

信息安全专业系列教材

# 信息安全概论

(第2版)

Xinxi  
Anquan Gailun

牛少彰 崔宝江 李剑 编著



北京邮电大学出版社  
www.buptpress.com

信息安全专业系列教材

# 信息安全概论

(第2版)

牛少彰 崔宝江 李 剑 编著

北京邮电大学出版社

·北京·

## 内 容 简 介

本书在第1版的基础上进行了修改和完善,并补充了一些信息安全近几年的研究成果,全书内容更加翔实和新颖。本书全面介绍了信息安全的基本概念、原理和知识体系,主要内容包括信息保密技术、信息认证技术、PKI与PMI认证技术、密钥管理技术、访问控制技术、网络的攻击与防范、系统安全、网络安全技术和信息安全管理等内容。

本书内容全面,既有信息安全的理论知识,又有信息安全的实用技术。文字流畅,表述严谨,并包括信息安全方面的一些最新成果。本书可作为高等院校信息安全相关专业的本科生、研究生的教材或参考书,也可供从事信息处理、通信保密及与信息安全有关的科研人员、工程技术人员和技术管理人员参考。

### 图书在版编目(CIP)数据

信息安全概论/牛少彰,崔宝江,李剑编著.—2版.—北京:北京邮电大学出版社,2007

ISBN 978-7-5635-1486-1

I. 信… II. ①牛…②崔…③李… III. 信息系统—安全技术 IV. TP309

中国版本图书馆CIP数据核字(2007)第116573号

---

书 名:信息安全概论(第2版)

作 者:牛少彰 崔宝江 李 剑

责任编辑:张珊珊

出版发行:北京邮电大学出版社

社 址:北京市海淀区西土城路10号(邮编:100876)

北方营销中心:电话:010-62282185 传真:010-62283578

南方营销中心:电话:010-62282902 传真:010-62282735

E-mail: publish@bupt.edu.cn

经 销:各地新华书店

印 刷:北京市梦宇印务有限公司

开 本:787mm×960mm 1/16

印 张:17.25

字 数:370千字

印 数:1—5000册

版 次:2004年4月第1版 2007年9月第2版 2007年9月第1次印刷

---

ISBN 978-7-5635-1486-1/TN·509

定 价:28.00元

· 如有印装质量问题,请与北京邮电大学出版社营销中心联系 ·

# 信息安全专业系列教材(第2版)

## 编委会

主 编 杨义先

编 委 (排名不分先后)

章照止 钮心忻 牛少彰 徐国爱

卓新建 崔宝江 张 茹 谷利泽

郑康锋 辛 阳 李 剑 李 晖

裘晓峰 马春光

## 第 2 版总序

发展 21 世纪中国信息安全要靠教育,而搞好信息安全教育就需要好的教材。2004 年,北京邮电大学信息安全中心完成了第一套信息安全专业本科系列教材,该套教材被评为“北京市高等教育精品教材立项项目”,而后又被教育部列入“普通高等教育‘十五’国家级规划教材”。至今,三年多的时间过去了,这套教材在信息安全专业的教学中发挥了重要的作用,起到了较好的教学效果,受到教师和学生的好评。

在这三年中,我们始终致力于包括专业建设、课程建设、师资建设、教材建设、实训基地建设、实验室建设及校企就业(创业)平台建设等在内的信息安全本科专业的全面建设。2005 年,作为组长单位,我们完成了教育部“信息安全专业规范研究”和“信息安全学科专业发展战略研究”课题;召开了“全国高校本科‘信息安全专业规范与发展战略研究’成果发布与研讨会”;在国内第一次制定了信息安全专业规范,从知识领域、知识单元和知识点三个层次构建学科专业教学的知识体系;由通识教育内容、专业教育内容和综合教育内容三大部分构建课程参考体系;采用顶层设计的方法构建了带有实践性环节的教学体系;在国内第一次较全面地提出信息安全学科专业教学改革与创新研究的发展思路和政策建议,成果提交教育部教学指导委员会,对于引导高等学校信息安全学科专业教学改革与建设,指导信息安全学科专业评估,促进信息安全学科专业教学规范建设与管理,提高专业教育质量和水平有重要的作用。多所举办信息安全专业的高校都参照课题成果调整了自己的教学计划、课程体系和实验方案。

