International Telecommunication Union

Security Standardization in ITU-T

Telecommunication Standardization Bureau

Simão Campos, Counsellor, Simao.Campos@itu.int

ITU Seminar on Standardization
Accra, Ghana, 27-28 May 2004

Overview

- High-level directives >>
- Areas of work >>
- Involved ITU-T Study Groups >>
- Highlights of the work >>
- Resources >>
- Conclusion >>

- *Additional Slides* >>

High level directives

ITU Plenipotentiary Conference 2002

Resolution 130 - Strengthening the role of ITU in information and communication network security

resolves

1 to review ITU's current activities in information and communication network security;

2 to intensify work within existing ITU study groups in order to:

a) reach a common understanding on the importance of information and communication network security by studying standards on technologies, products and services with a view to developing recommendations, as appropriate;

b) seek ways to enhance exchange of technical information in the field of information and communication network security, and promote cooperation among appropriate entities;

c) report on the result of these studies annually to the ITU Council.

world summit
on the **information society**
Geneva 2003 - Tunis 2005

- Two Phases:
  - Geneva, 10–12 December 2003
  - Tunis, 16–18 November 2005
- Website www.itu.int/wsis/
- Phase 1 Output Documents:
  - *Declaration of Principles*
  - *Plan of Action*
  - *URL:* >>
    http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160

Declaration of Principles

- Build confidence and security in the use of ICTs (Sec.5, pg.5, para.35, 36, 37)
  - Strengthening the trust framework
  - Prevention of cybercrime/misuse of ICT
  - Fight SPAM (unsolicited electronic messages)

Plan of Action (Action Line C5)

- Cooperation of all stakeholders (gov'ts, civil society, private sector)
- Guidelines, legislation, share good practices
- User education (privacy, etc)
- National legal instruments for formal recognition of electronic documents (e.g. authentication)
- Strengthen real-time incident handling and response
- Development of secure and reliable applications
- Contributions to the intergov'l agencies working groups (e.g. ITU)

Areas of work

A Taxonomy…

- General Guidance/Architecture
  - Network perspective
  - Users' perspective
- System/Application-Specific
  - Secure Infrastructure
  - End-to-end security

General Guidance

- Overall concepts and architecture
- Public Key Infrastructure (PKI) /
  Privilege Management Infrastructure (PMI)
- Incident Handling

Specific Implementations

- Secure Infrastructure
  - The underlying network provides the needed security
  - IP Cablecom (← IETF's IPSec)
  - Segregated Management Plane
  - Signalling (SS7, BICC)
  - Restoration
- End-point security
  - Does not assume that underlying network is capable to provide needed security (e.g. H.323 system and T.36 secure fax transmission)

Areas of work

- **Not only IP !!!**
- General Guidance
  - ITU-T Study Group 17 (*Lead SG for Communications Security*)
  - ITU-T Study Group 2
- System/Application-Specific
  - ITU-T Study Group 16 (Multimedia, H.323 in particular)
  - ITU-T Study Group 9 (IP-Cablecom)
  - ITU-T Study Group 4 (Management)
  - ITU-T Special Study Group IMT2000 & Beyond
  - ITU-T Study Group 11 (Signalling)

Vulnerabilities, Threats and Risks

- **Vulnerability:** by threat model (e.g. SS7), design (e.g. Ambiguities in BGP), implementation (e.g. SNMP, ASN.1) or configuration (e.g. 802.11b)
- **Threat:** people willing to exploit a vulnerability (hackers, criminals, terrorists, etc)
- **Risk:** the consequences of such an exploitation (data loss, fraud, loss of public confidence, etc)
- While threats change over time, security vulnerabilities exist throughout the
  life of a protocol
  → Risks must be continuously reassessed !!!

Involved ITU-T Study Groups

ITU-T Study Groups

www.itu.int/ITU-T/

- ***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, including TMN
- **SG 5** Protection against electromagnetic environment effects
- **SG 6** Outside plant
- **SG 9** **Integrated broadband cable networks and television and sound transmission**
- ***SG 11*** *Signalling requirements and protocols*
- ***SG 12*** *End-to-end transmission performance of networks and terminals*
- ***SG 13*** *Multi-protocol and IP-based networks and their internetworking*
- ***SG 15*** *Optical and other transport networks*
- **SG 16** **Multimedia services, systems and terminals**
- **SG 17** **Data networks and telecommunication software**
- ***SSG*** *Special Study Group "IMT-2000 and beyond"*
- **TSAG** Telecommunication Standardization Advisory Group

Highlights
SG 17

ITU-T Study Group 17

- Lead Study Group for Communication System Security
  - Coordination/prioritization of security efforts
  - Development of core security Recommendations
  - Manage the ITU-T Security Project
  - Maintain Compendia on Security-related Recommendations and Security Definitions

- Existing Recommendations include
  - Security architecture, model, frameworks, and protocols for open systems (X.800- & X.270-series)
  - Trusted Third Party Services (X.842/X.843)
  - Public-key and attribute certificate frameworks (X.509)
  - Security architecture for end-to-end communications (X.805)

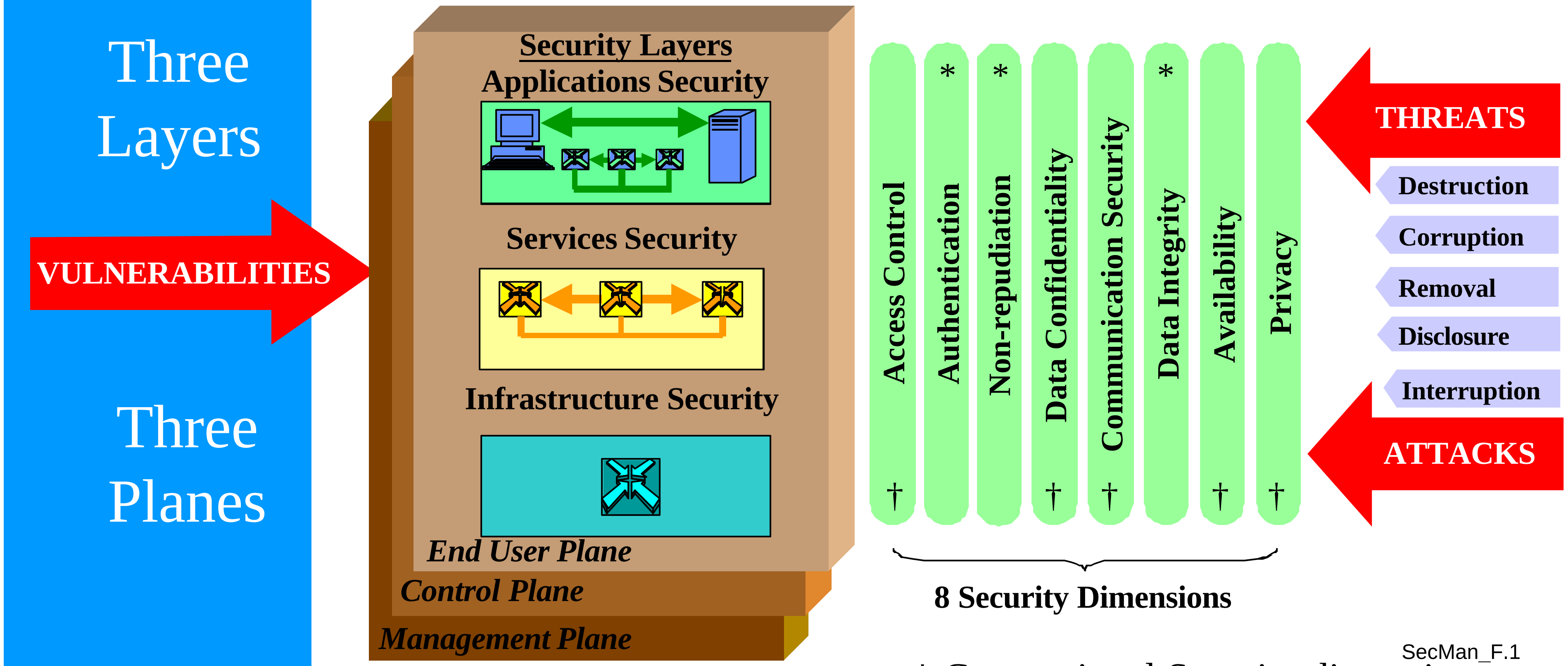
ITU-T SG 17 Security Focus

- **Authentication (X.509) -** *Rev.Planned: 2005*
  - Ongoing enhancements as a result of more complex uses: alignment with LDAP; distributed page resources; other
- **Security Architecture** (X.805) Approved 2003
  - For end-to-end communications
- **Telebiometric Multimodal Model** (X.1081, ex-X.tb)
  - A framework for the specification of security and safety aspects of telebiometrics
- **Security Management System** (X.1051, ex-X.ism)
  - For risk assessment, identification of assets and implementation characteristics
- **Mobile Security** (X.1121 and X.1122, ex-X.msec)
  - For mobile end-to-end data communications

X.805 - Security Architecture for End-to-End Communications

Three Layers

Three Planes



SecMan_F.1

* Conventional Security dimensions

† New concepts in X.805 (next slide)

- Vulnerabilities can exist in each Layer, Plane and Dimension
- 72 Security Perspectives (3 Layers ✖ 3 Planes ✖ 8 Dimensions)

X.805 – Security Dimensions

- X.805 differentiates *Privacy (association of users to their action) /Confidentiality (eavesdropping, tampering, etc)*
- *Communication* security dimension ensures that information flows only between authorized end points (information is not diverted or intercepted between these end points)
- *Access Control* security: prevention of unauthorized access to resources. It is related but beyond authentication.
- *Availability* dimension: avoid network interruption (includes network restoration, disaster recovery, etc)

Mobile Security – Multi-part standard

- X.1121 – Framework of security technologies for mobile end-to-end data communications

  - describes security threats, security requirements, and security functions for mobile end-to-end data communication

  - from the perspectives of the mobile user and application service provider (ASP)

