



最前沿、最权威、最完整、最实用的

网络安全解决方案

计算机网络安全 工程师宝典

○ 陈庄 巫茜 等著

COMPUTER
NETWORK SECURITY
ENGINEER BOOK



重庆出版集团  重庆出版社

计算机网络安全 工程师宝典

陈庄 巫茜 王柯柯 郭彦 曹琼 邹航 著

重庆出版集团  重庆出版社

图书在版编目(CIP)数据

计算机网络安全工程师宝典 / 陈庄, 巫茜著. -重庆:
重庆出版社, 2010.10
ISBN 978-7-229-03043-8

I. ①计… II. ①陈… ②巫… III. ①计算机网络-
安全技术-教材 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2010)第 187791 号

计算机网络安全工程师宝典

JISHUANGJI WANGLUOANQUAN GONGCHENGSHI BAODIAN

陈庄 巫茜 王柯柯 郭彦 曹琼 邹航 著



重庆出版集团 出版
重庆出版社

重庆市长江二路 205 号 邮政编码 400016 <http://www.cqph.com>

出版人: 罗小卫

责任编辑: 傅钟波

重庆升光电力印务有限公司印刷

重庆市天下图书有限责任公司发行

重庆市北部新区高新园财富大道 19 号财富三号 B 幢 1-8 邮政编码 401121

全国新华书店经销

开本: 787mm×1092mm 1/16 印张: 33.5 字数: 465 千字

版次: 2010 年 11 月第 1 版 印次: 2010 年 11 月第 1 次印刷

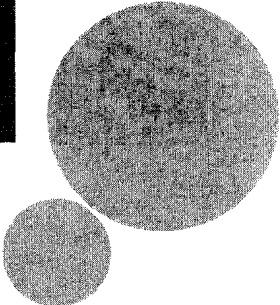
书号: ISBN 978-7-229-03043-8

定价: 88 元

如有印装质量问题, 请向重庆市天下图书有限责任公司调换: 023-63658950

版权所有, 侵权必究

内容提要



本书密切结合我国计算机网络安全技术和设计的前沿知识,全面系统地介绍了计算机网络安全技术和设计的内涵、意义、方法和原理。全书共分为三篇,第1篇介绍网络安全技术相关内容,共分9章,主要内容包括计算机网络基础、网络安全技术概述、密码技术、防火墙技术、入侵检测技术、虚拟专用网、反病毒技术、无线网络安全技术、常用系统的网络安全策略等;第2篇介绍网络安全设计相关内容,共分7章,主要内容包括网络安全设计概论、物理安全设计、网络安全设计、主机安全设计、应用安全设计、数据安全设计和网络安全系统设计方案等;第3篇为实验篇,包括网络信息探测、入侵检测、网络监听、邮件加密、虚拟机安装、SSL软件、密码学等实验项目。

本书内容深入浅出,既注重理论研究,又注重实际操作应用,而且包含丰富的习题和实验题目,特别适合作为高等院校计算机网络安全类专业学生的教材,也可作高职高专和有关培训机构的教材,还可供企事业单位从事网络安全设计和管理的技术人员阅读、参考。

前言

随着计算机技术、现代通信技术和网络技术的发展,尤其是 Internet 的广泛应用,计算机的应用更加广泛与深入,计算机网络和人们的工作与生活的联系也越来越密切。在受益于计算机网络便利的同时,人们也发现自己的计算机信息系统不断受到侵害,其形式多样、技术先进且复杂,令人防不胜防。因此,伴随着计算机网络在政治、经济、文化、教育、通信、军事等方面的作用日益增大,社会对计算机网络依赖的日益增强,网络安全问题成了一个热点。

计算机网络安全是指保护网络系统中的软件、硬件及信息资源,使之免受偶然或恶意的破坏篡改和泄露,保证网络系统的正常运行、网络服务不中断。它是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多学科的综合性学科。影响网络安全的因素很多,保护网络安全的技术手段也很多,主要包括防火墙技术、入侵检测技术、安全评估技术、防病毒技术、加密技术、身份认证技术等等。为了保护网络系统的安全,必须结合网络的具体需求,将多种安全措施进行整合设计一个

完整的、立体的、多层次的网络安全防御体系,建立一个全面的网络安全解决方案。

本书密切结合我国计算网络安全技术和设计的前沿知识,全面系统地介绍了计算机网络安全技术和设计的内涵、意义、方法和原理。全书共分3篇,16章,其中,第1章~第3章、第7章、第10章由陈庄教授编写,第8、9章、第3篇由巫茜编写,第4、5章由郭彦编写,第6章由曹琼编写,第11、12、15章由王柯柯、邹航共同编写,全书由陈庄、巫茜总纂。