积极搭建信息安全专业校际交流平台。组织成立了“全国信息安全本科教材编写委员会”和“全国信息安全本科专业师资交流与培训互助组”。主持召开了“全国信息安全专业教学经验交流和师资培训研讨会”及“全国信息安全专业实验室建设和实验课程教学经验交流研讨会”。在四川绵阳建设了占地两万六千多平方米的全国信息安全专业本科生实习实训基地,接收了来自全国近 30 所高校的本科生进入该基地参加丰富多彩的实训。

努力建设精品课程。召开了“全国高校信息安全专业精品课程建设经验交流会议”,来自全国各地高校的专家齐聚北邮,介绍与交流了精品课程建设的经验。组织建设了全国第一批信息安全实验室,并且编写出版了信息安全实验指导教材,2007 年,我们的《现代密码学》课程申报了北京市精品课程,已经被专家评审通过,目前正在申报 2007 年度“国家精品课程”。

三年多的时间过去了,信息安全的教育和产业都取得了丰硕的成果,随着信息安全向更高层次的发展,其趋势已经从基础的网络层建设开始向内容层建设过渡。为适应信息安全教育的发展需要,积极探索培养创新型高素质人才,我们按照制定的学科发展战略和专业规范的精神,结合近几年的教学实践,对原信息安全专业本科系列教材进行了全面修订。这次修订不仅对原来的系列教材在第1版的基础上进行修改和完善,还补充了信息安全最新的研究成果,使教材的内容更加翔实和新颖。同时,在原有体系的基础上又增加了一些新的课程教材。在新修订的系列教材中,目前有《信息安全概论(第2版)》、《现代密码学及其应用》、《网络安全(第2版)》、《信息安全管理》、《计算机病毒原理与防治(第2版)》、《数字版权管理》、《计算机系统安全》、《网络安全实验教程》、《信息安全专业科技英语》、《防火墙、入侵检测与VPN》、《对称密码学及其应用》、《信息安全导论》等12本教材。随着信息安全专业教学的需要,今后还将不断有新的教材补充进来。希望通过对内容的精心组织和设计能促进信息安全课程的建设,同时涌现出更多的信息安全精品课程。

在这次修订中,我们组织了强大的师资队伍,将多次讲授相关课程的教师充实到本次修订队伍中。经过反复研讨,本着理论与实际相结合的原则,对原来的系列教材进行了较大的修改和扩充,我们希望这套新修订的系列教材能够满足国内各类高校信息安全本科专业以及相关方向的不同需求。

虽然我们在这次修订中投入了很大精力,但是由于水平有限,时间仓促,且信息安全专业的发展速度非常快,不足之处和错误在所难免,我们衷心期望使用和关心该系列教材的师生,继续对新的系列教材提出宝贵意见和建议。

本系列教材也是国家重点基础研究发展计划(973)(课题编号:2007CB310704和2007CB311203)资助的成果,并在积极申报“普通高等教育‘十一五’国家级规划教材”。

在本系列教材的修订过程中,得到了北京邮电大学出版社的大力支持,同时也得到了北京邮电大学信息安全中心成员的支持与配合,在此一并表示感谢。

教授、博士生导师、全国政协委员

杨义先

# 第 1 版前言

随着信息社会的到来,人们在享受信息资源所带来的巨大的利益的同时,也面临着信息安全的严峻考验。信息安全已经成为世界性的现实问题,信息安全问题已威胁到国家的政治、经济、军事、文化、意识形态等领域,同时,信息安全问题也是人们能否保护自己个人隐私的关键。信息安全是社会稳定安全的必要前提条件。本书全面介绍了信息安全的基本概念、原理和知识体系,主要内容包括信息保密技术、信息认证技术、访问控制技术、密钥管理技术、数据库安全、网络安全技术、信息安全标准和信息安全管理等内容。

