21世纪计算机科学与技术系列教材（本科）

信息安全概论

凌捷 谢赞福 编著

华南理工大学出版社

21 世纪计算机科学与技术系列教材(本科)

信息安全概论

凌　捷　谢赞福　**编著**

華南理工大學出版社

·广州·

内 容 简 介

本书系统地介绍了信息安全的理论、方法、技术和应用。主要内容包括：信息安全的概念、信息安全模型与标准、主要的加密算法及其理论基础、数字签名与身份认证、网络安全协议（SSL、SET、IPSec）、防火墙与反病毒技术、入侵检测系统、数据库加密与安全、安全审计与安全评估、电子商务安全、电子政务安全、WEB 应用安全等。

本书内容取材新颖、先进、实用，编排合理，可作为计算机科学与技术、软件工程、网络工程、电子信息、通信工程、自动化和管理信息系统等信息类专业的教材，也可供从事信息安全工作的管理人员和工程技术人员参考。

图书在版编目（CIP）数据

信息安全概论/凌捷，谢赞福编著. —广州：华南理工大学出版社，2005.8（2007.2 重印）

（21 世纪计算机科学与技术系列教材（本科））

ISBN 978-7-5623-2223-8

Ⅰ. 信… Ⅱ. ①凌…②谢… Ⅲ. 信息系统-安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2005）第 089130 号

总 发 行： 华南理工大学出版社（广州五山华南理工大学 17 号楼，邮编 510640）

营销部电话：020-87113487　87111048（传真）

E-mail: scutc13@scut.edu.cn　http://www.scutpress.com.cn

责任编辑： 詹志青　欧建岸

印 刷 者： 湛江日报社印刷厂

开　　本： 787mm×960mm　1/16　**印张：**25.5　**字数：**514 千

版　　次： 2005 年 8 月第 1 版　2007 年 2 月第 2 次印刷

印　　数： 3001～5000 册

定　　价： 35.50 元

编 委 会

总 序

放眼五洲风云，惊心世界科技。进入21世纪才短短几年，但科技进步更加日新月异。以信息科技为核心的高新技术的发展，极大地改变了人们的生产、生活方式和国际经济、政治关系，以经济为基础、科技为先导的综合国力竞争更为激烈。在这样激烈的竞争中，我们清醒地看到，我国生产力和科技、教育还比较落后，实现现代化，实现中华民族的伟大复兴还有很长的路要走。而在这方面，党中央已经明确提出，开发人力资源，加强人力资源能力的建设，是关系到我国发展的重大问题。培养和造就一代年轻人才，是一项紧迫而重大的战略任务。

培养和造就一代年轻人才，靠什么？靠教育，靠对年轻一代进行德智体美劳全方位的教育。培养一代掌握当前科技核心信息技术（计算机科学技术即是其重要分支）的人才，就要靠更加精心、更加有力度的教育。

而在计算机科学的教育中，除了教师、设备之外，重要的条件是教材。教师、设备、教材三者互为补充，构成计算机科学教育不可或缺的要素。在某种意义下，教材还可以认为是前导性的。惟其如此，计算机器协会（ACM）在1968年，当美国许多大学刚刚设立计算机科学系的时候，就集中了全美国计算机科学的权威教授、专家和各主要大学的代表，制定了计算机科学教育的基本框架、课程设置以及各门课程的基本内容和大纲。美国那个时期的课程设置和教材，几乎无一例外都是根据“课程表68”的思想形成和编写的。而后电气与电子工程师学会（IEEE）也参与了制定计算机科学教育的计划。作为迎接新世纪的重要举措，他们一起推出了反映当代计算机科学前沿知识和全面要求（所谓全面要求，指它不仅讨论了专业知识的内容，还讨论了知识产权、计算机病毒防范、伦理道德、职业规范、社会影响等问题）的ACM和IEEE“课程表2001”。在众多的学科门类中，对于青年一代的教育予以如此重视的，除计算机科学外，大概无第二个了。这既反映了计算机科学（包括作为其总体的信息科学技术）的核心地位，也反映了教材在教育中的特殊地位。

也就在1968年，当年的图灵奖获得者理·W·汉明（R W Hamming）

走向图灵奖讲演台时谈到:“我们需要为我们的学生到2000年时做准备,那时他们许多人即将达到他们事业的顶峰。”我们也要立足现在,把教育的目标放到30年后,我们现在的教育也要为到2035年时我们的学生做准备,那时他们许多人即将达到他们事业的顶峰。根据我国发展的规划,这也就是我国进入建国100周年倒计时的时刻,就是我们要实现中华民族全面复兴的时候,就是我国在综合国力要名列世界前茅的时候。因此,我们现在就要为这一个宏伟目标做准备。

