

计算机系列教材

# 网络安全原理与实践

陈伟 李频 编著



清华大学出版社

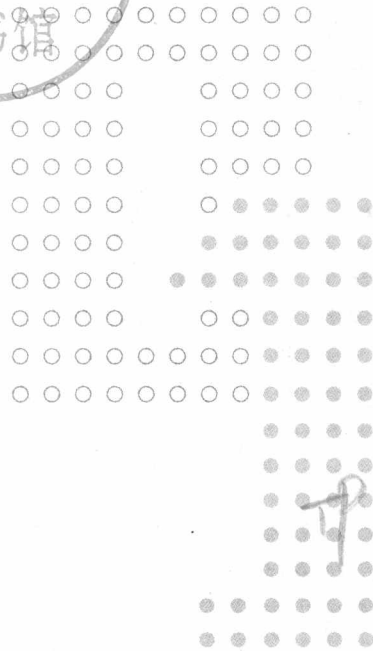
014056587

TP393.08  
719

计算机系列教材

陈伟 李频 编著

# 网络安全原理与实践



TP393.08  
719



北航 C1741443

清华大学出版社  
北京

782820410

## 内 容 简 介

本书围绕网络安全技术体系的建立,系统介绍了计算机网络安全知识和理论,全书共分17章,内容包括网络安全基础、网络安全威胁、密码学概述、对称加密、公钥密码、消息认证和散列函数、鉴别和密钥分配协议、身份认证和访问控制、PKI技术、IPSec协议、电子邮件安全、Web安全、防火墙技术、虚拟专用网、入侵检测系统和网络诱骗系统、无线网络安全、恶意代码。本书既重视基础原理和基本概念的阐述,又紧密联系当前的前沿科技知识,注重理论和实践的统一,可以有效加深学生对于网络安全的理解,培养学生的创新能力。

本书可作为信息安全、计算机、信息管理、电子商务等专业本科生和研究生的教材,也可供从事相关专业的教学、科研和工程人员参考。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

### 图书在版编目(CIP)数据

网络安全原理与实践/陈伟,李频编著. —北京:清华大学出版社,2014

计算机系列教材

ISBN 978-7-302-35654-7

I. ①网… II. ①陈… ②李… III. ①计算机网络—安全技术—高等学校—教材 IV. ①TP393.08

中国版本图书馆CIP数据核字(2014)第053008号

责任编辑:白立军 顾冰

封面设计:常雪影

责任校对:梁毅

责任印制:宋林

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦A座 邮 编:100084

社 总 机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, [c-service@tup.tsinghua.edu.cn](mailto:c-service@tup.tsinghua.edu.cn)

质量反馈:010-62772015, [zhiliang@tup.tsinghua.edu.cn](mailto:zhiliang@tup.tsinghua.edu.cn)

课件下载: <http://www.tup.com.cn>, 010-62795954

印 刷 者:北京富博印刷有限公司

装 订 者:北京市密云县京文制本装订厂

经 销:全国新华书店

开 本:185mm×260mm

印 张:20.5

字 数:511千字

版 次:2014年7月第1版

印 次:2014年7月第1次印刷

印 数:1~2000

定 价:34.50元

产品编号:054620-01

随着计算机网络的发展,信息安全越来越受到人们的关注,信息安全已成为发展最为迅速的学科领域之一。人员、技术和管理是信息安全保障的三大要素,虽然人员和管理在安全领域所扮演的角色非常重要,但技术要素才是基础,一个信息安全工程师首先必须对安全技术的功能和其弱点有深入的理解。对于信息安全专业人才培养来说,使学生掌握信息安全技术理论和应用是关键。

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,我国从此开始了信息安全本科生的培养。2002年又批准了18所高等学校建立信息安全本科专业,之后信息安全本科人才培养进入热潮阶段。在信息安全本科生培养初期,教材比较匮乏,一般信息安全专业课使用各个学校的内部讲义或面向研究生的教材,2007年后出现了大量的信息安全本科专业教材,课程涵盖密码学、系统安全、网络安全、网络攻防、信息安全实验等。

南京邮电大学2002年获批准建立信息安全本科专业,在信息安全学科专业领域,特别是网络安全方向拥有一支学术水平较高的专家队伍,承担了网络安全领域的多项科研课题,能够从事本科至博士生的多层次人才培养。我们在十多年信息安全本科生人才培养的过程中积累了一点经验,通过对多种教材的使用有了一定的心得,体会到信息安全专业是一门对实践性要求很高的学科,如果在教学中不能将理论与实践相结合,学生难以有效地掌握知识点。在编写本书之前,我们将本书定位为适应本科生教学使用,偏向网络安全、理论与实践相结合的教材。编写时以网络安全理论为本位,以实际能力为目标,注意原理联系实践,尽量多介绍一些实际问题,让读者增加感性认识。

