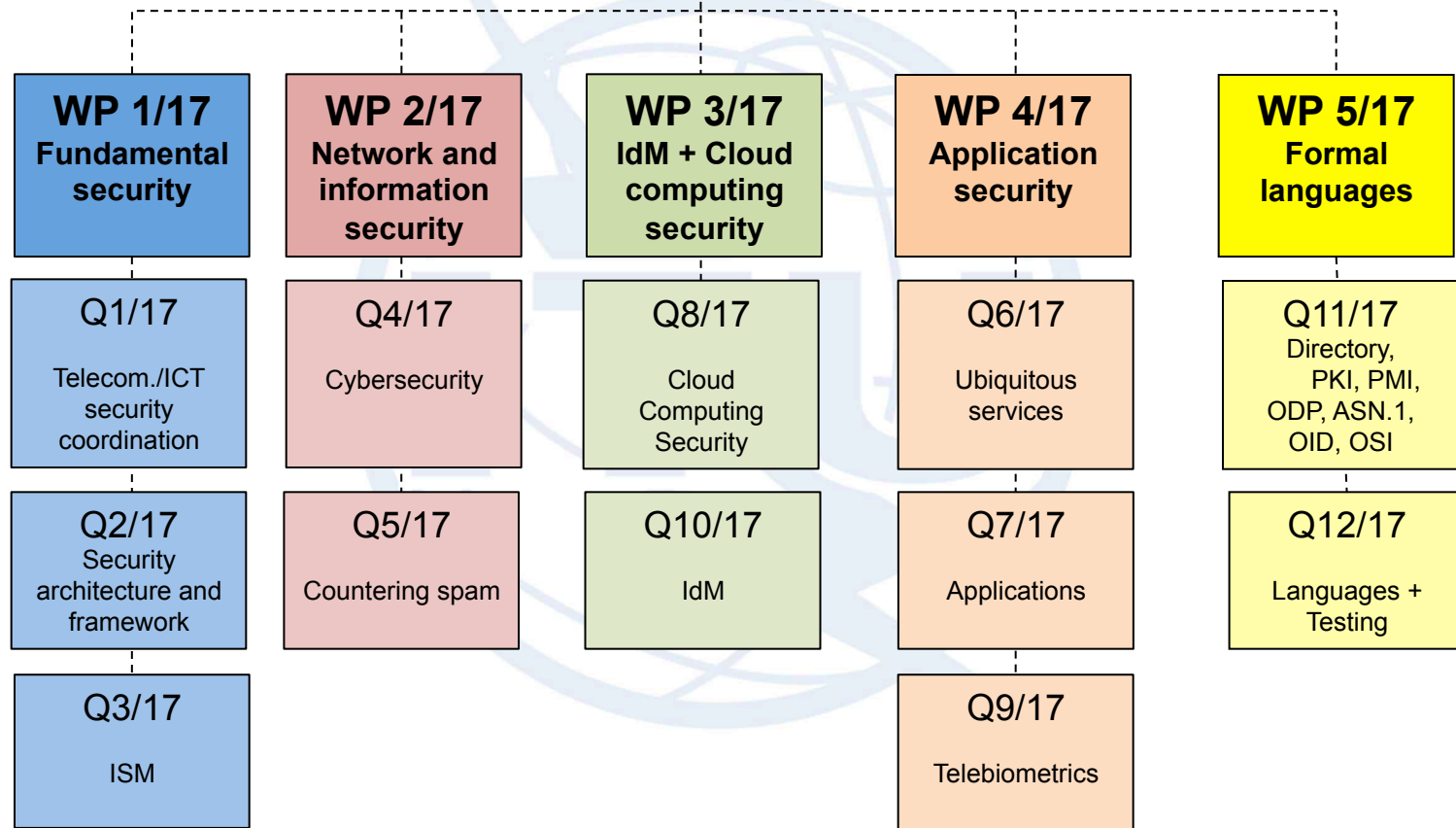# Study Group 17 (Security)

ITU Sector of Standardization (ITU-T)

Vasily Dolmatov

ITU-T Study Group 17 Overview

- Primary focus is to build confidence and security in the use of Information and Communication Technologies (ICTs)

- Meets twice a year. Last meeting had 160 participants from 33 Member States, 17 Sector Members, 2 Associates, and 2 Academia.

