国 际 电 信 联 盟

ITU-T X.1544

(04/2013)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络安全信息交换 – 事件/事故/探索法交换

常见攻击模式列举和分类

ITU-T X.1544 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法交换	**X.1540–X.1549**
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1544 建议书

常见攻击模式列举和分类

摘要

ITU-T X.1544建议书是基于XML/XSD，对攻击模式进行识别、描述和列举的规范。攻击模式是从攻击者角度出发进行捕捉和沟通的强有力的机制。它们对软件开发的常用方法进行描述。攻击模式源自于设计模式的概念，适用于破坏性而不是建设性的内容，由深入分析特定的现实世界中的开发实例而生成。CAPEC的目标是提供公共和开放的攻击模式目录，以及综合方案和分级分类。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1544	2013-04-26	17

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

页码

引言

常见攻击模式列举和分类(CAPEC)的建议书是基于XML/XSD的规范，用于识别、描述和列举攻击模式。攻击模式是从攻击者角度出发进行捕捉和沟通的强有力的机制。它们对软件开发的常用方法进行描述。攻击模式源自于设计模式的概念，适用于破坏性而不是建设性的内容，由深入分析特定的现实世界中的开发实例而生成。CAPEC的目标是提供公共和开放的攻击模式目录，以及综合方案和分级分类。

CAPEC有助于：

- 实现攻击模式标准化的捕捉和描述
- 将已知的攻击模式收集整理为综合列表，以便被社区持续，有效地利用
- 对攻击模式进行分类，使得用户能够很容易地确定适合其上下文的整个列表的子集
- 关联攻击模式与薄弱环节(CWE，通用缺陷列表)，以便通过显式引用使其发挥效用

ITU-T X.1544建议书在开发过程中铭记可维护性的重要性，另外在可能的范围内，考虑ITU-T X.1544建议书和“CAPEC兼容性的要求和建议”版本1.0（由MITRE公司于2012年8月30日出版（https://capec.mitre.org/compatible/requirements_v1.0.html）之间的技术兼容性。

ITU-T X.1544 建议书

常见攻击模式列举和分类

1 范围

本建议书提供了公共和开放的攻击模式的结构化交换，以及综合方案和分级分类。

2 参考文献

以下ITU-T建议书和其他参考文献所包含的规定，通过本文件的引用，构成本建议书的规定。在本标准出版时，标明的版本是有效的。所有的建议书和其他参考文献都会被修订；因此本建议书的用户被鼓励探讨采用最新版本的建议书和下面列出的其他参考文献的可能性。当前有效的ITU-T建议书列表将会定期公布。引用本建议书的文件未给出，因为本建议书是一份独立的文件。

[ITU-T X.1500] ITU-T X.1500建议书（2011年），网络安全信息交换概述。

3 定义

3.1 其他地方定义的术语

3.1.1 review authority 审查权[b-ITU-T X.1520]：进行审查的实体。

注 — MITRE 是目前唯一的审查机关。

3.1.2 vulnerability 脆弱性[ITU-T X.1500]：软件中的任何弱点，可以用来破坏系统或它所包含的信息。

3.2 本建议书定义的术语

本建议书定义了以下术语：

3.2.1 accuracy percentage 准确度百分比：在审查样例的安全元素中引用正确的CAPEC标识符所占百分比。

3.2.2 attack instance 攻击实例：针对应用程序或系统，利用系统中的漏洞或薄弱环节进行的特定的，详细的进攻。

3.2.3 attack pattern 攻击模式：在自然情况下观察到的针对应用程序或系统的常见攻击方法的抽象(例如，SQL注入攻击，中间人攻击，会话劫持等)。
注 — 一个单一的攻击模式可能潜在关联许多不同的攻击实例。

3.2.4 capability 能力：提供有关攻击实例和模式信息的评估工具，动态应用程序安全测试(DAST)工具、渗透测试工具、开发框架工具、威胁建模工具、数据库、网页站点、咨询或服务等。

