Summary of ITU-T Study Groups with security-related activities

Prepared for ITU-T Security Workshop, 3rd/4th October 2005

SG 2: Operational aspects of service provision, networks and performance
(Lead Study Group for service definition, numbering and routing)

http://www.itu.int/ITU-T/studygroups/com02/index.asp

SG2 is responsible for studies relating to principles of service provision, definition and operational requirements of service emulation; numbering, naming, addressing requirements and resource assignment including criteria and procedures for reservation and assignment; routing and interworking requirements; human factors; operational aspects of networks and associated performance requirements including network traffic management, quality of service (traffic engineering, operational performance and service measurements); operational aspects of interworking between traditional telecommunication networks and evolving networks; evaluation of feedback from operators, manufacturing companies and users on different aspects of network operation.

Security-related Questions:

- Q.1/2 (A/2) Application of Numbering, Naming, and Addressing Plans for telecommunications and Service and Operational aspects of numbering, including service definition (F.851)
- Q.1/2 (A/2) Application of Numbering, Naming, and Addressing Plans for telecommunications and Service and Operational aspects of numbering, including service definition (F.851)

SG4: Telecommunication Management
(Lead Study Group on telecommunication management.)

http://www.itu.int/ITU-T/studygroups/com04/index.asp

Contributed by Martin Soukup and Greg Jones
SG4 is responsible for studies regarding the management of telecommunication services, networks, and equipment, including support for next generation networks (NGN) and the application and evolution of the telecommunication management network (TMN) framework. Additionally, it is responsible for other telecommunication management studies relating to designations, transport-related operations procedures, and test and measurement techniques and instrumentation.

As the lead study group for management activities, Study Group 4 work on security addresses the following areas:
a) Architectural considerations and requirements for the management interfaces,
b) Detailed requirements for securing the management network (also referred to as the management plane), specifically as the networks are becoming converged, c) Protocol and models to support securing management information and management of security parameters.

Management of Telecommunications network is defined at different levels of abstractions, from managing network element level information to management services offered to the customer. The security requirements for the information exchanged between management systems and between management systems and network elements depend on whether the management networks are within one administration or between administrations. Based on the architectural principles, explicit requirements, mechanisms and protocol support have been defined in existing Recommendations and additional ones are under development.

History

X.736 Security Alarm Reporting (1992)
- Defines a mechanism for reporting alarms for security events

X.740 Security Audit Trail Function (1992)
- Defines a protocol for generation/collection of security audit information

X.741 Objects and attributes for access control (1993)
- Defines the information necessary for implementation and management of access control infrastructure

M.3016 TMN Security Overview (1998)
- Overviews the security threats to a TMN and security services which may be applied to protect against them

Q.813 Security Transformations Application Service Element for Remote Operations Service Element (STASE-ROSE)
Q.815 Specification of a security model for whole message protection (2000)
Q.817 TMN PKI - Digital certificates and certificate revocation lists profiles (2001)

Recent Work

M.3016 series (2005)

The M.3016 series replaces the original (1998) M.3016 document
Describes the relevance and applicability of security in the context of the TMN language
Rather than mandating a set of services for threat protection, provides a framework for specific organizations to make appropriate specification of the use of available mechanisms

Covers the following threats in the TMN

- Masquerading
- Eavesdropping
- Unauthorized access
- Loss or corruption of information
- Repudiation
- Forgery
- Denial of service

Covers the following security features

- Confidentiality
- Data Integrity
- Accountability
- Availability

M.3016.0

- Defines Security Objectives and Threats in the context of the TMN

M.3016.1

- Defines Security Requirements and how they address Threats

M.3016.2

- Defines Security Services and how they address Requirements

M.3016.3

- Defines Security Mechanisms (functional blocks) and how they address Services

M.3016.4

- Defines a Profile Proforma for defining the specification of which Mechanisms, Services, and Requirements must and should be supported in a given technological or regional domain (specified by each SDO)

Implications of Recent Work

M.3016.4 provides a proforma mechanism allowing other SDOs to state required compliancy levels to the relevant threats to a TMN in their domain.