本书内容全面,既有信息安全的理论知识,又有信息安全的实用技术,并包括信息安全方面的一些最新成果。本书可作为高等院校信息安全相关专业的本科生、研究生的教材或参考书,也可供从事信息处理、通信保密及与信息安全有关的科研人员、工程技术人员和技术管理人员参考。本书的教学时数约为 34 学时,每章后面均有小结并配有习题。

在本书编写的过程中,赵义斌参加了第 2 章和第 3 章初稿的编写,李志虎参加了第 7 章的编写,刘歆编写了第 9 章,郭春碌参加了第 6 章的编写,翟军华参加了第 8 章的编写,张晓芬、邓雁城、郭延龄、谢正程参加了书稿的讨论。此外,刘歆还在本书的整理和校对方面做了许多工作。

在本书的编写过程中,还得到了很多老师同学的关心和帮助。北京邮电大学出版社为本书的出版付出了大量的工作,借此表示衷心感谢。

限于编者水平有限,书中难免有疏漏和错误之处,恳请读者批评指正。

作 者

## 第 2 版前言

本书第 1 版在使用过程中得到了多方肯定,取得了较好的教学效果。结合近几年的教学实践,我们在第 1 版的基础上进行了修改和完善,并根据信息安全近几年的研究成果进行了补充,使全书内容更加翔实和新颖。全书进一步梳理了信息安全的基础理论部分,增加了对信息安全实际工作的指导,尽可能全面地反映信息安全近几年来的最新理论和技术成果。

本书除了保持第 1 版的内容外,还增加了以下内容和特色:

(1) 除全面介绍了信息安全的基本概念、原理和知识体系外,从信息安全技术、安全管理和政策法规 3 个方面论述了信息安全,并增加信息安全的实施指导,介绍了信息安全的防范原理和主要模型。

(2) 除详细论述了信息安全的核心技术,包括密码技术、信息认证技术、密钥管理技术以及信息安全研究的新领域——信息隐藏——外,对身份认证技术进行了较为详细的介绍,将 PKI 认证技术独立成为一章。

(3) 在网络安全技术部分,除修改原有的访问控制技术、防火墙技术、虚拟专用网技术、入侵检测技术和计算机病毒防治外,还介绍了目前普遍关心的内网安全技术方面的内容。

(4) 将原来的数据库安全技术改为系统安全,除修改原有的数据库安全外,对整个的系统安全进行了论述。

(5) 为了更好地做好信息安全的防范工作,做到知己知彼,增加了对网络攻击内容的介绍。

(6) 对整个信息安全管理部分进行整合,将原来的信息安全标准合并到信息安全管理部分,介绍了信息安全管理标准和整个流程。

通过补充和完善,使本书在同类教材中具有内容全面、题材新颖、全面反映近年来的最新成果、理论联系实际等特色。

在本书第 2 版中,第 8 章由崔宝江编写,第 10 章由牛少彰和李剑共同编写,其余各章由牛少彰编写,全书最后由牛少彰统稿。

信息安全概论第 2 版在新版的信息安全专业系列教材中将继续起到承上启下的作



用,对读者继续了解密码学在信息安全中的作用以及进入后续专题的学习进行衔接。同时,本书又自成体系,非信息安全专业可单独使用,用于全面了解信息安全领域的有关理论、概念、技术原理、实际工作指导和最新研究成果。