3.2.5 map/mapping 变换/映射：资料库中的攻击模式元素和元素相关的CAPEC内容之间的关系的说明书。

3.2.6 owner 所有者[基于 b-ITU-T X.1520]:：对能力负责的托管人(实际的个人或公司) (如本建议书定义)。

3.2.7 repository 资料库：显示或隐式的支持某项能力的攻击模式元素的集合，例如，攻击模式数据库，DAST工具或网页站点的攻击实例集合。

3.2.8 review 审查：确定某项能力是否是CAPEC兼容的过程。

3.2.9 review version 审查版本：标注的CAPEC版本，用于确定某项能力的CAPEC兼容性。

3.2.10 security element 安全元素：关联一个特定攻击模式的数据库记录，评估探测，攻击实例，开发，有效载荷等。

3.2.11 task 任务：工具的探测，检查，签名等，用于执行某些操作，生成相应的安全信息(即，安全元素)。

3.2.12 tool 工具：一个软件应用程序或设备，通过仿真，评估或特征化系统的潜在攻击，从而对应用程序或系统进行安全属性测试，例如，评估工具、DAST工具、渗透测试工具、开发框架工具、威胁建模工具。

3.2.13 user 用户[基于 b-ITU-T X.1520]：消费者或潜在有能力的消费者（如本建议书中定义）。

3.2.14 weakness 弱点(薄弱环节)：软件代码，设计，架构或实施中的缺点或缺陷，在某些时候可能成为漏洞，或可能引入其他漏洞。

4 缩略语和缩写词

本建议书使用下列缩略语和缩写词：

CAPEC 常见攻击方式列举和分类

CCR 覆盖声明要求书

CIA 机密性、完整性或可用性

CWE 共同弱点列举

DAST 动态应用程序安全测试工具

GUI 图形用户界面

IDS 入侵检测系统

POC 接触点

5 惯例

本建议书中的关键词“需”、“须”、“不得”、“应”、“不应”、“建议”、“可以”和“可选”按照《ITU-T 作者指南》进行解释。（可获取于 http://www.itu.int/oth/T0A0F000004/en）。

6 高层次的需求

以下条目定义了CAPEC标识符正确使用的相关概念、角色和责任，用于不同安全测试能力(工具、资料库和服务)之间的数据共享，以及允许这些安全测试的能力同时使用，以促进安全测试工具和服务的比较。

