



ITU-T NETWORK SECURITY INITIATIVES

MIKE HARROP
Rapporteur SG17 Q4

ETSI Security Workshop
January 2007



ITU-T

Overview of Presentation

- o Show the context of ITU-T security standards activities
- o Highlight some of key areas of focus
- o Report on some of the results being achieved



ITU-T

Context of ITU-T security standards work



High Level Security Drivers

ITU-T

- ITU Plenipotentiary Conference (PP-02)
 - Intensify efforts on security

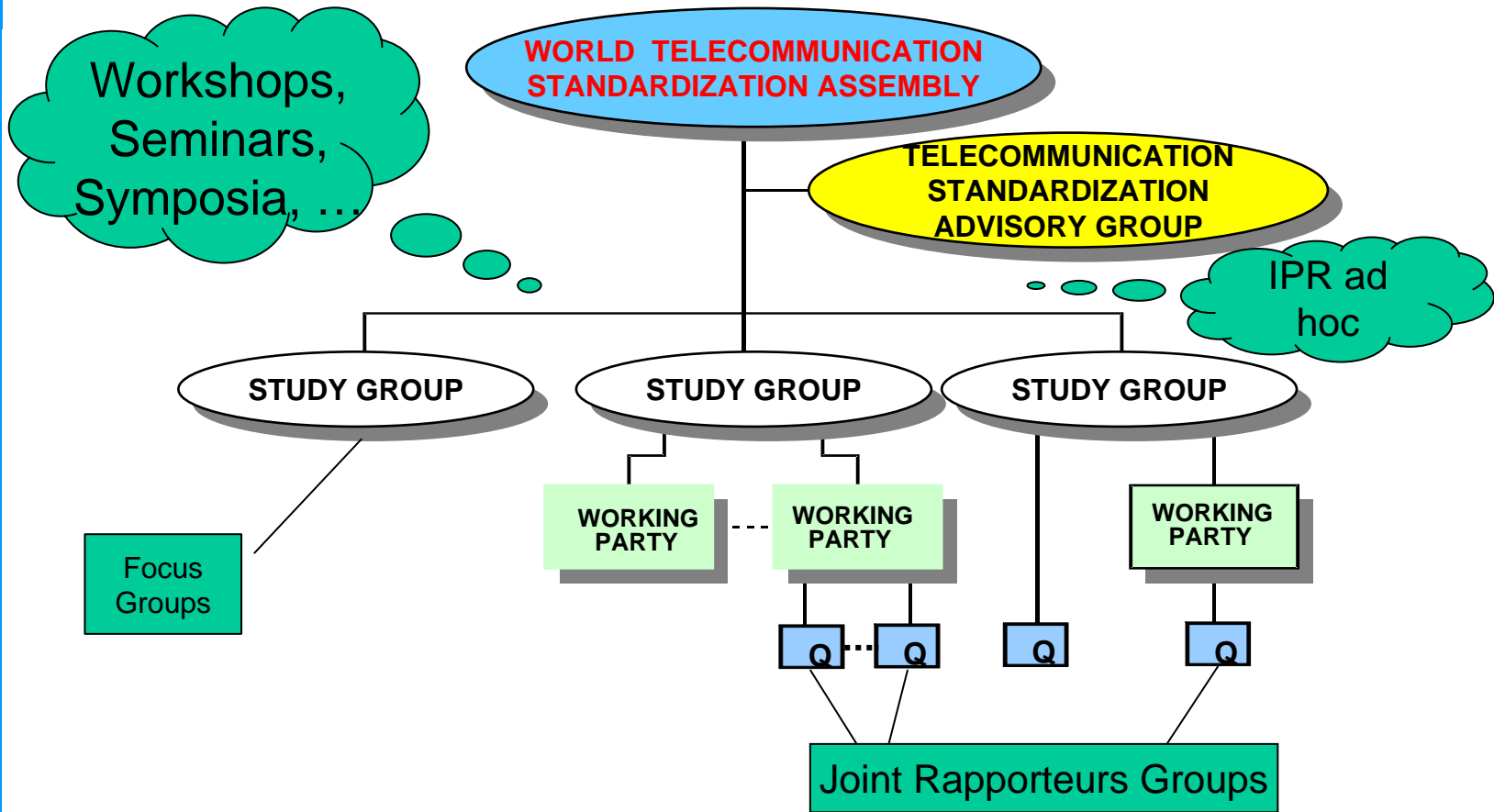
- World Telecommunications Standardization Assembly (WTSA-04)
 - Security robustness of protocols
 - Combating/Countering spam

