An ITU-T Vision on SPAM

Telecommunication Standardization Bureau

Richard Hill

Counsellor, ITU-T Study Group 2

ITU WSIS Thematic Meeting on Countering SPAM
Geneva, 7-9 July 2004

Overview

o Information about ITU

o High-level directives

o Understanding the problem

o Towards a standards-based solution

o Some existing ITU-T foundational standards

o Some additional ITU Resources

o Conclusion

About ITU...

What is ITU?

o International treaty organization founded in 1865 to facilitate international interconnection of telegraphy

o Unique partnership of industry and governments

o Three sectors:

- Development (aid to developing countries)
- Radio (radio spectrum and satellite slot allocations)
- Standardization (formerly CCITT, for example modem standards) (now called ITU-T; secretariat is called TSB)

o In ITU-T industry and government work together to develop mutually agreed non-binding Recommendations

ITU-T membership

o *Member States:*   **189**

o *Sector Members:*   **162**   *ROAs*
                        171   *SIOs*
                        47   *others (including ISOC, regional, International organizations, etc.)*

o *Associates*   **84**

o *New applicants:*   *2003:* **55**
                        2002: **47**
                        2001: **75**
                        2000: **66**

Most active ITU-T sector members

ROAs

- France Telecom
- Telekom. Polska
- China Telecom. Corp.
- BT
- Deutche Telekom
- KDDI
- Bharat Sanchar Nigam
- Telenor ASA
- AT&T
- NTT DoCoMo
- Telecom Italia
- TeliaSonera
- Belgacom

SIOs

- NTT
- Cisco
- Nortel
- ETRI
- Huawei
- Siemens
- L. M. Ericsson
- ZTE
- Alcatel
- Infineon
- Lucent
- NEC
- Fujitsu

What is ITU's Situation (1/3)
ITU-T Approval and publication times

	before 1988	1989-1993	1993-1996	1997-2000	2001-2004
Approval time	4 years	2 years	18 months	9 months (exceptional case: 5 months)	2-9 months
Publication time	2-4 years	2 years	1-1.5 year	6-12 months	3-9 months

Notes:

1. Pre-published Recommendations, available on ITU-T Website, from a few days to four weeks after approval of the text.

2. Recs in force, pre-published, superseded/obsolete: available on ITU-T Website.

3. Forms of publication: paper, CD-ROM, electronic bookshop, online, etc.

4. FREE ONLINE ACCESS SINCE JANUARY 2001 (one free access per member, 3 free downloads for public)

5. "Approval time" counted between "determination/consent" and final approval

What is ITU's Situation (2/3)

o ITU-T is a dynamic, well-respected industry-government partnership (650 Sector Members)

o Examples of ITU-T Recommendations:

- G.723.1 & G.729 - Speech coding for Voice over IP and other applications
- H.323 - Packet based multimedia communication systems - the protocols behind Voice over IP, along with:
  - H.245 - Control protocol for multimedia communications
  - H.248 - Gateway control protocol (developed jointly with IETF)
- X.509 – Public Key Infrastructure (encryption)
- V.90 - 56kbit/s PSTN modems - providing ubiquitous worldwide Internet access
- G.99x series - xDSL Recommendations for broadband access

