITU-T SG17 Structure

<table>
<thead>
<tr>
<th>Question No.</th>
<th>Question Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td>Telecommunication/ICT security coordination</td>
</tr>
<tr>
<td>2/17</td>
<td>Security architecture and framework</td>
</tr>
<tr>
<td>3/17</td>
<td>Telecommunication information security management</td>
</tr>
<tr>
<td>4/17</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>5/17</td>
<td>Countering spam by technical means</td>
</tr>
<tr>
<td><strong>6/17</strong></td>
<td><strong>Security aspects of telecommunication services, networks and Internet of Things</strong></td>
</tr>
<tr>
<td>7/17</td>
<td>Secure application services</td>
</tr>
<tr>
<td>8/17</td>
<td>Cloud computing security</td>
</tr>
<tr>
<td>9/17</td>
<td>Telebiometrics</td>
</tr>
<tr>
<td>10/17</td>
<td>Identity management architecture and mechanisms</td>
</tr>
<tr>
<td>11/17</td>
<td>Generic technologies (Directory, PKI, PMI, ASN.1, OIDs) to support secure applications</td>
</tr>
<tr>
<td>12/17</td>
<td>Formal languages for telecommunication software and testing</td>
</tr>
<tr>
<td>13/17</td>
<td>Security aspects for Intelligent Transport System</td>
</tr>
<tr>
<td>14/17</td>
<td>Security aspects for Distributed Ledger Technologies</td>
</tr>
</tbody>
</table>

Q6 is the leading Question for 5G security in SG17
Activities related to 5G Security in SG17 (1)

- **Q2/17 (Security architecture and framework)**
  - network aspects including SDN for 5G security
    - X.SDsec: Guideline on software-defined security in SDN/NFV network
    - X.sdnsec-3: Security guideline of Service Function Chain based on SDN
    - X.ssc: Security Service Chain Architecture
    - X.srnv: Security Requirements of Network Virtualization

- **Q6/17 (Security aspects of telecommunication services, networks and IoT)**
  - mobile and infrastructure (including IoT) aspects for 5G security
    - X.1362 (2017): Simple encryption procedure for IoT
    - X.sdnsec-1: Security services using SDN
    - X.5Gsec-q: Security guidelines for applying quantum-safe algorithms in 5G systems
    - X.ssp-iot: Security requirements and framework for IoT service platform
    - X.iotsec-3: Technical framework of PII handling system in IoT environment
    - X.secup-iot: Secure Software Update Procedure for IoT Devices
    - X.nb-iot: Security Requirements and Framework for Narrow Band Internet of Things
    - X.ibc-iot: Security Requirements and Framework of Using Identity-Based Cryptography Mechanism in IoT
Activities related to 5G Security in SG17 (2)

• Q7/17 (Secure application services)
  – application/service aspects for 5G security
  – X.srfb: Security requirements and framework for big data analytics in mobile internet services

• Q8/17 (Cloud Computing Security)
  – Cloud computing and big data infrastructure for 5G security
  – X.sgtBD: Security guidelines of lifecycle management for telecom big data
  – X.sgBDIP: Security guidelines for big data infrastructure and platform
  – X.SRIaaS: Security requirements of public infrastructure as a service (IaaS) in cloud computing
  – X.SRNaaS: Security requirements of network as a service (NaaS) in cloud computing

• Q11/17 (Generic technologies to support secure applications)
  – cryptographic profiles for 5G security
  – X.509, etc
  – X.orf-gs: OID-based resolution framework for IoT group services
ITU Workshop on 5G Security
19 March 2018

- 125 participants
- Speakers from Nokia, KT, China Mobile, KAIST Huawei, TNO, Trialog, Horst Görtz Institute, King’s College London.
5G end-to-end Security Framework

**UE Security**
- Malwares
- Side channel attacks
- Zombies
- ...

**Access Network Security**
- Air Interface security
- Fronthaul & Backhaul security
- MEC security
- SDN/NFV security
- Cloud security
- ...

**Core Network Security**
- Network capability exposure security
- Internetworking security
- SBA security
- Network slicing security
- SDN/NFV security
- Cloud security
- ...

**Service/Application Security**
- Service security (traditional/verticals)
- Big Data security
- Web security
- Cloud security
- Information security
- ...

