<<计算机网络安全技术与应用>>

图书基本信息

书名：<<计算机网络安全技术与应用>>

13位ISBN编号：9787030159373

10位ISBN编号：7030159373

出版时间：2005-9

出版时间：科学出版社

作者：彭新光

页数：319

字数：410000

前言

在高度信息化的21世纪，人们越来越认识到信息教育的重要性。
人们都迫切希望信息教育能有较大发展。
教育信息化也是摆在我们面前的重要任务。
教育部明确要求高等教育实行信息化，要求在未来5年内实现信息化教育课程的数量达到15%～30%。
信息社会离不开计算机技术，知识经济需要大量的计算机高级人才。
我国正在加强计算机的高等教育，正着眼于为新世纪培养高素质的计算机人才，以适应信息社会高速发展的需要。
当前，全国各类高等院校都在各专业基础课程计划中增加计算机的课程内容，而作为与计算机科学密切相关的计算机、通信、信息等专业，更是在酝酿着教学的全面改革，以期规划出一整套面向2l世纪的、具有中国高校计算机教育特色的课程计划和教材体系。
教育部《关于加强高等学校本科教育工作提高教育质量的若干意见》（教字【2001】4号）文件也强调指出：“ 要大力提倡编写、引进和使用先进教材。
教材的质量直接体现着高等教育和科学研究的发展水平，也直接影响本科教学的质量。
高等学校要结合学科、专业的调整，加快教材的更新换代。
”为推动高校教学改革，提高教学质量，我们重点抓了21世纪高等教育教学改革项目，组织并支持了“ 面向21世纪计算机系列教材规划 ”研究课题。
该课题组成员均由高校计算机系的专家教授组成。
他们有多年丰富的教学经验，也具有很强的科研能力。
该课题的主要目标是密切结合国民经济的需要，优化计算机教材体系结构，力求将国际、国内计算机领域的新概念、新理论、新技术吸收到本系列教材中，编写出具有科学性、先进性、系统性、实用性、实践性很强的教材，经过推广使用，反复修改，不断提高。

<<计算机网络安全技术与应用>>

内容概要

本书从计算机网络安全基础理论、工作原理、技术应用和研究前沿多个方面对计算机网络安全技术进行了全面与系统地介绍，内容基本覆盖了当前计算机网络安全领域的核心技术，书中介绍的各种网络安全技术可直接应用于网络安全工程。

本书采用理论、原理、应用和研究为主线的导次知识体系撰写风格，不仅可作为高等院校计算机、通信、信息及电子商务等专业高年级学生或研究生教材，也适用于网络安全技术培训或相关工程技术人员使用。

<<计算机网络安全技术与应用>>

书籍目录

第1章 计算机网络安全概述 1.1 网络安全基本概念 1.1.1 网络安全定义 1.1.2 网络安全目标 1.1.3 网络安全模型 1.1.4 网络安全策略 1.2 网络安全漏洞 1.2.1 软件漏洞 1.2.2 网络协议漏洞 1.2.3 安全管理漏洞 1.2.4 网络威胁来源 1.3 信息安全评价标准 1.3.1 信息安全评价标准简介 1.3.2 美国可信计算机系统评价标准 1.3.3 其他国家信息安全评价标准 1.3.4 国际通用信息安全评价标准 1.3.5 国家信息安全评价标准 1.4 国家信息安全保护制度 1.4.1 信息系统建设和应用制度 1.4.2 信息安全等级保护制度 1.4.3 国际联网备案与媒体进出境制度 1.4.4 安全管理与计算机犯罪报告制度 1.4.5 计算机病毒与有害数据防治制度 1.4.6 安全专用产品销售许可证制度 1.5 本章知识点小结 习题第2章 信息加密技术基础 2.1 信息加密理论基础 2.1.1 信息编码基础知识 2.1.2 数论基础知识 2.1.3 算渚和杂性基础知识 2.2 信息加密方式与标准 2.2.1 信息加密概念 2.2.2 信息加密方式 2.2.3 数据加密标准 2.3 公钥信息加密算法 2.3.1 RSA加密算法 2.3.2 Diffie-Hellman算法 2.3.3 EIGamal加密算法 2.3.4 椭圆曲线加密算法 2.4 信息加密产品简介 2.4.1 PGP加密软件简介 2.4.2 CryptoAPI加密软件简介 2.5 本章知识点小结 习题第3章 身份认证与访问控制 3.1 身份标识与鉴别 3.1.1 身份标识与鉴别概念 3.1.2 身份认证的过程 3.2 口令认证方法 3.2.1 口令管理 3.2.2 脆弱性口令 3.3 生物身份认证 3.3.1 指纹身份认证技术 3.3.2 视网膜身份认证技术 3.3.3 语音身份认证技术 3.4 访问控制 3.4.1 访问控制概念 3.4.2 自主访问控制 3.4.3 强制访问控制 3.5 本章知识点小结 习题第4章 防为墙工作原理及应用 4.1 防火墙简介 4.1.1 防火墙简介 4.1.2 包过滤防火墙 4.1.3 代理服务防火墙 4.1.4 复合防火墙 4.1.5 个人防火墙 ……第5章 网络攻击技术分析第6章 入侵检测系统第7章 计算机病毒防治第8章 安全通信协议第9章 电子邮件系统的安全第10章 无线网络的安全附录 英文缩写对照表参考文献

章节摘录

插图：1.安全策略总则无论是制定总体安全策略，还是制定安全管理实施细则，都应当根据网络安全特点遵守均衡性、时效性和最小限度原则。
（1）均衡性原则由于软件漏洞、协议漏洞、管理漏洞和网络威胁永远不可能消除，网络安全必定是计算机网络的永恒主题。
无论制定多么完善的网络安全策略，还是使用多么先进的网络安全技术，网络安全也只是一个相对概念，因为世上没有绝对的安全系统。
此外，网络易用性和网络效能与安全强度是一对天生的矛盾。
夸大网络安全漏洞和威胁不仅会浪费大量投资，而且会降低网络易用性和网络效能，甚至有可能引入新的不稳定因素和安全隐患。
忽视网络安全比夸大网络安全更加严重，有可能造成机构或国家重大经济损失，甚至威胁到国家安全。
因此，网络安全策略需要在安全需求、易用性、效能和安全成本之间保持相对平衡，科学制定均衡的网络安全策略是提高投资回报和充分发挥网络效能的关键。
（2）时效性原则由于影响网络安全的因素随时间有所变化，导致网络安全问题具有显著的时效性。
例如，网络用户增加、信任关系发生变化、网络规模扩大、新安全漏洞和攻击方法不断暴露都是影响网络安全的重要因素。
因此，网络安全策略必须考虑环境随时间的变化。
（3）最小限度原则网络系统提供的服务越多，安全漏洞和威胁也就越多。
因此，应当关闭网络安全策略中没有规定的网络服务；以最小限度原则配置满足安全策略定义的用户权限；及时删除无用账号和主机信任关系，将威胁网络安全的风险降至最低。

编辑推荐

《计算机网络安全技术与应用》是由科学出版社出版的。

版权说明