



网络安全技术 概论

南湘浩 陈钟 编著

A Profile to Network Security Techniques

国防工业出版社

网络安全技术概论

A Profile to Network Security Techniques

南湘浩 陈 钟 编著

国防工业出版社

·北京·

图书在版编目(CIP)数据

网络安全技术概论/南湘浩,陈钟编著. —北京:国防工业出版社,2003.7

ISBN 7-118-03144-5

I.网... II.①南... ②陈... 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(2003)第 032852 号

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号)

(邮政编码 100044)

新艺印刷厂印刷

新华书店经售

*

开本 850×1168 1/32 印张 11 $\frac{1}{4}$ 300 千字
2003 年 7 月第 1 版 2003 年 7 月北京第 1 次印刷
印数:1—3000 册 定价:30.00 元

(本书如有印装错误,我社负责调换)

致 读 者

本书由国防科技图书出版基金资助出版。

国防科技图书出版工作是国防科技事业的一个重要方面。优秀的国防科技图书既是国防科技成果的一部分,又是国防科技水平的重要标志。为了促进国防科技和武器装备建设事业的发展,加强社会主义物质文明和精神文明建设,培养优秀科技人才,确保国防科技优秀图书的出版,原国防科工委于1988年初决定每年拨出专款,设立国防科技图书出版基金,成立评审委员会,扶持、审定出版国防科技优秀图书。

国防科技图书出版基金资助的对象是:

1. 在国防科学技术领域中,学术水平高,内容有创见,在学科上居领先地位的基础科学理论图书;在工程技术理论方面有突破的应用科学专著。

2. 学术思想新颖,内容具体、实用,对国防科技和武器装备发展具有较大推动作用的专著;密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。

3. 有重要发展前景和有重大开拓使用价值,密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。

4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在总装备部的领导下开展工作,负责掌握出版基金的使用方向,评审受理的图书选题,决定资助的图书选题和资助金额,以及决定中断或取消资助等。经评审给予资助的图书,由总装备部国防工业出版社列选出版。

国防科技事业已经取得了举世瞩目的成就。国防科技图书承

担着记载和弘扬这些成就,积累和传播科技知识的使命。在改革开放的新形势下,原国防科工委率先设立出版基金,扶持出版科技图书,这是一项具有深远意义的创举。此举势必促使国防科技图书的出版随着国防科技事业的发展更加兴旺。

设立出版基金是一件新生事物,是对出版工作的一项改革。因而,评审工作需要不断地摸索、认真地总结和及时地改进,这样,才能使有限的基金发挥出巨大的效能。评审工作更需要国防科技和武器装备建设战线广大科技工作者、专家、教授,以及社会各界朋友的热情支持。

让我们携起手来,为祖国昌盛、科技腾飞、出版繁荣而共同奋斗!

国防科技图书出版基金

评审委员会

国防科技图书出版基金 第四届评审委员会组成人员

名誉主任委员	陈达植			
顾问	黄宁			
主任委员	刘成海			
副主任委员	王峰	张涵信	张又栋	
秘书长	张又栋			
副秘书长	彭华良	蔡镛		
委员	于景元	王小谟	甘茂治	冯允成
(按姓名笔画排序)	刘世参	杨星豪	李德毅	吴有生
	何新贵	佟玉民	宋家树	张立同
	张鸿元	陈火旺	侯正明	常显奇
	崔尔杰	韩祖南	舒长胜	

前 言

本书是解放军信息工程大学信息安全实验室和北京大学计算机系信息安全实验室合作编写的。本书共分 10 章,参与编写的人员有北京大学计算机科学技术系信息安全实验室王昭博士后(病毒防治)、唐礼勇博士(安全网关)、唐文博士生(公钥快速算法)、颜强博士(安全评估)、胡建斌博士(入侵检测)、信息工程大学信息安全实验室陆浪如博士(安全模型)、李益发博士(鉴别逻辑)、徐志大博士(虚拟专网)。

