

21
世纪

高职高专新概念教材

蔡立军 主 编

李立明 李 峰 副主编

计算机网络安全技术

21 Shi Ji Gao Zhi Gao Zhuan Xin Gai Nian Jiao Cai



中国水利水电出版社
www.waterpub.com.cn

21 世纪高职高专新概念教材

计算机网络安全技术

蔡立军 主编

李立明 李 峰 副主编

中国水利水电出版社

内 容 提 要

本书详细地介绍了计算机网络安全技术的基础理论、原理及其实现方法。内容包括：计算机网络安全技术概论、实体安全与硬件防护技术、计算机软件安全技术、网络安全防护技术、备份技术、密码技术与压缩技术、数据库系统安全、计算机病毒及防治、防火墙技术和系统平台与网络站点的安全。全书涵盖了计算机网络安全需要的“攻、防、测、控、管、评”等多方面的基础理论和实施技术。

本书从工程应用角度出发，立足于“看得懂、学得会、用得上”，在内容安排上将理论知识与工程应用有机结合，突出适应性、实用性和针对性。书中介绍的许多安全配置实例都来自作者多年的实践，读者可在今后工作中直接应用。

本书可以作为高职高专计算机专业及相近专业和本科计算机相近专业的教材，也可作为计算机网络安全培训、自学教材；也是网络工程技术人员、网络管理员、信息安全管理技术人员的技术参考书。本书还为授课教师免费提供电子教案，此教案用 PowerPoint 制作，可以任意修改。需要者请与北京万水电子信息有限公司联系，联系电话：(010) 68359168-331。

图书在版编目 (CIP) 数据

计算机网络安全技术 / 蔡立军主编. — 北京：中国水利水电出版社，2001
(21 世纪高职高专新概念教材)

ISBN 7-5084-0891-8

I. 计… II. 蔡… III. 计算机网络—安全技术—高等学校：技术学校—教材 IV. TP393.08

中国版本图书馆 CIP 数据核字 (2001) 第 084640 号

书 名	计算机网络安全技术
主 编	蔡立军
副 主 编	李立明 李 峰
出版 发行	中国水利水电出版社 (北京市三里河路 6 号 100044) 网址: www.waterpub.com.cn E-mail: mchannel@263.net (万水) sales@waterpub.com.cn 电话: (010) 63202266 (总机)、68331835 (营销中心)、82562819 (万水)
经 售	全国各地新华书店和相关出版物销售网点
排 版	北京万水电子信息有限公司
印 刷	北京蓝空印刷厂
规 格	787mm×1000mm 16 开本 22.25 印张 484 千字
版 次	2002 年 1 月第 1 版 2004 年 12 月第 6 次印刷
印 数	23001—28000 册
定 价	28.00 元

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换

版权所有·侵权必究

21 世纪高职高专新概念教材

编委会名单

主任委员 刘 晓 柳菊兴

副主任委员 胡国铭 张栾勤 王前新 黄元山 柴 野
张建钢 陈志强 宋 红 汤鑫华 王国仪

委 员 (按姓氏笔画排序)

马洪娟	马新荣	尹朝庆	方 宁	方 鹏
毛芳烈	王 祥	王乃钊	王希辰	王国思
王明晶	王泽生	王绍卜	王春红	王路群
东小峰	台 方	叶永华	宁书林	田 原
田绍槐	申 会	刘 猛	刘尔宁	刘慎熊
孙明魁	安志远	许学东	闫 菲	何 超
宋锦河	张 晞	张 慧	张弘强	张怀中
张晓辉	张浩军	张海春	张曙光	李 琦
李存斌	李作纬	李珍香	李家瑞	李晓桓
杨永生	杨庆德	杨名权	杨均青	汪振国
肖晓丽	闵华清	陈 川	陈 炜	陈语林
陈道义	单永磊	周杨娣	周学毛	武铁敦
郑有想	侯怀昌	胡大鹏	胡国良	费名瑜
赵 敬	赵作斌	赵秀珍	赵海廷	唐伟奇
夏春华	徐 红	徐凯声	徐雅娜	殷均平
袁晓州	袁晓红	钱同惠	钱新恩	高寅生
曹季俊	梁建武	蒋金丹	蒋厚亮	覃晓康
谢兆鸿	韩春光	詹慧尊	雷运发	廖哲智
廖家平	管学理	蔡立军	黎能武	魏 雄

