ITU-T Security Standard Activities

Koji NAKAO

Information Security Fellow, KDDI Corporation
Rapporteur, Security Management, Q7/SG 17, ITU-T
Chair of ISO/IEC JTC 1/SC 27/WG 4, Japan, &
Co-Chair of RAISS Forum
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

* Significant security work ** Lead Study Group on Security
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 new or revised Recommendations under development in SG 17 are available on the SG 17 web page at http://www.itu.int/itu-t/studygroups/com17
Security Standardization in ITU-T SG17 in relation to the other activities

ITU-T: Security for Telecom in SG17

- Secure Networking (Arc, NGN..)
- Cyber Security for Telecom
- Security Management for Telecom
- Telebiometorics
- AP Security (Web, Mobile, Home)
- SPAM

OMA
- DRM
- WPKI/WTLS

3GPP2
- NFCC

Forum: for the specific objective

Telecom

IETF: Internet Security Technologies
- AAA
- PKI
- SSL/TLS
- IPsec
- S/MIME

IEEE: for Chip vender
- IEEE802.1x
- IEEE P1363

SC27
- Encryption Algorithms
- Authentication mechanism
- Information Security Management for general
- Key management
- IC Card security
- Common Criteria for products security

ISO: General Technologies

SC17

SC37

Elementary Technologies
Against New Threats

• Facing a thousands of threats: Scan, DoS, DDoS, Virus, Worm, SPAM, Spyware, Other Malcodes...

• Occurrence of new threats: Botnets, Phishing, Farming...

Malicious activities directly connect to Business.
New Threat: Botnets

According to analysis of Agobot source code.

Owner of Botnets (HERDER)

DDoS!

IRC SV

Sometimes, many IRC Servers are used. It is configured at the site which Herder has hacked.

Malicious orders are transmitted via IRC

Internet

PCs at home and company

Infected PCs

TARGET

DDoS, SPAM, any
Video image : Bot
SPAM mail business by means of Zombie PCs

1. Send Mail Request
2. SPAM Mails
3. Mail Users
4. From Telecom-ISAC
Phishing fraud by means of Zombie PCs

Original Site

Web

Phishing Site

①

② Send Mail request

③

④ Mail Users

⑤

⑥

⑦

SPAM mails

Zombie PCs

From Telecommunication ISAC Japan
Security standardization
Collaboration is key

Specific Systems, Services, Applications
Security in ITU-T are developed by
SG 2, 3, 4, 5, 6, 9, 11, 13, 15, 16, 19

Core Technology and Common Security
Techniques in ITU-T are developed
by SG 17

JTC 1 SC 27, 37...
IETF
ATIS, ETSI, OASIS, etc.
Security standardization
Collaboration is key

- **World Standards Cooperation (WSC)** ISO, IEC, ITU
- **Global Standards Collaboration (GSC)** Regional, National SDOs and ITU-T, ITU-R
  - exchange information between participating standards organizations to facilitate collaboration and to support the ITU as the preeminent global telecommunication and radiocommunication standards development organization
  - Resolution GSC-11/17 Cybersecurity
- **Security Standardization Exchange Network (SSEN)**
  - an *informal* association of individual security practitioners with direct experience of, or strong interest in, security standardization
  - facilitate the informal exchange of information on security-standards-related matters to increase overall awareness of issues of common interest with the intention of helping to advance the development of needed standards and minimizing overlap and duplication of effort in security standards development
Security standardization
Collaboration is key


- Terms of Reference
  - To oversee standardization activities in ISO, IEC and ITU-T relevant to the field of security
  - To provide advice and guidance to the ISO Technical Management Board, the IEC Standardization Management Board and the ITU-T Telecommunication Standardization Advisory Group (TSAG) relative to the coordination of work relevant to security, and in particular to identify areas where new standardization initiatives may be warranted
  - To monitor implementation of the SAG-S Recommendations

- International workshop on security topics planned in conjunction with each SAG-S meeting
  - International Workshop on Transit Security, Washington DC, 4-5 October 2007

- Security portal under development
Focus Group: Security Baseline for Network Operators (FG SBNO)

- 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
- Achieved
  - Surveyed network operators by means of a questionnaire
- Next step:
  - Develop text to be proposed to SG 17 for progressing as an ITU-T publication
Focus Group: Identity Management (FG IdM)


