

21 世纪高等院校计算机网络工程专业规划教材

基于案例的网络安全 技术与实践

朱宏峰 朱丹 孙阳 刘天华 编著

可下载教学资料

<http://www.tup.tsinghua.edu.cn>

清华大学出版社



21世纪高等院校计算机网络工程专业规划教材

基于案例的网络安全 技术与实践

朱宏峰 朱丹 孙阳 刘天华 编著

清华大学出版社
北京

内 容 简 介

本书主要介绍了研究和掌握网络安全技术必备的基本数学方法、安全协议以及相关的网络安全典型知识,主要内容包括密码学数学基础、古典密码、计算密码、物理密码、基本安全协议、N 方安全协议、网络安全体系结构、网络实体安全、网络安全协议、访问控制与 VPN、防火墙与隔离网闸、入侵检测技术、计算机病毒等方法与技术,并同步介绍了这些方法与技术在实际应用中的典型案例。

本书适用于计算机专业本科生以及对当前密码学与网络安全感兴趣的技术人员。

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

基于案例的网络安全技术与实践/朱宏峰等编著.--北京:清华大学出版社,2012.12

21 世纪高等院校计算机网络工程专业规划教材

ISBN 978-7-302-30245-2

I. ①基… II. ①朱… 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(2012)第 233157 号

责任编辑:闫红梅 李 晔

封面设计:何凤霞

责任校对:李建庄

责任印制:何 芊

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 刷 者:北京密云胶印厂

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:24.25 字 数:608 千字

版 次:2012 年 12 月第 1 版 印 次:2012 年 12 月第 1 次印刷

印 数:1~3000

定 价:39.00 元

产品编号:047110-01

前言

《基于案例的网络安全技术与实践》涉及网络中的各个层次,犹如血液一般渗透到计算机实际应用过程中的各个环节。为了对整体有一个清晰的把握,通常可以把计算机系统划分为5个纵向层次:硬件材料→硬件设计与实现→操作系统→系统软件→应用软件,类似地,网络安全系统也可以分成一个5层体系:数学基础→密码学→安全协议→网络安全→应用安全,本书着重阐述中间3层内容。

本教材编写的出发点主要针对3种“问题”学生:一是“高分低能”型,其核心问题是“重知识而轻能力”;二是“眼高手低”型,其核心问题是“知其然而不知其所以然”;三是“小学生”型,其核心问题是“无兴趣则不学”,传统教学方法无效。

为了解决上述问题,我们编写了基于“兴趣”的启发式网络工程教材:《基于案例的网络安全技术与实践》。由于这门课程的特殊性(与密码和安全相关的有趣实例非常多),可以基于“兴趣”进行展开,每章都可以从一个趣味盎然的实例开始阐述,然后进行启发式的讲解,一环套一环,吸引学生一步步进入教师节奏,从而达到良好的教学效果。因此,教材每一章编写的基本思路是:实例(吸引读者)→分析(为什么这样做?)→原理(具体怎么做?)→实践(实验)→总结(形成体系)→习题(锻炼思维),其中,习题部分将突出批判精神,引导学生以辩证思维方式看问题,进而将学生培养成为能够善于独立思考、有创造力的复合型人才。

此外,本书还具备以下特点:

(1) 整体的连贯性。本书整体上按照网络安全系统从低到高的层次阐述,重点针对“密码学→安全协议→网络安全”3个层次进行展开,且前者都是作为后者的“黑盒”来体现,使条理更为清晰。“数学基础”部分只给出简明扼要的知识点,而“应用安全”则适度的分布在各个章节以及实验练习中。

(2) 案例的趣味性。本书图文并茂,深入浅出。采用简单有趣的案例来说明其实质,然后再将问题的“计算”或“规模”复杂化,叙述过程中的“对比”、“流程”、“交互”等问题将以图表的形式体现。同时抓住时机,引出知识点。

(3) 知识的系统性。本书最终目的是培养学生的能力与创造力,因此在全书选材上不仅注意理论与实际的结合,更加注重对兴趣的培养,在基本知识掌握的基础上,适当给出当前的发展方向,从而培养出大局观思维与微创新能力“双强”的优秀毕业生。