**Generic Security Enablers**
- Cryptography (incl. Quantum-safe Cryptography)
- Security situation awareness
- Security emergency response
- IDM
- PKI
- DLT (?)
- AI/ML
- Authentication technologies (incl. biometrics)
- Threat intelligence handling
- Security testing and certification
Study Topics ongoing on 5G security in ITU-T SG17

- X.5Gsec-q: Security guidelines for applying quantum-safe algorithms in 5G systems
  - To give a complete security assessment on 5G systems when commercial quantum computers are available
  - To introduce the usage of the quantum-safe symmetric algorithms, and the quantum-safe asymmetric algorithms in 5G systems
  - To align the security levels between quantum-safe symmetric algorithms and quantum-safe asymmetric algorithms
Potential Study Topics on 5G security in ITU-T SG17 (1)

• Understanding differences between 5G and previous generations
  – New ecosystem, new trusted model, security framework/architecture

• New security threats specific to 5G and their impacts
  – Revisit cyber attacks in the context of major 5G scenarios
  – Threats from quantum computers

• New security requirements of 5G
  – Battery-efficiency, energy-saving security mechanisms
  – Ultra reliable and low latency security mechanisms
Potential Study Topics on 5G security in ITU-T SG17 (2)

• New security solutions for 5G
  – Authentication, data protection scheme
  – Global PKI, or optimization of PKI
  – Network slicing, mobile edge computing

• Other security aspects of 5G system
  – Utilize exposed 5G network capabilities for security purposes
  – Security assurance and multi-layer security certification
  – Security management automation aspects using AI and machine learning
  – Reference implementations or best practices
Next steps for 5G security in ITU-T SG17

• Identify specific security issues in the context of 5G which SG17 can work on, design a roadmap for 5G security study and standardization in SG17
• Agree on an initial roadmap for 5G security study and standardization in SG17, and identify gaps for SG17 to study in the area of 5G security standardization
• Assign new contributions in this area, establish some initial work items, and solicit more contributions in this area
• Establish/maintain the liaison relationship in this area with related groups, such as ETSI, 3GPP SA3, NGMN, GSMA, IETF, OASIS, etc

ITU-T SG17 welcomes the feedback and involvement from ETSI
 شكرا
谢谢
Thank you
Merci
Спасибо
Gracias
<table>
<thead>
<tr>
<th>Standardization Body</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETSI</td>
<td>7</td>
</tr>
<tr>
<td>IEEE</td>
<td>110</td>
</tr>
<tr>
<td>NGMN</td>
<td>18</td>
</tr>
<tr>
<td>ITU-R</td>
<td>1</td>
</tr>
<tr>
<td>ITU-T SG11</td>
<td>36</td>
</tr>
<tr>
<td>ITU-T SG13</td>
<td>18</td>
</tr>
<tr>
<td>ITU-T SG17</td>
<td>17</td>
</tr>
<tr>
<td>ITU-T SG20</td>
<td>3</td>
</tr>
</tbody>
</table>

Results: 203 found(s)

- **IEEE 1609.2-2016**
  - **Subject:** IEEE Standard for Wireless Access in Vehicular Environments -- Security Services for Applications and Management Messages
  - **Responsible group:** IEEE
  - **Topic(s):** Wireless; IMT-2020

- **IEEE 1609.2a-2017 (Amendment to IEEE Std 1609.2-2016)**
  - **Subject:** IEEE Standard for Wireless Access in Vehicular Environments -- Security Services for Applications and Management Messages -- Amendment 1
  - **Responsible group:** IEEE
  - **Topic(s):** IMT-2020

- **IEEE 1609.3-2016**
  - **Subject:** IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services
  - **Responsible group:** IEEE
  - **Topic(s):** IMT-2020

- **IEEE 1609.4-2016**
  - **Subject:** IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation
  - **Responsible group:** IEEE
### Results: 43 found(s)

<table>
<thead>
<tr>
<th>ITU-T Y.4114 (07/2017)</th>
<th>Subject: Specific requirements and capabilities of the Internet of things for big data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Responsible group: 20</td>
</tr>
<tr>
<td></td>
<td>Topic(s): IMT-2020</td>
</tr>
<tr>
<td></td>
<td>... Numbering, addressing and naming Y.500–Y.599 Operation, administration and maintenance Y.600–Y.699 Security Y.700–Y.799 Performance Y.800–Y.899 INTERNET PROTOCOL ASPECTS General Y.1...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TS 24.502</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject: Access to the 3GPP 5G System (5GS) via non-3GPP access networks; Stage 3</td>
</tr>
<tr>
<td>Responsible group: 3GPP TSG CT1</td>
</tr>
<tr>
<td>Topic(s): IMT-2020</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ITU-T Y.3110 (09/2017)</th>
<th>Subject: IMT-2020 Network Management and Orchestration Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Responsible group: ITU-T SG13</td>
</tr>
<tr>
<td></td>
<td>Topic(s): IMT-2020</td>
</tr>
<tr>
<td></td>
<td>...he status and events of the instantiated slice resources for the purpose of fault, performance, and security management. ☐ The IMT-2020 Slice Lifecycle Management is required to manage the lifecycle of the ma...</td>
</tr>
</tbody>
</table>

| ITU-T Y.IMT2020-reqts (under study) |