- Large program of work:

  - 11 new work items added to work program in 2015
  - Results of September 2015 meeting:
    approval of 3 Recommendations, 1 Amendment;
    6 Recommendations in TAP; 14 Recommendations (1 new, 12 revised, 1 corrigendum) consented.
  - 93 new or revised Recommendations and other texts are currently under development

- Work organized into 5 Working Parties with 12 Questions

- 4 Correspondence groups,
  5 interim Rapporteur groups meetings took place.

- See SG17 web page for more information
  http://itu.int/ITU-T/go/sg17

ITU-T SG17, Security

WP 1/17 **Fundamental security**	WP 2/17 **Network and information security**	WP 3/17 **IdM + Cloud computing security**	WP 4/17 **Application security**	WP 5/17 **Formal languages**
Q1/17 Telecom./ICT security coordination	Q4/17 Cybersecurity	Q8/17 Cloud Computing Security	Q6/17 Ubiquitous services	Q11/17 Directory, PKI, PMI, ODP, ASN.1, OID, OSI
Q2/17 Security architecture and framework	Q5/17 Countering spam	Q10/17 IdM	Q7/17 Applications	Q12/17 Languages + Testing
Q3/17 ISM			Q9/17 Telebiometrics	

SG17, Working Party Structure

- **WP 1 "Fundamental security"**   **Chairman: Koji NAKAO**
  - Q1/17   Telecommunication/ICT security coordination
  - Q2/17   Security architecture and framework
  - Q3/17   Telecommunication information security management

- **WP 2 "Network and information security"**   **Chairman: Sacid SARIKAYA**
  - Q4/17   Cybersecurity
  - Q5/17   Countering spam by technical means

- **WP 3 "Identity management and cloud computing security"**   **Chairman: Heung Youl YOUM**
  - Q8/17   Cloud computing security
  - Q10/17 Identity management architecture and mechanisms

- **WP 4 "Application security"**   **Chairman: Antonio GUIMARAES**
  - Q6/17   Security aspects of ubiquitous telecommunication services
  - Q7/17   Secure application services
  - Q9/17   Telebiometrics

- **WP 5 "Formal languages"**   **Chairman: George LIN**
  - Q11/17 Generic technologies to support secure applications
  - Q12/17 Formal languages for telecommunication software and testing

ITU-T Joint Coordination Activity on Identity Management (JCA-IdM)

- Coordinates the ITU-T identity management (IdM) work.
- Ensures that the ITU-T IdM work is progressed in a well-coordinated way between study groups, in particular with SG2, SG13, SG15, SG16, and SG17.
- Acts as a point of contact within ITU-T and with other SDOs/Fora on IdM in order to avoid duplication of work and assist in implementing the IdM tasks
- In carrying out the JCA-IdM's external collaboration role, representatives from other relevant recognized SDOs/Fora and regional/national organizations may be invited to join the JCA-IdM.
- Maintains [IdM roadmap and landscape document/WIKI](#).

Question 2/17
Security Architecture and Framework

- Responsible for general security architecture and framework for telecommunication systems

- In this study period, Q2/17 has developed one new Recommendation (X.1037), and one new supplement (X.Suppl.23).