- X.1122 – Guideline for implementing secure mobile systems based on PKI

  - describes considerations of implementing secure mobile systems based on PKI, as a particular security technology

- Security Policy (under development)

  - different quality of security service needs to satisfy various requirements of security services of both user and ASP

Telebiometrics – X.1081

- Model for security and public safety in telebiometrics
- Authentication based on “what you are” instead of “what you know” (PIN #,etc) – augments “what you have” (ID cards, etc)
- Biometric authentication
  - Provide a framework for developing a taxonomy of biometric devices
  - Facilitate the development of authentication mechanisms based on both static (e.g., fingerprints) and dynamic (e.g. gait or signature pressure variation) personal attributes

SG 17 security challenge

- SG 17 is the "Lead Study Group" for security issues in ITU-T >>
- Lead Study Group work is organized into several questions:
  - G/17, Security Project
  - H/17, Security Architecture and Framework
  - I/17, Cyber Security
  - J/17, Security Management
  - K/17, Telebiometrics
  - L/17, Secure Communication Services

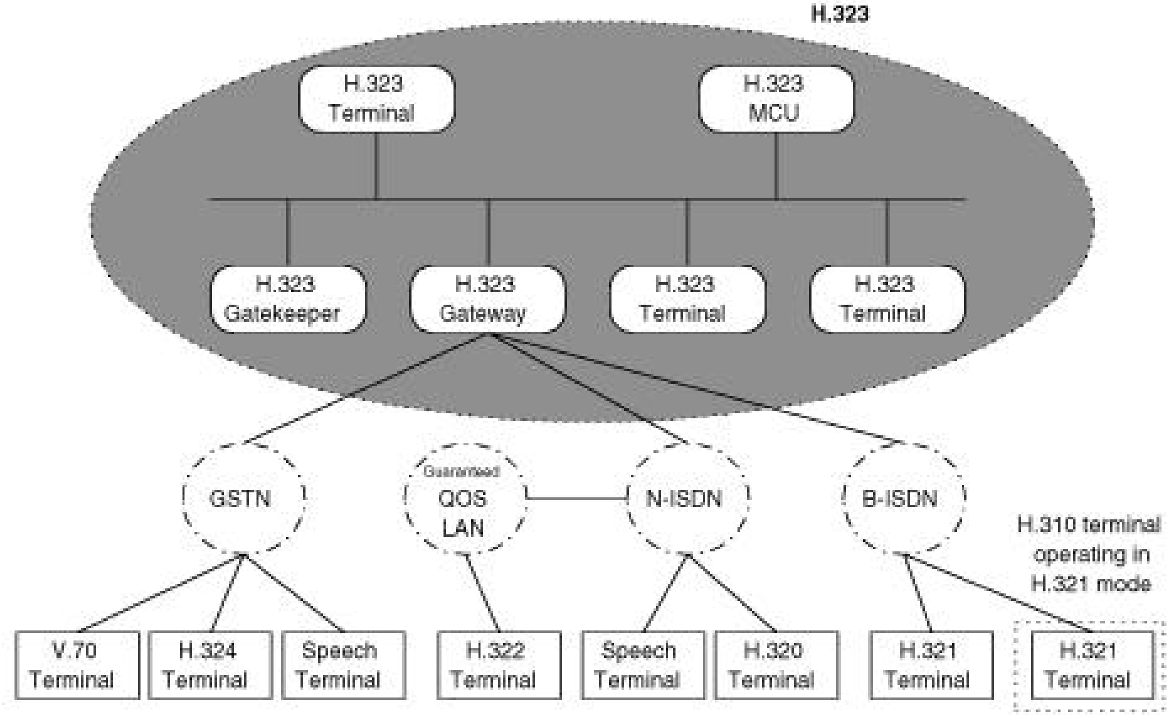
(Note: Question numbers above will be revised after WTSA-04)

Highlights
SG 16

Security studies in ITU-T SG 16 (application-specific)

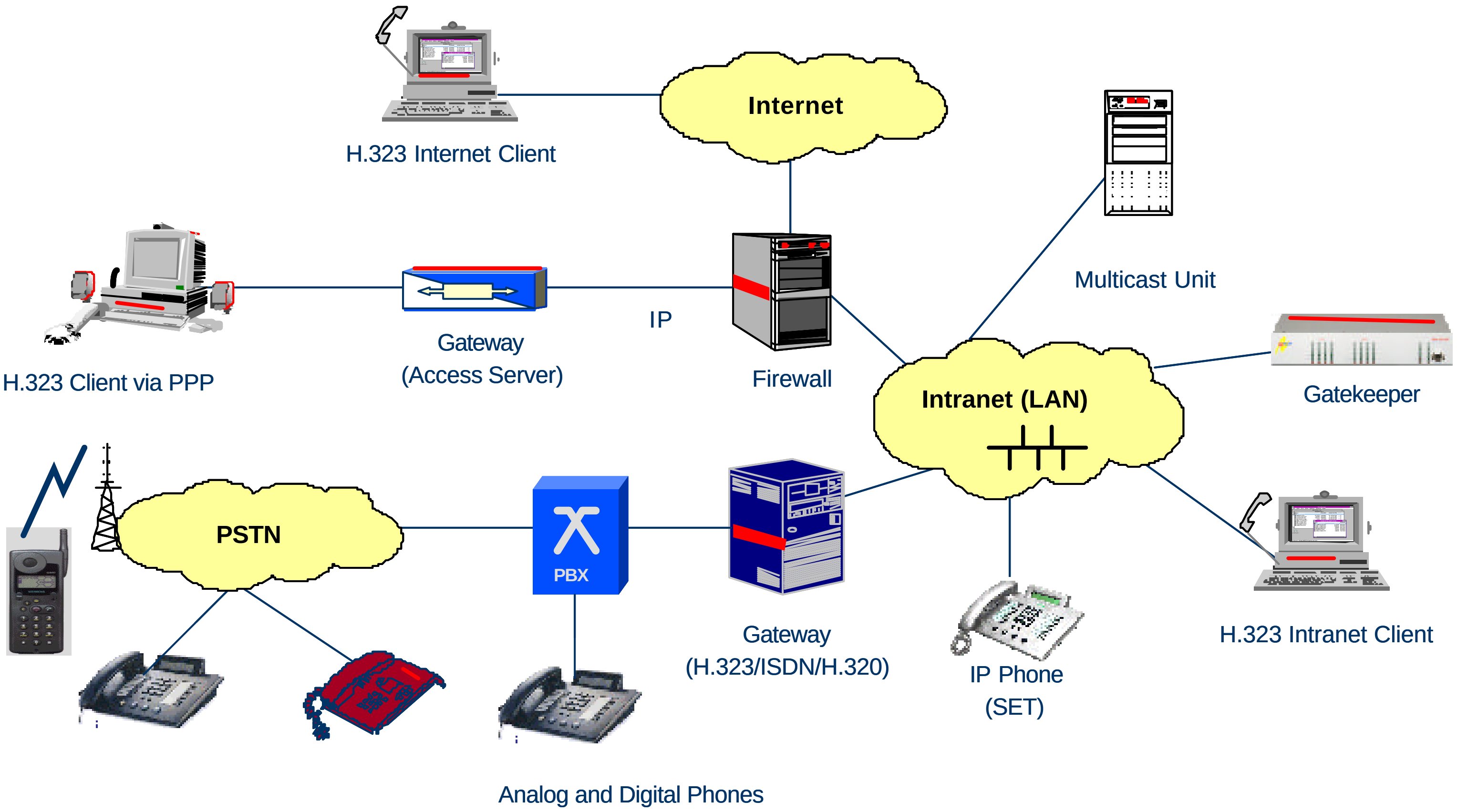
- “Lead Study Group” on Multimedia and on E-business/E-Commerce >>
- Focal point for security issues in the SG: *Question G/16 - “Multimedia Security”*
  - Secure H.323-based IP Telephony
    - *H.235 and associated security profiles*
    - *H.530: Security for H.323 mobility*
  - Secure H.320 Audio/Video and T.120 Data Conferencing
  - Secure H.248 Media Gateway Decomposition
  - H.350-series: MM Directory (H.235 extension)
  - T.36: Secure fax transmission
  - Security aspects in TDR & E-health