- World Summit on the Information Society (WSIS-05)
 - Cyber security



ITU-T

ITU-T Organizational Structure





ITU-T

ITU-T Study Groups

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

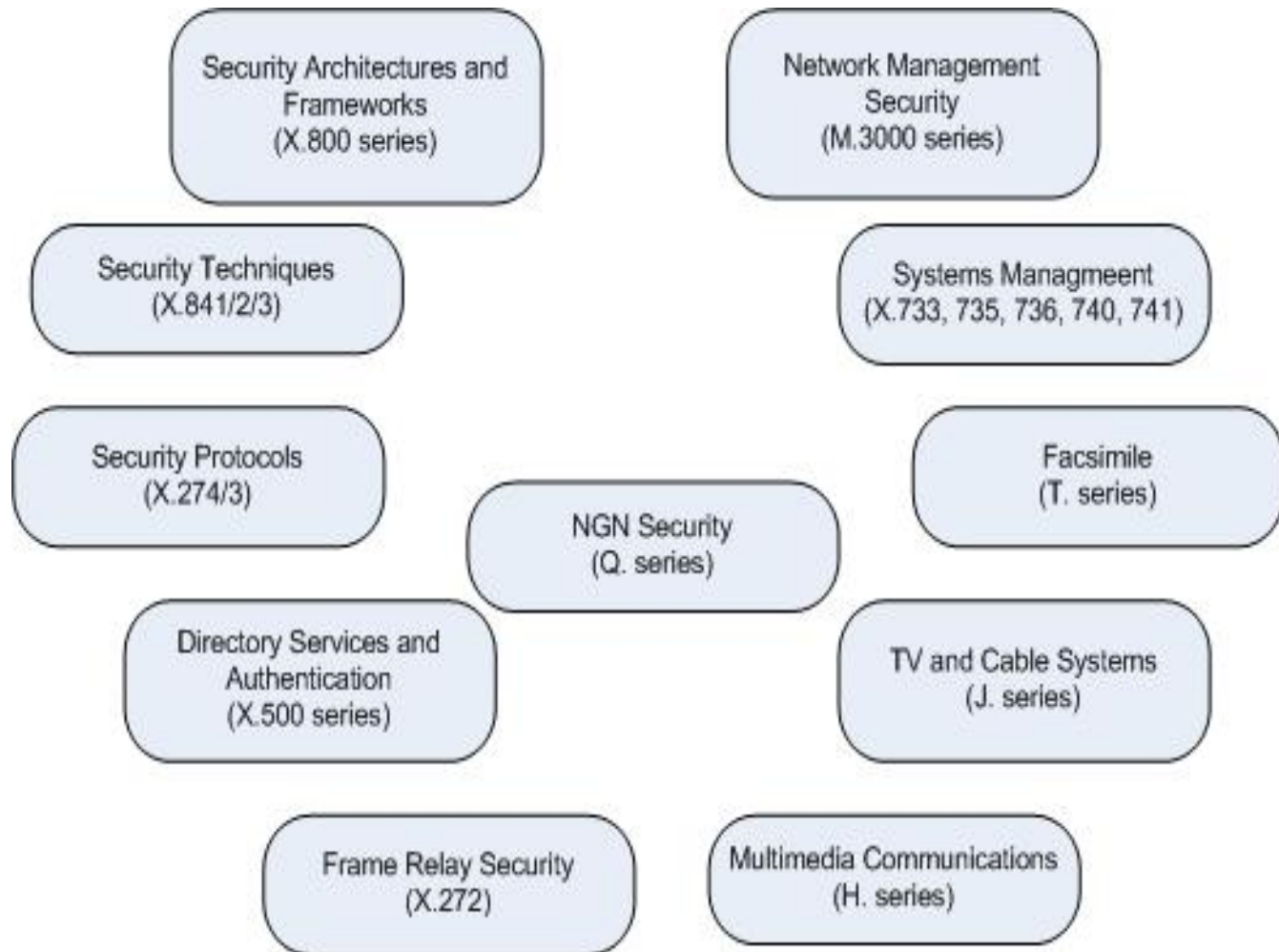
- *SG 2: Operational aspects of service provision, networks and performance*
- *SG 4: Telecommunication management*
- *SG 5: Protection against electromagnetic environment effects*
- *SG 6 Outside Plant and related indoor installations*
- *SG 9 Integrated broadband cable networks and television and sound 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: SG17 has overall security responsibility but almost all SGs have work with security implications and requirements.



