

信息安全系列教材

网络安全

主 编 丁建立

副主编 江荣安 许 峰 崔 鸿

牛丹梅 王小军 黄淑宽



WUHAN UNIVERSITY PRESS

武汉大学出版社

TP393.08/223

2007

信息安全系列教材

网络安全

主 编 丁建立

副主编 江荣安 许 峰 崔 鸿

牛丹梅 王小军 黄淑宽



WUHAN UNIVERSITY PRESS

武汉大学出版社

图书在版编目(CIP)数据

网络安全/丁建立主编. —武汉:武汉大学出版社, 2007. 9

信息安全系列教材

ISBN 978-7-307-05847-7

I. 网… II. 丁… 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(2007)第 147393 号

责任编辑:黄金文 史 敏 责任校对:程小宜 版式设计:支 笛

出版发行:武汉大学出版社 (430072 武昌 珞珈山)

(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.com.cn)

印刷:湖北金海印务公司

开本:787×1092 1/16 印张:20.375 字数:487千字

版次:2007年9月第1版 2007年9月第1次印刷

ISBN 978-7-307-05847-7/TP·277 定价:30.00元

版权所有,不得翻印;凡购买我社的图书,如有缺页、倒页、脱页等质量问题,请与当地图书销售部门联系调换。

前言

随着信息技术空前繁荣,人们对计算机和网络的依赖性越来越大,信息被暴露和非法使用、网络受到攻击的可能性大大增加。经济全球化、互联网应用的普及、国家信息化建设的深入,使得信息安全已经成为国家安全保障体系的核心组成部分。一个国家的信息获取能力和信息安全保障能力是 21 世纪综合国力、经济竞争能力和生存能力的重要组成部分,信息安全事故的频发已成为信息社会十分突出的问题。

从本质上来讲,网络安全就是网络上的信息安全,是指网络系统的硬件、软件及其系统中的数据受到保护,不受偶然的或者恶意的原因而遭到破坏、更改、泄露,系统连续可靠正常地运行,网络服务不中断。从广义来说,凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。从用户(个人、企业等)的角度来说,他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护,避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私,对用户资源进行破坏。从网络运行和管理者角度说,他们希望对本地网络信息的访问、读写等操作受到保护和控制,避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁,制止和防御网络黑客的攻击。对安全保密部门来说,他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵,避免机要信息泄露,避免对社会产生危害,对国家造成巨大损失。从社会教育和意识形态角度来讲,网络上不健康的内容,会对社会的稳定和人类的发展造成阻碍,必须进行控制。

本书主要从网络安全的基本原理和实践技术两个角度出发,分析目前常见的各种安全威胁,指出问题根源,提出网络安全的任务。内容基本涵盖目前主要的网络安全技术,既注重基本原理的阐述,又关注网络安全的新动向,并适时增加了实践的新技术,每章均安排有习题,重要内容安排了典型案例。

全书共分 14 章。第 1 章是网络安全概述,在分析常见的安全威胁与攻击、安全问题根源基础上,给出网络信息安全的内涵。第 2 章是安全框架与评估标准,介绍了 ISO/OSI 安全体系结构和动态的自适应网络安全模型,给出了国际安全评价标准和我国计算机安全等级划分与相关标准。第 3 章是身份认证,阐述了身份认证的基本原理,分别介绍了单机状态下的身份认证、网络环境下的身份认证以及 Windows NT 安全子系统。第 4 章是授权与访问控制,在阐述了基本概念、基本原理、常用实现方法和访问控制策略基础上,给出了一个 Windows NT 提供的安全访问控制手段的实例。第 5 章是系统平台安全,分别介绍了 UNIX 系统安全、Windows NT 安全以及网络应用安全平台。第 6 章是 IP 的安全,在分析 IP 安全体系结构基础上,给出了 Windows 2000 对于 IPSec 的支持实例。第 7 章是电子邮件的安全,分析了 S/MIME 和垃圾邮件,实例介绍 PGP 软件的使用。第 8 章是 Web 与电子商务的安全,介绍了 Web 安全防护技术和电子商务的安全,重点阐述了 SSL 和主页防修改技术。第 9 章是防火墙技术,



