

<<网络安全技术及应用>>

图书基本信息

书名：<<网络安全技术及应用>>

13位ISBN编号：9787111259305

10位ISBN编号：7111259300

出版时间：2009-2

出版时间：贾铁军 机械工业出版社 (2009-02出版)

作者：贾铁军 编

页数：386

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## &lt;&lt;网络安全技术及应用&gt;&gt;

## 前言

随着计算机网络技术的快速发展,我国在网络化建设方面取得了令人瞩目的成就。

电子银行、电子商务和电子政务的广泛应用,使计算机网络已经深入到国家的政治、经济、文化和国防建设的各个领域,遍布现代信息化社会工作和生活的各个层面,“数字化经济”和全球电子交易一体化正在形成。

计算机网络安全不仅关系到国计民生,还与国家安全密切相关,不仅涉及国家政治、军事和经济各个方面,而且影响国家的安全和主权。

随着计算机网络的广泛应用和网络之间数据传输量的急剧增大,网络安全的重要性尤为突出。

因此,网络技术中最关键也最容易被忽视的安全问题,正在危及网络的发展和运用,而且已经成为各国关注的焦点,也成为研究热点和人才需求的新领域。

随着信息技术的发展与应用,网络安全的内涵在不断地延伸。

从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性,进而又发展为“攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)”等多方面的基础理论和实施技术。

网络安全是一个综合、交叉学科领域,要综合利用数学、物理、通信和计算机等诸多学科的长期知识积累和最新发展成果,不断发展和完善。

为满足高校应用型人才培养的需要,我们编写了本书。

本书的主要作者20多年来,在高校从事计算机网络与安全等领域的教学、科研和学科专业管理工作,特别是在公安院校多次主持过计算机网络安全方面的科研项目研究,积累了大量宝贵的实践经验。

全书共分12章,重点介绍了计算机网络安全的基本知识、原理及应用技术,主要内容包括:计算机网络安全概述和基本安全问题;网络安全技术的基本概念、内容和方法;网络协议安全、安全体系结构、网络安全管理技术、安全服务与安全机制、无线网安全技术及应用;入侵检测技术、黑客的攻击与防范技术;身份认证与访问控制技术;网络安全中的密码与加密技术;病毒及恶意软件的防护技术;防火墙技术及应用;操作系统与站点安全技术、数据与数据库安全技术;电子商务安全技术及应用等。

书中给出了很多实例,以及作者经过多年的实践总结出来的案例及研究成果。

书中带“\*”部分为选学内容。

本书重点介绍了最新成果、防范技术、处理技术、方法和实际应用。

其特点如下:(1)内容先进,结构新颖。

书中吸收了国内外大量的新知识、新技术、新方法和国际通用准则,注重科学性、先进性、操作性。

(2)注重实用性和特色。

坚持“实用、特色、规范”原则,突出实用及素质能力培养,在内容安排上,通过大量案例将理论知识与实际应用有机结合。

(3)资源配套,便于教学。

为了方便教学,在本书配套的辅助教材《网络安全技术及应用实践教程》中提供了同步实验、学习指导、练习测试等内容,供师生选用。

本书由贾铁军主编、统稿并编写第1-6、11、12章,沈学东任副主编并编写第10章,王小刚编写第7章,王坚编写第8章并完成部分习题解答和课件制作,苏庆刚编写第9章。

叶春明对全书进行了审阅,于森参加了本书大纲的讨论、审校等工作,邹佳芹对全书的文字、图表进行了校对编排并完成了资料查阅等工作,在此一并表示感谢。

同时,感谢对本书编著给予大力支持和帮助的海军工程大学有关领导和同仁。

因作者水平有限,书中难免存在不妥之处,欢迎提出宝贵意见和建议。

## <<网络安全技术及应用>>

### 内容概要

《网络安全技术及应用》突出“实用、新颖、有特色、操作性强”的特点。全书共分12章，主要包括网络安全技术基础知识、网络安全管理技术、黑客攻防与入侵检测技术、身份认证与访问控制技术、密码与加密技术、病毒及恶意软件防护技术、防火墙应用技术、操作系统与站点安全技术、数据库系统安全技术、电子商务安全技术及应用等内容。

