



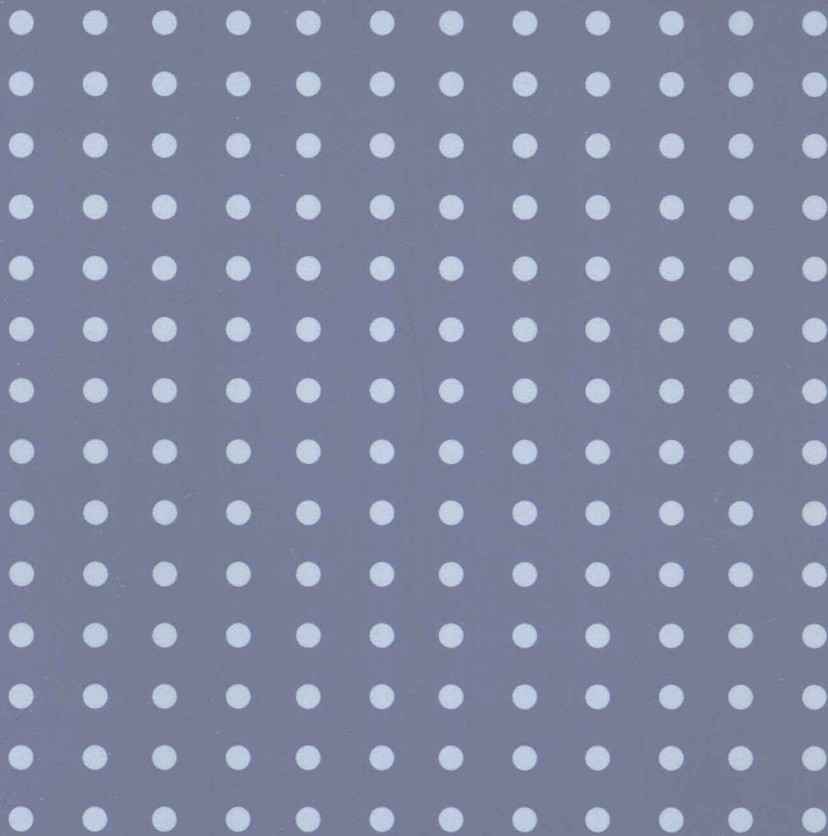
普通高等教育“十一五”国家级规划教材

重点大学计算机专业系列教材

网络与信息安全基础

主 编 周继军 蔡 毅

副主编 苏渭珍 陈 钟 王 颖



清华大学出版社





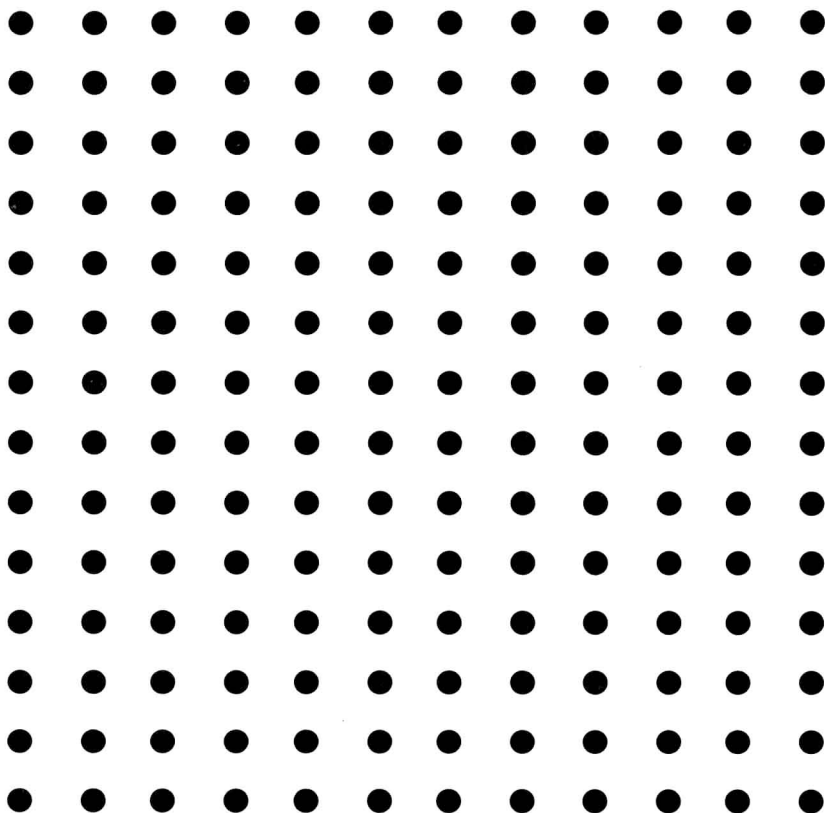
普通高等教育“十一五”国家级规划教材

重点大学计算机专业系列教材

网络与信息安全基础

主 编 周继军 蔡 毅

副主编 苏渭珍 陈 钟 王 颖



清华大学出版社

北京

内 容 简 介

本书全面地介绍了计算机网络安全的情况和发展趋势。全书共分 14 章,内容包括网络安全概述、网络安全与信息加密技术概述、数字签名和认证技术、信息隐藏技术、计算机病毒及防范技术、远程访问技术、数据库安全技术、ASP 和 ASP.NET 的安全技术、电子邮件的安全技术、入侵检测系统技术、网络协议的缺陷和安全技术、网络隔离技术、虚拟专用网络技术和无线网络的安全技术等热门课题的内容。

本书概念准确、内容新颖、图文并茂。既重视基础原理和基本概念的阐述,又紧密联系当前的前沿科技知识,注重理论和实践的有机统一。

本书适用于高等学校计算机相关专业的本科生和专科生,也可以作为培训教材和网络安全技术开发人员的工具书,对电力、金融、交通、电信等部门和相关企事业单位的信息主管及普通工作人员也有一定的参考价值。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

网络与信息安全基础/周继军,蔡毅主编. —北京:清华大学出版社,2008.8

(重点大学计算机专业系列教材)

ISBN 978-7-302-17572-8

I. 网… II. ①周… ②蔡… III. 计算机网络—安全技术—高等学校—教材 IV. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 064375 号

责任编辑:付弘宇 顾 冰

责任校对:时翠兰

责任印制:王秀菊

出版发行:清华大学出版社

地 址:北京清华大学学研大厦 A 座