本书在编写过程中参考了大量文献,并已尽可能详尽地罗列在书后的参考文献中,但仍难免有遗漏,谨向被遗漏的作者表示歉意,并向所有的作者表示诚挚的感谢。

本书内容深入浅出,既注重理论研究,又注重实际操作,包含了大量的图例、案例、练习和实验题目,特别适合作为高等院校计算机网络安全类专业学生的教材,其中大量的实训内容可供高职高专和有关培训机构使用,本书也可供企事业单位从事网络安全设计和管理的技术人员参阅。

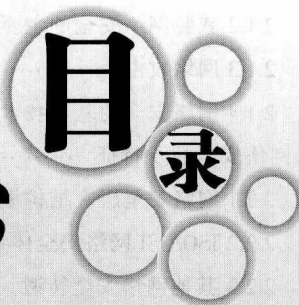
由于编者水平有限,时间仓促,书中不妥和错误之处在所难免,恳请读者包涵并不吝赐教,以便再版时修改。

编者

2010年11月



CONTENTS



计算机网络安全技术篇

第 1 章 计算机网络基础

1.1 计算机网络概念	2
1.1.1 计算机网络的定义	2
1.1.2 计算机网络的发展概况	3
1.1.3 计算机网络的基本功能	3
1.2 计算机网络体系结构	4
1.2.1 计算机网络体系结构特点	4
1.2.2 ISO/OSI 开放系统互联参考模型	4
1.3 计算机网络互联部件	6
1.3.1 计算机与外部设备	6
1.3.2 网络连接设备	6
1.3.3 传输介质	9
1.3.4 网络协议	10
1.3.5 网络协议	11
1.4 TCP/IP 网络协议和服务	11
1.4.1 TCP/IP 的概念	11
1.4.2 TCP/IP 的层次结构	11
1.4.3 TCP/IP 协议与安全服务	14
思考题	14

第 2 章 网络安全技术概述

2.1 网络安全技术概念	15
--------------------	----



2.1.1 网络安全定义及特征	15
2.1.2 威胁网络安全的主要因素	17
2.1.3 网络攻击	20
2.1.4 网络安全的基本技术	24
2.2 网络安全技术特征	26
2.2.1 网络安全层次结构模型	26
2.2.2 ISO/OSI 网络安全体系结构	27
2.2.3 其他网络安全转型	30
2.2.4 网络安全技术评估标准	30
2.3 网络安全技术分类	33
2.3.1 被动的网络安全技术	33
2.3.2 主动的网络安全技术	34
2.4 网络安全技术发展趋势	35
2.4.1 防火墙技术发展趋势	35
2.4.2 入侵检测技术发展趋势	35
2.4.3 防病毒技术发展趋势	36
思考题	37

第 3 章 密码技术

3.1 密码技术概论	38
3.1.1 密码技术基本概念	38
3.1.2 密码技术的数学表述	39
3.1.3 密码技术发展历程	40
3.2 对称密码技术	41
3.2.1 对称密码技术概论	41
3.2.2 古典对称密码技术	41
3.2.3 现代对称密码技术——DES 算法	44
3.3 非对称密码系统	51
3.3.1 非对称密码技术概论	51
3.3.2 著名非对称加密技术——RSA 算法	53
3.3.3 PKI 系统	55
思考题	56



第4章 防火墙技术

4.1 防火墙概念	57
4.1.1 防火墙的定义	57
4.1.2 防火墙的原理与组成	58
4.1.3 防火墙的分类	59
4.1.4 防火墙的功能及重要性	62
4.1.5 防火墙技术发展动向和趋势	63
4.2 防火墙体系结构	64
4.2.1 双重宿主主机体系结构	64
4.2.2 被屏蔽主机体系结构	65
4.2.3 被屏蔽子网体系结构	66
4.3 防火墙设计及实现	66
4.3.1 防火墙主要性能指标	66
4.3.2 防火墙安全设计策略	69
4.3.3 典型防火墙的设计与实现	70
4.4 防火墙应用案例	73
4.4.1 防火墙的选择原则	73
4.4.2 防火墙的部署方法和步骤	75
4.4.3 典型的防火墙产品	75
4.4.4 典型防火墙产品的应用	77
思考题	92

第5章 入侵检测技术

5.1 入侵检测概念	93
5.1.1 入侵检测的定义	93
5.1.2 入侵检测系统的分类	94
5.1.3 入侵检测的发展动向和趋势	95
5.2 入侵检测原理	96
5.2.1 入侵检测系统的标准模型	96
5.2.2 入侵检测系统的分析方法	97
5.2.3 入侵检测系统的部署	100
5.3 入侵检测应用案例	101
5.3.1 入侵检测系统的选择原则	101