- Recommendations currently under study include:

  - **X.gsiiso,** Guidelines on security of the individual information service for operators

  - **X.sdnsec-2**, Security requirements and reference architecture for Software-Defined Networking

  - **X.tigsc**, Technical implementation guidelines for ITU-T X.805

  - **X.sgmvno,** ITU-T X.805 – Supplement on Security guideline for mobile virtual network operator (MVNO)

- Relationships with ISO/IEC JTC 1 SCs 27 and 37, IEC TC 25, ISO TC 12, IETF, ATIS, ETSI, 3GPP, 3GPP2

Question 3/17
Telecommunication information security management

- Responsible for information security management - X.1051, etc.
- Developing specific guidelines including:
  - **X.1051 (revised)**, Information technology – Security techniques – Information security management guidelines for telecommunications based on ISO/IEC 27002
  - **X.gpim,** Code of practice for personally identifiable information protection(common text with ISO/IEC 29151)
  - **X.sgsm**, Information security management guidelines for small and medium telecommunication organizations
  - **X.sup-gisb,** ITU-T X.1054 – Supplement on Best practice for implementation of Rec. ITU-T X.1054 | ISO /IEC 27014 on governance of information security
  - **X.sup-gpim**, ITU-T X.gpim - Supplement on Code of practice for personally identifiable information protection based on ITU-T X.gpim
- Close collaboration with ISO/IEC JTC 1/SC 27

Question 4/17
Cybersecurity

- Recommendation in TAP approval process
  - **X.1521 (revised, X.cvss)**, Common vulnerability scoring system 3.0

- Recommendations on CYBEX currently under study include:
  - **X.1500 Amd.9,** Overview of cybersecurity information exchange – Amendment 9 - Revised structured cybersecurity information exchange techniques
  - **X.nessa,** Access control models for incidents exchange networks
  - **X.simef,** Session information message exchange format (SIMEF)

- Recommendations (non-CYBEX) currently under study include:
  - **X.cogent,** Design considerations for improved end-user perception of trustworthiness indicators
  - **X.samtn**, Security assessment techniques in telecommunication/ICT networks
  - **X.sbb**, Security capability requirements for countering smartphone-based botnets

- In this study period, Q4/17 has developed eight new Recommendations (X.1208, X.1210, X.1211, X.1303*bis,*, X.1525, X.1544, X.1546, X.1582), 2 revised Recommendations (X.1520, X.1526), six new Amendments (X.1500 Amds.3-8), 2 new supplements (X.Suppl.18, X.Suppl.20), and 1 revised supplement (X.Suppl.10).

Question 5/17
Countering spam by technical means

- Lead group in ITU-T on countering spam by technical means in support of WTSA-12 Resolution 52 (Countering and combating spam)

- In this study period, Q5/17 has developed 1 new Recommendation (X.1246), and one Corrigendum (X.1243 Cor.1):

- Recommendations currently under study include:
  - **X.1247 (X.tfcmm),** Technical framework for countering mobile messaging spam
  - **X.cspim,** Technical requirements for countering instant messaging spam (SPIM)
  - **X.gcsfmpd**, ITU-T X.1231 – Supplement on guidance of countering spam for mobile phone developers
  - **X.gcspi**, ITU-T X.1242 – Supplement on Guideline for countermeasures against short message service (SMS) phishing incidents
  - **X.ticsc**, ITU-T X.1245 – Supplement on Technical measures and mechanism on countering the spoofed call in the visited network of VoLTE

- Effective cooperation with ITU-D, IETF, ISO/IEC JTC 1, 3GPP, OECD, M3AAWG, ENISA and other organizations

Question 8/17
Cloud computing security

- In this study period, Q8/17 has developed
  2 new Recommendations (X.1601, X.1631),
  and one revised Recommendation (X.1601).
- Recommendations currently under study include:
  - Security aspects of cloud computing
    - **X.CSCDataSec,** Guidelines for cloud service customer data security
    - **X.dsms**, Data security requirements for the monitoring service of cloud computing
    - **X.1642 (X.goscc),** Guidelines for the operational security of cloud computing
  - Security aspects of service oriented architecture
    - **X.1602 (X.sfcsc),** Security requirements for software as a service application environments

- Working closely with ITU-T SG13, ISO/IEC JTC 1/SCs 27 and 38, and Cloud Security Alliance on cloud computing

Question 10/17
Identity Management (IdM)

- In this study period, Q10/17 has developed 1 new Recommendation (X.1255).