目 录

第一篇 引 言

第 1 章 网络安全概述	3
1.1 计算机网络安全的概念	3
1.1.1 计算机网络安全的定义	3
1.1.2 计算机网络安全含义	4
1.2 计算机网络安全攻击与防御	5
1.2.1 潜伏者——谁是主要威胁	5
1.2.2 层次化网络安全的核心问题	6
1.2.3 网络安全的攻防体系	7
1.2.4 影响网络安全的因素	9
1.3 计算机网络安全宏观层次	10
1.3.1 安全立法	10
1.3.2 安全管理	11
1.3.3 安全技术措施	11
1.4 计算机网络安全法律和法规	12
1.4.1 国外的相关法律和法规	12
1.4.2 我国的相关法律和法规	13
1.5 小结	17
1.6 习题	17
第 2 章 数学基础	18
2.1 数论基础	18
2.1.1 整除及辗转相除	18
2.1.2 算术基本定理	19
2.1.3 同余式	20
2.1.4 费马小定理和欧拉定理	21
2.2 抽象代数基础	21
2.3 离散概率基础	22
2.4 信息论基础	23
2.5 计算到底有多难：复杂性理论基础	24

2.5.1	基本概念	24
2.5.2	计算模型与判定问题	26
2.5.3	复杂性类	27
2.6	计算困难问题及其假设	29
2.6.1	大整数因子分解问题和 RSA 问题	29
2.6.2	离散对数和 Diffie-Hellman 问题	31
2.6.3	椭圆曲线和双线性对问题	32
2.7	小结	38
2.8	习题	38

第二篇 密码学——奠基之石

第 3 章	古典密码	41
3.1	一些有趣的解谜实例	41
3.2	密码演化：从艺术到完美	42
3.3	密码学基本概念	44
3.4	古典替换密码体制	49
3.4.1	古典单码加密法	49
3.4.2	古典多码加密法	52
3.5	古典换位密码体制	54
3.6	隐写术：在敌人面前通信	54
3.7	小结	55
3.8	习题	56
第 4 章	计算密码	57
4.1	对称密钥密码	57
4.1.1	计算对称密码的特点	57
4.1.2	流密码基本概念	58
4.1.3	流密码实例	59
4.1.4	分组密码基本概念	64
4.1.5	分组密码实例：DES 算法	65
4.2	公开密钥密码	70
4.2.1	从对称密码到非对称密码	70
4.2.2	实现：Diffie-Hellman 密钥交换	71
4.2.3	中间人攻击	72
4.2.4	RSA 密码系统：凑成欧拉定理	73
4.3	散列函数	74
4.3.1	我的“奶酪”完整么	74
4.3.2	鸽洞原理与随机预言	75

4.3.3	直觉的错误：生日攻击	76
4.3.4	实例：MD5	77
4.4	消息认证与消息认证码	79
4.5	数字签名	81
4.5.1	数字签名基本概念	81
4.5.2	基于素数域上离散对数问题的数字签名方案	82
4.5.3	基于因子分解问题的签名方案	86
4.5.4	签密方案实例	87
4.6	小结	89
4.7	习题	90
4.8	实验	91
第5章	物理密码	92
5.1	两种主要的物理密码	92
5.1.1	量子密码	92
5.1.2	混沌密码	93
5.2	量子密码研究综述	94
5.2.1	量子密码与经典密码的辩证关系	95
5.2.2	量子密码的目标与特性	96
5.2.3	量子密码的安全性与攻击	98
5.2.4	抗量子密码技术	99
5.2.5	量子密码研究与应用的新方向	99
5.3	量子密码基础理论：量子信息科学基础	100
5.3.1	什么是量子	100
5.3.2	量子信息	101
5.3.3	量子比特和布洛赫球标识法	101
5.3.4	海森堡(Heisenberg)测不准原理	103
5.3.5	量子不可克隆定理	104
5.3.6	量子信息与线性代数	105
5.4	量子密码基础理论：量子密码学基础	112
5.4.1	量子密码学概述	112
5.4.2	量子密码与传统密码的异同点	115
5.4.3	量子一次一密	115
5.4.4	量子单向函数	115
5.4.5	量子密码安全性挑战	116
5.5	小结	117
5.6	习题	118