本书围绕网络安全体系的建立展开,第1章和第2章介绍网络安全的基本概念和目前存在的网络安全威胁,后续章节可以分为三大部分,第一部分为密码学,这部分为网络安全的基础,主要包含第3~6章,本书不过多讨论密码学中的算法设计和安全性证明,重点介绍各种密码的主要思想和算法特点,目标是让读者能在不同应用场景下选择合适的密码方法;第二部分为网络安全协议,由于网络技术的出现,原有的在单机上的安全保护技术遇到了挑战,网络安全协议主要解决此类问题,主要包含第7~10章,还有第12章的部分内容;第三部分为网络安全技术,相比密码学和网络安全协议,读者在现实生活中更容易接触到这些应用技术,这些技术主要会应用在网络攻防中,主要包含第11~17章。本书适合32~64学时使用,部分章节可作为选学内容。

本书既注重网络安全基础理论,又着眼培养读者解决网络安全问题的实际能力。本书的特点是突出网络安全的特色,理论与实践相结合,文字简明通俗易懂,用循序渐进的方式叙述网络安全知识,对网络安全的原理与技术的难点的介绍适度,适合本科生教学使用。

本书由南京邮电大学计算机学院信息安全系组织编写,为南京邮电大学“十二五”规划教材,第3~6章、第15~17章由陈伟编写,其余章节由李频编写完成。本书在编写过程中参阅了大量文献,还参考了互联网上信息安全的相关资料,在此一并向作者表示衷心的感谢。硕士研究生杨龙、李晨阳、吴震雄、姜海东、顾杨、龚沛华、许若妹等参与部分文字的录入和插图绘制工作,此书的出版得到了多位专家的指导和帮助,在此一并表示感谢。

正如互联网的设计会存在漏洞一样,限于作者的水平,本书难以避免会存在错误,我们将会虚心聆听读者指出的任何一处错误,恳请广大读者批评指正。作者的E-mail为 champway@163.com, lipin7421@163.com。

作者

2013年10月

第1章 网络安全基础 /1

1.1 网络安全的概念 /1

1.2 主要的网络安全威胁 /2

1.3 TCP/IP 协议簇的安全问题 /4

1.3.1 链路层协议的安全隐患 /4

1.3.2 网络层协议的安全隐患 /5

1.3.3 传输层协议的安全隐患 /5

1.3.4 应用层协议的安全隐患 /6

1.4 OSI 安全体系结构 /7

1.4.1 安全服务 /7

1.4.2 安全机制 /7

1.5 网络安全服务及其实现层次 /8

1.5.1 机密性 /8

1.5.2 完整性 /9

1.5.3 身份认证 /9

1.5.4 访问控制 /10

1.5.5 不可否认 /10

1.5.6 可用性 /10

1.6 TCP/IP 协议簇的安全架构 /11

1.7 PPDR 安全模型 /12

1.8 可信计算机系统评价准则 /14

1.9 信息系统安全保护等级划分准则 /16

习题 /17

第2章 网络安全威胁 /18

2.1 隐藏攻击者的地址和身份 /18

2.2 踩点技术 /19

2.3 扫描技术 /19

2.3.1	主机扫描	/19
2.3.2	端口扫描	/19
2.3.3	操作系统探测	/21
2.3.4	漏洞扫描	/21
2.4	嗅探技术	/22
2.5	攻击技术	/22
2.5.1	社会工程	/23
2.5.2	口令破解	/23
2.5.3	IP 欺骗	/24
2.5.4	ARP 欺骗	/26
2.5.5	DNS 欺骗	/26
2.5.6	会话劫持	/26
2.5.7	拒绝服务攻击	/27
2.5.8	缓冲区溢出攻击	/30
2.6	权限提升	/33
2.7	掩盖踪迹	/33
2.8	创建后门	/33
2.9	Web 攻击技术	/34
2.9.1	SQL 注入攻击	/34
2.9.2	XSS 攻击	/37
	习题	/39
<b>第3章 密码学概述 /40</b>		
3.1	密码学起源	/40
3.2	密码的基本概念	/42
3.2.1	密码编码学	/42
3.2.2	密码分析学	/43
3.2.3	密钥管理学	/46
3.3	传统密码技术	/48
3.3.1	置换密码	/48