Functional view of H.323



- H.323 was the first VoIP protocol ever defined

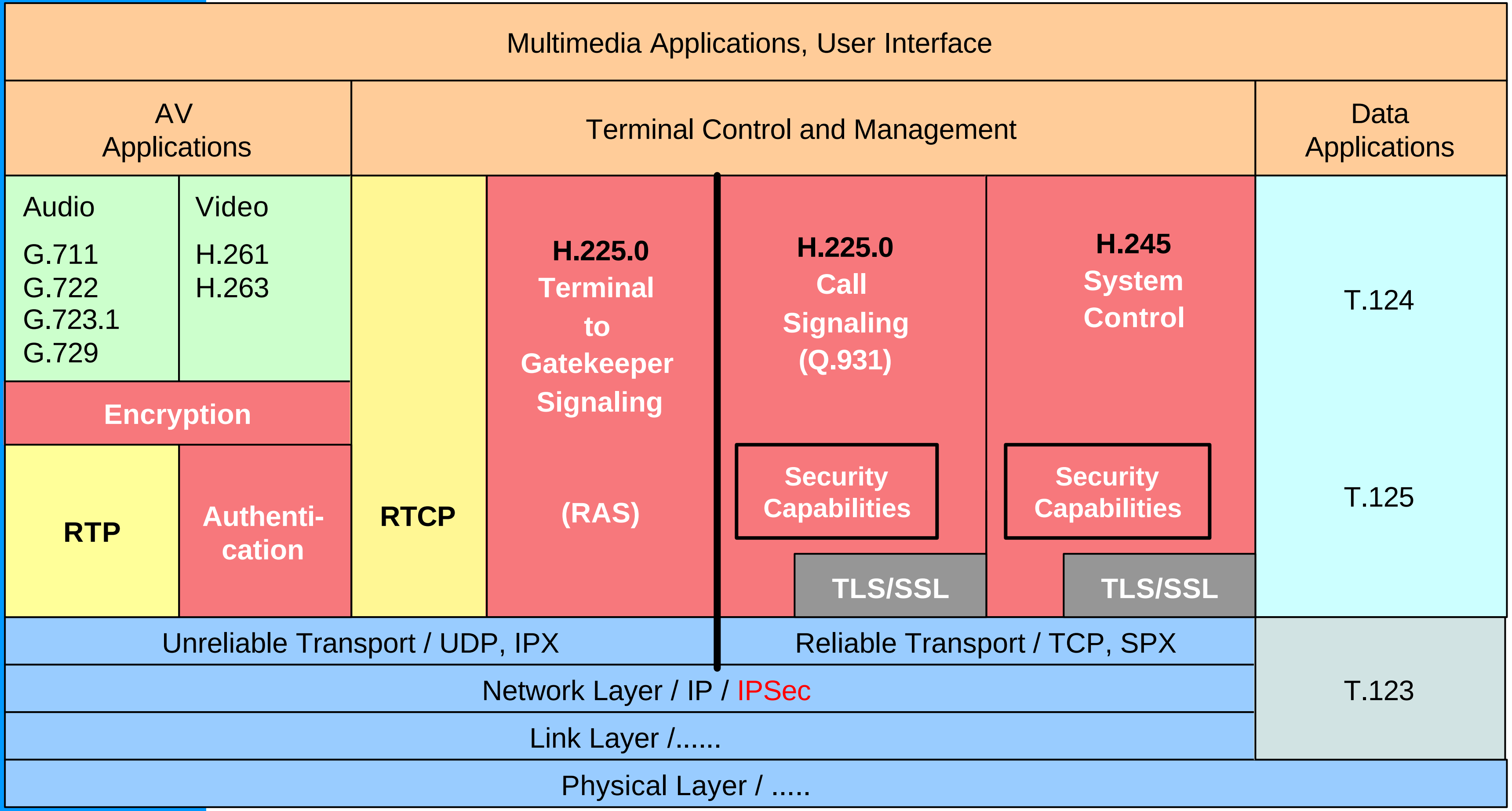
H.323 deployment scenarios



H.323 System

- The ***H.323 system*** *provides for packet-based multimedia conferencing services, including monomedia applications such as voice-over-IP. Besides H.323, the following Recommendations are part of the H.323 System:*
  - H.225.0 – Describes three signalling protocols (RAS, Call Signalling, and “Annex G”)
  - H.245 – Multimedia control protocol (common to H.310, H.323, and H.324)
  - H.235 – Security within H.245-based systems
  - H.246 – Interworking with the PSTN
  - H.350-series – MM Directory Services
  - H.360 – QoS MM Architecture
  - H.450.x – Supplementary services
  - H.460.x – Various H.323 protocol extensions
  - H.501 – Protocol for mobility management and inter/intra-domain communication
  - H.510 – User, terminal, and service mobility
  - H.530 – Security specification for H.510

Endpoint Security Provision for H.323



Multimedia Applications, User Interface

AV Applications

Terminal Control and Management

Data Applications

Audio

G.711
G.722
G.723.1
G.729

Video

H.261
H.263

Encryption

RTP

Authentication

RTCP

H.225.0
Terminal to Gatekeeper Signaling

(RAS)

H.225.0
Call Signaling
(Q.931)

Security Capabilities

TLS/SSL

H.245
System Control

Security Capabilities

TLS/SSL

T.124

T.125

Unreliable Transport / UDP, IPX

Reliable Transport / TCP, SPX

T.123

Network Layer / IP / IPSec

Link Layer /......

Physical Layer / .....

Scope of H.323 | **Scope of H.235** | **Transport Scope** | **Scope of T.120**

Secure Fax Transmission (ITU-T Rec. T.36)

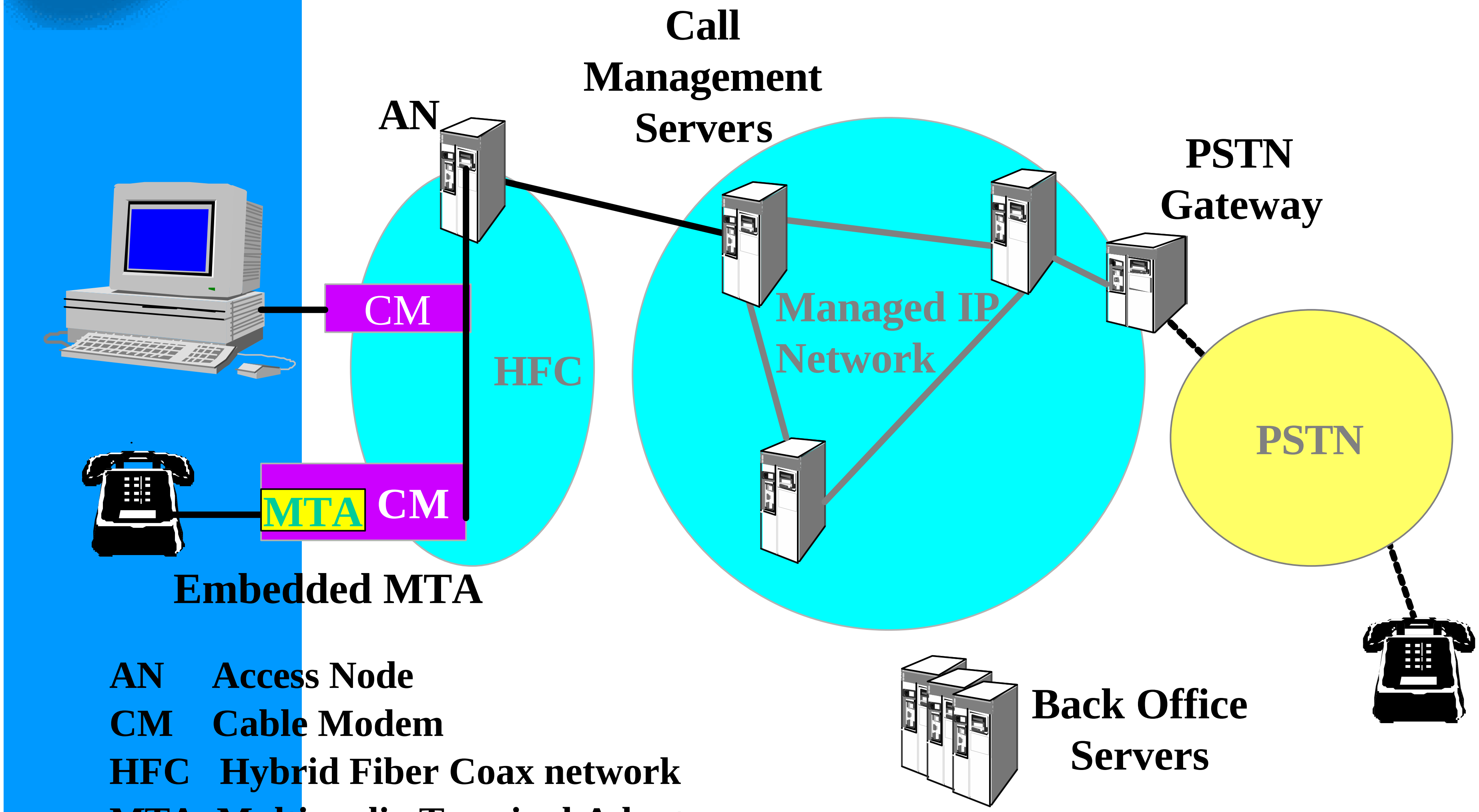
- Encryption of end-points using HKM/HFX40 or RSA
- Security services:
  - Mutual authentication (mandatory).
  - Security service (optional), which includes Mutual authentication, Message integrity, and Confirmation of message receipt.
  - Security service (optional), which includes Mutual authentication, Message confidentiality (encryption), and Session Key establishment.
  - Security service (optional), which includes Mutual authentication, Message integrity, Confirmation of message receipt, Message confidentiality (encryption), and Session Key establishment.

Highlights
SG 9

Security studies in ITU-T SG 9 (application specific)

- IPCablecom project
  - Interactive services over cable TV networks using IP protocol
  - J.170, IPCablecom security specification
  - Types of threat in IPCablecom:
    - Network attacks
    - Theft of service
    - Eavesdropping
    - Denial of Service
  - Security based on IPSec mechanisms

IPCablecom Components



AN	Access Node
CM	Cable Modem
HFC	Hybrid Fiber Coax network
MTA	Multimedia Terminal Adapter
PSTN	Public Switched Tel. Network

IPCablecom Recommendations

Architecture

- J.160 Architecture

Signalling

- J.162 Network Call Signalling (NCS)
- J.165 IPCablecom Signalling Transport Protocol
- J.171 Trunk Gateway Control Protocol

Quality of Service

- J.163 Dynamic QoS

Media/Codecs

- J.161 Audio Codec Reqs

OSS

- J.164 Event Messaging
- J.166 MIB Framework
- J.167 MTA Provisioning
- J.168 MTA MIB
- J.169 NCS MIB

Security

- J.170 Security

Security studies in other SGs

- SG 2
  - E.408 (ex-E.sec.1): *Telecommunication networks security requirements* >>
  - E.409 (ex-E.sec.2)*: Incident organization and security incident handling* >>
  - *Handbook on IP Policy* (under development) >>
- SG 13
  - Y.1271 (ex-Y.roec): *Framework to support emergency communications* >>
  - Will include a clause on Security in all Recommendations to be developed
- SGs 4, 11, 15, SSG
  - Incorporating security requirements in their Recommendations (see supplemental material)

