

Date: 1 November 2007
Original: English

Document 2/4-E

Contribution to the Second Meeting of the Internet Governance Forum

ITU-T Security Initiatives – an Update

Michael Harrop

Rapporteur ITU-T SG 17 Q4, Communications Security Project

Introduction

In 2006, the ITU-T prepared a broad overview of the ITU-T security initiatives as input to the Internet Governance Forum (http://www.intgovforum.org/Substantive_1st_IGF/05%20-%20IGF-Sec_overviewRev.doc). This paper provides an update to last year's contribution.

The ITU-T Study Groups

The current four-year ITU Study Period will end in 2008. As noted last year, 12 Study Groups (SGs) of the ITU-T have been identified as having security-related activities in the current Study Period. These are listed in Table 1.

ITU-T Recommendations (i.e. standards) are published with reference numbers that indicate the particular area of standardization (e.g. the X. series covers data networks and open system communications; the H. series addresses audiovisual and multimedia systems). Figure 1 illustrates the security standards building blocks across the various series of Recommendations.

Much of the security work is concentrated in Study Group 17, *Security, Languages and Telecommunications Software*, which has been designated the Lead Study Group for telecommunications security issues. SG 17's security-related Questions (i.e. ITU project areas) are summarized in Table 2.

<u>Study Group 2: Operational aspects of service provision, networks and performance</u> (Lead Study Group for service definition, numbering and routing)
<u>Study Group 4: Telecommunication management</u>
<u>Study Group 5: Protection against electromagnetic environment effects</u>
<u>Study Group 6 Outside Plant and related indoor installations</u>
<u>Study Group 9 Integrated broadband cable networks and television and sound transmission</u>
<u>Study Group 11 Signalling requirements and protocols</u> (Lead Study Group on Signalling and Protocols and Intelligent Networks.)
<u>Study Group 12 Performance and quality of service</u>
<u>Study Group 13 Next Generation Networks</u> (Lead Study Group for NGN and satellite matters.)
<u>SG 15: Optical and other transport networks</u>
<u>SG 16: Multimedia services, systems and terminals</u> (Lead Study Group on multimedia terminals, systems and applications, and on ubiquitous applications (such as e-health and e-business)).
<u>Study Group 17: Security, languages and telecommunication software</u> (Lead Study Group on telecommunication security)
<u>SG 19: Mobile Telecommunications Networks</u>

Table 1: ITU-T Study Groups with security responsibilities

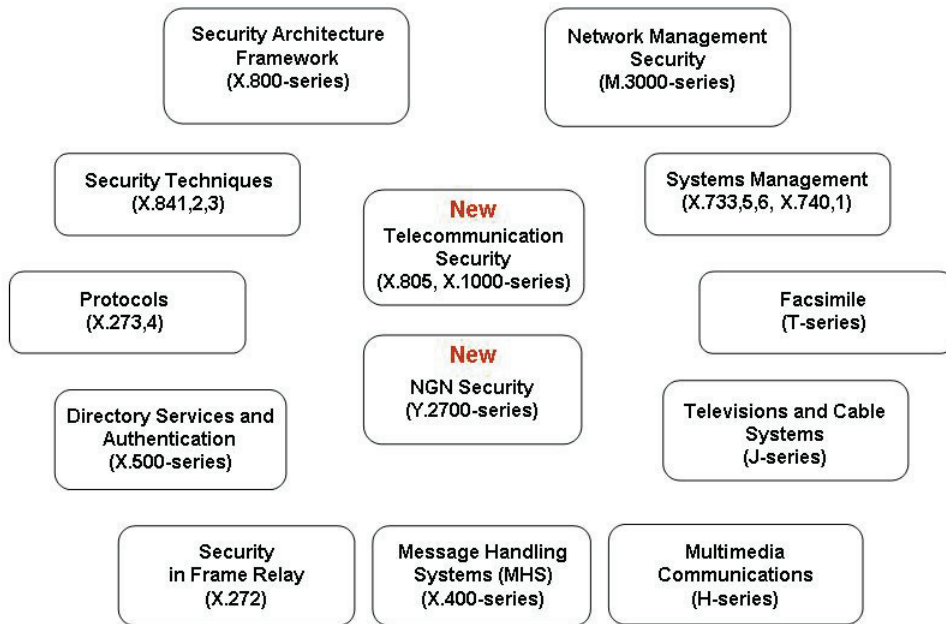


Figure 1: ITU-T Security Building Blocks

Q1	End-to-end Multicast Communications with QoS Managing Facility
Q2	Directory services, Directory systems, and public-key/attribute certificates
Q3	Open Systems Interconnection (OSI)
Q4	Communications Systems Security Project
Q5	Security Architecture and Framework
Q6	Cyber Security
Q7	Security Management
Q8	Telebiometrics
Q9	Secure Communication
Q10	ASN.1 and other data languages
Q14	Testing languages, Methodologies and Framework
Q17	Countering spam by technical means

