



21 世纪大学本科
计算机专业系列教材

阙喜戎 孙锐 编著
龚向阳 王纯

信息安全原理及应用

<http://www.tup.com.cn>

- 根据教育部高教司主持评审的《中国计算机科学与技术学科教程 2002》组织编写
- 与美国 ACM 和 IEEE/CS 《Computing Curricula 2001》同步

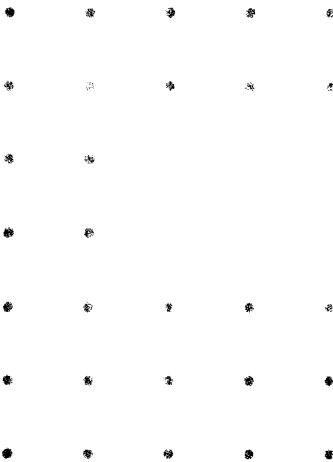


清华大学出版社

21世纪大学本科计算机专业系列教材

信息安全原理及应用

阙喜戎 孙锐 编著
龚向阳 王纯



清华大学出版社
北京

内 容 简 介

本书重点介绍:密码学理论基础(信息理论基础、复杂性理论基础);主要的加密算法及其理论基础(密码学的技术实现);密码协议和安全协议(密码学的实际运用);常用的系统安全技术和网络安全技术(实用技术)。本书从理论到技术实现和实际运用等方面对信息安全进行了全面的阐述,强调通过技术实现和实际运用加深对理论的理解,并且反过来为技术实现和实际运用提供指导。

本书深入而全面地探讨了信息安全领域人们关心的问题 and 相应的解决途径;注重运用常用的一些系统安全技术和网络安全技术在具体实践中保护网络信息系统的安全,解决实际问题。

本书可作为高等院校有关专业本科生和研究生的教材,也可作为通信工程师、计算机网络工程师和软件工程师的参考读物。

版权所有,翻印必究。

本书封面贴有清华大学出版社激光防伪标签,无标签者不得销售。

图书在版编目(CIP)数据

信息安全原理及应用/阙喜戎,孙锐,龚向阳,王纯编著. —北京:清华大学出版社,2003
(21世纪大学本科计算机专业系列教材)

ISBN 7-302-06551-9

I. 信… II. ①阙… ②孙… ③龚… ④王… III. 信息系统—安全技术—高等学校—教材 IV. TP309

中国版本图书馆 CIP 数据核字(2003)第 027068 号

出 版 者: 清华大学出版社(北京清华大学学研大厦,邮编 100084)

<http://www.tup.com.cn>

责任编辑: 张瑞庆 徐跃进

印 刷 者: 清华大学印刷厂

发 行 者: 新华书店总店北京发行所

开 本: 787×960 1/16 印张: 23.5 字数: 535 千字

版 次: 2003 年 7 月第 1 版 2003 年 7 月第 1 次印刷

书 号: ISBN 7-302-06551-9/TP·4908

印 数: 0001~6000

定 价: 29.80 元

21 世纪是知识经济的时代,是人才竞争的时代。随着 21 世纪的到来,人类已步入信息社会,信息产业正成为全球经济的主导产业。计算机科学与技术信息产业中占据了最重要的地位,这就对培养 21 世纪高素质创新型计算机专业人才提出了迫切的要求。

为了培养高素质创新型人才,必须建立高水平的教学计划和课程体系。在 20 多年跟踪分析 ACM 和 IEEE 计算机课程体系的基础上,紧跟计算机科学与技术的发展潮流,及时制定并修正教学计划和课程体系是尤其重要的。计算机科学与技术的发展对高水平人才的要求,需要我们从总体上优化课程结构,精炼教学内容,拓宽专业基础,加强教学实践,特别注重综合素质的培养,形成“基础课程精深,专业课程宽新”的格局。

为了适应计算机科学与技术学科发展和计算机教学计划的需要,要采取多种措施鼓励长期从事计算机教学和科技前沿研究的专家教授积极参与计算机专业教材的编著和更新,在教材中及时反映学科前沿的研究成果与发展趋势,以高水平的科研促进教材建设。同时适当引进国外先进的原版教材。

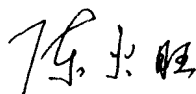
为了提高教学质量,需要不断改革教学方法与手段,倡导因材施教,强调知识的总结、梳理、推演和挖掘,通过加快教案的不断更新,使学生掌握教材中未及时反映的学科发展新动向,进一步拓广视野。教学与科研相结合是培养学生实践能力的有效途径。高水平的科研可以为教学提供最先进的高新技术平台和创造性的工作环境,使学生得以接触最先进的计算机理论、技术和环境。高水平的科研还可以为高水平人才的素质教育提供良好的物质基础。学生在课题研究中不但能了解科学研究的艰辛和科研工作者的奉献精神,而且能熏陶和培养良好的科研作风,锻炼和培养攻关能力和协作精神。

