

□ 信息安全系列丛书

计算机 网络安全的 理论与实践

(第2版)

【美】王杰

Computer Network Security
Theory and Practice

□ 信息安全系列丛书

计算机 网络安全的 理论与实践

(第2版)

【美】王杰

Computer Network Security
Theory and Practice

JISUANJI WANGLUO ANQUAN
DE LILUN YU SHIJIAN

 高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

图书在版编目(CIP)数据

计算机网络安全理论与实践/(美)王杰编著.—2版.—北京:高等教育出版社,2011.6

ISBN 978-7-04-031798-5

I. ①计… II. ①王… III. ①计算机网络-安全技术 IV. ①TP393.08

中国版本图书馆CIP数据核字(2011)第083745号

策划编辑 刘英 责任编辑 刘英 封面设计 张雨薇 版式设计 范晓红
责任校对 金辉 责任印制 张泽业

出版发行	高等教育出版社	网 址	http://www.hep.edu.cn
社 址	北京市西城区德外大街4号		http://www.hep.com.cn
邮政编码	100120	网上订购	http://www.landaco.com
印 刷	三河市华润印刷有限公司		http://www.landaco.com.cn
开 本	787×1092 1/16	版 次	2006年10月第1版
印 张	24.25		2011年6月第2版
字 数	500 000	印 次	2011年6月第1次印刷
购书热线	010-58581118	定 价	49.00元
咨询电话	400-810-0598		

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换
版权所有 侵权必究
物 料 号 31798-00

第 2 版前言

本书第 2 版是在第 1 版和英文版的基础上修订和补充而成的。它在保持第 1 版的结构和指导思想下增加了以下内容：彩虹表及其在字典攻击中的应用，RC4 序列密码安全性讨论，中国余数定理及其在证明 RSA 算法正确性的应用，漩涡散列函数，OCB 操作模式，无线网状网安全问题，Linux 操作系统中的防火墙设置，微软 Windows 便携式执行格式病毒传播原理及第二代万维网技术的一些安全问题，行为分析入侵检测技术和 Honeynet 计划。第 2 版还充实了第 1 版中的部分章节，包括电子邮件安全协议、无线局域网安全协议和无线个人网安全协议。为便于自学，第 2 版在书后还给出了部分习题的解答。此外，第 2 版对某些英语名词的翻译作了一些修改，比如 phishing 在第 1 版译为钓取，而译为网络钓鱼更为贴切。

第 2 版共分九章。

第 1 章介绍网络安全的概貌。首先讨论网络安全的任务，综述常见的网络攻击类型和防范措施，然后讨论攻击者的分类及定义网络安全模型。

第 2 章介绍对称密钥加密算法和密钥生成算法。首先讨论加密算法的设计要求，介绍 Feistel 分组密码结构，DES 和 AES 标准分组密码加密算法，RC4 序列密码加密算法和讨论它们的完全性，然后介绍分组密码使用模式及密钥生成算法。

第 3 章介绍公钥密码体系和密钥管理方法。首先讨论公钥密码体系的指导思想，介绍 Diffie-Hellman 密钥交换体系，RSA 公钥密码体系和椭圆曲线公钥密码体系，然后介绍密钥传递和管理方法。

第 4 章介绍数据认证方法。首先讨论安全散列函数的设计要求，介绍散列函数结构，SHA-512 散列函数，漩涡散列函数，信息认证代码算法，HMAC 算法模式，OCB 操作模式和生日攻击，然后介绍数字签名标准，双签名协议和盲签协议。

第 5 章介绍常用的网络安全协议。首先讨论在网络体系各层配置密码算法的优缺点，介绍公钥基础设施，然后介绍网络层 IPsec 协议、传输层 SSL/TLS 协议、应用层电子邮件安全协议、Kerberos 身份认证协议及安全外壳协议。

第 6 章介绍设置在数据链路层的无线网安全协议。首先介绍无线局域网体系结构,有线隐私等价协议的安全问题和改进后的网络安全存取协议,然后介绍无线个人网蓝牙安全协议,并讨论无线网际网的安全问题。

第 7 章介绍网络周边安全体系。首先讨论防火墙的设计思想,介绍网络层数据包过滤、传输层线路网关、应用层代理服务器和堡垒主机等防火墙技术,然后介绍防火墙设置方案,网址转换技术和在 Linux 操作系统中设置防火墙的基本方法。

