Geneva, 28 November 2016

Ref:	**TSB Circular 246** SG17/MEU	**To:** - Administrations of Member States of the Union
Tel:	+41 22 730 5866	
Fax:	+41 22 730 5853	
E-mail:	tsbsg17@itu.int	**Copy to:** - ITU-T Sector Members; - ITU-T Associates; - ITU Academia; - The Chairman and Vice-Chairmen of ITU-T Study Group 17; - The Director of the Telecommunication Development Bureau; - The Director of the Radiocommunication Bureau
Subject:	**Meeting of ITU-T Study Group 17, 22-30 March 2017, Geneva, with a view to approving draft Recommendations ITU-T X.1058 (X.gpim), X.1080.0 (X.pbact), X.1126 (X.msec-11), X.1212 (X.cogent), X.1362 (X.iotsec-1), X.1373 (X.itssec-1), and X.1550 (X.nessa) in accordance with the provisions of Resolution 1, Section 9, of WTSA (Rev. Dubai 2012)**	

Dear Sir/Madam,

1 At the request of the Chairman of ITU-T Study Group 17: *Security*, I have the honour to inform you that this Study Group, which will meet from 22 March 2017 to 30 March 2017, intends to apply the procedure described in Resolution 1, Section 9, of WTSA (Dubai, 2012) for the approval of the above-mentioned draft Recommendations.

2 The titles, summaries and locations of the draft ITU-T Recommendations proposed for approval will be found in Annex 1.

3 Any ITU Member State, Sector Member, Associate or Academic Institution aware of a patent held by itself or others which may fully or partly cover elements of the draft Recommendations proposed for approval is requested to disclose such information to TSB, in accordance with the Common Patent Policy for ITU-T/ITU-R/ISO/IEC.

Available patent information can be accessed online via the ITU-T website (www.itu.int/ipr/).

4 Having regard to the provisions of Resolution 1, Section 9, I should be grateful if you would inform me by 2400 hours UTC on 13 March 2017 whether your Administration assigns authority to ITU-T Study Group 17 that these draft Recommendations should be considered for approval at the Study Group meeting.

Should any Member States be of the opinion that consideration for approval should not proceed, they should advise their reasons for disapproving and indicate the possible changes that would facilitate further consideration and approval of the draft Recommendations.

5 If 70% or more of the replies from Member States support consideration for approval of these draft Recommendations at the Study Group meeting, one Plenary session will be devoted on 30 March 2017 to apply the approval procedure.

I accordingly invite your Administration to send a representative to the meeting. **The Administrations of Member States of the Union are invited to supply the name of the head of their delegation. If your Administration wishes to be represented at the meeting by a recognized operating agency,** a scientific or industrial organization or another entity dealing with telecommunication matters, the Director should be duly informed, in accordance with Article 19, No. 239, of the ITU Convention.

6 The agenda and all relevant information concerning the ITU-T Study Group 17 meeting will be available from Collective letter 1/17.

7 After the meeting, the Director of TSB will notify, in a circular, the decision taken on these Recommendations. This information will also be published in the ITU Operational Bulletin.

Yours faithfully,

Chaesub Lee
Director of the Telecommunication
Standardization Bureau

Annex: 1

Annex 1
(to TSB Circular 246)

Summary and location

1 Draft Recommendation ITU-T X.1058 (ex X.gpim) (R 69 Rev.1)

Information technology - Security techniques - Code of practice for Personally Identifiable Information protection

Summary

The number of organizations processing personally identifiable information (PII) is increasing, as is the amount of PII that these organizations deal with. At the same time, societal expectations for the protection of PII and the security of data relating to individuals are also increasing. A number of countries are augmenting their laws to address the increased number of high profile data breaches. This Recommendation | International Standard establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of Personally Identifiable Information (PII). In particular, this Recommendation | International Standard specifies guidelines based on ISO/IEC 27002, taking into consideration the requirements for processing PII which may be applicable within the context of an organization's information security risk environment(s).

