



ITU-T NETWORK SECURITY INITIATIVES

TED HUMPHREYS



ITU-T

Overview of Presentation

- Provide a brief overview of ITU-T security standards activities
- Highlight some of the recent key achievements, particularly those resulting from the October workshop *New Horizons for Security Standardization*



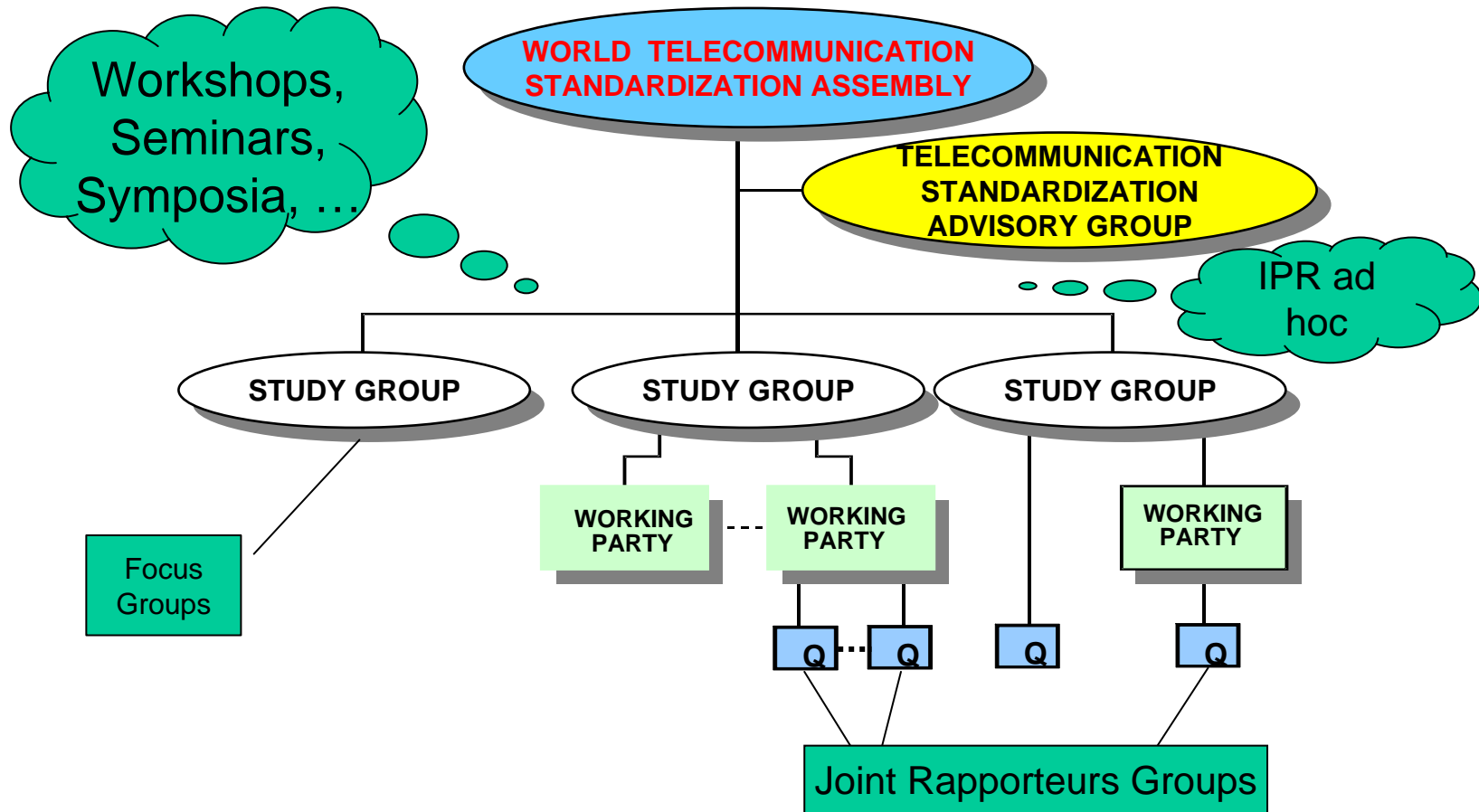
ITU-T

Overview of ITU-T security standards work



ITU-T

ITU-T Organizational Structure





ITU-T

ITU-T Study Groups

ITU-T work is divided up between Study Groups (SGs).