What is ITU's Situation (3/3) ITU-T – Electronic Publishing

- o All Recommendations available online

- o Key databases (for example, telephone country codes) available online

- o Working documents available online

See http://www.itu.int/ITU-T/

ITU-T positioning

Task Force

IETF

Intergovernment

ITU-T

NGOs
ISO,IEC,
IEEE, ETSI, ECMA
TTC, Committee T1,
ARIB, TIA, SCTE

Forums & Consortia

1394TA	3GPP	3GPP2	AIM	AMF	AMI-C
AOEMA	AOW	ATMF	BINTERMS	Bluetooth	Cable Modems
CBOP	CDG	CIF	CII	CommerceNet	CommerceNet J
COS	CTFJ	DHF	DISA	DOPG	DSLF
ECE	ECHONET	ECOM	ECTF	EDIFICE	EEMA
EIDX	EMA	EMF	ERTICO	EWOS	FCIA
FCIA-J	FIPA	FRF	FSAN	GSM Assoc.	HNF
Home API	HomePNA	HRFWG	IDB Forum	IFIP	IFSA
IMTC	IMWA	IrDA	ITS America	ITS UK	JAVA
JCTEA	JECALS	JEDIC	JEMA	JICSAP	JIMM
JMF	LONMARK	MCPC	MDG.org	MITF	MMCF
Mobile Web	MOPA	MPLSF	MSForum	MWIF	OASIS
ODVA	OIF	OMG	OSGi	PCCA	PCISIG
PCMCIA	PHS MoU	PICMG	POF	Salutation	SCF
SDR	SSIPG	STA	TINA-C	TMForum	TOG
TSC	UMTS	USBIF	UWCC	W3C	WAP
WDF	Web 3D	WfMC	WIN Forum	WLIF	XTP Forum

Cooperation

o A.4 – Communication with forums/consortia

o A.5 – Organizations qualified for referencing

o A.6 – Communication with SDOs

o MoUs

- MoU between IEC, ISO, ITU and UN/ECE Concerning Standardization in the Field of Electronic Business, 24 March 2000

- MoU between ITU and ETSI, 14 June 2000

Members for Rec. A.4, A.5 and A.6 Forums/SDOs

A.4	A.5	A.6
ASN.1 Consortium	ARIB (Association of Radio Industries and Businesses)	ARIB
ATM Forum	ATM Forum	Committee T1
DSL Forum	Committee T1	CCSA
ETIS (e-and telecommunication info. services)	CCSA	ECMA
FRF (Frame Relay Forum)	DSL Forum	ETSI
IMTC (Multimedia)	ECMA Standardizing Information & Communication Systems	IEEE
IPDR Organization	ETSI (European Telecommunications Standards Institute)	JCTEA
IPv6 Forum	FRF	NIST
MPLS (Multi Protocol Label Switching) Forum	IEEE (Institute of Electrical and Electronics Engineers)	SCTE
MSF (Multiservice Switching Forum)	ISOC/IETF (Internet Society/Internet Engineering Task Force)	TIA
OASIS	JCTEA (Japan Cable Television Engineering Association)	TTA
OIF (Optical Internetworking Forum)	MPLS Forum	TTC
OMG (Object Management Group)	NIST (National Institute of Standards and Technology)	
SDL Forum Society	OASIS	
TM Forum (Tele Management Forum)	OIF	
W3C (World Wide Web Consortium)	OMG	
	SCTE (Society of Cable Telecommunications Engineers)	
	TIA (Telecommunications Industry Association)	
	TM Forum	
	TTA (Telecommunications Technology Association)	
	TTC (Telecommunication Technology Committee)	

How does ITU-T Develop Recommendations?

o Consensus of Sector Members and Member States

o Work typically driven by Sector Members

o Open (for members), transparent, bottom-up process

o Sensitive to national sovereignty: will only cover matters not considered to be national

o Recommendations are not binding, but tend to be followed because they represent a true consensus

Approval methods

o TAP – traditional approval process(Res. 1)
- Determination at physical meeting
- Approval at physical meeting
- Text available before approval meeting

o AAP – alternative approval process (Rec. A.8)
- Consent at physical meeting
- Last call period
- Approval if no substantive comments
- Additional review or revert to SG or TAP

