International Telecommunication Union

ITU-T Network Security Initiatives

Michael Harrop

Rapporteur SG 17 Communications Security Project

ITU-T

Overview of Presentation

- Show the context of ITU-T security standards activities
- Provide an overview of the key security work of SG17 and SG13
- Highlight some of the results being achieved and show how this work can be of help to you

Context of ITU-T security standards work

ITU-T

High Level Security Drivers

- ITU Plenipotentiary Conference (PP-02) & (PP-06)
  - Intensify efforts on security
- World Telecommunications Standardization Assembly (WTSA-04)
  - Security robustness of protocols
  - Combating/Countering spam
- World Summit on the Information Society (WSIS-05)
  - Cyber security

Security Standards Development

- Most security standards development is done in Study Group 17 (SG17), the Lead Study Group for communications security.

- However, the work of most SGs has some security implications. (E.g. SG13 (NGN) requires a section on security in each of its Recommendations.)

ITU-T

Study Groups with Significant Security Work

- SG 2 Operational aspects of service provision, networks and performance
- SG 4 Telecommunication management
-
- SG 11 Signalling requirements and protocols
- SG 13 Next generation networks
- SG 16 Multimedia terminals, systems and applications
- SG 17** Security, languages and telecommunication software

** Lead Study Group on Security

ITU-T Security Building Blocks

ITU-T

Security Architecture Framework (X.800-series)

Network Management Security (M.3000-series)

Security Techniques (X.841,2,3)

Systems Management (X.733,5,6, X.740,1)

New
Telecommunication Security (X.805, X.1000-series)

Protocols (X.273,4)

Facsimile (T-series)

New
NGN Security (Y.2700-series)

Directory Services and Authentication (X.500-series)

Televisions and Cable Systems (J-series)

Security in Frame Relay (X.272)

Message Handling Systems (MHS) (X.400-series)

Multimedia Communications (H-series)

SG17:Security, languages and telecommunication software

- SG 17 is the Lead Study Group on telecommunication security - It is responsible for coordination of security across all study groups.
- Subdivided into three Working Parties (WPs)
  - *WP1 - Open systems technologies;*
  - *WP2 - Telecommunications security; and*
  - *WP3 - Languages and telecommunications software*
- Most (but not all) security Questions are in WP2

Current SG 17 security-related Activities

Working Party 1:

- Q1 — End-to-end Multicast Communications with QoS Managing Facility
- Q2 — Directory services, Directory systems, and public-key/attribute certificates
- Q3 — Open Systems Interconnection (OSI)

Working Party 2:

- Q4 — Communications Systems Security Project
- Q5 — Security Architecture and Framework
- Q6 — Cyber Security
- Q7 — Security Management
- Q8 — Telebiometrics
- Q9 — Secure Communication Services
- Q17 — Countering spam by technical means

Current SG 17 security-related Activities - 2

Working Party 3:

- Q10 ASN.1 and other data languages
- Q14 Testing languages, Methodologies and Framework

Focus Groups

- Security Baseline for Network Operators
- Identity Management

Working Party 2/17 Work Areas

Telecom Systems Users

Telecom Systems

Telebiometrics
Q.8/17

* Multimodal model framework
* System mechanism
* Protection procedure

Security Management
Q.7/17

* ISMS-T
* Incident management
* Risk assessment methodology

Secure Communication Services
Q.9/17

* Secure mobile communications
* Home network security
* Web services security

Cyber Security
Q.6/17

* Vulnerability information sharing…
* Incident handling operations
* Identity management

Countering spam by technical means
Q.17/17

* Technical anti-spam measures

Security Architecture and Framework
Q.5/17

* Architecture,
* Model,
* Concepts,
* Frameworks

Q.4/17

Communications System Security Project *Vision, Project, Roadmap, …

Overview of current security Questions and Recommendations under development

Q4/17: Communications Systems Security Project

- Overall Security Coordination and Vision
- Outreach and promotional activities
  - ICT Security Standards Roadmap
  - Security Compendium
  - ITU-T Security manual
- Focus Group on Security Baseline For Network Operators

Q5/17: Security Architecture and Framework

- To investigate new security requirements and solutions and how security architectures and frameworks can be developed to achieve cost-effective comprehensive security solutions that can be applied to various types of networks, services and applications in a multi-vendor environment

- Also responsible for maintenance and enhancements of X.800 series Recommendations