项目总策划 雨 轩

编委会办公室 主 任 周金辉

副主任 孙春亮 杨庆川

参编学校名单

(按第一个字笔划排序)

- | | |
|---------------|--------------|
| 三门峡职业技术学院 | 华中科技大学 |
| 山东大学 | 华东交通大学 |
| 山东交通学院 | 华北电力大学工商管理学院 |
| 山东建工学院 | 华北航天工业学院 |
| 山东省电子工业学校 | 江汉大学 |
| 山东农业大学 | 江西渝州电子工业学院 |
| 山东省农业管理干部学院 | 江西赣西学院 |
| 山东省教育学院 | 西安外事学院 |
| 山东商业职业技术学院 | 西安欧亚学院 |
| 山西阳泉煤炭专科学校 | 西安铁路运输职工大学 |
| 山西运城学院 | 西安联合大学 |
| 山西经济管理干部学院 | 孝感职业技术学院 |
| 广州市职工大学 | 杨陵职业技术学院 |
| 广州铁路职业技术学院 | 昆明冶金高等专科学校 |
| 中华女子学院山东分院 | 武汉大学动力与机械学院 |
| 中国人民解放军第二炮兵学院 | 武汉大学信息工程学院 |
| 中国矿业大学 | 武汉工业学院 |
| 中南大学 | 武汉工程职业技术学院 |
| 天津市一轻局职工大学 | 武汉广播电视大学 |
| 天津职业技术师范学院 | 武汉化工学院 |
| 长沙大学 | 武汉电力职业技术学院 |
| 长沙民政职业技术学院 | 武汉交通管理干部学院 |
| 长沙交通学院 | 武汉科技大学工贸学院 |
| 长沙航空职业技术学院 | 武汉商业服务学院 |
| 长春汽车工业高等专科学校 | 武汉理工大学 |
| 北京对外经济贸易大学 | 武汉铁路职业技术学院 |
| 北京科技大学职业技术学院 | 河南济源职业技术学院 |
| 北京科技大学成人教育学院 | 郑州工业高等专科学校 |
| 石油化工管理干部学院 | 陕西师范大学 |
| 石家庄师范专科学校 | 南昌水利水电高等专科学校 |
| 辽宁交通高等专科学校 | 哈尔滨金融专科学校 |
| 华中电业联合职工大学 | 济南大学 |

序

根据 1999 年 8 月教育部高教司制定的《高职高专教育基础课程教学基本要求》(以下简称《基本要求》)和《高职高专教育专业人才培养目标及规格》(以下简称《培养规格》)的精神,由中国水利水电出版社北京万水电子信息有限公司精心策划,聘请我国长期从事高职高专教学、有丰富教学经验的教师执笔,在充分汲取了高职高专和成人高等学校在探索培养技术应用性人才方面取得的成功经验和教学成果的基础上,撰写了此套《21 世纪高职高专新概念教材》。

为了编写本套教材,出版社进行了广泛的调研,走访了全国百余所具有代表性的高等专科学校、高等职业技术学院、成人教育高等院校以及本科院校举办的二级职业技术学院在广泛了解情况、探讨课程设置、研究课程体系的基础上,经过学校申报、征求意见、专家评选等方式,确定了本套书的主编,并成立了编委会。每本书的编委会聘请了多所学校主要学术带头人或主要从事该课程教学的骨干,教学大纲的确定以及教材风格的定位均经过编委会多次认真讨论。

本套《21 世纪高职高专新概念教材》有如下特点:

(1) 面向 21 世纪人才培养的需求,结合高职高专学生的培养特点,具有鲜明的高职高专特色。本套教材的作者都是长期在第一线从事高职高专教育的骨干教师,对学生的基本情况、特点和认识规律等有深入的了解,在教学实践中积累了丰富的经验。因此可以说,每一本书都是教师们长期教学经验的总结。

(2) 以《基本要求》和《培养规格》为编写依据,内容全面,结构合理,文字简练,实用性强。在编写过程中,作者严格依据教育部提出的高职高专教育“以应用为目的,以必需、够用为度”的原则,力求从实际应用的需要(实例)出发,尽量减少枯燥、实用性不强的理论概念,加强了应用性和实际操作性强的内容。

