Geneva, 27 September 2012

|  |  |
| --- | --- |
| **Telecommunication StandardizationBureau** |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Ref:Tel:Fax: | **TSB Circular 311**COM 17/MEU+41 22 730 5866+41 22 730 5853 | - To Administrations of Member States of the Union |
| E-mail: | tsbsg17@itu.int  | **Copy:**- To ITU-T Sector Members;- To ITU-T Associates;- To ITU-T Academia;- To the Chairman and Vice-Chairmen of Study Group 17;- To the Director of the Telecommunication Development Bureau;- To the Director of the Radiocommunication Bureau |

|  |  |
| --- | --- |
| Subject: | **Meeting of Study Group 17 with a view to approving draft new Recommendations ITU-T X.1126, X.1154, X.1526 and X.1544 in accordance with the provisions of Resolution 1, Section 9, of WTSA (Johannesburg, 2008),Geneva, 26 April 2013** |

Dear Sir/Madam,

1 At the request of the Chairman of Study Group 17, *Security*, I have the honour to inform you that this Study Group, which will meet from 17 to 26 April 2013, intends to apply the procedure described in Resolution 1, Section 9, of WTSA (Johannesburg, 2008) for the approval of the above-mentioned draft new Recommendations.

2 The titles, summaries and location of the draft new 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 on‑line via the ITU‑T website ([www.itu.int/ITU-T/ipr/](http://www.itu.int/itu-t/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 5 April 2013** whether your Administration assigns authority to Study Group 17 that these draft new 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 new Recommendations.

5 If 70% or more of the replies from Member States support consideration for approval of these draft new Recommendations at the Study Group meeting, one Plenary session will be devoted **on 26 April 2013** 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 Study Group 17 meeting will be available from the Collective letter to be issued in the future.

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,

Malcolm Johnson
Director of the Telecommunication
Standardization Bureau

**Annex: 1**

**ANNEX 1
(to TSB Circular 311)**

**Summary and location of the texts**

**Draft new Recommendation ITU-T X.1126 (X.msec-6), Security aspects of smartphones
COM 17 – R 67**

**Summary**

With the continuous development of functionalities and expansion of applications, smartphones are facing many security threats, which can cause serious social and economic problems. The objectives of Recommendation ITU-T X.1126 are to protect the personal privacy of users and to improve information security of smartphones.

This Recommendation identifies smartphone threats which are categorized into vulnerabilities and attacks. In order to satisfy such security objectives, this Recommendation specifies a hierarchical security framework and relevant security requirements for smartphones. With regard to the security framework, this Recommendation provides necessary security solutions through system improvements and security tools.

**Draft new Recommendation ITU-T X.1154 (X.sap-4), General framework of combined authentication on multiple identity service provider environments
COM 17 – R 68**

**Summary**

Recently, many application services, especially financial services, require more reliable or combined authentication methods such as multifactor authentication due to the increase in identity (ID) theft. For example, one-time password authentication and other new authentication methods are used instead of the traditional password-based authentication.

The combinations of authentication methods provide multiple identity service providers (IdSPs) the ability to enhance the assurance of authentication. Recommendation ITU-T X.1154 provides the general framework of combined authentication in multiple IdSP environments for a service provider. In this Recommendation, three types of combined authentication methods are considered: multifactor authentication, multi-method authentication and multiple authentications.

The framework in this Recommendation describes models, basic operations and security requirements for each model component and each message between the model components to maintain an overall level of authentication assurance in situations of a combination of multiple IdSPs.

In addition, the framework also describes models, basic operations and security requirements to support the authentication service that manages a combination of multiple IdSPs.

**Draft new Recommendation ITU-T X.1526 (X.oval), Open vulnerability and assessment language
COM 17 – R 64**

**Summary**

This Recommendation on the use of the Open Vulnerability and Assessment Language (OVAL), an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analysing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language.

The OVAL community has developed three schemas written in Extensible Markup Language (XML) to serve as the framework and vocabulary of the OVAL Language. These schemas correspond to the three steps of the assessment process: an OVAL System Characteristics schema for representing system information, an OVAL Definition schema for expressing a specific machine state, and an OVAL Results schema for reporting the results of an assessment.

Content written in the OVAL Language is located in one of the many repositories found within the community. One such repository is known as the OVAL Repository. It is the central meeting place for the OVAL Community to discuss, analyse, store, and disseminate OVAL Definitions. Each definition in the OVAL Repository determines whether a specified software vulnerability, configuration issue, program, or patch is present on a system.

The information security community contributes to the development of OVAL by participating in the creation of the OVAL Language on the OVAL Developers Forum and by writing definitions for the OVAL Repository through the OVAL Community Forum. An OVAL Board consisting of representatives from a broad spectrum of industry, academia, and government organizations from around the world oversees and approves the OVAL Language and monitors the posting of the definitions hosted on the OVAL Web site. This means that OVAL reflects the insights and combined expertise of the broadest possible collection of security and system administration professionals worldwide.

**Draft new Recommendation ITU-T X.1544 (X.capec), Common attack pattern enumeration and classification
COM 17 – R 65**

**Summary**

The common attack pattern enumeration and classification (CAPEC)Recommendation is an XML/XSD based specification for the identification, description, and enumeration of attack patterns. Attack patterns are a powerful mechanism to capture and communicate the attacker’s perspective. They are descriptions of common methods for exploiting software. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples. The objective of CAPEC is to provide a publicly available catalogue of attack patterns along with a comprehensive schema and classification taxonomy.

CAPEC enables:

* Standardizing the capture and description of attack patterns
* Collecting known attack patterns into an integrated enumeration that can be consistently and effectively leveraged by the community
* Classifying attack patterns such that users can easily identify the subset of the entire enumeration that is appropriate for their context
* Linking the attack patterns and the weaknesses (CWEs) that they are effective against through explicit references.

As many sources and examples as possible are leveraged from the CAPEC community and other interested parties, to develop the specific and succinct definitions of the CAPEC Dictionary elements and a variety of views and classification tree structures.

\_\_\_\_\_\_\_\_\_\_\_\_