<http://www.tup.com.cn>

邮 编:100084

社 总 机:010-62770175

邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 装 者:北京鑫海金澳胶印有限公司

经 销:全国新华书店

开 本:185×260 印 张:23.25 字 数:559 千字

版 次:2008 年 8 月第 1 版 印 次:2008 年 8 月第 1 次印刷

印 数:1~4000

定 价:35.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。联系电话:(010)62770177 转 3103 产品编号:021333-01

出版说明

随着国家信息化步伐的加快和高等教育规模的扩大,社会对计算机专业人才的需求不仅体现在数量的增加上,而且体现在质量要求的提高上,培养具有研究和实践能力的高层次的计算机专业人才已成为许多重点大学计算机专业教育的主要目标。目前,我国共有16个国家重点学科、20个博士点一级学科、28个博士点二级学科集中在教育部部属重点大学,这些高校在计算机教学和科研方面具有一定优势,并且大多以国际著名大学计算机教育为参照系,具有系统完善的教学课程体系、教学实验体系、教学质量保证体系和人才培养评估体系等综合体系,形成了培养一流人才的教学和科研环境。

重点大学计算机学科的教学与科研氛围是培养一流计算机人才的基础,其中专业教材的使用和建设则是这种氛围的重要组成部分,一批具有学科方向特色优势的计算机专业教材作为各重点大学的重点建设项目成果得到肯定。为了展示和发扬各重点大学在计算机专业教育上的优势,特别是专业教材建设上的优势,同时配合各重点大学的计算机学科建设和专业课程教学需要,在教育部相关教学指导委员会专家的建议和各重点大学的大力支持下,清华大学出版社规划并出版本系列教材。本系列教材的建设旨在“汇聚学科精英、引领学科建设、培育专业英才”,同时以教材示范各重点大学的优秀教学理念、教学方法、教学手段和教学内容等。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