阐述了防火墙的基本概念、类型、体系结构,介绍了防火墙的基本技术与附加功能、防火墙技术的几个新方向、常见的防火墙产品。第10章是网闸技术,介绍了网闸的基本概念、结构与特点,阐述了网闸的配置,并进行网闸典型案例剖析。第11章是VPN技术,在阐述了VPN的基本原理、应用领域及关键安全技术,分析了VPN的实现方法,介绍了VPN产品与解决方案。第12章是无线网络安全技术,介绍了常见无线网络攻击与无线网络安全对策,分析了无线通信安全与无线VPN安全。第13章是网络侦查与取证技术,介绍了网络扫描技术与工具,分析了网络监听、口令破译、蜜罐技术,给出了网络取证的原则与步骤。第14章是入侵检测技术,介绍了入侵检测系统的分类、系统结构、分析方法以及入侵检测的发展方向,并对典型入侵检测系统进行了介绍。

在武汉大学出版社的组织下,中国民航大学丁建立教授担任本书主编,担任本书副主编的有:大连理工大学江荣安、河海大学许峰、中国民航大学崔鸿、杭州电子科技大学王小军、河南科技大学牛丹梅、福州大学黄淑宽。具体分工是:丁建立主持编写第1~2章,江荣安主持编写第3~4章,黄淑宽主持编写第5~6章,许峰主持编写第7~8章,牛丹梅主持编写第9~10章,崔鸿主持编写第11~12章,王小军主持编写第13~14章。本书由崔鸿补充习题,丁建立负责统稿。

在本书的编写过程中,中国民航大学计算机科学与技术学院的硕士研究生计金玲参与了部分资料的收集与整理,王新茹为本书的排版做了部分工作。在此对所有参与本书编写工作的老师和同学们表示衷心感谢。在此要特别感谢武汉大学张焕国教授、武汉大学王丽娜教授,武汉大学出版社黄金文副编审对教材所给予的建议与帮助。

由于作者水平有限,书中难免有不妥和错误之处,恳请读者与同行批评指正。

编者

2007年7月

信息安全系列教材

编 委 会

主 任:张焕国,武汉大学计算机学院,教授

副 主 任:何大可,西南交通大学信息科学与技术学院,教授

黄继武,中山大学信息科技学院,教授

贾春福,南开大学信息技术科学学院,教授

编 委:(排名不分先后)

