

网络安全 概论

李 涛 编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

安全技术大系

国家自然科学基金
教育部博士点基金

资助项目

网络安全概论

李涛 编著

电子工业出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书全面系统地介绍了网络安全的概念、原理及体系架构,详细论述了密码技术、公钥基础设施(PKI)、特权管理基础设施(PMI)、网络层安全性问题,以及 Web、电子邮件、数据库安全和操作系统的安全性问题,并对最新的防火墙技术、网络攻击技术和黑客入侵检测技术、计算机取证技术以及数据备份与恢复技术进行了全面的阐述。

本书取材新颖,内容丰富,可作为高等学校计算机、信息技术类本科生、研究生教材,亦可供网络安全领域专业科研人员参考使用。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究。

图书在版编目(CIP)数据

网络安全概论 / 李涛编著. —北京: 电子工业出版社, 2004.11

(安全技术大系)

ISBN 7-121-00374-0

I.网... II.李... 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(2004)第 095707 号

责任编辑: 孙学瑛

印 刷: 北京天竺颖华印刷厂

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

经 销: 各地新华书店

开 本: 787×980 1/16 印张: 31 字数: 623 千字

印 次: 2004 年 11 月第 1 次印刷

印 数: 5000 册 定价: 42.00 元

凡购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系。联系电话:(010) 68279077。质量投诉请发邮件至 zlts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

序

随着网络经济和网络社会时代的到来, Internet 将会进入一个无处不有、无所不在的境地。经济、文化、军事和社会活动将会强烈地依赖计算机网络, 作为国家重要基础设施的网络的安全和可靠性问题已成为世界各国共同关注的焦点。而 Internet 原有的跨国界、无主管性、不设防、缺乏法律约束性, 为各国带来机遇的同时也带来了巨大的风险。

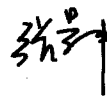
在信息网络已成为国家重要基础设施的情况下, 信息战将是一种跨国界、隐蔽性、低花费和跨领域(军事、经济、社会、资源)的无硝烟的战争。其高技术性和战争情报的不确定性给信息战的防御带来了较大的难度。美国国防部专门组织了“信息战执行委员会”研究国家信息战的战略, 并对所属网络和 Internet 网点进行了大量的攻击演练。国家级金融支付中心、证券交易中心、空中管制中心、电信网管中心、铁路调度中心、军事指挥中心等必将成为信息战的主要攻击目标。我国在信息化进程中对此必须早有准备。

近年来, 随着 Internet 的发展, 利用网络安全的脆弱性, 黑客在网上的攻击活动每年正以 10 倍的速度增长。形形色色的黑客攻击者是一个各怀鬼胎的复杂群体, 把网上任何漏洞和缺陷作为靶子, 无孔不入。如: 修改网页进行恶作剧, 非法进入主机破坏程序, 窜入银行网络转移资金, 窃取网上信息兴风作浪, 进行电子邮件骚扰, 阻塞用户和窃取密码等等。政府、军事和金融网络更是他们攻击的主要目标。

网络安全是一门新兴的交叉性学科, 综合运用了数学、物理、生物、通讯及计算机技术等诸多学科的基础理论和最新研究成果, 同时还涉及政治、法律、军事等复杂层面。显然, 若没有长期、系统、深入的研究和应用实践, 要全面论述网络安全的理论与技术是不可能的。

《网络安全概论》是李涛教授及其所领导的计算机网络与安全研究所多年来潜心网络安全理论与技术的研究成果, 对网络安全的各个层面进行了全面的论述。本书选材新颖、内容翔实、覆盖面广, 既详细论述了网络安全的基础理论, 同时又对网络安全的应用技术及研究前沿进行了准确的评价。全书层次结构清晰, 行文流畅, 篇、章相对独立, 阅读容易。

《网络安全概论》是近年来网络信息安全领域中一本难得的好书，可作为大学计算机专业教材，为我国的网络安全专业人才的培养提供了有力的支持。



中国科学院院士

前 言

网络安全关系到国家安全。网络安全的理论及其应用技术研究,不仅受到学术界以及工业界的关注,同时也受到各国政府的高度重视。为了本国的利益,美国等西方发达国家将网络安全技术及产品视为如同核武器一样的秘密技术,立法限制其向我国出口,换句话说,凡出口到我国的网络安全产品均是不安全的。为保障我国网络基础设施的安全,国家安全部、公安部等明确要求使用国产的网络安全产品来确保我国网络的安全。