1. 面向学科发展的前沿,适应当前社会对计算机专业高级人才的培养需求。教材内容以基本理论为基础,反映基本理论和原理的综合应用,重视实践和应用环节。

2. 反映教学需要,促进教学发展。教材要能适应多样化的教学需要,正确把握教学内容和课程体系的改革方向。在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养,为学生知识、能力、素质协调发展创造条件。

3. 实施精品战略,突出重点,保证质量。规划教材建设的重点依然是专业基础课和专业主干课;特别注意选择并安排了一部分原来基础比较好的优秀教材或讲义修订再版,逐步形成精品教材;提倡并鼓励编写体现重点大学

计算机专业教学内容和课程体系改革成果的教材。

4. 主张一纲多本,合理配套。专业基础课和专业主干课教材要配套,同一门课程可以有多个具有不同内容特点的教材。处理好教材统一性与多样化的关系;基本教材与辅助教材以及教学参考书的关系;文字教材与软件教材的关系,实现教材系列资源配套。

5. 依靠专家,择优落实。在制订教材规划时要依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时,要引入竞争机制,通过申报、评审确定主编。书稿完成后要认真实行审稿程序,确保出书质量。

繁荣教材出版事业,提高教材质量的关键是教师。建立一支高水平的以老带新的教材编写队伍才能保证教材的编写质量,希望有志于教材建设的教师能够加入到我们的编写队伍中来。

教材编委会

前言

随着计算机的迅速发展,各大院校都开设了计算机专业,报考计算机专业的学生也越来越多。但是,当学生们离开学校,面临就业和工作的时候,就会发现他们在校学习的一些专业知识有可能已经过时了,而且离实际工作需要存在不小的差距。

造成这种局面的原因有两个方面,一方面,有些学校的计算机教材更新速度比较缓慢,课堂讲授的还是 BASIC 语言、C 语言等基础课程,而新技术的课程几乎没有,陈旧的知识自然引不起学生学习的兴趣。另一方面,学生受到社会上浮躁、急功近利等风气的影响,对基础知识的学习兴趣不大,总想接触实际有用的东西。

编写这本教材的目的就是向学习计算机专业的学生介绍当前比较热门的网络安全技术,同时通过图例和动手实验,提高计算机专业学生的动手实践能力。

网络技术的飞速发展使得新的网络技术和标准不断问世。本书并没有长篇累牍地讲解基本原理,而是总结性地介绍了相关的理论知识,并把容易混淆的知识进行了比较。

本书在保证内容丰富的前提下,注重理论与实际的结合,每章都有课后习题帮助读者复习和巩固所学的内容,并启发读者思考。

本书有配套的实验教材《网络与信息安全基础实验教程》,除第 1 章“网络安全概述”外,其他各章都设计了对应的实验,以便于学生在学完基础理论后,通过动手实验来加深对知识的理解。

本书的编写得到了北京亿中邮信息技术有限公司白玥、高琛工程师的大力支持。华为 3COM 技术有限公司的季勇军、陈旭工程师对本书的初稿提出了很多宝贵意见。北京联信永益科技有限公司的沈虹工程师和深信服电子科技有限公司华北区的官俊东工程师也为本书提供了很多有价值的建议。另外,解放军信息工程大学的王颖硕士也参加了本书的部分编写工作。对此笔者表示诚挚的谢意。

2006 年,本书已入选“十一五”国家级规划教材。在此笔者要感谢北京大

学信息科学与技术学院的领导和清华大学出版社在规划、编写和出版中的大力支持和帮助。

由于时间仓促,加上编者水平有限,书中难免还存在一些缺点甚至错误,恳请广大读者和专家批评指正。读者在本书及课件等相关资源的使用中遇到任何问题或有何建议,请发邮件至: fuhy@tup.tsinghua.edu.cn。欢迎读者与我们进行交流,帮助我们提高编写质量。

