ITU-T
The leader in standards for Telecommunication Systems Security

In the development of Recommendations, ITU-T study groups (SG) take security into account as a matter of course. Study Group 17, as the Lead SG on Communication System Security, handles the general security guidance and coordination of the security-related work across all ITU-T study groups.

Current important security work in ITU-T includes:

Next Generation Network (NGN) Security Framework
NGN security is crucial. ITU-T addresses security aspects in NGN architecture, Quality of Service (QoS), network management, mobility, billing and payment.

Multimedia
With the foundations for multimedia conferencing security in place, improvements continue towards higher levels of end-to-end privacy and confidentiality, sophisticated key management, better inter-working with SIP/SDP and smooth NAT/firewall proxy traversal.

Security Frameworks Guidelines
This includes revision to X.805 and a guideline on cyberattack protection

Security Management
Complements X.1051, methodologies for incident management and risk management are considered.

Awareness
A list of security-related ITU-T Recommendations and a compendium of ITU-T approved security definitions is maintained at: www.itu.int/itudoc/itu-t/com17/activity

Secure Communication Services
Enhancements to security specifications for mobile end-to-end data communication, consideration of security requirements for web services and application protocols.

For further information on ITU-T Study Groups:
www.itu.int/ITU-T/studygroups

A security manual “Security in telecommunications and information technology - An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications” is electronically available at: www.itu.int/itudoc/itu-t//85097.html

Examples of key ITU-T Recommendations on security issues

E.408 – Telecommunication networks security requirements
Provides an overview of security requirements and a framework that identifies security threats to telecommunication networks in general (both fixed and mobile, voice and data) and gives guidance for planning countermeasures that can be taken to mitigate the risks arising from the threats.

X.805 – Security architecture for systems providing end-to-end communications
Defines the general security-related architectural elements that, when appropriately applied, can provide end-to-end network security. It addresses security concerns for the management, control and use of network infrastructure, services and applications.