然而,由于种种原因,目前我国有关网络安全技术及其产品的研发与美国等西方发达国家相比尚有一定的距离。正因为如此,我们更应加倍努力,迎头赶上。

在这种背景下,为促进我国网络安全技术的进步,在国家自然科学基金、教育部博士点基金的资助下,笔者结合自己多年来在网络安全研究中的心得,特编拙著,以期抛砖引玉,为我国的网络安全事业尽一点微薄之力。

全书共四篇 13 章。第一篇论述了网络安全的基础理论,共 3 章:第 1 章阐述了网络安全面临的威胁、网络安全服务和网络安全的基本模型;第 2 章就网络安全的基础——密码技术和信息隐藏技术进行了较为详细的讨论;第 3 章全面论述了公钥基础设施 PKI 的定义、内容和服务,同时介绍了特权管理基础设施 PMI。

第二篇讨论了网络安全的应用,共 3 章:第 4 章着重阐述了安全电子邮件的工作模式、相关的一些协议、标准和评估准则;第 5 章探讨了 IP 层的安全问题,重点阐述了 IPSec 协议的体系结构、原理和应用方式,同时就 VPN 技术以及下一代 IP 规范 IPv6 进行了讨论;第 6 章讨论了 Web 安全的实现方法,并详细阐述了 SSL、TLS、SET 等 Web 安全实现技术,最后就 SSL/TLS 的开放源码软件包 OpenSSL 进行了讨论。

第三篇就操作系统以及数据库安全问题进行了专题讨论,共 2 章:第 7 章分析了操作系统的安全机制,阐述了安全操作系统的设计原则、方法,并探讨了 Windows、UNIX、Linux 操作系统的一些安全漏洞;第 8 章阐述了数据库安全,讨论了常用的数据库安全措施,并介绍了数据库加密、DBMS 隐通道审计等前沿内容,随后分析了流行数据库 ORACLE 的安全性。

第四篇详细论述了网络安全的防护技术,共 5 章:第 9 章阐述了防火墙技术,包括防火墙的定义、功能、体系架构及其实现技术;第 10 章探讨了几种常见的网络攻击技术,包括扫描技术、拒绝服务攻击、缓冲区溢出攻击、嗅探器攻击等,并简要阐述了计算机病毒的特点、分类及防治办法;第 11 章就入侵检测技术进行了讨论,包括基于专家系统、神经网络、人工免疫等最新的 IDS 技术,并详细分析了 Linux 下的一个入侵检测系统——snort,剖析了其基本原理及实现技术;第 12 章探讨了网络安全的前沿技术——计

算机取证,详细阐述了计算机取证的原则、方法、步骤等,简要介绍了常用的取证工具,并阐述了证据分析的方法;第13章讨论了数据备份和恢复技术,并就目前的热门技术——容灾系统进行了讨论,详细介绍了容灾等级的定义,容灾计划的制订步骤等。

笔者非常感谢杨频副教授(博士)、赵辉博士、刘念博士、张建华博士、赵奎博士、胡晓勤博士,以及研究生甘玲、杨立、王健、浦海挺、李敏榆、廖竣锴、丁菊玲、仰石、肖康等人的努力。他们为本书收集了大量的文献、资料,并进行了细致的整理工作。笔者还要特别感谢研究生刘莎、郭京、王丹丹、刘颖娜、杨进、漆莲芝、周念念、王丽辉、杜雨、卢正添、王志明对本书进行了繁琐的校对工作,为本书的最后出炉作出了贡献。

