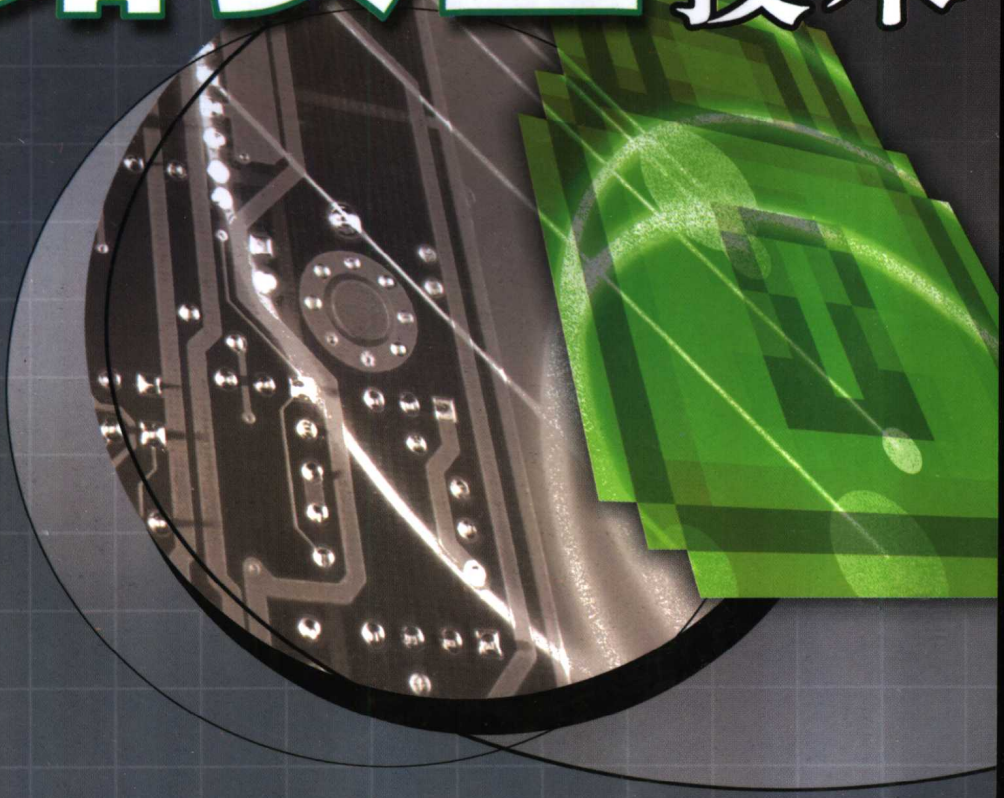
网络安全理论与技术



杨义先　钮心忻　编著

人民邮电出版社
POSTS & TELECOM PRESS

网络安全理论与技术

杨义先　钮心忻　编著

人民邮电出版社

图书在版编目(CIP)数据

网络安全理论与技术/杨义先，钮心忻编著. —北京：人民邮电出版社，2003.10
ISBN 7-115-11557-5

Ⅰ.网… Ⅱ. ①杨… ②钮… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2003）第 075105 号

网络安全理论与技术

◆ 编　　著　杨义先　钮心忻
责任编辑　陈万寿

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www. ptpress.com.cn
读者热线　010-67129258
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：38
字数：922 千字　　2003 年 10 月第 1 版
印数：1-4 000 册　　2003 年 10 月北京第 1 次印刷

ISBN 7-115-11557-5/TN・2151

定价：59.00 元

本书如有印装质量问题，请与本社联系 电话：（010）67129223

内 容 提 要

本书从理论和技术两个方面对网络信息安全的相关知识进行全面和系统介绍。本书是作者及北京邮电大学信息安全中心近十年来的科研成果的总结，书中大部分内容在国内外同类书籍中较为少见，不少还是首次出现，其体系架构、描述方式和材料取舍都充分考虑了我国现阶段信息化进程的特色。

全书共分四篇，分别介绍网络安全概论、安全网管、安全支付和安全通信。全书内容覆盖了信息安全保障体系、操作系统与安全、网络系统与安全、数据库系统与安全、防火墙、入侵检测、安全协议、安全网管、电子支付、电子现金、安全微支付、网络银行、安全固网电信系统、安全移动通信系统、安全短信系统、安全邮件系统等网络信息安全理论与技术方面的主要内容。