任重而道远。我国现在还很难说已经有了能和上面所述ACM和IEEE“课程表2001”在思路上、在内容上相符的教材。我们认为,在教材建设上,借鉴和采用个别的外文教材是可以的和无碍的,但是如同整个教育必须走我们自己的路一样,在教材建设上我们也一定要走自己的路。

广东省作为经济大省强省,现在明确提出要成为教育强省。作为在广东的计算机科学工作者,我们深感自己在发展我国特别是广东省的计算机科学教育中责任重大。因此,我省计算机学会与华南理工大学出版社共同组织了全省各高等院校计算机专业骨干教师编写这套《21世纪计算机科学与技术本科系列教材》,希望这套教材能为计算机专业提供优秀的教学用书。这套教材以培养未来人才为目标,以ACM和IEEE“课程表2001”为指导,结合我国计算机教育实际情况,以着力提倡创新精神和提倡实践动手能力为主线,注重教材内容的系统性、科学性和准确性以及文字的流畅性、可读性。

我们虔诚希望我们的努力能切切实实推动我国,特别是广东省计算机教育水平上一个台阶。

姜云飞
韩国强
苏运霖

2003年9月

前　言

21 世纪将人类带入了信息时代，在社会信息化的进程中，信息已成为社会发展的重要资源。信息技术革命给人类带来的高效率和高效益是否能真正实现，很大程度上取决于信息安全能否得以保证。

信息安全是近几年迅速发展起来的新兴学科，随着网络应用的不断普及，其重要性日益突出，世界各国都给予极大的关注和投入。信息安全保障体系是 21 世纪综合国力、国际竞争力的重要组成部分，影响国家的全面发展和长远利益。随着信息安全技术与信息安全产业的快速发展，社会对信息安全人才的需求在不断增加。在高等教育领域大力推进信息安全的专业化教育，将是国家在信息安全领域掌握自主权、占领先机的重要举措。我国教育部已将“信息安全概论”课程列入计算机、电子信息、通信、管理信息等信息类专业的教学计划中，而且越来越多的高校开设了本科信息安全专业。科技部门也加大了支持力度，国家“863”和“975”计划都专门设立了信息安全主题，重点支持信息安全领域关键技术的研究和产业化。有关部门也出台了相应的法规、标准、指南，成立了相应的测评认证机构，加强对信息安全的监管。

信息安全是一个综合的交叉学科，涉及数学、计算机、通信、信息、法律、管理等许多学科，内容广泛。本书有侧重地介绍信息安全的基础理论和技术原理，分别阐述了信息安全的概念，密码学概论（选择有代表性的对称密码系统 DES、公钥密码系统 RSA、ELGamal、椭圆曲线密码系统 ECC），数字签名技术与身份认证技术，网络安全协议，防火墙与反病毒技术，入侵检测系统，数据库加密技术，安全审计与安全评估，网络应用的安全等内容。每章均配备了一定数量的习题。为让读者更好地掌握基本概念、基本原理及基本技能，理论联系实际，本书的第 10 章还提供信息安全防范实训指导。

本书共 10 章，其中第 1、第 2、第 4、第 5、第 7、第 8 章由凌捷编写，第 3、第 6、第 9 章及第 10 章由谢赞福编写，全书由凌捷统稿。本书的编写得到华南理工大学出版社的大力支持以及广东省高校学科建设项目的资助，也得到了很多学者的鼓励和帮助。书中直接和间接引用了一些较新的安全标准及同行专家的研究结果，资讯来源已在参考文献列出。广东工业大学计算机学院的研究生徐少强、李红蕾、谢锐、李振军等为本书的编写做了很多工作，在此一并表示感谢。

随着信息技术的不断进步和社会需求的变化，信息安全技术也将不断地发展，我们希望本书的出版能为我国的计算机和信息安全教育事业的发展起到添砖

加瓦的作用，也希望得到各位读者的支持，并期待着与大家共同探讨信息安全技术的发展动向及课程教学的体会。由于编者水平所限，书中错漏在所难免，敬请读者和同行专家批评指正。