Allows a consistent language, set of mechanisms, which could be shared and/or interoperable in implementation and documentation method which eases analysis and information sharing between domains and other bodies

The M.3016 series is viewed as a key aspect of NGN Management;
it is included in:

- The NGN Management Roadmap issued by the NGNMFG
- M.3060 on the Principles of NGN Management

Future Work

- Internationalization through proforma approach of TMOC Issue 56 Security Management System in a M.3016 series style including integration of X.7xx series documents.
- M.3016 extension to cover service management, management application security, X interface support, and security availability.
- Addition of UML Security Profile to M.3020 methodology.

Potential Future Work

- Alignment of security audit trail function with current IDS mechanisms and IETF
- Endorsement of OASIS SPML (Security Provisioning Markup Language

SG 5: Protection against electromagnetic environment effects

http://www.itu.int/ITU-T/studygroups/com05/index.asp

Contributed by Jeffrey Boksiner

SG5 is responsible for studies relating to protection of telecommunication networks and equipment from interference and lightning as well as for studies related to electromagnetic compatibility (EMC), to safety and to health effects connected with electromagnetic fields produced by telecommunication installations and devices, including cellular phones.

During the current Study Period the security aspects of the work of ITU-T Study Group 5 (SG5) are addressed under Question 15, *Security of telecommunication and information systems regarding the electromagnetic environment*. This is a new Question approved for the current Study Period.
Electromagnetic threats involve malicious man-made high power transient phenomena such as High-Altitude Electromagnetic Pulse (HEMP) and emissions from High-Power Electromagnetic (HPEM) generators including High-Power Microwave (HPM) and Ultra-Wideband (UWB) sources. Also, electromagnetic security involves addressing information leaks from telecommunication networks by unexpected radio emission from equipment.
In general, SG5 is responsible for studies relating to protection of telecommunication networks and equipment from interference and lightning as well as for studies related to electromagnetic compatibility (EMC), and to electrical safety and to health effects connected with electromagnetic fields produced by telecommunication installations and devices. In fulfilling its mission in the past SG 5 has worked on several Questions and developed a number of Recommendations and Handbooks that contribute indirectly to the security of the network against electromagnetic threats. However, presently SG5 has a Question specifically dedicated to Electromagnetic Security and is developing several Recommendations to address this issue.
Study items to be considered include, but are not limited to:

- Technical requirements for preventing information leaks by unexpected radio emission from equipment and protection of telecommunication systems from attacks using high power radio waves (HEMP, HPEM)
- Mitigation methods such as electromagnetic shielding
- Methodology for evaluating the protective measures

The presently proposed structure for the ITU-T K series Recommendations on electromagnetic security is based on the information security management system for telecommunication of ITU-T Recommendation X.1051. The overall structure is shown in the following diagram

ITU-T X.1051

|___(A)K.sec (new Recommendation)
| |_____(B) K.hemp (new Recommendation)
| |_____(C) K.hpem (new Recommendation)
| |_____(D) K.leakage (new Recommendation)
| |_____K.43,K.48, etc (existing Recommendations)
| |_____K.44,K.45,K.20,K.21, etc (existing Recommendations)
|_____(E) K.secmiti (new Recommendation)

where the new proposed Recommendations dedicated to Electromagnetic Security are the following:

(A) K.sec: Concept, Risk assessment, and how to select / know the requirement (B)-(D), and K series.

(B) K.hepm: Describes the electromagnetic environment for High-Altitude Electromagnetic Pulse

(C) K.hpem: Describes the for High-Power Electromagnetic environment

(D) K.leakage: Will address information leakage through unintentional emission

(E) K.secmiti: Will provide mitigation methods for the various threats.

In the past several years, IEC Subcommittee 77C has developed several publications describing the HEMP and HPEM environment (conducted and radiated) for civil systems and equipment. SG5 has established a liaison with IEC SC 77C and has recently held a technical workshop with chairman of IEC SC 77C William Radasky.

SG 6: Outside Plant and related indoor installations

http://www.itu.int/ITU-T/studygroups/com06/index.asp

Responsible for studies relating to outside plant such as the construction, installation, jointing, terminating, protection from corrosion and others forms of damage from environment impact, except electromagnetic processes, of all types of cable for public telecommunications and associated structures.