编 者

2008年2月

目录

第 1 章 网络安全概述	1
1.1 为什么要重视网络安全	1
1.1.1 网络安全的现状	1
1.1.2 加强青少年的网络安全意识	2
1.2 什么是攻击	2
1.2.1 收集信息的主要方式	2
1.2.2 攻击的主要手段	3
1.2.3 入侵的常用策略	5
1.2.4 攻击对象排名	6
1.3 入侵层次分析	6
1.4 设置安全的网络环境	8
1.4.1 关于口令安全性	8
1.4.2 局域网安全	9
1.4.3 广域网安全	10
1.4.4 制订安全策略	11
1.5 安全操作系统简介	11
1.6 网络管理员的素质要求	12
1.7 校园网络的安全	13
1.7.1 校园网安全特点	13
1.7.2 校园网安全的隐患	14
1.7.3 校园网安全重点在于管理	15
习题	16
第 2 章 网络安全与信息加密技术浅析	17
2.1 加密技术概述	17
2.1.1 加密技术的起源	17
2.1.2 加密的理由	18

2.1.3	数据安全的组成	19
2.1.4	信息安全的体系结构	19
2.1.5	密码的分类	19
2.2	数据加密	20
2.2.1	数据加密技术	21
2.2.2	数据加密算法	23
2.3	加密技术的发展	27
2.3.1	密码专用芯片集成	27
2.3.2	量子加密技术的研究	27
2.4	加密技术的应用	28
2.4.1	加密技术在电子商务方面的应用	28
2.4.2	加密技术在 VPN 中的应用	28
2.5	基于双钥技术的现代加密方法	29
2.5.1	双钥技术工作原理分析	29
2.5.2	公共密钥加密系统的优点	30
	习题	30
第 3 章	数字签名和认证技术	31
3.1	数字证书简介	31
3.1.1	证书介绍	31
3.1.2	Windows 证书存储	34
3.1.3	证书用途	35
3.1.4	Authenticode 技术	40
3.2	SSL 的工作原理	40
3.3	SSL 基本结构的集中管理	41
3.3.1	SSL 的实施	41
3.3.2	Web 服务器组的局限性	42
3.3.3	将 SSL 和 BIG-IP 进行整合	43
3.4	用 SSL 安全协议实现 Web 服务器的安全性	44
3.5	SSL 的安全漏洞及解决方案	45
3.5.1	SSL 易受到的攻击	46
3.5.2	SSL 针对攻击的对策	47
	习题	49
第 4 章	信息隐藏技术	50
4.1	信息隐藏技术概述	50
4.1.1	信息隐藏技术的发展	50
4.1.2	信息隐藏模型	51
4.1.3	信息隐藏的特点	52

4.2	数字水印技术	52
4.3	信息隐藏技术的应用	54
4.3.1	数字内容保护	54
4.3.2	隐蔽通信	55
4.3.3	安全监测	56
4.4	隐秘通信技术	57
4.4.1	基本原理	57
4.4.2	隐秘通信研究现状	59
4.4.3	基于网络协议的隐秘通信	61
4.4.4	基于阙下信道的隐秘通信	64
4.4.5	常用音频视频隐写技术	65
4.5	信息隐藏应用软件	72
4.5.1	JSteg 软件	72
4.5.2	JPHide&Seek	74
4.5.3	S-Tools	75
4.5.4	Steganos Security Suite 2006	78
	习题	82
第 5 章	计算机病毒及防范技术	83
5.1	病毒的起源和发展	83
5.2	病毒的定义及分类	86
5.2.1	病毒的定义	86
5.2.2	病毒的分类	86
5.3	VBS 病毒的起源与发展及其危害	88
5.3.1	VBS 的运行基础	88
5.3.2	VBS 病毒的发展和危害	88
5.3.3	VBS 病毒的原理及其传播方式	89
5.4	共享蠕虫的原理及用 VB 编程的实现方法	92
5.4.1	了解蠕虫病毒	92
5.4.2	编写一个蠕虫病毒	96
5.5	缓冲区溢出与病毒攻击的原理	98
5.5.1	缓冲区溢出	98
5.5.2	缓冲区溢出的根源在于编程错误	99
5.5.3	缓冲区溢出导致“黑客”病毒横行	99
5.6	木马程序	99
5.6.1	木马程序的发展历程	100
5.6.2	木马程序的隐藏技术	100
5.6.3	木马程序的自加载运行技术	101
5.6.4	通过查看开放端口判断木马或其他黑客程序的方法	103