o Non-normative texts approved at Study Group level
- e.g. Appendices, Supplements, Handbooks
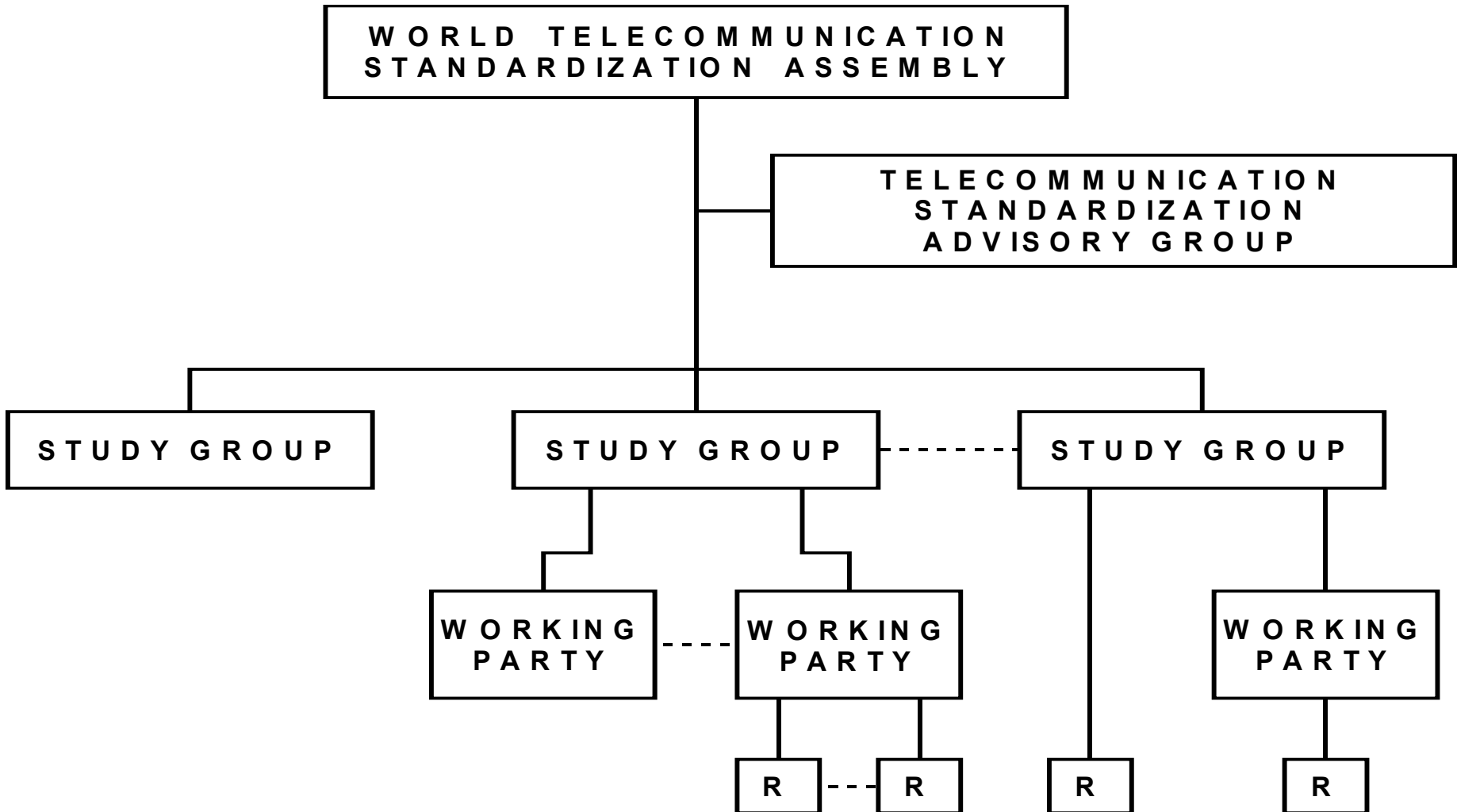
Approval time for ITU-T Recommendations

o Before 1988   4 years

o 1989-1993   2 years

o 1993-1996   18 months

o 1997-2000   9 months (5 months in exceptional circumstances)

o 2000 ➔   Minimum 4 weeks (AAP)
     Average 8 weeks (AAP)
     9 months (TAP – regulatory matters)