虽然我们尽力进行修订和创新,但是由于编者水平有限,时间仓促,书中难免有疏漏和错误之处,恳请使用和关心该教材的广大读者批评指正。

作 者

# 目 录

## 第 1 章 概述

1.1 信息的定义、性质和分类	1
1.1.1 信息的概念	1
1.1.2 信息的特征	3
1.1.3 信息的性质	4
1.1.4 信息的功能	4
1.1.5 信息的分类	5
1.2 信息技术	6
1.2.1 信息技术的产生	6
1.2.2 信息技术的内涵	7
1.3 信息安全概述	8
1.3.1 信息安全概念	8
1.3.2 信息安全属性	9
1.4 信息安全威胁	10
1.4.1 基本概念	10
1.4.2 安全威胁	10
1.4.3 网络攻击	13
1.5 信息安全的实现	14
1.5.1 信息安全技术	14
1.5.2 信息安全管理	18
1.5.3 信息安全与法律	18
1.5.4 网络的安全防范	19
小结	20
思考题	21

## 第 2 章 信息保密技术

2.1 古典密码	22
2.2 分组加密技术	28

2.2.1	基本概念	28
2.2.2	标准算法的介绍	29
2.2.3	分组密码的分析方法	42
2.3	公钥加密技术	43
2.3.1	基本概念	43
2.3.2	RSA 公钥密码算法	44
2.3.3	ElGamal 算法	46
2.3.4	椭圆曲线算法	47
2.4	流密码技术	48
2.4.1	流密码基本原理	48
2.4.2	二元加法流密码	50
2.4.3	几种常见的流密码算法	53
2.5	电子信封技术	54
2.6	信息隐藏技术	54
2.6.1	信息隐藏技术的发展	55
2.6.2	信息隐藏的特点	56
2.6.3	信息隐藏的方法	56
2.6.4	信息隐藏的攻击	58
	小结	59
	思考题	60

### 第 3 章 信息认证技术

3.1	Hash 函数和消息完整性	61
3.1.1	基本概念	61
3.1.2	常见的 Hash 函数	62
3.1.3	消息认证码	65
3.2	数字签名技术	66
3.2.1	数字签名的基本概念	66
3.2.2	常用的数字签名体制	68
3.2.3	盲签名和群签名	70
3.3	身份认证技术	72
3.3.1	基本概念	73
3.3.2	身份认证系统的分类	74
3.3.3	常见的身份认证技术	74
3.4	认证的具体实现	79
3.4.1	认证的具体实现与原理	79

3.4.2 认证方式的实际应用.....	83
小结 .....	86
思考题 .....	87

#### 第4章 PKI与PMI认证技术

4.1 数字证书.....	88
4.1.1 X.509数字证书.....	88
4.1.2 证书撤销列表.....	90
4.2 PKI系统.....	91
4.2.1 系统的功能.....	91
4.2.2 系统的组成.....	92
4.2.3 PKI相关标准.....	93
4.3 常用信任模型.....	94
4.4 基于PKI的服务 .....	94
4.4.1 核心服务.....	95
4.4.2 支撑服务.....	95
4.4.3 PKI的应用.....	95
4.5 PKI与PMI的关系 .....	96
4.5.1 授权管理.....	96
4.5.2 属性证书.....	97
4.5.3 PMI结构模型 .....	98
小结 .....	99
思考题 .....	99

#### 第5章 密钥管理技术

5.1 密钥管理概述 .....	100
5.2 对称密钥的管理 .....	102
5.2.1 对称密钥交换协议 .....	102
5.2.2 加密密钥交换协议 .....	103
5.3 非对称密钥的管理 .....	104
5.3.1 非对称密钥的技术优势 .....	104
5.3.2 非对称密钥管理的实现 .....	105
5.4 密钥管理系统 .....	105
5.4.1 基本概念 .....	106
5.4.2 密钥的分配 .....	106
5.4.3 计算机网络密钥分配方法 .....	108

5.4.4	密钥注入和密钥存储 .....	109
5.4.5	密钥更换和密钥吊销 .....	111
5.5	密钥产生技术 .....	112
5.5.1	密钥产生的制约条件 .....	112
5.5.2	如何产生密钥 .....	113
5.5.3	针对不同密钥类型的产生方法 .....	115
5.6	密钥的分散管理与托管 .....	116
5.6.1	密钥分散技术 .....	116
5.6.2	密钥的分散、分配和分发 .....	117
5.6.3	密钥的托管技术 .....	117
5.6.4	部分密钥托管技术 .....	119
	小结 .....	120
	思考题 .....	120