Security-related Questions:
Q.1/6 (A/6) Environmental and Safety Procedures for Outside Plant
Q.6/6 (F/6) Optical fibre cable network maintenance

SG9: Integrated broadband cable networks and television and sound transmission
(Lead Study Group on integrated broadband cable and television networks.)

http://www.itu.int/ITU-T/studygroups/com09/index.asp

SG9 is responsible for studies relating to:

a) Use of cable and hybrid networks, primarily designed for television and sound programme delivery to the home, as integrated broadband networks to also carry voice or other time critical services, video on demand, interactive services, etc.

b) Use of telecommunication systems for contribution, primary distribution and secondary distribution of television, sound programmes and similar data services.

As the lead study group on integrated broadband cable and television networks it evaluates threats and vulnerabilities to broadband networks and services, documents security objectives, evaluates countermeasures, and defines security architectures.

Security related activities have focused on the following areas:

a) *Secure broadband services:* provide security services for broadband access networks. Namely, authentication of the cable modem, cryptographic key management, privacy and integrity of transmitted data, and secure download of cable modem software

b) *Secure VoIP services:* IPCablecom is a special project on time-critical interactive services over cable television network using IP-protocol, in particular Voice and Video over IP. Security services provided in IPCablecom include authentication of the Multimedia Terminal Adapter (MTA) to the service provider, authentication of the service provider to the MTA, secure device provisioning and configuration, secure device management, secure signalling, and secure media.

c) *Secure home networking services:* Enhanced Cable Modems can provide home networking services such as firewalls and Network Address Translation. Security services provided for enhanced Cable Modems include authentication of the Multimedia Terminal Adapter (MTA) to the service provider, authentication of the service provider to the MTA, secure device provisioning and configuration, secure device management, packet-filtering/firewall functionality, secure firewall management, and secure download of enhanced cable modem software.

d) *Secure application environments for interactive television services:* Interactive television services rely on the security services defined in Java and the Multimedia Home Platform (MHP) specification.

Security-related Questions:

Q.3/9 (C/9) Methods and practices for conditional access, protection against unauthorized copying and against unauthorized redistribution ("redistribution control" for digital cable television distribution to the home) (J.93, J.96 Amd 1)

Q.8/9 (H/9) Cable television delivery of digital services and applications that use Internet Protocols (IP) and/or packet-based data (J.112)

Q.9/9 (I/9) Voice and video IP applications over cable television networks (J.160, J.170, J.191)

Q.10/9 (J/9) The extension of cable-based services over broadband in Home Networks

SG11: Signalling requirements and protocols
(Lead Study Group on Signalling and Protocols and Intelligent Networks.)

http://www.itu.int/ITU-T/studygroups/com11/index.asp

Contributed by: Yukio Hiramatsu

ITU-T Study Group 11 is the lead Study Group on signalling and protocols and on intelligent networks. Most of SG 11's current Recommendations were developed for trusted TDM based networks in which point to point connections could be used to ensure communications security. SG 11 recognized that introduction of IP technology into the network would present new security challenges. In recognition of the introduction of IP technology and the need to be able to provide signalling and control information capability in this evolving network in a secure manner, SG 11 generated a suite of questions related to signalling requirements and protocol that took into account these new security challenges in 2004.

The ITU-T SG 13 FGNGN was developed to jumpstart NGN activities within the ITU-T and it was assigned responsibilities for many NGN areas, including the development of generic architectures, signalling requirements as well as generic security requirements. The FGNGN will complete is programmed activities in December 2005 and at that time the responsibilities for generation of NGN standards deliverables will move back to their respective host Study Groups. Thus, responsibility for developing NGN signalling requirements and protocol deliverables will move back to SG 11. SG 11 is prepared to accept the challenge of developing signalling requirements and protocol standards for this new environment. Study Group 11 has developed a security action plan, consistent with the approach laid out in Recommendation X.805. One aspect of this plan requires that a security section to be added to all new and revised Recommendations.

In particular on a going forward basis, SG 11 will continue to be responsible for generating signalling requirements and protocols that will be used to perform various functions, e.g. session establishment as well as for call admission control. These requirements are obliged to include content to ensure the security of the network and its resources.

SG 11 is looking forward to addressing these challenges.

