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

- Information about ITU
- High-level directives
- Understanding the problem
- Towards a standards-based solution
- Some existing ITU-T foundational standards
- Some additional ITU Resources
- Conclusion
About ITU...
What is ITU?

- International treaty organization founded in 1865 to facilitate international interconnection of telegraphy
- Unique partnership of industry and governments
- 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)
- In ITU-T industry and government work together to develop mutually agreed non-binding Recommendations
ITU-T membership

- Member States: 189
- Sector Members: 162
  - ROAs: 162
  - SIOs: 171
  - Others (including ISOC, regional, International organizations, etc.): 47
- Associates: 84
- 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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval time</td>
<td>4 years</td>
<td>2 years</td>
<td>18 months</td>
<td>9 months (exceptional case: 5 months)</td>
<td>2-9 months</td>
</tr>
<tr>
<td>Publication time</td>
<td>2-4 years</td>
<td>2 years</td>
<td>1-1.5 year</td>
<td>6-12 months</td>
<td>3-9 months</td>
</tr>
</tbody>
</table>

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


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)

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

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

<table>
<thead>
<tr>
<th>Task Force</th>
<th>Intergovernment</th>
<th>NGOs</th>
</tr>
</thead>
<tbody>
<tr>
<td>IETF</td>
<td>ITU-T</td>
<td></td>
</tr>
</tbody>
</table>

### Organizations

- **1394TA**
- **AOEMA**
- **CBOP**
- **COS**
- **ECE**
- **EIDX**
- **FCIA-J**
- **Home API**
- **IMTC**
- **JCTEA**
- **JMF**
- **Mobile Web**
- **ODVA**
- **PCMCIA**
- **SDR**
- **TSC**
- **WDF**

- **3GPP**
- **AOOW**
- **CDG**
- **CTFJ**
- **ECHONET**
- **EMA**
- **FIPA**
- **HomePNA**
- **IMWA**
- **JECALS**
- **LONMARK**
- **MOPA**
- **OIF**
- **PHS MoU**
- **SSIPG**
- **UMTS**
- **Web 3D**

- **3GPP2**
- **ATMF**
- **CIF**
- **CTFJ**
- **ECOM**
- **EMF**
- **FRF**
- **HomePNA**
- **IrDA**
- **JEDIC**
- **MCPC**
- **OMG**
- **PICMG**
- **STA**
- **USBIF**

- **AIM**
- **BINTERMS**
- **CII**
- **DHF**
- **ECTF**
- **ERTICO**
- **FSAN**
- **IDB Forum**
- **ITS America**
- **JEMA**
- **MDG.org**
- **MSForum**
- **POF**
- **TINA-C**
- **UWCC**

- **AMF**
- **AMI-C**
- **Bluetooth**
- **CommerceNet**
- **DOPG**
- **EDIFICE**
- **GWOS**
- **FCIA**
- **GSM Assoc.**
- **IFIP**
- **IFSA**
- **ITF**
- **ITF UK**
- **JAVA**
- **JICSAP**
- **MITF**
- **OASIS**

- **WIFI**
- **OSS**
- **PCCA**
- **SCF**
- **Salutation**
- **SCF**
- **TMForum**
- **TOG**
- **WAP**

### Other Organizations

- **1394TA**
- **AOEMA**
- **CBOP**
- **COS**
- **ECE**
- **EIDX**
- **FCIA-J**
- **IMTC**
- **JCTEA**
- **JMF**
- **Mobile Web**
- **ODVA**
- **PCMCIA**
- **SDR**
- **TSC**
- **WDF**

- **3GPP**
- **AOOW**
- **CDG**
- **CTFJ**
- **ECHONET**
- **EMA**
- **FIPA**
- **HomePNA**
- **IMWA**
- **JECALS**
- **LONMARK**
- **MOPA**
- **OIF**
- **PHS MoU**
- **SSIPG**
- **UMTS**
- **Web 3D**