(3) 采用“问题(任务)驱动”的编写方式,引入案例教学和启发式教学方法,便于激发学习兴趣。本套书的编写思路与传统教材的编写思路不同:先提出问题,然后介绍解决问题的方法,最后归纳总结出一般规律或概念。我们把这个新的编写原则比喻成“一棵大树、问题驱动”的原则。即:一方面遵守先见(构建)“树”(每本书就是一棵大树),再见(构建)“枝”(书的每一章就是大树的一个分枝),最后见(构建)“叶”(每章中的若干小节及知识点)的编写原则;另一方面采用问题驱动方式,每一章都尽量用实际中的典型实例开头(提出问题、明确目标),然后逐渐展开(分析解决问题),在讲述实例的过程中将本章的知识点融入。这种精选实例,并将知识点融于实例中的编写方式,可读性、可操作性强,非常适合高职高专的学生阅读和使用。本书读者通过学习构建本书中的“树”,由“树”找“枝”,

济南交通高等专科学校
济南铁道职业技术学院
荆门职业技术学院
贵州无线电工业学校
贵州电子信息职业技术学院
恩施职业技术学院
黄冈职业技术学院
黄石计算机学院
湖北工学院
湖北丹江口职工大学
湖北交通职业技术学院
湖北汽车工业学院
湖北经济管理大学

湖北药检高等专科学校
湖北经济学院
湖北教育学院
湖北鄂州大学
湖北水利水电职业技术学院
湖南大学
湖南工业职业技术学院
湖南计算机高等专科学校
湖南省轻工业高等专科学校
湖南涉外经济学院
湖南郴州师范专科学校
湖南商学院
湖南税务高等专科学校

前 言

计算机网络安全问题是各国、各部门、各行业以及每个计算机用户都十分关注的重要问题。随着 Internet 与 Intranet 的普及和广泛应用,计算机技术和网络技术已深入到社会的各个领域,人类对计算机、对网络的依赖程度越来越大。计算机网络安全问题也变得越来越大,成为了维护国家和社会稳定的一个焦点。为了提高我国各级计算机网络主管部门的安全意识,普及计算机网络安全知识,提高国内的安全技术水平,有效地保护我国计算机网络安全,对高职高专计算机专业及相近专业和本科计算机相近专业学生开设计算机网络安全技术课程十分必要,也很迫切。这门课程是计算机网络课程的延伸,涉及到的问题也正是广大网络工程技术人员极为关心的、亟待解决的问题。

本书从工程应用角度出发,立足于“看得懂、学得会、用得上”,方法与技术并重,深入浅出、循序渐进。全书共 10 章,主要内容有:计算机网络安全技术概论(第一章);实体安全与硬件防护技术(第二章);软件系统安全(第三章);网络安全防护技术(第四章);数据信息安全,包括备份技术、密码技术与压缩技术、数据库安全等(第五、六、七章);病毒防治技术(第八章);网络站点安全,包括防火墙技术、系统平台的安全、Web 站点安全、防黑客技术(第九、十章)。每章都有典型案例。全书涵盖了计算机网络安全需要的“攻、防、测、控、管、评”等多方面的基础理论和实施技术。

作为面向 21 世纪的高职高专新概念教材,本书选题适当,以必需、够用为度,讲清概念、结合实际、强化训练,突出适应性、实用性和针对性,有利于学生学以致用,解决实际工作中所遇到的问题,是一本计算机网络安全和安全管理维护的实用教材。

本书具有教材和技术资料的双重特征,既可以作为高职高专计算机专业及相近专业和本科计算机相近专业教材,也适合作为计算机网络安全的培训、自学教材,同时也是网络管理员、信息安全管理人員和网络工程技术人员的技术参考资料。

本书配有电子教案(用 PowerPoint 制作,可以任意修改),使用本教材的学校可以与水利电力出版社联系。

本书由蔡立军主编,李立明、李峰任副主编。参加本书编写大纲讨论与部分编写工作的有:雷建军、舒望皎、杜红兵等。刘红飞、凌红武、邓玉华、陈霞、陈知、余俊良、李中发、罗俊、周志芳、唐美玲、张宝红、蔡辉、黄生群等做了本书的文字录入和图表制作工作。在此一一表示感谢。