作　者

2005 年 5 月于广州

目　录

1 概　论 …… (1)
1.1 信息安全的概念 …… (1)
1.2 信息安全的主要内容 …… (3)
1.2.1 物理安全 …… (3)
1.2.2 运行安全 …… (3)
1.2.3 管理和策略 …… (4)
1.3 信息安全的模型 …… (7)
1.3.1 多级安全模型 …… (8)
1.3.2 多边安全模型 …… (11)
1.4 信息安全的标准 …… (13)
1.4.1 信息安全标准的分类 …… (13)
1.4.2 安全管理标准 BS 7799 简介 …… (14)
1.5 信息安全的发展趋势 …… (20)
本章小结 …… (21)
练习与思考 …… (22)
2 密码学概论 …… (23)
2.1 古典密码体制 …… (26)
2.1.1 Caesar 密码 …… (26)
2.1.2 Playfair 密码 …… (28)
2.1.3 Vigenere 密码 …… (29)
2.1.4 Hill 密码 …… (30)
2.1.5 转轮技术 …… (31)
2.2 对称密码体制 …… (33)
2.2.1 DES …… (33)
2.2.2 AES …… (53)
2.3 公钥密码体制 …… (56)
2.3.1 RSA 算法 …… (57)
2.3.2 ELGamal 算法 …… (62)

2.3.3 ECC 算法 …… (64)
本章小结 …… (68)
练习与思考 …… (68)
3 数字签名与身份认证 …… (69)
3.1 报文鉴别 …… (69)
3.1.1 报文鉴别概述 …… (69)
3.1.2 报文摘要 MD 算法 …… (72)
3.1.3 报文加密函数 …… (73)
3.2 散列函数 …… (74)
3.2.1 一个简单散列函数 …… (75)
3.2.2 单向散列函数 …… (76)
3.2.3 散列函数的一般结构 …… (77)
3.2.4 压缩函数的构造原理 …… (78)
3.3 数字签名体制 …… (79)
3.3.1 RSA 数字签名体制 …… (79)
3.3.2 ELGamal 数字签名体制 …… (80)
3.3.3 DSS 数字签名体制 …… (83)
3.3.4 数字签名中的问题与改进 …… (84)
3.3.5 数字签名的发展方向 …… (85)
3.4 身份认证技术 …… (86)
3.4.1 身份鉴别 …… (86)
3.4.2 Kerberos 网络用户认证系统 …… (89)
3.4.3 电话远程身份认证技术 …… (89)
3.4.4 基于在线手写签名的身份认证技术 …… (90)
3.4.5 公钥基础设施 PKI …… (91)
3.4.6 授权管理基础设施 PMI …… (92)
3.4.7 数字证书认证中心 …… (93)
3.4.8 数字证书的应用 …… (94)
3.5 身份认证的实现 …… (96)
3.5.1 拨号认证协议 …… (96)
3.5.2 Kerberos 认证协议 …… (101)
3.5.3 X.509 认证协议 …… (107)
本章小结 …… (108)

练习与思考 …… (109)

4 网络安全协议 …… (111)

4.1 SSL 协议 …… (111)

4.1.1 SSLv3 概况 …… (111)

4.1.2 SSLv3 协议的结构 …… (113)

4.1.3 SSL 记录层协议 …… (114)

4.1.4 修改密文规约协议 …… (117)

4.1.5 告警协议 …… (117)

4.1.6 握手协议 …… (118)

4.1.7 密码计算 …… (125)

4.2 SET 协议 …… (126)

4.2.1 SET 概述 …… (126)

4.2.2 双向签名 …… (127)

4.2.3 SET 系统结构 …… (128)

4.2.4 SET 证书 …… (130)

4.2.5 支付处理 …… (131)

4.3 IPSec 协议 …… (135)

4.3.1 IPSec 概述 …… (135)

4.3.2 IPSec 的安全体系结构 …… (137)

4.3.3 IPSec 服务 …… (138)

4.3.4 IPSec 的工作模式 …… (139)

4.3.5 认证头（AH）协议 …… (140)

4.3.6 封装安全载荷（ESP）协议 …… (144)

4.3.7 安全关联 …… (146)

4.3.8 安全数据库 …… (147)

4.3.9 密钥管理和密钥交换 …… (151)

本章小结 …… (162)

练习与思考 …… (163)

5 防火墙与反病毒技术 …… (164)

5.1 防火墙的概念 …… (164)

5.1.1 防火墙的概念及作用 …… (164)

5.1.2 防火墙的发展 …… (167)