ITU-T

ITU-T Security Building Blocks





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



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 WP2 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

Overview of current security Questions and Recommendations under development



ITU-T

SG 17 Security Recommendations under development - 1

Q4 Communications Systems Security Project

X.sbno, Security baseline for network operators

Security Roadmap

Security in Telecommunications and Information Security Manual

Q5 Security Architecture and Framework

X.805+, Division of the security features between the network and the users

X.805nsa, Network security certification based on ITU-T Recommendation X.805

X.ngn-akm, Framework for authentication and key management for link layer security of NGN

X.pak, Password-authenticated key exchange (PAK)

X.spn, Framework for creation, storage, distribution and enforcement of security policies for networks



ITU-T

SG 17 Security Recommendations under development - 2

Q6 Cyber Security

X.cso, Overview of cybersecurity

X.sds, Guidelines for Internet Service Providers and End-users for Addressing the Risk of Spyware and Deceptive Software

X.cvlm, Guidelines on Cybersecurity Vulnerability Life-cycle Management

X.vds, A vendor-neutral framework for automatic checking of the presence of vulnerabilities information update

Q7 Security Management

X.1051 (R), Information security management guidelines for telecommunications based on ISO/IEC 27002

X.rmg, Risk management guidelines for telecommunications

X.sim, Security incident management guidelines for telecommunications

Q8 Telebiometrics

X.bip, BioAPI interworking protocol

X.physiol, Telebiometrics related to human physiology

X.tai, Telebiometrics authentication infrastructure

X.tpp-1, A guideline of technical and managerial countermeasures for biometric data security

X.tpp-2, A guideline for secure and efficient transmission of multi-modal biometric data

X.tsm-1, General biometric authentication protocol and profile on telecommunication systems

X.tsm-2, Profile of telecommunication device for Telebiometrics System Mechanism (TSM)



SG 17 Security Recommendations under development - 3

ITU-T

Q9 Secure Communication Services

- X.crs, Correlative reacting system in mobile network
- X.homesec-1, Framework of security technologies for home network
- X.homesec-2, Certificate profile for the device in the home network
- X.homesec-3, User authentication mechanisms for home network service
- X.msec-3, General security value added service (policy) for mobile data communication
- X.msec-4, Authentication architecture in mobile end-to-end data communication
- X.p2p-1, Requirements of security for peer-to-peer and peer-to-multi peer communications
- X.p2p-2, Security architecture and protocols for peer to peer network
- X.sap-1, Guideline on secure password-based authentication protocol with key exchange
- X.sap-2, Secure communication using TTP service
- X.websec-1, Security Assertion Markup Language (SAML) - X.1141 now in AAP Last Call
- X.websec-2, eXtensible Access Control Markup Language (XACML) - X.1142 now in AAP Last Call
- X.websec-3, Security architecture for message security in mobile web services

Q17 Countering spam by technical means

- X.csreq, Requirement on countering spam
- X.fcs, Technical framework for countering email spam
- X.gcs, Guideline on countering email spam
- X.ocsip, Overview of countering spam for IP multimedia application
- X.tcs, Technical means for countering spam



ITU-T

SG 17 Security Recommendations under development - 4

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



ITU-T

Recent Initiatives

Workshops



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 Speakers, panelists, chairs from ATIS, ETSI, ITU, ISO/IEC, IETF, OASIS, RAIS , 3GPP



ITU-T

Workshop Objectives

- Provide an overview of key international security standardization activities;
- Seek to find out from stakeholders 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

Workshop on Digital Identity for Next Generation Networks

- Joint ITU-T/EU IST Daidalos Project workshop
- Held on 5th December 2006
- Objectives:
 - To investigate approaches and analyze gaps in current standards
 - To identify future challenges and find common goals to provide direction to the current work in different projects and SDOs



