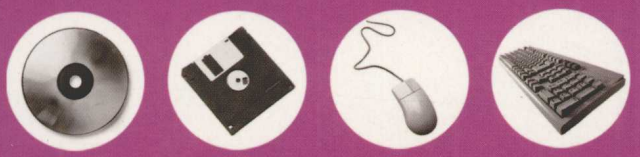
高等院校计算机系列教材

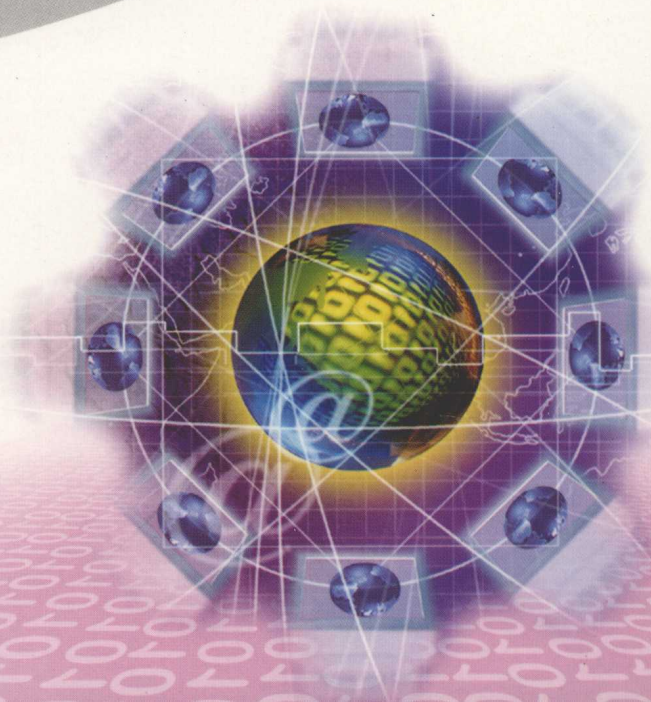


GAODENGYUANXIAO
JISUANJI
XILIEJIAOCAI

网络与信息安全

总主编：陈火旺　主　编：李峰　李平

湖南省计算机学会规划教材　中南大学出版社



WLYXXAQ
WANGLUO
YUXINXI ANQUAN

高等院校计算机系列教材

GAODENGYUANXIAO JISUANJI XILIEJIAOCAI

网络与信息安全

总主编：陈火旺　湖南省计算机学会规划教材　中南大学出版社

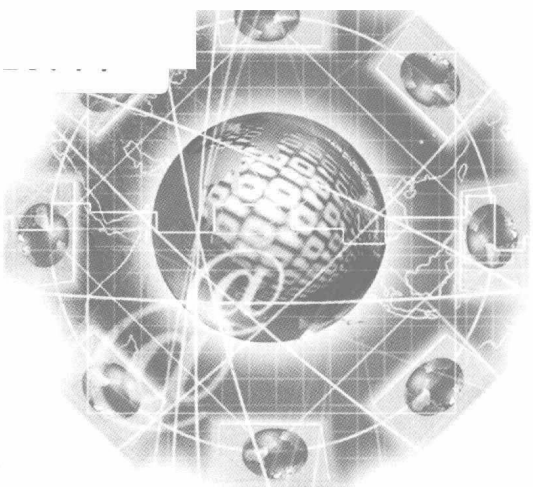
主　编：李　峰　李　平

副主编：鲁荣波　邓晓衡　王　静　蔡碧野

编　委：（按姓氏笔画排序）

刘　青　刘军万　李梦醒　张连明

谭　邦



图书在版编目(CIP)数据

网络与信息安全/李峰,李平主编. —长沙:中南大学出版社,2005.8

ISBN 7-81105-153-2

Ⅰ.网... Ⅱ.①李...②李... Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2005)第 074574 号

网络与信息安全

李峰 李平 主编

□责任编辑 邓立荣
□责任印制 文桂武
□出版发行 中南大学出版社
社址:长沙市麓山南路 邮编:410083
发行科电话:0731-8876770 传真:0731-8710482
□印 装 核工业 230 研究所印刷厂

□开 本 787×1092 1/16 □印张 17.5 □字数 432 千字
□版 次 2005 年 8 月第 1 版 □2005 年 8 月第 1 次印刷
□书 号 ISBN 7-81105-153-2/TP·018
□定 价 25.00 元

高等院校计算机系列教材编委会

总　序

21 世纪，人类社会已经步入信息时代，信息产业推动着全球经济的蓬勃发展，改变着人类的联系与交换方式，从某种意义上说，信息革命是人类历史上又一次深刻的社会变革。无疑，在以信息产业为基础的知识经济社会中，计算机科学与技术具有举足轻重的地位。有鉴于此，当今世界各国皆把培养高素质的创新型计算机科学与技术专业人才作为一项重要的战略任务来抓。早在 1984 年，邓小平同志就强调指出："计算机的普及要从娃娃抓起"，从此开启了中国信息革命的征程。经过 20 多年的努力，我国的计算机教育虽然取得了令人瞩目的成就，但离知识经济社会的要求还有很大的差距。据 2005 年信息产业部的数据显示，我国的信息化人才资源指数仅为 13.43，每年短缺信息化专业人才达 100 万之多。因此，快速培养和造就一大批高素质的计算机与信息人才，乃是我国高等教育所面临的一项严峻挑战。为此，我们必须改革和完善现有计算机与信息技术学科的教学计划和课程体系，优化课程结构，精炼教学内容，拓宽专业基础，强化实践环节，注重学生的知识、能力和综合素质的培养。