由于书稿涉及许多新的内容和研究领域,尽管笔者已经尽了最大的努力,但仍感问题难免,望各位同仁不吝赐教,以利再版修订,为我国的网络安全事业共同出力。

笔 者

目 录

第一篇 网络安全基础	1
第1章 概述	3
1.1 网络安全的含义	3
1.2 影响网络安全的因素	4
1.2.1 网络系统自身的脆弱性	4
1.2.2 安全威胁	6
1.3 网络安全模型	10
1.4 网络安全服务	11
1.4.1 保密性	11
1.4.2 身份验证	12
1.4.3 完整性	12
1.4.4 不可抵赖性	13
1.4.5 访问控制	13
1.4.6 可用性	13
1.5 安全评估标准	14
1.5.1 可信任计算机标准评估准则 (TCSEC)	14
1.5.2 国家标准	16
1.6 网络安全体系结构	17
1.6.1 概述	17
1.6.2 ISO/OSI 安全体系结构	17
1.6.3 因特网安全体系结构	23
1.7 物理安全	24
1.8 网络安全	26
1.8.1 内外网隔离及访问控制系统	26
1.8.2 内部网不同网络安全域的隔离及访问控制	26
1.8.3 网络安全检测	27
1.8.4 安全审计	30
1.8.5 网络反病毒	31
1.8.6 网络备份系统	32
1.9 信息安全	32

1.9.1 鉴别	32
1.9.2 数据传输安全系统	33
1.9.3 数据存储安全系统	35
1.9.4 信息内容审计系统	35
1.10 安全管理	37
1.10.1 安全管理的基本内容	37
1.10.2 安全管理原则	39
1.10.3 安全管理的实现	40
1.11 动态安全体系结构模型	42
1.11.1 基于时间的 PDR 模型	42
1.11.2 P2DR 模型	43
1.11.3 动态自适应安全模型	44
1.11.4 全网动态安全体系 APPDRR 模型	45
1.11.5 信息安全保障体系 IA 与 PDRR 模型	46
1.12 小结	46
第 2 章 密码技术	48
2.1 密码技术的起源和历史	48
2.2 对称密码	48
2.2.1 基本原理	49
2.2.2 分组密码	49
2.2.3 流密码	58
2.3 公钥密码	62
2.3.1 基本原理	62
2.3.2 常见的公钥密码算法	63
2.3.3 应用比较	68
2.3.4 公钥密码、对称密码技术比较	69
2.4 消息验证和数字签名	71
2.4.1 消息验证	71
2.4.2 数字签名	76
2.5 信息隐藏	80
2.5.1 基本概念	80
2.5.2 历史回顾	82
2.5.3 信息隐藏分类	82

2.5.4	发展现状	83
2.6	数字水印	84
2.6.1	术语	84
2.6.2	模型	85
2.6.3	历史回顾	86
2.6.4	数字水印分类	86
2.6.5	发展现状	87
2.6.6	数字水印设计准则	88
2.6.7	数字水印评估	89
2.7	小结	90
第3章	公钥基础设施 PKI	91
3.1	概述	91
3.1.1	安全需求	91
3.1.2	PKI 的定义	92
3.1.3	PKI 的内容	93
3.2	PKI 服务	96
3.2.1	认证	96
3.2.2	完整性	97
3.2.3	保密性	98
3.2.4	不可否认性	98
3.2.5	安全时间戳	99
3.2.6	安全公证	99
3.3	证书和密钥管理	100
3.3.1	数字证书	100
3.3.2	证书管理	103
3.3.3	密钥管理	108
3.4	信任模型	110
3.4.1	严格层次信任模型	110
3.4.2	分布式信任模型	111
3.4.3	以用户为中心的信任模型	112
3.4.4	交叉认证	113
3.5	特权管理基础设施 PMI	113
3.5.1	属性证书与 PMI	114

3.5.2 PMI 模型	118
3.6 小结	120
第二篇 网络安全应用	121
第4章 电子邮件安全	123
4.1 电子邮件概述	123
4.1.1 系统组成与工作模式	123
4.1.2 相关协议与标准	124
4.1.3 安全需求	132
4.2 电子邮件安全	132
4.2.1 安全电子邮件工作模式	133
4.2.2 PEM	136
4.2.3 PGP	137
4.2.4 S/MIME	143
4.2.5 MOSS	148
4.3 安全电子邮件系统	152
4.3.1 邮件服务器安全	152
4.3.2 安全电子邮件的发送与接收	154
4.4 小结	154
第5章 IP 安全	156
5.1 概述	156
5.1.1 IP 安全概述	156
5.1.2 IPSec 的作用方式	157
5.1.3 IPSec 的实施	158
5.1.4 IPSec 的优势	159
5.2 IPSec 安全体系结构	159
5.2.1 IPSec 协议的组成	159
5.2.2 IPSec 的相关标准	160
5.3 IPSec 服务	161
5.3.1 机密性保护	161
5.3.2 完整性保护及身份验证	161
5.3.3 抗拒绝服务攻击 DoS	162
5.3.4 防止中间人攻击	162
5.3.5 完美向前保密	162