第 8 章介绍抗恶意软件的技术。首先讨论计算机病毒和病毒分类,介绍病毒、蠕虫和特洛伊木马传播原理,然后介绍服务阻断攻击,万维网安全性及抗恶意软件方法。

第 9 章介绍入侵检测技术。首先讨论入侵检测的基本思想,介绍网检系统、机检系统、混合系统、特征检测、行为分析和数据挖掘等检测技术,然后介绍诱饵体系。

附录 A 给出部分习题的解答,并特别在第 6 章的习题解答中介绍了一个如何破译无线局域网 WEP 安全协议加密算法的方法,并给出了程序的源代码。

第 2 版的结构与英文版基本相同。英文版的写作得到许多同行的建议和帮助,特别是 Gordan College 的 Stephen Brinton 教授审阅了英文版初稿的第 1~5 章和第 7~8 章,麻省大学罗威尔分校陈冠岭教授审阅了第 6 章,付新文教授提供了不少相关资料和建议,美国银行 (Bank of America) 网络安全工程师 Jared Karro 审阅了全部章节, Worcester Polytechnic Institute 楼文菁教授审阅了第 1~2 章和第 6 章。麻省大学罗威尔分校部分博士研究生和硕士研究生亦对英文版和中文第 2 版的写作提供了帮助,他们是 (按英文和拼音姓氏为序): Anthony Kolodziej、Blake Skinner、Bora Seng、David Einstein、Hengky Susanto、Jeff Brown、Karen Uttecht、Michael Court、Nathaniel Tuck、Ryan Buckley、William Brown、杜春燕、方正、侯强、李楠、李优、刘忠丽、潘炯、杨杰、袁旭。此外, Stephen Brinton、方正、潘炯、杨杰协助提供了习题解答。作者谨在此致以诚挚的谢意。

感谢高等教育出版社编辑刘英博士对本书的编辑加工。

作者在 2008 年秋季和 2009 年秋季用本书英文版给本系研究生讲授计算机网络安全课程,授课用的 PPT 幻灯片可在 <http://www.cs.uml.edu/~wang/NetSec> 网页上找到。

作者在授课的基础上对本书作了进一步修订。尽管如此,本书不妥之处在所难免,恳请读者及采用本书的教师发现错误后通知作者。来信和建议请寄至作者的电子信箱: wang@cs.uml.edu。

王杰 (J. Wang), 美国麻省大学罗威尔分校

2011 年 1 月

第 1 版前言

网络安全是计算机科学的新分支，也是信息产业的新领域。它的产生源于网络通信的保密需要，它的发展得益于人们为应对侵犯网络通信和连网计算机系统的各种攻击所做出的锲而不舍的努力。随着互联网应用的深入和普及，如何不断地采取更有效的安全措施保护网络通信内容不被窃取、篡改和伪造以及保护连网计算机系统免受侵扰已变得至关重要。除军事和金融通信以外，网络安全如今已成为电子商务、信息管理及资源共享等领域不可缺少的工具和保障，因而也越来越受到政府、商业及家庭计算机用户的重视。毫无疑问，网络安全将继续成为计算机科学研究与应用中一个举足轻重的领域。

互联网是在有线电话网的基础上发展起来的，由于当初在设计互联网通信协议时忽视了安全因素，导致互联网通信存在许多本来可以避免的缺陷和漏洞。为了解决互联网技术中的一系列问题，包括网络安全问题，美国国家科学基金会已号召研究人员探索和开发新一代互联网技术，研究互联网如果从零开始，应该有怎样的体系结构才能更好地适应今后的发展并解决现有的网络安全问题。无论结果如何，维护网络安全的努力将是持续不断的，原因包括以下几点：第一，旧的网络安全机制可能由于计算理论的进展、计算机性能的提高或新技术的产生而不再有效。第二，旧的网络安全问题解决之后，新的网络安全问题又将不断出现。第三，新的应用可能需要新的安全措施加以保护。比如近年来出现的网络安全攻击，特别是对大型企业计算机系统的攻击，已从几年前用蠕虫和服务阻断所进行的撒网式攻击变成更具针对性的攻击了。

经过多年的努力，特别是最近十几年的研究与实践，网络安全已逐渐形成了一些成熟的理论和有效的方法。学习这些理论与方法将为今后研究网络安全和开发安全系统打下良好的基础，同时也为系统安全管理提供牢靠的依据。因此，网络安全已成为美国各大学计算机科学系本科生与研究生的主要课程。中国的大学近年来也开始逐渐重视网络与信息安全的教学。