本书可作为高等学校信息安全、密码学、信息与计算科学、通信与信息系统、信号与信息处理、应用数学、控制理论与控制技术、模式识别与智能系统、计算机系统结构、计算机软件与理论、计算机应用技术、军事通信学、软件工程等专业的研究生和高年级学生的教学参考书，也可作为相关领域科技工作者的实用工具书或技术培训教材。另外，书中介绍的许多算法、协议、方案等都可以直接应用于工程实践，书中提出的许多理论问题也有助于激发更多的后继研究。

序

网络技术是双刃剑，一方面它正在而且还将更广泛和深刻地改变传统的生产、经营、管理和生活方式，成为新的经济增长点和先进文化的重要传播工具；另一方面，信息网络国际化、社会化、开放化、个人化的特点，使国家的“信息边界”防不胜防，对网络使用的依赖性越强，网络安全和信息安全稍有不慎，后果越严重。目前国际上围绕信息的获取、使用和控制的竞争愈演愈烈，网络信息安全在维护国家安全、保持社会稳定、保障经济发展、保护个人隐私方面起的作用日益突显，网络信息安全保障能力已经成为21世纪综合国力、经济竞争实力和生存与发展能力的重要标志，同时，网络信息安全技术也已成为新世纪世界各国争相攀登的制高点。

网络信息安全是一门技术交叉的学科，它综合利用了数学、物理、生物、通信技术和计算机技术等诸多学科的基础理论和最新发展成果。网络信息安全又是一门发展迅速的年轻学科，网络信息安全领域“攻”与“防”的高智商对抗不断丰富着网络信息安全技术。网络信息安全还是一门社会科学与工程管理学科，它涉及战略、法律、政策、管理、产业和人才培养的各个方面，其应用渗透到政治、经济、科技、文化和军事等诸多领域，构筑国家网络安全保障体系是一项艰巨复杂的系统工程。显然，如果没有长期深入的研究和实践就不可能全面系统地论述网络信息安全的理论与技术。

《网络安全理论与技术》一书是杨义先教授及其领导的北京邮电大学信息安全中心积近十年的科研成果磨成的一“剑”，从理论、技术、管理、法规等层次对网络信息安全相关知识进行了全面而深入的阐述，既详细阐述基础理论，又充分介绍最新进展，在深入论述专项技术的同时兼顾系统全局性。本书选材和对技术的评价得当，反映了作者对信息安全在通信网络中定位的准确把握，也体现了作者对网络信息安全技术发展的辩证战略眼光，更值得称道的是给读者留下不少思考空间，书中提出的许多理论与实践问题有助于激发更多的后继研究。书中大部分内容在国内外同类书籍中较为少见，不少还是首次出现，其体系架构、描述方式和材料取舍都充分考虑了我国现阶段信息化进程的时代特色。本书还反映了作者对尽快构建一个技术先进、管理高效、安全可靠、自主产权的国家网络安全保障体系的一些新颖见解。本书结构清晰，各篇相对独立又能相互呼应，文字通顺，使枯燥的网络信息安全问题读来饶有趣味。《网络安全理论与技术》堪称一本难得的好书，既是应时之作，又有收藏价值。

邬贺铨

中国工程院院士，中国工程院副院长
国家信息化专家咨询委员会委员

此为试读，需要完整PDF请访问：www.ertongbook.com

作 者 简 介

杨义先，1983 年 7 月毕业于成都电讯工程学院应用数学专业，1986 年 7 月获北京邮电学院应用数学专业硕士学位，1988 年 12 月获北京邮电大学电子与通信系统专业博士学位。1992 年 10 月至今任北京邮电大学教授，首届长江学者特聘教授。1993 年至今任北京邮电大学信息安全专业博士生导师。从事信息安全、信号与信息处理、密码学专业的教学、科研和成果转化工作。已发表论文 300 余篇，出版著作 10 余部。作者与本书相关研究成果曾获 1991 年国家教委科技进步奖二等奖、1991 年国家级有突出贡献的中青年专家称号、1991 年国家级有突出贡献的中国博士学位获得者、1991 年首届政府特殊津贴获得者、1992 年邮电部科技进步奖一等奖、1997 年国家教委科技进步奖二等奖、1997 年军队科技进步奖二等奖、1997 年邮电部科技进步奖一等奖。