- *SG 2: Operational aspects of service provision, networks and performance*
- *SG 4: Telecommunication management*
- *SG 5: Protection against electromagnetic environment effects*
- *SG 6 Outside Plant and related indoor installations*
- *SG 9 Integrated broadband cable networks and television and sound transmission*
- *SG 11 Signaling requirements and protocols*
- *SG 12 Performance and quality of service*
- *SG 13 Next Generation Networks*
- *SG 15: Optical and other transport networks*
- *SG 16: Multimedia services, systems and terminals*
- *SG 17: Security, languages and telecommunication software*
- *SG 19: Mobile Telecommunications Networks*

Note that SG17 has overall security responsibility but much of the work has security implications and requirements



ITU-T

ITU-T security building blocks

Security Architecture Framework

- X.800 – Security architecture
- X.802 – Lower layers security model
- X.803 – Upper layers security model
- X.805 – Security architecture for systems providing end-to-end communications
- X.810 – Security frameworks for open systems: Overview
- X.811 – Security frameworks for open systems: Authentication framework
- X.812 – Security frameworks for open systems: Access control framework
- X.813 – Security frameworks for open systems: Non-repudiation framework
- X.814 – Security frameworks for open systems: Confidentiality framework
- X.815 – Security frameworks for open systems: Integrity framework
- X.816 – Security frameworks for open systems: Security audit and alarms framework

Protocols

- X.273 – Network layer security protocol
- X.274 – Transport layer security protocol

Security in Frame Relay

- X.272 – Data compression and privacy over frame relay networks

Security Techniques

- X.841 – Security information objects for access control
- X.842 – Guidelines for the use and management of trusted third party services
- X.843 – Specification of TTP services to support the application of digital signatures

Directory Services and Authentication

- X.500 – Overview of concepts, models and services
- X.501 – Models
- X.509 – Public key and attribute certificate frameworks
- X.519 – Protocol specifications

Network Management Security

- M.3010 – Principles for a telecommunications management network
- M.3016 – TMN Security Overview
- M.3210.1 – TMN management services for INT-2000 security management
- M.3320 – Management requirements framework for the TMN X-interface
- M.3400 – TMN management functions

Systems Management

- X.733 – Alarm reporting function
- X.735 – Log control function
- X.736 – Security alarm reporting function
- X.740 – Security audit trail function
- X.741 – Objects and attributes for access control

Facsimile

- T.30 Annex G – Procedures for secure Group 3 document facsimile transmission using the HKM and HFX system
- T.30 Annex H – Security in facsimile Group 3 based on the RSA algorithm
- T.36 – Security capabilities for use with Group 3 facsimile terminals
- T.503 – Document application profile for the interchange of Group 4 facsimile documents
- T.563 – Terminal characteristics for Group 4 facsimile apparatus

Televisions and Cable Systems

- J.91 – Technical methods for ensuring privacy in long-distance international television transmission
- J.93 – Requirements for conditional access in the secondary distribution of digital television on cable television systems
- J.170 – IP-Cablecom security specification

Multimedia Communications

- H.233 – Confidentiality system for audiovisual services
- H.234 – Encryption key management and authentication system for audiovisual services
- H.235 – Security and encryption for H-series (H.233 and other H.245-based) multimedia terminals
- H.323 Annex J – Packet-based multimedia communications systems – Security for H.323 Annex F (Security for simple endpoint types)
- H.350.2 – Directory services architecture for H.235
- H.530 – Symmetric security procedures for H.323 mobility in H.510