第三篇 安全协议——衔接之桥

第 6 章 安全协议概述	121
6.1 安全协议的基本概念	121
6.1.1 游戏规则的建立	121
6.1.2 游戏规则的目的	122
6.1.3 游戏角色	123
6.2 安全协议的分类	123
6.2.1 按照游戏角色的数量进行分类	123
6.2.2 按照是否有仲裁方进行分类	124
6.2.3 其他方法	126
6.3 安全协议的模型与分析方法	127
6.4 安全协议的目标与研究层次	129
6.5 安全协议的设计原则	130
6.6 安全协议的可证明理论	131
6.6.1 密码体制的攻击游戏	131
6.6.2 随机预言模型下的安全性证明	133
6.6.3 标准模型下的安全性证明	134
6.7 小结	135
6.8 习题	135
第 7 章 基本安全协议	136
7.1 认证协议	136
7.1.1 认证：通信前的首要问题	136
7.1.2 认证协议的基本技术	141
7.1.3 常规认证协议	142
7.2 密钥交换协议	143
7.2.1 可信模型	143
7.2.2 安全性讨论	144
7.3 认证及密钥交换协议	144
7.3.1 认证及密钥交换协议基本分类	144
7.3.2 典型认证及密钥交换协议	145
7.3.3 设计一个密钥交换协议	147
7.4 小结	149
7.5 习题	150
第 8 章 两方安全协议	151
8.1 零知识协议：完美的证明	151

8.1.1	零知识思想	151
8.1.2	交互证明系统	152
8.1.3	零知识证明	153
8.2	比特承诺协议：说到就该做到	154
8.2.1	比特承诺简介	154
8.2.2	比特承诺实例	154
8.3	掷币协议：看运气	155
8.4	电话扑克协议：公平的游戏	157
8.5	不经意传输协议：版权的秘密	158
8.6	可否认认证协议：换种角度思考	161
8.7	同步秘密交换协议：同时签约的升华	163
8.8	小结	166
8.9	习题	166
第 9 章	多方安全协议	167
9.1	基本多方安全协议	167
9.1.1	秘密共享：权力集中还是分散	167
9.1.2	可验证秘密共享：坚实的架构	169
9.1.3	BD 协议：提高效率	173
9.1.4	保密的多方计算初探	174
9.1.5	理性密码学：博弈的游戏	175
9.2	电子选举协议	176
9.2.1	电子选举协议：公平和隐私	176
9.2.2	安全电子选举模型	177
9.2.3	安全电子选举结构	178
9.2.4	安全电子选举优缺点与实例	179
9.3	美丽的交易：电子商务的安全	180
9.3.1	解构商业：现实场景分析	180
9.3.2	核心技术之一：盲签名	181
9.3.3	核心技术之二：群签名	182
9.4	小结	184
9.5	习题	184