前提

6.1 能力所有者应当是有效的法律实体，例如一个组织或一个特定的个体，拥有一个有效的电话号码、电子邮件地址和街道邮箱地址。

6.2 能力必须提供超过CAPEC本身提供的额外价值或信息(即，名称、描述、风险、参考文献以及相关的缺陷信息)。

6.3 能力所有者必须提供与审查机构沟通的技术联络点，其具有资格回答能力关于任何CAPEC相关功能的问题。

6.4 能力必须向公众，或消费群体提供，采用生产版本或发布版本。

6.5 为了CAPEC的兼容性，能力所有者必须向认证机构提供完整的“CAPEC兼容性需求评估表”。

6.6 能力所有者必须向审查机构提供资料库的完全访问权，以使得当局可以确定资料库是否满足所有相关的映射精度要求。

6.7 能力所有者必须允许审查机构使用资料库来识别任意的应被添加至CAPEC的攻击模式。

6.8 能力所有者必须同意遵守所有的CAPEC兼容性的强制性要求，其中包括能力的特定类型的强制性要求。

功能

6.9 为了CAPEC的兼容性，能力必须允许用户使用CAPEC标识符(“CAPEC-可搜索”)来查找安全元素。

6.10 为了CAPEC的兼容性，当能力呈现安全元素给用户时，它必须允许用户获取与之关联的CAPEC标识符(“CAPEC-输出”)。

6.11 为了CAPEC的兼容性，能力映射必须准确地关联安全元素到相应的CAPEC标识符(“映射准确度”)。

6.12 为了CAPEC的兼容性，能力的文件必须充分描述CAPEC，CAPEC兼容性以及能力的CAPEC相关功能如何使用(“CAPEC-文件”)。

6.13 为了CAPEC的兼容性，能力公开可用的文件必须明确列出CAPEC标识符，且能力所有者考虑作为能力的部分功能进行覆盖(“CAPEC-覆盖”)。

6.14 为了CAPEC的兼容性，能力公开可用的网站应该为能力提供CAPEC覆盖，使用XML文件形式的CAPEC覆盖声明要求书(CCR)。

6.15 能力必须标注CAPEC版本使用的日期(“版本使用”)。

6.16 能力必须满足附件A规定的特定能力类型的任何额外要求。

6.17 对于发布媒体，能力必须满足附件B说明的所有要求。

6.18 能力不需要完成以下内容：

- 使用 CAPEC 相同的描述或引用；
- 在其资料库中包括每个 CAPEC 标识符。

杂项

6.19 如果能力不能满足上述的所有适用要求(6.1至6.18条)，则能力所有者不应该声明它是CAPEC兼容。

7 准确性

假如能力映射是正确的，CAPEC的兼容性仅仅有利于数据共享和数据相关。因此，CAPEC兼容的能力必须满足下列的最小程度的准确要求。

7.1 资料库必须有100%的准确度。

7.2 在审查期间，能力所有者必须纠正任何审查机构发现的映射错误。

7.3 审查期结束后，能力所有者应该在映射错误初始报告后的一个合理时间间隔内对它进行纠正，比如在能力资料库的两个版本内或六个月内，取两者中时间较短的一个。

7.4 能力所有者应准备和签署一份声明表示，尽能力所有者的知识所知，没有错误的映射。

7.5 如果能力基于或使用另一个CAPEC兼容的能力(“源”能力)，以及能力所有者开始注意到源能力的映射错误，则能力所有者必须向源能力的所有者报告这些错误。

8 文件

以下要求适用于能力提供的文件。

8.1 文件中必须包含CAPEC和CAPEC兼容性的一份简要说明，这可以根据来自于CAPEC网页站点上的部分文件。

8.2 文件必须描述用户使用CAPEC标识符，如何在能力的资料库中查找个人安全元素。

8.3 文件必须描述用户如何从能力资料库的单个元素中获取CAPEC标识符。

8.4 如果文件包括一个索引，则它应该包括术语“CAPEC”下面的CAPEC相关文件的引用。

9 CAPEC 版本使用

用户必须知道使用的是什么版本的CAPEC，用于能力的资料库映射到相应的CAPEC。能力所有者可以显示映射的当前情况，通过使用映射更新时的CAPEC版本号或日期。

9.1 能力必须确定用于创建或更新映射的CAPEC版本号或更新日期，通过下列的至少一项内容：变更日志，新功能列表，帮助文件，或一些其他的机制。对应于版本或更新日期，能力是“最新的”。