由于作者水平有限,书中的错误和缺点在所难免,欢迎读者批评指正。

编 者

2001 年 8 月于岳麓山

顺“枝”摸“叶”，最后达到构建自己所需要的“树”的目的。

(4) 配有实验指导和实训教程，便于学生练习提高。

(5) 配有动感电子教案。为顺应教育部提出的教材多元化、多媒体化发展的要求，每本教材都配有电子教案，以满足广大教师进行多媒体教学的需要。电子教案用 PowerPoint 制作，教师可根据授课情况任意修改。

(6) 提供相关教材中所有程序的源代码，方便教师直接切换到系统环境中教学，提高教学效果。

总之，本套教材凝聚了数百名高职高专一线教师多年的教学经验和智慧，内容新颖，结构完整，概念清晰，深入浅出，通俗易懂，可读性、可操作性和实用性强。

本套教材适用于高等职业学校、高等专科学校、成人及本科院校举办的二级职业技术学院和民办高校。

新世纪吹响了我国高职高专教育蓬勃发展的号角，新世纪对高职教育提出了新的要求，高职教育占据了全面素质教育中所不可缺少的地位，在我国高等教育事业中占有极其重要的位置，在我国社会主义现代化建设事业中发挥着日趋显著的作用，是培养新世纪人才所不可缺少的力量。相信本套《21 世纪高职高专新概念教材》的出版能为高职高专的教材建设和教学改革略尽绵薄之力，因为我们提供的不仅是一套教材，更是自始至终的教育支持，无论是学校、机构培训还是个人自学，都会从中得到极大的收获。

当然，本套教材肯定会有不足之处，恳请专家和读者批评指正。

21 世纪高职高专新概念教材编委会

2001 年 3 月

目 录

序

前言

第一章 计算机网络安全技术概论	1
本章学习目标	1
1.1 计算机网络安全概念	1
1.2 计算机网络系统面临的威胁	3
1.2.1 计算网络系统面临的威胁	3
1.2.2 安全威胁的来源	5
1.2.3 威胁的具体表现形式	7
1.3 计算机网络系统的脆弱性	7
1.3.1 操作系统安全的脆弱性	7
1.3.2 网络安全的脆弱性	8
1.3.3 数据库管理系统安全的脆弱性	9
1.3.4 防火墙的局限性	9
1.3.5 其他方面的原因	9
1.4 计算机网络安全技术的研究内容和发展过程	9
1.4.1 研究内容	9
1.4.2 发展过程	11
1.5 计算机网络安全的三个层次	12
1.5.1 安全立法	12
1.5.2 安全管理	19
1.5.3 安全技术措施	19
1.6 网络安全的设计和基本原则	19
1.6.1 安全需求	20
1.6.2 网络安全设计应考虑的问题	21
1.6.3 网络安全系统设计的基本原则	22
1.6.4 网络安全设计的关键	25
1.7 安全技术评价标准	26
本章小结	29
习题一	29

第二章 实体安全与硬件防护技术.....	31
本章学习目标.....	31
2.1 实体安全技术概述.....	31
2.1.1 影响实体安全的主要因素.....	32
2.1.2 实体安全的内容.....	32
2.2 计算机房场地环境的安全防护.....	33
2.2.1 计算机房场地的安全要求.....	33
2.2.2 设备防盗.....	34
2.2.3 机房的三度要求.....	34
2.2.4 防静电措施.....	35
2.2.5 电源.....	35
2.2.6 接地与防雷.....	37
2.2.7 计算机场地的防火、防水措施.....	41
2.3 安全管理.....	42
2.3.1 硬件资源的安全管理.....	42
2.3.2 信息资源的安全与管理.....	42
2.3.3 健全机构和岗位责任制.....	43
2.3.4 完善的安全管理规章制度.....	44
2.4 电磁防护.....	47
2.5 硬件防护.....	49
2.5.1 存储器保护.....	50
2.5.2 虚拟存储保护.....	51
2.5.3 输入/输出通道控制.....	52
本章小结.....	52
习题二.....	53
第三章 计算机软件安全技术.....	54
本章学习目标.....	54
3.1 计算机软件安全技术概述.....	54
3.2 文件加密技术.....	56
3.2.1 数据文件加密原理.....	56
3.2.2 可执行文件的加密方式.....	57
3.3 软件运行中的反跟踪技术.....	59
3.3.1 跟踪工具及其实现.....	59
3.3.2 软件运行中的反跟踪技术.....	59
3.3.3 实例：编制具有反跟踪功能的加密盘.....	62

