

# ITU-T NETWORK SECURITY INITIATIVES

Michael Harrop  
The Cottingham Group

.....



## Overview of Presentation

- Show the context of ITU-T security standards activities
- Highlight some of key areas of work on SG17 Working Party 2 and SG13 Q15
- Report in a little more detail on some of the results being achieved



# 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



# 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

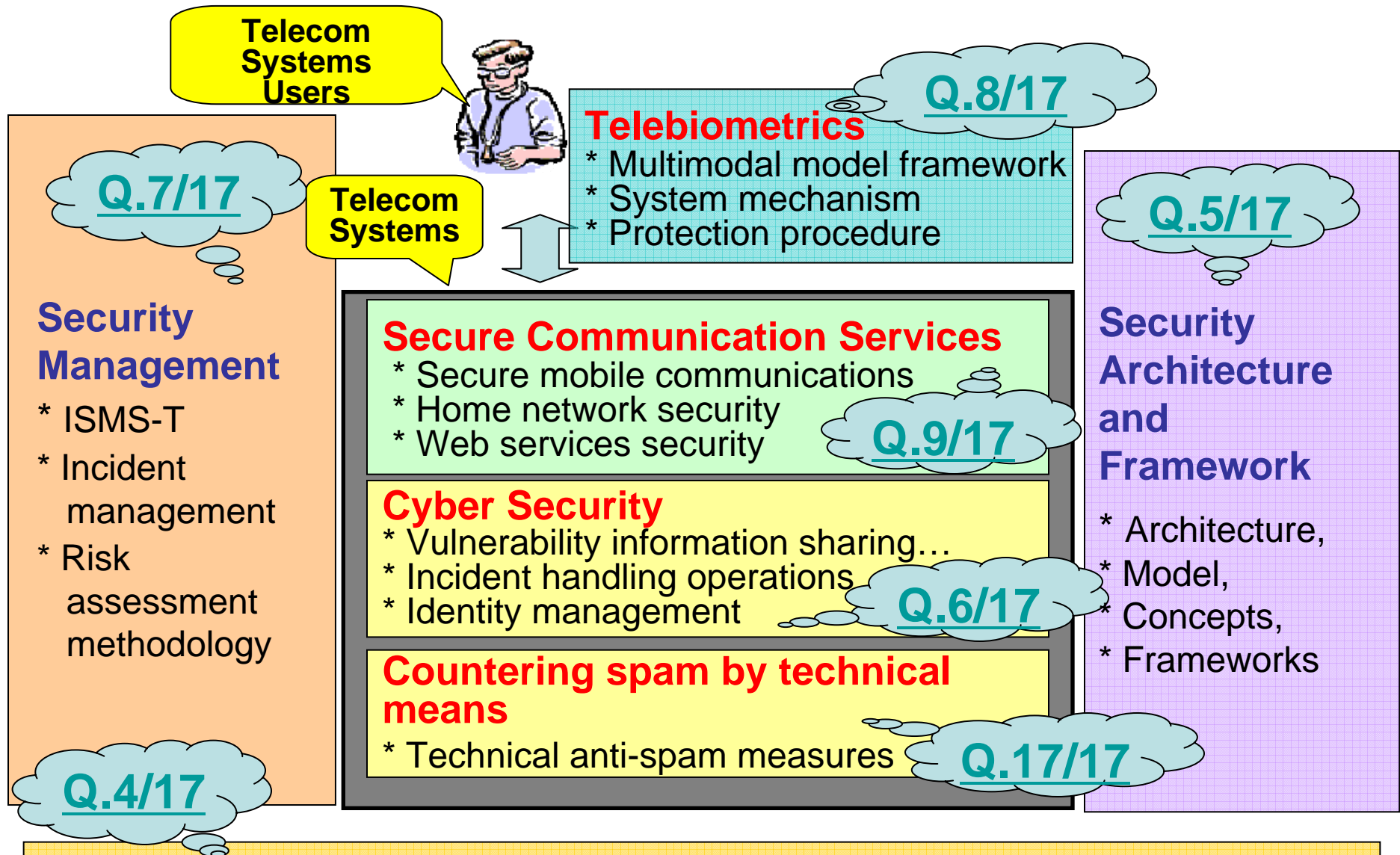
### Working Party 3:

- 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





# Overview of current security Questions and Recommendations under development



ITU-T

## Q4: Communications Systems Security Project

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



## Q5: 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



# 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

## Q6: 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

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



ITU-T

## Q8: Telebiometrics

- o 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.
- o Builds on existing work relating to personal identification and authentication using telebiometrics
- o It is being undertaken in close cooperation with related standards work being undertaken in other SDOs.



ITU-T

## Examples of Q8 Recommendations

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



ITU-T

## Q9: 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.

# Examples of Q9 Recommendations

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



## Q.17: Combating spam by technical means

Study items under consideration include:

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

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



## SG 17 Security Recommendations under development

- o 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](http://www.itu.int/itu-t/studygroups/com17)



ITU-T

## SG13 Q.15 – NGN Security

- o All SG 13 Recommendations have a section on security
- o Q15 aims to assure the security of the telecommunications infrastructure as PSTNs evolve to NGNs.
- o 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
- o NGN security activities and Recommendations are listed under “Work Program”
  - <http://www.itu.int/ITU-T/studygroups/com13/index.asp>



ITU-T

## Recent SG17 Workshops

- o 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
- o Digital Identity for Next Generation Networks
  - Held in December 2006 jointly with ITU-T/EU IST Daidalos Project
- o Conformance & Interoperability and Testing
  - Held in December 2006 to raise awareness of conformance and interoperability testing issues



ITU-T

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



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 In September, the FG will present the resulting security baseline as a proposed ITU-T Recommendation



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

- 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 will list security best practices



ITU-T

## Roadmap - 2

- o Part 2 is a searchable database that includes ATIS, ITU-T, ISO/IEC JTC1, IETF, ETSI IEEE and OASIS security standards.
- o The database format allows searching and to allows organizations to manage their own data
- o Publicly available under *Special Projects and\_Issues* at:
  - [www.itu.int/ITU-T/studygroups/com17/index](http://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

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



ITU-T

## 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)



ITU-T

## Summary

- WP2 security work is producing solid results to address current and emerging threats
- Threats are not going to diminish. We need to continue to focus on the security issue when developing all new ICT standards
- It is very important that we continue to work in concert with other SDOs and agencies with an interest in ICT security



*Thank you*