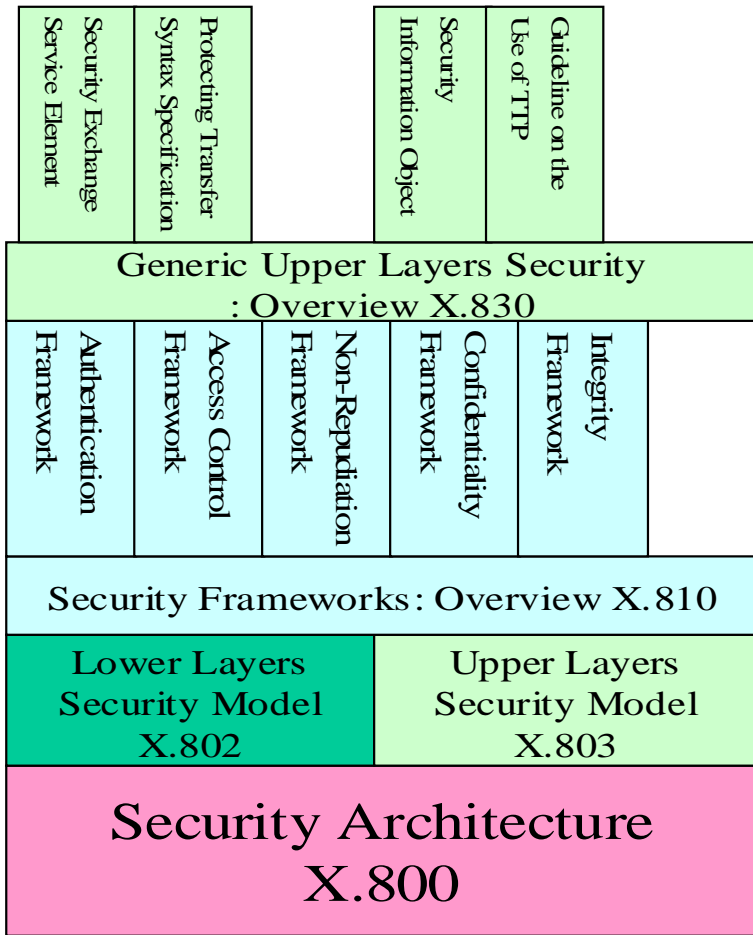
ITU-T

Study Group 17: 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



Study Group 17 Security Focus in previous Study Period (2001-2004)



Communication System Security

Information Security Management (Telecom ISMS)

Mobile Security

Tele-biometrics

Countering Spam by technical means

N
E
W

Existing Recommendations in X.800-series



ITU-T

Current SG 17 security-related Questions

Working Party 1:

- 1/17 End-to-end Multicast Communications with QoS Managing Facility
- 2/17 Directory services, Directory systems, and public-key/attribute certificates
- 3/17 Open Systems Interconnection (OSI)

Working Party 2:

- 4/17 **Communications Systems Security Project**
- 5/17 Security Architecture and Framework
- 6/17 Cyber Security
- 7/17 Security Management
- 8/17 Telebiometrics
- 9/17 Secure Communication
- 17/17 Countering spam by technical means



ITU-T

SG 17 Security Questions (2005-2008)

Telecom Systems Users

Telecom Systems

Telebiometrics

- *Multimodal Model Fwk
- *System Mechanism
- *Protection Procedure
- *X.1081

Q8/17

Q7/17

Security Management

- *ISM Guideline for Telecom
- *Incident Management
- *Risk Assessment Methodology
- *etc...
- *X.1051

Secure Communication Services

- *Mobile Secure Communications
- *Home Network Security
- *Security Web Services
- *X.1121, X.1122

Q9/17

Q5/17

Security Architecture & Framework

- *Architecture, Model, Concepts, Frameworks, etc...
- *X.800 series
- *X.805

Cyber Security

- *Overview of Cyber-security
- *Vulnerability Information Sharing
- * Incident Handling Operations

Q6/17

New

Countering SPAM

- *Technical anti-spam measures

Q17/17

New

Q4/17

Communications System Security *Vision, Coordination, Roadmap, Compendia...