《网络安全技术及应用》提供配套的电子教案，并配有辅助教材《网络安全技术及应用实践教程》，内容包括学习指导、实验教学、练习测试和课程设计等。

《网络安全技术及应用》可作为应用型本科院校计算机类、信息类、电子商务类和管理类专业的信息安全相关课程的教材，也可作为培训及参考用书，还可作为高职院校相关专业师生的选修教材。

## 书籍目录

前言第1章 网络安全概论1.1 网络安全概述1.1.1 网络安全的概念及技术特征1.1.2 网络安全的研究目标及内容1.1.3 网络安全的威胁1.2 网络安全风险分析1.2.1 网络系统安全分析1.2.2 操作系统安全分析1.2.3 数据库的安全问题1.2.4 防火墙的局限性1.2.5 管理及其他问题1.3 网络安全模型及保障体系1.3.1 网络安全模型1.3.2 网络信息安全保障体系1.3.3 网络安全关键技术1.3.4 国内外网络安全技术对比1.4 网络安全的法律法规1.4.1 国外的法律法规1.4.2 我国有关的法律法规1.5 安全技术评估标准1.5.1 国外网络安全评估标准1.5.2 国内安全评估通用准则1.6 小结1.7 练习与实践第2章 网络安全技术基础2.1 网络协议安全概述2.1.1 网络协议安全分析2.1.2 网络安全层次结构及安全协议2.2 网络安全体系结构2.2.1 开放系统互连参考模型2.2.2 Internet网络体系层次结构2.2.3 网络安全层次特征体系2.2.4 IPv6的安全性2.3 安全服务与安全机制2.3.1 安全服务的基本类型2.3.2 支持安全服务的基本机制2.3.3 安全服务和安全机制的关系2.3.4 安全服务与网络层次的关系2.4 虚拟专用网(VPN)技术2.4.1 VPN的组成及特点2.4.2 VPN的主要安全技术2.4.3 IPSec概述2.4.4 VPN技术的实际应用2.5 无线局域网安全2.5.1 无线网络安全概述2.5.2 无线VPN安全解决方案2.5.3 无线网络安全技术应用2.6 常用的网络命令2.6.1 ping命令2.6.2 ipconfig命令2.6.3 netstat命令2.6.4 net命令2.6.5 at命令2.7 小结2.8 练习与实践第3章 网络安全管理技术3.1 网络安全管理概述3.1.1 安全管理的概念和内容3.1.2 安全管理的步骤及功能3.1.3 安全管理防护体系3.1.4 网络信息安全政策体系3.2 网络安全管理技术概述3.2.1 网络安全管理技术及结构模型3.2.2 网络管理协议3.2.3 网络安全策略及主机网络防护3.2.4 网络安全管理解决方案3.3 实体安全防护技术3.3.1 实体安全概述3.3.2 主机环境安全要求3.3.3 设备安全管理3.3.4 其他防护措施3.4 小结3.5 练习与实践第4章 黑客攻防与入侵检测4.1 网络黑客概述4.2 黑客攻击的动机及步骤4.2.1 黑客攻击的动机和分类4.2.2 黑客攻击的过程4.3 常用的黑客攻防技术4.3.1 端口扫描攻防4.3.2 网络监听攻防4.3.3 密码破解攻防4.3.4 特洛伊木马攻防4.3.5 缓冲区溢出攻防4.3.6 拒绝服务攻击与防范4.3.7 其他攻防技术4.4 防范攻击的措施4.5 入侵检测系统概述4.5.1 入侵检测系统功能及特点4.5.2 入侵检测系统分类及检测过程4.5.3 常用入侵检测技术4.5.4 