Updates:
ITU-T Study Group 17
Standardization of “Security”
SG17 Responsibility & mandates
WTSA-16 approved the role of SG17:

- ITU-T Study Group 17 - Security

ITU-T Study Group 17 is responsible for building confidence and security in the use of information and communication technologies (ICT). This includes studies relating to cybersecurity, security management, countering spam and identity management. It also includes security architecture and framework, protection of personally identifiable information, and security of applications and services for the Internet of things (IoT), smart grid, smartphone, software-defined networking (SDN), Internet Protocol television (IPTV), web services, social network, cloud computing, big data analytics, mobile financial system and telebiometrics.

Study Group 17 is also responsible for the application of open system communications, including directory and object identifiers, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems, test specification languages in support of conformance testing to improve the quality of Recommendations.
SG17 Lead study responsibilities
WTSA-16 assigned the LSG responsibilities of SG17:

- Security
- Identity management (IdM)
- Languages and description techniques

A lead study group is responsible for the study of the appropriate core Questions.
In addition, in consultation with the relevant study groups and in collaboration, where appropriate, with other standards bodies, the lead study group has the responsibility to define and maintain the overall framework and to coordinate, assign (recognizing the mandates of the study groups) and prioritize the studies to be carried out by the study groups, and to ensure the preparation of consistent, complete and timely Recommendations.
<table>
<thead>
<tr>
<th>Chairman</th>
<th>Heung Youl YOUM</th>
<th>Korea (Republic of)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice-Chairmen (9)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mr. Y. Miyake</td>
<td>Japan</td>
<td></td>
</tr>
<tr>
<td>Ms. I. Furey</td>
<td>The United States</td>
<td></td>
</tr>
<tr>
<td>Mr. V. Dolmatov</td>
<td>Russian Federation</td>
<td></td>
</tr>
<tr>
<td>Mr. G. LIN</td>
<td>P.R. China</td>
<td></td>
</tr>
<tr>
<td>Mr. P-K. Kettin-Zanga</td>
<td>Central African Republic</td>
<td></td>
</tr>
<tr>
<td>Ms. W. Latrous</td>
<td>Tunisia (Republic of)</td>
<td></td>
</tr>
<tr>
<td>Mr. Mohamed M.K. ELHAJ</td>
<td>Sudan</td>
<td></td>
</tr>
<tr>
<td>Mr. G. Evren</td>
<td>Turkey</td>
<td></td>
</tr>
<tr>
<td>Mr. H.D. Miguel</td>
<td>Argentina</td>
<td></td>
</tr>
</tbody>
</table>
WTSA-16 confirmed the 12 Questions of SG17:

<table>
<thead>
<tr>
<th>Question number</th>
<th>Question title</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td>Telecommunication/ICT security coordination</td>
<td>Continuation of Q1/17</td>
</tr>
<tr>
<td>2/17</td>
<td>Security architecture and framework</td>
<td>Continuation of Q2/17</td>
</tr>
<tr>
<td>3/17</td>
<td>Telecommunication information security management</td>
<td>Continuation of Q3/17</td>
</tr>
<tr>
<td>4/17</td>
<td>Cybersecurity</td>
<td>Continuation of Q4/17</td>
</tr>
<tr>
<td>5/17</td>
<td>Countering spam by technical means</td>
<td>Continuation of Q5/17</td>
</tr>
<tr>
<td>6/17</td>
<td>Security aspects of telecommunication services and networks</td>
<td>Continuation of Q6/17</td>
</tr>
<tr>
<td>7/17</td>
<td>Secure application services</td>
<td>Continuation of Q7/17</td>
</tr>
<tr>
<td>8/17</td>
<td>Cloud computing security</td>
<td>Continuation of Q8/17</td>
</tr>
<tr>
<td>9/17</td>
<td>Telebiometrics</td>
<td>Continuation of Q9/17</td>
</tr>
<tr>
<td>10/17</td>
<td>Identity management architecture and mechanisms</td>
<td>Continuation of Q10/17</td>
</tr>
<tr>
<td>11/17</td>
<td>Generic technologies (Directory, Public-Key Infrastructure (PKI), Public-Key Infrastructure (PKI), Abstract Syntax Notation 1 (ASN.1), Object Identifiers (OIDs)) to support secure applications</td>
<td>Continuation of Q11/17</td>
</tr>
<tr>
<td>12/17</td>
<td>Formal languages for telecommunication software and testing</td>
<td>Continuation of Q12/17</td>
</tr>
</tbody>
</table>
Draft new SG17 structure

- **Q1/17** Telecommunication/ICT security coordination

  **Working Party 1 “Telecommunication/ICT Security”**
  - **Q2/17** Security architecture and framework
  - **Q3/17** Telecommunication information security management
  - **Q6/17** Security aspects of telecommunication services and networks

- **Working Party 2 “Cyberspace security”**
  - **Q4/17** Cybersecurity
  - **Q5/17** Countering spam by technical means

- **Working Party 3 “Application security”**
  - **Q7/17** Secure application services
  - **Q8/17** Cloud computing security
  - **Q12/17** Formal languages for telecommunication software and testing

- **Working Party 4 “Identity management and authentication”**
  - **Q9/17** Telebiometrics
  - **Q10/17** Identity management architecture and mechanisms
  - **Q11/17** Generic technologies to support secure applications