5.4 安全关联与策略	163
5.4.1 SA 参数	163
5.4.2 SA 的管理	164
5.4.3 安全策略数据库	165
5.4.4 SA 选择器	165
5.5 验证头 AH	166
5.5.1 AH 功能	166
5.5.2 AH 的头格式	166
5.5.3 AH 的两种模式	167
5.5.4 AH 的处理过程	168
5.6 封装安全有效载荷 ESP	169
5.6.1 ESP 功能	169
5.6.2 ESP 的头格式	169
5.6.3 ESP 的两种模式	170
5.6.4 ESP 的处理过程	171
5.7 因特网密钥交换协议 IKE	172
5.7.1 ISAKMP 协议	173
5.7.2 IKE	175
5.8 VPN 技术	177
5.8.1 VPN 概述	177
5.8.2 VPN 的解决方案	178
5.9 IPv6	181
5.9.1 IPv6 概述	181
5.9.2 IPv6 的新特性	181
5.10 小结	183
第 6 章 Web 安全	184
6.1 概述	184
6.1.1 Web 安全威胁	184
6.1.2 Web 安全的实现方法	185
6.2 SSL 技术	186
6.2.1 SSL 概述	186
6.2.2 SSL 体系结构	187
6.2.3 SSL 记录协议	189

6.2.4	更改密码规格协议	191
6.2.5	警告协议	191
6.2.6	SSL 握手协议	192
6.2.7	SSL 协议的安全性	194
6.3	TLS 协议	195
6.3.1	版本号	195
6.3.2	MAC 计算	195
6.3.3	伪随机函数 PRF	196
6.3.4	警告码	196
6.3.5	密码组	196
6.3.6	客户端证书类型	196
6.3.7	certificate_verify 和结束消息	197
6.3.8	密码计算	197
6.3.9	填充	197
6.4	安全电子交易 SET	197
6.4.1	SET 交易流程	198
6.4.2	双重签名	200
6.5	OpenSSL 简介	201
6.5.1	OpenSSL 概述	201
6.5.2	OpenSSL 命令接口	204
6.5.3	OpenSSL 应用程序接口	212
6.6	小结	221
第三篇	系统安全	223
第 7 章	操作系统安全	225
7.1	概述	225
7.1.1	术语	225
7.1.2	安全操作系统的发展状况	227
7.2	操作系统的安全机制	231
7.2.1	身份鉴别机制	231
7.2.2	访问控制机制	232
7.2.3	最小特权管理机制	237
7.2.4	可信通路机制	238
7.2.5	隐通道的分析与处理	238

7.2.6 安全审计机制	242
7.3 操作系统的安全设计	244
7.3.1 基本概念	245
7.3.2 设计原则	246
7.3.3 安全模型	247
7.3.4 设计方法	250
7.3.5 安全评测	252
7.4 操作系统的常见安全漏洞及对策	253
7.4.1 UNIX/Linux 常见安全漏洞及对策	253
7.4.2 Windows 系统常见安全漏洞及对策	258
7.5 小结	263
第 8 章 数据库安全	264
8.1 概述	264
8.1.1 安全威胁	265
8.1.2 安全级别	266
8.2 存取控制	267
8.3 数据完整性	268
8.4 数据库审计	268
8.4.1 审计类别	269
8.4.2 可审计事件	269
8.4.3 审计数据的内容	270
8.4.4 审计与 DBMS 体系结构的关系	270
8.4.5 常用审计技术	272
8.4.6 审计的分析	272
8.5 数据库加密	273
8.5.1 基本要求	273
8.5.2 加密层次	275
8.5.3 数据项加密	275
8.5.4 加密影响	276
8.6 DBMS 的隐通道审计	277
8.6.1 数据库中的存储隐通道	277
8.6.2 审计存储隐通道的必要性	278
8.6.3 审计存储隐通道应解决的一般问题	279