钮心忻，1997 年毕业于香港中文大学电子工程系，获博士学位。现为北京邮电大学信息安全中心副教授，从事网络信息安全、软件无线电、信号与信息处理等方面的科研和教学工作。已经在包括 IEEE Trans. on AES 等在内的国内外著名学术刊物上发表论文 30 余篇，完成专著数部，作为项目负责人承担了多项国家级和省部级科研项目，并于 1999 年获信息产业部科技进步奖三等奖。

前　言

作为到目前为止国内外内容最为丰富的网络安全专著，本书将系统而深入地描述以网络安全概论、安全网管、安全支付、安全通信等为代表的网络安全主流理论与技术。但是，我们仍然感到书中内容还有遗缺，网络安全所涉及的内容实在太多，永远无法穷尽。下面简述我们对网络安全的几点粗浅认识，供广大读者朋友参考，不当之处欢迎读者批评指正。

网络安全需要辩证法。网络安全是一门高智商的对抗性学科，作为矛盾主体的“攻”与“守”双方，始终处于“成功”和“失败”的轮回变化之中，没有永远的胜利者，也不会有永远的失败者。“攻”与“守”双方当前争斗的暂时动态平衡体现了网络安全的现状，而“攻”与“守”双方的“后劲”则决定了网络安全今后的走向。“攻”与“守”双方既相互矛盾又相互统一，他们始终都处于互相促进、循环往复的状态之中。更具体地说，安全是相对的，不安全才是绝对的，用户不应轻易被商家所宣传的“绝对安全的完整解决方案”之类的神话所迷惑，同时，用户也不应该一劳永逸地呆在自己曾经建设的安全网络之中，必须随时对网络进行安全维护和更新。

网络安全需要它山石。作为一门直接由社会需求所推动的新学科，网络安全正随着社会需求的不断丰富、不断变化而迅速发展，因此，网络安全不能孤立于其他已经成熟的任何学科，必须充分吸收其他学科的营养以适应自己的快速成长。既然，以孙子兵法为代表的军事理论已经在现代“商战”中被广泛应用，而且取得了突出成就，那么，它们为什么不能够在现代“网战”中发挥应有的作用呢？许多用户始终愿意错误地相信“有安全措施总是比没有安全措施强，即使这些安全措施并不可靠”，但是，他们却忘记了“备周则意怠”这一千古兵训。到目前为止，虽然没有人有意识地将兵法战术引入网络安全的研究之中，但是，现在网络安全中的许多思想和技术的确与兵书中的许多计策不谋而合，比如，逃避入侵检测的渐近攻击法就基于“常见而不疑”的思想；新出现的信息隐藏技术就是典型的“瞒天过海”；黑客们调用别人的计算机资源发动的分布式拒绝服务攻击与“借刀杀人”如出一辙；“攻”、“守”双方的许多新技巧都是“出奇制胜”的典范；对付黑客的蜜罐技术难道不是“李代桃僵”吗？我们希望在不远的将来，人们能够有意识地将军事理论引入网络安全研究之中，为此建立全新而实用的网络安全理论与技术。

网络安全需要生力军。到目前为止，研究网络安全的主力军主要来自信息技术等领域的自然科学工作者。首先，应该肯定这些科研人员经过自己的艰苦努力已经取得了若干杰出成就，但是，与其他学科相比，网络安全的涉及面实在太广，需要太多的知识背景和想象力，比如，军事学家当然更擅长于建立网络安全对抗理论，从而使得网络安全能够在完整的理论体系指导下健康地发展；法律专家能够通过公正的法律体系限制众多的攻击行为，从而净化网络环境，减少网络安全的压力；教育学家可以通过提高全民素质来提高“网民”的道德水准，从而形成全民抗“黑”的有利之“势”；经济学家可以通过分析“攻”与“守”双方的当前成本开销来客观现实地为网络安全定位；管理专家能够通过有效的管理事半功倍地实现网