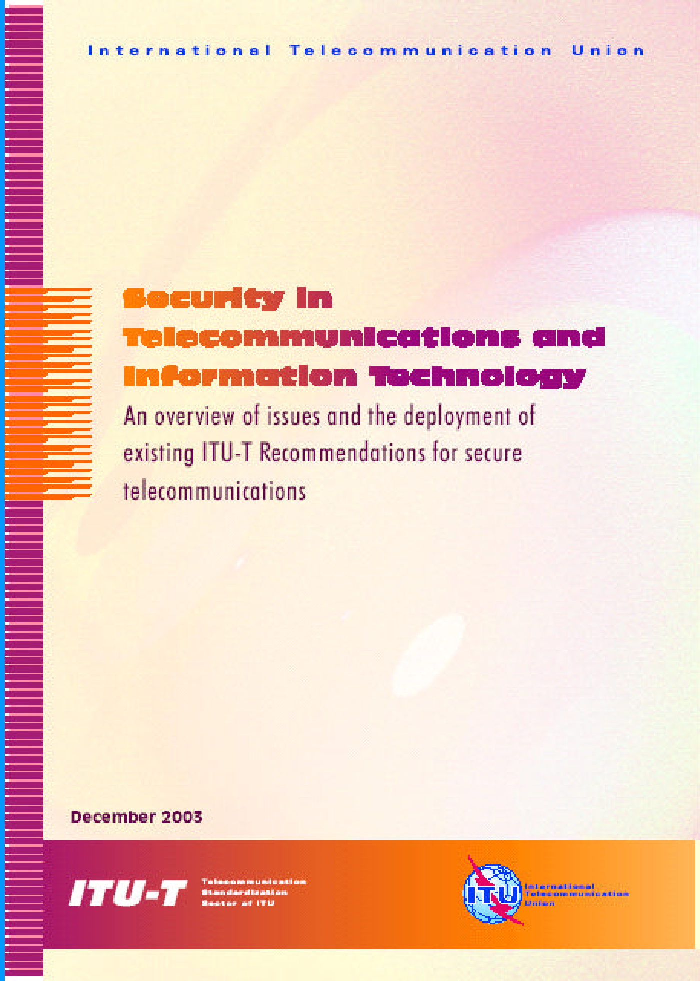
Security collaboration

- ISO/IEC JTC 1, Information Technology
  - SC 6, Telecommunications and Information Exchange Between Systems
  - SC 27, IT Security Techniques
  - SC 37, Biometrics
- IETF

Other ITU-T Resources

- Security Manual
- SG 17's Catalogue of ITU-T Security Recommendations
- SG 17's Compendium of Security Definitions
- Workshops

ITU-T Manual on Security in Telecommunications and Information Technology



International Telecommunication Union

Security in Telecommunications and Information Technology

An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications

December 2003

ITU-T Telecommunication Standardization Sector of ITU

International Telecommunication Union

- A.k.a. the “Security Manual”
- An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications
- Prepared by TSB with support from experts
- 1st edition: Dec.2003; 2nd: Oct.2004

“Security Manual” – Some Details

- Highlights and offers a bird’s eye view of how to use numerous ITU-T Recs to secure the communication infrastructure and associated services and applications
- Value added: how to use ITU-T Recs help to solve security issues – not a description of them
- Focuses on completed work, not upcoming/ ongoing work
- Free download: www.itu.int/ITU-T/edh/files/security-manual.pdf

Catalogue of ITU-T Security Recommendations

http://www.itu.int/ITU-T/studygroups/com17/ccsecurity.html

- Example: ITU-T Rec. X.509

  Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (03/00 – v4)

"This Recommendation defines a framework for public-key certificates and attribute certificates, and defines a framework for the provision of authentication services by Directory to its users. It describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed using cryptographic techniques.

Catalogue example: ITU-T Rec. X.509 (cont'd)

*While simple authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services. The frameworks defined may be used to profile application to Public Key Infrastructures (**PKI**) and Privilege Management Infrastructures (**PMI**). The framework for public-key certificates includes specification of data objects used to represent the certificates themselves as well as revocation notices for issued certificates that should no longer be trusted. While it defines some critical components of a **PKI**, it does not define a **PKI** in its entirety. However, it provides the foundation upon which full **PMIs** and their specifications would be built. Information objects for holding PKI and PMI objects in the Directory and for comparing presented values with stored values are also defined.*

Compendium of Security Definitions

http://www.itu.int/ITU-T/studygroups/com17/ccsecurity.html

- **Example: Definitions of public-key**
  - 3.3.43/X.509
    - (In a ***public key*** cryptosystem) that key of a user's key pair which is publicly known.
  - 3.3.11/X.810
    - A key that is used with an ***asymmetric*** cryptographic algorithm and that can be made publicly available.
  - 3(26)/J.170
    - The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.

Security Workshops (Past and Future)

- ITU-T Workshop on Security
  Seoul, Korea, *13-14 May 2002*
  http://www.itu.int/ITU-T/worksem/security/index.html

- ITU workshop - Creating trust in critical network Infrastructures
  Seoul, Korea, *20-22 May 2002*
  http://www.itu.int/osg/spu/ni/security/

- Cybersecurity Symposium
  Florianópolis, Brazil, *4 October 2004*

Conclusions

Conclusions

- ITU-T has actively dealt with security issues *long before* IP & the Internet
- ITU-T has significant work in the General Guidance/ Framework area as well as for specific system security (H.323, IPCablecom, etc)
- Security issues are considered in relevant ITU-T Study Groups to minimize security vulnerabilities of the *design* and *threat-model* categories
- High-level Guidelines (WTSA, WSIS) reinforce the importance of ITU-T Security work for acceptance of ICTs and bridging the “Digital Divide”
- In addition to Recommendations, several ITU-T resources are available: Workshops, Manual, Glossary and Compendium

Thank You!

Simão Ferraz de Campos Neto joined the ITU-TSB in 2002 and is the Counsellor for ITU-T Study Group 16, where standardization work takes place on multimedia services, protocols, systems, terminals and media coding. He was the Coordinator in TSB of the 2003 ITU-T Informal Forum Summit, and has also organized several workshops (IP and Multimedia in Satellites, Telecommunications for Disaster Relief and recently on Standardization in E-health).

Prior to joining ITU in 2002, Mr Campos worked as a scientist in COMSAT Laboratories performing standards representation and quality assessment for digital voice coding systems. Mr Campos authored several academic papers and portion papers, as well as serving in the review committee of several IEEE-sponsored conferences. He was the editor of the TSB Security Manual.

Mr Campos is a Senior Member of the IEEE and received an MSc from the State University of Campinas, Brazil, on Telecommunications in 1993 and a BSc in Electronic Engineering from the same university in 1986.

Supplemental Material

- ITU-T Recommendation X.509
- Study Group 16 efforts on security
- Study Groups 4, 11, 15 & SSG
- ITU-T Activities on TDR

ITU-T Security Building Blocks

Security Architecture Framework

X.800–Security architecture
X.802–Lower layers security model
X.803–Upper layers security model
X.805–Security architecture for systems providing end-to-end communications
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–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 services
X.843–Specification of TTP services to support the application of digital signatures

Directory Services and Authentication

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 telecommunications 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

Facsimile

T.30 Annex G–Procedures for secure Group 3 document facsimile transmission using the HKM and HFX system
T.30 Annex H–Security in facsimile Group 3 based on the RSA algorithm
T.36–Security capabilities for use with Group 3 facsimile terminals
T.503–Document application profile for the interchange of Group 4 facsimile documents
T.563–Terminal characteristics for Group 4 facsimile apparatus

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 (H.323 and other H.245-based) multimedia terminals
H.323 Annex J–Packet-based multimedia communications systems – Security for H.323 Annex F (Security for simple endpoint types)
H.350.2–Directory services architecture for H.235
H.530–Symmetric security procedures for H.323 mobility in H.510

X.509

- 1st edition in 1988; 5th in preparation
- Written to satisfy multiple needs
- Extensibility allows organizations to enhance as needed
- Good cooperation between ITU, ISO, and IETF
- In products such as securing browser traffic and signing executable code
- Laws enabling electronic/digital signature

X.509 Specifies

- Public-key certificate
  - binds name of entity to a public key
  - if certificate issuer trusted then the entity can be authenticated by the use of the associated private key
- Attribute certificate
  - asserts an entity’s privileges, i.e. its right, to access information or services
  - replaces the need for managing rights in the asset holding system

X.509 *is* widely used…

- Public-key certificates are widely deployed
  - prevents the classic *man-in-the-middle* attack
  - used in Secure Sockets Layer (SSL) to secure browser traffic
  - protect email content and authenticates source
  - replacing notarized signatures in some areas
- Initial products did not need to be pure
  - e.g. early, and some current, browsers do not check certificate revocation status
- Some attribute certificate implementations are being studied

X.805 is a Multi Part Standard

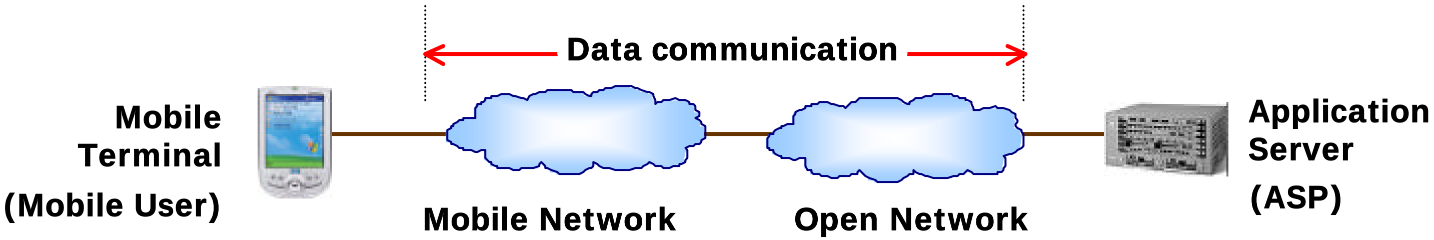
- Joint Project with ISO/IEC JTC 1/SC 27, “Information technology – Security techniques – IT network security”
  - Part 1: Network security management
  - Part 2: Network security architecture (X.805)
  - Part 3: Securing communications between networks using security gateways
  - Part 4: Remote access
  - Part 5: Securing communications across networks using virtual private networks