3.4	防止非法复制软件的技术	63
3.4.1	软件加密的必要性	64
3.4.2	常用的防止非法复制软件的技术	64
3.4.3	实例：几种加密软件的使用原理及方法	73
3.5	保证软件质量的安全体系	76
3.5.1	概述	76
3.5.2	软件故障的分类	77
3.5.3	软件测试工具	79
	本章小结	79
	习题三	80
第四章	网络安全防护技术	81
	本章学习目标	81
4.1	网络安全概述	81
4.1.1	网络安全的定义	81
4.1.2	网络安全的研究内容	82
4.1.3	Internet 安全面临的威胁	83
4.1.4	个人上网用户面临的网络陷阱	88
4.2	计算机网络的安全服务和安全机制	89
4.2.1	计算机网络的安全服务	89
4.2.2	计算机网络的安全机制	90
4.2.3	安全服务和安全机制的关系	94
4.2.4	安全服务机制的配置	94
4.2.5	安全服务与层的关系的实例	98
4.3	网络安全防护措施	99
4.3.1	网络的动态安全策略	99
4.3.2	网络的安全管理与安全控制机制	100
4.3.3	网络安全的常规防护措施	103
4.3.4	网络安全控制措施	106
4.3.5	网络安全实施过程中需要注意的一些问题	110
	本章小结	113
	习题四	113
第五章	备份技术	114
	本章学习目标	114
5.1	备份技术概述	114
5.1.1	备份的基本知识	115

5.1.2	网络备份	118
5.1.3	数据失效与备份的意义	118
5.1.4	与备份有关的概念	119
5.2	备份技术与备份方法	120
5.2.1	硬件备份技术	120
5.2.2	软件备份技术	124
5.2.3	双机互联硬件备份方法	125
5.2.4	利用网络资源备份	127
5.2.5	系统备份软件——Norton Ghost	128
5.2.6	同步动态备份软件——Second Copy 2000	131
5.2.7	多平台网络备份系统——Amanda	133
5.2.8	重新认识 Windows 98 的备份技术	135
5.3	备份方案的设计	138
5.3.1	系统备份方案的要求及选择	138
5.3.2	日常备份制度设计	142
5.3.3	灾难恢复措施设计	144
5.4	典型的网络系统备份方案实例	145
5.4.1	基于 CA ARC Serve 的备份方案设计	145
5.4.2	一个证券网络系统的备份方案	146
	本章小结	147
	习题五	148
第六章	密码技术与压缩技术	149
	本章学习目标	149
6.1	密码技术概述	149
6.1.1	密码通信系统的模型	150
6.1.2	密码学与密码体制	150
6.1.3	加密方式和加密的实现方法	153
6.2	加密方法	155
6.2.1	加密系统的组成	155
6.2.2	四种传统加密方法	155
6.3	密钥与密码破译方法	158
6.4	常用信息加密技术介绍	160
6.4.1	DES 算法	160
6.4.2	IDEA 算法	162
6.4.3	RSA 公开密钥密码算法	163

6.4.4	典型 HASH 算法——MD5 算法.....	167
6.4.5	信息认证技术.....	168
6.5	Outlook Express 下的安全操作实例	169
6.6	数据压缩	171
6.6.1	数据压缩概述.....	171
6.6.2	ARJ 压缩工具的使用.....	172
6.6.3	WinZip 的安装和使用	175
	本章小结	177
	习题六	177
第七章	数据库系统安全	179
	本章学习目标	179
7.1	数据库系统简介	179
7.2	数据库系统安全概述	181
7.2.1	数据库系统的安全性要求.....	181
7.2.2	数据库系统的安全的含义.....	183
7.2.3	数据库的故障类型	183
7.2.4	数据库系统的基本安全架构.....	185
7.2.5	数据库系统的安全特性	186
7.3	数据库的数据保护	187
7.3.1	数据库的安全性.....	187
7.3.2	数据库中数据的完整性.....	191
7.3.3	数据库并发控制.....	192
7.4	死锁、活锁和可串行化.....	194
7.4.1	死锁与活锁.....	194
7.4.2	可串行化.....	195
7.4.3	时标技术.....	196
7.5	数据库的备份与恢复	197
7.5.1	数据库的备份	197
7.5.2	数据库的恢复.....	198
7.6	攻击数据库的常用方法	199
7.7	数据库系统安全保护实例	201
7.7.1	SQL Server 数据库的安全保护	201
7.7.2	Oracle 数据库的安全性策略	207
	本章小结	211
	习题七	211