本书主要围绕着两条主线展开。第一条主线是以计算机密码学为根基而建立起来的各种安全协议和相应的工业化标准,它以加密算法和网络安全协议设计为主导。第二条主线是为弥补通信协议缺陷和系统漏洞而发展出来的防火墙、抗恶意软件和入侵检测等技术,它以网络设置和管理为主导。网络安全的这两条主线相辅相成,缺一不可。遗憾的是,现有的网络安全教材基本上围绕网络安全的第一条主线展开的。围绕第二条主线展开的书则通常是面向系统管理人员而编写的,不太适合作为教材使用。本书是为弥补这一缺陷所做的一点尝试,其宗旨是以较短的篇幅向读者深入浅出、系统地介绍计算机网络安全理论与实践的主要研究成果和发展动向,使读者在一个学期的学时之内既学到理论知识又学到实用的安全技术。由于篇幅的限制,本书在不影响全局的条件下放弃了一些内容。一本书只能做一本书的事,愿本书能达到预期目标。

本书作为教材,其对象是高等院校修过计算机网络课程的高年级本科生和一年级研究生。本书亦可作为计算机工作者和系统管理人员的参考书或自修读物。

本书对专用英语名词的汉语翻译尽量与大众习惯保持一致,同时也参考了中国台湾和海外华人社团的一些用法。有些名词的汉语翻译虽然有待斟酌,但却已经被广泛使用,故不便改动。如果某个名词存在多种流行译法,本书将尽量采用意译的方法。如互联网也称为因特网或网际网,因特网是音译,网际网是直译,互联网是意译,本书采用互联网这一译法。又如网络协议层次结构的底层有物理层和实体层两种译法,物理层是直译,实体层是意译,本书采用实体层这一译法。为了方便读者阅读,书后附有专用名词汉英对照表。

本书在介绍加密算法时涉及数论及离散概率里的一些熟知的概念和定理,自学的读者如果对算法不予深究可省略这些内容。本书的一部分练习具有一定难度,需要读者有一定的系统编程经验,包括二进制数操作和二进制文件存取及编写网络应用程序的经验。后者主要是指建立在 TCP/IP 通信协议上的套接字编程。这些练习是为以本书为教材的计算机科学系和计算机工程系的学生而设计的。不过,即使不做这些练习,也不会影响读懂本书的任何章节。所以,读者如果只希望对网络安全有全面的了解,但没有时间或不愿花时间编写程序的话,则可跳过这些程序练习。

本书的基本结构如下所述。第 1 章介绍网络安全的研究领域,讨论网络安全所要解决的问题。第 2~4 章介绍网络安全领域的标准常规加密算法,公钥密码体系,密钥的产生、输送与管理方法,公钥证书,数据认证方法。第 5 章介绍实用网络安全协议和无线网安全协议。第 6~8 章介绍防火墙、抗恶意软件和入侵检测系统。标有星号的章节内容较深,故作为本科生教材时可略去。习题分常规、中等难度(以 * 为记)、较难(以 ** 为记)三种级别。本科生应能完成不带星号的习题,研究生应能完成不带星号和带一个星号的习题,学有余力的本科生和研究生可试做带两个星号的习题。带星号的编程练习也可以作为实验设计。有些练习的内容是在

带星号的章节内讲授的，所以虽然不难，也标上了一个星号。

本书是根据作者多年来积累的网络安全教学经验和学生们的反馈，在以前写过的讲义的基础上整理、补充和加工而成的。本书内容除少部分外，均在本系的高年级本科生和研究生的网络安全课程中讲授过。作者在 2006 年春季特别用本书的手稿给本系研究生讲授网络安全课程，并在此基础上对本书手稿做了进一步的加工和修改。尽管如此，本书不妥之处在所难免，恳请读者及采用本书为教材的人员一旦发现错误后尽快通知作者。来信和建议请寄到作者的电子邮箱：wang@cs.uml.edu，或寄到作者的通信地址：J. Wang, Department of Computer Science, University of Massachusetts, Lowell, MA 01854, USA。

作者有幸从 1996 年起一直从事计算机网络安全本科生与研究生课程的设计与教学，并从 2002 年起组织并参与了本校网络与信息安全中心每周一次的讨论班，在此期间得到许多同事、学生和校外专家的帮助，谨在此表示感谢。感谢在北卡罗来纳州任教时的同事保罗·杜沃 (Paul Duvall) 教授和现在的同事大卫·马丁 (David Martin) 教授的帮助。杜沃教授是美国国家安全局 (NSA) 的密码学专家，马丁教授是计算机保密和软件法检的专家。我从他们那里获益良多。

