ITU-T Work on security

WSIS Action Line C5 Facilitation Meeting: "Promoting Global Cybersecurity"

15-16 May 2006

Georges Sebek
International Telecommunication Union (ITU)

Standards

Cooperation

Awareness

ITU-T Study Groups

- SG 2 Operational aspects of service provision, networks and performance
- SG 3 Tariff and accounting principles including related telecommunications economic and policy issues
- 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 Signalling requirements and protocols
- SG 12 Performance and quality of service
- SG 13 Next generation networks
- SG 15 Optical and other transport network infrastructures
- SG 16 Multimedia terminals, systems and applications
- **SG 17 Security, languages and telecommunication software**
- SG 19 Mobile telecommunication networks

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.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

Telecommunication Security

- **X.805** – Security architecture for systems providing end-to-end communications
- **X.1051** – Information security management system – Requirements for telecommunications (ISMS-T)
- **X.1081** – A framework for specification of security and safety aspects of telebiometrics
- **X.1121** – Framework of security technologies for mobile end-to-end communications
- **X.1122** – Guideline for implementing secure mobile systems based on PKI

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 IMT-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

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** – IPCablecom 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.323 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

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

Message Handling Systems (MHS)

- **X.400/F.400** – Message handling system and service overview
- **X.402** – Overall architecture
- **X.411** – Message transfer system: Abstract service definition and procedures
- **X.413** – Message store: Abstract service definition
- **X.419** – Protocol specifications
- **X.420** – Interpersonal messaging system
- **X.435** – Electronic data interchange messaging system
- **X.440** – Voice messaging system

ITU-T Recommendations are available from the ITU website http://www.itu.int/publications/bookshop/how-to-buy.html (this site includes information on limited free access to ITU-T Recommendations)

Current important security work in ITU-T includes

Telebiometrics, Security management, Mobility security, Emergency telecommunications

For further information on ITU-T and its Study Groups: http://www.itu.int/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
- Summaries of all draft Recommendations under development in SG 17 are available on the SG 17 web page at www.itu.int/itu-t/studygroups/com17

Telecom Systems Users

Telecom Systems

Q.8/17

Telebiometrics
*Multimodal Model Framework
*System Mechanism
*Protection Procedure

Q.7/17

Security Management
*ISMS-T
*Incident Management
*Risk Assessment Methodology

Q.9/17

Secure Communication Services
*Mobile Secure Communications
*Home Network Security
*Security Web Services

