

高等学校网络空间安全专业规划教材

网络安全

沈鑫剡 等 编著



清华大学出版社

网络安全

沈鑫剡 俞海英 伍红兵 李兴德 编著

内 容 简 介

本书将网络安全理论、网络安全协议和主流网络安全技术有机集成在一起,既能让读者掌握完整、系统的网络安全理论,又能让读者具备运用网络安全协议和主流网络安全技术解决实际网络安全问题的能力。

全书内容分为三部分,一是网络安全理论,包括加密算法、报文摘要算法等;二是网络安全协议,包括 IPsec、TLS、HTTPS、DNS Sec、SET、S/MIME 等;三是主流网络安全技术,包括以太网安全技术、无线局域网安全技术、互联网安全技术、虚拟专用网络、防火墙、入侵检测系统、病毒防御技术和计算机安全技术等。主流网络安全技术是本书的重点。

本书以通俗易懂、循序渐进的方式叙述网络安全知识,并通过大量的例子来加深读者对网络安全知识的理解。本书内容组织严谨,叙述方法新颖,是一本理想的计算机专业本科生的网络安全教材,也可作为计算机专业研究生的网络安全教材,对从事网络安全工作的工程技术人员,也是一本非常好的参考书。

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/沈鑫刻等编著. —北京:清华大学出版社,2017

(高等学校网络空间安全专业规划教材)

ISBN 978-7-302-46723-6

I. ①网… II. ①沈… III. ①计算机网络—网络安全—高等学校—教材 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 040284 号

责任编辑:袁勤勇 薛 阳

封面设计:傅瑞学

责任校对:焦丽丽

责任印制:李红英

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

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

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

印 装 者:清华大学印刷厂

经 销:全国新华书店

开 本:185mm×260mm

印 张:27.75

字 数:637 千字

版 次:2017 年 8 月第 1 版

印 次:2017 年 8 月第 1 次印刷

印 数:1~2000

定 价:59.00 元

产品编号:069871-01



本书有机集成网络安全理论、网络安全协议和主流网络安全技术,结合网络安全理论讨论主流网络安全技术的实现原理,让读者知其所以然。

在具体网络环境下讨论运用网络安全协议和网络安全技术解决实际网络安全问题的方法和过程,培养读者运用网络安全协议和网络安全技术解决实际网络安全问题的能力。

配套的实验教材《网络安全实验教程》与本书相得益彰,使得课堂教学和实验形成良性互动。



对于一本以真正将读者领进网络安全知识殿堂为教学目标的教材,一是必须提供完整、系统的网络安全理论,这样才能让读者理解网络安全技术的实现机制,具有进一步研究网络安全技术的能力;二是必须深入讨论当前主流网络安全技术,同时,结合网络安全理论讨论主流网络安全技术的实现原理,让读者知其所以然。三是需要在具体网络环境下讨论运用网络安全协议和网络安全技术解决实际网络安全问题的方法和过程,让读者具备运用网络安全协议和网络安全技术解决实际网络安全问题的能力,解决读者学以致用用的问题。

本书的特点是将网络安全理论、网络安全协议和主流网络安全技术有机集成在一起。既能让读者掌握完整、系统的网络安全理论,又能让读者具备运用网络安全协议和主流网络安全技术解决实际网络安全问题的能力。

全书内容分为三部分,一是网络安全理论,包括加密算法、报文摘要算法等;二是网络安全协议,包括 IPSec、TLS、HTTPS、DNS Sec、SET、S/MIME 等;三是主流网络安全技术,包括以太网安全技术、无线局域网安全技术、互联网安全技术、虚拟专用网络、防火墙、入侵检测系统、病毒防御技术和计算机安全技术等。主流网络安全技术是本书的重点。

本书有配套的实验书《网络安全实验教程》,实验教材提供了在 Cisco Packet Tracer 软件实验平台上运用本书提供的理论和技术设计,配置和调试各种满足不同安全性能的安全网络的步骤和方法,学生可以用本书提供的安全协议和安全技术指导实验,再通过实验来加深理解本书内容,使得课堂教学和实验形成良性互动。

作为一本无论在内容组织、叙述方法还是教学目标都和传统网络安全教材有一定区别的新书,书中疏漏和不足之处在所难免,殷切希望使用本书的老师和学生批评指正。作者 E-mail 地址为: shenxinshan@163.com。