第八章 计算机病毒及防治	212
本章学习目标	212
8.1 计算机病毒概述	212
8.1.1 计算机病毒的定义	212
8.1.2 计算机病毒的发展历史	212
8.1.3 计算机病毒的分类	216
8.1.4 计算机病毒的特点	217
8.1.5 计算机病毒的隐藏之处和入侵途径	218
8.1.6 现代计算机病毒的流行特征	219
8.1.7 计算机病毒的破坏行为	221
8.1.8 计算机病毒的作用机制	221
8.2 DOS 环境下的病毒	224
8.2.1 DOS 基本知识介绍	224
8.2.2 常见 DOS 病毒分析	227
8.3 宏病毒	230
8.3.1 宏病毒的分类	231
8.3.2 宏病毒的行为和特征	231
8.3.3 宏病毒的特点	232
8.3.4 宏病毒的防治和清除方法	232
8.4 网络计算机病毒	236
8.4.1 网络计算机病毒的特点	236
8.4.2 网络对病毒的敏感性	237
8.4.3 网络病毒实例——电子邮件病毒	239
8.5 反病毒技术	241
8.5.1 计算机病毒的检测	241
8.5.2 计算机病毒的防治	243
8.5.3 计算机感染病毒后的修复	247
8.6 软件防病毒技术	248
8.6.1 防、杀毒软件的选择	248
8.6.2 反病毒软件	250
8.6.3 常用反病毒软件产品	252
8.7 典型病毒实例——CIH 病毒介绍	252
8.7.1 CIH 病毒简介	252
8.7.2 恢复被 CIH 病毒破坏的硬盘信息	253
8.7.3 CIH 病毒的免疫	255

本章小结	255
习题八	256
第九章 防火墙技术	257
本章学习目标	257
9.1 防火墙技术概述	257
9.1.1 防火墙的定义	257
9.1.2 防火墙的发展简史	258
9.1.3 设置防火墙的目的和功能	259
9.1.4 防火墙的局限性	260
9.1.5 防火墙技术发展动态和趋势	261
9.2 防火墙技术	262
9.2.1 防火墙的技术分类	262
9.2.2 防火墙的主要技术及实现方式	269
9.2.3 防火墙的常见体系结构	274
9.3 防火墙设计实例	276
9.3.1 防火墙产品选购策略	276
9.3.2 典型防火墙产品介绍	279
9.3.3 防火墙设计策略	280
9.3.4 Windows 2000 环境下防火墙及 NAT 的实现	281
本章小结	285
习题九	286
第十章 系统平台与网络站点的安全	287
本章学习目标	287
10.1 Windows NT 系统的安全性	287
10.1.1 Windows NT 的 Registry 的安全性	287
10.1.2 NT 服务器和工作站的安全漏洞及解决建议	289
10.1.3 NT 与浏览器有关的安全漏洞及防范措施	297
10.1.4 基于 Windows NT 操作系统的安全技术	301
10.1.5 Windows 操作系统的安全维护技术	304
10.2 UNIX 系统的安全性	306
10.2.1 UNIX 系统安全	306
10.2.2 UNIX 网络安全	311
10.3 Web 站点的安全	320
10.3.1 Web 站点安全概述	320
10.3.2 Web 站点的安全策略	321

10.4 反黑客技术.....	325
10.4.1 黑客的攻击步骤.....	325
10.4.2 黑客的手法.....	326
10.4.3 防黑客技术.....	329
10.4.4 黑客攻击的处理对策.....	330
本章小结.....	331
习题十.....	331
附录.....	332
附录 A 常用备份工具软件.....	332
附录 B 黑客与计算机安全站点.....	336
参考文献.....	338