第四篇 网络安全——应用之钥

第 10 章	网络安全体系结构	187
10.1	安全模型	187
10.1.1	P2DR 模型	187
10.1.2	PDRR 模型	189

10.1.3	WPDRRC 模型	189
10.2	网络安全体系结构	190
10.2.1	Internet 网络体系层次结构	190
10.2.2	网络安全体系结构框架	191
10.3	安全策略与运行生命周期	198
10.3.1	安全策略定义	198
10.3.2	安全系统的开发与运行	200
10.3.3	安全系统的生命周期	201
10.4	小结	202
10.5	习题	202
第 11 章	网络实体安全	204
11.1	计算机网络机房与环境安全	205
11.1.1	机房的安全等级	205
11.1.2	机房的安全保护	206
11.1.3	机房的三度要求	207
11.1.4	机房的电磁干扰防护	209
11.1.5	机房接地保护与静电保护	212
11.1.6	机房电源系统	214
11.1.7	机房的防火、防水与防盗	215
11.2	计算机网络机房存储介质防护	216
11.2.1	存储介质防护	216
11.2.2	虚拟存储器保护	218
11.3	安全管理	218
11.3.1	安全管理的定义	218
11.3.2	安全管理的原则与规范	219
11.3.3	安全管理的主要内容	220
11.3.4	健全管理机构 and 规章制度	224
11.4	小结	227
11.5	习题	227
第 12 章	网络安全协议	228
12.1	数据链路层安全通信协议	228
12.1.1	PPP 协议	228
12.1.2	PPTP 协议	231
12.1.3	L2TP 协议	231
12.2	网络层安全通信协议	235
12.2.1	IPSec 协议簇概述	236
12.2.2	IPSec 协议簇中的主要协议	238

12.3	传输层安全通信协议	244
12.3.1	SSL/TLS 协议簇	244
12.3.2	SSL/TLS 应用	251
12.3.3	安全性分析	252
12.4	应用层安全通信协议	253
12.4.1	电子邮件安全协议	253
12.4.2	SET 协议	256
12.4.3	SNMP 协议	261
12.4.4	S-HTTP 协议	265
12.5	小结	265
12.6	习题	266
12.7	实验	266
第 13 章	访问控制与 VPN 技术	267
13.1	访问控制技术概述	267
13.1.1	访问控制技术概念	267
13.1.2	访问控制技术一般方法	268
13.2	自主访问控制	271
13.2.1	自主访问控制概述	271
13.2.2	自主访问控制访问模式	275
13.2.3	自主访问控制实例	276
13.3	强制访问控制	281
13.3.1	强制访问控制概述	281
13.3.2	强制访问控制的模型	282
13.3.3	强制访问控制实例	283
13.4	基于角色的访问控制	285
13.4.1	基于角色的访问控制概述	285
13.4.2	基于角色的访问控制中的角色管理	286
13.4.3	ROLE-BASE 模型实现	286
13.5	VPN 概述	289
13.5.1	VPN 的工作原理	289
13.5.2	VPN 系统结构与分类	291
13.6	VPN 实现的关键技术	293
13.6.1	隧道技术	293
13.6.2	加密技术	294
13.6.3	QoS 技术	294
13.7	VPN 设计实例	295
13.7.1	内联网 VPN 设计方案	295
13.7.2	外联网 VPN 构建方案	297

13.7.3 远程接入 VPN 构建方案	297
13.8 小结	298
13.9 习题	298

第 14 章 防火墙与隔离网闸

14.1 防火墙概述	299
14.1.1 防火墙的概念	299
14.1.2 防火墙的特性	299
14.1.3 防火墙的功能	300
14.2 防火墙体系结构	301
14.2.1 双重宿主主机体系结构	301
14.2.2 屏蔽主机体系结构	302
14.2.3 屏蔽子网体系结构	302
14.2.4 防火墙体系结构的组合形式	303
14.3 防火墙技术	303
14.3.1 防火墙所采用的主要技术	303
14.3.2 防火墙的分类	304
14.3.3 防火墙的缺点	308
14.4 防火墙设计实例	308
14.4.1 常见攻击方式和防火墙防御	308
14.4.2 基于 PIX 系列防火墙设计实例	309
14.5 隔离网闸概述	312
14.6 物理隔离网闸	312
14.6.1 物理隔离网闸定义	312
14.6.2 物理隔离的技术原理	313
14.6.3 物理隔离网闸的组成	314
14.6.4 物理离网闸的功能	314
14.6.5 物理隔离网闸的应用定位	315
14.6.6 物理隔离网闸与防火墙	317
14.7 网络隔离产品配置实例	318
14.7.1 产品介绍	318
14.7.2 配置模式与配置方法	318
14.8 小结	320
14.9 习题	320
14.10 实验	321

