|  |  |
| --- | --- |
| **电信标准化局** | **logo_C_** |
|  |  |

2012年9月27日，日内瓦

|  |  |  |
| --- | --- | --- |
| 文号：  电话：  传真： | **电信标准化局第311号通函**  COM 17/MEU  +41 22 730 5866  +41 22 730 5853 | - 致国际电联各成员国主管部门 |
| 电子 邮件： | [tsbsg17@itu.int](mailto:tsbsg17@itu.int) | **抄送：**  - ITU-T部门成员；  - ITU-T部门准成员；  - ITU-T学术成员；  - 第17研究组正副主席；  - 电信发展局主任；  - 无线电通信局主任 |

|  |  |
| --- | --- |
| 事由： | **第17研究组按照世界电信标准化全会（2008年，约翰内斯堡） 第1号决议第9节的规定为批准ITU-T X.1126、X.1154、X.1526和X.1544新建议书草案而召开的会议**  **2013年4月26日，日内瓦** |

尊敬的先生/女士：

1 应第17研究组（安全）主席的请求，我荣幸地告知您，该研究组将于2013年4月17至26日召开会议，并将采用世界电信标准化全会（2008年，约翰内斯堡）第1号决议第9节规定的程序来批准上述新建议书草案。

2 建议批准的新的ITU-T建议书草案的标题、摘要及其出处见**附件1**。

3 所有了解自己或他人持有的专利可能整体或部分地涉及建议批准的（一项或多项）建议书草案内容的国际电联成员国、部门成员、部门准成员或学术机构，均需按照  
ITU-T/ITU-R/ISO（国际标准化组织）/IEC（国际电工委员会）的共同专利政策，向电信标准化局披露这类信息。

可通过ITU-T网站（[www.itu.int/ITU-T/ipr/](http://www.itu.int/itu-t/ipr/)）在网上获取已公布的专利信息。

4 考虑到第1号决议第9节的规定，请您在**2013年4月5日**协调世界时24时告知我，贵主管部门是否同意授权第17研究组在该研究组会议上审议并批准上述新建议书草案。

如有成员国认为不应进入审议批准程序，则应阐明其反对原因并提出可能的修改意见，以推动对相关新建议书草案的进一步审议，以便批准。

5 如果70%以上的成员国在回复中支持在该研究组会议上审议并批准上述新建议书草案，则将于**2013年4月26日**召开一次全体会议，实施该批准程序。

为此，我邀请贵主管部门派出一名代表参加会议。请**国际电联成员国的主管部门**提供其代表团团长的姓名。如果贵主管部门希望由一家经认可的运营机构、一个科学或工业组织或处理电信问题的另一实体作为代表参加会议，则应按照国际电联《公约》第19条第239款的规定，将有关情况适时向主任通报。

6 有关第17研究组会议的议程和所有相关信息将在未来发布的集体函中提供。

7 会后电信标准化局主任将以通函的形式通报就这几份建议书做出的决定。此信息还将在《国际电联操作公报》中公布。

顺致敬意!

电信标准化局主任  
 马尔科姆•琼森

**附件：1件**

**（电信标准化局第311号通函）  
附件1**

案文摘要和出处

**ITU-T X.1126 (X.msec-6)新建议书草案 – 智能电话安全方面问题（COM 17 – R 67)**

摘要

随着功能性的进一步发展和应用的不断扩展，智能电话面临越来越多的安全威胁，由此带来严重的社会和经济问题。ITU-T X.1126建议书的目标是保护用户的个人隐私并改善智能电话的信息安全。

本建议书将智能电话面临的威胁分类为脆弱性和攻击。为满足这些安全目标，本建议书具体规定了智能电话的分层安全框架和相关安全要求。在安全框架方面，本建议书提供通过系统改善和安全工具的必要安全解决方案。