5.7 计算机日常使用的安全建议	106
习题	106
第 6 章 远程访问技术	107
6.1 常见远程连接的方法	107
6.1.1 利用拨号技术来实现远程连接	107
6.1.2 利用 VPN 实现远程连接	108
6.1.3 无线远程连接	110
6.2 远程访问技术和支持遇到的问题	111
6.3 使用 Windows 2000 操作系统实现远程访问服务	111
6.3.1 Windows 2003 服务器端设置	112
6.3.2 客户端设置	115
6.4 Windows 2000 远程控制的三种安全解决方法	118
6.4.1 Windows 2000 终端服务结合 Zebedee 软件的使用	118
6.4.2 在 SSH 上使用 VNC 软件	120
6.4.3 VPN 技术应用在 Windows 2000 远程控制	120
6.5 Windows XP 系统中的远程控制	121
6.5.1 Windows XP 远程协助的应用	121
6.5.2 Windows XP “远程桌面”的应用	122
6.5.3 远程桌面与终端服务的区别和联系	127
6.6 Windows XP 远程控制的安全机制	127
6.7 SSL VPN 将成为远程访问技术的主流	131
习题	131
第 7 章 数据库安全技术	132
7.1 数据库安全简介	132
7.1.1 数据库的安全问题	132
7.1.2 容易忽略的数据库安全	133
7.2 SQL 数据库的安全规划	135
7.2.1 SQL 数据库简介	135
7.2.2 SQL 数据库的安全规划	136
7.3 管理 SQL Server 的安全性	138
7.3.1 SQL Server 标准登录模式	139
7.3.2 SQL Server 集成登录模式	140
7.3.3 使用 Enterprise Manager 建立登录账号	140
7.3.4 管理 SQL Server 用户	141
7.3.5 管理 SQL Server 角色	142
7.3.6 管理 SQL Server 许可	146
7.4 针对 SQL Server 的攻击与防护	148

7.5	SQL 数据库的备份	151
7.6	SQL 数据库的还原	152
	习题	155
第 8 章	ASP 和 ASP.NET 的安全技术	156
8.1	ASP 和 ASP.NET 技术概述	156
8.1.1	ASP 工作原理	156
8.1.2	ASP 的安全特点	157
8.1.3	IIS 6.0 与早期版本的区别	158
8.2	对 IIS Web Server 进行 DoS 攻击	161
8.3	MS ODBC 数据库连接溢出导致 NT/9x 拒绝服务攻击	163
8.4	ASP 安全建议	164
8.4.1	以 Windows NT 的安全机制为基础	164
8.4.2	利用 IIS 安全机制	168
8.5	提高 IIS 5.0 的执行效率	174
8.5.1	启用 HTTP 的持续作用	174
8.5.2	不启用日志	175
8.5.3	设定非独立的处理程序	175
8.5.4	调整缓存数量	175
8.5.5	不使用 CGI 程序	176
8.5.6	增加 IIS 5.0 服务器的 CPU 数量	176
8.5.7	不启用 ASP 检错功能	176
8.5.8	静态网页采用 HTTP 压缩	177
8.6	自定义 IIS 安全策略	177
8.6.1	防止数据库注入攻击	177
8.6.2	主页自动恢复程序	178
8.6.3	定时打开或关闭 IIS 服务器目录	179
	习题	181
第 9 章	电子邮件的安全技术	182
9.1	邮件服务器软件的现状	182
9.1.1	邮件安全成为重中之重	182
9.1.2	邮件的组件与协作	183
9.1.3	邮件的存档	183
9.2	邮件服务器的发展趋势	183
9.2.1	Web 邮件技术	184
9.2.2	多域邮件服务	184
9.2.3	Linux 邮件服务器	184
9.2.4	安全防护	184