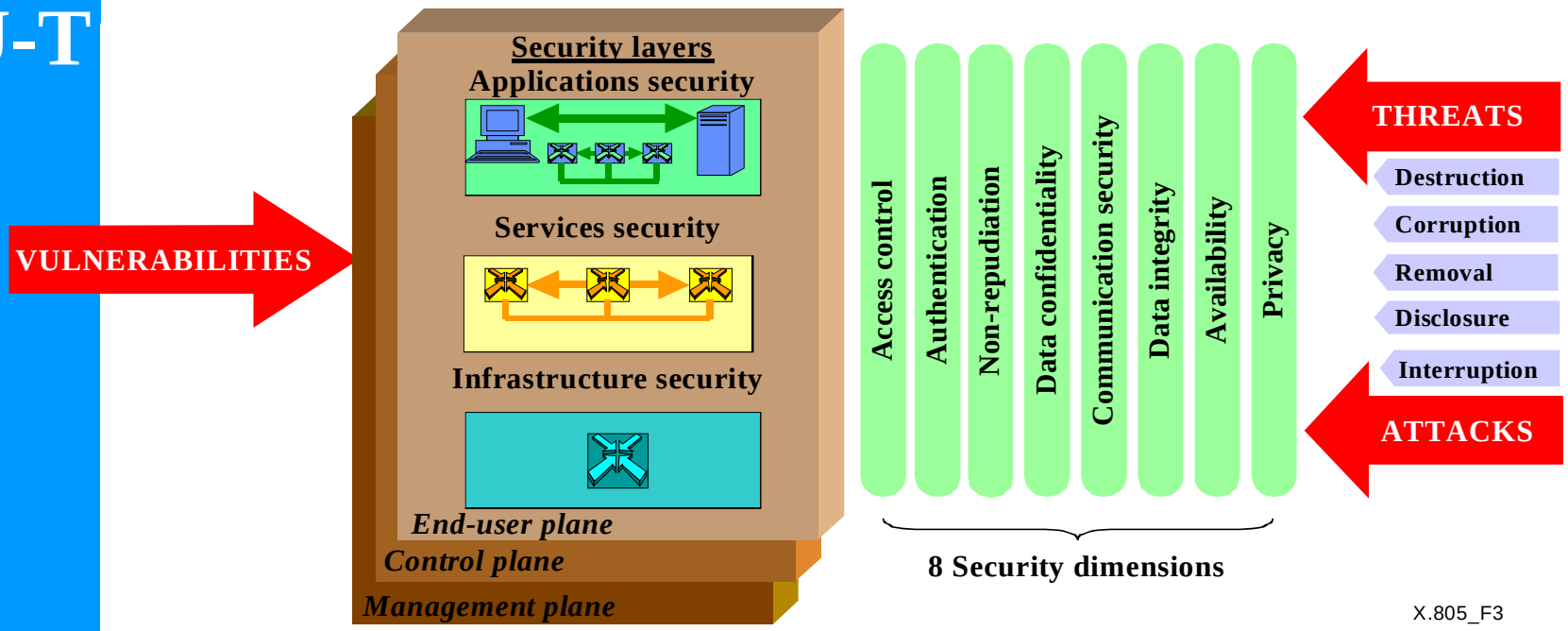
ITU-T

Examples of Q5 Recommendations

- X.805, *Security Architecture for Systems Providing End-to-end Communications* Approved in 2003
- ISO/IEC Standard 18028-2, *Network security architecture*
  - Published in 2006
- ITU-T Recommendation X.1035, *Password-authenticated key exchange (PAK) protocol*
  - Approved in 2006

X.805 - Security Architecture for Systems Providing End-to-end Communications

ITU-T



X.805 defines a network security architecture for providing end-to-end network security. The architecture can be applied to various kinds of networks where the end-to-end security is a concern and independently of the network's underlying technology.

ITU-T

Q6/17: Cyber Security

- Considers aspects of cyber security standardization, in particular:
  - processes for distribution, sharing and disclosure of vulnerability information.
  - standardized procedures for incident handling operations in cyber space.
  - strategies for protection of critical network infrastructure.