3.3.2	代换密码	/49
3.3.3	一次一密	/51
3.3.4	转轮机	/52
3.3.5	电码本	/53
	习题	/55
	<b>第4章 对称加密</b>	<b>/56</b>
4.1	流密码	/56
4.1.1	流密码结构	/57
4.1.2	RC4 算法	/59
4.2	分组密码	/60
4.2.1	数据加密标准(DES)	/61
4.2.2	三重 DES	/69
4.2.3	高级加密标准(AES)	/70
4.3	随机数和伪随机数	/76
4.3.1	随机数的应用	/77
4.3.2	真随机数发生器、伪随机数发生器和伪随机函数	/78
4.4	分组密码的工作模式	/79
4.4.1	ECB 模式	/79
4.4.2	CBC 模式	/80
4.4.3	CFB 模式	/81
4.4.4	CTR 模式	/82
	习题	/83
	<b>第5章 公钥密码</b>	<b>/85</b>
5.1	简介	/85
5.1.1	公钥密码体制的设计原理	/86
5.1.2	公钥密码分析	/89
5.2	Diffie-Hellman 密钥交换	/90



5.3	RSA	/93
5.3.1	算法描述	/93
5.3.2	RSA 算法中的计算问题	/95
5.3.3	RSA 的安全性	/96
5.4	椭圆曲线密码算法	/97
5.4.1	椭圆曲线	/97
5.4.2	有限域上的椭圆曲线	/98
5.4.3	椭圆曲线上的密码	/99
	习题	/100
<b>第 6 章 消息认证和散列函数 /102</b>		
6.1	对认证的要求	/102
6.2	消息认证码	/103
6.2.1	消息认证码的应用场景	/104
6.2.2	基于 DES 的消息认证码	/105
6.3	安全散列函数	/106
6.3.1	对散列函数的要求	/108
6.3.2	简单散列函数	/109
6.3.3	生日攻击	/109
6.3.4	SHA 安全散列算法	/111
6.3.5	HMAC	/113
6.4	数字签名	/115
6.4.1	数字签名原理	/116
6.4.2	数字签名流程	/117
	习题	/118
<b>第 7 章 鉴别和密钥分配协议 /119</b>		
7.1	鉴别协议	/119
7.1.1	Needham-Schroeder 双向鉴别协议	/120
7.1.2	改进的 Needham-Schroeder 协议	/121

- 7.1.3 单向鉴别协议 /123
- 7.2 密钥分配协议 /124
  - 7.2.1 对称密钥的分配 /124
  - 7.2.2 公开密钥的分配 /126
  - 7.2.3 使用公开加密算法分配对称密钥 /126
- 习题 /128

**第8章 身份认证和访问控制 /129**

- 8.1 单机状态下的身份认证 /129
  - 8.1.1 基于口令的认证方式 /130
  - 8.1.2 基于智能卡的认证方式 /131
  - 8.1.3 基于生物特征的认证方式 /131
- 8.2 S/KEY 认证协议 /132
  - 8.2.1 一次性口令技术 /132
  - 8.2.2 最初的 S/KEY 认证协议 /133
  - 8.2.3 改进的 S/KEY 认证协议 /134
- 8.3 Kerberos 认证协议 /135
  - 8.3.1 简单的认证会话 /136
  - 8.3.2 更加安全的认证会话 /137
  - 8.3.3 Kerberos v4 认证会话 /138
  - 8.3.4 Kerberos 的跨域认证 /140
  - 8.3.5 Kerberos 的优缺点 /141
- 8.4 访问控制 /142
  - 8.4.1 访问控制的基本原理 /142
  - 8.4.2 自主访问控制 /143
  - 8.4.3 强制访问控制 /146
  - 8.4.4 基于角色的访问控制 /148

- 习题 /151

第9章 PKI 技术 /152

- 9.1 理论基础 /152
  - 9.1.1 CA 认证与数字证书 /152
  - 9.1.2 信任关系与信任模型 /154
- 9.2 PKI 的组成 /157
  - 9.2.1 认证机构 /157
  - 9.2.2 证书库 /158
  - 9.2.3 PKI 应用接口系统 /159
- 9.3 PKI 的功能和要求 /159
  - 9.3.1 密钥和证书管理 /160
  - 9.3.2 对 PKI 的性能要求 /164
- 9.4 PKI 的优缺点 /164
- 习题 /165