为了适应计算机科学与技术学科发展和教育的需要，湖南省计算机学会，参照《中国计算机科学与技术学科教程 2002》，组织了一批长期从事计算机科学与技术专业教学与科研的学者参与编撰了这套由中南大学出版社出版的《高等院校计算机系列教材》，希望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，以优秀教材促进教学质量的提高。该系列教材具有如下特点：

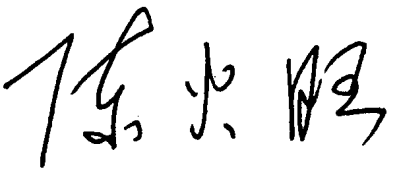
1. 教材参照《中国计算机科学与技术学科教程 2002》建议的教学大纲、知识领域、知识单元和知识点，结合作者多年教学与科研经验来编写，注重基本理论、基础知识的梳理、推演与挖掘，注意知识的更新，跟踪新技术、新成果的发展，并将之吸收到教材中来，力求开阔学生视野，逐步形成"基础课程精深，专业课程宽新"的格局，努力提高教材质量。

2. 注重理论联系实际，注意能力培养。力图通过案例教学、课堂讨论、课程实验设计与实习，训练学生掌握知识、运用知识分析并解决实际问题的能力以满足学生今后从事科研和就业的需要。

3. 在规范教材编写体例的同时，注重写作风格的灵活性：每册的每个章节包括教学目的、本章小结、思考题与练习题，每门教材都配有 PPT 电子教案，并做到层次分明、逻辑性强、概念清楚、图文并茂、表达准确、可读性强。

这套教材的编写吸纳了广大计算机科学与技术教育工作者多年的教学与科研成果，凝聚了作者们的辛勤劳动，也得到了湖南省各高等院校相关专业领导和专家的大力支持。我相信这套教材的出版，对我国计算机科学与技术专业本科教学质量的提高将有很好的促进作用。

由于编委和作者们水平与时间的限制，教材中难免还有不足之处，恳请广大读者批评指正。



2005 年 7 月

前 言

随着互联网络的迅猛发展，安全问题越来越引起人们的关注。由于其开放性和匿名性的特点，互联网络在改变着人们的工作效率和生活方式，给社会、企业乃至个人带来了前所未有的便利的同时，也决定了单纯的互联网不可避免地存在信息安全隐患。从当初的计算机网络病毒的产生和传播，到现在网络犯罪、信用欺诈等带有明显破坏性的网络恶意行为的出现，无一不说明了信息网络安全绝不仅是IT行业内的问题，而是一个社会问题，是一个包括多学科的系统安全工程问题。

从学科研究的角度来看，信息安全是一个综合性强、交叉性广的学科领域，涉及数学、通信、计算机等诸多学科的知识和研究成果。正由于网络与信息安全问题是当前研究的热点以及网络应用的焦点问题，越来越多的高等院校先后开设了信息安全等相关课程。本书作为湖南省计算机学会组织编写的《湖南省高等院校计算机课程系列教材》之一，根据安全技术的最新研究成果和研究进展，结合平时的教学体会，编写而成。

本书注重跟踪网络与信息安全领域内的最新研究成果，比较全面系统地介绍了：安全基础理论，包括信息安全理论基础、对称及非对称加密体系、数字签名及安全验证机制等；互联网络中常用的安全技术，包括IPSec技术、网络安全的集成技术、PKI体系、Web及电子邮件的安全性，以及操作系统的安全等；新型网络应用中的信息安全技术，如在无线及Adhoc网络中的安全应用研究等。本书紧紧围绕“互联网络中的信息安全”这个中心主题，以基础理论、技术机制再到应用实践为线索对信息安全进行了有重点的阐述，力图使读者能够较全面地了解网络与信息安全领域内要研究的问题、相应的解决机制，并能逐渐地培养出运用安全技术在具体实践中解决实际问题的能力。

全书共分13章。教学过程中教师可根据具体情况酌情选用本书的相关章节。同时，本书也配备了相应的多媒体课件，供授课教师参考。全书由李峰教授和李平博士担任主编，其中第1章由李峰编写，第2章由李平编写，第3、4章由鲁荣波编写，第5章由刘青编写，第6章由蔡碧野编写，第7章由李梦醒编写，第8、9章由王静编写，第10章由张连明编写，第11章由邓晓衡编写，第12章由刘军万编写，第13章由谭邦编写，另外，王静、蔡碧野还参与了全书的统稿工作。本书在编写过程中得到了湖南省计算机学会和中南大学出版社的大力支持，孙星明教授、肖建华教授、曾碧卿副教授认真审阅了全书，提出了大量宝贵的修改意见。在此深表感谢！