作 者

2017 年 5 月



第 1 章 概述 /1

1.1	信息和信息安全	1
1.1.1	信息、数据和信号	1
1.1.2	信息安全定义	2
1.1.3	信息安全发展过程	2
1.1.4	信息安全目标	5
1.2	网络安全	6
1.2.1	引发网络安全问题的原因	6
1.2.2	网络安全内涵	7
1.3	安全模型	10
1.3.1	安全模型含义和作用	10
1.3.2	P2DR 安全模型	11
1.3.3	信息保障技术框架	13
小结		17
习题		18

第 2 章 网络攻击 /19

2.1	网络攻击定义和分类	19
2.1.1	网络攻击定义	19
2.1.2	网络攻击分类	19
2.2	嗅探攻击	20
2.2.1	嗅探攻击原理和后果	20
2.2.2	集线器和嗅探攻击	21
2.2.3	交换机和 MAC 表溢出攻击	21
2.2.4	嗅探攻击的防御机制	22
2.3	截获攻击	22
2.3.1	截获攻击原理和后果	22
2.3.2	MAC 地址欺骗攻击	23
2.3.3	DHCP 欺骗攻击	24
2.3.4	ARP 欺骗攻击	26



2.3.5	生成树欺骗攻击	28
2.3.6	路由项欺骗攻击	29
2.4	拒绝服务攻击	31
2.4.1	SYN 泛洪攻击	31
2.4.2	Smurf 攻击	32
2.4.3	DDoS	35
2.5	欺骗攻击	37
2.5.1	源 IP 地址欺骗攻击	37
2.5.2	钓鱼网站	37
2.6	非法接入和登录	39
2.6.1	非法接入无线局域网	39
2.6.2	非法登录	41
2.7	黑客入侵	42
2.7.1	信息收集	42
2.7.2	扫描	43
2.7.3	渗透	45
2.7.4	攻击	47
2.7.5	黑客入侵防御机制	48
2.8	病毒	48
2.8.1	恶意代码定义	48
2.8.2	恶意代码分类	48
2.8.3	病毒一般结构	50
2.8.4	病毒分类	51
2.8.5	病毒实现技术	53
2.8.6	病毒防御机制	55
小结		55
习题		56

第 3 章 加密算法 /58

3.1	基本概念和分类	58
3.1.1	基本概念	58
3.1.2	加密传输过程	60
3.1.3	密码体制分类	60
3.2	对称密钥体制	60
3.2.1	分组密码体制和流密码体制	61
3.2.2	分组密码体制	61
3.2.3	流密码体制	73
3.2.4	对称密钥体制的密钥分配过程	75



3.3 非对称密钥体制	78
3.3.1 公开密钥加密算法原理	78
3.3.2 RSA 公开密钥加密算法	79
3.3.3 公开密钥加密算法密钥分发原则	80
3.4 两种密钥体制的特点和适用范围	80
3.4.1 两种密钥体制的特点	80
3.4.2 两种密钥体制的有机结合	80
小结	81
习题	81

第4章 报文摘要算法 /83

4.1 基本概念和特点	83
4.1.1 完整性检测	83
4.1.2 报文摘要算法特点	84
4.2 MD5	85
4.2.1 添加填充位	85
4.2.2 分组操作	85
4.2.3 MD5 运算过程	86
4.3 SHA	88
4.3.1 SHA-1 与 MD5 之间的异同	88
4.3.2 SHA-1 运算过程	89
4.3.3 SHA-1 与 MD5 安全性和计算复杂性比较	89
4.4 HMAC	90
4.4.1 完整性检测要求	90
4.4.2 HMAC 运算思路和运算过程	90
4.5 报文摘要应用	91
4.5.1 完整性检测	91
4.5.2 消息鉴别	92
4.5.3 口令安全存储	93
4.5.4 数字签名	93
小结	99
习题	100

第5章 接入控制和访问控制 /101

5.1 身份鉴别	101
5.1.1 身份鉴别定义和分类	101
5.1.2 主体身份标识信息	102
5.1.3 单向鉴别过程	102



5.1.4	双向鉴别过程	104
5.1.5	第三方鉴别过程	105
5.2	Internet 接入控制过程	107
5.2.1	终端接入 Internet 需要解决的问题	107
5.2.2	PPP 与接入控制过程	109
5.3	EAP 和 802.1X	113
5.3.1	引出 EAP 的原因	113
5.3.2	EAP 操作过程	115
5.3.3	EAP over PPP	116
5.3.4	802.1X 操作过程	117
5.4	RADIUS	121
5.4.1	RADIUS 功能	121
5.4.2	RADIUS 消息格式、类型和封装过程	122
5.4.3	RADIUS 应用	124
5.5	Kerberos 和访问控制过程	125
5.5.1	访问控制过程	125
5.5.2	鉴别服务器实施统一身份鉴别机制	127
5.5.3	Kerberos 身份鉴别和访问控制过程	128
	小结	131
	习题	131