9.2 每一个新版本的能力应该达到最新的一个CAPEC版本，在能力向用户公布之前其时间不超过四个月。如果能力不能满足这一要求，则它是“过时的”。

9.3 新的CAPEC版本或更新在CAPEC网页站点上出现后，能力所有者应该公布其更新能力资料库的进度。

10 CAPEC 兼容性的废止

10.1 如果审查机构已经证实能力是CAPEC兼容的，但是随后的某时刻审查机构有证据表明要求不再满足，则审查机构可能废止其认证。

10.1.1 审查机构必须明确不满足的特定要求。

10.2 审查机构必须确定能力所有者的行为或声明是否存在“有意误导”。

10.2.1 审查机构可能按照其意愿来解释短语“有意误导”。

10.3 审查机构不应该考虑废止某项特定功能的CAPEC兼容性认证，往往超过六个月一次。

警告和评估

10.4 审查机构必须对能力所有者和技术联络点（POC）提供废止警告，且至少在废止预计执行的2个月前。

10.4.1 如果审查机构发现能力所有者存在有意误导的行为或声明，则审查机构可能跳过警告期。

10.5 如果能力所有者认为要求都得到满足，则能力所有者可以回应废止警告，通过提供特定的细节表明提供的能力满足相应的要求。

10.6 如果能力所有者在警告阶段修改其能力，使其符合要求，则审查机构应该终止能力的废止行动。

废止

10.7 审查机构可能推迟废止日期。

10.8 审查机构必须公开，某能力的CAPEC兼容性已被撤销。

10.9 如果审查机构发现能力所有者关于CAPEC兼容性的要求存在有意误导的行为，则废止应该持续至少一年。

10.10 审查机构可能公开废止原因。

10.11 能力所有者可能关于废止行为在同一网站上发表公开声明。

10.12 如果认证被废止，能力所有者不得在废止期间申请新的审查。

11 审查机构

11.1 审查机构必须对于特定的CAPEC版本审查相关能力的CAPEC兼容性，即审查版本。

11.2 审查机构必须清楚地确定审查版本，用于确定能力的兼容性。

11.3 审查机构必须清楚地确定CAPEC兼容性要求文件的版本，用于明确能力的兼容性。

11.4 审查机构必须就CAPEC映射准确程度，检查能力资料库中的每个元素。

11.5 审查机构应该每年至少审查一项能力的映射准确程度。

11.6 根据任何希望开始CAPEC 兼容性过程的有效能力所有者的要求，审查机构必须提供一份CAPEC 兼容性申报表。

11.7 根据任何已经提交完整CAPEC 兼容性申报表的能力所有者的要求，审查机构必须提供一份CAPEC 兼容性要求评估表的复本。

附件A

特定类型的要求

（本附件是本建议书的组成部分）

由于各种各样的能力使用CAPEC，某些能力的类型可能有独特的特征，需要特别关注CAPEC的兼容性。

A.1 能力必须满足与其特定类型相关的所有额外要求。

A.1.1 如果能力是评估工具、DAST工具、渗透测试工具、开发框架工具、威胁建模工具或产品，集成一个或多个这些项目类型的结果，则它必须满足工具要求，第A.2.1 - A.2.8节。

A.1.2 如果能力是一项服务(例如安全性评估服务，渗透测试服务或教育培训服务)，则它必须满足安全性服务的需求，第A.3.1-A.3.5节。

A.1.3 如果能力是已知攻击，基于网络的资源或信息网站的在线数据库，则它必须满足在线能力要求第A.4.1-A.4.3节。

A.2 工具的要求

A.2.1 工具必须允许用户使用CAPEC标识符来定位其关联的任务(“CAPEC-可检索”)，通过提供以下的至少一项：“查找”或“搜索”功能，工具的任务名称和CAPEC标识符之间的映射，或由审查机构的其他机制进行决定。

A.2.2 对于任何标识单独安全元素的报告，该工具必须允许用户确定这些元素关联的CAPEC标识符(“CAPEC-输出”)，通过执行以下操作的一个或多个：直接在报告中包括CAPEC标识符，在工具的任务名称和CAPEC标识符之间提供映射，或由审查机构使用一些其他机制来有效确定。

A.2.3 公开获得的文件必须清晰地列出CAPEC标识符，以使能力所有者考虑工具在实例化过程中的有效性(“CAPEC-兼容性覆盖声明”)。

A.2.4 能力的公开可用网页站点可能为能力提供CAPEC兼容性覆盖声明，使用CCR XML文件的形式。

A.2.5 任何要求的报告或映射必须满足附件B规定的媒体要求。

A.2.6 工具，或能力所有者，应该为用户提供一个全CAPEC标识符的列表，并与工具的任务相关联。

A.2.7 工具应该允许用户选择一组任务，通过提供一个包含CAPEC标识符列表的文件。

A.2.8 工具的界面应该允许用户浏览，选择和取消选择一组任务，通过使用单个的CAPEC标识符。

A.2.9 如果工具不具有与CAPEC标识符关联的任务，如用户在A.2.5或A.2.6工具要求书中的说明，则该工具应该通知用户，它不能执行相关联的任务。

A.3 安全服务的要求

安全服务可能在其工作中使用CAPEC兼容的工具，但是它们可能不会为客户提供直接访问工具的权力。因此，对于客户而言识别和比较不同服务的能力可能是困难的。安全服务要求记录了这些潜在的限制。

A.3.1 安全服务必须能够使用CAPEC标识符来告诉用户哪一个安全元素被测试或由提供的服务覆盖(“CAPEC-可搜索”)，通过执行以下操作中的一个或多个：提供用户CAPEC标识符列表，用于确定被测试的元素或服务覆盖的元素；向用户提供服务元素和CAPEC标识符之间的映射；响应用户提供的CAPEC标识符列表，通过确定哪一个CAPEC标识符被测试或被服务覆盖，或通过使用一些其他机制。