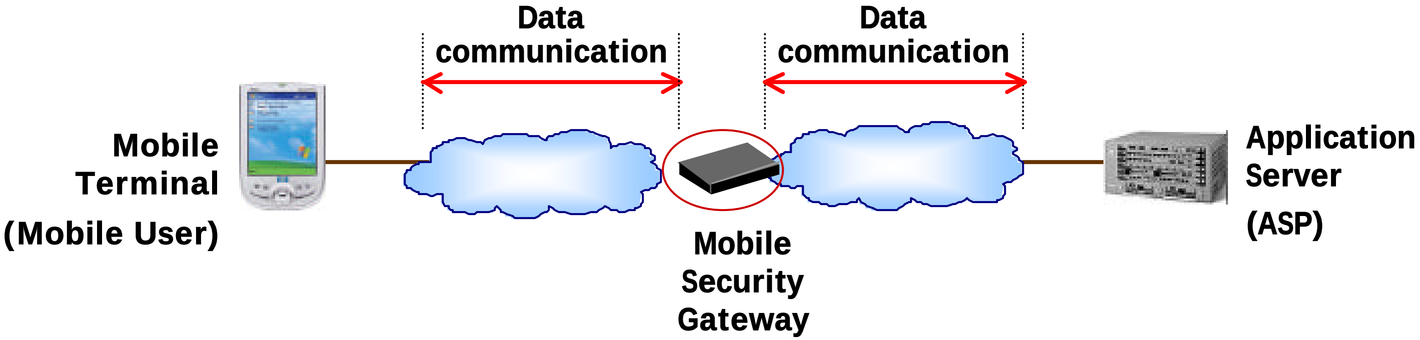
General Communication Framework

Gateway Framework

X.1121

Security framework for mobile end-to-end data communications

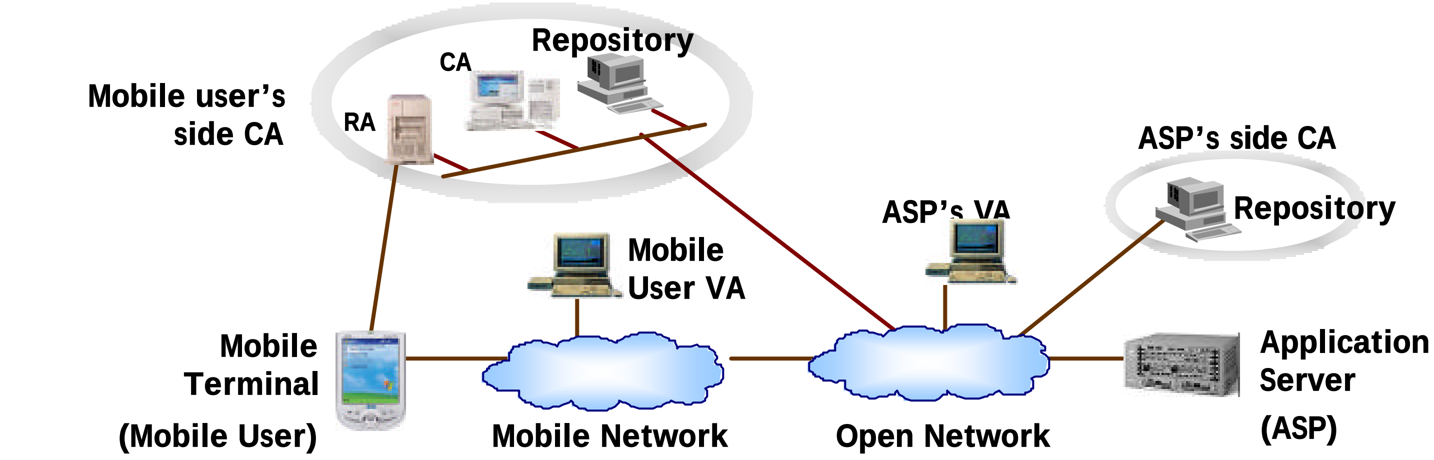




- Security threats
- Relationship of security threats and models
- Security requirements
- Relationship of security requirements and threats
- Security functions for satisfying requirements

Secure mobile systems based on PKI

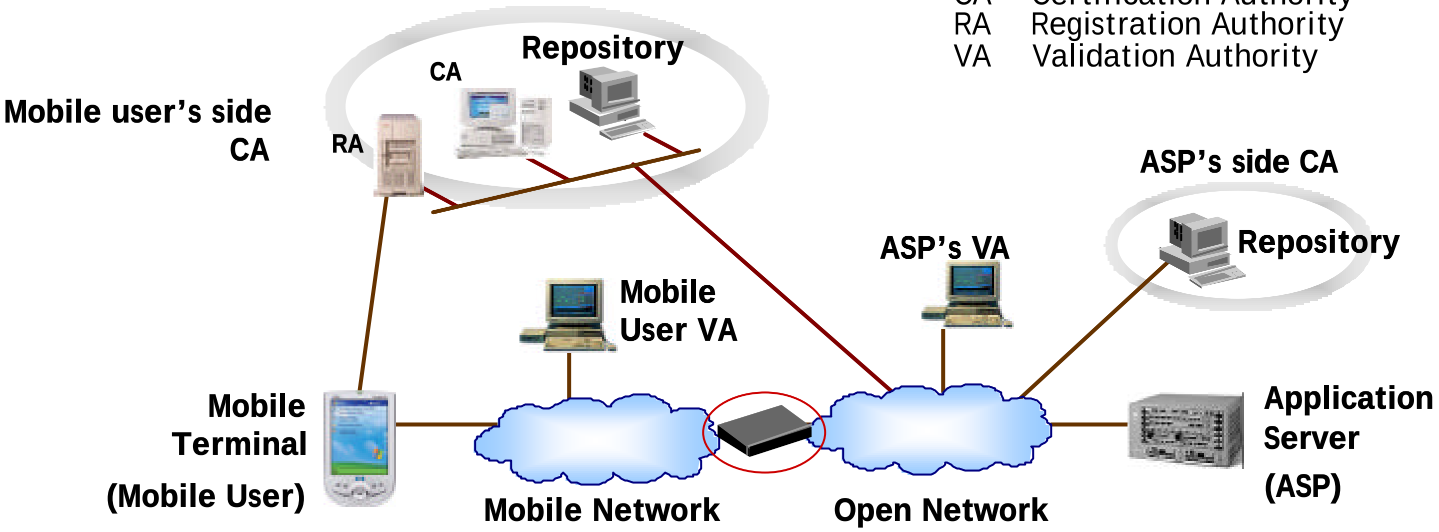
General Model



ASP Application Service Provider
CA Certification Authority
RA Registration Authority
VA Validation Authority

Gateway Model

X.1122



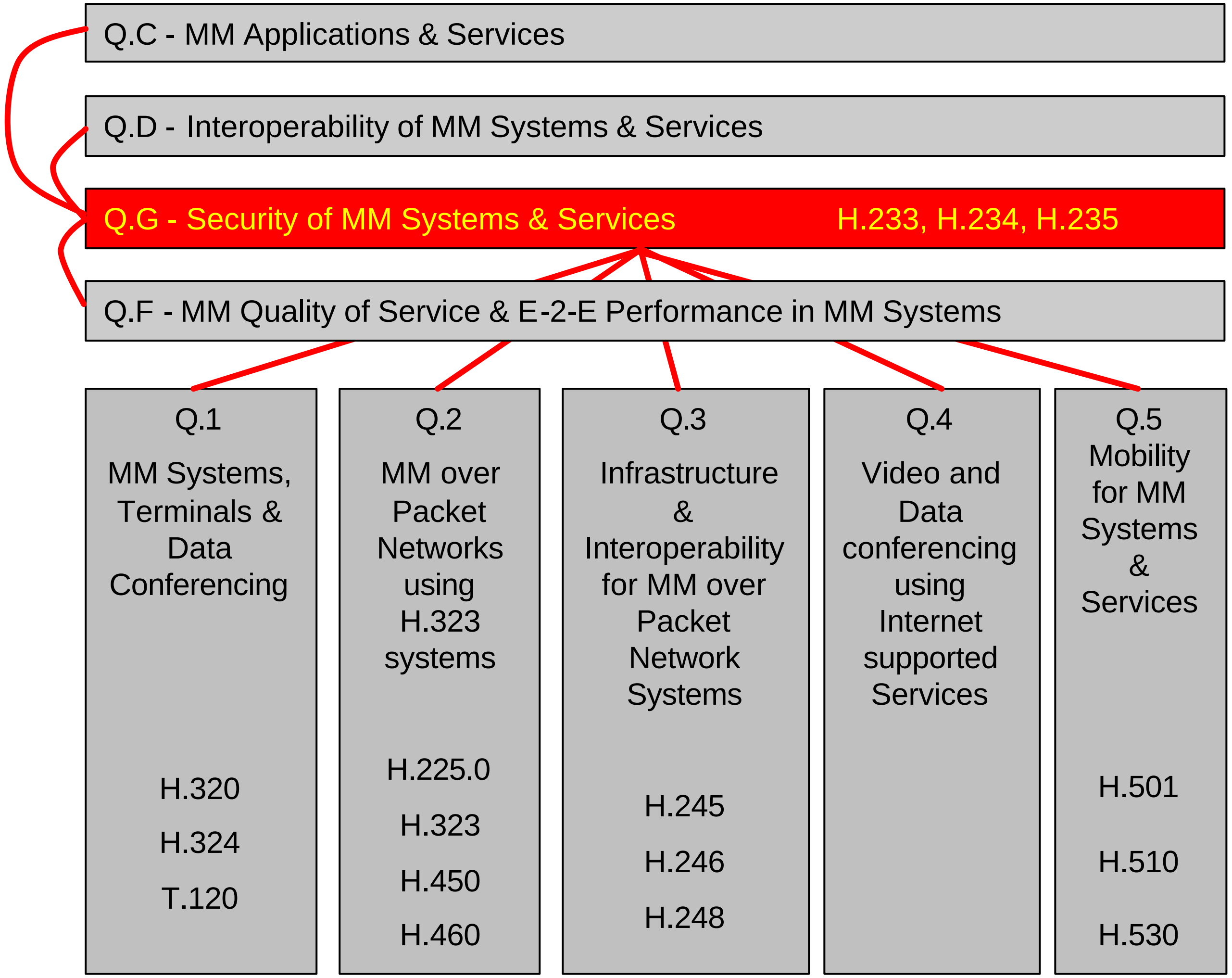
Q.G/16 Security of Multimedia Systems and Services