东 北

张国印,哈尔滨工程大学计算机科学与技术学院副院长,教授

姚仲敏,齐齐哈尔大学通信与电子工程学院,教授

江荣安,大连理工大学电信学院计算机系,副教授

姜学军,沈阳理工大学信息科学与工程学院,副教授

华 北

王昭顺,北京科技大学计算机系副主任,副教授

李风华,北京电子科技学院研究生工作处处长,教授

李 健,北京工业大学计算机学院,教授

王春东,天津理工大学计算机科学与技术学院,副教授

丁建立,中国民航大学计算机学院,教授

武金木,河北工业大学计算机科学与软件学院,教授

张常有,石家庄铁道学院计算机系,副教授

田俊峰,河北大学数学与计算机学院,教授

王新生,燕山大学计算机系,教授

杨秋翔,中山大学电子与计算机科学技术学院网络工程系主任,副教授

西 南

彭代渊,西南交通大学计算机与通信工程学院,教授

王 玲,四川师范大学计算机科学学院院长,教授

何明星,西华大学数学与计算机学院副院长,教授

代春艳,重庆工商大学计算机科学与信息工程学院

陈 龙,重庆邮电大学计算机科学与技术学院,副教授

杨德刚,重庆师范大学数学与计算机科学学院

黄同愿,重庆工学院计算机学院

郑智捷,云南大学软件学院信息安全系主任,教授

谢晓尧,贵州师范大学副校长,教授

华东

徐炜民,上海大学计算机工程与科学学院,教授

楚丹琪,上海大学教务处,副教授

孙 莉,东华大学计算机科学与技术学院,副教授

李继国,河海大学计算机及信息工程学院,副教授

张福泰,南京师范大学数学与计算机科学学院,教授

王 箭,南京航空航天大学信息科学技术学院,副教授

张书奎,苏州大学计算机科学与技术学院,副教授

殷新春,扬州大学信息工程学院副院长,教授

林柏钢,福州大学数学与计算机科学学院,教授

唐向宏,杭州电子科技大学通信工程学院,教授

侯整风,合肥工业大学计算机学院计算机系主任,教授

贾小珠,青岛大学信息工程学院,教授

郑汉垣,福建龙岩学院数学与计算机科学学院副院长,高级实验师

中南

钟 珞,武汉理工大学计算机学院院长,教授

赵俊阁,海军工程大学信息安全系,副教授

王江晴,中南民族大学计算机学院院长,教授

宋 军,中国地质大学(武汉)计算机学院

麦永浩,湖北警官学院信息技术系副主任,教授

亢保元,中南大学数学科学与计算技术学院,副教授

李章兵,湖南科技大学计算机学院信息安全系主任,副教授

唐韶华,华南理工大学计算机科学与工程学院,教授

杨 波,华南农业大学信息学院,教授

王小明,暨南大学计算机科学系,教授

喻建平,深圳大学计算机系,教授

何炎祥,武汉大学计算机学院院长,教授

王丽娜,武汉大学计算机学院副院长,教授

执行编委:黄金文,武汉大学出版社计算机图书事业部主任,副编审

内 容 摘 要



本书主要从网络安全的基本原理和实践技术两个角度出发,分析目前常见的各种安全威胁,指出问题根源,提出网络安全的任务。全书共分 14 章,从安全框架与评估标准出发,分别介绍了身份认证、授权与访问控制、系统平台安全、IP 的安全、电子邮件的安全、Web 与电子商务的安全、防火墙技术、网闸技术、VPN 技术、无线网络安全技术、网络侦查与取证技术、入侵检测技术等。内容基本涵盖目前主要的安全技术,既注重基本原理的阐述,又关注网络安全的新动向,适时增加了实践的新技术,每章均安排有习题,重要内容均安排了典型案例。

本书重点突出,难易适当,实例丰富,实用性强。可作为各高等院校开设的信息安全相关专业的本科教材,也可供初学、准备从事相关研究的研究生参考,对从事网络安全研究和网络安全管理等领域的人员有参考价值。



序 言

21 世纪是信息的时代,信息成为一种重要的战略资源,信息的安全保障能力成为一个国家综合国力的重要组成部分。一方面,信息科学和技术正处于空前繁荣的阶段,信息产业成为世界第一大产业。另一方面,危害信息安全的事件不断发生,信息安全的形势是严峻的。

信息安全事关国家安全,事关社会稳定,必须采取措施确保我国的信息安全。

我国政府高度重视信息安全技术与产业的发展,先后在成都、上海和武汉建立了信息安全产业基地。

发展信息安全技术和产业,人才是关键。人才培养,教育是根本。2001 年经教育部批准,武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准,武汉大学又建立了信息安全的硕士点、博士点和企业博士后产业基地。自此以后,我国的信息安全专业得到迅速的发展。到目前为止,全国设立信息安全专业的高等院校已达 50 多所。我国的信息安全人才培养进入蓬勃发展阶段。

为了给信息安全专业的大学生提供一套适用的教材,武汉大学出版社组织全国 40 多所高校,联合编写出版了这套《信息安全系列教材》。该套教材涵盖了信息安全的主要专业领域,既有基础课教材,又有专业课教材,既有理论课教材,又有实验课教材。

