国 际 电 信 联 盟

ITU-T X.1214

(03/2018)

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

网络空间安全 – 网络安全

电信/信息通信技术网络的安全评定技术手段

ITU-T X.1214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	X.1080–X.1099
安全应用和服务(1)	
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(1)	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	
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(2)	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
安全协议(2)	X.1450–X.1459
网络安全信息交换	
网络安全综述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息要求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全综述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实现	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1214 建议书

电信/信息通信技术网络的安全评定技术手段

摘要

ITU-T X.1214建议书向电信领域的开发者、制造商、运营商和个人安全专家介绍了针对基于软件的电信/信息通信技术（ICT）网络元素的安全评定方法和最佳做法，以解决其基于软件的元素的安全问题。传统的电路交换网络和基于分组的网络皆面临来自外部和内部的、以电信/ICT网络各个部分为目标的不同威胁与攻击。本建议书涵盖电信/ICT网络方面的以下内容：

– 检测漏洞；

– 安全评定方法。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1214	2018-03-29	17	11.1002/1000/13404

关键词

双字节分析、模糊测试、渗透测试、安全评定、安全测试、源代码审核、漏洞扫描

* 如访问建议书，请在您的Web浏览器地址栏中输入网址http://handle.itu.int/，然后输入建议书的唯一识别码。例如http://handle.itu.int/11.1002/1000/11830-en。

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）在电信、信息和通讯技术领域是国际电信联盟的常设机构。国际电信联盟电信标准化部门负责研究技术、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。

世界电信标准化大会（WTSA），每四年举行一次，负责确定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第一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和适应性等），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

国际电联提醒注意：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、有效性或适应性不做任何立场。

至本建议书截止之日起，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，这可能并非最新消息，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

引言

电信/ICT网络在多数国家的经济增长中发挥至关重要的作用，从而导致各国政府对电信行业进行监管，包括要求确保电信设备和网络的安全性。电信运营商应采用稳健和妥善管理的安全计划，以确保其网络中基于软件的各个元素免受内外部的恶意攻击，同时确保顺应本地的监管环境。为此，需要根据全球认可的安全标准和最佳做法为这些基于软件的元素制定一个非常有效的安全评定机制。

面临瞬息万变的威胁局面，长期保持一个机构网络的安全性是一项艰巨而耗时的工作。各机构不得不为纠正安全漏洞付出昂贵的代价。这些费用涉及补救工作、客户保护和保留计划、法律活动、应对商业伙伴的失望情绪、员工生产率降低和收入减少等问题。有效的安全评估方法有助于各机构避免这些财务陷阱，在攻击和安全漏洞发生前及早发现并解决对其基于软件的资产和功能构成威胁的风险。从安全角度而言，包括政府、金融行业和电信在内的各个市场对独立评估的需要与日俱增。

本建议书主要强调了电信/ICT网络运营商和服务提供商为及早发现和评估其基于软件的元素漏洞可采用的安全评定技术手段。

ITU-T X.1214建议书

电信/信息通信技术网络的
安全评定技术手段

1 范围

本建议书探讨了电信/信息通信技术（ICT）网络中基于软件的元素可采用的安全评定技术手段。无论是传统的电路交换网络，还是下一代基于分组的网络均面临针对电信/ICT网络基于软件的元素各个部分的各种内外部威胁和攻击。网络部署前对基于软件的各组成部分的安全评估有助于运营商和服务提供商大大加强这些网络的可靠性。因此，该领域需要标准化，从而为开发人员、制造商、运营商和每一位安全专家提供对基于软件的元素的全面的安全评定标准和最佳做法。

本建议书包括以下可以单独和酌情综合使用的功能。

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。所有的建议书及其他参考文献都会得到修订；因此鼓励本建议书的用户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。本建议书中对文件的引用没有给出，因为本建议书是一份独立的文件。

[ITU-T X.1520] ITU-T X.1520 (2014)建议书，常见漏洞和暴露风险

[ITU-T X.1524] ITU-T X.1524 (2012)建议书，通用缺陷列表（CWE）

[ITU-T X.1544] ITU-T X.1544 (2013)建议书，常见攻击模式列举和分类

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 存储库（repository）[ITU-T X.1524]：支持功能的与安全相关的软件缺陷元素的含蓄或明确集合，如安全缺陷数据库、代码分析器中的模式集，或网站。