- Established December 2006 by SG 17
- The objectives of the FG IdM are
  - to perform requirements analysis based on use case scenarios, in order
  - to identify generic IdM framework components, so that
  - a standards gap analysis can be completed, in order
  - to identify new standards work and the bodies (ITU and other SDOs) that should perform the work

- Working Group structure
  - Ecosystem and Lexicon Working Group
  - Use Cases Working Group
  - Requirements Working Group
  - Framework Working Group

- Aggressive schedule
  - Meetings held: February, April and May 2007; WG meeting June, July and August 2007
ICT Security Standards Roadmap

- Part 1 contains information about organizations working on ICT security standards
- Part 2 is the database of existing security standards
- Part 3 is a list of standards in development
- Part 4 identifies future needs and proposed new standards
- Part 5 includes security best practices

European Network and Information Security Agency (ENISA) and the Network and Information Security Steering Group (NISSG) are collaborating with ITU-T in the development of the Roadmap
ICT Security Standards Roadmap

- Part 2 currently includes ICT security standards from
  - ITU-T
  - ISO/IEC JTC 1
  - IETF
  - IEEE
  - ATIS
  - ETSI
  - OASIS

- Data is available in a database format to allow searching by organization and topic and to allow organizations to manage their own data

- We invite you to contribute content to the Roadmap, provide feedback and help us develop it to meet your needs
Other projects

- **Security in Telecommunications and Information Technology (ITU-T Security manual)**
  - Overview of existing ITU-T Recommendations for secure telecommunications
  - Third edition of June 2006 to be available in the six official languages of the ITU

- **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
The ITU Global Cybersecurity Gateway

LIVE at: http://www.itu.int/cybersecurity

Provides an easy-to-use information resource on national, regional and international cybersecurity-related activities and initiatives worldwide.
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  http://www.itu.int/ITU-T
- Study Group 17  http://www.itu.int/ITU-T/studygroups/com17
  - e-mail:  tsbsg17@itu.int
- ITU-T Lighthouse  http://www.itu.int/ITU-T/lighthouse
- ITU-T Workshops  http://www.itu.int/ITU-T/worksem
ITU-T SG 17 work on security

- Q.4/17 - Communications systems security project
- Q.5/17 - Security architecture and framework
- Q.6/17 - Cyber security
- Q.7/17 - Security management
- Q.8/17 - Telebiometrics
- Q.9/17 - Secure communication services
- Q.17/17 - Countering spam by technical means
Working Party 2/17 Work Program

Telecom Systems Users

Q.7/17

Security Management
* ISMS-T
* Incident management
* Risk assessment methodology

Q.4/17

Telebiometrics
* Multimodal model framework
* System mechanism
* Protection procedure

Q.8/17

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

Q.9/17

Cyber Security
* Vulnerability information sharing...
* Incident handling operations
* Identity management

Q.6/17

Countering spam by technical means
* Technical anti-spam measures

Q.17/17

Telecom Systems

Communications System Security Project
* Vision, Project, Roadmap, …
ITU-T SG 17 Question 4
Communications Systems Security Project
SG 17 – Q.4/17 results achieved

- Successful workshop organized at start of Study Period to consider future direction of security standards

- Security Standards Roadmap developed – includes security standards from ITU, ISO/IEC, IEEE, IETF, ATIS, ETSI, OASIS, 3GPP

- Security Compendium and Security Manual maintained and updated

- Security Baseline for Network Operators developed
SG 17 – Q.4/17 challenges

- Overall shortage of participants and contributors

- Roadmap issues/challenges:
  - Taxonomy (always a challenge!)
  - Finding out about new standards and when to post them
  - Appearance of the database
  - Need to develop a short guide to the update process
Security Roadmap

- The listing of standards has been converted to a searchable database
- Further updating is planned to ease navigation
- A new section (Part 5) has been added on (non-proprietary) Best Practices
SG 17 – Q.4/17 focus for next study period

• Will continue to be primary SG contact for security coordination issues
• Will maintain and update outreach material
  – Security Manual
  – Security Roadmap
  – Security Compendium
• Responsibilities will be limited to coordination and outreach – no Recommendations
ITU-T SG 17 Question 5
Security architecture and framework
Supplement to X.800-X.849, Guidelines for implementing system and network security

Recommendation X.805 has been a foundation of Q.5/17 security studies and shaped the scope of its work.
• Q.5/17 has developed Recommendations that further develop the concepts of X.805 and provide guidance on their implementation

• **X.1031**, *Security architecture aspects of end users and networks in telecommunications* - provides guidance on applying the concepts of the X.805 architecture for distributing the security controls between the telecommunication networks and the end user’s equipment.