- Horizontal Question that deals with security issues applicable to Multimedia Systems, Services, and Terminals
  - PSTN terminals: H.324
  - B-ISDN terminals: H.310 (videoconferencing)
  - N-ISDN terminals: H.320 (videoconferencing)
  - IP-based terminals: H.323 family (including conferencing & VoIP)
  - Gateways: inter-MM terminals (H.246) and IP-PSTN (H.248.x/Megaco series)
  - Data conferencing

For more details: see Annex G of the MediaCom2004 project

http://www.itu.int/ITU-T/studygroups/com16/mediacom2004

Security in the MediaCom Project



Q.C - MM Applications & Services

Q.D - Interoperability of MM Systems & Services

Q.G - Security of MM Systems & Services H.233, H.234, H.235

Q.F - MM Quality of Service & E-2-E Performance in MM Systems

Q.1 MM Systems, Terminals & Data Conferencing

H.320

H.324

T.120

Q.2 MM over Packet Networks using H.323 systems

H.225.0

H.323

H.450

H.460

Q.3 Infrastructure & Interoperability for MM over Packet Network Systems

H.245

H.246

H.248

Q.4 Video and Data conferencing using Internet supported Services

Q.5 Mobility for MM Systems & Services

H.501

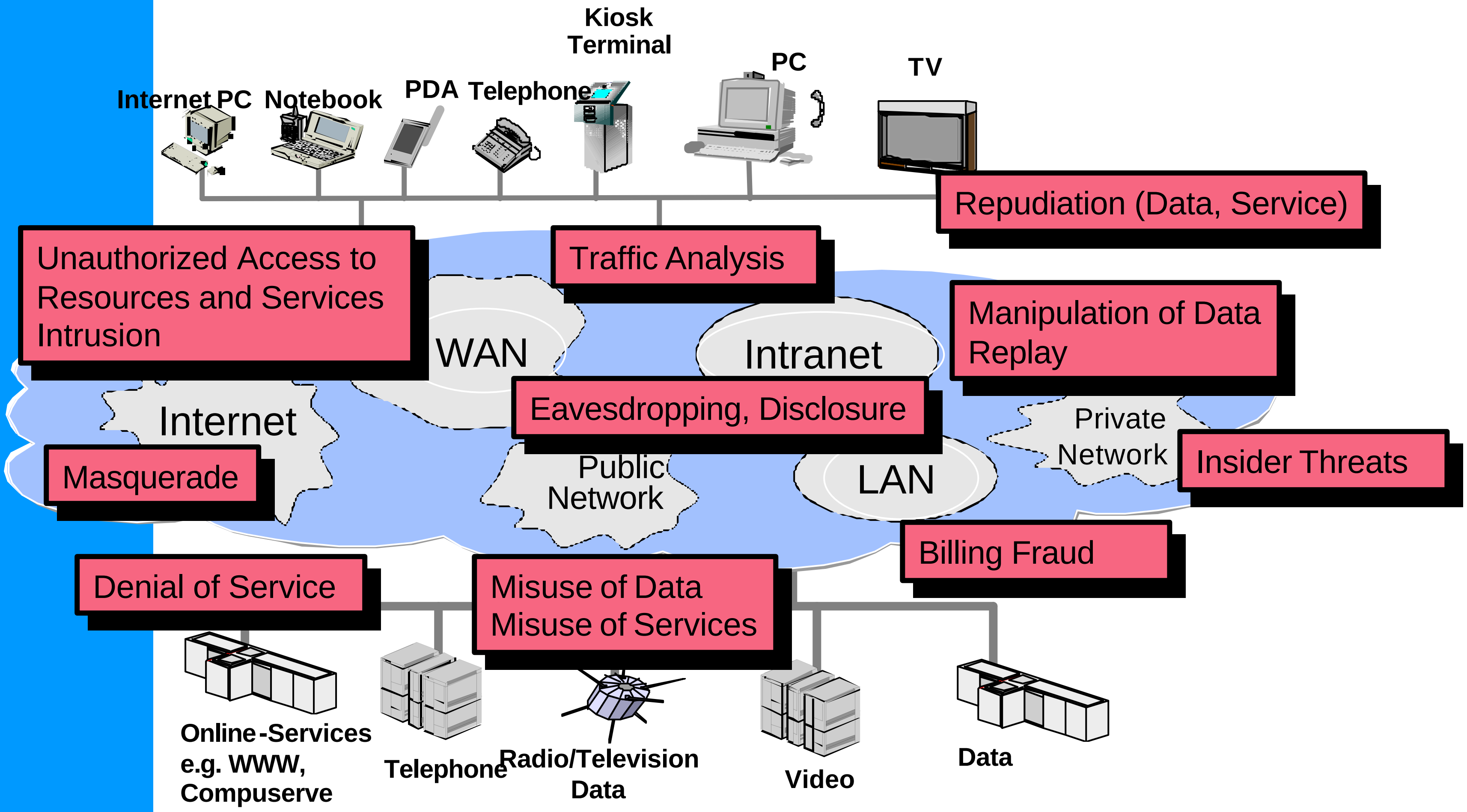
H.510

H.530

Target Multimedia Applications with Security Needs

- Voice/Video Conferencing
- Data Conferencing
- IP Telephony (Voice over IP)
- Media Gateway Decomposition (H.248.x/Megaco)
- MM Mobility
- Instant Messaging and MM-Presence

Risks in Multimedia Communication



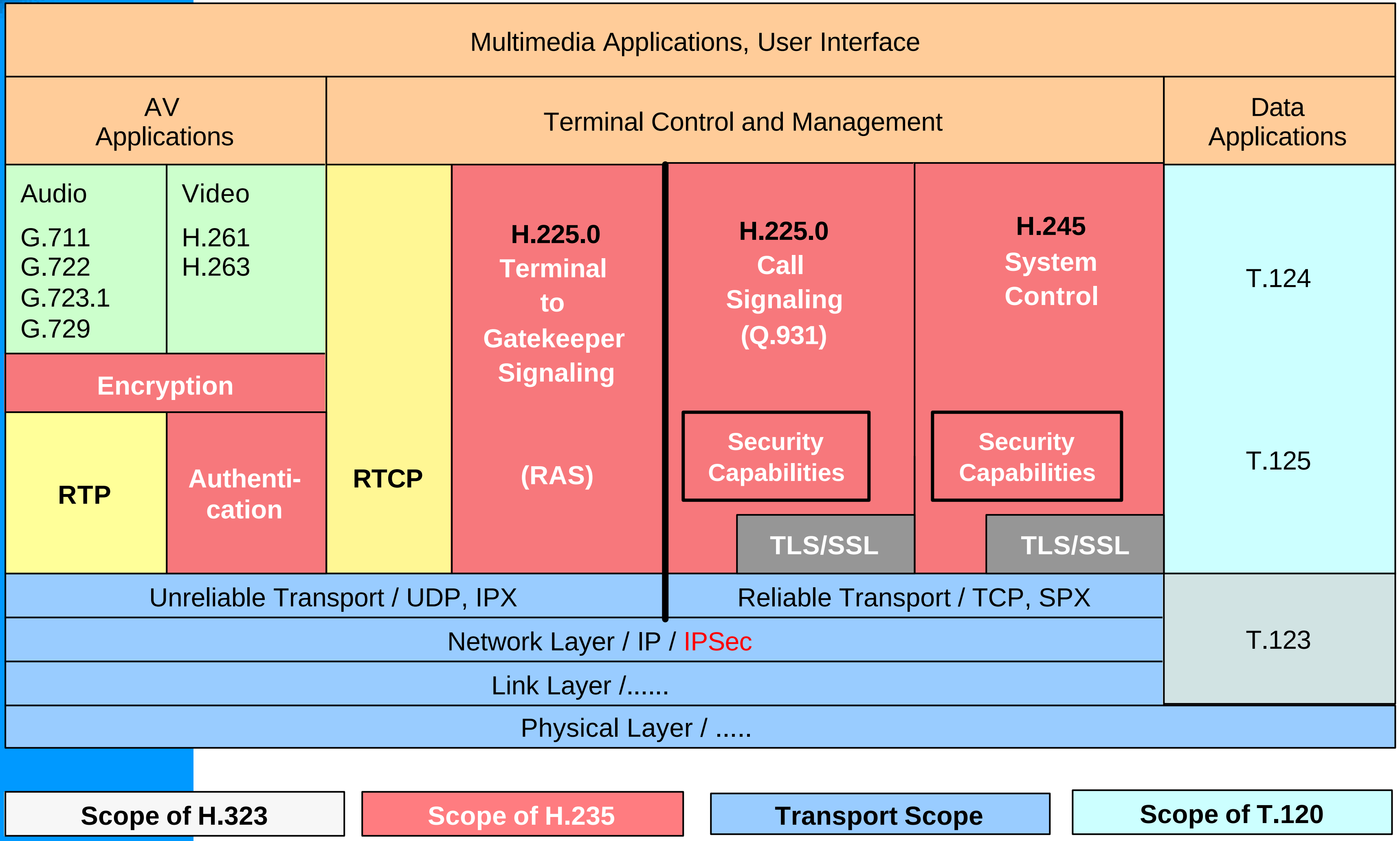
Specific IP Telephony Security Challenges

- IP Telephony is real-time, point-2-point or multi-point
  - secure fast setup/connect
  - real-time security processing of media data
  - real-time certificate processing
  - IKE security handshakes take too long
- Security measures must be integrated in proprietary platforms and in VoIP stacks
  - security can best be added at application layer
  - tight interaction with voice CODECs and DSPs
  - low overhead for security: small code size, high performance, etc
  - “Windows 5000” is not the answer!
- Secure management of the systems
  - secure password update
  - secure storage in databases
- Scalable security from small enterprise to large Telco environments
- Security should be firewall friendly

H.235: Security for Packet-Switched MM

- Builds upon ITU-T Rec. X.509
- Features:
  - Cryptographic protection of control protocols & media
  - Negotiation of cryptographic services, algorithms and capabilities
  - Integrated key management functions / secure point-to-point and multipoint communications
  - Interoperable security profiles
  - Sophisticated security techniques (Elliptic curves, anti-spamming & AES)
  - May use existing Internet security packages and standards (IPSec, SSL/TLS)

H.235 – “H.323 Security”
Security Protocol Architecture



Multimedia Applications, User Interface

AV Applications

Terminal Control and Management

Data Applications

Audio

G.711
G.722
G.723.1
G.729

Video

H.261
H.263

Encryption

RTP

Authentication

RTCP

H.225.0
Terminal to Gatekeeper Signaling
(RAS)

H.225.0
Call Signaling (Q.931)

Security Capabilities

TLS/SSL

H.245
System Control

Security Capabilities

TLS/SSL

T.124

T.125

Unreliable Transport / UDP, IPX

Reliable Transport / TCP, SPX

Network Layer / IP / IPSec

Link Layer /......