AAP = Alternative Approval Procedure

TAP = Traditional Approval Procedure

ITU-T structure

```
┌─────────────────────────────────────────────┐
│       WORLD  TELECOMMUNICATION               │
│       STANDARDIZATION  ASSEMBLY              │
└─────────────────────────────────────────────┘
                    │
                    │      ┌──────────────────────────────────┐
                    │      │      TELECOMMUNICATION           │
                    ├──────│      STANDARDIZATION             │
                    │      │      ADVISORY  GROUP             │
                    │      └──────────────────────────────────┘
                    │
   ┌────────────────┼────────────────────────┐
┌──────────────┐  ┌──────────────┐        ┌──────────────┐
│ STUDY GROUP  │  │ STUDY GROUP  │- - - - │ STUDY GROUP  │
└──────────────┘  └──────────────┘        └──────────────┘
                    │        │              │          │
              ┌──────────┐ ┌──────────┐     │      ┌──────────┐
              │ WORKING  │-│ WORKING  │     │      │ WORKING  │
              │ PARTY    │ │ PARTY    │     │      │ PARTY    │
              └──────────┘ └──────────┘     │      └──────────┘
                            │     │         │          │
                          ┌───┐ ┌───┐    ┌───┐      ┌───┐
                          │ R │-│ R │    │ R │      │ R │
                          └───┘ └───┘    └───┘      └───┘
```

R = RAPPORTEUR GROUP

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

ITU-T Study Group 17

o 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
  - Network / Protocol perspective
o 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 Study Group 2

o Lead SG on Service Definition, Numbering, Routing and Global Mobility → Users' perspective

- principles of service provision, definition and operational requirements of service emulation;
- numbering, naming, addressing requirements and resource assignment
- routing and interworking requirements;
  - **human factors**
  - operational aspects
- networks and associated performance requirements
- interworking between traditional and evolving telecommunication networks;

o Existing Recommendations include

- 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) >>

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.

- o Two Phases:
  - Geneva, 10–12 December 2003
  - Tunis, 16–18 November 2005
- o Website www.itu.int/wsis/
- o 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

o 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)

o Cooperation of all stakeholders (gov'ts, civil society, private sector)

o Guidelines, legislation, share good practices

o User education (privacy, etc)

o National legal instruments for formal recognition of electronic documents (e.g. authentication)

o Strengthen real-time incident handling and response

o Development of secure and reliable applications

o Contributions to the intergov'l agencies working groups (e.g. ITU)

Understanding the problem

A Taxonomy...

o General Guidance/Architecture

   o Network perspective ($\rightarrow$ *SG 17*)

   o Users' perspective ($\rightarrow$ *SG 2*)

o System/Application-Specific
($\rightarrow$ *SGs 4, 9, 11, 13, 15, 16, SSG*)

- Secure Infrastructure

- End-to-end security

Vulnerabilities, Threats and Risks

o **Vulnerability:** something to be exploited...
- threat model (e.g. SS7)
- design (e.g. Ambiguities in BGP4 parameters)
- implementation (e.g. SNMP & ASN.1)
- configuration (e.g. 802.11b – WiFi)

o **Threat:** *people* willing to exploit a vulnerability (hackers, criminals, terrorists, etc)

o **Risk:** the *consequences* of such an exploitation (data loss, fraud, loss of public confidence, etc)

o While *threats* change over time, security *vulnerabilities* exist throughout the life of a protocol

→ *Risks* must be continuously reassessed !!!

SPAM: a security risk

(among other things...)

o Security vulnerabilities...

- Threat analysis

- Implementation

- Configuration

o ... combined with a security threat (abusive e-mailers, virus creators, etc)

o ... produces a security risk: SPAM

Towards a standards-based solution

What to do?

o Pragmatism

o Learned-lessons for a comprehensive framework

- X.400
- SMTP

o Foundational standards

- Protocol requirements
  → *Standardizers & Implementors*
- Best practices → *Users' perspective*

o New or revised standards

o Transitional measures

o Clarify role of different players: ICT industry; governments; users (merchants; ISPs; private persons)

Lessons Learned

o Security considerations are a must!

o Understand SMTP vulnerabilities; e.g.