5.1.3 防火墙的分类 …… (170)
5.2 包过滤型防火墙 …… (174)
5.2.1 包过滤的原理 …… (174)
5.2.2 包过滤技术的发展 …… (175)
5.2.3 包过滤规则 …… (175)
5.2.4 包过滤的设置 …… (176)
5.2.5 数据包过滤特性 …… (179)
5.2.6 包过滤的缺点 …… (186)
5.3 代理服务器型防火墙 …… (186)
5.3.1 代理服务器的原理 …… (187)
5.3.2 代理型防火墙的发展 …… (189)
5.3.3 代理服务器的物理形式 …… (190)
5.3.4 代理服务器的特点 …… (191)
5.4 防火墙的体系结构 …… (191)
5.4.1 双宿主主机防火墙 …… (192)
5.4.2 屏蔽主机防火墙 …… (193)
5.4.3 屏蔽子网防火墙 …… (194)
5.5 防火墙的局限性 …… (197)
5.6 计算机病毒及其特征 …… (201)
5.7 计算机病毒分析 …… (204)
5.7.1 计算机病毒的组成 …… (204)
5.7.2 计算机病毒的工作原理 …… (205)
5.7.3 计算机病毒的传播途径 …… (208)
5.7.4 计算机病毒的检测 …… (209)
5.7.5 计算机病毒的清除技术 …… (210)
本章小结 …… (213)
练习与思考 …… (213)

6 入侵检测系统 …… (215)
6.1 入侵检测原理 …… (215)
6.1.1 基本概念 …… (215)
6.1.2 入侵检测系统 …… (216)
6.1.3 入侵检测原理 …… (218)
6.1.4 入侵检测系统的分类 …… (221)

6.1.5　入侵检测系统结构 …… (223)
6.2　入侵检测的数学模型 …… (232)
6.3　入侵检测的特征分析 …… (233)
6.3.1　特征分析 …… (233)
6.3.2　协议分析 …… (236)
6.3.3　入侵检测过程 …… (238)
6.4　入侵检测响应机制 …… (242)
6.4.1　入侵检测系统的通用模型 …… (242)
6.4.2　对响应的需求 …… (244)
6.4.3　自动响应 …… (244)
6.4.4　蜜罐 …… (245)
6.4.5　主动攻击模型 …… (247)
6.5　常见入侵检测系统的比较 …… (247)
6.5.1　入侵检测系统的部署 …… (247)
6.5.2　目前入侵检测产品存在的若干问题 …… (250)
6.5.3　RealSecure 简介 …… (251)
6.5.4　Cisco Secure IDS …… (253)
6.5.5　瑞星入侵检测系统 RIDS－100 …… (255)
6.5.6　IDS 的若干补充工具 …… (257)
6.5.7　入侵防御系统（IPS） …… (258)
6.6　入侵检测技术的发展趋势 …… (260)
6.6.1　评价入侵检测系统性能的指标 …… (260)
6.6.2　入侵检测系统存在的主要问题 …… (261)
6.6.3　入侵技术的发展与演化 …… (262)
6.6.4　入侵检测技术研发动态 …… (262)
6.6.5　入侵检测技术的发展方向 …… (264)
本章小结 …… (265)
练习与思考 …… (265)

7　数据库加密与安全 …… (269)
7.1　数据库安全的概念 …… (269)
7.1.1　数据库简介 …… (269)
7.1.2　数据库的安全要求 …… (271)
7.1.3　数据库的完整性 …… (273)

7.1.4 数据库的安全性与恢复 …… (275)
7.1.5 数据库安全标准 …… (276)
7.2 数据库加密技术 …… (279)
7.2.1 数据库加密的必要性 …… (279)
7.2.2 数据库加密的特点 …… (280)
7.2.3 数据库加密的技术要求 …… (281)
7.2.4 数据库加密方法 …… (282)
7.2.5 数据库加密的不同层次 …… (287)
7.2.6 数据库加密系统 …… (288)
7.2.7 数据库加密系统的有关问题 …… (290)
7.3 数据库安全策略 …… (291)
7.3.1 安全分析 …… (291)
7.3.2 安全代理模型 …… (292)
7.3.3 DM3 的安全技术 …… (292)
7.3.4 自主访问与强制访问控制 …… (293)
7.3.5 隐通道分析技术 …… (293)
7.3.6 安全性策略 …… (294)
7.4 Oracle 的安全访问控制 …… (297)
7.5 SQL Server 安全性简介 …… (299)
7.5.1 安全层次和模式 …… (299)
7.5.2 SQL Server 的登录和服务器角色 …… (300)
7.5.3 SQL Server 数据库访问 …… (301)
7.5.4 SQL Server 权限的授予 …… (302)
7.6 SYBASE 的安全管理 …… (303)
本章小结 …… (306)
练习与思考 …… (306)