这套书的特点是内容全面,技术新颖,理论联系实际。教材结构合理,内容翔实,通俗易懂,重点突出,便于讲解和学习。它的出版发行,一定会推动我国信息安全人才培养事业的发展。

诚恳希望读者对本系列教材的缺点和不足提出宝贵的意见。

编委会

2006 年 9 月 19 日



目 录

第 1 章 网络安全概述	1
1.1 常见的安全威胁与攻击	1
1.1.1 安全威胁	1
1.1.2 网络攻击	3
1.2 安全问题根源	6
1.3 网络信息安全的内涵	8
习题 1	9
第 2 章 安全框架与评估标准	10
2.1 ISO/OSI 安全体系结构	10
2.2 动态的自适应网络安全模型	13
2.3 五层网络安全体系	16
2.4 六层网络安全体系	18
2.5 国际安全评价标准	19
2.5.1 美国国防部评价准则	20
2.5.2 欧洲评价准则	21
2.5.3 加拿大评价准则	22
2.5.4 美国联邦评价准则	22
2.5.5 国际评价准则	23
2.6 我国计算机安全等级划分与相关标准	23
习题 2	26
第 3 章 身份认证	27
3.1 基本概念	27
3.2 单机状态下的身份认证	28
3.2.1 账户/口令认证方式	28
3.2.2 IC 卡认证方式	29
3.2.3 生物特征认证方式	30
3.3 网络环境下的身份认证	37
3.3.1 动态口令认证	38
3.3.2 USB Key 身份认证	40
3.3.3 RADIUS 协议认证	41



3.3.4 单点登录 (SSO)	42
3.4 Windows NT 安全子系统	44
习题 3	47
第 4 章 授权与访问控制	48
4.1 概念原理	48
4.2 访问控制策略	49
4.2.1 自主访问控制	49
4.2.2 强制访问控制	50
4.2.3 基于角色的访问控制	51
4.2.4 访问控制实现技术	54
4.3 Windows NT 的安全访问控制	56
4.3.1 NTFS 文件系统	57
4.3.2 NTFS 的用户和用户组	57
4.3.3 文件系统的访问控制	58
4.3.4 注册表的访问控制	60
4.3.5 打印机的访问控制	60
习题 4	61
第 5 章 系统平台安全	62
5.1 系统平台安全概述	62
5.1.1 系统平台的概念	62
5.1.2 系统平台面临的威胁	62
5.1.3 系统平台的安全机制	64
5.2 UNIX 系统安全	65
5.2.1 UNIX 系统简介	65
5.2.2 UNIX 系统的安全机制	67
5.2.3 UNIX 系统的安全管理	70
5.3 Windows NT 安全	72
5.3.1 Windows NT 的安全性简介	72
5.3.2 Windows NT 的安全模型	73
5.3.3 Windows NT 的安全机制	74
5.4 网络应用安全平台	78
5.4.1 网络应用安全平台的概述	78
5.4.2 网络应用安全平台的功能	78
习题 5	80
第 6 章 IP 的安全	81
6.1 IP 安全概述	81
6.1.1 IP 的数据报的头格式	81