• **X.1036**, *Framework for creation, storage, distribution and enforcement of policies for network security* further develops the concept of the security policy described in X.805.

• **Supplement to X.800-X.849**, *Guidelines for implementing system and network security* provides guidelines for implementing system and network security utilizing the concepts of X.805 and other security Recommendations and standards.
SG 17 – Q.5/17 strategic direction

- Development of a comprehensive set of Recommendations for providing standard security solutions for telecommunications in collaboration with other Standards Development Organizations and ITU-T Study Groups.
- Studies and development of a trusted telecommunication network architecture that integrates advanced security technologies.
- Maintenance and enhancements of Recommendations in the X.800-series and X.103x-series.
- Coordination of studies on NGN security (with Question 15/13)
SG 17 – Q.5/17 challenges

• Authentication and key agreement is one of the most complex and challenging security procedures. Question 5/17 has developed Recommendations that contribute to the standards solutions for authentication and key management

• X.1034, Guidelines on Extensible Authentication Protocol based Authentication and Key Management in a Data Communication Network
  – Establishes a framework for the EAP-based authentication and key management for securing the link layer in an end-to-end data communication network.
  – Provides guidance on selection of the EAP methods.

• X.1035, Password-Authenticated Key Exchange Protocol (PAK)
  – Specifies a protocol, which ensures mutual authentication of both parties in the act of establishing a symmetric cryptographic key via Diffie-Hellman exchange.
SG 17 – Q.5/17 major accomplishments

- **Recommendations** developed by Q.5/17:
  - **X.1031**, *Security architecture aspects of end users and networks in telecommunications*
  - **X.1034**, *Guidelines on Extensible Authentication Protocol based Authentication and Key Management in a Data Communication Network*
  - **X.1035**, *Password-Authenticated Key Exchange Protocol (PAK)*
  - **X.1036**, *Framework for creation, storage, distribution and enforcement of policies for network security*

- A **Supplement** developed by Q.5/17
  - **Supplement to X.800 - X.849 series** *Guidelines for implementing system and network security*

- Other technical documents prepared by Q.5/17
  - In response to the WTSA Resolution 50, Question 5/17 has prepared *Guidelines for designing secure protocols using ITU-T Recommendation X.805*.

- Major coordination activity conducted by Q.5/17
  - Question 5/17 has coordinated security studies with Question 15 of SG 13, *NGN Security* ensuring alignment of the standards work in both groups.
SG 17 – Q.5/17 actions for next study period

- How should a comprehensive, coherent communications security solution be defined?
- What is the architecture for a comprehensive, coherent communications security solution?
- What is the framework for applying the security architecture in order to establish a new security solution?
- What is the framework for applying security architecture in order to assess (and consequently improve) an existing security solution?
- What are the architectural underpinnings for security?
- What new Recommendations may be required for providing security solutions in the changing environment?
- How should architectural standards be structured with respect to existing Recommendations on security?
- How should architectural standards be structured with respect to the existing advanced security technologies?
- How should the security framework Recommendations be modified to adapt them to emerging technologies and what new framework Recommendations may be required?
- How are security services applied to provide security solutions?
ITU-T SG 17 Question 6
Cyber Security
SG 17 – Q.6/17 motivation

- Network connectivity and ubiquitous access is central to today’s IT systems
- Wide spread access and loose coupling of interconnected IT systems and applications is a primary source of widespread vulnerability
- Threats such as: denial of service, theft of financial and personal data, network failures and disruption of voice and data telecommunications are on the rise
- Network protocols in use today were developed in an environment of trust
- Most new investments and development is dedicated to building new functionality and not on securing that functionality
- An understanding of cybersecurity is needed in order to build a foundation of knowledge that can aid in securing the networks of tomorrow
SG 17 – Q.6/17 scope

- Definition of Cybersecurity
- Security of Telecommunications Network Infrastructure
- Security Knowledge and Awareness of Telecom Personnel and Users
- Security Requirements for Design of New Communications Protocol and Systems
- Communications relating to Cybersecurity
- Security Processes – Life-cycle Processes relating to Incident and Vulnerability
- Security of Identity in Telecommunication Network
- Legal/Policy Considerations
- IP traceback technologies
- Authentication Assurance
SG 17 – Q.6/17 challenges

