ITU-T The leader in standards for Communication Systems Security

ITU-T Study Group 17 is the lead ITU-T Study Group for communication systems security matters.

Current important security work in ITU-T includes:

Telebiometrics
Focusing on telebiometric devices connected to open networks, and the need to model taxonomy of telebiometric methods, devices and solutions for security purposes.

Security Management
Identifying which security controls should be in place requires careful planning and attention to detail. This work addresses the study of information security management systems (ISMS) such as risk assessment, identification of assets and implementation characteristics for telecommunication operators.

Mobility Security
The consideration of security problems resulting from mobile device restrictions such as low power, small memory size, small display, with the intent to develop security solution based on the requirements for the mobile environment.

Emergency Telecommunications
The study of the security issues for emergency telecommunication services, considering the vulnerabilities of these systems and networks, and the solutions required.

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

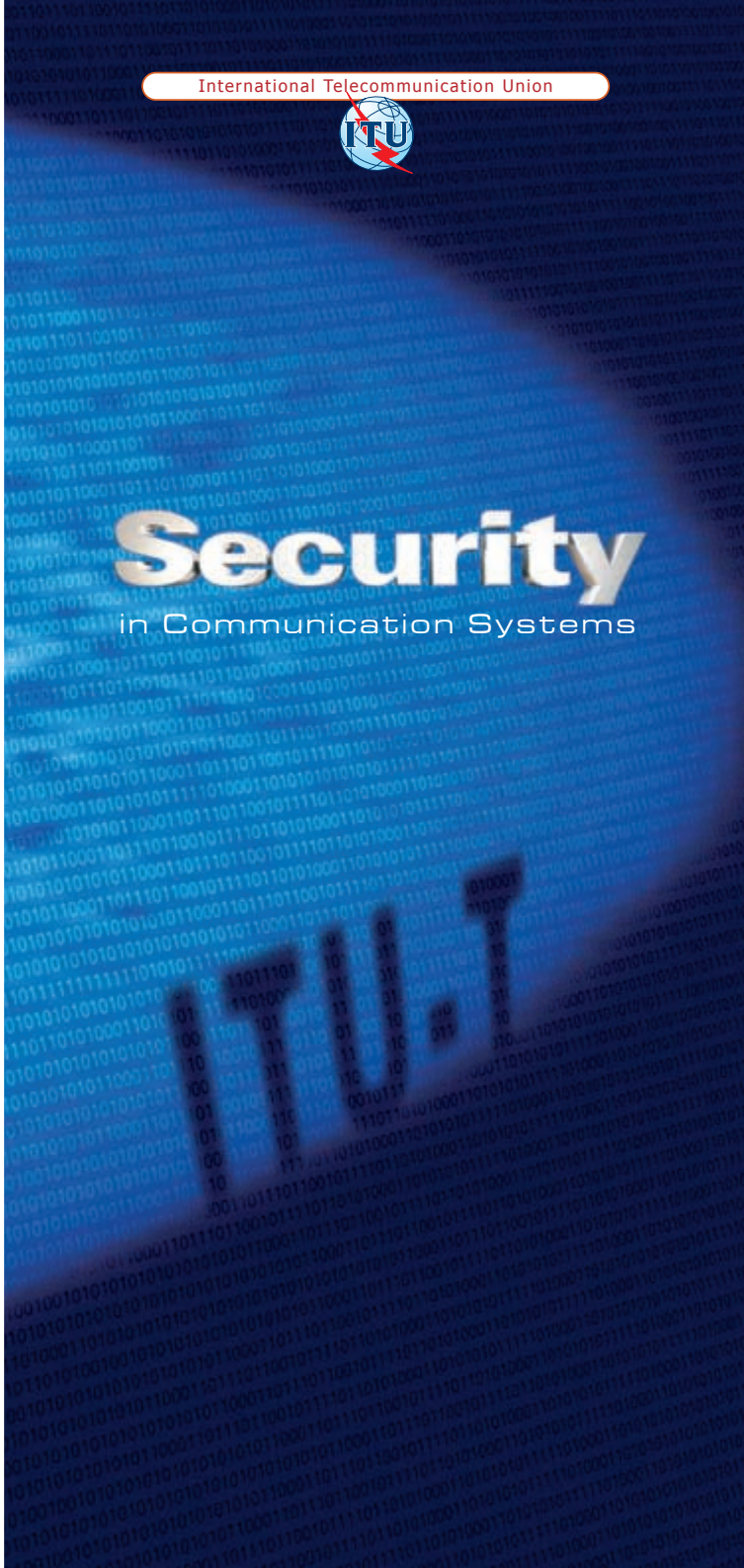
A list of security-related ITU-T Recommendations and a compendium of ITU-T approved security definitions can be found at:
http://www.itu.int/itudoc/itu-t/com17/activity

Examples of key ITU-T Recommendations on security issues

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 in the session. The certificate is also used to authenticate and protect e-mail and is the cornerstone of time-stamping services. Many countries now allow electronic documents to be considered equivalent to a paper document. An electronic document with a digital signature that is supported by an X.509 certificate is recognized in many countries as the most credible form of electronic document.

H.235 – Security and encryption for H-Series multimedia terminals
– defines the security infrastructure and security services such as authentication and privacy, i.e. data encryption, for use by the H.3xx series of multimedia terminals in both point-to-point and multipoint applications, e.g. the increasingly common H.323 terminals for operation on IP-based networks. The Recommendation utilizes the general facilities supported in Recommendation H.245 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 the IPCablecom architecture, which details how cable television operators can deliver a two-way capability to provide a variety of IP time critical services, including voice communications.



08.05.2002

ITU-T Security Building Blocks

Network Management Security

M.3010 – Principles for a telecommunications management network
M.3016 – Overview of TMN security
M.3210 – Security management for IMT-2000
M.3320 – Management requirements framework for the TMN X interface
M.3400 – TMN management functions

Directory Services & Authentication

X.500 – Overview of concepts models and services
X.501 – Models
X.509 – Public-key and attribute certificate frameworks
X.519 – Protocol specification

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

Security Architecture Framework

X.800 – Security architecture for OSI for ITU applications
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

Protocols

X.273 – OSI – Network layer security protocol
X.274 – OSI – Transport layer security protocol

Facsimile

T.30 Annex G – Procedures for secure G3 document facsimile transmission using the HKM and HFX system
T.30 Annex H – Procedures for security in facsimile Group 3 based on the RSA algorithm
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

Security in Frame Relay

X.272 – Data compression and privacy over frame relay networks

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 delivery of digital television or cable television systems
J.170 – IPCablecom security specification

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

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 terminals
H.323 Annex J – Packet based multimedia communications systems – Security for simple endpoint types

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)