A.3.2 对于任何指出个人安全元素的报告，服务必须允许用户确定这些元素相关联的CAPEC标识符（“CAPEC-输出”），通过执行以下操作中的一个或多个：允许用户直接在报告中包括CAPEC标识符，为用户提供安全元素和CAPEC标识符之间的映射，或通过使用一些其他机制。

A.3.3 公开获得的文件必须清晰地列出CAPEC标识符，以使能力所有者考虑安全服务有效地覆盖其发售（“CAPEC-兼容性覆盖声明”）。

A.3.4 能力的公开可用的网页站点可能提供关于其的CAPEC兼容性覆盖声明，采用CCR XML文件的形式。

A.3.5 服务所提供的任何要求的报告或映射必须满足附件B规定的媒体的要求。

A.3.6 如果服务为用户提供了直接访问已标识安全元素的产品，则该产品应该是CAPEC兼容的。

A.4 在线能力的要求

A.4.1 在线能力必须允许用户从在线能力资料库（“CAPEC-可搜索”）中发现相关的安全要素，通过提供下述之一：搜索功能，返回相关元素的CAPEC标识符；关联每个元素与相关CAPEC标识符的映射；或一些其他的机制。

A.4.1.1 在线能力应该提供URL“模板”，允许电脑程序轻松地构建链接，用于访问在线能力的要求A.4.1款描述的搜索功能。

构建链接的例子：
http://www.example.com/cgi-bin/db-search.cgi?capecid=XXX
http://www.example.com/capec/xxx.html

A.4.1.2 如果该网站可公开访问，而无需登录，则CGI程序应接受“GET”方法。

A.4.2 对于任何单独安全元素的报告，在线能力必须允许用户确定这些元素关联的CAPEC标识符（“CAPEC-输出”），通过执行下列操作中的至少一个：允许用户直接在报告中包

括CAPEC标识符，向用户提供安全性元素和CAPEC标识符之间的映射，或通过一些其他的机制。

A.4.3 公开获得的文件必须明确列出CAPEC标识符，以使能力所有者考虑在线能力资料库进行覆盖(“CAPEC-兼容性覆盖声明”)。

A.4.4 能力的公开可用的网页站点可能提供能力的CAPEC兼容性覆盖声明，作为CAPEC CCR XML文件。

A.4.5 如果在线能力并没有提供对个人安全元素的详细信息，则在线能力必须提供映射，关联每个元素及其相关的CAPEC标识符。

附件B

媒体要求

（本附件是本建议书的组成部分）

B.1 CAPEC兼容性能力使用的分发媒体必须使用本附件包含的媒体格式。

B.2 媒体格式必须满足该格式的特定要求。

B.3 电子文件（HTML、文字处理器、PDF、ASCII文本等）。

B.3.1 文件必须是常见的格式，支持“查找”或“搜索”功能（“CAPEC搜索”），比如原始ASCII文本，HTML或PDF。

B.3.2 如果文件只提供单个元素的简短名字或标题，则它必须列出这些元素相关的CAPEC标识符（“CAPEC-输出”）。

B.3.3 文件应该包括元素到CAPEC标识符的映射，其中列出了每个元素的相应页。

B.4 图形用户界面

B.4.1 GUI必须为用户提供搜索功能，它允许用户输入CAPEC标识符以及检索相关的元素（“CAPEC-可搜索”）。

B.4.2 如果图形用户接口 （GUI）列出单个元素的细节，则它必须列出映射到该元素的CAPEC标识符（“CAPEC-输出”）。否则，GUI必须向用户提供映射，其格式满足B.3.1款电子文件的要求。

B.4.3 GUI应该允许用户导出或访问CAPEC相关的数据，采用满足B.3.1款电子文件要求的另一种格式。

参考资料

[b-ITU-T X.1520] ITU-T X.1520建议书（2011），常见漏洞和披露。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2013年，日内瓦