- How should the current Recommendations be further enhanced for their wide deployment and usage?
- How to harmonize common IdM data models across the ITU
- How to define and use the term Identity within the ITU
- How to detect and predict future threats and risks to networks
- How to harmonize various IdM solutions
- What are the best strategies to improve Cybersecurity
- How to maintain a living list of IdM terms and definition and use it informally across the ITU
SG 17 – Q.6/17 highlights of activities

Completed Recommendations

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.1205</td>
<td>Overview of Cybersecurity</td>
</tr>
<tr>
<td>X.1206</td>
<td>A vendor-neutral framework for automatic checking of the presence of vulnerabilities information update</td>
</tr>
<tr>
<td>X.1207</td>
<td>Guidelines for Internet Service Providers and End-users for Addressing the Risk of Spyware and Deceptive Software</td>
</tr>
<tr>
<td>X.1250*</td>
<td>Requirements for global identity management trust and interoperability</td>
</tr>
<tr>
<td>X.1303</td>
<td>Common Alerting Protocol (CAP 1.1)</td>
</tr>
</tbody>
</table>

* Currently in the approval process
Recommendations under development

This Recommendation | International Standard provides a framework for entity authentication assurance which is the quantification of the risks that an entity is who or what he/she/it claims to be. In other words, entity authentication assurance is a measure of the confidence or risks associated with the authentication process and mechanisms.

ITU-T X.gopw, Guideline on preventing worm spreading in a data communication network
This Recommendation describes worm and other malicious codes spreading patterns and scenarios in a data communication network. The Recommendation provides guidelines for protecting users and networks from such malicious codes.
Recommendations under development

ITU-T X.idif, User Control enhanced digital identity interchange framework
This Recommendation defines a framework that covers how global interoperable digital identity interchange can be achieved and how an entity’s privacy is enhanced by providing an entity more control over the process of identity interchange. In addition, the Recommendation defines the general and functional requirements of the framework that should be satisfied. Based on the requirements, a framework is defined with basic functional building blocks for identity interchange and enhancing entity control.

ITU-T X.idm-dm, Common identity data model
This Recommendation develops a common data model for identity data that can be used to express identity related information among IdM systems.
SG 17 – Q.6/17 actions for next study period

- Enhance current Recommendations to accelerate their adoption
- Work with SG 2 in Trusted Service Provider Identifier (TSPID)
- Collaborate with Questions 5, 7, 9, 17/17 and with SG 2 in order to achieve better understanding of various aspects of network security
- Collaborate with IETF, OASIS, ISO/IEC JTC1, Liberty Alliance and other standardization bodies on Cybersecurity
- Work with OASIS on maintaining the OASIS Common Alerting Protocol V1.1 (ITU-T Recommendation X.1303)
- Study new Cybersecurity issues – How should ISPs deal with botnets, evaluating the output of appropriate bodies when available.
- Study technical aspects of Traceback techniques
- Joint work is ISO/JTC1 SC 27 on Entity Authentication Assurance
- Progress work with Liberty Alliance on Identity Authentication Frameworks
- Working with SG 4 and SG 13 on common IdM Data Models.
- Developing frameworks for User control enhanced digital identity interchange framework
- Developing guideline on protection for personally identifiable information in RFID application
- Developing requirements for security information sharing framework
- Developing guideline on preventing worm spreading in a data communication network
- Maintaining the IdM Lexicon document
SG 17 – Q.6/17 collaboration with other SDOs

- ISO/IEC JTC 1/SC 27
- IEC/TC 25
- IETF
- IEEE
- Liberty Alliance
- OASIS
- W3C
- 3GPP
- ETSI/TISPAN
ITU-T SG 17 Question 7
Security management
SG 17 – Q.7/17 scope

For telecommunications organizations, information and the supporting processes, facilities, networks and communications medias are all important business assets.

In order for telecommunications organizations to appropriately manage these business assets and to correctly continue the business activity, Information Security Management is extremely necessary.