Examples of Q6 Recommendations

- Overview of Cybersecurity (X.1205, formerly X.cso)
- A vendor-neutral framework for automatic checking of the presence of vulnerabilities information update (X.vds)
- Guidelines for Internet Service Providers and End-users for Addressing the Risk of Spyware and Deceptive Software (X.sds)
- Identity Management Framework (X.idmf)
- Common Alerting Protocol (CAP v1.1), (X.1303, formerly X.cap)

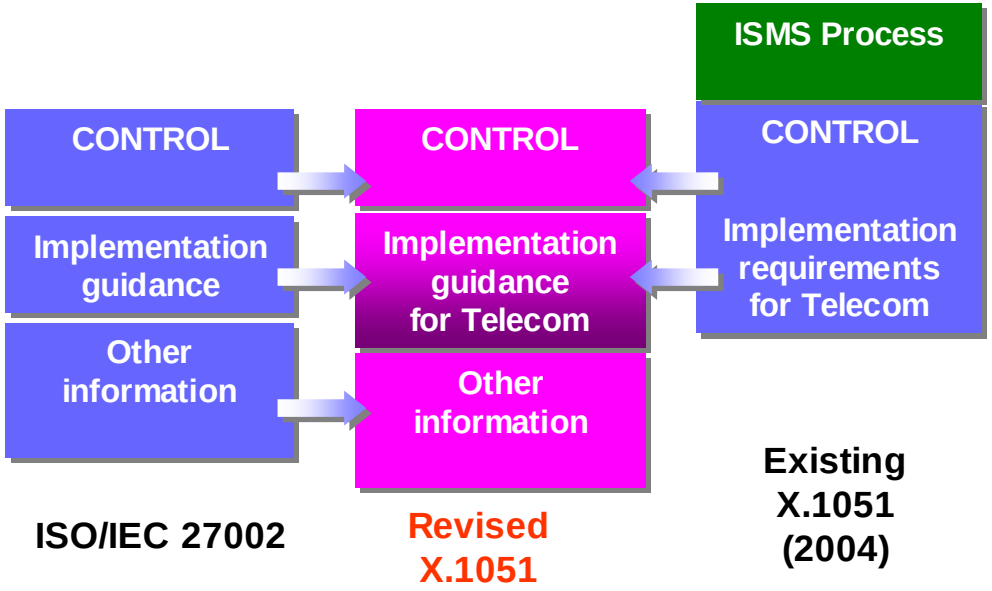
Q7/17: Security Management

- **Key Q7 projects:**
  - **Information Security Management Guidelines for telecommunications (X.1051)**
  - **Risk Management Methodology**
  - **Incident Management**

Information security management guidelines for telecommunications (Revised X.1051 / ISO / IEC 27002)

Revised X.1051

- Security policy
- Organising information security
- Asset management
- Human resources security
- Physical & environmental security
- Communications & operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance



Approach to develop the revised Recommendation X.1051

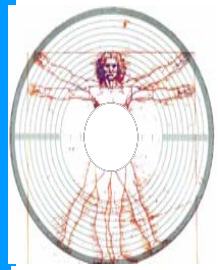
Q8/17: Telebiometrics

- Focuses on how identification and authentication of users be improved by the use of safe and secure telebiometric methods and how issues of biometric authentication technologies for telecommunications can be identified.
- Builds on existing work relating to personal identification and authentication using telebiometrics
- It is being undertaken in close cooperation with related standards work being undertaken in other SDOs.

Q.8/17 Study areas on Biometric Processes

X.tai: Telebiometrics Authentication Infrastructure
X.bip: BioAPI Interworking Protocol
X.tsm: Telebiometrics System Mechanism
X.tpp: Telebiometrics Protection Procedure

X.1081
X.Physiol
Safety conformity



Biometric Sensors

Acquisition (capturing)

NW

Extraction

NW

Matching

Score

NW

Decision

NW

Application

Yes/No

Storage

NW

NW:Network

dates

Examples of Q8 Recommendations

- X.1081, The telebiometric multimodal model framework – A framework for the specification of security and safety aspects of telebiometrics
- X.physiol, Telebiometrics related to human physiology
- X.tsm-1, General biometric authentication protocol and profile on telecommunication system