第 6 章 安全协议 /133

6.1	安全协议概述	133
6.1.1	产生安全协议的原因	133
6.1.2	安全协议功能	134
6.1.3	安全协议体系结构	135
6.2	IPSec	135
6.2.1	IPSec 概述	136
6.2.2	AH	139
6.2.3	ESP	141
6.2.4	IKE	142
6.3	TLS	145
6.3.1	TLS 引出原因和发展过程	145
6.3.2	TLS 协议结构	146
6.3.3	TLS 记录协议	146
6.3.4	握手协议实现身份鉴别和安全参数协商过程	147
6.3.5	HTTPS	151
6.4	应用层安全协议	152



6.4.1	DNS Sec	153
6.4.2	SET	158
6.4.3	PGP	169
6.4.4	S/MIME	171
6.5	IPSec、TLS 和应用层安全协议比较	175
6.5.1	功能差别	175
6.5.2	适用环境	175
小结		176
习题		176

第 7 章 以太网安全技术 /179

7.1	以太网解决安全威胁的思路	179
7.1.1	以太网相关威胁和引发原因	179
7.1.2	以太网解决安全威胁的思路	180
7.2	以太网接入控制技术	180
7.2.1	以太网接入控制机制	181
7.2.2	静态配置访问控制列表	182
7.2.3	安全端口	183
7.2.4	802.1X 接入控制过程	184
7.2.5	以太网接入控制过程防御的网络攻击	186
7.3	防欺骗攻击机制	187
7.3.1	防 DHCP 欺骗攻击机制和 DHCP 侦听信息库	187
7.3.2	防 ARP 欺骗攻击机制	189
7.3.3	防源 IP 地址欺骗攻击机制	190
7.4	生成树欺骗攻击与防御机制	190
7.4.1	实施生成树欺骗攻击的条件	190
7.4.2	防生成树欺骗攻击机制	191
7.5	虚拟局域网	191
7.5.1	虚拟局域网降低攻击危害	191
7.5.2	虚拟局域网安全应用实例	192
小结		194
习题		194

第 8 章 无线局域网安全技术 /196

8.1	无线局域网的开放性和安全问题	196
8.1.1	频段的开放性	196
8.1.2	空间的开放性	197
8.1.3	开放带来的安全问题和解决思路	197



8.2	WEP	199
8.2.1	WEP 加密和完整性检测过程	199
8.2.2	WEP 帧结构	200
8.2.3	WEP 鉴别机制	201
8.2.4	基于 MAC 地址鉴别机制	201
8.2.5	关联的接入控制功能	202
8.2.6	WEP 的安全缺陷	203
8.3	802.11i	207
8.3.1	802.11i 增强的安全功能	207
8.3.2	802.11i 加密和完整性检测机制	208
8.3.3	802.11i 鉴别机制	215
8.3.4	动态密钥分配机制	221
8.4	WPA2	222
8.4.1	WPA2 企业模式	223
8.4.2	WPA2 个人模式	223
	小结	225
	习题	225

第 9 章 互联网安全技术 /228

9.1	互联网安全技术概述	228
9.1.1	路由器和互联网结构	228
9.1.2	互联网安全技术范畴和功能	230
9.2	安全路由	230
9.2.1	防路由项欺骗攻击机制	231
9.2.2	路由项过滤	232
9.2.3	单播反向路径验证	232
9.2.4	策略路由	233
9.3	流量管制	234
9.3.1	拒绝服务攻击和流量管制	234
9.3.2	信息流分类	235
9.3.3	管制算法	236
9.3.4	流量管制抑止拒绝服务攻击机制	237
9.4	NAT	239
9.4.1	NAT 概述	239
9.4.2	动态 PAT 和静态 PAT	242
9.4.3	动态 NAT 和静态 NAT	244
9.4.4	NAT 的弱安全性	246
9.5	VRRP	247



