ICS 35.020
L 80

中华人民共和国国家标准

GB/T 25068.4—2010/ISO/IEC 18028-4:2005

信息技术　安全技术　IT网络安全 第4部分:远程接入的安全保护

Information technology—Security techniques—IT network security—Part 4:Securing remote access

(ISO/IEC 18028-4:2005,IDT)

2010-09-02 发布　　2011-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 25068 在《信息技术　安全技术　IT 网络安全》总标题下，拟由以下 5 个部分组成：

——第 1 部分：网络安全管理；

——第 2 部分：网络安全体系结构；

——第 3 部分：使用安全网关的网间通信安全保护；

——第 4 部分：远程接入的安全保护；

——第 5 部分：使用虚拟专用网的跨网通信安全保护。

本部分为 GB/T 25068 的第 4 部分。

本部分使用翻译法等同采用国际标准 ISO/IEC 18028-4:2005《信息技术　安全技术　IT 网络安全　第 4 部分：远程接入的安全保护》(英文版)。该国际标准中缺少“规范性引用文件”的章条，为保持与该国际标准编排方式的一致，本部分未添加相应的章条。

本部分更正了部分术语(条款 2.10 中 DHCP 全称中的“Control”更正为“Configuration”；条款 2.28 中 RADIUS 全称中的“Access”更正为“Authentication”；条款 2.43 中 TKIP 全称中的“implementation”更正为“integrity”；条款 7.2.2 中 S/MIME 全称中的“exchange”更正为“extensions”)。

本部分更正了部分错误(附录 E.1 中误表示为“行为”的“删除或关闭不必要的服务和应用”和“配置操作系统用户鉴别”更正为“标题”表示形式；附录 E.3 中的“SSI”更正为“SSL”)。

8.4.3 中“窃听威胁只能用加密与之对抗”中的“只能”过于绝对，修改为“大多”，为今后技术发展预留了空间。

8.7 中增加了使用国家加密标准的规定。

本部分的附录 A、附录 B、附录 C、附录 D、附录 E、附录 F 为资料性附录。

本部分由全国信息安全标准化技术委员会(TC 260)提出并归口。

本部分起草单位：黑龙江省电子信息产品监督检验院、中国电子技术标准化研究所、哈尔滨工程大学、北京励方华业技术有限公司、山东省标准化研究院。

本部分主要起草人：王希忠、黄庶、刘亚东、黄俊强、马遥、方舟、王大萌、树彬、张清江、王智、许玉娜、张国印、李健利、冯亚娜、曲家兴、邱益民、王运福。

引　言

在信息技术领域,在组织内部和组织之间使用网络的需求日益增加。因此,安全使用网络的要求必须得到满足。

在远程接入网络领域要求特定措施时,IT 安全宜得到适当安排。GB/T 25068 的本部分为远程接入网络(或使用电子邮件、文件传输,或只是远程工作)提供指南。

信息技术　安全技术　IT网络安全
第4部分:远程接入的安全保护

1　范围

GB/T 25068的本部分规定了安全使用远程接入(使用公共网络将一台计算机远程连接到另一台计算机或某个网络的方法及其IT安全含义)的安全指南。本部分介绍不同类型的远程接入以及使用的协议,讨论与远程接入相关的鉴别问题,并提供安全建立远程接入时的支持。

本部分适用于那些计划使用这种连接或者已经使用这种连接并且需要其安全建立及安全操作方式建议的网络管理员和技术员。

2　术语和定义

下列术语和定义适用于本部分。

2.1

接入点　Access Point;AP

提供从无线网络接入到地面网络的系统。

2.2

高级加密标准　Advanced Encryption Standard;AES

一种对称加密机制。

注:AES提供可变的密钥长度并允许按美国联邦信息处理标准(FIPS)197的规范有效实现。

2.3

鉴别　authentication

确信实体是其所声称身份的措施。在用户鉴别的情况下,通过所知的东西(例如口令)、拥有的东西(例如令牌)或个人特征(生物特征)识别用户。强鉴别既可以基于强机制(例如生物特征),也可以利用这些因子中至少两个(称为"多因子鉴别")。

2.4

回叫　call-back

一种在收到有效标识符(ID)参数后向预先定义或建议位置(和地址)呼叫的机制。

2.5

挑战—握手鉴别协议　Challenge-Handshake Authentication Protocol;CHAP

一种在RFC1994中定义的3次鉴别协议。

2.6

数据加密标准　Data Encryption Standard;DES

一种众所周知的使用56比特密钥的对称加密机制。因其密钥长度短,DES已被AES取代,但仍在多重加密模式中使用,例如,3DES或三重DES(FIPS 46-3)。

2.7

非军事区　de-militarised zone;DMZ

一种本地网络或站点网络的隔离区,其访问借助防火墙实现的特定策略来控制。DMZ不是内部网络的一部分并被认为不太安全。