The scope of this question is to provide GUIDELINES and BASELINES of Information Security Management to be appropriately applied for telecommunications organizations. Studies related on this issue can be a little bit extended to cover the following items:

- information security management guidelines (baseline)
- information incident management guidelines
- risk management and risk profiles guidelines
- assets management guidelines
- policy management guidelines
- information security governance
- etc.
SG 17 – Q.7/17 strategic directions

**Information Security Governance**

**Information Security Management Guidelines**

**X.1051**

**Baseline**

**Framework**

**X.ismf**

**Information Security Governance**

**X.sim: Security Incident Mang.**

**Vulnerability Handling**

**Announcement**

**Incident Handling**

**Alert Handling**

**Other Incident Management**

**Other Managements**

**Policy Mang.**

**Asset Mang.**

**Risk Mang.**

**Assets Management Methodology**

**Based on the proposals from NSMF**

**Practical Implementation Methodologies**

**Policy**

**Assets**

**Personnel**

**Physical**

**Operational Security**

**Access Controls**

**Organizational Security**

**BCP**

**Incident Management**

**Systems Security**

**Vulnerability Handling**

**Alert Handling**
SG 17 – Q.7/17 challenges

- How should information assets in telecommunications systems be identified and managed?
- How should information security policy for telecommunications systems be identified and managed?
- How should specific management issues for telecommunications organizations be identified?
- How should information security management system (ISMS) for telecommunications organizations be properly constructed by using the existing standards (ISO/IEC and ITU-T)?
- How should measurement of information security management in telecommunications be identified and managed?
- How should an information security governance framework be identified and managed?
- How should the small and medium telecommunications organizations be managed and applied for security?
SG 17 – Q.7/17 highlights of achievements

Recommendations

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.1051</td>
<td>Information security management guideline for telecommunications organizations based on ISO/IEC 27002</td>
</tr>
<tr>
<td>X.rmg*</td>
<td>Risk management and risk profile guide</td>
</tr>
<tr>
<td>X.sim*</td>
<td>Security incident management guidelines for telecommunications</td>
</tr>
<tr>
<td>X.ismf*</td>
<td>Information Security Management Framework for Telecommunications</td>
</tr>
</tbody>
</table>

* Currently under development
SG 17 – Q.7/17 actions for next study period

- Review the existing management Recommendations/Standards in ITU-T and ISO/IEC management standards as for assets identification and security policy management.
- Study and develop a methodology of assets identification and policy management for telecommunications based on the concept of information security management (X.1051).
- Study and develop information security management framework for telecommunications based on the concept of information security management (X.1051).
- Study and develop security management guidelines for small and medium telecommunications based on the concept of information security management (X.1051).
- Study and develop a methodology to construct information security management system (ISMS) for telecommunications organizations based on the existing standards (ISO/IEC and ITU-T).
- Study and develop an information security governance framework for telecommunications that encompasses information technology and information security management.
SG 17 – Q.7/17 collaboration with SDOs

- ISO/IEC JTC 1/SC27
- ETSI
- TTC
- NIST
ITU-T SG 17 Question 8
Telebiometrics
SG 17 – Q.8/17 scope

Digital key / Secure protocol / Authentication infrastructure / System mechanism / Protection procedure

Biometric Sensors

Acquisition (capturing) → NW → Extraction → NW → Matching → Storage → NW → Score → NW → Decision → NW → Application

Safety conformity

NW: Network
SG 17 – Q.8/17 strategic direction

Security and Protection for telebiometric application systems

Protection procedures

System mechanism among Client/Server/TTP

BioAPI interworking protocol

Authentication infrastructure Biometric Digital key

Safety in interaction with sensors
SG 17 – Q.8/17 challenges

- How should security countermeasures be assessed for particular applications of telebiometrics?
- How can identification and authentication of users be improved by the use of interoperable models for safe and secure telebiometric methods?
- What mechanisms need to be supported to ensure safe and secure manipulation of biometric data in any application of telebiometrics, e.g., telemedicine or telehealth?
- How should the current Recommendations be further enhanced for their wide deployment and usage?
SG 17 – Q.8/17
highlight of activities
Approved Recommendations

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.1082</td>
<td>Telebiometrics related to human physiology</td>
</tr>
<tr>
<td>X.1083</td>
<td>BioAPI Interworking Protocol</td>
</tr>
<tr>
<td>X.1084</td>
<td>Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles on telecommunication systems</td>
</tr>
<tr>
<td>X.1088</td>
<td>Telebiometrics digital key – A framework for biometric digital key generation and protection</td>
</tr>
<tr>
<td>X.1089</td>
<td>Telebiometrics authentication infrastructure</td>
</tr>
</tbody>
</table>
SG 17 – Q.8/17 actions for next study period