进入 21 世纪,我国高等教育进入了前所未有的大发展时期,时代的进步与发展对高等教育质量提出了更高、更新的要求。2001 年 8 月,教育部颁发了《关于加强高等学校本科教学工作,提高教学质量的若干意见》。文件指出,本科教育是高等教育的主体

和基础,抓好本科教学是提高整个高等教育质量的重点和关键。随着高等教育的普及和高等学校的扩招,在校大学本科计算机专业学生的人数将大量上升,对适合 21 世纪大学本科计算机科学与技术学科课程体系要求的,并且适合中国学生学习的计算机专业教材的需求量也将急剧增加。为此,中国计算机学会和清华大学出版社共同规划了面向全国高等院校计算机专业本科生的“21 世纪大学本科计算机专业系列教材”。本系列教材借鉴美国 ACM 和 IEEE/CS 最新制定的《Computing Curricula 2001》(简称 CC2001)课程体系,反映当代计算机科学与技术学科水平和计算机科学技术的新发展、新技术,并且结合中国计算机教育改革成果和中国国情。

中国计算机学会教育专业委员会和全国高等学校计算机教育研究会,在清华大学出版社的大力支持下,跟踪分析 CC2001,并结合中国计算机科学与技术学科的发展现状和计算机教育的改革成果,研究出了《中国计算机科学与技术学科教程 2002》(China Computing Curricula 2002,简称 CCC2002),该项研究成果对中国高等学校计算机科学与技术学科教育的改革和发展具有重要的参考价值和积极的推动作用。

“21 世纪大学本科计算机专业系列教材”正是借鉴美国 ACM 和 IEEE/CS CC2001 课程体系,依据 CCC2002 基本要求组织编写的计算机专业教材。相信通过这套教材的编写和出版,能够在内容和形式上显著地提高我国计算机专业教材的整体水平,继而提高我国大学本科计算机专业的教学质量,培养出符合时代发展要求的具有较强国际竞争力的高素质创新型计算机人才。



中国工程院院士

国防科学技术大学教授

21 世纪大学本科计算机专业系列教材编委会名誉主任

2002 年 7 月

前 言

计算机系统和信息的安全问题很早就已经存在,例如大家所熟知的计算机病毒问题就是一个典型的例子。随着社会进入信息化时代,由于互联网的开放性,计算机和信息的安全问题将更加突出。而且,随着网络使用者和网上应用的增加,特别是电子商务所涉及的金额不断提高,网络 and 连接在网络上的信息系统已经开始面临各种复杂的、严峻的安全威胁。为了维护信息化社会的有序运作,需要大量的基础扎实、技术过硬的网络信息安全人才。针对这种情况,大多数高等院校陆续开设了信息安全原理及应用方面的课程,社会上各类继续教育机构也纷纷开展了网络信息安全方面的培训。作者在从事信息安全原理及应用相关课程的教学时,一直没有找到很合适的教材。恰逢中国计算机学会组织编写“21 世纪大学本科计算机专业系列教材”,于是根据密码学和计算机网络安全的新发展和新趋势,结合平时的教学体会和学生反馈,编写了此书。

信息安全是一个综合的、交叉的学科领域,涉及数学、信息、通信和计算机等诸多学科的长期知识积累和最新发展成果。本书主要阐述现代密码技术的原理及其在信息系统安全中的应用,重点内容包括:密码学的理论基础(信息理论基础、复杂性理论基础);加密算法及其理论基础(密码学的技术实现);密码协议和安全协议(密码学的实际运用);常用的一些系统安全技术和网络安全技术(实用技术)。希望读者在阅读本书后,能够认识网络信息安全领域人们关心的问题 and 相应的解决途径;对信息安全的关键技术——密码学,应从理论要求、技术实现和实际运用等方面有一个较全面的了解;并能运用常用的一些系统安全技术和网络安全技术在具体实践中保护网络信息系统的安全,解决实际问题。

全书共分 12 章。在教学安排时,可根据学时及学生基础安排学习本书的全部或部分章节。同时,本书也配备了相关的教学课件和材料,以便教师授课时选用。本书的第 1、第 10、第 12 章由阙喜戎编写,第 2、第 3、第 4、第 5、第 6 章由孙锐编写,第 7 章由王纯编写,第 8、第 9、第 11 章由龚向阳编写。阙喜戎负责全书的总体规划与内容组织,并对