不同入侵检测系统的比较4.5.5 入侵检测系统的抗攻击技术4.5.6 入侵检测技术的发展趋势4.6 小结4.7 练习与实践第5章 身份认证与访问控制5.1 身份认证技术概述5.1.1 身份认证的概念5.1.2 身份认证技术方法5.2 登录认证与授权管理5.2.1 双因素安全令牌及认证系统5.2.2 用户登录认证5.2.3 认证授权管理案例5.3 数字签名技术5.3.1 数字签名的概念及功能5.3.2 数字签名的种类5.3.3 数字签名的技术实现方法5.4 访问控制技术5.4.1 访问控制概述5.4.2 访问控制的模式及管理5.4.3 访问控制的安全策略5.4.4 认证服务与访问控制系统5.4.5 准入控制与身份认证管理案例5.5 安全审计技术5.5.1 安全审计概述5.5.2 系统日志审计5.5.3 审计跟踪5.5.4 安全审计的实施5.6 WindowsNT中的访问控制与安全审计5.6.1 WindowsNT中的访问控制5.6.2 WindowsNT中的安全审计5.7 小结5.8 练习与实践第6章 密码与加密技术6.1 密码技术概述6.1.1 密码技术的相关概念6.1.2 密码学与密码体制6.1.3 数据及网络加密方式6.2 密码破译与密钥管理6.2.1 密码破译方法6.2.2 密钥管理6.3 实用加密技术概述6.3.1 对称加密技术6.3.2 非对称加密及单向加密6.3.3 无线网络加密技术6.3.4 实用综合加密方法6.3.5 加密高新技术及发展6.4 数字信封和数字水印6.4.1 数字信封6.4.2 数字水印6.5 小结6.6 练习与实践第7章 数据库系统安全技术7.1 数据库系统安全概述7.1.1 数据库系统的组成7.1.2 数据库系统安全的含义7.1.3 数据库系统的安全性要求7.1.4 数据库系统的安全框架与特性7.2 数据库的数据保护7.2.1 数据库的安全性7.2.2 数据库的完整性7.2.3 数据库并发控制7.3 数据备份与恢复7.3.1 数据备份7.3.2 数据恢复7.4 小结7.5 练习与实践第8章 病毒及恶意软件的防护8.1 计算机病毒概述8.1.1 计算机病毒的概念及发展8.1.2 计算机病毒的分类8.1.3 计算机病毒的特点8.1.4 计算机中毒的异常表现8.2 病毒的组成结构与传播8.2.1 计算机病毒的组成结构8.2.2 计算机病毒的传播8.2.3 计算机病毒的触发与生存8.2.4 特种及新型病毒实例分析8.3 病毒的检测、清除与防范8.3.1 计算机病毒的检测8.3.2 计算机病毒的清除8.3.3 计算机病毒的防范8.3.4 木马的检测、清除与防范8.3.5 病毒和反病毒的发展趋势8.4 恶意软件的查杀和防护8.4.1 恶意软件概述8.4.2 恶意软件的清除8.5 金山毒霸2008概述8.6 小结8.7 练习与实践第9章 防火墙应用技术9.1 防火墙概述9.1.1 防火墙的功能9.1.2 防火墙的特性9.1.3 防火墙的主要缺点9.2 防火墙的类型9.2.1 以防火墙的软硬件形式分类9.2.2 以防火墙技术分类9.2.3 以防火墙体系结构分类9.2.4 防火墙在性能等级上的分类9.3 防火墙的主要应用9.3.1 企业网络体系结构9.3.2 内部防火墙系统应用9.3.3 外围防火墙系统设计9.3.4 用防火墙阻止SYNFlood攻击9.4 小结9.5 习题与实践第10章 操作系统