9.5.1 容错网络结构	247
9.5.2 VRRP 工作原理	248
9.5.3 VRRP 应用实例	253
小结	254
习题	255

第 10 章 虚拟专用网络 /258

10.1 VPN 概述	258
10.1.1 企业网和远程接入	258
10.1.2 VPN 定义和需要解决的问题	260
10.1.3 VPN 分类	262
10.2 第三层隧道和 IPSec	264
10.2.1 VPN 结构	265
10.2.2 内部网络之间 IP 分组传输过程	267
10.2.3 IPSec 和安全传输过程	269
10.3 第二层隧道和 IPSec	272
10.3.1 远程接入过程	272
10.3.2 PPP 帧封装过程	274
10.3.3 L2TP	275
10.3.4 VPN 接入控制过程	281
10.3.5 IPSec 和安全传输过程	284
10.3.6 Cisco Easy VPN	285
10.4 SSL VPN	290
10.4.1 第二层隧道和 IPSec 的缺陷	290
10.4.2 SSL VPN 实现原理	291
小结	294
习题	295

第 11 章 防火墙 /297

11.1 防火墙概述	297
11.1.1 引出防火墙的原因	297
11.1.2 防火墙定义和工作机制	298
11.1.3 防火墙分类	299
11.1.4 防火墙功能	301
11.1.5 防火墙的局限性	302
11.2 分组过滤器	302
11.2.1 无状态分组过滤器	302
11.2.2 有状态分组过滤器	306



11.3	电路层代理	318
11.3.1	Socks 和电路层代理实现原理	318
11.3.2	电路层代理应用环境	320
11.3.3	电路层代理安全功能	324
11.4	应用层网关	324
11.4.1	应用层网关概述	325
11.4.2	Web 应用防火墙工作原理	325
11.4.3	Web 应用防火墙应用环境	328
11.5	三种防火墙的特点	329
11.5.1	三种防火墙的安全功能	329
11.5.2	三种防火墙的应用环境	330
11.5.3	三种防火墙综合应用实例	330
	小结	332
	习题	333
第 12 章 入侵检测系统 /336		
12.1	IDS 概述	336
12.1.1	入侵定义和手段	336
12.1.2	引出 IDS 的原因	337
12.1.3	入侵检测系统通用框架结构	338
12.1.4	入侵检测系统的两种应用方式	339
12.1.5	IDS 分类	340
12.1.6	入侵检测系统工作过程	342
12.1.7	入侵检测系统的不足	345
12.1.8	入侵检测系统发展趋势	346
12.1.9	入侵检测系统的评价指标	346
12.2	网络入侵检测系统	347
12.2.1	网络入侵检测系统结构	347
12.2.2	信息流捕获机制	348
12.2.3	网络入侵检测机制	350
12.2.4	安全策略配置实例	356
12.3	主机入侵检测系统	359
12.3.1	黑客攻击主机系统过程	360
12.3.2	主机入侵检测系统功能	360
12.3.3	主机入侵检测系统工作流程	360
12.3.4	拦截机制	361
12.3.5	主机资源	363
12.3.6	用户和系统状态	363



12.3.7 访问控制策略配置实例.....	364
小结.....	365
习题.....	366

第 13 章 病毒防御技术 /368

13.1 病毒作用过程.....	368
13.1.1 病毒存在形式.....	368
13.1.2 病毒植入方式.....	369
13.1.3 病毒隐藏和运行.....	369
13.1.4 病毒感染和传播.....	371
13.1.5 病毒破坏过程.....	371
13.1.6 病毒作用过程实例.....	372
13.2 基于主机防御技术.....	374
13.2.1 基于特征的扫描技术.....	375
13.2.2 基于线索的扫描技术.....	376
13.2.3 基于完整性检测的扫描技术.....	376
13.2.4 基于行为的检测技术.....	377
13.2.5 基于模拟运行环境的检测技术.....	377
13.3 基于网络防御技术.....	378
13.3.1 防火墙.....	378
13.3.2 网络入侵检测系统.....	379
13.3.3 防毒墙.....	380
13.3.4 数字免疫系统.....	381
小结.....	381
习题.....	382

第 14 章 计算机安全技术 /383

14.1 计算机安全威胁和安全技术.....	383
14.1.1 安全威胁.....	383
14.1.2 安全技术.....	384
14.2 访问控制.....	384
14.2.1 基本术语.....	384
14.2.2 访问控制模型.....	385
14.2.3 审计.....	390
14.2.4 Windows 7 访问控制机制.....	391
14.3 Windows 7 防火墙.....	395
14.3.1 入站规则和出站规则.....	396
14.3.2 Windows 7 防火墙配置实例.....	397



14.4 Windows 7 网络管理和监测命令	406
14.4.1 ping	407
14.4.2 tracert	408
14.4.3 ipconfig	410
14.4.4 arp	411
14.4.5 nslookup	413
14.4.6 route	414
14.4.7 netstat	416
小结	419
习题	419