SG 12: Performance and quality of service
(Lead Study Group on Quality of Service and performance**)**

http://www.itu.int/ITU-T/studygroups/com12/index.asp

SG 12 is responsible for Recommendations on the end-to-end transmission performance of terminals and networks, in relation to the perceived quality and acceptance by users of text, data, speech, and multi-media applications. Although this work includes the related transmission implications of all networks (e.g., those based on PDH, SDH, ATM and IP as well as NGNs) and all telecommunication terminals (e.g., handset, hands-free, headset, mobile, audiovisual, and interactive voice response), a special focus is given to IP QoS, interoperability and implications for NGN, and also includes work on performance and resource management.

Security-related Questions:
Q.13/12 (M/12) Multimedia QoS/QoE performance requirements and assessment methods
Q.17/12 (M/13) Performance of IP-based networks
Q.18/12 (N/13) Transmission error and availability performance (G.827)

SG 13: Next Generation Networks
(Lead Study Group for NGN and satellite matters.)

http://www.itu.int/ITU-T/studygroups/com13/index.asp

Contributed by: Igor Faynberg

SG 13 is responsible for studies relating to the architecture, evolution and convergence of next generation networks including frameworks and functional architectures, signaling requirements for NGN, NGN project management coordination across study groups and release planning, implementation scenarios and deployment models, network and service capabilities, interoperability, impact of IPv6, NGN mobility and network convergence and public data network aspects.
Recognizing that security is one of the defining features of NGN, SG 13 has established a special question for the detailed studies on security – Question 15, *NGN Security*. The question is focused on studies of the NGN-specific security issues and development of the standard security solutions for NGN. One of the essential goals of SG 13 is to put in place a set of standards that will guarantee, to the maximum degree possible, the security of the telecommunications infrastructure as PSTNs evolve to NGNs.
The major study items on security will provide the answers to at least the following questions:

- What new Recommendations, enhancements to existing Recommendations or guidance to other Study Groups are needed to standardize identification and cataloguing NGN threats and vulnerabilities?
- What are the security requirements of NGNs to effectively counter these threats? Which of these requirements should be included in all NGNs and which could be offered as an optional service?
- What new Recommendations or guidance are necessary to enable comprehensive, end-to-end security in NGNs that span across multiple heterogeneous administrative domains?
- What new Recommendations or guidance are necessary to enable attachment of terminals in a secure fashion, including Authentication, Authorization, and Accounting (AAA) considerations, to NGNs?

The major tasks of SG 13 with regard to security include:

- Lead the NGN-specific security project-level issues within SG 13 and with other Study Groups. Recognizing SG 17's overall role as the Lead Study Group for Telecommunication Security, advise and assist SG 17 on NGN security coordination issues.
- Determine how to apply Recommendation X.805 *Security Architecture for Systems Providing End-to-end Communication* within the context of an NGN environment.
- Ensure the developed NGN architecture is consistent with accepted security principles.
- Ensure AAA principles are integrated as required throughout the NGN.

On all NGN-related security matters SG 13 works in close cooperation with ITU-T Study Groups 2, 4, 9, 11, 15, 16, 17, and 19. In addition, SG 13 has a special relationship with the ITU-T NGN Focus Group (FGNGN). Through the liaison process and the active participation of its representatives, SG 13 has been actively involved in security studies conducted by the FGNGN Security Capabilities working group (FGNGN WG 5). The FGNGN WG 5 plans to transfer (by the end of 2005) its security work to SG 13. The expected output of the FGNGN WG 5 are two documents: *Security Requirements for NGN Release 1* and *Security Requirements for NGN Release.* These documents will be further developed within SG 13 with the goal of establishing new security Recommendations for NGN.

ITU-T SG 17 (Lead Study Group on security) is another group within ITU-T, which SG 13 has especially close relationship with. It has been decided that all SG 13 Recommendations having security-related specifications should be reported to Study Group 17 in order to allow timely updating of the "Catalogue of the approved security Recommendations" and "Compendium of ITU-T Approved Security Definitions."

In addition to collaboration on security within ITU, SG 13 also continues building its cooperation on security with other standards development organizations. Working relationship with the IETF (Internet, Security, and Transport Areas), 3GPP and 3GPP2, and DSL Forum are among most important to SG 13 for its security studies.