**ITU-T X.1154 (X.sap-4)新建议书草案 – 多身份服务提供商环境中混合认证的一般性框架（COM 17 – R 68）**

**摘要**

最近以来，许多应用服务，特别是金融服务，要求得到更可靠的或混合认证方法的支持，例如多因数认证，因为身份（ID）盗窃问题日益严重。例如，目前得到使用的是一次性密码认证和其他新的认证方法，而非传统的基于密码的认证。

混合认证方法为多身份服务提供商（IdSP）提供了加强认证保障的能力。ITU-T X.1154建议书为服务提供商提供多IdSP环境中的混合认证的一般性框架。本建议书考虑了三种类型的混合认证方法：多因数认证、多方法认证和多重认证。

本建议书中的框架描述模型、基本操作和每个模型成份的安全要求，以及每个模型成份之间的每一条信息，以便在多IdSP混合环境中保持认证的总体保障水平。

此外，该框架还描述支持认证服务（管理多IdSP的合并）的模型、基本操作和安全要求。

**ITU-T X.1526 (X.oval)新建议书草案 – 开放漏洞和评估语言（COM 17 – R 64）**

摘要

有关开放漏洞和评估语言（OVAL）使用的本建议书描述一项促进公开提供的安全内容的国际化、信息安全和社区标准，以实现这种信息在整个安全工具和业务层面的传送的标准化。OVAL包括用于对系统细节进行编码的语言，以及整个语言界持有的各类内容存储库。语言对评估程序的主要三个步骤进行了标准化：呈现用于测试的系统配置信息；分析表现特定机器状态（漏洞、配置、补丁状态等）的系统；报告这种评估的结果。存储库是使用语言的一系列公开提供和开放的内容。

OVAL语言界在扩展标记语言（XML）中开发了三种方案，作为OVAL语言的框架和词汇。这些方案与评估程序的三个步骤相对应：表现系统信息的OVAL系统特性方案、表示特定机器状态的OVAL定义方案和报告评估结果的OVAL结果方案。

OVAL语言中书写的内容置于语言界内众存储库之一，其中一个这类存储库称为OVAL存储库，这是OVAL语言界讨论、分析、存储和传播OVAL定义的集中会晤地点。OVAL存储库中的每一个定义均确定系统是否存在特定的软件漏洞、配置问题、程序或补丁。

信息安全领域人士通过参加OVAL开发商论坛和通过在OVAL社区论坛中书写OVAL存储库定义为创建OVAL语言并开发OVAL作出了贡献。由来自世界各地业界、学术机构和政府组织组成的OVAL委员会负责监督和批准OVAL语言，并监督OVAL网站托管的定义的发布。这意味着OVAL反映了世界范围内最为广泛的安全和系统管理专业人士的真知灼见和专业技术知识。

**ITU-T X.1544 (X.capec)新建议书草案 – 通用攻击模式列表和分类（COM 17 – R 65）**

摘要

有关通用攻击模式列表和分类（CAPEC）的本建议书是基于XML/XSD规范的，旨在确定、描述攻击模式并对之进行列表。攻击模式是强有力的机制，可以捕捉和相互沟通攻击者的视角。本建议书主要描述利用软件的通用方法，其源泉是用于破坏性而非建设性环境的设计规律概念，并由深入分析现实世界的具体利用示例而产生。CAPEC的目标是提供公开开放的攻击模式目录，以及综合方案和分类分类学。

CAPEC有助于：

* 实现捕捉和描述攻击模式的标准化
* 将已知攻击模式收集整理为综合列表，以便相关人员连贯一致和有效地加以使用
* 将攻击模式进行分类，以便用户轻而易举地确定适合其环境的整个列表的相关部分
* 将攻击模式与薄弱环节（CWE（通用缺陷列表））相联系，以便通过明确参引使其发挥效用。

本建议书使用了尽可能多的来自CAPEC界和其他相关方的渠道和示例，制定了CAPEC字典要素的具体和简明扼要定义，以及一系列不同观点和分类树状结构。

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