英文缩写词 /420

参考文献 /425

第 1 章

概 述

信息技术范畴中的信息是指计算机中用文字、数值、图形、图像、音频和视频等多种类型的数据所表示的内容。网络环境下的信息系统由主机、链路和转发结点组成。信息分为由主机存储和处理的信息,经过链路传输的信息,转发结点中等待转发的信息等。因此,网络环境下的信息安全的内涵包括与保障网络环境下的信息系统中分布在主机、链路和转发结点中的信息不受威胁,没有危险、危害和损失相关的理论、技术、协议和标准等。网络环境下的信息安全也称为网络安全。

1.1 信息和信息安全

信息的表示方式和承载方式是不断变化的,因此,信息安全的目标和内涵也是不断变化的。目前提供服务的信息系统主要是网络环境下的信息系统,因此,信息安全目标与内涵都是基于保障网络环境下的信息系统的服务功能定义的。

1.1.1 信息、数据和信号

1. 信息

信息的定义多种多样,信息技术中的信息通常采用以下定义:信息是对客观世界中各种事物的运动状态和变化的反映,是客观事物之间相互联系和相互作用的表征,表现的是客观事物运动状态和变化的本质内容。

信息之所以重要,是因为它小到可以反映一个项目、一次活动的本质内容,如项目和活动计划、项目和活动实施过程等;大到可以反映一个企业、一个国家的本质内容,如企业核心技术、企业财务状况、国家核心机密等。这些本质内容事关项目、活动的成败,企业和国家的兴衰存亡。

2. 数据

数据是记录信息的形式,可以用文字、数值、图形、图像、音频和视频等多种类型的数据表示信息。由于计算机统一用二进制数表示各种类型的数据,因此,计算机统一用二进制数表示信息。

3. 信号

信号(Signal)是数据的电气或电磁表现。信号可以是模拟的,也可以是数字的,模拟信号是指时间和幅度都是连续的信号。数字信号是指时间和幅度都是离散的信号。由于计算机统一用二进制数表示各种类型的数据,因此,在计算机网络中,信号其实是二进制

位流的电气或电磁表现。

1.1.2 信息安全定义

安全是指不受威胁,没有危险、危害和损失。因此,信息安全是指信息系统中的信息不会因为偶然的或者恶意的原因而遭受破坏、更改和泄漏,信息系统能够持续、不间断地提供信息服务。

1.1.3 信息安全发展过程

1. 物体承载信息阶段

1) 信息表示形式

早期用于承载信息的是物体,如纸张、绢等,将表示信息的文字、数值、图形等记录在纸张、绢等物体上。完成信息传输过程需要将承载信息的物体从一个物理位置运输到另一个物理位置。

2) 存在威胁

物体承载信息阶段,对信息的威胁主要有两种,一是窃取承载信息的物体,二是损坏承载信息的物体。

3) 安全措施

这个阶段的安全措施主要有物理安全和加密两种。物理安全用于保证记录信息的物体在储存和运输过程中不被窃取和毁坏。

加密是使得信息不易读出和还原的操作过程。如果记录在物体上的信息是加密后的信息,即使获得记录信息的物体,也无法读出或还原加密前的信息,即原始信息。如斯巴达克人将羊皮螺旋形地缠在圆柱形棒上后再书写文字,书写文字后的羊皮即使落入敌方手中,如果不能将羊皮螺旋形地缠在相同直径的圆柱形棒上,也是无法正确读出原始文字内容的。

古罗马采用凯撒密码。凯撒密码将每一个字符用字符表中后退三个的字符代替,这种后退是循环的,字符 Z 后退一个的字符是 A。这样原文 GOOD MORNING,用凯撒密码加密后变为 JRRG PRUQLKLJ,如果不知道凯撒密码的处理方法,即使得到文本 JRRG PRUQLKLJ,也无法还原原文 GOOD MORNING。

2. 有线通信和无线通信阶段

1) 信息传输过程

首先对表示信息的文字、数值等数据进行编码,然后将编码转换成信号,经过有线和无线信道将信号从一个物理位置传播到另一个物理位置。也可以经过有线和无线信道直接将音频和视频信号从一个物理位置传播到另一个物理位置。

2) 存在的威胁

有线通信和无线通信阶段,信息最终转换成信号后经过有线和无线信道传播,而信号传播过程中可能被侦听,因此,敌方可以侦听到经过有线和无线信道传播的信号,并通过侦听到的信号还原出信息。