全书进行了修改和定稿。

本书在编写过程中得到了“21 世纪大学本科计算机专业系列教材”编委会的指导, 国际科技大学计算机学院宁洪教授认真地审阅了全书, 并提出了许多宝贵意见; 北京邮电大学计算机学院刘辰教授给予本书多方面的帮助; 北京邮电大学交换技术与通信网国家重点实验室宽带网中心的领导和同事热情支持了本书的编写工作; 清华大学出版社大力支持了本书的出版工作。此外, 为了编著本书我们参考和吸收了国内外许多同行学者的研究成果, 许多朋友都为此书付出了辛勤的劳动, 在此一并表示衷心感谢。

随着技术的进步和需求的变化, 信息安全技术还会不断地发展, 我们希望得到各位读者的支持, 也期待着与大家共同探讨信息安全技术的发展动向及相关课程的教学体会。由于我们水平有限, 书中错误在所难免, 欢迎读者批评指正。

作 者

于北京邮电大学计算机学院

rongqx@bupt.edu.cn

2003 年 1 月

目 录

第 1 章 信息系统安全概述	1
1.1 网络信息系统的脆弱性	1
1.1.1 网络信息系统的主要威胁	4
1.1.2 攻击的种类	6
1.2 安全需求和安全服务	8
1.2.1 网络信息系统安全的基本需求	8
1.2.2 安全服务	11
1.2.3 安全服务的实施位置	12
1.2.4 安全机制	14
1.3 安全策略	15
1.4 网络系统安全评估标准	17
1.4.1 美国的彩虹系列(Rainbow Series)	17
1.4.2 欧洲信息技术安全评估规则(ITSEC)	19
1.4.3 加拿大可信计算标准(CTCS)	19
1.4.4 信息技术安全评价通用准则(CC)	19
1.4.5 信息保障技术框架(IATF)	20
1.5 信息系统安全模型	21
1.6 加密功能的实施方式	24
1.6.1 链到链加密	24
1.6.2 端到端加密	25
1.6.3 两者的结合	27
1.7 流量的保密性	28

1.8 本章小结	29
1.9 思考题	29

第2章 密码学的基本概念和信息理论基础

2.1 基本概念	30
2.1.1 什么是密码学	30
2.1.2 密码学的发展历史	30
2.1.3 3个术语	31
2.1.4 密码体制的分类	32
2.1.5 密码分析	32
2.1.6 鉴别、完整性和不可否认性	33
2.2 传统密码及其破译	34
2.3 Shannon 的保密系统信息理论	38
2.3.1 保密系统的数学模型	38
2.3.2 完善保密性	40
2.3.3 伪密钥和唯一解距离	41
2.4 Simmons 认证系统的信息理论	42
2.4.1 认证系统的数学模型	43
2.4.2 认证码的信息论下界	45
2.5 概率论基础	46
2.6 本章小结	49
2.7 思考题	49

第3章 密码学的复杂性理论基础

3.1 算法复杂性	52
3.2 问题复杂性	53
3.3 零知识证明理论(交互与非交互)	54
3.3.1 零知识的基本概念	54
3.3.2 交互零知识证明理论	56
3.3.3 非交互零知识证明理论	58
3.4 本章小结	60
3.5 思考题	60

第 4 章 对称密钥密码体制——流密码	61
4.1 流密码的分类及其工作模式	61
4.2 线性反馈移位寄存器和 B-M 算法	64
4.2.1 基本概念	64
4.2.2 定义和相关定理	65
4.2.3 两个密码学问题	66
4.3 布尔函数的非线性准则	68
4.3.1 布尔函数的表示	68
4.3.2 非线性度	70
4.3.3 线性结构	71
4.3.4 退化性	72
4.3.5 相关免疫性	73
4.3.6 严格雪崩准则与扩散准则	75
4.4 本章小结	76
4.5 思考题	77
第 5 章 对称密钥密码体制——分组密码	78
5.1 原理及设计原则	78
5.2 Feistel 密码结构	80
5.3 数据加密标准(DES)	81
5.3.1 DES 的产生背景	81
5.3.2 DES 算法描述	82
5.3.3 实现效果	86
5.3.4 安全性分析	87
5.4 其他分组密码	89
5.4.1 IDEA	89
5.4.2 RC5	91
5.4.3 Rijndael	93
5.5 分组密码的工作模式	94
5.5.1 密码分组链接模式	94
5.5.2 密码反馈模式	95
5.5.3 输出反馈模式	96