3.1.2 漏洞（vulnerability）[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。

3.1.3 缺陷（weakness）[ITU-T X.1524]：软件编码、设计、架构或部署中的缺点或瑕疵，它们可在某个时候成为漏洞，或催生其它漏洞。

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 双字节分析（binary analysis）：识别机器语言可执行文件中缺陷的技术手段。

3.2.2 模糊测试（fuzzing）：通过提供意外输入并监测例外情况发现软件中未知或零日漏洞的技术手段。

3.2.3 变更（mutation）：分割输入数据包中的单独字节、词或字符串。

3.2.4 渗透测试（penetration testing）：评估利用所发现的漏洞的影响的技术手段。

3.2.5 安全评定（security assessment）：识别安全漏洞和风险的明确研究。

3.2.6 基于签名的扫描（signature based scanning）：一种将目标内容与已知签名数据库相比较从而确定漏洞的扫描手段。

如与某一个签名匹配，扫描软件则发现漏洞并提出补救行动建议。

3.2.7 源代码审核（source code review）：识别用高级语言编写的软件代码段中的缺陷的技术手段。

3.2.8 工具（tool）：审核主机、网络、软件、双字节、软件应用或设备或其他人工制品并产生有关漏洞、缺陷或暴露情况信息的软件应用或设备，如漏洞扫描软件、模糊测试工具、源代码审核工具、双字节分析软件或渗透测试工具。

3.2.9 漏洞扫描（vulnerability scanning）：识别目标内已知或已公布的漏洞的技术手段。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

CAPEC 通用攻击模式列举和分类

CVE 通用漏洞和暴露情况

CWE 通用缺陷列举

DUT 测试中的设备

ICT 信息通信技术

OS 操作系统

SQL 结构化查询语言

5 惯例

无。

6 基本概念 – 安全测试

电信/ICT网络通常由来自不同供应商的各种不同设备组成。为进行评定必须制定高度可信赖的第三方认证计划，以便发现并评估设备软件、固件和硬件实施中包含的安全缺陷和漏洞。产品的安全评估主要是检测和验证存在的漏洞。漏洞检测可以分为两大类别（见第6.1和6.2节）。

6.1 检测已知或公布的漏洞

在常用软件产品上发现软件漏洞习以为常。这些漏洞是由国家漏洞数据库和若干其他数据库（如通用漏洞和暴露情况（CVE））公布的。因此，有效管理公布的漏洞是现代企业安全工作的一项重要活动。人工跟踪系统中出现的所有漏洞并予以适当纠正是一项艰巨的任务。现有的自动化手段可通过基于签名的草棉检测到这些漏洞并参考[b-CVE]予以确认。

6.2 检测未知或零日漏洞

此类检测涉及发现至今尚未公布的漏洞。检测方法多种多样，每种方法各有利弊。没有一种方法是完美无缺的，也没有一种方法包治百病。用于未知或零日漏洞检测的工具和手段包括模糊测试、源代码审核工具和双字节分析工具等。有关这些工具的详情将在第7.2至7.5节阐述。

7 安全测试手段

如上所述，检测基于软件的元素中的漏洞的方法多种多样且各有利弊。没有一种方法可应对一个目标的所有可能漏洞。因此，有效的评定机制必须采用多种方式，详情见第7.1至7.5节。

7.1 漏洞扫描

网络漏洞扫描软件是一项用来扫描网络架构并报告在网络基于软件的元素中所发现的漏洞的设备或软件。在漏洞扫描中，漏洞签名数据库与从网络扫描中获得的信息相比较，从而产生一个网络中假设存在的漏洞清单。有时，软件亦包含渗透测试手段，为实际利用已发现的漏洞以全面认证其存在提供可能。漏洞分析是评估所发现的漏洞的严重性的过程。各机构的操作环境通常都存在大量漏洞，其中一些漏洞可以导致比其他漏洞更高的安全风险，举例而言，一些软件漏洞如被利用将产生严重的后果。因此，必须评定最严重的问题并及时纠正。

漏洞扫描通常实施于与互联网相连以及未与互联网相连但与内部网络相连的系统，从而评定软件漏洞。

用于漏洞扫描的工具、存储库和服务须为与[ITU-T X.1520]规定的要求和功能兼容的CVE。

7.2 模糊测试

模糊测试被定义为通过提供意外输入并监测例外情况发现软件中未知或零日漏洞的方法。这一通常为自动或半自动的程序包含重复操作并向目标软件提供数据以完成处理。目标软件可能是协议堆、应用或文件，据此，模糊测试亦可为协议模糊测试、应用模糊测试或文件模糊测试。研究人员或测试人员无需了解目标的内部工作程序，因此该方式有时亦称为黑箱测试方式。