第10章 IPSec 协议 /167

- 10.1 IPSec 安全体系结构 /167
  - 10.1.1 IPSec 概述 /167
  - 10.1.2 安全关联和安全策略 /168
- 10.2 IPSec 安全协议——AH /169
  - 10.2.1 AH 概述 /169
  - 10.2.2 AH 头部格式 /170
  - 10.2.3 AH 运行模式 /171
- 10.3 IPSec 安全协议——ESP /173
  - 10.3.1 ESP 概述 /173
  - 10.3.2 ESP 头部格式 /173
  - 10.3.3 ESP 运行模式 /174
- 10.4 IPSec 密钥管理协议——IKE /176
- 10.5 IPSec 的安全问题 /177
- 10.6 IPSec 的使用现状 /178
- 习题 /179

第 11 章 电子邮件安全 /180

11.1 电子邮件的安全威胁 /180

11.2 安全电子邮件标准 /181

11.3 PGP 标准 /182

11.3.1 PGP 的功能 /182

11.3.2 PGP 消息格式及收发过程 /184

11.3.3 PGP 密钥的发布和管理 /185

11.3.4 PGP 的安全性分析 /186

习题 /189

第 12 章 Web 安全 /190

12.1 Web 安全威胁 /190

12.1.1 对 Web 服务器的安全威胁 /190

12.1.2 对 Web 浏览器的安全威胁 /191

12.1.3 对通信信道的安全威胁 /191

12.2 Web 安全的实现方法 /192

12.3 SSL 协议 /193

12.3.1 SSL 概述 /193

12.3.2 更改密码规格协议 /195

12.3.3 警告协议 /195

12.3.4 SSL 记录协议 /195

12.3.5 SSL 握手协议 /196

12.3.6 SSL 的安全性分析 /198

12.3.7 TLS 协议 /200

12.4 OpenSSL 简介 /200

12.4.1 OpenSSL 结构 /201

12.4.2 OpenSSL 功能 /202

12.4.3 Windows 平台下 OpenSSL 的编译和安装 /203

12.4.4	SSL 通信的实现	/204
12.5	SET 协议	/207
12.5.1	SET 概述	/207
12.5.2	SET 的优缺点	/209
	习题	/210
<b>第 13 章</b>	<b>防火墙技术</b>	<b>/212</b>
13.1	防火墙的基本概念	/212
13.1.1	定义	/212
13.1.2	防火墙应满足的条件	/213
13.1.3	防火墙的功能	/213
13.1.4	防火墙的局限性	/214
13.2	防火墙的类型与技术	/214
13.2.1	包过滤防火墙	/214
13.2.2	状态检测防火墙	/215
13.2.3	应用层网关	/217
13.2.4	代理服务器	/217
13.3	防火墙的体系结构	/218
13.3.1	双宿/多宿主主机模式	/218
13.3.2	屏蔽主机模式	/219
13.3.3	屏蔽子网模式	/220
13.4	防火墙技术的几个新方向	/221
13.4.1	透明接入技术	/221
13.4.2	分布式防火墙技术	/221
13.4.3	以防火墙为核心的网络安全体系	/222
13.4.4	防火墙的发展趋势	/222
	习题	/223
<b>第 14 章</b>	<b>虚拟专用网</b>	<b>/224</b>
14.1	VPN 概述	/224

14.2	VPN 的分类	/224
14.3	各种 VPN 技术分析	/225
14.3.1	MPLS 技术	/225
14.3.2	IPSec 技术	/226
14.3.3	GRE 技术	/226
14.3.4	SSL 技术	/227
14.3.5	SOCKS 技术	/228
14.3.6	SSH 技术	/228
14.3.7	PPTP 和 L2TP 技术	/228
14.4	PPTP 的安全问题	/230
14.5	VPN 的使用现状	/231
	习题	/232
<b>第 15 章 入侵检测系统和网络诱骗系统 /233</b>		
15.1	入侵检测概述	/233
15.1.1	入侵检测的概念	/233
15.1.2	入侵检测的历史	/234
15.1.3	入侵检测系统的功能	/235
15.1.4	入侵检测系统的分类	/236
15.1.5	入侵检测系统的体系结构	/238
15.2	入侵检测技术	/240
15.2.1	异常检测技术	/240
15.2.2	误用检测技术	/241
15.2.3	其他入侵检测技术	/242
15.3	IDS 的标准化	/243
15.3.1	IDS 标准化进展现状	/243
15.3.2	入侵检测工作组	/244
15.3.3	公共入侵检测框架	/244
15.4	入侵检测的发展	/245
15.4.1	入侵检测技术的发展方向	/246
15.4.2	从 IDS 到 IPS 和 IMS	/247
15.5	网络诱骗系统	/248