ITU-T

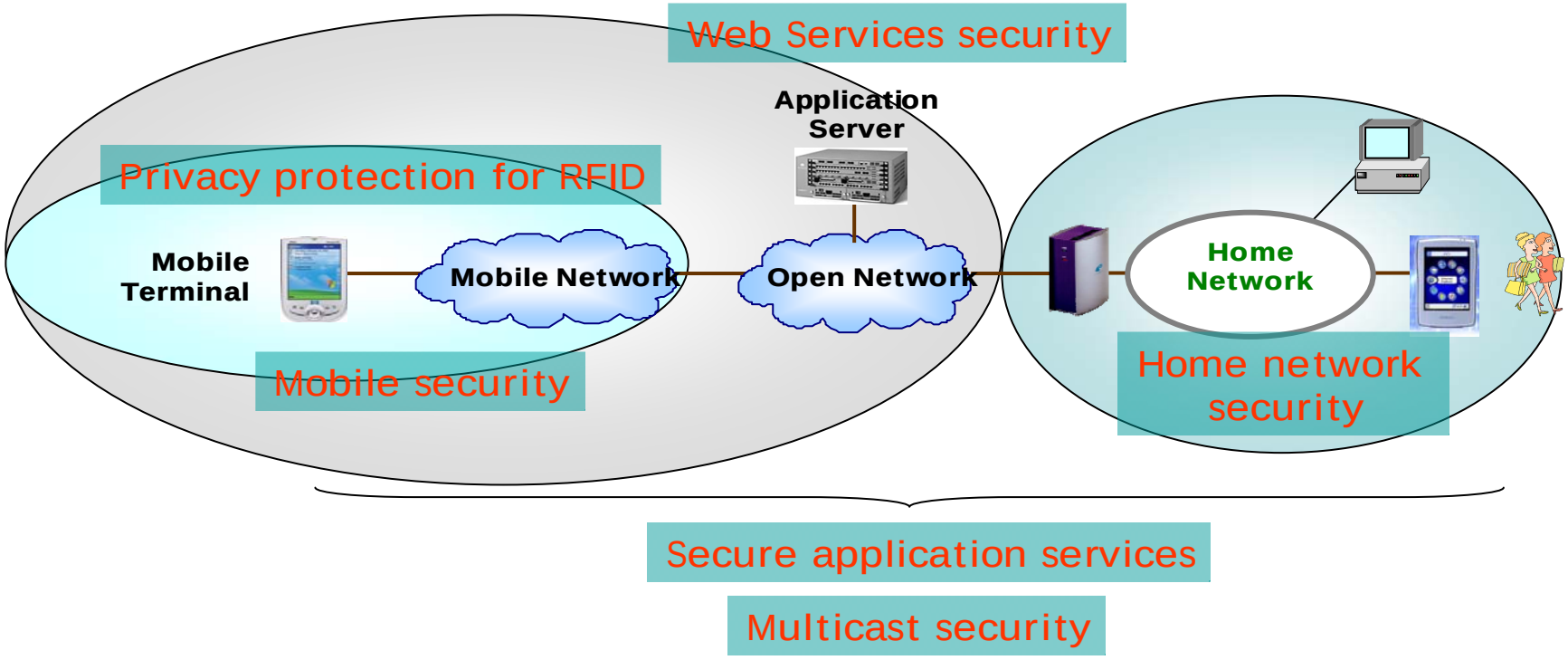
Q9/17: Secure Communication Services

- This Question examines:
  - How secure communication services can be identified and defined in mobile communication or web services;
  - How threats to communications services can be identified and handled;
  - the technologies for supporting secure communication services; and
  - how secure interconnectivity between communication services can be maintained.

Q.9/17 Focus

- Develop a set of standards of secure application services, including
  - Mobile security Under study
  - Home network security Under study
  - Web services security Under study
  - Secure application services Under study
  - Privacy protection for RFID Under study
  - Multicast security Under study
  - Multimedia content protection To be studied