5.3.2 典型的入侵检测系统介绍	102
思考题	136

第 6 章 虚拟专用网(VPN)技术

6.1 VPN 概述	137
6.1.1 VPN 的概念	137
6.1.2 VPN 的体系结构	138
6.1.3 VPN 的应用领域	138
6.2 VPN 隧道协议	139
6.2.1 VPN 隧道技术的概念	139
6.2.2 VPN 隧道技术对比	147
6.3 VPN 加密方案	149
6.4 VPN 过滤规则	150
6.5 VPN 技术应用	152
6.5.1 VPN 技术应用概况	152
6.5.2 VPN 技术应用案例	153
思考题	156

第 7 章 反病毒技术

7.1 计算机病毒概念	157
7.1.1 计算机病毒定义	157
7.1.2 计算机病毒的发展史	158
7.1.3 计算机病毒的分类	160
7.1.4 计算机病毒的基本特点	161
7.1.5 计算机感染病毒的基本症状	162
7.2 常用反病毒技术	163
7.2.1 特征码技术	163
7.2.2 虚拟机技术	164
7.2.3 病毒疫苗技术	165
7.2.4 云计算技术	165
7.2.5 管理措施	166
7.3 常用反病毒软件	167
7.3.1 卡巴斯基反病毒软件	167
7.3.2 瑞星杀毒软件	169



7.3.3 美杜莎主动防御系统	172
思考题	178

第8章 无线网络安全技术

8.1 无线网络概述	179
8.1.1 无线网络分类	180
8.1.2 无线网络特点	181
8.2 无线网络标准	181
8.2.1 IEEE802.11 协议	181
8.2.2 蓝牙协议	184
8.2.3 HiperLAN	184
8.2.4 HomeRF	185
8.3 无线网络的安全威胁	186
8.3.1 无线网络的安全脆弱性	186
8.3.2 无线网络的安全需求	186
8.3.3 无线网络的安全威胁	187
8.3.4 无线保护接入安全机制	191
8.4 无线网络安全技术应用案例	194
思考题	198

第9章 常用系统的网络安全策略

9.1 Windows 操作系统安全策略	199
9.2 网站系统安全策略	202
9.2.1 网站系统的安全隐患	202
9.2.2 网站系统的安全策略	203
9.3 电子邮件系统安全策略	206
9.4 电子商务系统安全策略	209
9.5 电子办公系统的安全策略	213
思考题	219

计算机网络安全设计篇

第10章 网络安全设计概论

10.1 网络安全设计的目标和原则	221
10.1.1 网络安全设计的目标	221



10.1.2 网络安全设计的原则	222
10.2 网络安全设计的内容和步骤	224
10.2.1 网络安全设计的内容	224
10.2.2 网络安全设计的步骤	226
10.3 网络安全设计的风险分析	228
思考题	230

第 11 章 物理安全设计

11.1 机房环境	231
11.1.1 机房场地安全	231
11.1.2 机房环境安全	232
11.1.3 机房安全	235
11.2 物理实体	240
11.2.1 设备布置安全	240
11.2.2 设备供电安全	241
11.2.3 网络设备安全	241
11.2.4 传输介质安全	243
11.2.5 存储介质安全	248
11.2.6 设备防盗窃和防破坏	250
11.2.7 设备防电磁辐射	250
11.2.8 设备监控安全	251
11.3 物理访问	252
11.3.1 实体访问控制	253
11.3.2 信息访问控制	254
11.4 综合实例	255
思考题	258

第 12 章 网络安全设计

12.1 网络系统结构	259
12.1.1 网络系统结构概述	259
12.1.2 安全区域划分	261
12.1.3 物理隔离	263
12.1.4 带宽管理	274
12.2 网络系统访问控制	277



12.2.1 网络访问控制	277
12.2.2 拨号访问控制	281
12.2.3 网络边界安全	283
12.3 网络系统入侵防范	284
12.3.1 入侵防范概述	284
12.3.2 网络入侵防范系统	286
12.3.3 入侵防御设计实例	288
思考题	290

第 13 章 主机安全设计

13.1 主机安全系统的结构	291
13.2 主机身份鉴别	292
13.2.1 主机身份鉴别概念及其基本要求	292
13.2.2 主机身份鉴别的方式	293
13.3 主机访问控制	295
13.3.1 主机访问控制概念及其基本要求	295
13.3.2 主机访问控制的主要类型	295
13.3.3 主机访问控制的主要措施	296
13.4 主机安全审计	297
13.4.1 主机安全审计概念及其基本要求	297
13.4.2 主机安全审计的基本步骤	298
13.4.3 主机安全审计策略	300
13.5 主机入侵防范	301
13.5.1 主机入侵防范概念及其基本要求	302
13.5.2 主机入侵防范的工作原理	302
13.5.3 主机入侵防范系统的主要功能及性能指标	302
13.5.4 主机入侵防范系统的评价准则	303
13.6 Windows 系统主机安全设计	304
13.6.1 Windows 系统安全策略配置	304
13.6.2 Windows 系统身份鉴别	308
13.6.3 Windows 系统的访问控制策略	313
13.6.4 Windows 系统的安全审计策略	318
13.6.5 Windows 系统的入侵防范	321

