5th ETSI Security Workshop
20-22 January 2010, Sophia Antipolis, France

ITU-T Security work

Arkadiy Kremer

ITU-T SG 17 Chairman

"We have received a strong message from our members that ITU is, and will remain the world's pre-eminent global telecommunication and ICT standards body. And we hear also, and very clearly, that ITU should continue on its mission to connect the world, and that bringing the standardization gap, by increasing developing countries participation in our work, is an essential prerequisite to achieve this goal".

Malcolm Johnson, TSB Director

(Closing speech at the WTSA-08)

Telecom security standardization is an essential part of IP-based networks and services development

- Integration of telecommunication and security infrastructures is constantly increasing
- Convergence of services where voice, data/video and broadcasting are appearing on all types of network platforms
- Internet is a part of telecommunication infrastructure
- Next-generation business model for network operators demands subscriber-centric data consolidation
- Any device or application which does not work under security Recommendations might be a weakest link in telecom security infrastructure

Telecom security standardization reflects rapidly-developing technologies and operators' trends

Network security ➡ business infrastructure security

ICT security ➡ information critical infrastructure security

Personal data protection ➡ IdM

Security management ➡ security collaboration

Security architecture ➡ SOA security ➡ cloud computing

ITU-T security activities

- □ Most of the ITU-T SGs have responsibilities for standardizing specific security aspects (TMN security, IPCablecom security, future networks security, multimedia security, disaster management, electromagnetic environment and climate change security issues, etc.)

- □ ITU-T SG 17 provides security coordination within ITU-T SGs, ITU sectors and externally with the ISO/IEC JTC 1/SC 27, ETSI, IETF, Liberty Alliance/Kantara Initiative, FIDIS, OASIS and others through SAG-S, projects, workshops, JCA-IdM, JCA-CIT, LSs, common texts of Recommendations, etc.

- □ ITU-T SG 17 is the Lead Study Group for:

- Telecommunications security
- Identity management
- Languages and description techniques

ITU-T SG 17 history

Study Period	Name
17/9/2001-2004	Data networks and telecommunication software
2005-2008	Security, languages and telecommunication software
2009-2012	Security

ITU-T SG 17 structure

Working Party 1: Network and information security

- Q 1 Telecommunications systems security project
- Q 2 Security architecture and framework
- Q 3 Telecommunications information security management
- Q 4 Cybersecurity
- Q 5 Countering spam by technical means

Work items under development in WP1

• Guidelines on security of the individual information service for operators
• Architecture of external interrelations for a telecommunication network security system • Information security governance framework
• Information security management framework for telecommunications
• Requirement of security information sharing framework • Abnormal traffic detection and control guideline for telecommunication network
• Frameworks for botnet detection and response • Digital evidence exchange file format • Guideline on preventing malicious code spreading in a data communication network • Mechanism and procedure for distributing policies for network security • Framework for countering cyber attacks in SIP-based services • Traceback use cases and capabilities • Framework for countering IP multimedia spam • Functions and interfaces for countering email spam sent by botnet • Technical means for countering spam Interactive countering spam gateway system • Technical means for countering VoIP spam • Cybersecurity information exchange framework • An OID arc for cybersecurity information exchange • Cyber attack tracing event exchange format

ITU-T SG 17 structure (cont.)

Working Party 2: Application security

- Q 6 Security aspects of ubiquitous telecommunication services
- Q 7 Secure application services
- Q 8 Telebiometrics
- Q 9 Service oriented architecture security

Work items under development in WP2

• Functional requirements and mechanisms for secure transcodable scheme of IPTV • Key management framework for secure IPTV services • Algorithm selection scheme for SCP descrambling • SCP interoperability scheme • Security requirement and framework for multicast communication • Security aspects of mobile multi-homed communications • Security framework for ubiquitous sensor network and middleware security guidelines • Secure routing mechanisms for wireless sensor network • SAML 2.0 • XACML 2.0 • Security requirements and mechanisms of peer-to-peer-based telecommunication network • Management framework for one time password based authentication service • Security framework for enhanced web based telecommunication services • Security requirements and mechanism for reconfiguration of mobile device with multiple communication interfaces • The general framework of strong authentication on multiple authentication authorities environment • A guideline on anonymous authentication for e-commerce service • Telebiometrics issues

ITU-T SG 17 structure (cont.)