- Recommendations under development:
  - **X.1256 (X.authi),** Guidelines and framework for sharing network authentication results with service applications
  - **X.1257 (X.iamt),** Identity and access management taxonomy
  - **X.eaaa,** Enhanced entity authentication based on aggregated attributes

- Engagement
  - JCA-IdM
  - Related standardization bodies: ISO/IEC JTC 1 SCs 6, 27 and 37; IETF; ATIS; ETSI INS ISG, OASIS; Kantara Initiative; OMA; NIST; 3GPP; 3GPP2; Eclipse; OpenID Foundation; OIX; etc.

Question 6/17
Security aspects of ubiquitous telecommunication services

- Responsible for multicast security, home network security, mobile security, networked ID security, IPTV security, ubiquitous sensor network security, intelligent transport system security, and smart grid security.

- In this study period, Q6/17 has developed 2 new Recommendations (X.1198, X.1314), 2 technical corrigenda (X.1311 Cor.1, X.1314 Cor.1), and 2 new supplements (X.Suppl.19, X.Suppl.24).

- Recommendations currently under study include:
    - **X.iotsec-1,** Simple encryption procedure for Internet of Things (IoT) environments
    - **X.iotsec-2**, Security framework for Internet of Things
    - **X.itssec-1,** Software update capability for ITS communications devices
    - **X.itssec-2,** Security guidelines for V2X communication systems
    - **X.msec-9**, Functional security requirements and architecture for mobile phone anti-theft measures
    - **X.sdnsec-1**, Requirements for security services based on software-defined networking
    - **X.sgsec-1,** Security functional architecture for smart grid services using telecommunication network
    - **X.sgsec-2**, Security guidelines for home area network devices in smart grid systems

- Close relationship with JCA-IPTV and ISO/IEC JTC 1/SC 6/WG 7

Question 7/17
Secure application services

- Responsible for web security, security protocols, peer-to-peer security
- In this study period, Q7/17 has developed 8 new Recommendations (X.1144, X.1154, X.1155, X.1156, X.1157, X.1158, X.1159, X.1163), and 2 new supplements (X.Suppl.21, X.Suppl.22).

- Recommendations currently under study include:
  - **X.websec-6**, Security framework and requirements for open capabilities of telecommunication services
  - **X.websec-7**, Reference monitor for online analytics services
  - **X.websec-8,** Security protection guidelines for value-added services for telecommunication operator

- Relationships include: OASIS, OMA, W3C, ISO/IEC JTC 1/SC 27, Kantara Initiative

Question 9/17
Telebiometrics

- In this study period, Q9/17 has developed 1 new Recommendation (X.1092).

- Recommendations under development:
  - **X.bhsm,** Information technology – Security Techniques – Telebiometric authentication framework using biometric hardware security module
  - **X.pbact,** Privacy-based access control in telebiometrics
  - **X.tam,** A guideline to technical and operational countermeasures for telebiometric applications using mobile devices
  - **X.th-series,** e-Health and world-wide telemedicines
    - **X.th2,** Telebiometrics related to physics
    - **X.th3,** Telebiometrics related to chemistry
    - **X.th4,** Telebiometrics related to biology
    - **X.th5,** Telebiometrics related to culturology
    - **X.th6,** Telebiometrics related to psychology
    - **X.th13,** Holosphere to biosphere secure data acquisition and telecommunication protocol

- Close working relationship with ISO/IEC JTC 1/SCs 17, 27 and 37, ISO TCs 12, 68 and 215, IEC TC 25, IETF, IEEE

Question 11/17
Generic technologies to support secure applications

- Q11/17 consists of four main parts:
  - X.500 directory, Public-Key Infrastructure (PKI), Privilege Management Infrastructure (PMI)
  - Abstract Syntax Notation 1 (ASN.1), Object Identifier (OID)
  - Open Distributed Processing (ODP)
  - Open Systems Interconnection (OSI)

- In this study period, Q11/17 has developed 4 new Recommendations (F.511, X.675, X.696, X.1341), 27 revised Recommendations (X.667, X.680-X.683, X.690-X.696, X.906, X.911), and 11 Corrigenda (X.680 Cor.2, X.682 Cor.1, X.683 Cor.1, X.690 Cor.2, X.694 Cor.2, X.520 Cor.1, X.691 Cor.3, X.691 Cor.4, X.226 Cor.1, X.227bis Cor.1, X.509 Cor.1) to the X.500-, X.680-, and X.690-series of Recommendations, and 1 Technical Report.