8.6.4	DBMS 中审计存储隐通道的特有问题的	281
8.6.5	数据库系统中存储隐通道的审计分析的	283
8.6.6	存储隐通道的审计分析流程的	284
8.6.7	DBMS 审计记录方法的	284
8.7	Oracle 数据库的安全性的	285
8.7.1	存取控制的	285
8.7.2	特权和角色的	287
8.7.3	审计的	288
8.7.4	数据完整性的	288
8.8	小结的	291
第四篇	网络安全防护的	293
第 9 章	防火墙技术的	295
9.1	概述的	295
9.1.1	防火墙的功能和策略的	295
9.1.2	防火墙的局限性的	297
9.2	防火墙的分类的	297
9.2.1	包过滤防火墙的	298
9.2.2	代理防火墙的	300
9.3	防火墙的体系结构的	301
9.3.1	双宿/多宿主主机模式的	302
9.3.2	屏蔽主机模式的	302
9.3.3	屏蔽子网模式的	303
9.4	防火墙的规则	303
9.4.1	逻辑过滤规则的	304
9.4.2	文件过滤规则的	305
9.4.3	内存过滤规则的	307
9.5	防火墙的实现技术的	310
9.5.1	基于 MS Windows 的防火墙技术的	310
9.5.2	基于 Linux 的防火墙技术的	313
9.6	小结的	322
第 10 章	攻击技术的	323
10.1	黑客攻击技术的	323
10.1.1	扫描技术的	323

10.1.2	拒绝服务 DoS 攻击技术	325
10.1.3	缓冲区溢出	328
10.1.4	嗅探器攻击 sniffer	330
10.2	黑客攻击工具	332
10.2.1	扫描工具	332
10.2.2	DoS 攻击工具	335
10.3	计算机病毒	338
10.3.1	发展简述	338
10.3.2	特点	339
10.3.3	分类	340
10.3.4	防治	342
10.4	小结	345
第 11 章	入侵检测技术	346
11.1	概述	347
11.1.1	IDS 功能与模型	347
11.1.2	IDS 系统结构	348
11.1.3	发展方向	349
11.2	IDS 的基本原理	350
11.2.1	监测策略	350
11.2.2	IDS 类型	353
11.2.3	IDS 基本技术	356
11.3	snort 入侵检测系统	363
11.3.1	概述	363
11.3.2	安装和使用	363
11.3.3	snort 规则	375
11.3.4	snort 的模块结构	377
11.3.5	snort 的总体流程	379
11.4	小结	382
第 12 章	计算机取证	384
12.1	电子证据	385
12.1.1	电子证据的概念	386
12.1.2	电子证据的特点	386
12.1.3	常见电子证据	388

12.2 计算机取证原则	389
12.2.1 获取证物	391
12.2.2 分析证物	392
12.2.3 保存证物	392
12.3 计算机取证步骤	392
12.3.1 证据的获取	393
12.3.2 位拷贝	394
12.3.3 分析检查	394
12.3.4 取证提交	395
12.3.5 证据存档	396
12.3.6 证据呈供	396
12.4 计算机取证方法	396
12.4.1 取证模型	396
12.4.2 取证方法	398
12.5 证据分析	401
12.5.1 一般的证据分析技术	401
12.5.2 电子证据分析的工具	402
12.5.3 日志系统分析	402
12.5.4 一种支持计算机取证的日志系统	407
12.5.5 电子证据审查	408
12.6 计算机取证常用工具	408
12.6.1 软件取证工具	408
12.6.2 硬件取证工具	415
12.7 计算机取证的法律问题	416
12.7.1 电子证据的真实性	416
12.7.2 电子证据的证明力	418
12.7.3 取证工具的法律效力	419
12.7.4 其他困难和挑战	421
12.8 小结	422
第 13 章 数据备份及恢复	423
13.1 概述	423
13.1.1 数据完整性	423
13.1.2 数据备份	426