- **3GPP2**
- **ATMF**
- **CIF**
- **DHF**
- **ECOM**
- **EMF**
- **FRF**
- **HomePNA**
- **IrDA**
- **JEDIC**
- **MCPC**
- **OMG**
- **PICMG**
- **STA**
- **USBIF**

- **AIM**
- **BINTERMS**
- **CII**
- **DHF**
- **ECTF**
- **ERTICO**
- **FSAN**
- **IDB Forum**
- **ITS America**
- **JEMA**
- **MDG.org**
- **MSForum**
- **POF**
- **TINA-C**
- **UWCC**

- **AMF**
- **AMI-C**
- **Bluetooth**
- **CommerceNet**
- **DOPG**
- **EDIFICE**
- **GWOS**
- **FCIA**
- **GSM Assoc.**
- **IFIP**
- **IFSA**
- **ITF**
- **JICSAP**
- **MITF**
- **OASIS**

- **WIFI**
- **OSS**
- **PCCA**
- **SCF**
- **Salutation**
- **SCF**
- **TMForum**
- **TOG**
- **WAP**

**ITU WSIS Thematic Meeting on Countering SPAM / Geneva, 7-8 July 2004**
Cooperation

- A.4 - Communication with forums/consortia
- A.5 - Organizations qualified for referencing
- A.6 - Communication with SDOs
- 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
<table>
<thead>
<tr>
<th>A.4</th>
<th>A.5</th>
<th>A.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN.1 Consortium</td>
<td>ARIB (Association of Radio Industries and Businesses)</td>
<td>ARIB</td>
</tr>
<tr>
<td>ATM Forum</td>
<td>ATM Forum</td>
<td>Committee T1</td>
</tr>
<tr>
<td>DSL Forum</td>
<td>Committee T1</td>
<td>CCSA</td>
</tr>
<tr>
<td>ETIS (e-and telecommunication info. services)</td>
<td>CCSA</td>
<td>ECMA</td>
</tr>
<tr>
<td>FRF (Frame Relay Forum)</td>
<td>DSL Forum</td>
<td>ETSI</td>
</tr>
<tr>
<td>IMTC (Multimedia)</td>
<td>ECMA Standardizing Information &amp; Communication Systems</td>
<td>IEEE</td>
</tr>
<tr>
<td>IPDR Organization</td>
<td>ETSI (European Telecommunications Standards Institute)</td>
<td>JCTEA</td>
</tr>
<tr>
<td>IPv6 Forum</td>
<td>FRF</td>
<td>NIST</td>
</tr>
<tr>
<td>MPLS (Multi Protocol Label Switching Forum)</td>
<td>IEEE (Institute of Electrical and Electronics Engineers)</td>
<td>SCTE</td>
</tr>
<tr>
<td>MSF (Multiservice Switching Forum)</td>
<td>ISOC/IETF (Internet Society/Internet Engineering Task Force)</td>
<td>TIA</td>
</tr>
<tr>
<td>OASIS</td>
<td>JCTEA (Japan Cable Television Engineering Association)</td>
<td>TTA</td>
</tr>
<tr>
<td>OIF (Optical Internetworking Forum)</td>
<td>MPLS Forum</td>
<td>TTA</td>
</tr>
<tr>
<td>OMG (Object Management Group)</td>
<td>NIST (National Institute of Standards and Technology)</td>
<td>TTC</td>
</tr>
<tr>
<td>SDL Forum Society</td>
<td>OASIS</td>
<td></td>
</tr>
<tr>
<td>TM Forum (Tele Management Forum)</td>
<td>OIF</td>
<td></td>
</tr>
<tr>
<td>W3C (World Wide Web Consortium)</td>
<td>OMG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCTE (Society of Cable Telecommunications Engineers)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TIA (Telecommunications Industry Association)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TM Forum</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TTA (Telecommunications Technology Association)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TTC (Telecommunication Technology Committee)</td>
<td></td>
</tr>
</tbody>
</table>
How does ITU-T Develop Recommendations?