5.5.4 级连模式	96
5.6 攻击分组密码的典型方法	97
5.6.1 强力攻击	97
5.6.2 差分分析	98
5.6.3 线性分析	100
5.6.4 其他攻击方法	103
5.7 本章小结	104
5.8 思考题	104
第6章 公钥密码体制	106
6.1 基本思想	106
6.2 数论简介	108
6.2.1 素数	108
6.2.2 概率素性检验和因子分解	114
6.2.3 离散对数	117
6.3 RSA 算法	118
6.3.1 RSA 密码算法描述	119
6.3.2 RSA 算法的实现	120
6.3.3 RSA 安全性分析	122
6.4 椭圆曲线密码体制	124
6.4.1 域 K 上的椭圆曲线	124
6.4.2 椭圆曲线中的点加运算及其几何意义	125
6.4.3 椭圆曲线上的多倍点运算和离散对数问题	128
6.4.4 椭圆曲线基本协议举例	129
6.4.5 相关标准	130
6.5 本章小结	131
6.6 思考题	131
第7章 密钥管理	132
7.1 密钥长度	132
7.1.1 密钥应该多长	133
7.1.2 对称密钥长度	133
7.1.3 公钥密钥长度	135

7.1.4	对称密钥和公钥密钥长度的比较	136
7.2	密钥生成	137
7.2.1	密钥选择	137
7.2.2	随机密钥及随机数	138
7.2.3	非线性密钥空间	142
7.3	密钥分配	143
7.3.1	对称密钥加密体制的密钥分配	143
7.3.2	公钥加密体制的密钥分配	149
7.4	密钥保护	155
7.4.1	密钥的有效期	155
7.4.2	存储密钥	156
7.4.3	销毁密钥	157
7.4.4	备份密钥	157
7.4.5	密钥托管	157
7.5	本章小结	163
7.6	思考题	163
第 8 章	报文鉴别技术	164
8.1	报文鉴别与鉴别系统	164
8.1.1	报文鉴别的必要性	164
8.1.2	报文鉴别系统	165
8.1.3	基于报文加密方式的鉴别	165
8.1.4	采用报文鉴别码的鉴别方式	168
8.1.5	基于散列函数的鉴别方法	170
8.2	报文鉴别码	172
8.2.1	MAC 的安全性	172
8.2.2	基于 DES 的报文鉴别码	174
8.3	散列函数报文鉴别	174
8.3.1	散列函数的性质	174
8.3.2	简单散列函数的构造	175
8.4	散列函数的安全性	177
8.4.1	生日攻击	177
8.4.2	简单散列函数的安全性	179

8.4.3	强行攻击	180
8.4.4	密码分析和安全散列函数	181
8.5	MD5 消息摘要算法	182
8.5.1	MD5 的设计目标	182
8.5.2	算法原理	183
8.5.3	MD5 的压缩函数	185
8.5.4	MD5 的安全性	189
8.6	安全的散列算法	189
8.6.1	SHA-1 算法原理	189
8.6.2	SHA-1 的压缩函数	191
8.6.3	SHA-1 的安全性	194
8.7	RIPEMD-160 散列算法	194
8.7.1	RIPEMD-160 算法原理	194
8.7.2	RIPEMD-160 的压缩函数	197
8.7.3	RIPEMD-160 的安全性	200
8.8	本章小结	201
8.9	思考题	201
第 9 章	数字签名与身份认证	202
9.1	数字签名	202
9.1.1	应用需求和数字签名的产生	202
9.1.2	直接数字签名	203
9.1.3	基于仲裁的数字签名	204
9.2	鉴别协议	205
9.2.1	相互鉴别	206
9.2.2	单向鉴别	210
9.3	数字签名标准	212
9.4	身份认证技术	214
9.4.1	概述	215
9.4.2	基本的身份认证方法	216
9.4.3	分布式环境中的身份认证	217
9.5	Kerberos 认证服务	218
9.5.1	设计目标	218