随着安全技术研究的深入和应用领域的延伸，网络与信息安全的内涵在不断地丰富和充实。由于编者水平有限，我们对这一新兴领域的研究还不很深入，书中难免存在错误和不足之处，欢迎广大读者和专家提出批评改进意见。

本书配有PPT电子课件，需要使用的教师请与出版社联系。电子邮箱：hn－cyz@163.com。

编 者

2005年7月

目 录

第1章 概 论

本章介绍了如下几个方面的内容：①信息安全的基本概念；②网络的脆弱性及安全威胁；③安全机制与安全策略；④安全评估标准；⑤网络安全模型。通过本章的学习，要求学生达到以下几点教学要求：

(1)掌握信息安全的基本概念，了解网络与信息安全的背景及研究的主要问题。

(2)了解网络系统的脆弱性和信息安全面临的安全主要威胁。

(3)掌握安全机制与安全策略中的基本要素。

(4)了解安全评估标准，掌握网络安全模型。

1.1 信息安全基本概念

人类已进入21世纪，无处不在的计算机网络连接了科研、文化、经济与国防等各个领域，数字化、信息化、网络化正在冲击、影响、改变着人类社会的各个方面。以Internet为代表的全球性信息化浪潮日益深刻，信息网络技术的应用正日益普及和广泛，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展，典型的如党政部门信息系统、金融业务系统、企业商务系统等。伴随网络的普及，安全问题日益成为影响网络效能的重要问题，而Internet所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求。这主要表现在：开放性的网络，导致网络技术是全开放的，任何个人或团体都可能获得，因而网络所面临的破坏和攻击可能是多方面的，如可能来自物理传输线路的攻击，也可以对网络通信协议和实现实施攻击，可以是对软件实施攻击，也可以是对硬件实施攻击。随着计算机及网络技术的飞速发展，网络中不安全因素也在逐渐增加。因此，不强化网络化的信息安全保障，不解决信息安全问题，信息化将不可能持续、健康地发展。

究竟什么是信息安全呢？根据词典上的解释，“安全”有两层含义：其一指“平安，无危险”；其二是“保护，保全”。在具体应用和实践中，情况就相当复杂了。从安全需求角度来讲，信息安全应包括以下六个基本要素：机密性、完整性、可靠性、可用性、可控性和不可抵赖性等，其主要特征表现如下：

- 机密性(Confidentiality)：机密性是网络信息不被泄露给非授权的用户、实体或过程，不被非法利用，即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性，如信息的加密传输、数据的保密存储等。机密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

- 完整性(Integrity)：完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。

• 可靠性(Reliability)：可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定的功能的特性。可靠性是系统安全的最基本要求之一，是所有网络信息系统的建设和运行目标。可靠性可以用公式描述为 R = MTBF/(MTBF + MTTR)，其中 R 表示可靠性，MTBF 表示平均故障间隔时间，MTTR 表示平均故障修复时间。因此，增大可靠性的有效思路是增大平均故障间隔时间或者减少平均故障修复时间。增大可靠性的具体措施包括：提高设备质量，严格质量管理，配备必要的冗余和备份，采用容错、纠错和自愈等措施，选择合理的拓扑结构和路由分配，强化灾害恢复机制，分散配置和负荷等。可靠性测度主要有三种：抗毁性、生存性和有效性。

• 可用性(Availability)：可用性是网络信息可被授权实体访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。

• 可控性 (Controllability)：可控性是指可以控制授权范围内的信息流向及行为方式，对信息的传播及内容具有控制能力。为保证可控性，首先系统能够控制谁能够访问系统和网络上的数据，以及如何访问(是只读还是可以修改等)，通常通过访问控制列表等方法来实现；其次需要对网络上的用户进行验证，可通过握手协议和鉴别进行身份验证；最后要将用户的所有活动记录下来便于查询审计。

• 不可抵赖性(Non - repudiation)：不可抵赖也称作不可否认性，是指在网络信息系统的信息交互过程中，确信参与者的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

概括地说，网络与信息安全的核心是通过计算机、网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储的消息的机密性、完整性、可靠性、可用性、可控性和不可抵赖性等。

国际标准化组织(International Standardization Organization，ISO)对信息安全的定义是："为数据处理系统建立和采用的技术和管理上的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。"此定义偏重于静态信息保护，而且没有考虑网络的因素。另一种考虑到网络因素的定义是："保护网络系统中的各种资源(包括计算机和网络设备、存储介质、软件、数据等)不因偶然或恶意的原因而遭到占用、毁坏、更改和泄露，系统能够连续正常运行 。"此定义侧重于动态意义的描述。

网络与信息安全是一门涉及计算机科学、网络技术、密码技术、通信技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。信息安全是一个关系国家安全和主权、社会稳定、民族文化的继承和发扬的重要问题。并且其重要性正随着全球信息化步伐的加快而变到越来越重要，信息安全问题刻不容缓。