- Enhance current Recommendations to accelerate their adoption to various telebiometric applications and populate the telebiometric database.
- Review the similarities and differences among the existing telebiometrics Recommendations in ITU-T and ISO/IEC standards.
- Study and develop security requirements and guidelines for any application of telebiometrics.
- Study and develop requirements for evaluating security, conformance and interoperability with privacy protection techniques for any application of telebiometrics.
- Study and develop requirements for telebiometric applications in a high functionality network.
- Study and develop requirements for telebiometric multi-factor authentication techniques based on biometric data protection and biometric encryption.
- Study and develop requirements for appropriate generic protocols providing safety, security, privacy protection, and consent “for manipulating biometric data” in any application of telebiometrics, e.g., telemedicine or telehealth.
- Prepare a manual on telebiometrics.
SG 17 – Q.8/17 collaboration with other SDOs

- ISO/IEC JTC 1/SCs 17, 27 and 37
- ISO/TC 68 and TC 12
- IEC/TC 25
- IETF
- IEEE
- International Bureau of Weight and Measurement (BIPM)
ITU-T SG 17 Question 9
Secure Communication Services
SG 17 – Q.9/17 focus

- Develop a set of standards of secure application services, including
  - Mobile security
  - Home network security
  - Web Services security
  - Secure application services
  - NID/USN security Under study
  - Multicast security Under study
  - IPTV security Under study
SG 17 – Q.9/17 position of each topic

Mobile Terminal

Mobile security

Content Provider

Home network security

Mobile Network

Home Gateway

IPTV security/Multicast security

STB

Home network security

Home Network

Ubiquitous Sensor Network

USN security

USN Application Server

USN gateway

NID security

NID Application Server

NID reader

Secure application services/Web Services security

Application Server

Client
SG 17 – Q.9/17 strategic direction

- For developing the draft Recommendations on IPTV security matters:
  - Participate the ITU-T IPTV-GSI event (January - December, 2008) to develop them being consistent with relevant Recommendations being developed by other Questions
  - Propose X.iptvsec-1 (Requirements and architecture for IPTV security matter) for consent by September 2008, to meet urgent market need
  - Based on X.iptvsec-1, continue to study a set of possible draft Recommendations which complement X.iptvsec-1 technologically
- Continue to develop a set of draft Recommendations in domain-specific areas:
  - Mobile network, Home network, (mobile) Web Services, application services, NID/USN service, IPTV service multicasting service, etc.
- Continue to adopt or update the mature standards (i.e., SAML, XACML) developed by other SDOs, especially by OASIS, in the area of Web Services security
- Develop a common text of X.usnsec-1 (Security framework for USN) with ISO/IEC JTC 1/SC 6 (as of June 2008)
- Keep maintaining liaison activities with 3GPP, 3GPP2, JTC 1/SC 6, 25, 27 to develop the relevant draft Recommendations
SG 17 – Q.9/17 challenges

- For the domain-specific draft Recommendations, it needs to strengthen the coordination work with other relevant Questions/SDOs to develop them to be consistent with their work.

- During this Study period, Q.9/17 has been focused on the security framework for various domain-specific networks. However, from now on it should be emphasized to develop the pragmatic draft Recommendations which have significant impact on industry for the domain-specific networks with the collaboration with industries, other relevant SDOs and network/service providers.

- For developing the draft Recommendations on IPTV security matters, the various detailed work items should continue to be identified in the future.
SG 17 – Q.9/17 major achievements

- **Mobile security**
  - X.1123, General security value added service (policy) for mobile data communication, Approved 2007
  - X.1124, Authentication architecture in mobile end-to-end data communication, Approved 2007
  - X.1125, Correlative reacting system in mobile network, Approved 2007

- **NID security**
  - X.1171, Framework for Protection of Personally Identifiable Information in Networked ID Services, Consented 2008

- **Home network security**
  - X.1111, Framework for security technologies for home network, Approved 2007
  - X.1112, Certificate profile for the device in the home network, Approved 2007
  - X.1113, Guideline on user authentication mechanisms for home network service, Approved 2007
  - X.homesec-4 Authorization framework for home network, to be consented 2008

- **USN security**
  - X.usnsec-1 Requirement and Framework for Ubiquitous Sensor Network, New work item in 2007
SG 17 – Q.9/17 major achievements (2)

- **Multicast Security**
  - X.mcsec-,1 Security Requirement and Framework in Multicast communication, New work item in 2007