Table 2: SG 17 Security-related Questions

Study Group 17 Security Coordination Initiatives and Outreach Activities

As the Lead Study Group for security, SG 17 continues to be engaged in various security coordination and outreach activities. In addition, SG17 has supported two Focus Groups over the past year. A summary of some of the key SG17 outreach and coordination activities is provided below.

Focus Groups

Focus Groups (FGs) can be established by the ITU-T to augment the work program and to address specific needs as they are identified. Focus Groups can be created very quickly and are usually short-lived. They allow for the rapid development of specifications in their chosen areas. They choose their own working methods, leadership, financing, and types of deliverables and are open to participation by non-ITU-T member organizations.

The Focus Group Security Baseline for Network Operators completed its work in September 2007. The objective of the group was to define a security baseline against which network operators could assess their network and information security posture in terms of what security standards are available, which of these standards should be used to meet particular requirements, when they should be used, and how they should be applied. The resulting report will be published as a Supplement to the X.800 – X.849 series of Recommendations.

The Focus Group on Identity Management has attracted wide participation and interest and has produced a substantial number of deliverables and reports. The FG objectives were to facilitate and advance the development of a generic Identity Management framework. As a result of extensive discussion at the September 2007 SG 17 meeting, a number of steps were agreed for future consideration of Identity Management work. The work can be tracked via the following web link:

www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

Security Standards Roadmap

The Security Standards Roadmap is an on-line resource that provides information on existing security standards and on-going standards work. During the past year, the Roadmap has been expanded and enhanced in a number of areas. Links are now provided to published security standards of the ITU-T, ISO/IEC JTC1, IETF, ATIS, ETSI IEEE and OASIS. In May 2007 we moved the listing of approved standards to a database format that allows a user to search for security standards by organization or by topic. Another development was the addition of a new section that lists security best practices. In January 2007, ITU-T was pleased to welcome the European Network and Information Security Agency (ENISA) and the Network and Information Security Steering Group (NISSG) as partners in the development of the Roadmap.

The Roadmap is available at: www.itu.int/ITU-T/studygroups/com17/ict/index.html

Other SG 17 Security Resources

In addition to the Roadmap, SG 17 continues to develop and maintain several documents of interest:

- A website has been developed for the SG 17 Lead Study Group on Telecommunication Security at <http://www.itu.int/ITU-T/studygroups/com17/tel-security.html>.

- The Security Compendium includes a Catalogue of approved ITU-T Recommendations related to Telecommunication Security (available at <http://www.itu.int/ITU-T/studygroups/com17/cat005.doc>) and an extract of ITU-T approved security definitions (available at <http://www.itu.int/ITU-T/studygroups/com17/tel-security.html>). The Compendium will be updated in April 2008
- The publication [Security in Telecommunications and Information Technology](#) (also known as the ITU-T Security Manual) is available on the SG 17 website as well as in printed and CD format.
The manual is expected to be updated next in the second quarter of 2008.
- Summaries of all SG 17 Recommendations under development or revision may be found at http://www.itu.int/ITU-T/studygroups/com17/SG_17final-summaries.doc.
- "Security Guidance for ITU-T Recommendations" to help ensure security considerations have been adequately addressed in Recommendations is available at <http://www.itu.int/ITU-T/studygroups/com17/tel-security.html>.
- Information summarizing ITU-T security-related activities is available at http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000050001MSWE.doc.
- Information summarizing other ITU security-related activities is available at http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000070001MSWE.doc.

Workshops and Symposia

SG17 experts have participated in a number of workshops and seminars over the past year including the ETIS Security Conference, the World Summit on the Information Society (WSIS), the Global Standards Collaboration (GSC 12) meeting and the Hanoi Regional Workshop on Cybersecurity and Critical Information Infrastructure Protection. Presentations from these and other speaking engagements are available on the ITU-T SG 17 website at:

www.itu.int/ITU-T/special-projects/security/presentations.html

Summary

The ITU-T continues to pursue a very active program to try to ensure that security is built in to communications standards. We welcome the opportunity to collaborate with other organizations, particularly our colleagues in other standards-setting fora. By working together, pooling our resources and expertise, we will produce more timely and effective solutions to counter current and evolving threats to network security.