Main security-related Questions:
Q.2/13 - Requirements and implementation scenarios for emerging services in NGN
Q.6/13 - NGN mobility and fixed-mobile convergence
Q.8/13 - Service scenarios and deployment models of NGN
Q.10/13 - Interoperability of satellite with terrestrial and Next Generation Networks (NGNs)
Q.15/13 - NGN Security
It should be noted that Question 15/13 has a major responsibilities for studies of security for NGN.

SG 15: **Optical and other transport networks**
(Lead Study Group on Access Network Transport and on Optical Technology.)

http://www.itu.int/ITU-T/studygroups/com15/index.asp

Question 14 in Study Group 15 (Q.14/15) is responsible for specifying the management and control requirements and supporting information models for transport equipment. Q.14/15 has been following the ITU-T established TMN concept and framework for the definition of these requirements and models. Security management is one of the five key TMN management functional categories. Security management has been within the scope of and under study by Q.14/15.

a) Requirements for transport equipment management: G.7710/Y.1701, G.784, and G.874 address the Equipment Management Functions (EMFs) inside a transport Network Element that are common to multiple technologies, specific to SDH NE, and specific to OTN NE, respectively. Applications are described for Date & Time, Fault Management, Configuration Management, Account Management, Performance Management and Security Management. These applications result in the specification of EMF functions and their requirements. Security management requirements in these Recommendations are currently under study.

b) Data Communication Network Architecture and Requirements: G.7712/Y.1703 defines the architecture requirements for a Data Communications Network (DCN) which may support distributed management communications related to the Telecommunications Management Network (TMN), distributed signaling and routing communications related to the Automatically Switched Optical Network (ASON), and other distributed communications (e.g., Orderwire or Voice Communications, Software Download). Various applications (e.g., TMN, ASTN, etc.) require a packet based communications network to transport information between various components. For example, the TMN requires a communications network, which is referred to as the Management Communications Network (MCN) to transport management messages between TMN components (e.g., NEF component and OSF component). ASON requires a communications network, which is referred to as the Signalling Communications Network (SCN) to transport signalling messages between ASTN components (e.g., Call Controller, Connection Controller). G.7712/Y.1703 references M.3016 for MCN security requirements. SCN security requirements are defined in G.7712/Y.1703.

c) Distributed Call and Connection Management: G.7713/Y.1704 provides the requirements for the distributed call and connection management for both the User Network Interface (UNI) and the Network Node Interface (NNI). The requirements in this Recommendation specify the communications across interfaces to effect automated call operations and connection operations. Security attributes are specified, along with others, to allow verification of call and connection operations (e.g., this may include information to allow authentication of the call request, and possibly integrity checking of call request).

d) Architecture and requirements for routing in the automatically switched optical networks: G.7715/Y.1706 specifies the requirements and architecture for the routing functions used for the establishment of switched connections (SC) and soft permanent connections (SPC) within the framework of the ASON. The main areas covered in this Recommendation include the ASON routing architecture, functional components including path selection, routing attributes, abstract messages and state diagrams. This Recommendation references ITU-T Rec. M.3016 and X.800 for security considerations. In particular, it states that, depending on the context of usage of a routing protocol, the overall security objectives defined in ITU-T Rec. M.3016 of confidentiality, data integrity, accountability and availability may take on varying levels of importance. A threat analysis of a proposed routing protocol should address the following items based on ITU-T Rec. X.800; i.e. masquerade, eavesdropping, unauthorized access, loss or corruption of information (includes replay attacks), repudiation, forgery and denial of service.

e) Framework of ASON Management: G.7718/Y.1709 addresses the management aspects of the ASON control plane and the interactions between the management plane and the ASON control plane. Fault management, configuration management, accounting management, performance managements, and security management requirements for the Control plane components are included.

Main security-related Questions:

- Q.14/15 – Management and control of transport systems and equipment

SG 16: **Multimedia services, systems and terminals**
(Lead Study Group on multimedia services, systems and terminals, e-business and e-commerce.)

http://www.itu.int/ITU-T/studygroups/com16/index.asp

Study Group 16 is the lead study group on multimedia services, systems and terminals, and lead on e-business and e-commerce. Question G (of WP 2/16) covers "Security of Multimedia Systems and Services" and addresses the following security issues.