- **IPTV security**
  - X.iptvsec-1, Functional Requirements and architecture for IPTV security aspects, New work item in 2008
  - X.iptvsec-2, Requirement and mechanism for Secure Transcodable Scheme, New work item in 2008
  - X.iptvsec-3, Key management framework for secure IPTV communications, New work item in 2008

- **Web Services security**
  - X.1143, Security architecture for message security in mobile Web Services, Approved 2007

- **Secure applications services**
  - X.1151, Guideline on strong password authentication protocols, Approved 2007
  - X.1152, Secure end-to-end data communication techniques using Trusted Third Party services, Consented 2008
  - X.1161, Framework for secure peer-to-peer communications, Consented 2008
  - X.1162, Security architecture and operations for peer-to-peer network, Consented 2008
Divide Q.9/17 into two Questions: Q.O/17 and Q.P/17, considering the enormous workloads.

**Q.9/17 for current Study Period**
- Secure Communication Service
  - Mobile Security
  - Home network security
  - NID/USN security
  - Multicast security
  - IPTV security
  - Web Service security
  - Secure application security

**Q.O/17 for Next Study Period**
- Security aspects for ubiquitous telecommunication service
  - Mobile Security
  - Home network security
  - NID/USN security
  - Multicast security
  - IPTV security, etc.

**Q.P/17 for Next Study Period**
- Secure application services
  - Web Service security
  - Secure application service, etc.
SG 17 – Q.17/17: Countering spam by technical means

ITU-T SG 17 Question 17
Countering spam by technical means

• Scope
• Strategic direction
• Challenges
• Highlights of activities
• Actions for next study period
• Collaboration with SDOs
SG 17 – Q.17/17 scope

- Develop a set of standards for countering spam by technical means, including:
  
  - General technical strategies and protocols for countering spam
  
  - Guidelines, frameworks and protocols for countering email spam, IP multimedia spam, SMS spam and other new types of spam
SG 17 – Q.17/17 strategic direction

Technical strategies on countering spam (X.1231)

- Technologies involved in countering email spam (X.1240)
- Technical framework for countering email spam (X.1241)
- Overall aspects of IP multimedia application spam (X.1244)

- Framework Recommendations: IP multimedia application area (X.fcsip)
- Technology Recommendations: Interactive countering spam gateway system (X.tcs-1) etc.
- Technical means for countering email spam (X.tcs) TBD

- SMS spam Filtering System Based on Users’ Rules (X.ssf)
SG 17 – Q.17/17
challenges

• 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 advanced telecommunication network technologies (for example, SMS, instant messaging, VoIP) offer unique opportunities for spam that require unique solutions?
• What technical work is already being undertaken within the IETF, in other fora, and by private sector entities to address the problem of spam?
• What telecommunication network standardization work, if any, is needed to effectively counter spam as it relates to the stability and robustness of the telecommunication network?
SG 17 – Q.17/17 highlights of activities

Approved Recommendations

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.1231</td>
<td>Technical Strategies on Countering Spam</td>
</tr>
<tr>
<td>X.1240</td>
<td>Technologies involved in countering email spam</td>
</tr>
<tr>
<td>X.1241</td>
<td>Technical framework for countering email spam</td>
</tr>
<tr>
<td>X.1244*</td>
<td>Overall aspects of IP multimedia application spam</td>
</tr>
</tbody>
</table>

* Currently in approval process
SG 17 – Q.17/17 actions for next study period

• Act as the lead group in ITU-T on technical means for countering spam
• Establish effective cooperation with the relevant ITU Study Groups, other standard bodies and appropriate consortia and fora.
• Identify and examine the telecommunication network security risks introduced by the constantly changing nature of spam.
• Develop a comprehensive and up-to-date resource list of the existing technical measures for countering spam in a telecommunication network that are in use or under development.
• Determine whether new Recommendations or enhancements to existing Recommendations, including methods to combat delivery of spyware, worm, phishing, and other malicious contents via spam and combat compromised networked equipment including botnet delivering spam.
• Provide regular updates to the Telecommunication Standardization Advisory Group and to the Director of the Telecommunication Standardization Bureau to include in the annual report to Council.
SG 17 – Q.17/17 collaboration with SDOs

• **Standardization bodies:**
  – IETF
  – ISO/IEC JTC 1

• **Other bodies:**
  – OECD
  – MAAWG.
Thank you for listening Q&A