Question 11/17 (cnt'd)
Generic technologies to support secure applications
(parts: Directory, PKI, PMI)

■ Recommendations under development:

- **X.500 (revised, 8th ed)**, Information technology – Open Systems Interconnection – The Directory – Overview of concepts, models and services
- **X.501 (revised, 8th ed)**, Information technology – Open Systems Interconnection – The Directory – Models
- **X.509 (revised, 8th ed)**, Information technology – Open Systems Interconnection – The Directory – Public-key and attribute certificate frameworks
- **X.511 (revised, 8th ed)**, Information technology – Open Systems Interconnection – The Directory – Abstract Service Definition
- **X.518 (revised, 8th ed),** Information technology – Open Systems Interconnection – The Directory – Procedures for Distributed Operations
- **X.519 (revised, 8th ed),** Information technology – Open Systems Interconnection – The Directory – Protocols
- **X.520 (revised, 8th ed),** Information technology – Open Systems Interconnection – The Directory – Selected Attribute Types
- **X.521 (revised, 8th ed),** Information technology – Open Systems Interconnection – The Directory – Selected object classes
- **X.525 (revised, 8th ed),** Information technology – Open Systems Interconnection – The Directory – Replication
- **X.pki-em**, Information Technology - Public-Key Infrastructure: Establishment and maintenance
- **X.pki-prof,** Information Technology - Public-Key Infrastructure: Profile

Question 11/17 (cnt'd)
Generic technologies to support secure applications
(parts: ASN.1, OID)

- Developing and maintaining the heavily used Abstract Syntax Notation One (ASN.1) and Object Identifier (OID) specifications

- Recommendations are in the X.680 (ASN.1), X.690 (ASN.1 Encoding Rules), X.660/X.670 (OID Registration), and X.890 (Generic Applications, such as Fast Infoset, Fast Web services, etc.) series

- Giving advice on the management of OID Registration Authorities, particularly within developing countries, through the OID Project Leader Olivier Dubuisson

- Approving new top arcs of the Object Identifier tree as necessary

- Promoting use of OID resolution system by other groups such as SG16

- Repository of OID allocations and a database of ASN.1 modules

- Promoting the term "description and encoding of structured data" as what ASN.1 is actually about

- ASN.1 Packed Encoding Rules reduces the bandwidth required for communication thus conserving energy (e.g., compared with XML)

- Recommendations under development:

    - **X.cms,** Cryptographic Message Syntax (CMS)

    - **X.oiddev**, Information technology – Use of object identifiers in the Internet of Things

    - **X.oid-iot**, ITU-T X.660 - Supplement on Guidelines for using object identifiers for the Internet of Things

Work is collaborative with ISO/IEC JTC 1/SC 6/WG 10

Question 12/17
Formal languages for telecommunication software and testing
(part: Formal languages for telecommunication software)

- Specification and Description Language (Z.100 series) under development:
  - **Z.100 (revised)**, Specification and Description Language - Overview of SDL-2010
  - **Z.100 Annex F1 (revised)**, Specification and Description Language – Overview of SDL-2010 - SDL formal definition: General overview
  - **Z.100 Annex F2 (revised)**, Specification and Description Language – Overview of SDL-2010 - SDL formal definition: Static semantics
  - **Z.100 Annex F3 (revised)**, Specification and Description Language – Overview of SDL-2010 - SDL formal definition: Dynamic semantics
  - **Z.101 (revised)**, Specification and Description Language – Basic SDL-2010
  - **Z.102 (revised)**, Specification and Description Language – Comprehensive SDL-2010
  - **Z.103 (revised)**, Specification and Description Language – Shorthand notation and annotation in SDL-2010