## 第 6 章 访问控制技术

6.1	访问控制的模型 .....	121
6.1.1	自主访问控制模型 .....	123
6.1.2	强制访问控制模型 .....	124
6.1.3	基于角色的访问控制模型 .....	126
6.1.4	基于任务的访问控制模型 .....	128
6.1.5	基于对象的访问控制模型 .....	130
6.1.6	信息流模型 .....	130
6.2	访问控制策略 .....	131
6.2.1	安全策略 .....	131
6.2.2	基于身份的安全策略 .....	132
6.2.3	基于规则的安全策略 .....	134
6.3	访问控制的实现 .....	134
6.3.1	访问控制的实现机制 .....	134
6.3.2	访问控制表 .....	134
6.3.3	访问控制矩阵 .....	135
6.3.4	访问控制能力列表 .....	135
6.3.5	访问控制安全标签列表 .....	136
6.3.6	访问控制实现的具体类别 .....	137
6.4	安全级别与访问控制 .....	138
6.5	访问控制与授权 .....	140
6.5.1	授权行为 .....	140

6.5.2	信任模型 .....	140
6.5.3	信任管理系统 .....	143
6.6	访问控制与审计 .....	143
6.6.1	审计跟踪概述 .....	143
6.6.2	审计内容 .....	144
	小结 .....	145
	思考题 .....	145

## 第7章 网络的攻击与防范

7.1	网络的攻击 .....	146
7.1.1	黑客与网络攻击 .....	146
7.1.2	网络攻击技术回顾与演变 .....	147
7.1.3	网络攻击的整体模型描述 .....	149
7.2	网络攻击实施和技术分析 .....	150
7.2.1	权限获取及提升 .....	151
7.2.2	缓冲区溢出攻击技术原理分析 .....	153
7.2.3	拒绝服务攻击技术原理分析 .....	154
7.3	网络防范的策略和方法 .....	156
7.3.1	网络安全策略 .....	156
7.3.2	网络防范的方法 .....	157
7.4	网络防范的原理及模型 .....	159
7.4.1	网络防范的原理 .....	159
7.4.2	网络安全模型 .....	160
	小结 .....	161
	思考题 .....	162

## 第8章 系统安全

8.1	操作系统安全 .....	163
8.1.1	操作系统攻击技术 .....	163
8.1.2	操作系统安全机制 .....	164
8.1.3	Windows XP 的安全机制 .....	165
8.2	软件系统安全 .....	166
8.2.1	软件系统攻击技术分析 .....	166
8.2.2	开发安全的程序 .....	168
8.2.3	IIS 应用软件系统的安全性 .....	169
8.3	数据库安全 .....	169

8.3.1	数据库攻击技术分析 .....	170
8.3.2	数据库安全的基本技术 .....	170
8.3.3	SQL Server 和 Oracle 的安全防范 .....	172
8.4	数据备份和恢复 .....	173
8.4.1	数据的安全威胁 .....	173
8.4.2	数据的加密存储 .....	174
8.4.3	数据备份和恢复技术 .....	174
	小结 .....	176
	思考题 .....	177