**ITU-T Study Group 17**
Security
Recommendations related to ITS:
1) Draft Recommendation ITU-T X.1373 (X.itssec-1) → No change
2) Draft Recommendation ITU-T X.itssec-2 → Discussed at the interim meeting. No progress.
3) Proposal for a new question on ITS
Draft Recommendation ITU-T X.1373 (X.itssec-1)

- Secure software update capability for intelligent transportation system communications devices
  (Status: 2016-09/ Determined (now in TAP consultation process))

- **Scope:**
  - In the context of updates of software modules in the electric devices of vehicles in the intelligent transportation system (ITS) communication environment, **this Recommendation aims to provide a procedure of secure software updating for ITS communication devices for the application layer.** This includes a basic model of software update, its threat and risk analysis, security requirements and controls for software update and a specification of abstract data format of update software module.
  - **The procedure related to in-vehicle communication is the out of scope of this Recommendation.** For reference, the procedure used in-vehicle in this Recommendation is informative.
  - The procedure is intended to be applied to communication devices on ITS vehicles under vehicle-to-infrastructure (V2I) communication by means of the Internet and/or ITS dedicated networks. The procedure can be practically utilized by car manufactures and ITS-related industries as a set of standard secure procedures and security controls.
General Model for a remote software update in Draft Rec. ITU-T X.1373 (X.itssec-1)
Ref: TSB Circular 246
SG17/MEU

Tel: +41 22 730 5866
Fax: +41 22 730 5853
E-mail: tsbsg17@itu.int

Geneva, 28 November 2016

To:
- Administrations of Member States of the Union

Copy to:
- ITU-T Sector Members;
- ITU-T Associates;
- ITU Academia;
- The Chairman and Vice-Chairmen of ITU-T Study Group 17;
- The Director of the Telecommunication Development Bureau;
- The Director of the Radiocommunication Bureau

Subject: Meeting of ITU-T Study Group 17, 22-30 March 2017, Geneva, with a view to approving draft Recommendations ITU-T X.1058 (X.gpim), X.1080.0 (X.pba-ct), X.1126 (X.msec-11), X.1212 (X.cogent), X.1362 (X.iotsec-1), X.1373 (X.itssec-1), and X.1550 (X.nessa) in accordance with the provisions of Resolution 1, Section 9, of WTSA (Rev. Dubai 2012)

Deadline: 13 March
Draft Recommendation ITU-T X.itssec-2

- **Security guidelines for V2X communication systems**
  
  *(Timing: 2017-10 / Determination)*

  - Provides security guidelines for V2X communication systems. V2X means Vehicle-to-Vehicle (V2V), V2I (Vehicle-to-Infrastructure) and/or V2N (Vehicle-to-Nomadic Devices)

  - Includes analysis of threat and vulnerability for V2X communication systems

  - Provides the security requirements for V2X communication systems

Overview of the vehicular communication, in Draft Rec. ITU-T X.itssec-2
Content of X.itssec-2

1. Scope
2. References
3. Definitions
3.1 Terms defined elsewhere
3.2 Terms defined in this Recommendation
4. Abbreviations and acronyms
5. Conventions
6. Overview of the vehicular communication
7. Analysis on threat and vulnerability
7.1. V2V perspective
7.2. V2I perspective
7.3. V2N perspective
8. Security requirements
8.1. V2V perspective
8.2. V2I perspective
8.3. V2N perspective
9. Use cases for V2X security system
9.1. Vehicle registration service model
9.2. V2X entity authentication service model
9.3. V2X message confidentiality service model
9.4. TBD
Bibliography

This draft Recommendation will be actively discussed at the next SG17 meeting (March 22-30).
Title:
Proposal for a new Question on Security aspects for Intelligent Transport System

Rationales for a new Question on security aspects for ITS
• Having a new Question on security aspects for ITS in SG17 has following advantages:
  • Attracting much more participation from global car makers;
  • Accelerating to work on ITS security work (e.g., mechanisms and protocols for ITS security) in SG17 to meet the market needs;
  • Providing clear visibility of ITS security work, inside and outside ITU;
  • Providing a focal point for collaboration on ITS security with other relevant organizations; and
  • Making a centre of competence of ITS security, within ITU and across the world.

Proposal
It is proposed to establish a new Question on security aspects for ITS under ITU-T SG17 with the proposed question text given in Annex A, and to delete text related to ITS work in the description of Question 6/17, in the case there is agreement to create the new Question.
Future works in SG17 on ITS

- Confirm the result of TAP consultation on X.itssec-1;
- Improve the draft Rec. X.itssec-2;
- Discuss for establishing a new question for ITS security;
- Collaboration with related SDOs on ITS;
  - In ITU-T, SG16, CITS
  - Outside ITU-T, ISO/TC204, ISO/TC22
    (On 21 March, a meeting with a chair of TC204 (Dick Schnacke) and WG18 chair (Hans-Joachim Schade) is planned for collaboration.)
  - Vehicle companies, OEM vendors, etc.
- Roadmap of ITS security Recommendations to be developed in SG17 should be prepared.
Thank you for listening

Implement & use Security *

Design Security *

Monitor & review Security *

Maintain & improve Security *