本书在写作过程中,把教学、科研、工程结合起来,边研究边写作,是集体创作的成果。信息安全或网络安全技术是一个很大的题目,特别是在开放的互联网条件下提出了很多新问题,在一本书中很难做到系统而全面,因而只能抓住几个前沿的关键题目进行讨论。在本书中有的问题只是作为课题提出来,有的问题只做了一些初步探讨,有的问题则得出了比较明晰的结论,对今后的深入研究具有一定参考意义。

在信息安全领域中,法律、管理起着十分重要的作用。但是本书作为安全技术概论,着重于技术方面,有关法律法规、行政管理等方面的内容没有包括在本书中。

目 录

引言	1
第 1 章 公钥密码	7
1.1 基于 IFP 的算法	7
1.1.1 RSA 算法理论	7
1.1.2 RSA 相关计算	9
1.1.3 RSA 算法应用	11
1.2 基于 DLP 的算法	13
1.2.1 D-H 方案	13
1.2.2 Massey-Omura 方案	14
1.2.3 ElGamal 方案	15
1.2.4 DSS 方案(DSA)	15
1.3 基于 ECDLP 的算法	16
1.3.1 ECC 算法理论	17
1.3.2 ECC 计算方法	17
1.3.3 ECC 算法应用	21
1.3.4 算法效能比较	24
第 2 章 密钥管理	26
2.1 密钥管理构架(KMI)	28
2.1.1 静态配置	28
2.1.2 动态分发	33
2.2 公钥构架(PKI)	38
2.2.1 CA 公钥证书	39
2.2.2 密码模件	43
2.2.3 PKI 进展	48

2.3	种子公钥(SPK)	51
2.3.1	RSA 多重公钥(LPK)	52
2.3.2	离散对数组合公钥(CPK)	56
2.3.3	椭圆曲线组合公钥	57
2.3.4	种子公钥在电子政务中的应用	63
2.4	密钥的管理体制	67
2.4.1	管理模式	67
2.4.2	管理模式比较	69
2.4.3	管理模式应用	73
第3章	鉴别逻辑	78
3.1	主体鉴别	80
3.1.1	一般概念	80
3.1.2	主体鉴别特点	81
3.2	信任逻辑	83
3.2.1	问题的提出	83
3.2.2	认证链和信任链	84
3.2.3	信任的类型	85
3.2.4	信任的建立	88
3.2.5	鉴别协议	89
3.3	客体鉴别	94
3.3.1	一般概念	94
3.3.2	协议和分类	95
3.3.3	通信协议及其分类	96
3.3.4	密码协议及其安全性	97
3.3.5	协议分析的基本方法	98
3.4	BAN类逻辑	99
3.4.1	BAN逻辑	99
3.4.2	GNV逻辑	102
3.4.3	AT逻辑	107
3.4.4	SVO逻辑	110

3.5	Li 逻辑	113
3.5.1	基本概念和记号	113
3.5.2	消息及其相关概念	116
3.5.3	公式及其相关概念	117
3.5.4	鉴别系统的二阶语言	121
3.5.5	公理集	122
3.5.6	系统的演绎定理	125
3.5.7	协议安全性的一般讨论	127
3.5.8	协议分析的前提假设	129
第 4 章	安全模型	133
4.1	Bell-LaPadula 模型和 Biba 模型	133
4.1.1	Bell-LaPadula 模型	133
4.1.2	Biba 模型	139
4.2	信息流控制的格模型	143
4.2.1	形式定义	144
4.2.2	安全模型定义	145
4.2.3	格导出	145
4.2.4	隐含流和明确流	147
4.3	面向对象的安全模型	149
4.3.1	主体	149
4.3.2	客体	150
4.3.3	访问模型	151
4.3.4	授权	153
4.3.5	隐含授权规则	156
4.3.6	特权继承及复合客体	158
4.4	新一代安全模型	160
4.4.1	新一代模型简介	161
4.4.2	Iris 授权模型	162
4.4.3	数据隐藏模型	164
4.4.4	消息过滤模型	165