络安全目标等等。总之，网络安全应该是目标而不只是手段，无论用什么方法，只要能够达到网络安全的目的，就应该肯定。

网络安全需要服务观。如果把网络比喻为“红花”，那么安全就是“绿叶”。如果把网络比喻为“主角”，那么安全就是“配角”，虽然这个配角显得异常重要和不可获缺。网络安全是服务，是一种特殊的核心服务，网络安全的提供者和使用者都应该对此有清醒的认识。作为网络安全的科研人员，应该紧紧围绕网络的具体安全需求展开其科研工作，为了科研而进行的科研在此会显得毫无价值，当然，随时注意总结科研经验，提炼相关理论并用于指导后续研究仍然是十分重要的。为了提供良好的服务，网络安全的科研人员就必须对被服务对象有相当的了解，这就要求网络安全的科研人员必须具有相当宽广的知识基础，比如，很难想象不懂移动通信的人员能够为移动通信提供良好的安全服务。作为网络安全系统的用户对安全服务也要把握好适当的“度”，忽略安全的作法不可取，不计代价求安全的做法也不对。网络安全需要的东西还有许多，这里不再赘述。

在本书的写作过程中，我们一方面注意密切结合我国社会信息化的当前具体情况，另一方面也尽量体现我们对网络安全的上述几点认识，如果这些做法能够起到抛砖引玉的作用，我们就十分满意了。

本书的各篇、各章（甚至各节）都尽量相对独立，以适应各种需求之读者自由组合并阅读相关章节。比如，信息安全专业的研究生（包括博士生）或高年级本科生可以从头到尾认真阅读此书的全部内容，这样可以使他们对网络安全有一个比较全面系统的认识，为今后的进一步深造打下基础；密码学专业的研究生和高年级本科生可以重点阅读第一篇等有关内容；网络安全的工程技术人员可以集中学习第一篇和第二篇等有关内容；对通信领域的新型安全问题感兴趣的读者可以研读第一篇、第二篇、第四篇等有关内容；对关心电子商务安全的人员可以阅读第一篇、第三篇等有关内容。本书所列的详细章节目录可以帮助读者迅速了解每一章节的主题，并据此迅速找到自己关心的内容。

本书还附有相当详细的参考文献目录，希望如此众多的参考文献能够帮助那些有特殊兴趣的读者直接进入自己的专业领域并了解国际上的相关领域的最新动态。

本书是北京邮电大学信息安全中心全体成员多年来集体智慧的结晶。在本书写作过程中李中献博士、冯运波博士、夏光升博士、张振涛博士、李新博士、曾志峰博士、李鸿培博士、徐国爱博士、陈明奇博士、吴秋新博士、钟鸣博士、岳军巧博士、李志江博士、伊丽江博士、李明柱博士、白剑博士、张胜博士、朱红儒硕士、卢翔宇硕士、李志兵硕士、丘天豪硕士、李琛硕士、庄严硕士、王慰硕士、张小芬硕士等为本书提供了丰富的资料。特别感谢胡正名教授、温巧燕教授、罗守山教授、牛少彰教授、卓新建副教授、李梦东副教授。他们同心协力，率领北京邮电大学信息安全中心百余位研究人员对网络信息安全研究的丰富成果是本书的营养源泉。本书也是国家“863”项目（编号：2002AA143041）、国家“973”项目(编号：G1999035804)、国家自然科学基金项目(批准号：60073049，90204017)，以及国防科技保密通信重点实验室基金项目（51436060101DZ0801）的成果总结。

由于作者水平有限，书中难免出现各种失误和不当之处，欢迎大家批评指正。

作　者

目　录

第一篇　网络安全概论

第 1 章　信息安全保障体系 …… 3
1.1　深层防御 …… 3
1.1.1　健全法制 …… 3
1.1.2　加强管理 …… 5
1.1.3　完善技术 …… 9
1.1.4　培养人才 …… 15
1.2　全面保障 …… 16
1.2.1　PDRR 模型 …… 16
1.2.2　基础设施 …… 19
1.2.3　计算环境 …… 23
1.2.4　区域边界 …… 26
1.3　安全工程 …… 34
1.3.1　发掘需求 …… 35
1.3.2　构建系统 …… 36
1.3.3　检测评估 …… 38
1.3.4　风险管理 …… 39
1.4　技术对策 …… 40
1.4.1　知己知彼 …… 40
1.4.2　安全服务 …… 42
1.4.3　弹性策略 …… 45
1.4.4　互动策略 …… 47
第 2 章　操作系统与安全 …… 48
2.1　UNIX 与安全 …… 49
2.1.1　系统用户命令的安全问题 …… 49
2.1.2　系统用户安全要点 …… 52
2.1.3　系统管理员命令的安全问题 …… 53
2.1.4　系统管理员安全要点 …… 56
2.2　X Window 与安全 …… 58
2.2.1　为什么会出现 X Window 安全问题 …… 58
2.2.2　X Window 系统实用工具与安全问题 …… 60