用母语写此书是我的心愿，感谢高等教育出版社给我这个机会。

斯娃提·古塔 (Swati Gupta) 曾在 2002 年将作者的讲课内容做过详细笔记，刘本渊教授阅读了本书初稿的部分章节，助教杜春燕阅读了本书初稿的全部章节，部分曾在中国受过高等教育的博士研究生和硕士研究生也对本书的写作提供了帮助，他们是余芷君、钟宁、黄蓓 (按姓氏笔画为序)，谨在此致以诚挚的谢意。

写此书所花的时间和精力比约稿时预计的超出了许多。为写此书不可避免地占用了与家人共聚的时间，我对此深怀歉意。感谢妻子赵虹和儿子、女儿的谅解与支持。

愿此书能为中国计算机网络安全的高等教育的普及尽一点力量。

王杰 (J. Wang), 美国麻省大学罗威尔分校

2006 年 5 月

目 录

第 1 章 网络安全概论	1
1.1 网络安全的任务	2
1.1.1 网络安全的指导思想	2
1.1.2 信息安全的其他领域	3
1.2 基本攻击类型和防范措施	4
1.2.1 窃听	4
1.2.2 密码分析	4
1.2.3 盗窃登录密码	5
1.2.4 身份诈骗	12
1.2.5 软件剥削	17
1.2.6 抵赖	18
1.2.7 入侵	19
1.2.8 流量分析	19
1.2.9 服务阻断	20
1.2.10 恶意软件	22
1.2.11 其他攻击类型	25
1.3 攻击者类别	25
1.3.1 黑客	26
1.3.2 抄袭小儿	26
1.3.3 电脑间谍	27
1.3.4 恶意雇员	27
1.3.5 电脑恐怖分子	27
1.4 网络安全的基本模型	28
1.5 网络安全信息资源网站	29

1.5.1	CERT	29
1.5.2	SANS	29
1.5.3	微软安全顾问	29
1.5.4	NTBugtraq	29
1.6	结束语	30
	习题	30
第 2 章	常规加密算法	36
2.1	加密算法的设计要求	37
2.1.1	ASCII 码	37
2.1.2	排斥加密码	38
2.1.3	加密算法的要求	40
2.2	数据加密标准	41
2.2.1	Feistel 密码体系	42
2.2.2	子钥	44
2.2.3	DES 替换矩阵	44
2.2.4	DES 加密算法	46
2.2.5	解密算法和正确性证明	48
2.2.6	DES 安全强度	49
2.3	多重 DES	49
2.3.1	三重两钥 DES	49
2.3.2	两重 DES 和三重三钥 DES	50
2.3.3	中间相交攻击	50
2.4	高级加密标准	52
2.4.1	基本结构	52
2.4.2	S-匣子	54
2.4.3	AES-128 子钥	56
2.4.4	子钥相加	57
2.4.5	字节替换	57
2.4.6	行位移	58
2.4.7	列混合	58
2.4.8	AES-128 加密和解密算法	59
2.4.9	伽罗华域	60
2.4.10	S-匣子的构造	63
2.4.11	安全强度	64

2.5	加密算法的常用模式	64
2.5.1	电子密码本模式	65
2.5.2	密码段链模式	65
2.5.3	密码反馈模式	65
2.5.4	输出反馈模式	66
2.5.5	计数器模式	67
2.6	序列密码	67
2.6.1	RC4 加密算法	67
2.6.2	RC4 的安全弱点	68
2.7	密钥的产生	70
2.7.1	ANSI X9.17 密钥标准	70
2.7.2	BBS 伪随机二元字符发生器	71
2.8	结束语	71
	习题	72
第 3 章	公钥密码体系和密钥管理	78
3.1	公钥密码体系的基本概念	78
3.2	数论的一些基本概念和定理	80
3.2.1	模运算和同余关系	81
3.2.2	模下的逆元素	82
3.2.3	原根	83
3.2.4	求模下指数幂的快速算法	83
3.2.5	寻找大素数的快速算法	85
3.2.6	中国余数定理	86
3.2.7	有限连分数	87
3.3	Diffie-Hellman 密钥交换体系	88
3.3.1	密钥交换协议	89
3.3.2	中间人攻击	90
3.3.3	Elgamal 公钥体系	91
3.4	RSA 公钥体系	91
3.4.1	RSA 公钥、私钥、加密和解密	91
3.4.2	选取RSA参数的注意事项	94
3.4.3	RSA 数	97
*3.5	椭圆曲线公钥体系	98
3.5.1	离散椭圆曲线	100
3.5.2	椭圆曲线编码	100
3.5.3	椭圆曲线加密算法	102
3.5.4	椭圆曲线密钥交换	102