第 5 章 安全网关	171
5.1 控制原理和目标	171
5.1.1 出入关控制原理	171
5.1.2 网关安全目标	174
5.2 模型设计	177
5.2.1 模型元素	177
5.2.2 系统状态	178
5.2.3 动态运行过程	180
5.2.4 模型的实施	181
5.3 关键技术与实现	186
5.3.1 安全核心设计	186
5.3.2 不同层次下的出入关控制	194
5.3.3 应用示例	199
第 6 章 虚拟专网	203
6.1 概述	203
6.2 类型	205
6.2.1 Access VPN	206
6.2.2 Intranet VPN	206
6.2.3 Extranet VPN	207
6.3 协议	208
6.3.1 L2TP	209
6.3.2 GRE	211
6.3.3 MPLS	212
6.3.4 IPSec	213
6.3.5 协议成熟程度与应用	229
6.4 展望	230
第 7 章 入侵检测	232
7.1 入侵检测原理与技术	232
7.1.1 入侵检测的起源	232
7.1.2 入侵检测的分类	234

7.1.3	入侵检测的数学模型	242
7.1.4	入侵检测系统的需求特性	243
7.1.5	入侵检测的现状	245
7.2	入侵检测的响应机制	246
7.2.1	对响应的需求	246
7.2.2	自动响应	246
7.2.3	蜜罐	249
7.2.4	主动攻击模型	250
7.3	入侵检测标准化	251
7.3.1	CIDF 的体系结构	252
7.3.2	CIDF 的规范语言	253
7.3.3	CIDF 的通信机制	255
7.3.4	CIDF 的程序接口	257
7.4	入侵检测特征分析和协议分析	257
7.4.1	特征分析	257
7.4.2	协议分析	262
7.5	绕过入侵检测的若干技术	265
7.5.1	对入侵检测系统的攻击	265
7.5.2	对入侵检测系统的逃避	266
7.5.3	其他方法	267
第 8 章	安全评估	268
8.1	安全评估准则的发展历程	268
8.1.1	评估准则的发展过程	268
8.1.2	准则间的比较	270
8.1.3	向 CC 过渡的备忘录	271
8.2	彩虹系列	272
8.2.1	TCSEC(桔皮书)	272
8.2.2	TNI	275
8.3	信息安全评估通用准则(CC)	279
8.3.1	简介	279

8.3.2	CC 的一般模型	281
8.3.3	保护轮廓规范	289
8.3.4	安全目标规范	292
8.3.5	安全功能要求	295
8.3.6	安全自估要求	298
8.3.7	CC 认可协议	301
8.4	中国安全评估准则的体系建设	302
第 9 章	病毒防治	305
9.1	计算机病毒概述	305
9.1.1	病毒的定义	306
9.1.2	病毒的基本特征	306
9.1.3	病毒的分类	308
9.1.4	病毒的命名	315
9.1.5	病毒的发展历程	317
9.2	计算机病毒的基本原理	321
9.2.1	病毒的结构	321
9.2.2	病毒的工作流程	325
9.2.3	病毒的理论基础与作用机制	328
9.3	计算机病毒的防治对策	331
9.3.1	怎样发现病毒	331
9.3.2	病毒的防治技术	332
第 10 章	安全构件	337
10.1	基础构件	337
10.1.1	系统安全原则	338
10.1.2	安全控制指南	339
10.1.3	CobiT 构件	341
10.2	新安全构件	342
10.2.1	Parker 构件	342
10.2.2	克拉克 - 威尔逊整体构件(CWI)	345
参考文献	350

Contents

Foreword	1
Chapter 1 Public Key Algorithm	7
1.1 Algorithms Based on IFP	7
1.1.1 RSA Algorithm	7
1.1.2 Computation of RSA	9
1.1.3 Application for RSA	11
1.2 Algorithms Based on DLP	13
1.2.1 D-H Scheme	13
1.2.2 Massey-Omura Scheme	14
1.2.3 ElGamal Scheme	15
1.2.4 DSS(DSA)	15
1.3 Algorithms Based on ECDLP	16
1.3.1 ECC Algorithm	17
1.3.2 Computation of ECC	17
1.3.3 Application for ECC	21
1.3.4 Comparison for Algorithms	24
Chapter 2 Key Management	26
2.1 Key Management Infrastructure	28
2.1.1 Static Distribution	28
2.1.2 Dynamic Distribution	33
2.2 Public Key Infrastructure	38
2.2.1 CA Public Key Certificate	39
2.2.2 Cryptographic Module	43
2.2.3 PKI Procession	48

