

高·等·院·校·信·息·安·全·专·业·系·列·教·材

中国计算机学会教育专业委员会与清华大学出版社联合组织编写



名誉主编：何德全 编委会主任：肖国镇

Network Security

网 络 安 全

胡道元 闵京华 编著

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



清华大学出版社

华北水利水电学院图书馆



209341522

TP393.08
H468



高·等·院·校·信·息·安·全·专·业·系·列·教·材

Network Security

网络安全

胡道元 闵京华 编著



清华大学出版社
北京

934152

内 容 简 介

网络安全是在分布网络环境中,对信息载体(处理载体、存储载体、传输载体)和信息的信息处理、传输、存储、访问提供安全保护,以防止数据、信息内容或能力被非授权使用、篡改和拒绝服务。

全书共分4篇20章,全面讲述网络安全的基础知识(网络安全的人门和基础)、网络安全体系结构(开放系统互联安全体系结构和Internet安全体系结构)、网络安全技术(防火墙、VPN、IPSec、黑客技术、漏洞扫描、入侵检测、恶意代码与计算机病毒的防治、系统平台安全以及应用安全),以及网络安全工程(网络安全设计、管理、评估)。

本书内容翔实,结构合理,概念清楚,语言精炼,实用性强,易于教学。

本书可作为信息安全、计算机、通信等专业本科生、硕士生的教科书,也可供从事相关专业的教学、科研和工程人员参考。

版权所有,翻印必究。

本书封面贴有清华大学出版社激光防伪标签,无标签者不得销售。

图书在版编目(CIP)数据

网络安全/胡道元,闵京华编著. —北京:清华大学出版社,2003.12

(高等院校信息安全专业系列教材)

ISBN 7-302-07642-1

I. 网… II. ①胡… ②闵… 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(2003)第106649号

出 版 者: 清华大学出版社

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

社 总 机: 010-62770175

地 址: 北京清华大学学研大厦

邮 编: 100084

电 话: 010-62776969

组稿编辑: 张 民

文稿编辑: 王冰飞

印 刷 者: 北京市密云胶印厂

装 订 者: 北京国马印刷厂

发 行 者: 新华书店总店北京发行所

开 本: 185×230 印张: 30 字数: 592千字

版 次: 2004年1月第1版 2004年7月第2次印刷

书 号: ISBN 7-302-07642-1/TP·5604

印 数: 5001~8000

定 价: 39.00元

本书如存在文字不清、漏印以及缺页、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)62770175-3103 或 (010)62795704。

高等院校信息安全专业系列教材

编审委员会

名誉主编：何德全(中国工程院院士)

主任：肖国镇

委员：(按姓氏笔画为序)

方滨兴	冯登国	刘建亚	何大可	张玉清
杨波	吴刚	李建华	张焕国	陈克非
宫力	洪佩琳	胡振辽	胡铭曾	胡道元
侯整风	卿斯汉	钱德沛	曹珍富	谢冬青
焦金生	廖明宏	裴昌幸		

策划编辑：张民

本书责任编辑：方滨兴

序

在社会信息化的进程中,信息已成为社会发展的重要资源,信息安全也成为 21 世纪国际竞争的重要战场。为了保护国家的政治利益和经济利益,各国政府都非常重视信息和网络安全,信息安全已成为一个世纪性、全球性的研究课题。

我国的信息安全事业正在蓬勃发展,国家领导高度重视,各部门通力合作、统筹规划,大大加快了我国信息安全产业发展的步伐。随着信息安全产业的快速发展,社会对信息安全人才的需求在不断增加,在高等教育领域大力推进信息安全的专业化教育,将是国家在信息安全领域掌握自主权、占领先机的重要举措。

目前,许多大学和科研院所已创办了信息安全专业或是开设了相关课程。很高兴中国计算机学会教育专业委员会和清华大学出版社在近期联合组织了一系列信息安全专业的研讨活动。他们以严谨负责的态度,认真组织全国各高校和科研院所的专家、学者,共同研讨信息安全专业的教育方法和课程体系,并在进行大量前瞻性研究工作的基础上,启动了“高等院校信息安全专业系列教材”的编写工作。这套教材将是我国信息安全专业的第一套完整、权威的教材,相信可以对全国的高等院校信息安全专业的建设起到很好的促进作用。

希望中国计算机学会教育专业委员会和清华大学出版社能够将这个研究课题一直做下去,也希望这套教材能够取得成功并不断完善,以促进各高等院校培养出更多、更好的信息安全专门人才,为我国的信息安全事业做出更大的贡献。