- Lack of authentication mechanisms, that is positive identification of the sender (Eric Allman, creator of sendmail, *et alii*; and June 2004 US Federal Trade Commission Report to Congress *National Do Not Email Registry*)

- No mechanism for an inbound host to selectively refuse a message (J.Postel, RFC706, 1975)

o Consider solutions already available in other frameworks
   → *e.g. ITU-T Rec. X.400 & X.500*

o Collect the best of existing Best Practices

o Players: all

A way forward

o Pragmatic, multi-pronged approach

o Educate users for safe use of existing systems

o Identify relevant existing or new Foundational Standards

- ¡¡¡ **_Standards_**: *a technical specification developed in an **open** environment, through a **consensus-based** decision process !!!*

o Standardizers & Implementors: agree on Foundational standards; agree on specific Standards

o Governments: identify actions that can help solve the problem (executive and legislative actions)

o Implementors: closely apply the agreed Standards

o Users and User Groups: strive to adhere to defined standards and disseminate Best Practices

Roles of Government

o **Judicial**
- Enforce existing national legislation to curb abuses and ensure protection of consumer's rights
- Frameworks for cooperation across jurisdictions

o **Legislative**
- Create new or adapt existing national legislation to curb abuses and ensure protection of consumer's rights

o **Executive**
- Public education initiatives
- X.509 Public key Infrastructure / Digital Signature
  → Example: Spanish government
  http://www.cert.fnmt.es/ >>
- Joint activity between regulators:
  - Sharing skills, knowledge, experience
  - Where legislation exists, joint enforcement
- Multilateral frameworks for international cooperation (*ITU BDT: drafting group of 6 countries; Dec.2004*)

Roles of Industry

o Agree standards

- For authentication mechanisms (in SMTP, or on top of it, or in successor protocol)
- For subject field headers (e.g. "ADV:")
- For meta-tags to describe message content
- To communicate opt-in and/or opt-out lists
- etc.

o Recognize that the problem is more than just Spam…

Roles of Users

o Flock together

- Share experiences

- Develop Best Practices

- Participate in the debate, contribute to the "next steps" → influence the standardizers

- Learn about secure practices

o Recognize that the problem is more than just Spam…

- Irrelevant information & information overload

- Need of change in paradigm / practices:
    - (Opt-in) distribution channels (RSS)
    - Electronic collaboration tools / distributed workspaces
    - Instant messaging

Some existing ITU-T foundational standards

X.805 - Security Architecture for End-to-End Communications
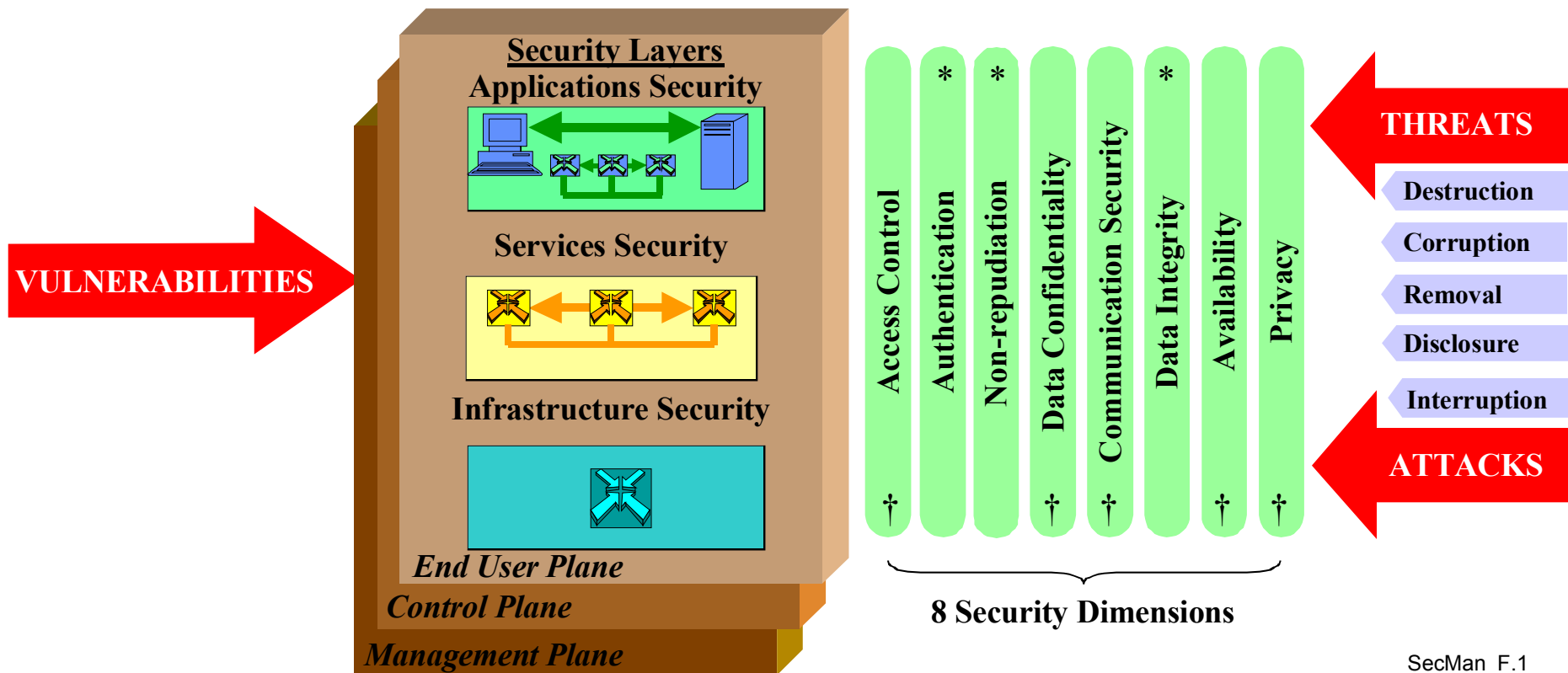
* Conventional Security dimensions
† New concepts in X.805 (extra slides)