3.5.5 椭圆曲线公钥体系的强度	103
3.6 钥匙传递和管理	103
3.6.1 主密钥和会话密钥	103
3.6.2 公钥证书	103
3.6.3 公钥机构网	104
3.6.4 匙圈	106
3.7 结束语	107
习题	107
第 4 章 数据认证	112
4.1 散列函数	112
4.1.1 散列函数的设计要求	113
4.1.2 构造密码散列函数的探索	114
4.1.3 标准散列函数的基本结构	114
4.1.4 SHA-512	115
4.1.5 漩涡散列函数	118
4.2 密码校验和	123
4.2.1 逻辑加密码校验和	123
4.2.2 信息认证码的设计要求	123
4.2.3 数据认证码	124
4.3 密钥散列信息认证码	124
4.3.1 散列信息认证码的设计要求	124
4.3.2 HMAC 算法模式	125
4.4 OCB 操作模式	125
4.4.1 基本运算	125
4.4.2 OCB 加密算法和标签的生成	127
4.4.3 OCB 解密算法和标签验证	128
4.5 生日攻击	128
4.5.1 冲撞概率和抗冲撞强度上界	129
4.5.2 集相交攻击	130
4.6 数字签名标准	132
4.7 双签协议和电子交易	134
4.7.1 双签应用示例	135
4.7.2 双签在 SET 中的应用	135
4.8 盲签协议和电子现钞	137
4.8.1 RSA 盲签协议	137
4.8.2 电子现钞	138

4.9 结束语	139
习题	139
第 5 章 实用网络安全协议	145
5.1 密码算法在网络各层中的置放效果	145
5.1.1 设在应用层的密码算法	147
5.1.2 设在传输层的密码算法	147
5.1.3 设在网络层的密码算法	148
5.1.4 设在数据链接层的密码算法	148
5.1.5 实现密码算法的硬件和软件	148
5.2 公钥基础设施	148
5.2.1 X.509公钥结构	149
5.2.2 X.509公钥证书格式	150
5.3 IPsec: 网络层安全协议	152
5.3.1 安全联结与应用模式	152
5.3.2 应用模式	153
5.3.3 认证格式	155
5.3.4 载荷安全封装格式	157
5.3.5 密钥交换协议	158
5.4 SSL/TLS: 传输层安全协议	161
5.4.1 ZIP 压缩算法简介	162
5.4.2 SSL 握手协议	164
5.4.3 SSL 记录协议	166
5.5 PGP 和 S/MIME: 电子邮件安全协议	167
5.5.1 R64 编码	168
5.5.2 电子邮件安全的基本机制	169
5.5.3 PGP	170
5.5.4 S/MIME	172
5.5.5 Kerberos 身份认证协议	172
5.5.6 基本思想	173
5.5.7 单域 Kerberos 协议	173
5.5.8 多域 Kerberos 协议	175
5.6 远程登录安全协议 SSH	177
5.7 结束语	178
习题	178

第 6 章 无线网安全性	183
6.1 无线通信和 802.11 无线局域网标准	183
6.1.1 无线局域网体系结构	184
6.1.2 802.11 概述	185
6.1.3 无线通信的安全性弱点	186
6.2 有线等价隐私协议	187
6.2.1 移动设备认证和访问控制	187
6.2.2 数据完整性验证	187
6.2.3 LLC 网帧的加密	189
6.2.4 WEP 的安全缺陷	190
6.3 Wi-Fi 访问保护协议	193
6.3.1 设备认证和访问控制	193
6.3.2 TKIP 密钥	194
6.3.3 TKIP 信息完整性码	196
6.3.4 TKIP 密钥混合	197
6.3.5 WPA 加密和解密机制	200
6.3.6 WPA 安全强度	201
6.4 IEEE 802.11i/WPA2	202
6.4.1 AES-128 密钥的生成	202
6.4.2 CCMP 加密与 MIC	203
6.4.3 802.11i 安全强度	203
6.5 蓝牙安全机制	204
6.5.1 Pico 网	205
6.5.2 安全配对	206
6.5.3 SAFER+ 分组加密算法	206
6.5.4 蓝牙算法 E_1 、 E_{21} 和 E_{22}	209
6.5.5 蓝牙认证	211
6.5.6 PIN 码破译攻击	212
6.5.7 蓝牙安全简单配对协议	213
6.6 无线网状网的安全性	213
6.7 结束语	215
习题	216
第 7 章 网络边防	219
7.1 防火墙基本结构	220
7.2 网包过滤防火墙	221
7.2.1 无态过滤	221
7.2.2 有态过滤	223