9.5.2	Kerberos 的设计思路	219
9.5.3	Kerberos 版本 4	223
9.5.4	Kerberos 领域	227
9.5.5	Kerberos 版本 4 的缺陷	229
9.5.6	Kerberos 版本 5	230
9.5.7	Kerberos 版本 5 的票据标志	233
9.6	X.509 认证服务	234
9.6.1	X.509 证书	235
9.6.2	用户证书的获取	237
9.6.3	证书的撤销	238
9.6.4	X.509 的认证过程	239
9.6.5	X.509 第 3 版的扩展	240
9.7	本章小结	242
9.8	思考题	242
第 10 章	IP 安全协议 (IPSec)	243
10.1	概述	243
10.2	IPSec 体系结构	246
10.2.1	IPSec 的相关标准文档	246
10.2.2	IPSec 的工作模式	247
10.2.3	IPSec 的实施位置	249
10.3	鉴别首部(AH)	250
10.3.1	AH 的格式	250
10.3.2	抗重播服务(antireplay)	251
10.3.3	完整性校验值(ICV)	253
10.3.4	AH 的工作模式	254
10.4	封装安全载荷(ESP)	254
10.4.1	ESP 的格式	254
10.4.2	填充和填充长度	255
10.4.3	加密和鉴别算法	256
10.4.4	ESP 的工作模式	257
10.5	安全关联(SA)	257
10.5.1	SA 的定义及参数	257

10.5.2	SA 的管理	260
10.5.3	SA 的组合方式	261
10.5.4	SA 的基本组合	261
10.5.5	SA 组合方式下的安全业务	263
10.6	密钥管理	264
10.6.1	ISAKMP	265
10.6.2	Oakley 密钥交换协议	270
10.6.3	IKE	271
10.7	本章小结	272
10.8	思考题	273
第 11 章	Web 的安全性	274
11.1	Web 应用所面临的安全性问题	274
11.2	安全套接字层(SSL)	277
11.2.1	SSL 的体系结构	277
11.2.2	SSL 的会话状态	277
11.2.3	SSL 记录协议	279
11.2.4	加密规约修改协议	281
11.2.5	报警协议	282
11.2.6	握手协议	282
11.3	传输层安全(TLS)	287
11.4	S-HTTP	288
11.5	安全电子交易(SET)	288
11.5.1	SET 的基本结构	289
11.5.2	双向签名	292
11.5.3	SET 的交易类型	293
11.5.4	购买请求	294
11.5.5	支付认可	296
11.5.6	支付货款	297
11.6	Web 相关的系统安全问题	298
11.6.1	CGI 的安全性	298
11.6.2	Web 中的可执行组件	300
11.6.3	Cookie	305

11.6.4	HTTP 的用户认证	305
11.7	本章小结	306
11.8	思考题	307
第 12 章	网络安全技术	308
12.1	防火墙技术	308
12.1.1	防火墙概述	308
12.1.2	防火墙的功能	310
12.1.3	防火墙基本类型	311
12.1.4	两种提高性能的相关技术	320
12.2	隐患扫描技术	325
12.3	入侵检测技术	327
12.3.1	入侵检测概述	327
12.3.2	入侵检测模型	329
12.3.3	入侵检测系统的分类	330
12.3.4	常用的入侵检测技术	333
12.3.5	CIDF 体系结构	337
12.3.6	入侵检测系统的设计要求	338
12.4	虚拟专用网技术及协议	339
12.4.1	虚拟专用网概述	339
12.4.2	VPN 的工作流程	342
12.4.3	VPN 的主要技术	343
12.4.4	VPN 服务分类	352
12.5	本章小结	353
12.6	思考题	354

第 1 章

信息系统安全概述

信息技术的发展带动了全球信息化的发展,从而使信息基础设施成为社会基础设施中必不可少的关键基础设施,与此同时,网络信息系统的安全问题也逐渐引起人们的重视。不解决信息安全问题,不强化网络化的信息安全保障,信息化将得不到可持续发展的健康发展。

在现实应用中,信息系统已由传统意义上的存放和处理信息的独立系统演变为互相连接、资源共享的系统集合,也就是说,信息系统同时也是一个网络系统。此外信息安全是一个极大的技术领域,本书的侧重点在于网络中的信息安全,因此为叙述和理解方便,本书中信息系统也被称为网络信息系统。

本章首先分析安全问题的起因及信息系统面临的各種攻击,然后介绍网络信息系统的安全需求、安全服务及知名的安全评估标准,使大家对网络信息系统的安全问题有个大致的了解。鉴于加密技术在处理安全问题时的广泛应用,本章最后对加密功能的实施进行了探讨。

1.1 网络信息系统的脆弱性

所谓网络信息系统,是指互相连接起来的独立自主的计算机信息系统的集合。网络信息系统中的计算机能够方便地交换信息、共享资源。随着现代通信技术和计算机技术的不断发展,计算机网络的规模以前所未有的速度快速增长,信息共享应用日益广泛和深入。不难发现,以个人计算机(PC)为中心的计算方式,正在向以网络为中心的计算方式发展。

网络信息系统促使了科学、技术、文化、教育和生产的快速发展,为提高现代人的生活质量提供了极大的便利。随着网络经济和网络社会时代的到来,网络将会进入一个