T.123

Physical Layer / .....

Scope of H.323

Scope of H.235

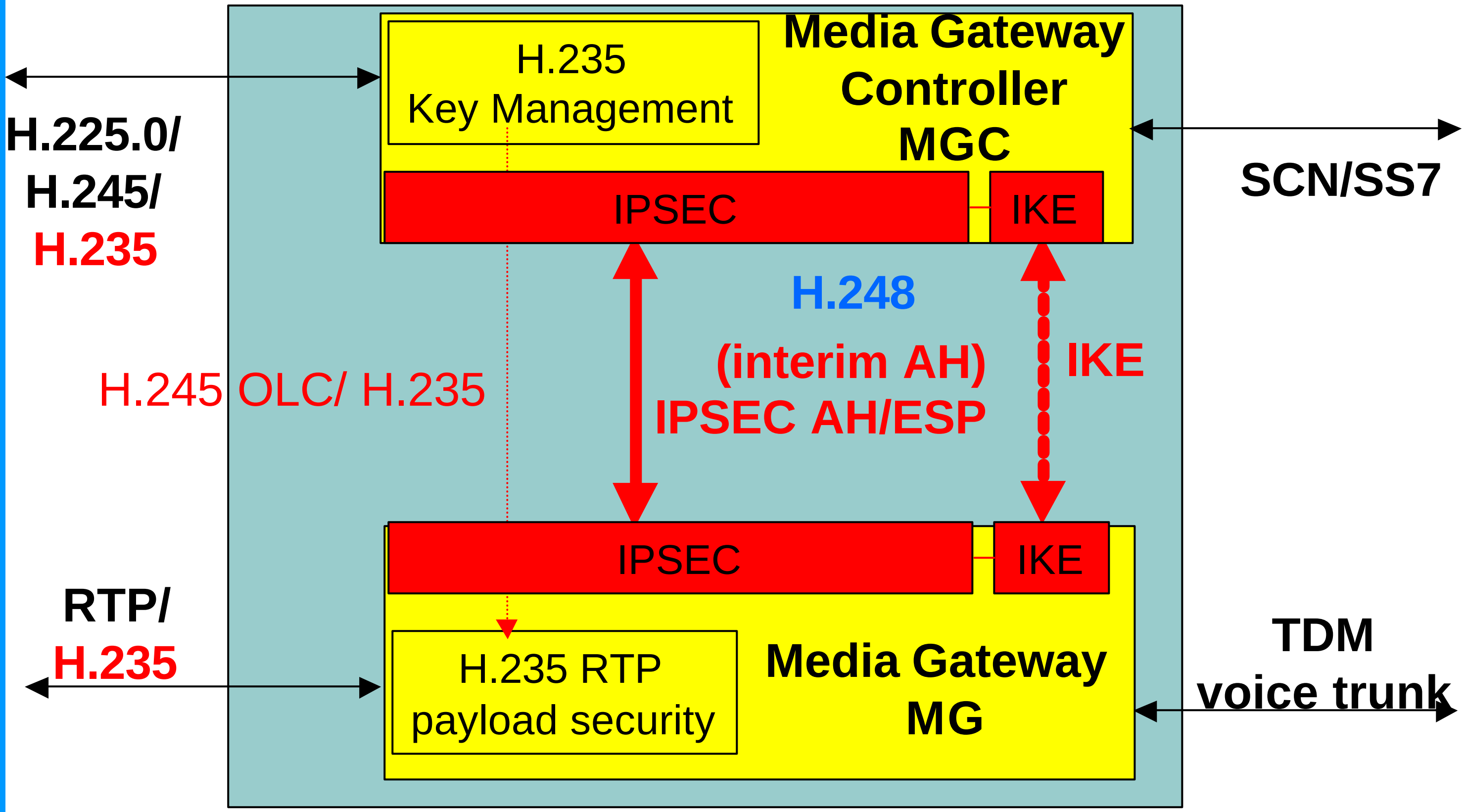
Transport Scope

Scope of T.120

H.530
The Security Problem of H.323 Mobility

- Provide secure user and terminal mobility in distributed H.323 environments beyond interdomain interconnection and limited gatekeeper zone mobility
- Security issues
  - Mobile Terminal/User authentication and authorization in foreign visited domains
  - Authentication of visited domain
  - Secure key management
  - Protection of signaling data between MT and visited domain

H.248.1 Security in decomposed Gateways



Security for Multimedia Terminals on circuit-switched networks

- H.233: “Confidentiality System for Audiovisual Services”
  - point-to-point encryption of H.320 A/V payload data by ISO 9979 registered algorithms: FEAL, DES, IDEA, B-CRYPT or BARAS stream ciphers
- H.234: “Key Management and Authentication System for Audiovisual Services”
  - uses ISO 8732 manual key management
  - uses extended Diffie-Hellman key distribution protocol
  - RSA based user authentication with X.509-like certificates by 3-way X.509 protocol variant

Security for Multimedia Conferencing – T.120 and Security –

- T.120 has very weak information security available (unprotected passwords), common state of the art cryptographic mechanisms are not supported
- OS security features do not prevent against typical T.120 threats (especially T.128 application sharing vulnerabilities);This problem already arises in simple pt-2-pt scenarios
- Additional threats exist for group-based multipoint scenarios: insider threats, lack of access control, “write token” not protected, unsecured conference management ,…
  - The T.120 “**virtual conference room**” needs integral and user friendly security protection: for authentication & role-based authorization, for confidentiality, for integrity, and security policy negotiation capabilities

Security for MM Applications and Systems in Emergency & Disaster Relief

- Security objectives:
  - prevent theft of service and denial of service by unauthorized user
  - support access control and authorization of ETS users
  - ensure the confidentiality and integrity of calls
  - provide rapid and user-friendly authentication of ETS users
- Relationship identified with QoS, network issues, robustness and reliability,…

Study Groups 4, 11, 15 and SSG (1)

- SG 4 has developed a set of security-related Recommendations, e.g.
  - M.3210 on TMN management services for IMT-2000 security
  - Q.815 on security model for message protection
  - Q.817 on TMN-PKI, Digital certificates and certificate revocation lists profiles
  - Work on security is carried out in Q.7, 9, 10 & 18/4

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

- SG 11 develops network signaling & control protocols incorporating appropriate security requirements
  - Work on security is carried out in Q.1-6 & 11/11

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

Study Groups 4, 11, 15 and SSG (2)

- SG 15 contributes to security work in the areas of reliability and communication security
  - Q.9/15 works on SDH protection switching & OTN protection switching. Network restoration requirements will be also considered.
  - Q.15-18/15 contain a study item on reliability.
  - Work on communication security is carried out in Q.14/15. Refer to G.784 on SDH management & G.875 on OTN management, addressing security management functions. G.7712 includes security for management & signaling communication networks.

  (see http://www.itu.int/ITU-T/studygroups/com15/index.asp)
- For SSG, security is a key aspect. Are studied threats, how to address threats, security architecture, cryptography, lawful interception,… Refer to Q.3/SSG.

  (see http://www.itu.int/ITU-T/studygroups/ssg/index.asp)

ITU-T Studies on Telecommunications for Disaster Relief (TDR)

TDR scope (1)