6.1.2 IP 安全面临的威胁	82
6.1.3 IP 安全的解决方案	83
6.2 IP 安全体系结构	84
6.2.1 IPSec 概述	84
6.2.2 安全关联 (Security Association, SA)	85
6.2.3 AH 协议	86
6.2.4 ESP 协议	89
6.2.5 Internet 密钥交换协议	92
6.2.6 加密和验证算法	93
6.2.7 IPSec 的实现方式	93
6.3 实例: Windows 2000 对于 IPSec 的支持	94
6.3.1 IPSec 组件	94
6.3.2 配置 IPSec 策略	95
习题 6	99
第 7 章 电子邮件的安全	100
7.1 电子邮件安全概述	100
7.1.1 电子邮件的工作原理	100
7.1.2 电子邮件的安全问题及防范解决办法	101
7.2 PGP	102
7.3 S/MIME	103
7.3.1 RFC 822	103
7.3.2 多用途 Internet 邮件扩展	104
7.3.3 S/MIME 的功能	110
7.3.4 S/MIME 消息	112
7.3.5 S/MIME 证书处理	115
7.3.6 增强的安全服务	117
7.4 垃圾邮件	117
7.4.1 垃圾邮件的定义	117
7.4.2 垃圾邮件产生的原因	117
7.4.3 垃圾邮件的过滤技术	118
7.5 实例: PGP 软件的使用	119
7.5.1 安装	120
7.5.2 生成密钥对	120
7.5.3 交换密钥	120
7.5.4 发送签名和加密邮件	120
7.5.5 接收加密邮件	120
7.5.6 解密邮件	120
习题 7	120



第8章 Web与电子商务的安全	121
8.1 Web与电子商务的安全分析	121
8.1.1 安全电子交易认证技术	121
8.1.2 安全认证协议	123
8.1.3 公钥基础设施(PKI)	125
8.1.4 用户私人信息的技术保护	126
8.2 Web安全防护技术	129
8.2.1 Web安全威胁	129
8.2.2 Web流量安全方法	129
8.3 SSL	130
8.3.1 SSL体系结构	131
8.3.2 SSL记录协议	132
8.3.3 改变加密规格协议	134
8.3.4 报警协议	134
8.3.5 握手协议	135
8.3.6 密码计算	139
8.3.7 传输层安全	140
8.4 SET协议及电子商务的安全	144
8.4.1 SET概述	144
8.4.2 SET协议工作流程	145
8.4.3 SET加密技术	146
8.4.4 SET认证	148
8.4.5 SET协议中安全不足之处及改进策略	149
8.4.6 SET协议与SSL协议的比较	149
习题8	149
第9章 防火墙技术	151
9.1 防火墙的基本概念	151
9.1.1 防火墙的概念	151
9.1.2 防火墙的功能	152
9.1.3 防火墙的局限性	153
9.1.4 防火墙的发展历史	154
9.2 防火墙的类型及主要技术	154
9.2.1 防火墙的类型	154
9.2.2 包过滤技术	156
9.2.3 代理服务技术	158
9.2.4 状态检测技术	161
9.2.5 自适应代理技术	163
9.3 防火墙的体系结构	163
9.3.1 包过滤防火墙	163



9.3.2 双穴主机结构防火墙	164
9.3.3 屏蔽主机防火墙	165
9.3.4 屏蔽子网防火墙	166
9.4 典型防火墙产品	168
9.4.1 防火墙的选择	168
9.4.2 典型防火墙产品	169
9.5 防火墙技术的发展趋势	174
习题 9	176
第 10 章 网络隔离与网闸	177
10.1 网络隔离技术	177
10.1.1 网络隔离技术的概念	177
10.1.2 网络隔离技术的原理	179
10.1.3 网络隔离技术要点与发展方向	184
10.2 网 闸	185
10.2.1 网闸技术的发展	185
10.2.2 网闸工作原理	186
10.2.3 网闸技术的实现	187
10.3 典型网闸产品	191
10.3.1 网闸产品的功能	191
10.3.2 国内外网闸产品	191
习题 10	198
第 11 章 VPN 技术	200
11.1 VPN 概述	200
11.1.1 VPN 概述	200
11.1.2 VPN 分类	200
11.1.3 VPN 基本原理	201
11.1.4 实现 VPN 的关键技术	202
11.2 隧道技术	203
11.2.1 第 2 层隧道协议	204
11.2.2 第 3 层隧道协议	204
11.3 用户认证	205
11.3.1 PPP 认证方式	205
11.3.2 基于服务器的认证方式——RADIUS	207
11.4 L2TP 协议	208
11.4.1 使用 L2TP 进行虚拟拨号	208
11.4.2 L2TP 两种实现模式	208
11.4.3 L2TP 协议工作流程	210
11.4.4 L2TP 头	211