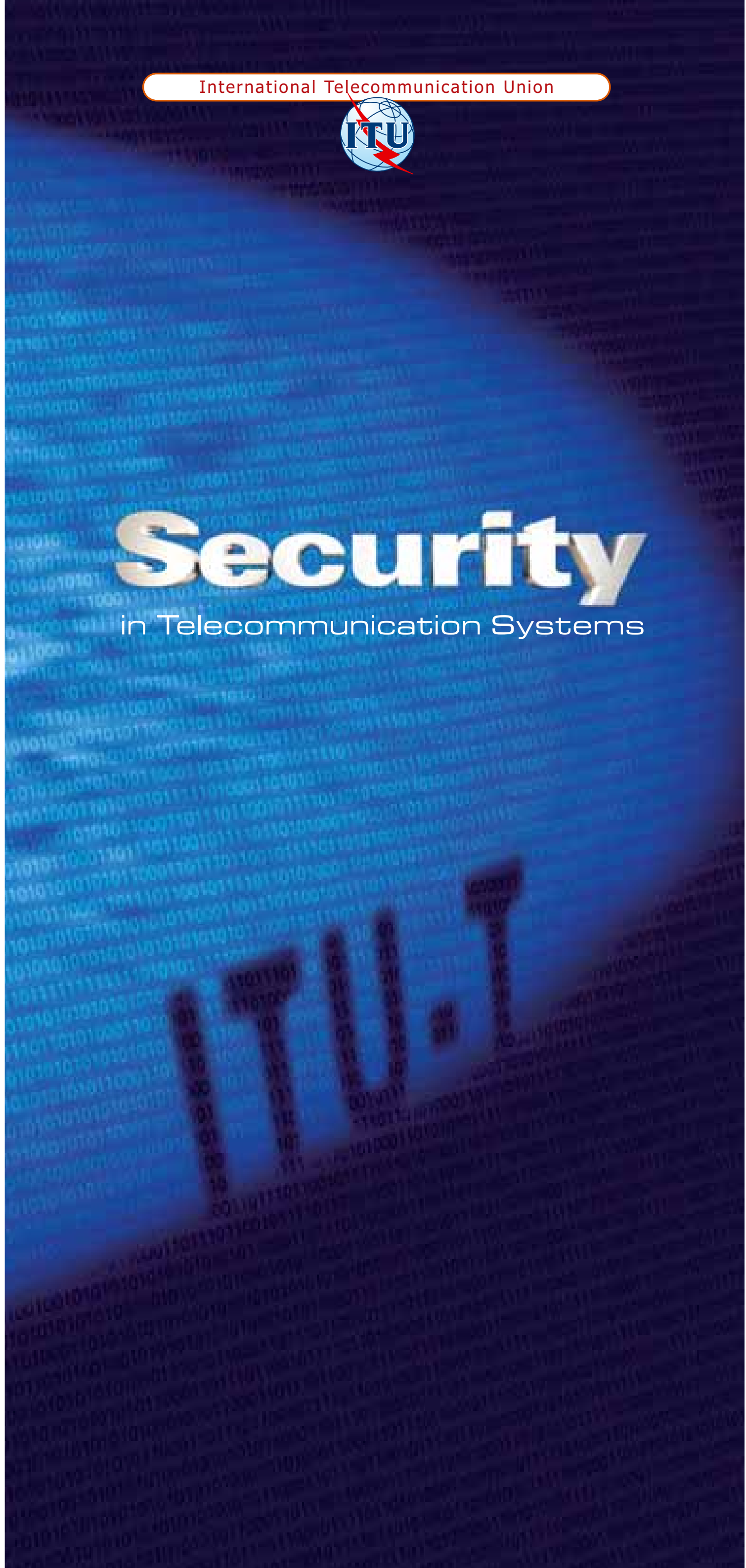
X.509 – The Directory: Public-key and attribute certificate frameworks
X.509 public-key certificates are widely used. In every secure browser session using SSL, a certificate is used to authenticate the web server and to agree on the encryption key that will be used to protect the information exchanged. The certificate is also used to authenticate and protect e-mail. An electronic document with a digital signature that is supported by an X.509 certificate is recognized as the most credible form of electronic document.

H.235 – Security and encryption for H-Series multimedia systems
Defines the security infrastructure and security services – e.g. authentication and privacy – for use by the H.300-Series multimedia systems in both point-to-point and multipoint applications (including VoIP and videoconferencing). The Recommendation utilizes the general facilities supported in Recommendation H.245 and H.225.0 and, as such, any standard which operates in conjunction with this control protocol may use this security framework.

J.170 – IPCablecom security specification
Defines the security requirements for IPCablecom architecture, which details how cable television operators can deliver two-way capability to provide a variety of IP time critical services, including voice communications.

X.1051 – Information security management system – Requirements for telecommunications (ISMS-T)
Provides the requirements of information security management for telecommunication organizations. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of overall business risks within telecommunications.

09.2004 standards@itu.int



International Telecommunication Union

ITU

Security
in Telecommunication Systems

ITU-T Security Building Blocks

Security Architecture and Frameworks

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

E.408 – Telecommunication network security requirements
E.409 – Incident organization and security incident handling: Guidelines for telecommunication organizations
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 the 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 (TTP) services
X.843 – Specification of TTP services to support the application of digital signatures

Directory Services and Authentication

H.350 – Series – Directory services architecture for multimedia conferencing
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 telecommunication 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 multimedia systems
H.323 Annex J – Packet based multimedia communications systems – Security for simple endpoint types
H.530 – Symmetric security procedures for H.323 mobility in H.510
T.123 Annex B – Network-specific data protocol stacks for multimedia conferencing: extended transport connections

Facsimile

T.36 – Security capabilities for use with Group 3 facsimile terminals
T.503 – A 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. See: http://www.itu.int/publications/bookshop/how-to-buy.html
(this site includes information on limited free access to ITU-T Recommendations)