Question 12/17 (cnt'd)
Formal languages for telecommunication software and testing
(part: Formal languages for telecommunication software)

- Specification and Description Language (Z.100 series) under development:
  - **Z.104 (revised)**, Specification and Description Language – Data and action language in SDL-2010
  - **Z.105 (revised)**, Specification and Description Language – SDL-2010 combined with ASN.1 modules
  - **Z.106 (revised)**, Specification and Description Language – Common interchange format for SDL-2010
  - **Z.107 (revised)**, Specification and Description Language – Object-oriented data in SDL-2010
  - **Z.109 (revised)**, Specification and Description Language – Unified modeling language profile for SDL-2010
  - **Z.111 (revised)**, Notations and guidelines for the definition of ITU-T languages
  - **Z.Imp100**, Specification and Description Language implementer's guide – Version 3.0.0

Security Coordination
Security activities in other ITU-T Study Groups

- **ITU-T SG2 Operational aspects & TMN**
  - International Emergency Preference Scheme, ETS/TDR
  - Disaster Relief Systems, Network Resilience and Recovery
  - Network and service operations and maintenance procedures, E.408
  - TMN security, TMN PKI,
- **ITU-T SG5 Environment and climate change**
  - protection from lightning damage, from Electromagnetic Compatibility (EMC) issues and also the effects of High-Altitude Electromagnetic Pulse (HEMP) and High Power Electromagnetic (HPEM) attack and Intentional Electromagnetic Interference (IEMI); EMC, resistibility and safety requirements
  - Mitigation methods against electromagnetic security threats
- **ITU-T SG9 Integrated broadband cable and TV**
  - Conditional access, copy protection, DRM, HDLC privacy,
  - DOCSIS privacy/security
  - IPCablecom 2 (IMS w. security), MediaHomeNet security gateway
- **ITU-T SG11 Signaling Protocols and Testing**
  - EAP-AKA for NGN
  - methodology for security testing and test specification related to security testing

Security Coordination (cnt'd)
Security activities in other ITU-T Study Groups

- ITU-T SG13 Future networks including cloud computing, mobile, NGN, SDN
  - Security and identity management in evolving networks, including SDN security
  - OpenID and OAuth in NGN
  - ID/locator split-based networks architectures
  - Deep packet inspection
  - Trusted ICT infrastructure
- ITU-T SG15 Networks and infrastructures for transport, access and home
  - Reliability, availability, Ethernet/MPLS/ring/shared mesh protection switching
  - Secure admission in home networks
  - Passive node elements with automated ID tag detection
- ITU-T SG16 Multimedia
  - Secure VoIP and multimedia security (H.234, H.323, etc.), NAT/FW traversal
  - Multimedia information access with tag-based identification
  - Common Alerting Services for Digital Signage
- ITU-T SG20 IoT and its applications including smart cities and communities (SC&C)
  - IoT security
  - security for smart cities and communities

Reference links

- Webpage for ITU-T Study Group 17
  - http://itu.int/ITU-T/studygroups/com17
- Webpage on ICT security standard roadmap
  - http://itu.int/ITU-T/studygroups/com17/ict
- Webpage for JCA on identity management
  - http://www.itu.int/en/ITU-T/jca/idm
- Webpage on lead study group on security
  - http://itu.int/en/ITU-T/studygroups/com17/Pages/telesecurity.aspx
- Webpage on lead study group on identity management
  - http://itu.int/en/ITU-T/studygroups/com17/Pages/idm.aspx
- Webpage on lead study group on languages and description techniques
  - http://itu.int/en/ITU-T/studygroups/com17/Pages/ldt.aspx
- ITU Security Manual: Security in Telecommunications and Information Technology
  - http://www.itu.int/pub/publications.aspx?lang=en&parent=T-HDB-SEC.05-2011

Thank you for your attention!

vasily.dolmatov@ties.itu.int