7.3	线路网关	224
7.3.1	基本结构	225
7.3.2	SOCKS 协议	226
7.4	应用网关	227
7.4.1	缓存网关	227
7.4.2	有态网包检查	227
7.4.3	其他类型防火墙	228
7.5	可信赖系统和堡垒主机	228
7.5.1	可信赖操作系统	228
7.5.2	堡垒主机和网关	229
7.6	防火墙布局	230
7.6.1	单界面堡垒系统	230
7.6.2	双界面堡垒系统	231
7.6.3	子网监控防火墙系统	231
7.6.4	多层 DMZ	232
7.6.5	网络安全基本拓扑结构	233
7.7	网络地址转换	234
7.7.1	动态 NAT	234
7.7.2	虚拟局域网	235
7.7.3	SOHO 防火墙	235
7.7.4	反向防火墙	236
7.8	防火墙设置	237
7.8.1	安全政策	237
7.8.2	设置 Linux 无态过滤防火墙	237
7.9	结束语	238
	习题	238
第 8 章	抗恶意软件	244
8.1	病毒	244
8.1.1	病毒种类	245
8.1.2	病毒感染机制	247
8.1.3	病毒结构	248
8.1.4	载体压缩病毒	249
8.1.5	病毒传播	251
8.1.6	Win32 病毒传染机制	251
8.1.7	病毒炮制工具包	252

8.2	蠕虫	253
8.2.1	常见蠕虫种类	253
8.2.2	莫里斯蠕虫	253
8.2.3	梅丽莎蠕虫	254
8.2.4	电子邮件附件	254
8.2.5	红色代码蠕虫	257
8.2.6	其他针对微软产品的蠕虫	258
8.3	病毒防治	259
8.3.1	常用杀毒方法	259
8.3.2	抗病毒软件产品	260
8.3.3	仿真杀毒	261
8.4	特洛伊木马	262
8.5	网络骗局	262
8.6	对等网络安全问题	264
8.6.1	P2P 安全弱点	264
8.6.2	P2P 安全措施	265
8.6.3	实时信息	265
8.7	万维网安全问题	266
8.7.1	万维网文件种类	266
8.7.2	万维网文件的安全性	267
8.7.3	ActiveX	268
8.7.4	Cookie	269
8.7.5	间谍软件	270
8.7.6	AJAX 安全性	271
8.8	分布式服务阻断攻击和防卫	272
8.8.1	主仆 DDoS 攻击	272
8.8.2	主仆 DDoS 反射攻击	273
8.8.3	DDoS 攻击的防御	273
8.9	结束语	275
	习题	275
第 9 章	入侵检测系统	279
9.1	基本概念	279
9.1.1	基本方法	280
9.1.2	安全审核	281
9.1.3	体系结构	283
9.1.4	检测政策	284
9.1.5	不可接受行为	285

9.2	网检和机检	285
9.2.1	网检系统	286
9.2.2	机检系统	287
9.3	特征检测	288
9.3.1	网络特征	289
9.3.2	行为特征	289
9.3.3	局外人行为和局内人滥用权限	290
9.3.4	特征检测方式	291
9.4	统计分析	292
9.4.1	事件计数器	292
9.4.2	事件计量器	292
9.4.3	事件计时器	293
9.4.4	资源利用率	293
9.4.5	统计学方法	293
9.5	行为推理	294
9.5.1	数据挖掘技术	294
9.5.2	行为推理实例	295
9.6	诱饵系统	295
9.6.1	诱饵系统种类	295
9.6.2	Honeyd	296
9.6.3	MWCollect 计划	298
9.6.4	Honeynet 计划	299
9.7	结束语	299
	习题	300
附录 A	部分习题解答	303
A.1	第 1 章习题解答	303
A.2	第 2 章习题解答	307
A.3	第 3 章习题解答	314
A.4	第 4 章习题解答	326
A.5	第 5 章习题解答	328
A.6	第 6 章习题解答	329
A.7	第 7 章习题解答	336
A.8	第 8 章习题解答	337
A.9	第 9 章习题解答	338