2.2.3 如何提高 X Window 的安全性 …… 62
2.2.4 X 系统的几个容易被忽略的漏洞 …… 64
2.3 Windows NT 与安全 …… 65
2.3.1 Windows NT 安全简介 …… 65
2.3.2 Windows NT 环境的设置 …… 67
2.3.3 Windows NT 的安全模型 …… 70
2.3.4 Windows 95/98 的安全性 …… 72
2.4 Linux 与安全 …… 72
2.4.1 Linux 体系结构 …… 72
2.4.2 Linux 网络接口 …… 73
2.4.3 Linux 的安全问题 …… 77
2.4.4 基于 Linux 的 IPSec 模型 …… 78
第 3 章 网络系统与安全 …… 81
3.1 计算机网络基础 …… 81
3.1.1 计算机网络的过去 …… 81
3.1.2 计算机网络的现在 …… 82
3.1.3 计算机网络的分类 …… 85
3.1.4 计算机网络存取控制方法 …… 88
3.2 开放系统的参考模型及其安全体系结构 …… 89
3.2.1 开放系统互连及参考模型 …… 90
3.2.2 开放系统参考模型分层的原则和优点 …… 91
3.2.3 ISO/OSI 对安全性的一般描述 …… 92
3.2.4 Novell NetWare 结构组成和安全体系结构 …… 93
3.3 网络中常见的攻击手段 …… 94
3.3.1 信息收集 …… 95
3.3.2 口令攻击 …… 96
3.3.3 攻击路由器 …… 96
3.3.4 攻击 TCP/IP …… 97
3.3.5 利用系统接收 IP 数据包的漏洞 …… 98
3.3.6 电子邮件攻击 …… 99
3.3.7 拒绝服务攻击 …… 99
3.4 常用网络服务的安全问题 …… 101
3.4.1 FTP 文件传输的安全问题 …… 101
3.4.2 Telnet 的安全问题 …… 101
3.4.3 WWW 服务的安全问题 …… 101
3.4.4 电子邮件的安全问题 …… 102
3.4.5 Usenet 新闻的安全问题 …… 102
3.4.6 DNS 服务的安全问题 …… 102
3.4.7 网络管理服务的安全问题 …… 102

3.4.8 网络文件系统的安全问题 …… 103
第4章 数据库系统与安全 …… 104
4.1 数据库系统基础 …… 104
4.1.1 数据库系统概念 …… 104
4.1.2 管理信息系统 …… 105
4.1.3 关系数据库 …… 109
4.1.4 数据库管理系统的体系结构 …… 112
4.2 数据库系统的安全 …… 116
4.2.1 数据库的安全策略 …… 116
4.2.2 数据库加密 …… 117
4.2.3 数据库的安全性要求 …… 121
4.2.4 安全数据库的设计原则 …… 123
4.3 Web 数据库的安全 …… 124
4.3.1 Web 与 HTTP 协议的安全 …… 124
4.3.2 CGI 程序的安全 …… 126
4.3.3 Java 与 JavaScript 的安全 …… 128
4.3.4 ActiveX 的安全 …… 129
4.3.5 Cookie 的安全 …… 130
4.4 Oracle 数据库的安全 …… 131
4.4.1 Oracle 数据库安全功能概述 …… 131
4.4.2 Oracle 数据库的安全管理方法 …… 131
4.4.3 Oracle 数据库的并发控制 …… 134

第二篇 安 全 网 管

第5章 防火墙 …… 139
5.1 防火墙技术概论 …… 139
5.1.1 防火墙的优缺点 …… 139
5.1.2 防火墙的包过滤技术 …… 141
5.1.3 防火墙的应用层网络技术（代理技术） …… 146
5.1.4 防火墙的电路级网关技术 …… 148
5.1.5 防火墙的状态检查技术 …… 150
5.1.6 防火墙的地址翻译技术 …… 150
5.1.7 防火墙的其他相关技术 …… 151
5.2 防火墙的体系结构 …… 152
5.2.1 包过滤型防火墙 …… 152
5.2.2 双宿主机型防火墙 …… 154
5.2.3 屏蔽主机型防火墙 …… 155
5.2.4 屏蔽子网型防火墙 …… 156