9.2.5	多语言	184
9.2.6	远程监控和性能调整	184
9.2.7	无限可扩展能力	184
9.3	电子邮件服务器的安全性分析	185
9.3.1	邮件服务器的工作原理	185
9.3.2	邮件服务器安全性分析	185
9.3.3	邮件服务器安全解决方案	187
9.4	反垃圾邮件技术解析	190
9.4.1	什么是垃圾邮件	190
9.4.2	安全问题	191
9.4.3	反垃圾邮件技术	191
9.5	邮件服务器的比较	199
9.5.1	Postfix 的特点	199
9.5.2	Qmail 的特点	200
9.5.3	Sendmail 与 Qmail 的比较	200
9.5.4	Exchange Server	202
	习题	204
第 10 章	入侵检测系统技术	205
10.1	入侵检测系统简介	205
10.1.1	入侵检测系统的发展	205
10.1.2	IDS 的定义	206
10.1.3	入侵检测系统模型	207
10.1.4	IDS 监测位置	208
10.1.5	入侵检测技术	209
10.1.6	信息收集	210
10.1.7	IDS 信号分析	211
10.2	IDS 的分类	212
10.2.1	根据检测原理分类	212
10.2.2	根据体系结构分类	215
10.2.3	根据输入数据特征分类	216
10.3	IDS 的体系结构	216
10.3.1	数据收集机制	216
10.3.2	数据分析机制	217
10.3.3	缩短数据收集与数据分析的距离	218
10.4	入侵检测系统面临的三大挑战	218
10.4.1	如何提高系统的检测速度	218
10.4.2	如何减少系统的漏报和误报	218
10.4.3	如何提高系统的互动性能	218

10.5	IDS 的误报、误警与安全管理	219
10.5.1	IDS 误报的典型情况	219
10.5.2	解决误报和误警问题的对策	219
10.6	入侵检测系统的弱点和局限	220
10.6.1	网络局限	220
10.6.2	检测方法的局限性	222
10.6.3	资源及处理能力局限	224
10.6.4	NIDS 相关系统的脆弱性	225
10.6.5	HIDS 的弱点和局限	225
10.6.6	NIDS 和 HIDS 的比较	226
10.7	IDS 展望	227
10.8	基于免疫学的 IDS	228
	习题	228
第 11 章	网络协议的缺陷和安全技术	230
11.1	TCP/IP 概述	230
11.1.1	TCP/IP 的特点	230
11.1.2	OSI 数据通信模型	231
11.1.3	TCP/IP 协议结构	231
11.2	数据传输概述	236
11.2.1	寻址、路由选择和多路复用	236
11.2.2	IP 地址	237
11.2.3	子网	238
11.2.4	Internet 的路由结构	239
11.2.5	路由器	239
11.2.6	路由表	239
11.2.7	地址转换	240
11.2.8	协议、端口和套接字接口	241
11.3	ARP 协议的缺陷及其在操作系统中的表现	242
11.3.1	网络设备的通信过程及 ARP 协议的工作原理	242
11.3.2	ARP 协议的缺陷及其在常见操作系统中的表现	243
11.4	DoS 攻击原理以及常见方法介绍	244
11.4.1	深入了解 TCP 协议	244
11.4.2	服务器的缓冲区队列	245
11.4.3	“拒绝服务”如何实现攻击	246
11.4.4	DDoS 攻击	247
11.5	DoS 攻击软件介绍	248
11.5.1	死亡之 ping	248
11.5.2	Smurf	248