11.4.5 小结.....	212
11.5 应用 IPSec 构建 VPN.....	212
11.5.1 概述.....	212
11.5.2 IKE 概述.....	213
11.5.3 IPSec 是如何工作的.....	214
11.5.4 IPSec 安全关联 (SA).....	216
11.5.5 使用 IPSec 的 VPN 实现.....	218
习题 11.....	222
第 12 章 无线网络安全.....	223
12.1 无线局域网的基本概念.....	223
12.1.1 无线局域网的传输媒质.....	223
12.1.2 无线局域网标准的演进.....	223
12.1.3 无线局域网网络结构.....	224
12.1.4 基础模式工作原理.....	226
12.2 早期的无线网络安全及安全漏洞.....	228
12.2.1 早期的无线网络安全.....	228
12.2.2 802.11 网络的安全方案.....	228
12.2.3 RC4 加密算法.....	230
12.2.4 802.11 的巨大安全漏洞.....	231
12.3 新无线局域网安全标准 802.11i.....	234
12.3.1 802.11i 标准体系结构.....	234
12.3.2 802.11i 标准工作流程.....	235
12.4 802.11i——认证.....	236
12.4.1 IEEE 802.1x 协议.....	236
12.4.2 EAP 协议.....	238
12.4.3 EAPOL.....	239
12.4.4 RADIUS.....	240
12.4.5 安全分层.....	241
12.4.6 在 EAP 中使用 TLS.....	242
12.5 802.11i——密钥分配.....	243
12.5.1 创建和交付 PMK.....	244
12.5.2 计算 PTK.....	244
12.5.3 四次握手.....	246
12.5.4 结束握手与组密钥分发.....	247
12.6 802.11i——数据加密.....	247
12.6.1 TKIP.....	248
12.6.2 CCMP.....	250
12.7 小结.....	254
习题 12.....	254

第 13 章 网络侦查与取证技术	255
13.1 网络侦查技术	255
13.1.1 网络扫描	255
13.1.2 网络监听	257
13.1.3 口令破解	259
13.2 取证技术	262
13.2.1 电子证据	262
13.2.2 计算机取证的定义与原则	266
13.2.3 计算机取证的步骤	269
13.2.4 计算机取证方法	272
13.2.5 证据分析	276
习题 13	277
第 14 章 入侵检测技术	278
14.1 黑客攻击与防范技术	278
14.1.1 入侵手段	278
14.1.2 入侵层次分析	281
14.2 入侵检测原理和主要方法	282
14.2.1 入侵检测概念	283
14.2.2 入侵检测的基本方法	283
14.3 入侵检测技术	285
14.3.1 基于概率统计的检测	285
14.3.2 基于神经网络的检测	285
14.3.3 基于专家系统的检测	286
14.3.4 基于模型推理的检测	287
14.3.5 基于免疫的检测	287
14.3.6 入侵检测的新技术	287
14.3.7 其他相关问题	287
14.4 入侵检测系统	288
14.4.1 入侵检测系统的构成	288
14.4.2 入侵检测系统的分类	289
14.4.3 入侵检测系统的介绍	290
14.5 常见 IDS 系统	293
14.5.1 NIDES	293
14.5.2 AAFID 系统	294
14.5.3 NetSTAT	295
14.5.4 GrIDS	295
14.5.5 IDA	296
14.6 入侵检测系统的评价	298
14.6.1 IDS 测试与评估概述	298



14.6.2 测试评估入侵检测系统的步骤	300
14.6.3 测试评估入侵检测系统中存在的问题	301
14.7 入侵检测技术发展方向	302
习题 14	304
参考文献	305