此为试读，需要完整PDF请访问：www.ertongbook.com

5.2.5 其他防火墙体系结构 …… 157
5.3 防火墙过滤规则的优化 …… 157
5.3.1 基于统计分析的动态过滤规则优化 …… 157
5.3.2 基于统计分析的自适应动态过滤规则优化 …… 160
5.3.3 基于统计分析的动态过滤规则分段优化 …… 161
5.3.4 具有安全检查特性的基于统计分析的动态过滤规则优化 …… 162
5.3.5 防火墙过滤规则动态优化的性能分析与仿真 …… 165
5.4 基于操作系统内核的包过滤防火墙系统的设计与实现 …… 168
5.4.1 预备知识 …… 168
5.4.2 基于 Windows 9x 的 NDIS 内核模式驱动程序的实现 …… 170
5.4.3 基于 Windows NT 的 NDIS 内核模式驱动程序的实现 …… 171
5.5 PC 防火墙的研究与实现 …… 173
5.5.1 问题的提出 …… 173
5.5.2 PC 的安全问题 …… 173
5.5.3 PC 防火墙及其功能需求 …… 174
5.5.4 PC 防火墙的一种实现方案 …… 175
第 6 章 入侵检测 …… 182
6.1 基础知识 …… 182
6.1.1 历史沿革与基本概念 …… 182
6.1.2 入侵检测系统的体系结构 …… 185
6.1.3 基于知识和行为的入侵检测 …… 189
6.1.4 入侵检测系统的信息源 …… 193
6.2 入侵检测标准 …… 197
6.2.1 入侵检测数据交换标准化 …… 197
6.2.2 通用入侵检测框架 …… 199
6.2.3 入侵检测数据交换格式 …… 204
6.2.4 通用入侵检测框架的语言 …… 206
6.3 入侵检测系统模型 …… 209
6.3.1 基于系统行为分类的检测模型 …… 209
6.3.2 面向数据处理的检测模型 …… 211
6.3.3 入侵检测系统和算法的性能分析 …… 212
6.3.4 入侵检测系统的机制协作 …… 214
6.4 基于进程行为的入侵检测 …… 217
6.4.1 基于神经网络的行为分类器 …… 218
6.4.2 基于概率统计的贝叶斯分类器 …… 220
6.4.3 基于进程行为分类器的入侵检测 …… 222
6.4.4 基于进程检测器的入侵检测系统原型 …… 225
第 7 章 安全协议 …… 226
7.1 IPSec 协议 …… 226

7.1.1 IPSec 体系结构 …… 227
7.1.2 IPSec 的实现途径 …… 236
7.1.3 IPSec 安全性分析 …… 238
7.1.4 一种新的分层 IPSec 体系结构 …… 245
7.2 密钥交换协议 …… 255
7.2.1 ISAKMP 的消息构建方式 …… 255
7.2.2 ISAKMP 的载荷类型 …… 256
7.2.3 安全联盟的协商 …… 256
7.2.4 建立 ISAKMP SA …… 257
7.2.5 IKE 的消息交换流程 …… 259
7.3 多方安全协议 …… 263
7.3.1 (*t*,*n*) 门限方案 …… 263
7.3.2 Pinch 在线机密分享方案及其弱点分析 …… 264
7.3.3 单一信息广播的安全协议 …… 268
7.3.4 多个信息广播的安全协议 …… 269
7.4 公平电子合同 …… 270
7.4.1 背景知识 …… 270
7.4.2 两方公平电子合同 …… 271
7.4.3 多方公平电子合同 …… 274
第 8 章 安全网管 …… 278
8.1 安全网管系统架构 …… 278
8.1.1 多层次安全防护 …… 278
8.1.2 安全网管系统 …… 279
8.1.3 系统部署 …… 280
8.1.4 功能特点 …… 281
8.2 网络控制代理 …… 281
8.2.1 网络控制代理的总体设计 …… 281
8.2.2 netfilter 架构 …… 282
8.2.3 攻击防范 …… 284
8.2.4 功能模块 …… 285
8.3 网络检测代理 …… 286
8.3.1 网络检测代理的总体设计 …… 286
8.3.2 网络数据的收集 …… 287
8.3.3 检测的方法、机制、策略和流程 …… 288
8.3.4 功能模块 …… 291
8.4 主机安全代理 …… 292
8.4.1 主机安全代理的总体设计 …… 292
8.4.2 虚拟设备驱动程序技术 …… 294
8.4.3 主要功能的实现 …… 295