2.3	Seeded Public Key (SPK)	51
2.3.1	RSA Lapped Public Key (LPK)	52
2.3.2	DLP Combined Public Key (CPK)	56
2.3.3	ECC Combined Public Key	57
2.3.4	Application of SPK in e-Government	63
2.4	Key Management System	67
2.4.1	Key Management mode	67
2.4.2	Comparison for Key management Modes	69
2.4.3	Application of Modes	73
Chapter 3	Logic of Authentication	78
3.1	Subject Authentication	80
3.1.1	General Concepts	80
3.1.2	Characteristic of Subject Authentication	81
3.2	Logic of Trust	83
3.2.1	introduction	83
3.2.2	The Chains of Certification and Trust	84
3.2.3	The Level of Trust	85
3.2.4	The Formation of Trust	88
3.2.5	Subject Authentication Protocol	89
3.3	Object Authentication	94
3.3.1	General Concepts	94
3.3.2	Types of Protocols	95
3.3.3	Communication Protocols and the Classifications	96
3.3.4	Cryptographic Protocols and Their Security	97
3.3.5	Basic Method of Protocol Analysis	98
3.4	BAN-like Logic	99
3.4.1	BAN Logic	99
3.4.2	GNY Logic	102

3.4.3	AT Logic	107
3.4.4	SVO Logic	110
3.5	Li Logic	113
3.5.1	Basic Concepts and notations	113
3.5.2	Message and Related Concepts	116
3.5.3	Formulae and Related Concepts	117
3.5.4	Order 2 Language for Authentication Logic	121
3.5.5	Set of Axioms	122
3.5.6	Deduction Theorem of System	125
3.5.7	Discussion on Security of Protocol	127
3.5.8	Preconditions of Protocol Analysis	129
Chapter 4	Security Models	133
4.1	Bell.LaPadula and Biba Model	133
4.1.1	Bell.LaPadula Model	133
4.1.2	Biba Model	139
4.2	Lattice model for flow control	143
4.2.1	Formal Definition	144
4.2.2	Definition of Security Model	145
4.2.3	Lattice Derivation	145
4.2.4	Implicit and Explicit Flow	147
4.3	Object-oriented Security Model	149
4.3.1	Subject	149
4.3.2	Object	150
4.3.3	Models for Access	151
4.3.4	Authorizations	153
4.3.5	Rules for Implicit Authorizations	156
4.3.6	Inheritance Hierarchies and Composite Objects	158
4.4	Security Models of New Generation	160
4.4.1	Introduction to Models of New Generation	161

4.4.2	Iris Authorization Models	162
4.4.3	Models for Data-hiding	164
4.4.4	Models for Message-filtering	165
Chapter 5	Security Gateway	171
5.1	Principles and Security Goal for Entry Control	171
5.1.1	Principles	171
5.1.2	Security Goal	174
5.2	Model Designing	177
5.2.1	Elements of model	177
5.2.2	Status of System	178
5.2.3	Running Status of System	180
5.2.4	Implementation of Model	181
5.3	Key Techniques	186
5.3.1	Security Kernel Design	186
5.3.2	Entry Control of Different Levels	194
5.3.3	Application Examples	199
Chapter 6	Virtual Private Network	203
6.1	Introduction	203
6.2	Types	205
6.2.1	Access VPN	206
6.2.2	Intranet VPN	206
6.2.3	Extranet VPN	207
6.3	Protocols	208
6.3.1	L2TP	209
6.3.2	GRE	211
6.3.3	MPLS	212
6.3.4	IPSec	213
6.3.5	Maturation of Protocols	229
6.4	Expectation	230
Chapter 7	Intrusion Detection System	232