何德全

中国工程院院士
高等院校信息安全专业系列教材编审委员会名誉主编
2003 年 7 月于北京

出版说明

21 世纪是信息时代,信息已成为社会发展的重要战略资源,社会的信息化已成为当今世界发展的潮流和核心,而信息安全在信息社会中将扮演极为重要的角色,它直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展,国家对信息安全人才的需求量不断增加,但目前信息安全人才极度匮乏,远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾,必须加快信息安全人才的培养,以满足社会的需求。为此,教育部继 2001 年批准在武汉大学开设信息安全本科专业之后,又批准了多所高等院校设立信息安全本科专业,而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信工程、数学等领域的交叉学科,对于这一新兴学科的培养模式和课程设置,各高校普遍缺乏经验,因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动,并成立了“高等院校信息安全专业系列教材”编审委员会,由我国信息安全领域著名专家何德全院士担任名誉主编,著名学者肖国镇教授担任编委会主任,共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则,认真研讨国内外高等院校信息安全专业的教学体系和课程设置,进行了大量前瞻性的研究工作,而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定,确定了编写教材的作者,这些作者绝大多数都是既在本专业领域有深厚的学术造诣,又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材,其特点是:

- ① 体系完整,结构合理,内容先进。
- ② 适应面广,能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。
- ③ 立体配套,除主教材外,还配有多媒体电子教案、习题与实验指导等。
- ④ 版本更新及时,紧跟科学技术的新发展。

为了保证出版质量,我们坚持宁缺毋滥的原则,成熟一本,出版一本,并保持不断更新,力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材,满足学生用书的基础上,还经由专家的推荐和审定,遴选了一批国外信息安全领域优秀的教材加入到本系列教材中,以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍,同时也欢迎广大读者提出宝贵意见,以便我们对本系列教材的组织、编写与出版工作不断改进,为我国信息安全专业的教材建设与人才培养做出更大的贡献。

我们的 E-mail 地址是: zhangm@tup.tsinghua.edu.cn; 联系人: 张民。

中国计算机学会教育专业委员会

清华大学出版社

2003 年 7 月

前言

我们生存的世界并不安宁,人们渴望有一个安全、和平的生存空间,随着信息技术的发展,特别是网络的发展,人们的诸多活动越来越多地依赖于网络空间,然而,网络空间并非总是安全的。

当前我国的网络安全正面临着严峻的挑战。一方面随着电子政务工程的启动、电子商务的开展以及国家关键基础设施的网络化,网络安全的需求更加严格和迫切。另一方面,黑客攻击、病毒传播以及形形色色的网络攻击日益增加,网络安全防线十分脆弱。

网络安全是在分布网络环境中,对信息载体(处理载体、存储载体、传输载体)和信息的信息处理、传输、存储、访问提供安全保护,以防止数据、信息内容或能力拒绝服务或被非授权使用、篡改。

从本质上讲,安全就是风险管理,风险是构成安全基础的基本观念。风险是丢失需要保护的资产的可能性,是威胁和漏洞的综合结果。没有漏洞的威胁就没有风险,而没有威胁的漏洞也没有风险。

“网络安全”是信息安全专业的主要专业课,学生应从以下三个方面掌握网络安全的基本原理、主要技术以及解决方案:

(1) 网络安全体系结构

由开放系统互连模型和 Internet 层次体系结构决定了网络安全体系结构的层次模型。网络安全体系结构描述网络信息体系结构在满足安全需求方面各基本元素之间的关系,反映信息系统安全需求和网络体系结构的共性。并由此派生了相应的网络安全协议、技术和标准。

(2) 网络安全技术

单一的网络安全技术和网络安全产品无法解决网络安全的全部问题。应根据应用需求和安全策略,综合运用各种网络安全技术,包括防火墙、VPN、IPSec、黑客技术、漏洞扫描、入侵检测、恶意代码与计算机病毒的防治、系统平台安全以及应用安全等。

(3) 网络安全工程

对网络安全进行的综合处理,要从体系结构的角度,用系统工程的方法,贯穿网络安全设计、开发、部署、运行、管理和评估的全过程。

本书共分4篇20章。第1篇为网络安全基础知识,共5章,是网络安全的入门和基础。第2篇为网络安全体系结构,共2章,讲述开放系统互连安全体系结构和Internet安全体系结构。第3篇为网络安全技术,共9章,讲述各种网络安全技术。第4篇为网络安全工程,共4章,分别讲述网络安全设计、管理、评估。

每章开始列出本章要点,最后给出小结,概要地总结本章的要点。每章结尾附有习题,帮助读者复习。

本书可作为信息安全、计算机、通信等专业本科生、硕士研究生的教科书,也可供从事相关专业的教学、科研和工程人员参考。

本书由胡道元教授主编并编著了第1章~第7章、第17、第18和第20章,闵京华博士编著了第14、第16和第19章,朱卫国编著了第15章,邵忠岗、黄新民、刘旺泉、陆新宇、邢羽嘉分别编著了第8章~第13章。赵青为书稿的编排、打印做了大量的工作。闵京华博士做了全书的最后校订工作。