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

X.400 – Message handling system and service overview

o Not widely implemented, but basic principles might be worth reusing (done for X.435 and IETF EDI standards)

o Defines Message Handling System (MHS) elements of service for
  - User Agent (UA)-to-UA [Mail Client]
  - Message Transfer Agent (MTA)-to-MTA,
  - UA-to-MTA, and
  - UA-to-Message Storage (MS) [Mail Server]

o Application Layer security services:
  - confidentiality,
  - integrity,
  - authentication,
  - non-repudiation and
  - access control

X.509 – OSI/The Directory: Public-key and attribute certificate frameworks

o 1st edition in 1988; 5th in preparation

o Written to satisfy multiple needs

o Extensibility allows organizations to enhance as needed

o Good cooperation between ITU, ISO, and IETF

o In products such as securing browser traffic and signing executable code

o Laws enabling electronic/digital signature

o Widely implemented, and imitated (e.g. LDAP)

Some additional ITU Resources

ITU Resources

o **ITU-T Recommendations**
http://www.itu.int/rec/recommendation.asp?type=series&parent=T-REC >>

o **ITU Activities on Countering Spam**
http://www.itu.int/osg/spu/spam/ >>

o **ITU SPU newslog on Spam**
http://www.itu.int/osg/spu/newslog/categories/spam/ >>

o **Virtual Conference on Regulatory Cooperation on Spam (30/Mar/2004)**
http://www.itu.int/ITU-D/treg/Events/Seminars/Virtual-events/Spam/ >>

o **Cybersecurity Symposium (4 October 2004)**

Conclusions

Conclusions: Problem recognition

o The social problems and network congestion caused by Internet SPAM are well recognized

o In the future, as the line between Internet appliances and telecommunications devices blur, there are opportunities for even greater misuse

o Action is needed, but the problem is complex

Conclusions: Key factors for success and challenges

o Understand existing vulnerabilities

o Take advantage of lessons learned and adopt a pragmatic, multi-pronged approach:

- patches & fixes for the short-term
- look for a mid- & long-term solution

o Develop a set of global and compatible open, consensus-based Standards, in particular for authentication

o Solutions need to consider national sovereignty & cost aspects

o Partnership between all players

o Rethink paradigms & practices to minimize information overload