模糊测试主要分两个类型，即生成的模糊测试和基于变更的模糊测试，分别见第7.2.1和第7.2.2节的说明。

7.2.1 生成的模糊测试

在此方法中，测试案例从研究具体的规范开始，以便了解所有支撑的数据结构和可接受的数值范围。之后生成目标输入以测试边界条件或违规情况。创建测试案例可能需要提前开展大量工作，但也有将其重复利用于相同协议或文件格式的多项应用测试的好处。

7.2.2 基于变更的模糊测试

基于变更的模糊测试对与目标相关的以包捕获形式存在的现有数据样本进行变更以创建测试案例。样本中每个单独的字节、词或字符串经过分割后发送至目标。这种方式几乎不需要初步研究并可在很短的时间内开发完成。然而，这种方式不够高效，因为它需要收集大量数据样本，以便对目标协议进行良好覆盖。

模糊测试最适用于可造成程序毁坏的问题，如缓冲溢出、跨网址指令码、服务拒绝攻击、格式故障和结构化查询语言（SQL）插入。模糊测试对于那些不会造成程序毁坏的安全威胁（如间谍软件、一些病毒、蠕虫、木马和键盘记录器）不太有效。

用于模糊测试的工具、存储库和服务须为与[ITU-T X.1524]规定的要求和功能兼容的CWE。

7.3 源代码审核

源代码审核是软件开发人员为发现缺陷或问题而采用的常见方式，亦称为白箱测试。审核既可以通过人工方式完成或在自动化手段的帮助下完成。鉴于软件程序通常包含数百万条代码，纯人工审核通常是不现实的。自动化手段可为简化工作提供宝贵的资源，但只能确定可能的漏洞或令人怀疑的代码。有时需要通过人工分析来确定检测到的问题是否确实有效，因为该工具也会错误的显示阳性结果。厂商或制造商不愿分享源代码是这种方式面临的最大局限。

用于源代码审核的工具、存储库和服务须为与[ITU-T X.1524]规定的要求和功能兼容的CWE。

7.4 双字节分析

使用机器语言说明，而不是源代码进行的安全评估通常被称为双字节分析。双字节分析通过利用可执行机器代码分析一项应用的控制和数据流产生一个行为模型，即攻击者看到的方式。与源代码工具不同的是，这种方式准确检测核心应用中的问题并将覆盖扩大至第三方数据库中发现的漏洞、预包装的组件以及排版软件或具体平台说明中引用的代码。

软件开发是一个多层程序，其中涉及的与日俱增的各类威胁（如来自恶意代码和后门的威胁）难以通过源代码审核工具加以确定，因为这些在源代码中是不可见的。这些威胁的最终形式可利用静态双字节分析在应用中发现。

用于双字节分析的工具、存储库和服务须为与[ITU-T X.1524]规定的要求和功能的兼容的CWE。

7.5 渗透测试

渗透测试是通过安全方式利用系统漏洞来评估基础设施安全性的主动和经认可的方式，包括操作系统（OS）、协议和应用错误、不适当的配置、甚至具有风险的最终用户行为。渗透测试的根本目的是测量系统或最终用户妥协的可行性并就此类事件对相关资源和操作产生的结果进行评估。这些测试通常使用人工或自动技术加以完成，以便对服务器、端点、应用、无线网络、网络设备、移动设备和其他可能的暴露点进行系统破坏。渗透测试目标可能是白箱（提供背景和系统信息）或黑箱（仅提供基本信息或无信息）。

通过进行渗透测试，可以提早发现最严重的漏洞，不太严重的漏洞或误判情况。这样，各机构就可以根据轻重缓急更明智地采取补救活动并实施必要的安全补丁。

用于渗透测试的工具、存储库和服务须为与[ITU-T X.1544]规定的要求和功能兼容的常见攻击模式列举和分类（CAPEC）。

附录I

流程图

（本附录不构成本建议书的组成部分）

将安全评定手段组织到流程图中是安全评定进程的良好开端。为编制该图，可考虑一个模型，其中评定始于网络最基础部分并延伸至网络内的综合系统。首先为软件元素的源代码提供安全性，之后为系统中的应用和数据库、直至网络中的各个系统以及总体部署网络提供安全性。