8 安全审计与安全评估标准 …… (307)
8.1 安全审计的原理 …… (307)
8.2 安全审计应用实例 …… (308)
8.2.1 Windows NT 中的安全审计 …… (308)
8.2.2 UNIX、Linux 中的安全审计 …… (311)
8.3 国内安全评估标准 …… (315)
8.3.1 概述 …… (315)

8.3.2 GB 17859—1999 …… (317)
8.4 国际安全评估标准 …… (320)
8.4.1 TCSEC …… (320)
8.4.2 通用准则 CC …… (326)
8.5 系统备份与灾难恢复 …… (337)
8.5.1 系统备份的定义 …… (337)
8.5.2 系统备份的主要技术 …… (337)
8.5.3 灾难备份建设的流程 …… (339)
本章小结 …… (342)
练习与思考 …… (343)

9 网络应用安全 …… (344)
9.1 网络应用安全概述 …… (344)
9.1.1 应用安全服务 …… (344)
9.1.2 应用安全的风险 …… (345)
9.1.3 应用安全需求 …… (346)
9.2 应用安全的体系结构 …… (346)
9.3 因特网的安全 …… (347)
9.3.1 因特网服务的安全隐患 …… (347)
9.3.2 因特网的脆弱性 …… (348)
9.4 Web 站点安全 …… (350)
9.4.1 安全策略制定原则 …… (350)
9.4.2 配置 Web 服务器的安全特性 …… (351)
9.4.3 排除站点中的安全漏洞 …… (351)
9.4.4 监视控制 Web 站点出入情况 …… (352)
9.5 网络监听 …… (353)
9.5.1 监听的可能性 …… (353)
9.5.2 在以太网中的监听 …… (353)
9.5.3 网络监听检测 …… (354)
9.6 E-mail 的安全 …… (355)
9.6.1 E-mail 工作原理及安全漏洞 …… (356)
9.6.2 匿名转发 …… (356)
9.6.3 E-mail 欺骗 …… (357)
9.6.4 E-mail 轰炸和炸弹 …… (357)

9.7 IP 电子欺骗 …… (357)
9.7.1 盗用 IP 地址 …… (357)
9.7.2 IP 电子欺骗的定义 …… (358)
9.7.3 IP 欺骗的对象及实施 …… (358)
9.7.4 IP 欺骗攻击的防备 …… (359)
9.8 口令安全 …… (359)
9.8.1 口令破解过程 …… (360)
9.8.2 设置安全的口令 …… (360)
9.9 电子商务安全 …… (361)
9.9.1 电子商务安全技术的发展 …… (361)
9.9.2 电子商务安全策略 …… (362)
9.9.3 SSL 协议 …… (363)
9.10 电子政务安全 …… (364)
9.10.1 电子政务面临的安全问题 …… (364)
9.10.2 电子政务安全策略 …… (365)
9.10.3 电子政务安全技术框架 …… (367)
9.11 WebST 网络应用安全平台 …… (368)
9.11.1 WebST 提供的安全功能 …… (368)
9.11.2 WebST 技术特点 …… (369)
9.11.3 WebST 与 CA + AAs 的解决方案 …… (370)
本章小结 …… (370)
练习与思考 …… (370)

10 信息安全防范实训指导 …… (372)
10.1 防火墙的安装与设置 …… (373)
10.2 防病毒软件的使用 …… (375)
10.3 密码学的应用 …… (376)
10.3.1 加密和解密软件的设计 …… (376)
10.3.2 使用 PGP 实现电子邮件安全 …… (376)
10.4 应用平台的安全设置 …… (377)
10.4.1 BIOS 密码和计算机开机密码的配置 …… (377)
10.4.2 Windows NT/2000/2003 的权限配置与安全审核 …… (378)
10.4.3 本地入侵 Windows NT 系统 …… (379)
10.4.4 网络监听获取 Windows NT 普通用户密码 …… (380)

10.4.5　远程攻击 Windows 2000 系统 …… (381)
10.4.6　Windows NT/2000/2003 的诊断与修复操作 …… (382)
10.4.7　如何发现系统漏洞——使用 X-SCANNER 扫描工具 …… (382)
10.4.8　如何发现系统漏洞——使用 X-Ray 对网络进行扫描 …… (383)
10.4.9　使用 Sniffer Pro 网络分析器 …… (383)
10.4.10　在 IIS 中限制对 WWW 的访问 …… (384)
10.4.11　在 IIS 中配置安全的 FTP 服务 …… (384)
10.4.12　响应的身份认证 …… (385)
10.4.13　剖析特洛伊木马 …… (385)
10.5　数据库安全配置 …… (386)
参考文献 …… (387)