## 第 9 章 网络安全技术

9.1	防火墙技术 .....	178
9.1.1	防火墙的作用 .....	178
9.1.2	防火墙技术原理 .....	181
9.1.3	防火墙的体系结构 .....	184
9.1.4	基于防火墙的 VPN 技术 .....	187
9.2	入侵检测技术 .....	189
9.2.1	入侵检测概述 .....	189
9.2.2	IDS 类型 .....	192
9.2.3	IDS 基本技术 .....	194
9.3	安全扫描技术 .....	198
9.3.1	安全扫描技术概述 .....	198
9.3.2	端口扫描和漏洞扫描 .....	201
9.3.3	安全扫描器的原理和结构 .....	203
9.4	内外网隔离技术 .....	205
9.4.1	用户级物理隔离 .....	206
9.4.2	网络级物理隔离 .....	207
9.4.3	单硬盘物理隔离系统 .....	209
9.5	内网安全技术 .....	211
9.5.1	移动存储介质管理 .....	212
9.5.2	网络行为监控 .....	212
9.5.3	内网安全的解决方案 .....	213
9.6	反病毒技术 .....	214
9.6.1	病毒概论 .....	214
9.6.2	病毒的特征 .....	215
9.6.3	计算机病毒的分类 .....	216

9.6.4 反病毒技术 .....	217
9.6.5 邮件病毒及其防范 .....	221
小结 .....	222
思考题 .....	223
<b>第 10 章 信息安全的管理</b>	
10.1 信息安全的标准与规范 .....	224
10.1.1 信息安全标准的产生和发展 .....	224
10.1.2 信息安全标准的分类 .....	225
10.1.3 标准化组织简介 .....	230
10.2 信息安全管理标准 .....	232
10.2.1 BS 7799 的发展历程 .....	233
10.2.2 BS 7799 的主要内容 .....	234
10.2.3 ISO 13335 .....	238
10.3 信息安全策略和管理原则 .....	239
10.3.1 信息安全策略 .....	239
10.3.2 安全管理原则 .....	241
10.3.3 信息安全周期 .....	242
10.4 信息安全审计 .....	243
10.4.1 安全审计原理 .....	243
10.4.2 安全审计目的 .....	243
10.4.3 安全审计功能 .....	244
10.4.4 安全审计系统的特点 .....	244
10.4.5 安全审计分类和过程 .....	244
10.5 信息安全与政策法规 .....	245
10.5.1 一些国家的国家法律和政府政策法规 .....	245
10.5.2 一些国家的安全管理机构 .....	246
10.5.3 国际协调机构 .....	248
10.5.4 我国的信息安全管理与政策法规 .....	249
小结 .....	254
思考题 .....	254
参考文献 .....	255



# 第 1 章

## 概 述

随着现代通信技术的迅速发展和普及,特别是随着通信与计算机相结合而诞生的计算机互连网络全面进入千家万户,信息的应用与共享日益广泛,且更为深入。世界范围的信息革命激发了人类历史上最活跃的生产力,人类开始从主要依赖物质和能源的社会步入物质、能源和信息三位一体的社会。各种信息化系统已成为国家基础设施,支撑着电子政务、电子商务、电子金融、科学研究、网络教育、能源、通信、交通和社会保障等方方面面,信息成为人类社会必需的重要资源。

与此同时,信息的安全问题日渐突出,情况也越来越复杂。从大的方面来说,信息安全问题已威胁到国家的政治、经济、军事、文化、意识形态等领域,因此很早就有人提出了“信息战”的概念并将信息武器列为继原子武器、生物武器、化学武器之后的第四大武器。从小的方面来说,信息安全问题也涉及到人们能否保护个人的隐私。

信息安全已成为社会稳定安全的必要前提条件。

信息安全,即关注信息本身的安全,以防止偶然的或未授权者对信息的恶意泄露、修改和破坏,从而导致信息的不可靠或无法处理等问题,使得我们在最大限度地利用信息为我们服务的同时而不招致损失或使损失最小。

### 1.1 信息的定义、性质和分类

在人类社会的早期,人们对信息的认识比较肤浅和模糊,对信息的含义没有明确的定义。到了 20 世纪特别是中期以后,科学技术的发展,特别是信息科学技术的发展,对人类社会产生了深刻的影响,迫使人们开始探讨信息的准确含义。

#### 1.1.1 信息的概念

1928 年,哈特莱(L. V. R. Hartley)在《贝尔系统技术杂志》(BSTJ)上发表了一篇题