11.5.3	Fraggle 攻击	249
11.5.4	OOB Nuke	250
11.5.5	Land 攻击	250
11.5.6	Teardrop 攻击	250
11.5.7	UDP Flood	251
11.5.8	分布式反射拒绝服务	252
习题		252
第 12 章	网络隔离技术	253
12.1	防火墙概述	253
12.1.1	什么是防火墙	253
12.1.2	防火墙的发展	254
12.1.3	防火墙能做什么	254
12.1.4	防火墙的种类	255
12.2	分布式防火墙	258
12.2.1	分布式防火墙的结构	258
12.2.2	分布式防火墙的特点	259
12.2.3	分布式防火墙的优势	260
12.2.4	分布式防火墙的分类	261
12.3	物理隔离技术	262
12.3.1	物理隔离技术的发展	262
12.3.2	国内网络现状及物理隔离要求	262
12.3.3	物理隔离卡的类型及比较	263
12.4	网闸在网络安全中的应用	264
12.4.1	网闸概述	264
12.4.2	网闸的概念	264
12.4.3	网闸工作原理	265
12.4.4	网闸的应用定位	266
12.4.5	网闸的应用领域	266
12.5	防水墙技术	267
12.5.1	防水墙的体系结构	267
12.5.2	防水墙系统设计理念	267
12.6	UTM 技术发展和现状	268
12.6.1	UTM 的起源和概述	268
12.6.2	UTM 的技术特点和优势	269
12.6.3	用户的使用现状	269
12.6.4	UTM 发展趋势	269
12.7	2003 年全球网络安全设备市场现状与特点	271
12.7.1	市场现状	271

12.7.2	市场特点	271
12.7.3	重点国家和地区网络安全设备市场发展概述	271
12.8	2003年中国网络安全设备市场规模与结构	272
12.8.1	市场规模与增长	272
12.8.2	产品结构	273
12.8.3	市场结构	274
12.8.4	市场特征	279
	习题	280
第13章	虚拟专用网络技术	281
13.1	VPN技术简介	281
13.1.1	VPN基本连接方式	282
13.1.2	VPN的基本要求	283
13.2	实现VPN的隧道技术	284
13.2.1	隧道技术列举	284
13.2.2	隧道技术的实现方式	285
13.2.3	隧道协议和基本隧道要求	285
13.3	VPN隧道协议及技术对比	286
13.3.1	点对点协议	286
13.3.2	点对点隧道协议	288
13.3.3	L2F协议	289
13.3.4	L2TP协议	289
13.3.5	IPSec隧道技术	290
13.3.6	SSL虚拟专网的新发展	293
13.3.7	IPSec VPN和MPLS VPN之比较	294
13.4	实现VPN的安全技术	296
13.4.1	认证技术	296
13.4.2	加密技术	296
13.4.3	密钥交换和管理	296
13.5	VPN组网方式	297
13.5.1	Access VPN: 客户端到网关	297
13.5.2	Intranet VPN: 网关到网关	297
13.5.3	Extranet VPN: 与合作伙伴企业网构成外联网	298
13.6	VPN技术的优缺点	299
13.7	VPN面临的安全问题	300
13.7.1	IKE协议并不十分安全	300
13.7.2	部署VPN时的安全问题	300
13.8	实现VPN的QoS技术	301
13.9	在路由器上配置VPN	302

13.10	软件 VPN 与硬件 VPN 的比较	303
13.11	Sinfor DLAN 产品简介	303
13.11.1	网络环境准备	305
13.11.2	安装环境准备	306
13.12	VPN 网络自建还是外包	306
13.12.1	大型企业自建 VPN	307
13.12.2	中小型企业外包 VPN	307
13.13	VPN 的发展趋势	307
	习题	308
第 14 章	无线网络的安全技术	309
14.1	无线网络概述	309
14.1.1	无线网络的发展	309
14.1.2	无线局域网的优点	310
14.1.3	无线局域网技术	310
14.1.4	无线通信技术比较	313
14.2	无线网络的分类	321
14.2.1	根据网络解决方案分类	322
14.2.2	根据连接方式分类	322
14.3	无线网络的安全	323
14.3.1	无线局域网的安全威胁	323
14.3.2	无线局域网的安全技术	323
14.3.3	无线局域网的安全策略	334
	习题	335
附录 A	与计算机网络安全相关的法律条文	336
附录 B	习题答案	338
参考文献	346