因此，整个安全评定应分两个阶段：

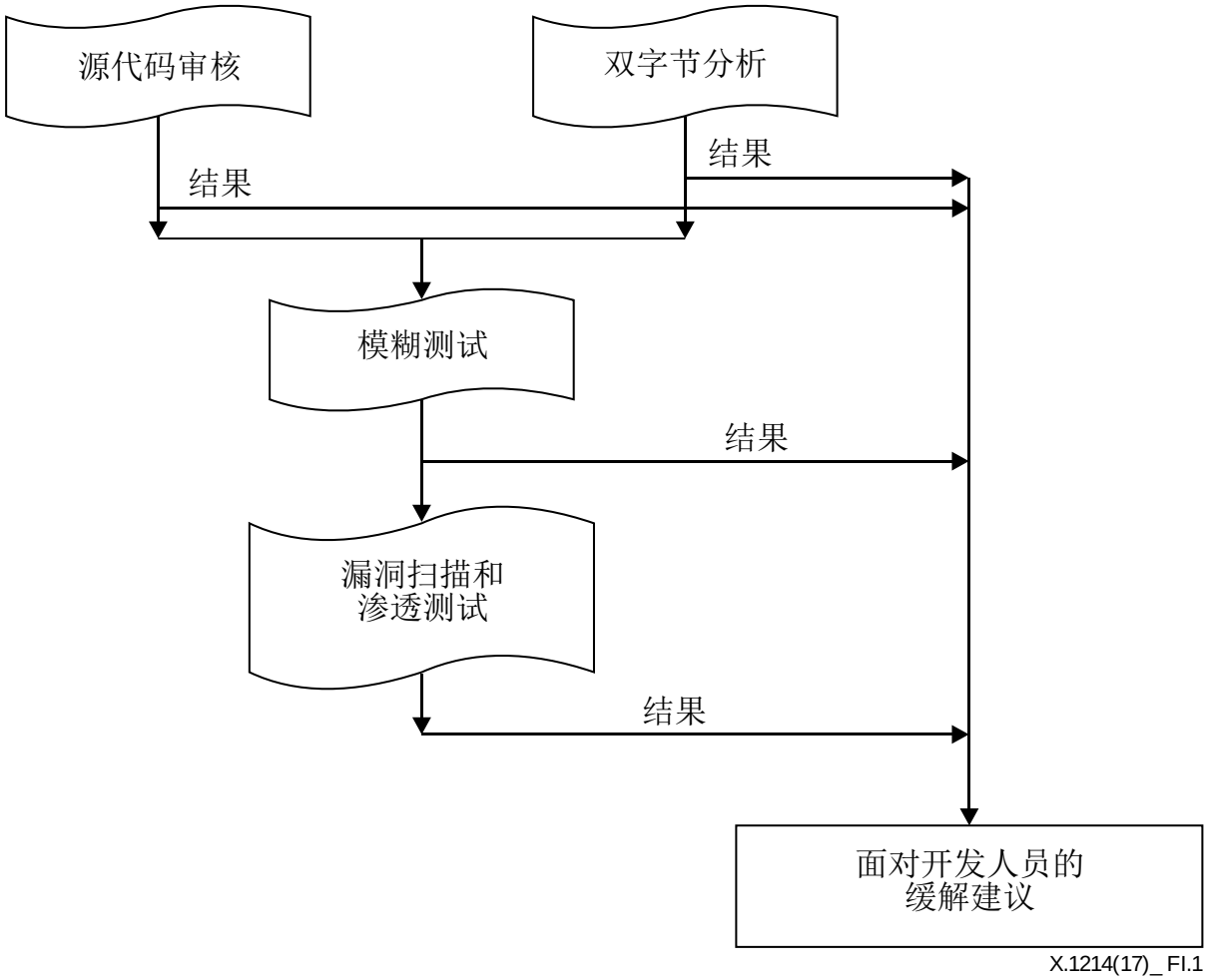
i 第一阶段为预部署阶段，使用所有阐述的安全评定手段进行全面检查，评定的结果应用于缓解所发现的漏洞。

ii 第二阶段为后部署阶段，在此阶段，目标已在网络中投入使用。对此目标实施所有评定手段或许不够现实。因此，网络分析人员可定期凭借漏洞扫描确保产品部署后发现的漏洞能够通过安装补丁定期得到修复。