作者

2003年7月

目 录

第 1 篇 网络安全基础知识

第 1 章 引论	3
1.1 网络安全概述	3
1.1.1 网络安全的概念	3
1.1.2 网络安全的属性	7
1.1.3 网络安全层次结构	8
1.1.4 网络安全模型	9
1.2 安全的历史回顾	11
1.2.1 通信安全	11
1.2.2 计算机安全	12
1.2.3 网络安全	13
1.3 网络安全处理	14
1.3.1 网络安全综合处理	14
1.3.2 网络安全处理过程	16
1.4 密码学	17
1.4.1 密码学的基本原理	17
1.4.2 对称密钥密码技术	18
1.4.3 公钥密码技术	19
1.5 本章小结	20
习题	20
第 2 章 风险分析	22
2.1 资产保护	22

2.1.1	资产的类型	22
2.1.2	潜在的攻击源	23
2.1.3	资产的有效保护	24
2.2	攻击	25
2.2.1	攻击的类型	25
2.2.2	主动攻击和被动攻击	26
2.2.3	访问攻击	27
2.2.4	篡改攻击	30
2.2.5	拒绝服务攻击	31
2.2.6	否认攻击	32
2.3	风险管理	32
2.3.1	风险的概念	32
2.3.2	风险识别	35
2.3.3	风险测量	37
2.4	本章小结	39
习题		40
第3章	安全策略	41
3.1	安全策略的功能	41
3.2	安全策略的类型	42
3.2.1	信息策略	42
3.2.2	系统和网络安全策略	43
3.2.3	计算机用户策略	45
3.2.4	Internet 使用策略	46
3.2.5	邮件策略	46
3.2.6	用户管理程序	47
3.2.7	系统管理程序	47
3.2.8	事故响应程序	48
3.2.9	配置管理程序	49
3.2.10	设计方法	50
3.2.11	灾难恢复计划	50
3.3	安全策略的生成、部署和有效使用	51
3.3.1	安全策略的生成	51
3.3.2	安全策略的部署	52

3.3.3 安全策略的有效使用	53
3.4 本章小结	54
习题	54
第4章 网络信息安全服务	56
4.1 机密性服务	57
4.1.1 文件机密性	57
4.1.2 信息传输机密性	57
4.1.3 通信流机密性	57
4.2 完整性服务	59
4.2.1 文件完整性	59
4.2.2 信息传输完整性	60
4.3 可用性服务	60
4.3.1 后备	60
4.3.2 在线恢复	60
4.3.3 灾难恢复	61
4.4 可审性服务	61
4.4.1 身份标识与身份鉴别	61
4.4.2 网络环境下的身份鉴别	62
4.4.3 审计功能	65
4.5 数字签名	65
4.6 Kerberos 鉴别	66
4.7 公钥基础设施	67
4.8 访问控制	69
4.9 本章小结	70
习题	71
第5章 网络安全处理	73
5.1 评估	73
5.1.1 网络评估	75
5.1.2 物理安全评估	75
5.1.3 策略和过程评估	76
5.1.4 预防措施评估	76

5.1.5 员工和管理员评估	76
5.1.6 评估结果	78
5.2 策略制定	78
5.3 实施	79
5.3.1 安全报告系统	79
5.3.2 各种安全机制的实施	80
5.4 安全培训	82
5.5 审计	82
5.6 网络安全实施流程	84
5.7 本章小结	85
习题	86

第 2 篇 网络安全体系结构

第 6 章 开放系统互连安全体系结构	89
6.1 网络体系结构及协议	89
6.1.1 分层和协议	89
6.1.2 开放系统互连参考模型	90
6.2 OSI 安全体系结构的 5 类安全服务	93
6.3 OSI 安全体系结构的安全机制	95
6.4 OSI 安全服务与安全机制的关系	100
6.5 在 OSI 层中的安全服务配置	101
6.6 OSI 安全体系的安全管理	102
6.7 本章小结	106
习题	106
第 7 章 Internet 安全体系结构	109
7.1 Internet 安全结构布局	109
7.1.1 Internet 提供的服务	109
7.1.2 Internet 不应提供的服务	111
7.1.3 通信结构	112
7.1.4 非军事区	116

7.1.5	网络地址转换	121
7.1.6	合作伙伴网络	124
7.2	网络安全层次模型	126
7.2.1	第二层保护的网路——链路层安全	126
7.2.2	第三层保护的网路——网络层安全	129
7.2.3	传输层保护的网路	132
7.2.4	应用层安全性	134
7.2.5	WWW 应用安全技术	137
7.3	OSI 安全体系到 TCP/IP 安全体系的映射	139
7.4	本章小结	140
	习题	140