## &lt;&lt;网络安全技术及应用&gt;&gt;

与站点安全10.1 WindowsVista操作系统的安全10.1.1 WindowsVista系统的安全性10.1.2 WindowsVista系统的安全配置10.2 UNIX操作系统的安全10.2.1 UNIX系统的安全性10.2.2 UNIX系统的安全配置10.3 Linux操作系统的安全10.3.1 Linux系统的安全性10.3.2 Linux系统的安全配置10.4 Web站点的安全10.4.1 Web站点安全概述10.4.2 Web站点的安全策略10.5 系统的恢复技术10.5.1 系统恢复和信息恢复10.5.2 系统恢复的过程10.6 小结10.7 练习与实践第11章 电子商务安全11.1 电子商务安全概述11.1.1 电子商务概述11.1.2 电子商务安全的概念11.1.3 电子商务的安全问题11.1.4 电子商务的安全要素11.1.5 电子商务的安全体系11.2 电子商务的安全技术和标准11.2.1 电子商务的安全技术11.2.2 网上交易安全协议11.2.3 安全电子交易11.3 构建基于SSL的Web安全站点11.3.1 基于Web信息安全通道的构建11.3.2 证书服务的安装与管理11.3.3 web服务器数字证书的获取11.3.4 Web服务器的SSL设置11.3.5 浏览器的SSL设置及访问11.4 电子商务安全解决方案11.4.1 数字证书解决方案11.4.2 电子商务安全技术发展趋势11.5 小结11.6 练习与实践第12章 网络安全解决方案12.1 网络安全方案概述12.1.1 网络安全方案的概念12.1.2 网络安全方案的内容12.2 网络安全方案目标及标准12.2.1 安全方案目标及设计原则12.2.2 评价方案的质量标准12.3 安全方案的要求及任务12.3.1 安全方案要求12.3.2 安全方案的主要任务12.4 安全方案的分析与设计12.4.1 安全方案分析与设计概述12.4.2 安全解决方案案例12.4.3 实施方案与技术支持12.4.4 检测报告与培训12.5 小结12.6 练习与实践附录附录A 练习与实践部分习题参考答案附录B 网络安全相关政策法规网址附录C 常用网络安全相关网站附录D 常用网络安全工具网址参考文献



## 章节摘录

1.4 网络安全的法律法规是网络安全体系的重要保障和基石，由于具体的国内外法律法规比较多，下面仅列出主要内容，其他具体条款和细节可参考本书附录列出的网站进行浏览查询。

1.4.1 国外的法律法规由于网络技术在全球广泛应用的时间并不长，同时发展与更新又非常快，在较短时期内不可能有十分完善的法律体系。

美国和日本是计算机网络技术水平和网络安全比较完善的国家，一些发展中和欠发达国家的相应法律法规还不够完善。

1.打击网络犯罪的国际合作立法20世纪90年代以来，针对利用计算机网络从事刑事犯罪的问题，许多国家都以法律手段打击网络犯罪。

到90年代末，这方面的国际合作也迅速发展起来。

为保障网络安全，着手在刑事领域作出国际间规范的典型是欧洲联盟（简称欧盟）。

欧盟于2000年年初及12月底两次颁布了《网络刑事公约》（草案）。

现在，已有美国、日本等43个国家表示了对这一公约草案的意愿。

在不同国家的刑事立法中，印度的有关做法具有一定代表性。

印度于2000年6月颁布了《信息技术法》，这是一部规范网络世界的基本法。

此外，还有一些国家修订了原有刑法，以适应保障计算机网络安全需要。

例如，美国2000年修订了1986年的《计算机反欺诈与滥用法》，增加了法人犯罪的责任及与印度的《信息技术法》第70条相同的规定等。

2.禁止破解数字化技术保护措施的法律手段1996年12月，世界知识产权组织在两个版权条约中作出了禁止擅自破解他人数字化技术保护措施的规定。

但它并不是版权人的一项权利，而是作为保障网络安全的一项主要内容来规范的。

至今，欧盟、日本、美国等大多数国家都把它作为一种网络安全保护法律。

3.与“入世”有关的网络法律问题1996年12月，联合国第51次大会通过了联合国贸易法委员会的《电子商务示范法》，这部示范法对于网络市场中的数据电文、网上合同成立及生效条件、运输等专项领域的电子商务等，都作了十分具体的规范。

1998年7月新加坡的《电子交易法》出台。

早在1999年12月的世贸组织西雅图外交会议上，确定了对“电子商务”规范的讨论将作为今后会议的一个重要议题。

4.其他有关立法一些发展中国家，除了制定保障网络健康发展的部门法之外，还专门制定了综合性的、原则性的网络基本法。

例如，韩国2000年1月修订的《信息通信网络利用促进法》中就有对“信息网络标准化”以及对成立“韩国信息通信振兴协会”等民间自律组织的规定等。

在印度，则依法成立了“网络事件裁判所”，以解决包括影响网络安全的诸多民事纠纷。

这种机构不是法院的一部分，也不是民间仲裁机构，而是地道的政府机构。

<<网络安全技术及应用>>

编辑推荐

《网络安全技术及应用》是高等院校规划教材·计算机科学与技术系列之一。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>