第 15 章 入侵检测技术

15.1 入侵检测概述	322
15.1.1 入侵检测系统的基本概念	322

15.1.2	入侵检测系统的结构	323
15.1.3	入侵检测系统的需求特性	323
15.1.4	入侵检测系统的分类	324
15.2	入侵检测的技术实现	325
15.2.1	入侵检测模型	325
15.2.2	误用与异常检测	328
15.2.3	分布式入侵检测	330
15.2.4	其他检测技术	331
15.3	入侵检测技术的性能指标和评估标准	331
15.3.1	影响入侵检测系统的性能指标	331
15.3.2	入侵检测系统测试评估标准	333
15.4	入侵检测系统实例: Snort	333
15.5	小结	340
15.6	习题	340
15.7	实验	340
第 16 章	计算机病毒、恶意代码及防范	341
16.1	计算机病毒概述	341
16.1.1	计算机病毒的概念	341
16.1.2	计算机病毒的特征	342
16.1.3	计算机病毒的分类	342
16.1.4	计算机病毒的传播	344
16.1.5	计算机病毒的防范方法	344
16.2	计算机网络病毒及防范方法	346
16.2.1	计算机网络病毒的特点	346
16.2.2	计算机网络病毒的防范方法	347
16.3	网络恶意代码及防范方法	349
16.3.1	网络恶意代码的概念	349
16.3.2	网络恶意代码的分类	350
16.3.3	网络恶意代码的关键技术	352
16.3.4	网络恶意代码的防范方法	357
16.4	网络病毒与恶意代码实例	358
16.5	小结	360
16.6	习题	360
16.7	实验	360
第 17 章	网络安全方案设计	361
17.1	大型网络安全整体解决方案	361
17.1.1	技术解决方案	361

17.1.2	安全服务解决方案	364
17.1.3	技术支持解决方案	366
17.1.4	实施建议与意见	367
17.2	某高校图书馆的网络安全方案	368
17.2.1	拓扑简要介绍	368
17.2.2	方案设备选型	369
17.3	小结	372
附录		373
参考文献		374

第一篇

引言

如果把一封信锁在保险柜中,把保险柜藏在纽约的某个地方……然后告诉你去看这封信,这并不是安全,而是隐藏。相反,如果把一封信锁在保险柜中,然后把保险柜及其设计规范和许多同样的保险柜给你,以便你和世界上最好的开保险柜的专家能够研究锁的装置,而你还是无法打开保险柜去读这封信,这才是安全的概念。

——Burce Schneier

Internet 的广泛应用使人们在生产方式、生活方式及思想观念等方面都发生了巨大变化,推动了人类社会的发展和人类文明的进步,把人类带入崭新的信息化时代。

计算机网络就像一把双刃剑,它在实现了信息交流与共享、极大便利和丰富了社会生活的同时,由于网络本身的脆弱性加上人为攻击与破坏,也对国家安全、社会公共利益以及公民个人合法权益造成现实危害和潜在威胁。因此,加强对信息网络安全技术和管理的研究,无论是对个人还是组织、机构,甚至国家、政府都有非同寻常的重要意义。

1.1 计算机网络安全的概念

1.1.1 计算机网络安全的定义

“安全”一词在字典中被定义为“远离危险的状态或特性”和“为防范间谍活动或蓄意破坏、犯罪、攻击或逃跑而采取的措施”。从这个角度来说,计算机网络安全是指为了使计算机网络运行正常,通过采用全方位的管理措施和强有力的技术手段,保证在一个网络环境里,使得经过计算机网络的数据保持保密性、完整性和可用性。

国际标准化组织(ISO)将计算机安全定义为“为数据处理系统和采取的技术的和管理的安全保护,保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露”。美国国防部国家计算机安全中心将计算机安全定义为:“一般说来,安全的系统会利用一些专门的安全特性来控制对信息的访问,只有经过适当授权的人,或者以这些人的名义进行的进程可以读、写、创建和删除这些信息”。我国公安部计算机管理监察司将计算机安全定义为“计算机安全是指计算机资产安全,即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害”。

上面是狭义的计算机网络安全的内容。广义上讲,凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络信息安全所要研究的领域。广义的计算机网络安全还应该包括网络实体安全,如机房的安全保护、防火措施、防水措施、静电防