在预部署阶段，首先，可以对软件元素的源代码进行分析并对所发现的错误予以纠正。之后，这些应用使用的数据库可以通过双字节分析得到处理。在双字节分析后，再进行模糊测试并进入最后阶段，即漏洞扫描和系统的渗透测试。总体评定的结果和发现应发送给相关开发人员，使他们能够为解决所有发现的漏洞采取纠正措施。

在后部署阶段，需要对整个网络需进行定期漏洞扫描。无论何时，一旦发现漏洞，必须予以修复。

描述过程的流程图见图I.1。



图I.1 – 安全评定手段流程图

附录II

其他加强ICT网络安全性的补充手段

（本附录不构成本建议书的组成部分）

本附录提供了进一步加强电信/ICT网络安全的一些手段。

II.1 密码强度评定

基于密码的认证广泛用于各类电信/ICT网络，如配置、管理、操作和维护和服务提供。这些密码的强度须经系统管理员评定，以便确定其不易受到攻击。为此，可进行密码击破。密码击破的机制多种多样，如字典攻击、强力攻击和彩虹表。

II.2 社交保密性评定

在一些情况下，可对机构内员工采取心理操纵以唆使他们泄露保密信息。这项活动称为信心把戏，目的是收集信息、欺诈或系统接入。为评定组织内个人或小组的信誉度可进行社交工程。当机构了解现存风险或感觉某人或某个组丢失的信息可能造成严重影响时可确定具体的目标。

II.3 功能性安全评定

尽管功能性安全评定没有具体的工具，该方法是对第II.1和第II.2节所讨论的各项漏洞检测手段的补充。

任何电信/ICT网络中使用的设备或网络元素都应具备以下安全功能：

i) 对用户配置和管理设备的本地认证；

ii) 对用户配置和管理设备的远程认证；

iii) 设备中安全密码存储；

iv) 安全密钥管理认证；

v) 防止非法软件补丁的设备保护机制；

vi) 设备的远程管理流量保护；

vii) 按照优先或许可情况进行的设备管理用户分类；

viii) 安全时间同步；

ix) 被测设备（DUT）审计（登录）事件生成；

x) DUT安全审计登录出口。

II.4 无线扫描

无线扫描可有助于各机构为缓解无线技术带来的安全风险而采取纠正措施。无线扫描工具应具备扫描国内或国外所有IEEE 802.11 [b-IEEE Std. 8802-11]无线设备的能力。无线扫描可确定扫描软件范围内非授权的无线设备并发现各机构范围外的无线信号，同时检测到可能的后门和安全违规情况。

II.5 使用安全加密模块和算法实施

加密算法用于加密和解密电信和ICT网络安全数据传送所需要的认证数据或用户数据。尽管加密算法设计缜密，实施中的错误却屡见不鲜。如电信/ICT网中部署了具有实施错误的非安全算法，攻击者可利用这些错误，从而导致潜在的重大数据丢失和欺诈入侵活动。因此，电信和ICT网络应使用高度安全的加密模块和算法。

II.6 网络嗅探

网络嗅探是监测网络通信、解码协议和审查标注兴趣信息字头的被动技术手段。该技术手段亦被称为网络监测器或网络分析器，可用于网络或系统管理人员合法的监测并排除网络流量故障。

通过使用网络嗅探技术手段获得的信息，管理人员或安全专家可确定错误包并使用数据发现瓶颈，从而帮助维护网络数据传输的安全性和高效性。

参考资料

[b-IEEE Std. 8802-11] ISO/IEC/IEEE 8802-11:2018(E) – *ISO/IEC/IEEE – International Standard – Information technology –Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*

[b-CVE] CVE Numbering Authorities (1999-2018*). Common vulnerabilities and exposures list.* Mitre Corporation.
https://cve.mitre.org/cve/

ITU-T 系列建议书

A系列　ITU-T工作的组织

D系列　资费和会计原则以及国际电信/ICT经济和政策问题

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　环境与ICT、气候变化、电子废物、节能；线缆和外部设备其他组件的建设、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，以及相关测量和测试

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　电话网络的数据通信

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、下一代网络、物联网和智慧城市

Z系列　电信系统的语言和一般软件问题

瑞士印刷
2018年，日内瓦