Q.6/17

Cyber Security
*Vulnerability Information Sharing…
*Incident Handling Operations

Countering spam by technical means
*Technical anti-spam measures

Q.17/17

Q.5/17

Security Architecture & Framework
*Architecture, Model, Concepts, Frameworks

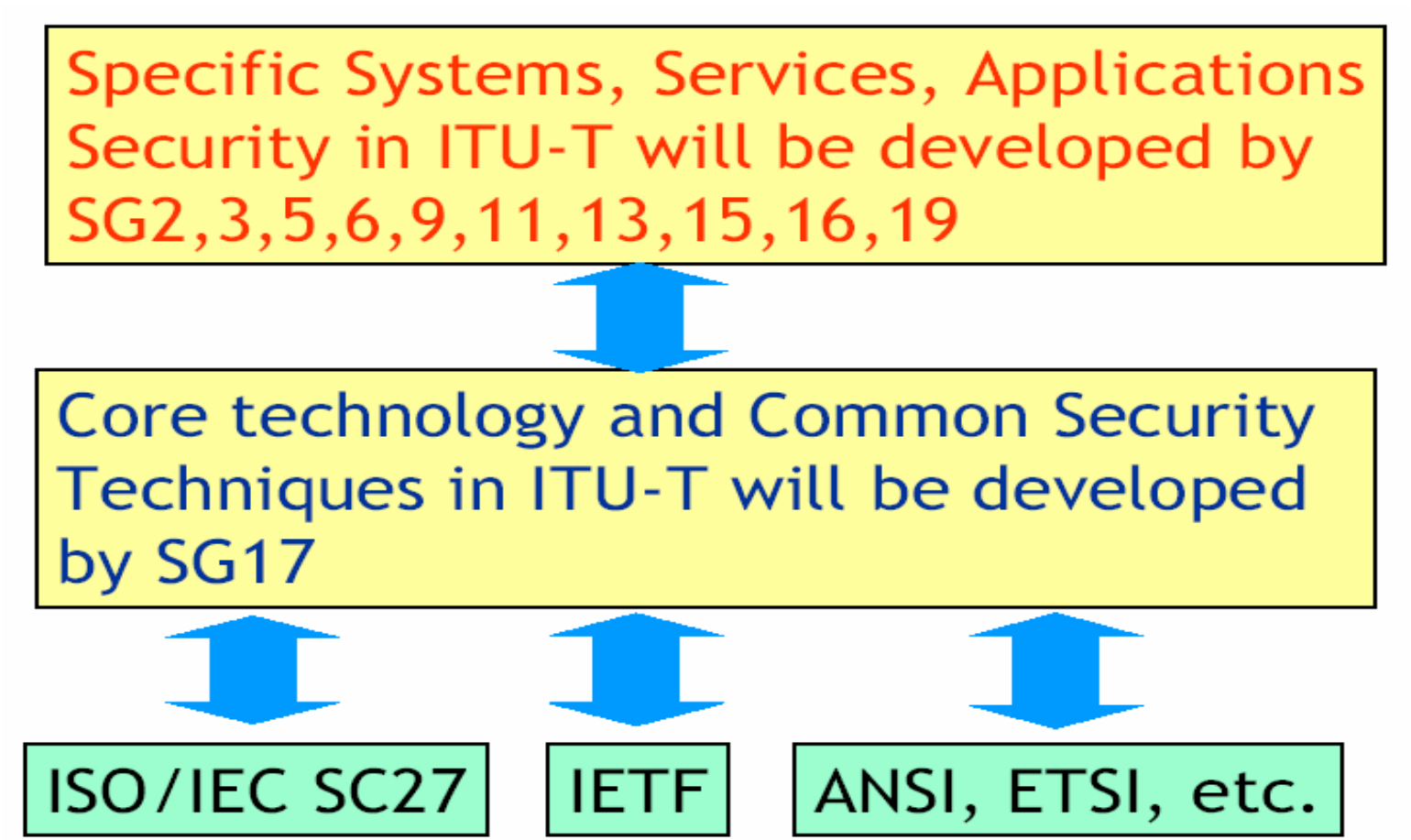
Q.4/17

Communications System Security Project *Vision, Project Roadmap, …

Extract from the SG 17 work

Recommendation		WP	Q.	Equivalent e.g., ISO/IEC
No.	Title			
X.1141 (X.websec-1)	Security assertion markup language (SAML)	2	9	OASIS SAML v2.0
X.1142 (X.websec-2)	eXtensible Access Control Markup Language (XACML)	2	9	OASIS XACML v2.0
X.cso	Overview of cybersecurity	2	6	
X.vds	A vendor-neutral framework for automatic checking of the presence of vulnerabilities information update	2	6	
X.cvlm	Guidelines on cybersecurity vulnerability lifecycle management	2	6	
X.sds	Guidelines for Internet service provides and end-users for addressing the risk of spyware and deceptive software	2	6	
X.gcs	Guideline on countering email spam	2	17	
X.csreq	Requirement on countering spam	2	17	
X.fcs	Technical framework for countering email spam	2	17	
X.ocsip	Overview of countering spam for IP multimedia applications	2	17	
X.tcs	Technical means for countering spam	2	17	

Security standardization Collaboration is key factor



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.
- Next Step
  - Survey network operators by means of a questionnaire

ICT security standards roadmap (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 will be a list of standards in development
- Part 4 will identify future needs and proposed new standards

Roadmap access

- 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).
- 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

Other projects

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

  www.itu.int/ITU-T/publications/index.html

- Security compendium:
  - catalogue of approved ITU-T Recommendations related to telecommunication security
  - extract of ITU-T approved security definitions
  - listing of ITU-T security related Questions

  www.itu.int/ITU-T/studygroups/com17/tel-security.html

- We are in the process of establishing a Security Experts Network (SEN) to maintain on-going dialogue on key issues of security standardization.

Observations

- Security is **everybody's business**
- Collaboration with other SDOs is **necessary**
- 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

Some useful web resources

- ITU-T Home page www.itu.int/ITU-T
- Study Group 17 www.itu.int/ITU-T/studygroups/com17
  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
- Security Roadmap www.itu.int/ITU-T/studygroups/com17/index