2 Draft Recommendation ITU-T X.1080.0 (ex X.pbact) (R 75)

Access control for telebiometrics data protection

Summary

Recommendation ITU-T X.1080.0, Access control for telebiometrics data protection, is a specification for how to protect telebiometrics information against unauthorized access. It does so by taking a service-oriented view, where only information necessary for a particular purpose is provided, i.e., access is given not only on a right-to-know basis, but also on a need-to-know basis. The heart of this Recommendation is an attribute specification included in an attribute certificate or public-key certificate that specifies in details what privileges a particular entity has for one or more service types. Security is provided by using a profile of the cryptographic message syntax (CMS). The CMS profile provides authentication, integrity and, when required, confidentiality (encryption). This profile is intended to provide security support for telebiometrics specifications in general. The profile assumes and is dependent upon a correct deployment of a public-key infrastructure (PKI). Recommendation ITU-T X.1080.0 is also dependent on a deployment of a privilege management infrastructure (PMI).

3 Draft Recommendation ITU-T X.1126 (ex X.msec-11) (R 76)

Guidelines on mitigating the negative effects of infected terminals in mobile networks

Summary

Recommendation ITU-T X.1126 provides guidelines to mobile operators to restrain the infected terminals by utilizing technologies in the mobile network to protect both subscribers and mobile operators. This Recommendation describes the characteristics and effects of malicious software caused by unhealthy ecosystems in the mobile environment. Based on network-side technologies, this Recommendation focuses on mitigating the vicious effects caused by infected terminals. This Recommendation defines and organizes the mitigating measures and corresponding technologies.

4 Draft Recommendation ITU-T X.1212 (ex X.cogent) (R 71)

Design considerations for improved end-user perception of trustworthiness indicators

Summary

Diverse kinds of attacks employ replicated content from trustworthy service providers, thereby deceiving end-users into believing its false trustworthiness. Recommendation ITU-T X.1212 describes design consideration for improved end-user perception of trustworthiness indicators. The appendices describe representative techniques for measuring end-user perception of such indicators.

5 Draft Recommendation ITU-T X.1362 (ex X.iotsec-1) (R 77)

Simple encryption procedure for Internet of things (IoT) environments

Summary

It is considered that the Internet of things (IoT) is one of the most important areas for future standardization. From the ITU-T perspective, IoT is defined as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things. In certain IoT environments, especially for IoT devices, there is a real-time processing requirement where tasks are processed within a certain period of time. To ensure data confidentiality and integrity protection, one of the most basic countermeasures is the application of data encryption/authentication algorithms. The problem with the standard applications of data encryption/authentication algorithms is that this requirement could not be met. Recommendation ITU-T X.1362 specifies encryption with associated mask data (EAMD) for the Internet of things (IoT) devices. It describes EAMD and how it provides a set of security services for traffic using it.

6 Draft Recommendation ITU-T X.1373 (ex X.itssec-1) (R 78 Rev.2)

Secure software update capability for intelligent transportation system communication devices

Summary

As intelligent transportation system (ITS) technologies improve, it has become common for vehicles to communicate with other entities such as other vehicles, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Since electric devices inside a vehicle such as electronic control units (ECUs), and electric toll collections (ETCs), system and car navigation systems are becoming more sophisticated. As a result, software modules inside those electric devices need to be appropriately updated for the purpose of bug fixing, and for performance and security improvements to avoid crucial accidents. In order to fulfil the above requirement, Recommendation ITU-T X.1373 provides secure software update procedures between software update server and vehicles with appropriate security controls. This Recommendation can be practically utilized by car manufactures and ITS-related industries as a set of standard capabilities for best practices.

7 Draft Recommendation ITU-T X.1550 (ex X.nessa) (R 72)

Access control models for incident exchange networks

Summary

Recommendation ITU-T X.1550 introduces existing approaches for implementing access control policies for incident exchange networks. This Recommendation introduces a variety of well-established access control models, sharing models as well as criteria for evaluating incident

exchange network performance. Standards-based solutions are considered to facilitate implementation of different access control models within different cybersecurity information sharing models and under diverse trust environments.

____