Position of Q9 topics



Examples of Q9 Recommendations

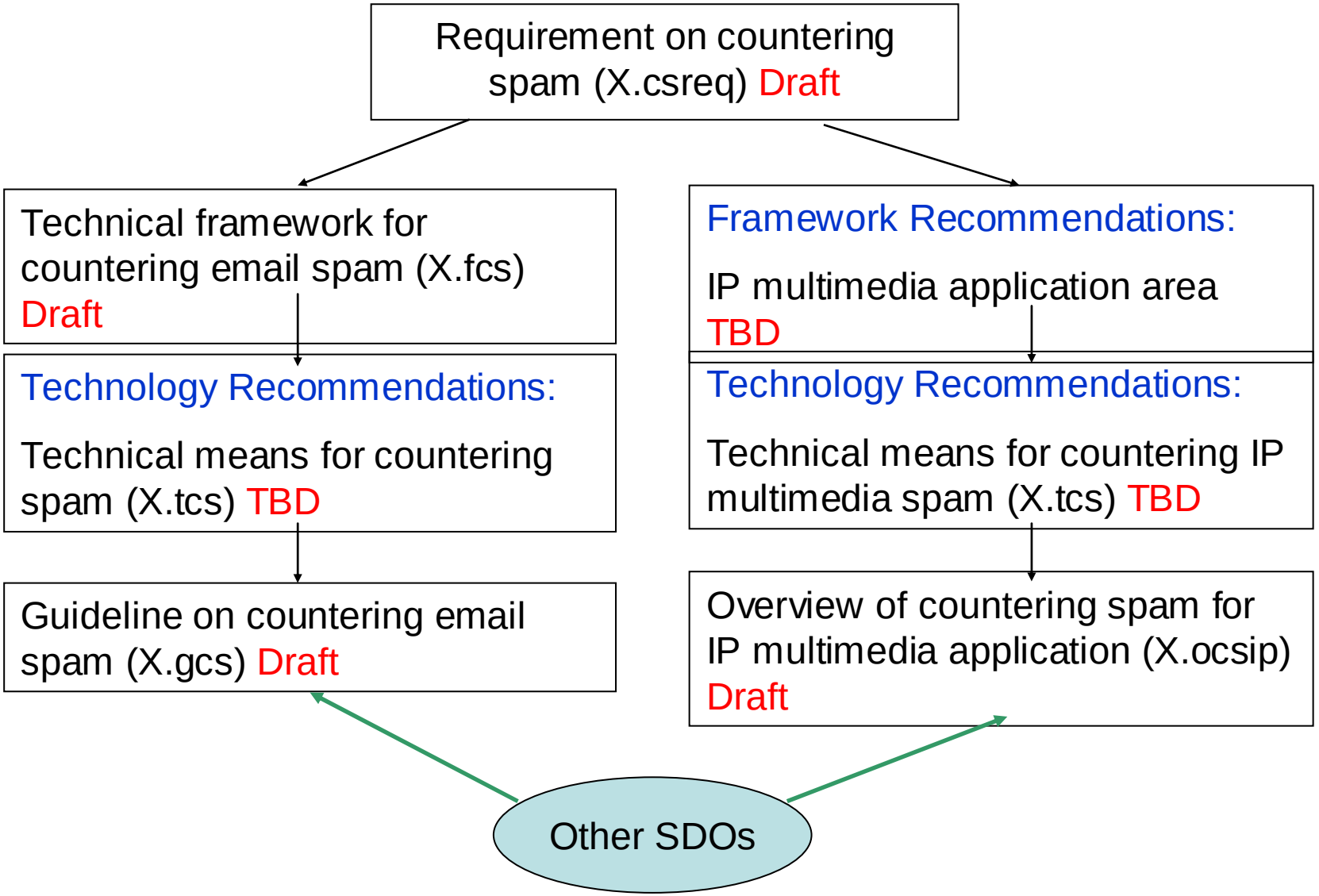
- X.1121, Framework of security technologies for mobile end-to-end data communications Approved 2004
- X.1122, Guideline for implementing secure mobile systems based on PKI Approved 2004
- X.msec-3, General security value added service (policy) for mobile data communication Approved 2007
- X.msec-4, Authentication architecture in mobile end-to-end data communication Approved 2007
- X.crs, Correlative reacting system in mobile network Approved 2007

Q.17/17: Combating spam by technical means

Study items under consideration include:

- What risks does spam pose to the telecommunication network?
- What technical factors associated with the telecommunication network contribute to the difficulty of identifying the sources of spam?
- How can new technologies lead to opportunities to counter spam and enhance the security of the telecommunication network?
- Do network technologies such as SMS, instant messaging & VoIP) offer unique opportunities for spam that require unique solutions?
- What technical work is already being undertaken in other fora, and the private sector to address the problem of spam?
- How does spam impact the stability and robustness of the telecommunication network and what network standardization work, if any, is needed to effectively counter spam

Examples of Q17 Recommendations



SG 17 Security Recommendations under development

- Summaries of all Study Group 17 Recommendations under development are available on the Study Group 17 web page at:

  www.itu.int/itu-t/studygroups/com17

SG13 Q.15 – NGN Security

- All SG 13 Recommendations have a section on security
- Q15 aims to assure the security of the telecomm infrastructure as PSTNs evolve to NGNs.
- Must address and develop network architectures that:
  - Provide for maximal network and end-user resource protection
  - Allow for highly-distributed intelligence end-to-end
  - Allow for co-existence of multiple networking technologies
  - Provide for end-to-end security mechanisms
  - Provide for security solutions that apply over multiple administrative domains