15.5.1	网络诱骗技术	/250
15.5.2	蜜罐的分类	/253
15.5.3	常见的网络诱骗工具及产品	/254
15.5.4	蜜罐的优缺点	/256
	习题	/257
<b>第 16 章 无线网络安全 /259</b>		
16.1	IEEE 802.11 无线局域网概述	/259
16.1.1	WiFi 联盟	/260
16.1.2	IEEE 802 协议架构	/261
16.1.3	IEEE 802.11 网络组成与架构模型	/262
16.2	IEEE 802.11i 无线局域网安全	/263
16.2.1	IEEE 802.11i 服务	/264
16.2.2	IEEE 802.11i 操作阶段	/264
16.2.3	发现阶段	/266
16.2.4	认证阶段	/267
16.2.5	密钥管理阶段	/269
16.2.6	保密数据传输阶段	/273
16.3	无线局域网中的安全问题	/274
16.3.1	无线网络密码破解	/274
16.3.2	无线阻塞攻击	/279
16.3.3	无线钓鱼攻击	/283
	习题	/286
<b>第 17 章 恶意代码 /287</b>		
17.1	恶意代码概述	/287
17.1.1	恶意代码的发展史	/288
17.1.2	恶意代码的分类	/289
17.1.3	恶意代码的危害及传播趋势	/291
17.2	计算机病毒	/291
17.2.1	计算机病毒的概念	/292

17.2.2	计算机病毒的结构	/292
17.2.3	计算机病毒的特点	/293
17.2.4	计算机病毒的分类	/294
17.2.5	计算机病毒的防范	/296
17.3	特洛伊木马	/296
17.3.1	特洛伊木马概述	/296
17.3.2	木马的结构和原理	/297
17.3.3	木马隐藏技术	/298
17.3.4	木马的分类	/299
17.3.5	木马植入手段	/301
17.3.6	木马的特点	/301
17.3.7	木马的防范技术	/302
17.4	蠕虫	/305
17.4.1	蠕虫概述	/305
17.4.2	蠕虫的结构	/306
17.4.3	蠕虫的特点	/306
17.4.4	蠕虫的防范技术	/307
17.4.5	病毒、木马、蠕虫的区别	/308
	习题	/309
	参考文献	/310



# 第1章 网络安全基础

## 1.1 网络安全的概念

21世纪是信息的时代,信息正成为重要的战略资源,信息的获取能力、处理能力和保障能力成为一个国家综合国力的重要组成部分。一个信息技术和信息产业落后的国家,无法成为世界强国,目前信息科学和技术正处于快速发展阶段,成为促进经济发展和社会进步的重要因素。另一方面,危害信息安全的事件不断出现,人们经常在新闻中听到黑客、木马、漏洞这些与信息安全有关的名词,网络银行账号、网络游戏账号、QQ账号被盗已经不再成为新闻,网络谣言、人肉搜索等网络暴力事件已经成为常见的现象,信息安全的形势严峻,信息技术的发展改善了人们的生活,但也让人们的敏感信息变得不安全。也许几十年前,人们只要把敏感文档锁进保险箱,就可以高枕无忧,可如今大部分的信息都是以二进制的形式存储在电子产品中,通过网络进行传送,人们已经没有保险箱可以保证这些信息的安全,信息安全事关国家安全和社会稳定,必须采取措施确保我国的信息安全。

### 1. 信息安全的含义

目前业界关于信息安全的定义和内含,尚没有形成一个统一的说法。不同的学者根据自己的研究和理解,给出了不同的诠释。尽管这些诠释不尽相同,但其主要内容却是相同的。

信息论的知识告诉我们,信息不能脱离它的载体而孤立存在。例如,有一份重要的文档使用微软公司软件 Office 编辑处理,并存储在计算机的硬盘中,可以通过网络用电子邮件发送给对方。在编辑发送过程中,Office 软件、硬盘、网络都是信息的载体,如果 Office 软件存在漏洞、计算机硬盘被偷走、网络数据被截取,这个重要的文档就会被泄密。我们不能脱离信息系统而孤立地谈论信息安全。因此,应当从信息系统安全角度来全面考虑信息安全的内含。信息系统安全主要包括四个层面:硬件安全、软件安全、数据安全和安全管理,其中的数据安全即是传统的信息安全。为了表述简单,在不会产生歧义时可以直接将信息系统安全简称为“信息安全”。

(1) 硬件安全:信息系统硬件的安全是信息系统安全的首要问题,包括硬件的稳定性、可靠性和可用性。

(2) 软件安全:如保护信息系统不被非法侵入,系统软件和应用软件不被非法复制、篡改,不受恶意软件的侵害等。

(3) 数据安全:采取措施确保数据免受未授权的泄露、篡改和毁坏,主要包括数据的机密性、完整性、不可否认性和可用性。