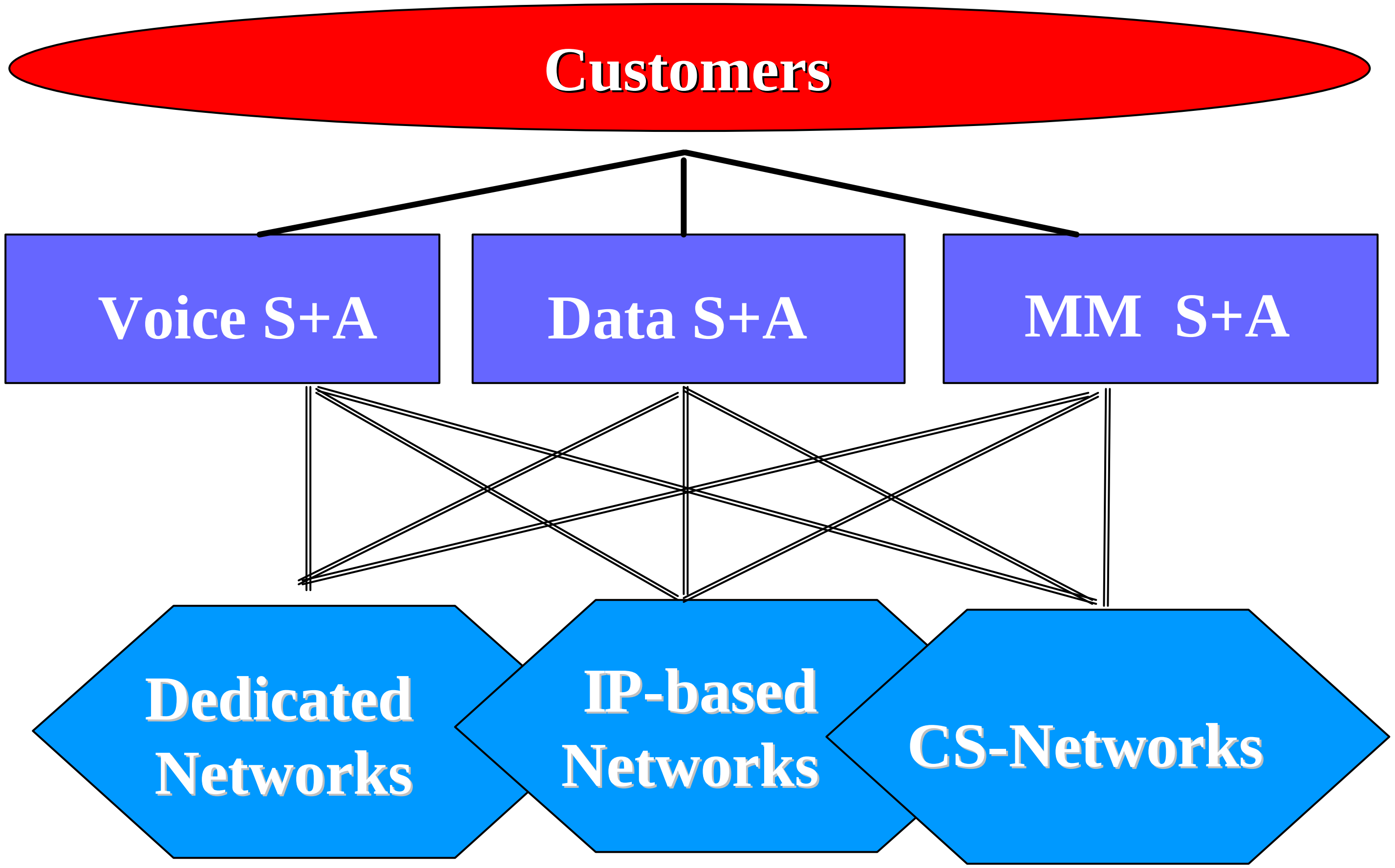
- During natural and manmade disasters, rapid organization and co-ordination of recovery operations is essential to save lives and restore the community infrastructure
- Recovery operations depend upon ready availability and access to telecommunication resources to support urgent communications
- Telecommunication networks often experience severe stress due to damaged infrastructure and very high traffic loads

TDR scope (2)

- There is a need to provide specific resources for authorized users (e.g. governments, fire brigades, police, medical services, etc…)
- The development and standardization of TDR capabilities provides the means for disaster recovery activities to effectively communicate
- Specific standardization activities are therefore required to efficiently support TDR requirements
- ITU-T can take advantage of its unique industry-government environment to produce relevant Recommendations

Telecommunication networks: normal operating conditions

S+A
Service
Applications



Customers

Voice S+A

Data S+A

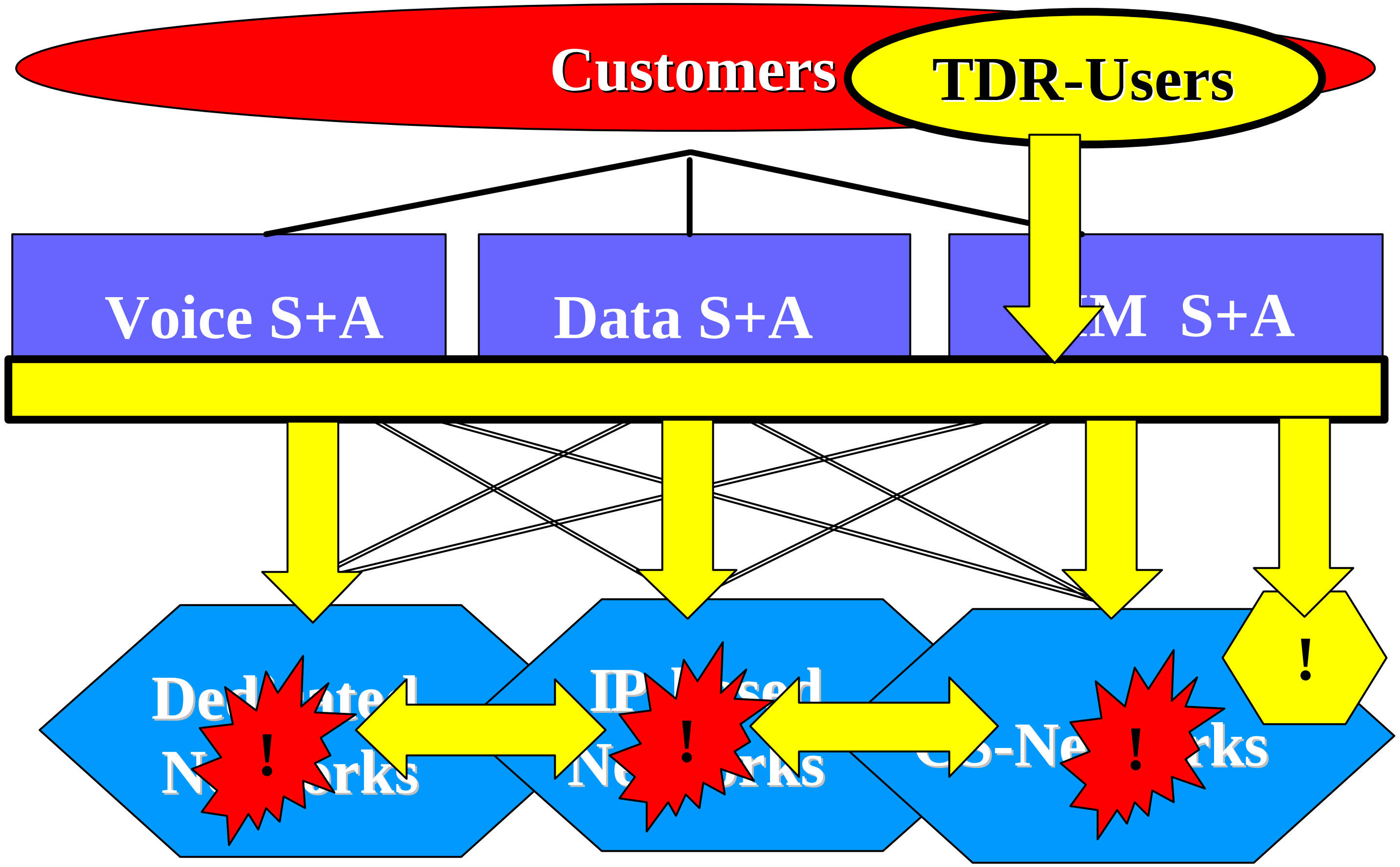
MM S+A

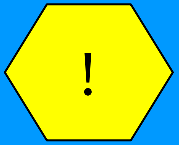
Dedicated Networks

IP-based Networks

CS-Networks

Telecommunication networks: operations in crisis situation





Dedicated
network

TDR scope (3)

- TDR is not the same thing as ETS!
- TDR addresses the need of authorized users in terms of facilities established on public network infrastructure, including the inter-working aspects with dedicated/private networks
- TDR work does not specifically address systems for the use of the public in general (Emergency numbers 112/911, broadcasting network to forward emergency relevant information to the public,...)
- Since ETS is more generic, TDR is the preferred term in order to avoid the confusion with the systems described above

Key issues for TDR standardization

- ***Customers:***
  - segmentation
  - requirements
- ***Services and applications (incl. QoS)***
  - use of existing facilities
  - extension (new needs?)
- ***Network capabilities for TDR support***
- ***Inter-working at***
  - Service and application level
  - Network level
- ***Regulatory framework***

TDR trends

- **Situation in the past:**
  -TDR are/were based on PSTN, ISDN, PLMN, 2G-mobile
  - Circuit switched technology
  - Voice centric applications
  - National solutions
  - Limited inter-working
- **Present trends:**
  - Use the possibility of multimedia (video)
  - New applications/services based on mobility, location-based information,…
  - Evolution to IP-based platforms
  - Needs for global solutions (international)
  - Improve inter-working between platforms (public/private)

The role of standards for TDR

- Interworking, compatibility, evolution, economy of scale, … are the main drivers for the development of a

  Family of standards to ensure global interoperability of emergency communications…

- - maintaining foundation of existing national capabilities
- - enabling new national capabilities to be established
- - expanding communications internationally on priority basis
- - mapping ETS indicators code at national gateways
- - facilitating orderly evolution to advancing technologies and enhanced capabilities

First steps towards TDR standardization in ITU-T

- Contributions submitted to several Study Groups to develop Recs. on ETS/TDR (2001)
- Development of first Recs. (E.106, draft Rec. F.706)
- Need for improved coordination and liaison with other SDOs recognized
- Experiences made during the events in 2001/2002
- Projects on Security (SG 17) and NGN (SG 13)
- Needs expressed by the ITU-T membership, to develop a global and harmonized set of standards for ETS/TDR capabilities in close co-operation with other SDOs
- Questionnaire on the use of public telecom services for emergency and disaster relief operations (TSB-Circular 132/15-11-2002)
- Organized a Workshop on Telecommunications for Disaster Relief (Geneva, 17-19 February 2003)
- Set-up of the TDR Partnership Coordination Panel (TSB-Circular 173, July 2003)

Development of TDR technical standards in close cooperation with ITU-R, ITU-D and other SDOs

- ITU-R: RF spectrum related aspects, Inter-working with BC- and satellites networks
- ITU-D: Requirements of developing countries
- ETSI (EMTEL,...)
- ISO/IEC
- IETF (WG iprep,..)
- T1/TIA
- 3GPP, 3GPP2,...
- ....

Conclusions: Key factors for success and challenges

- Understand users requirements
- Identify the regulatory framework
- Develop a set of global and compatible Standards
- Cost aspects
- Evolutionary approach
- National sovereignty
- Partnership between Member States, private sector, GOs and NGOs

See also http://www.itu.int/ITU-T/worksem/ets/index.html