8.4.4 功能模块 …… 297
8.5 管理中心 …… 299
8.5.1 功能和需求分析 …… 299
8.5.2 模块组成 …… 299
8.6 系统自身安全 …… 301
8.6.1 对付攻击 …… 301
8.6.2 安全通信 …… 302
8.6.3 设计原则 …… 305
8.6.4 应用示例 …… 306

第三篇 安 全 支 付

第9章 电子支付 …… 311
9.1 安全电子交易 …… 311
9.1.1 电子支付系统模型 …… 311
9.1.2 数字货币 …… 316
9.1.3 电子支付系统（EPS） …… 317
9.1.4 电子数据交换 …… 318
9.1.5 通用电子支付系统（UEPS） …… 319
9.2 无匿名性的电子支付系统 …… 320
9.2.1 First Virtual …… 320
9.2.2 O-card …… 322
9.2.3 iKP …… 323
9.2.4 SET …… 324
9.3 无条件匿名性的电子支付系统 …… 328
9.3.1 匿名需求 …… 328
9.3.2 盲签名技术 …… 329
9.3.3 Ecash …… 333
9.3.4 Brands …… 334
9.4 匿名性受控的电子支付系统 …… 336
9.4.1 公平盲签名 …… 337
9.4.2 公平的离线电子现金系统 …… 338
9.4.3 一种在线的公平支付系统 …… 340
9.4.4 基于可信方标记的电子现金系统 …… 342
9.4.5 NetCash …… 343
第10章 电子现金 …… 345
10.1 基础知识 …… 345
10.1.1 历史与现状 …… 345
10.1.2 电子现金的基本流程 …… 349

10.1.3 电子现金的特点 …… 350
10.1.4 电子现金关键技术 …… 350
10.2 基于零知识证明的电子现金模型 …… 350
10.2.1 基本概念及协议 …… 351
10.2.2 零知识证明简介 …… 353
10.2.3 基于零知识证明的电子现金模型 …… 354
10.2.4 基于 RSA 盲签名与二次剩余的电子现金方案 …… 358
10.3 比特承诺及其应用 …… 361
10.3.1 高效比特承诺方案 …… 362
10.3.2 基于比特承诺的身份认证方案 …… 365
10.3.3 基于比特承诺的部分盲签名方案 …… 367
10.3.4 基于部分盲签名的电子现金 …… 371
10.4 高效电子现金方案设计 …… 375
10.4.1 高效可分电子现金方案 …… 375
10.4.2 单项可分电子现金方案 …… 381
第 11 章 安全微支付 …… 386
11.1 微支付机制 …… 386
11.1.1 基于公钥机制的微支付系统 …… 387
11.1.2 基于宏支付的微支付系统 …… 388
11.1.3 基于共享密钥机制的微支付系统 …… 389
11.1.4 基于散列链的微支付系统 …… 392
11.1.5 基于概率机制的微支付系统 …… 395
11.1.6 基于散列冲突的微支付系统 …… 397
11.2 基于散列链的微支付系统 …… 398
11.2.1 基于 PayWord 的 WWW 微支付模型 …… 398
11.2.2 基于散列链的防欺诈微支付系统 …… 402
11.3 分布式环境中的微支付系统 …… 406
11.3.1 分布式微支付协议 …… 406
11.3.2 基于微支付的反垃圾邮件机制 …… 409
11.4 微支付在无线环境中的应用 …… 415
11.4.1 移动增值服务支付 …… 415
11.4.2 微支付在移动增值服务认证和支付中的应用 …… 416
11.4.3 微支付在移动 IP 认证和支付中的应用 …… 418
第 12 章 网络银行 …… 425
12.1 网络银行概述 …… 425
12.1.1 网络银行的发展 …… 425
12.1.2 网络银行的实现方式 …… 426
12.1.3 网络银行的安全性需求 …… 429
12.1.4 网络银行的结构与功能 …… 430