Q.15/13 NGN Security Recommendations

- Y.2701, Security requirements for NGN release 1
- Y.NGN Authentication
- Y.NGN Security Mechanisms, NGN Security Mechanisms and Procedures
- Y.NGN, Certificate Management
- Y.NGN AAA, The Application of AAA Service for network access control in UNI and ANI over NGN
- Y. IdMsec, NGN Identity Management Security
- NGN security activities and Recommendations are listed under “Work Program” at:
  www.itu.int/ITU-T/studygroups/com13/index.asp

ITU-T

A look at some specific SG 17 security projects and outreach activities

ITU-T

Recent SG17 Workshops

- New Horizons for Security Standardization
  - Held in Geneva 3-4 October 2005
  - Speakers, panelists, chairs from ATIS, ETSI, ITU, ISO/IEC, IETF, OASIS, RAIS , 3GPP
- Digital Identity for Next Generation Networks
  - Held in December 2006 jointly with ITU-T/EU IST Daidalos Project
- Conformance & Interoperability and Testing
  - Held in December 2006 to raise awareness of conformance and interoperability testing issues

Focus Group: Security Baseline for Network Operators

- Established October 2005 by SG 17
- Objectives:
  - Define a security baseline against which network operators can assess their network and information security posture in terms of what security standards are available, which of these standards should be used to meet particular requirements, when they should be used, and how they should be applied
  - Describe a network operator's readiness and ability to collaborate with other entities (operators, users and law enforcement authorities) to counteract information security threats
  - Provide meaningful criteria that can be used by network operators against which other network operators can be assessed, if required.
- Survey network operators and service providers conducted in November 2006 by means of a questionnaire
- Approved as a Supplement to X.800 series of Recs. (Sept. 2007)

ITU-T

Security Manual

- *Security in Telecommunications and Information Technology* – an overview of existing ITU-T recommendations for secure telecommunications.

- Available in hard copy and on the SG 17 part of the ITU-T publications web site at
- http://www.itu.int/publications/publications.aspx?lang=en&parent=T-HDB&selection=4&sector=2

ITU-T

Security compendium

- On-line catalogue of approved ITU-T Recommendations related to telecommunication security
  - Extract of ITU-T approved security definitions
  - Summary of ITU-T Study Groups with security-related activities
  - http://www.itu.int/ITU-T/studygroups/com17/tel-security.html

ITU-T

Security Standards Roadmap

- An on-line security standards resource.
- In collaboration with ENISA and NISSG
- Comprises 5 parts:
  - Part 1 contains information about organizations working on ICT security standards
  - Part 2 is database of existing security standards
  - Part 3 lists (or links to) current projects and standards in development
  - Part 4 will identify future needs and proposed new standards
  - Part 5 lists security best practices

ITU-T

Roadmap - 2

- Part 2 is a searchable database that includes ITU-T, ISO/IEC JTC1, ATIS, IETF, ETSI IEEE and OASIS security standards.
- The database format allows searching and to allows organizations to manage their own data
- Publicly available under *Special Projects and Issues* at:
  - www.itu.int/ITU-T/studygroups/com17/index
- We invite you to use the Roadmap, provide feedback and help us develop it to meet your needs

Other SG17 projects

- We have established a Security Standards Exchange Network (SSEN) to maintain on-going dialogue on key issues of security standardization.

The importance of Collaboration

- Internal and external collaboration is very important to the work of SG17
- Examples include:
  - Most other ITU-T SGs, ITU-D, ISO/IEC JTC1, IETF, ATIS, ETSI, OASIS etc
  - ENISA, NISSG (Roadmap)
  - Global Standards Collaboration (GSC)
  - ISO/IEC/ITU-T Strategic Advisory Group on Security (SAG-S)

Some of the things we've learned

- Threats are not going to diminish. We need to continue to focus on the security issue when developing all new ICT standards
- Security is everybody's business
- Collaboration with other SDOs is essential
- Security needs to be designed in upfront
- Security must be an ongoing effort
- Systematically addressing vulnerabilities (intrinsic properties of networks/systems) is key so that protection can be provided independent of what the threats (which are constantly changing and may be unknown) may be.

International Telecommunication Union

Thank you