New



ITU-T

Overview of ITU-T Security Standardization

-Collaboration is key factor-

Specific Systems, Services, Applications
Security in ITU-T will be developed by
SG2,3,5,6,9,11,13,15,16,19



Core technology and Common Security
Techniques in ITU-T will be developed
by SG17



ISO/IEC SC27

IETF

ANSI, ETSI, etc.



ITU-T

Some recent SG17 initiatives



ITU-T

New Horizons for Security Standardization Workshop

- o Security Workshop held in Geneva 3-4 October 2005
- o Hosted by ITU-T SG17 as part of security coordination responsibility
- o ISO/IEC JTC1 played an important role in planning the program and in providing speakers/panelists.
- o Speakers, panelists, chairs from:
 - ITU-T
 - ISO/IEC
 - IETF
 - Consortia - OASIS, 3GPP
 - Regional SDOs - ATIS, ETSI, RAIS



ITU-T

Workshop Objectives

- Provide an overview of key international security standardization activities;
- Seek to find out from stakeholders (e.g., network operators, system developers, manufacturers and end-users) their primary security concerns and issues (including possible issues of adoption or implementation of standards);
- Try to determine which issues are amenable to a standards-based solution and how the SDOs can most effectively play a role in helping address these issues;
- Identify which SDOs are already working on these issues or are best equipped to do so; and
- Consider how SDOs can collaborate to improve the timeliness and effectiveness of security standards and avoid duplication of effort.



ITU-T

Results

- Excellent discussions, feedback and suggestions
- Documented in detail in the Workshop report
- Results are reported under following topics:
 - *What are the crucial problems in ICT security standardization?*
 - *Meta issues and need for a global framework;*
 - *Standards Requirements and Priorities;*
 - *Liaison and information sharing;*
 - *User issues;*
 - *Technology and threat issues;*
 - *Focus for future standardization work;*
 - *Process issues;*
 - *Follow-on issues*
- The report is available on-line at:
 - www.itu.int/ITU-T/worksem/security/200510/index.html



ITU-T

ICT Security Standards Roadmap

(An SG 17 Work-in-progress)

- o Part 1 contains information about organizations working on ICT security standards
- o Part 2 is database of existing security standards
- o Part 3 will be a list of standards in development
- o Part 4 will identify future needs and proposed new standards



ITU-T

Roadmap access

- o Part 2 includes ITU-T, ISO/IEC JTC1 and IETF standards. It will be expanded to include other standards (e.g. regional and consortia specifications).
- o It will also be converted to a Database format to allow searching and to allow organizations to manage their own data
- o Publicly available under *Special Projects and_Issues* at:
 - www.itu.int/ITU-T/studygroups/com17/index
- o We invite you to use the Roadmap, provide feedback and help us develop it to meet your needs



ITU-T

Other SG17 projects

- *Security in Telecommunications and Information Technology* - an overview of existing ITU-T recommendations for secure telecommunications.
- Available on the SG 17 part of the ITU-T web site at
 - www.itu.int/ITU-T/publications/index.html
- We are in the process of establishing a Security Experts Network (SEN) to maintain on-going dialogue on key issues of security standardization.



ITU-T

What about the future?

- The threat scenario will continue to evolve
 - Attacks are widespread and innovative
 - Broad collaboration is needed to understand and respond to the threats

- Business needs to understand what is happening in the standards work and needs to anticipate events to defend competitive position and avoid bad things happening

- Participating directly in the standards work can have a real payoff - We welcome the opportunity to work together with you.



ITU-T

Some useful web resources

- ITU-T Home page www.itu.int/itu-t
- Study Group 17
e-mail: tsbsg17@itu.int
- Recommendations www.itu.int/ITU-T/publications/recs.html
- ITU-T Lighthouse www.itu.int/ITU-T/lighthouse
- ITU-T Workshops www.itu.int/ITU-T/worksem
- Roadmap www.itu.int/ITU-T/studygroups/com17/index



ITU-T

THANK YOU.
ANY QUESTIONS?