ITU-T

Digital Identity Focus Group

- Focus Group on Digital Identity established December 2006
- Aims to facilitate the development of a generic Identity Management Framework
- Participation open to other SDOs
- Meeting in Geneva 13-16 February 2007
- www.itu.int/ITU-T/studygroups/com17/index.asp



ITU-T

Workshop on Interoperability and Testing

- Held as part of WP3 meeting on 8th Dec. 2006
- Aimed to raise awareness of conformance and interoperability testing issues, with particular focus on testing needs for Next Generation Networks



ITU-T

Recent Initiatives

Specific projects



ITU-T

Q.15/13 – NGN Security

Aims to assure the security of the telecommunications 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



ITU-T

Q.17/17 – Combating spam by technical means

Study items to be considered 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



ITU-T

Focus Group: Security Baseline for Network Operators

- o Established October 2005 by SG 17
- o 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.
- o Survey network operators and service providers conducted in November 2006 by means of a questionnaire
- o Development of first draft Recommendations began in December 2006



ITU-T

ICT Security Standards Roadmap

(An SG 17 Work-in-progress)

- 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



ITU-T

Roadmap access

- Part 2 now includes ITU-T, ISO/IEC JTC1, IETF, ETSI IEEE and OASIS standards.
- It will also be converted to a Database format to allow searching and to allow 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



ITU-T

Other SG17 projects

- *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 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.

The ITU Global Cybersecurity Gateway



ITU-T

Cybersecurity Gateway Search Site Map Contact Us

CYBERSECURITY GATEWAY

Home For Citizens For Governments For Businesses For International Organizations

Information Sharing Watch and Warning Industry Standards and Solutions Laws and Legislation Privacy and Protection

Welcome to the Cybersecurity Gateway!

The purpose of the Cybersecurity Gateway is to provide an easy-to-use information resource on national and international cybersecurity related initiatives worldwide. In today's interconnected world of networks, threats can now originate anywhere - our collective cybersecurity depends on the security practices of every connected country, business, and citizen.

In this regard, we need national and international cooperation among those who seek to promote, develop and implement initiatives for a global culture of cybersecurity. In accordance with the theme of World Telecommunication Day/ World Information Society Day 2006, ongoing ITU work programmes, and follow-up of the World Summit on the Information Society (WSIS), a number of cybersecurity initiatives are under development by ITU. I invite you to explore the vast resources and links available through the Cybersecurity Gateway and join with us in promoting global cybersecurity.

Yoshio Utsumi
Secretary-General, ITU

CYBERSECURITY GATEWAY MAP

Search for Cybersecurity organizations in your country. Click on the interactive map to start your entity search.

Partnerships for Global Cybersecurity

Cybersecurity and Developing Economies

Spam | Spyware | Phishing | Scams and Frauds | Viruses and Trojans | Denial of Service | Information Security | Identity Management | Strategies | E-Government | Creating Trust

Copyright© International Telecommunication Union 2006

- o LIVE at: <http://www.itu.int/cybersecurity>
- o Provides an easy-to-use information resource on national, regional and international cybersecurity-related activities and initiatives worldwide.



ITU-T

Structure of the Cybersecurity Gateway

- The portal is geared towards four specific audiences: *"Citizens"; "Businesses"; "Governments", "International Organizations"*
- Database information collected within five main **themes**:
 1. Information sharing of national approaches, good practices and guidelines;
 2. Developing watch, warning and incident response capabilities;
 3. Technical standards and industry solutions;
 4. Harmonizing national legal approaches and international legal coordination and enforcement;
 5. Privacy, data and consumer protection.
- Additional information resources on the following **topics**: spam, spyware, phishing, scams and frauds, worms and viruses, denial of service attacks, etc.



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

- Security needs to be designed in upfront and to be an on-going effort

- SDOs need to collaborate (eliminate duplication)

- SDOs should aim to develop solutions that can support robust, secure, standards-based implementations that can provide protection regardless of the nature of the evolving threats



ITU-T

Some useful web resources

- ITU-T Home page www.itu.int/itu-t
- Study Group 17
e-mail: tsbsg17@itu.int
www.itu.int/itu-t/studygroups/com17
- 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
- Cybersecurity Portal <http://www.itu.int/cybersecurity>



ITU-T

THANK YOU.
ANY QUESTIONS?