12.2 基于电子支票的网络银行 …… 431
12.2.1 基于对称密码体制的电子支票 …… 431
12.2.2 CNOS 多签名体制 …… 434
12.2.3 基于 CNOS 多签名的电子支票 …… 438
12.3 基于电子现金的网络银行 …… 441
12.3.1 性能要求 …… 441
12.3.2 不可追踪性与盲签名 …… 442
12.3.3 基于 OSS 的盲签名体制 …… 445
12.4 网络银行实例 …… 448
12.4.1 网络银行软件结构 …… 448
12.4.2 网络银行安全机制 …… 450
12.4.3 安全网络证券交易系统 …… 453

第四篇 安 全 通 信

第 13 章 安全固定网电信系统 …… 459
13.1 电话防火墙 …… 460
13.1.1 单机电话防火墙概述 …… 460
13.1.2 单机电话防火墙的关键技术 …… 461
13.1.3 小型交换机防火墙 …… 463
13.2 联机防火墙的单片机设计与实现 …… 465
13.2.1 ATMEL AT90S4433 单片机及其开发系统 …… 465
13.2.2 联机电话防火墙的功能 …… 468
13.2.3 联机电话防火墙的原理及其实现 …… 469
13.3 电信固定网虚拟专网 …… 471
13.3.1 电信固定网 VPN 的体系结构 …… 471
13.3.2 一种基于 DSP 的电信固定网 VPN（替音电话） …… 472
13.3.3 替音电话算法的仿真结果 …… 476
13.4 电信固定网入侵检测 …… 483
13.4.1 电信固定网的常见攻击手段 …… 484
13.4.2 电话盗用攻击的检测 …… 485
13.4.3 搭线窃听攻击的检测 …… 487
第 14 章 安全移动通信系统 …… 489
14.1 GSM 安全机制 …… 489
14.1.1 移动通信面临的安全威胁 …… 489
14.1.2 GSM 系统的安全机制 …… 490
14.1.3 GSM 系统的安全缺陷 …… 492
14.2 GPRS 安全机制 …… 492
14.2.1 GPRS 系统的网络结构 …… 492

14.2.2 GPRS 系统的安全机制 …… 493
14.2.3 GPRS 系统的安全缺陷 …… 495
14.3 3G 安全机制 …… 496
14.3.1 安全结构 …… 497
14.3.2 网络接入安全机制 …… 499
14.3.3 接入链路数据完整性 …… 503
14.3.4 接入链路数据保密性 …… 504
14.3.5 密钥管理 …… 506
第 15 章 安全短信系统 …… 511
15.1 短消息服务与安全需求 …… 511
15.1.1 短消息服务的系统结构 …… 511
15.1.2 短消息服务的安全需求与现状 …… 512
15.1.3 SIM 卡执行环境 …… 513
15.2 基于短消息的移动电子商务安全协议 …… 515
15.2.1 基于短消息的移动电子商务安全需求 …… 515
15.2.2 基于短消息的身份认证协议 …… 516
15.2.3 移动电子商务的反拒认协议 …… 522
15.3 基于 SIM 卡的电子支付协议 …… 530
15.3.1 设计目的 …… 530
15.3.2 协议内容 …… 531
15.3.3 协议分析 …… 542
15.4 短消息应用系统实例 …… 543
15.4.1 业务简介 …… 543
15.4.2 系统结构 …… 543
15.4.3 应用系统的实现 …… 544
第 16 章 安全邮件系统 …… 550
16.1 电子邮件系统简介 …… 550
16.1.1 电子邮件系统的收发机制 …… 550
16.1.2 电子邮件的一般格式 …… 551
16.2 电子邮件系统的安全问题 …… 552
16.2.1 电子邮件的安全需求 …… 552
16.2.2 基于应用层的安全电子邮件 …… 553
16.2.3 基于网络层的安全电子邮件 …… 553
16.3 安全电子邮件系统实例 …… 554
16.3.1 IP 包的检测流程 …… 554
16.3.2 IP 包传送的不对称性 …… 555
16.3.3 TCP 段的重传机制 …… 556
16.3.4 加密后的 IP 包数据的编码问题 …… 557
16.3.5 E-mail 发送失败的一个例子 …… 557

此为试读,需要完整PDF请访问: www.ertongbook.com