Working party 3: Identity management and languages

- Q 10 Identity management architecture and mechanisms
- Q 11 Directory services, Directory systems, and public-key/attribute certificates
- Q 12 Abstract Syntax Notation One (ASN.1), Object Identifiers (OIDs) and associated registration
- Q 13 Formal languages and telecommunication software
- Q 14 Testing languages, methodologies and framework
- Q 15 Open Systems Interconnection (OSI)

Work items under development in WP3

• Baseline capabilities for enhanced global identity management trust and interoperability • A framework for user control of digital identity • Entity authentication assurance • Extended validation certificate • Common identity data model • Framework architecture for interoperable identity management systems • IdM terms and definitions • Security guidelines for identity management systems • Criteria for assessing the level of protection for personally identifiable information in identity management • Guideline on protection for personally identifiable information in RFID applications • Object identifier repository export format • Object identifier resolution system • Open distributed processing reference model issues • Use of UML for open distributed processing • SDL 2010 issues • Message sequence chart issues • User requirements notation issues • Testing and test control notation issues • Directories and secure directories

September 2009 SG 17 meeting results for TAP*

*TAP applied for Recommendations with policy and regulatory impact and takes an average of 6 months for completion

Recommendations approved

X.1250 Baseline capabilities for enhanced global identity management and interoperability

X.1251 A framework for user control of digital identity

Recommendations determined (first step of approval)

X.1252 Baseline identity management terms and definitions

X.1275 Guidelines on protection of personally identifiable information in the application of RFID technology

September 2009 SG 17 meeting results for AAP*

*AAP applied for technical Recommendations and takes an average of 2 months for completion

Recommendations consented (first step of approval)

X.1081, Amendment 1 The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics - Object identifier assignments under the Telebiometrics arc

X.1082, Amendment 1 Telebiometrics related to human physiology – Object identifier assignments under the Telebiometrics arc

X.902 (revised) Information technology – Open distributed processing – Reference model: Foundations

X.903 (revised) Information technology – Open distributed processing – Reference model: Architecture

X.906, Corrigendum 1 Information technology – Open distributed processing - Use of UML for ODP system specification

September 2009 SG 17 meeting results for non-normative texts

Supplement and Appendices approved:

X.Sup.6 (revised) ITU-T X.1240 series – Supplement on countering spam and associated threats

X.1081, Amendment 2 The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics – Appendix V, Hierarchy theory principles

Z.120, Amendment 1 (revised) Message sequence chart (MSC) – Appendix I, Application of MSC

Security projects

Security Compendium

– Includes catalogs of approved security-related Recommendations and security definitions extracted from approved Recommendations

Security Standards Roadmap

– Includes searchable database of approved ICT security standards from ITU-T and others (e.g., ISO/IEC, IETF, ETSI, IEEE, ATIS)

ITU-T Security Manual

- Aggregates all of the available information on the deployment of existing ITU-T Recommendations for secure telecommunications. It aims to act as a guide for technologists, middle level management and regulators to assist in the practical implementation of security functions

Summary

1. It is necessary to assure the continued relevance of security standards by keeping them current with rapidly-developing telecommunications technologies and operators' trends (in e-commerce, e-payments, e-banking, telemedicine, fraud-monitoring, fraud-management, fraud identification, digital identity infrastructure creation, billing systems, IPTV, Video-on-demand, grid network computing, ubiquitous networks, etc.).

2. Considerable attention has been recently given to the issue of trust between network providers and communication infrastructure vendors, in particular, in terms of communication hardware and software security. Issues of how trust can be established and/or enhanced need to be considered.

Summary

3. There are a number of standards in the field of telecommunications and information security. But a standard is the real standard when it is used in real-world applications. Business and governmental bodies need to learn more about standards from their business applications rather than from a technical point of view.

4. Implementations of ITU-T security Recommendations capable of being tested for conformance and interoperability. Implementations that cannot be tested, that involve extensive resources, or that require access to confidential information, are unacceptable. There needs to be some work to determine how the need for conformance and interoperability testing of implementations can be supported.

Forthcoming ITU-T security events

- ITU-T JCA-CIT meeting (Moscow, 30-31 March 2010)
- ITU-T JCA-IdM meeting (Moscow, 30-31 March 2010)
- ITU-T SG 17 meeting (Geneva, 07-16 April 2010)
- ITU-T Security Workshop (Geneva, 06-07 December 2010)
- ITU-T SG 17 meeting (Geneva, 08-17 December 2010)

NOTE: other activities (Rapporteur Groups, Correspondence Groups) shown at http://www.itu.int/ITU-T/studygroups/com17/meetings.html

Thank you!

Arkadiy Kremer
kremer@rans.ru