- Consensus of Sector Members and Member States
- Work typically driven by Sector Members
- Open (for members), transparent, bottom-up process
- Sensitive to national sovereignty: will only cover matters not considered to be national
- Recommendations are not binding, but tend to be followed because they represent a true consensus
Approval methods

- TAP - traditional approval process (Res. 1)
  - Determination at physical meeting
  - Approval at physical meeting
  - Text available before approval meeting
- 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
- Non-normative texts approved at Study Group level
  - e.g. Appendices, Supplements, Handbooks
Approval time for ITU-T Recommendations

- Before 1988: 4 years
- 1989-1993: 2 years
- 1993-1996: 18 months
- 1997-2000: 9 months (5 months in exceptional circumstances)
- 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 PARTY

WORKING PARTY

WORKING 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

- 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

- 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

- 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;

- 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
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.
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
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)
Understanding the problem
A Taxonomy...

- General Guidance/Architecture
  - Network perspective (SG 17)
  - Users’ perspective (SG 2)
- System/Application-Specific (SGs 4, 9, 11, 13, 15, 16, SSG)
  - Secure Infrastructure
  - End-to-end security
Vulnerabilities, Threats and Risks

- **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)

- **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 !!!
SPAM: a security risk

(among other things...)

- Security vulnerabilities...
  - Threat analysis
  - Implementation
  - Configuration

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

- ... produces a security risk: SPAM
Towards a standards-based solution
What to do?

- Pragmatism
- Learned-lessons for a comprehensive framework
  - X.400
  - SMTP
- Foundational standards
  - Protocol requirements
    → Standardizers & Implementors
  - Best practices → Users’ perspective
- New or revised standards
- Transitional measures
- Clarify role of different players: ICT industry; governments; users (merchants; ISPs; private persons)
Lessons Learned

- Security considerations are a must!
- 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)
- Consider solutions already available in other frameworks
  - *e.g.* ITU-T Rec. X.400 & X.500
- Collect the best of existing Best Practices
- Players: all
A way forward

- Pragmatic, multi-pronged approach
- Educate users for safe use of existing systems
- Identify relevant existing or new Foundational Standards
  - *Standards*: a technical specification developed in an open environment, through a consensus-based decision process!!!
- Standardizers & Implementors: agree on Foundational standards; agree on specific Standards
- Governments: identify actions that can help solve the problem (executive and legislative actions)
- Implementors: closely apply the agreed Standards
- Users and User Groups: strive to adhere to defined standards and disseminate Best Practices
Roles of Government

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

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

- 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

- 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.

- Recognize that the problem is more than just Spam...
Roles of Users

- Flock together
  - Share experiences
  - Develop Best Practices
  - Participate in the debate, contribute to the “next steps” → influence the standardizers
  - Learn about secure practices

- 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

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

VULNERABILITIES

THREATS
- Destruction
- Corruption
- Removal
- Disclosure
- Interruption

ATTACKS

SecMan_F.1

* Conventional Security dimensions
† New concepts in X.805 (extra slides)
X.400 – Message handling system and service overview

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

- 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]

- Application Layer security services:
  - confidentiality,
  - integrity,
  - authentication,
  - non-repudiation and
  - access control
X.509 – OSI/The Directory: Public-key and attribute certificate frameworks

- 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
- Widely implemented, and imitated (e.g. LDAP)
Some additional ITU Resources
ITU Resources

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

- ITU Activities on Countering Spam
  http://www.itu.int/osg/spu/spam/

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

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

- Cybersecurity Symposium (4 October 2004)
Conclusions
Conclusions: Problem recognition

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

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

- Action is needed, but the problem is complex.
Conclusions: Key factors for success and challenges

- Understand existing vulnerabilities
- 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
- Develop a set of global and compatible open, consensus-based Standards, in particular for authentication
- Solutions need to consider national sovereignty & cost aspects
- Partnership between all players
- Rethink paradigms & practices to minimize information overload