Advanced multimedia (MM) applications like telephony over packet-based networks, Voice-over-IP, interactive conferencing and collaboration; MM messaging, Audio/Video streaming and others are subject to a variety of crucial security threats in heterogeneous environments. Misuse, malicious tampering, eavesdropping, and denial-of-service attacks are just a few of the potential risks; especially on IP-based networks.
It is recognized that those applications have common security needs that could be satisfied by generic security measures; e.g. by network security. Yet, MM applications typically are subject to application-specific security needs that could best be fulfilled by security measures at the application layer. Question G focuses on the application-security issues of MM applications and takes complementary network security means into account as appropriate.

Main security-related Questions:
- Q.G/16 – Security of Multimedia Systems and Services

SG17: Security, languages and telecommunication software
(Lead Study Group for security)

http://www.itu.int/ITU-T/studygroups/com17/index.asp

SG 17 is responsible for studies relating to security, the application of open system communications including networking and directory, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems.

SG 17 has been designated the LSG for Telecommunication Security. Activities of the LSG for Telecommunication Security may be categorized as core activities centred on defining and maintaining overall security frameworks, and project management activities involving the coordination, assignment and prioritization of efforts that would lead to timely communication system security Recommendations.

A number of SG17 sub-projects have a specific security mandate:

4/17 Communications Systems Security Project

This Question is dedicated to the vision setting and the coordination and organization of the entire range of communications security activities within ITU-T. A top-down approach to the Security question will be used with collaboration with other Study Groups and other SDOs. This project is directed towards achieving a more focused effort at the project and strategic level.

5/17 Security Architecture and Framework

To achieve cost-effective comprehensive security solutions that can be applied to various types of networks, services and applications in a multi-vendor environment, network security should be designed around the standard security architectures and standard security technologies. Taking into account the security threats to communication environment and the current advancement of security countermeasures against the threats, this project examines new security requirements and solutions and how security architectures and frameworks can be developed to reflect the evolving environment.

6/17 Cyber Security

This question considers aspects of cyber security in the context of international standardization. In particular the question is examining the following areas of cyber security:

* processes for distribution, sharing and disclosure of vulnerability information.
* standard procedure for incident handling operations in cyber space.
* strategy for protection of critical network infrastructure.

7/17 Security Management

The aim of this question is to develop a set of Recommendations on security management for ITU-T, taking into account the need for collaboration with ISO/IEC JTC1. The question focuses particularly on identification and management of risk in telecommunications systems, and the alignment of the information security management system (ISMS) for telecommunications carriers with existing ISMS standards.

8/17 Telebiometrics

This question builds on existing work relating to personal identification and authentication using telebiometrics and is being undertaken in close cooperation with related standards work being undertaken in other SDOs. In particular it 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.

9/17 Secure Communication Services

Due to some specific characteristics of the mobile communications (e.g. over the air transmission, limited computing power and memory size of the small mobile devices), providing security is an especially challenging task that deserves special attention and study. 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.

SG 19: Mobile Telecommunications Networks
(Lead Study Group on mobile telecommunications networks and mobility)

http://www.itu.int/ITU-T/studygroups/com19/index.asp

Contributed by John Visser

SG19 (formerly the ITU-T Special Study Group on "IMT-2000 and Beyond") has included security as a key aspect of its referencing Recommendations for IMT-2000 (3G) Family Members identified in its Q.1741.x (3GPP) and Q.1742.x (3GPP2) series Recommendations. These include an evaluation of perceived threats and a list of security requirements to address these threats, security objectives and principles, a defined security architecture (i.e., security features and mechanisms), cryptographic algorithm requirements, lawful interception requirements, and lawful interception architecture and functions. These studies are dealt with in Question 3, 6 and 7/SSG. The prime objective of the Lawful Interception studies are to identify useful interception and monitoring related information that need to be provided by service providers to national law enforcement agencies. The interception related information and the content of communication may be technology independent or dependent on 3G or evolved 3G mobile networks.

Main security-related Questions:

Q.1/19 - Service and network capability requirements and network architecture
Q.3/SSG – Identification of existing and evolving IMT-2000 systems
Q.5/SSG – Convergence of evolving IMT-2000 networks with evolving fixed networks