第 3 篇 网络安全技术

第 8 章	防火墙	145
8.1	防火墙的原理	145
8.1.1	防火墙的概念	145
8.1.2	防火墙的功能	146
8.1.3	边界保护机制	147
8.1.4	潜在的攻击和可能的对象	148
8.1.5	互操作性要求	149
8.1.6	防火墙的局限性	149
8.1.7	防火墙的分类	150
8.1.8	防火墙的访问效率和安全需求	150
8.2	防火墙技术	151
8.2.1	包过滤技术	151
8.2.2	应用网关技术	152
8.2.3	状态检测防火墙	152
8.2.4	电路级网关	153
8.2.5	代理服务器技术	153
8.3	防火墙体系结构	154
8.3.1	双重宿主主机体系结构	154

8.3.2	被屏蔽主机体系结构	155
8.3.3	被屏蔽子网体系结构	156
8.4	堡垒主机	158
8.5	数据包过滤	158
8.5.1	数据包过滤的特点	158
8.5.2	数据包过滤的应用	159
8.5.3	过滤规则制定的策略	161
8.5.4	数据包过滤规则	163
8.6	状态检测的数据包过滤	164
8.7	防火墙的发展趋势	167
8.8	本章小结	168
	习题	169
第9章	VPN	170
9.1	VPN 概述	170
9.1.1	VPN 的概念	170
9.1.2	VPN 的类型	171
9.1.3	VPN 的优点	173
9.2	VPN 技术	173
9.2.1	密码技术	173
9.2.2	身份认证技术	175
9.2.3	隧道技术	175
9.2.4	密钥管理技术	176
9.3	第二层隧道协议——L2F、PPTP 和 L2TP	176
9.3.1	隧道协议的基本概念	176
9.3.2	L2F	178
9.3.3	PPTP	178
9.3.4	L2TP	180
9.3.5	PPTP 和 L2TP 的比较	183
9.4	第三层隧道协议——GRE	184
9.5	本章小结	186
	习题	186

第 10 章	IPSec	188
10.1	IPSec 安全体系结构	188
10.1.1	IPSec 的概念	188
10.1.2	IPSec 的功能	190
10.1.3	IPSec 体系结构	190
10.1.4	安全联盟和安全联盟数据库	191
10.1.5	安全策略和安全策略数据库	193
10.1.6	IPSec 运行模式	193
10.2	IPSec 安全协议——AH	194
10.2.1	AH 概述	194
10.2.2	AH 头部格式	195
10.2.3	AH 运行模式	196
10.2.4	数据完整性检查	198
10.3	IPSec 安全协议——ESP	199
10.3.1	ESP 概述	199
10.3.2	ESP 头部格式	199
10.3.3	ESP 运行模式	200
10.4	ISAKMP 协议	203
10.4.1	ISAKMP 概述	203
10.4.2	ISAKMP 包头部格式	204
10.4.3	ISAKMP 载荷头部	206
10.4.4	ISAKMP 载荷	207
10.4.5	ISAKMP 协商阶段	208
10.4.6	交换类型	209
10.5	IKE 协议	209
10.5.1	IKE 概述	209
10.5.2	IKE 交换模式	210
10.6	本章小结	210
	习题	210
第 11 章	黑客技术	212
11.1	黑客的动机	212
11.2	黑客攻击的流程	213

11.2.1	踩点	213
11.2.2	扫描	216
11.2.3	查点	217
11.2.4	获取访问权	217
11.2.5	权限提升	218
11.2.6	窃取	218
11.2.7	掩盖踪迹	218
11.2.8	创建后门	218
11.2.9	拒绝服务攻击	219
11.3	黑客技术概述	219
11.3.1	协议漏洞渗透	219
11.3.2	密码分析还原	221
11.3.3	应用漏洞分析与渗透	223
11.3.4	社会工程学	224
11.3.5	恶意拒绝服务攻击	226
11.3.6	病毒或后门攻击	228
11.4	针对网络的攻击	228
11.4.1	拨号和 VPN 攻击	229
11.4.2	针对防火墙的攻击	231
11.4.3	网络拒绝服务攻击	235
11.5	本章小结	237
	习题	238
第 12 章	漏洞扫描	239
12.1	计算机漏洞	239
12.1.1	计算机漏洞的概念	239
12.1.2	存在漏洞的原因	240
12.1.3	公开的计算机漏洞信息	241
12.2	实施网络扫描	243
12.2.1	发现目标	243
12.2.2	攫取信息	247
12.2.3	漏洞检测	256
12.3	常用的网络扫描工具	259