思考题	327
实验题	327

第 14 章 应用安全设计

14.1 应用身份验证	328
14.1.1 应用身份验证概念及其基本要求	328
14.1.2 应用身份验证的方式及措施	329
14.2 应用访问控制	331
14.2.1 应用访问控制概念及其基本要求	331
14.2.2 应用访问控制的主要措施	331
14.2.3 应用访问控制的基本功能	333
14.3 应用安全审计	334
14.3.1 应用安全审计概念及其基本要求	334
14.3.2 应用安全审计的基本功能	334
14.3.3 应用安全审计的基本流程	335
14.3.4 应用安全审计的总体目标	336
14.4 应用系统容错	337
14.4.1 应用系统容错概念及其基本要求	337
14.4.2 应用系统容错原理	338
14.4.3 应用系统容错的设计准则	338
14.4.4 应用系统容错的设计方法	339
14.4.5 应用系统容错的实现技术	341
14.4.6 应用系统容错评价指标	342
14.5 WEB 应用安全设计实例	344
14.5.1 WEB 浏览器安全配置	345
14.5.2 WEB 服务器安全配置	353
14.5.3 WEB 应用程序安全设计	359
思考题	368
实验题	368

第 15 章 数据安全设计

15.1 数据完整性	369
15.1.1 导致数据不完整的因素	369
15.1.2 鉴别数据完整性的技术	371



15.1.3 提高数据完整性的方法	371
15.1.4 检测数据完整性的工具	374
15.2 数据保密性	375
15.2.1 文件加密	375
15.2.2 通信加密	377
15.2.3 数据通信安全技术	379
15.3 数据备份与恢复	381
15.3.1 数据备份概述	381
15.3.2 数据恢复概述	381
15.3.3 备份系统结构	382
15.3.4 数据备份策略	383
15.3.5 数据备份方案设计	384
15.3.6 数据容灾系统	386
15.3.7 实例介绍一:使用 Windows Vista 备份工具备份数据	389
15.3.8 实例介绍二:使用 Windows Vista 还原工具还原数据	392
15.4 网络数据存储安全	395
15.4.1 直接附加存储 DAS	395
15.4.2 网络附加存储 NAS	395
15.4.3 存储区域网络 SAN	397
15.4.4 实例介绍:NAS 在校园网中的应用	399
思考题	400

第 16 章 网络安全系统设计方案编写及案例

16.1 网络安全系统设计方案编写	401
16.1.1 网络安全系统设计方案的基本特征	401
16.1.2 网络安全系统设计方案的基本构成及其编写要点	402
16.1.3 网络安全系统设计方案的质量要求	403
16.1.4 网络安全系统设计方案的评价准则	404
16.2 M 集团公司网络安全系统设计方案	405
16.2.1 概述	405
16.2.2 M 集团公司的网络安全现状及风险分析	406
16.2.3 M 集团公司的网络安全结构框架设计	409
16.2.4 M 集团公司网络安全系统的安全策略设计	417



16.2.5 M 集团公司网络安全系统的实施与管理服务	421
16.2.6 附录	424

计算机网络安全实验篇

实验一 网络信息探测实验	426
实验二 入侵检测实验	430
实验三 网络监听实验	442
实验四 邮件加密实验	450
实验五 虚拟机的安装和使用	460
实验六 SSL 软件安装及使用	473
实验七 古典加密算法实验	476
实验八 对称加密算法实验	481
实验九 非对称加密算法实验	487
实验十 VLAN 基础配置实验	492
实验十一 PKI 证书进行 IKE 协商认证实验	499
实验十二 防火墙配置实验 1	508
实验十三 防火墙配置实验 2	512
参考文献	517

计 算 机 网 络 安 全

技 术 篇

Skill

随着计算机的普及和计算机网络技术的发展，网络给用户带来了方便的同时，也给用户带来了诸多的不便以及相关安全问题。网络安全技术主要包括主机安全技术、认证技术、访问控制技术、密码与加解密技术、防火墙技术、入侵检测技术等学科内容的综合技术。

本篇将介绍计算机网络基础、网络安全技术概述、密码技术、防火墙技术、反病毒技术、无线网络安全技术、常用系统的网络安全策略等内容。

