

高职高专计算机专业系列教材

袁家政 编著

计算机网络安全 与应用技术



高职高专计算机专业系列教材

计算机网络安全与 应用技术

袁家政 编著

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书是一本面向高职高专和成人高等教育的教材,是作者长期从事计算机网络教学和网络设计的经验总结。

本书主要从网络安全的基本知识、密码技术、防火墙技术、Windows 98/NT/2000 系统的安全、黑客技术与防范措施、网络防毒技术、Internet/Intranet 的安全性和实训等几个方面编写,全书共 9 章。

本书突出计算机网络安全的管理、配置及维护的操作,紧紧跟踪网络安全的最新成果和发展方向。书中提供大量网络安全与对抗的实例,并从实例中引出概念,然后进行归纳总结,帮助读者掌握计算机网络安全的基本原理,了解计算机现有系统的安全设置、安全漏洞,从而胜任一般系统的安全设计及管理维护工作。

本书适合于广大在校学生学习,也可供有关工程技术人员阅读。

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

计算机网络安全与应用技术/袁家政编著. —北京:清华大学出版社,2002

高职高专计算机专业系列教材

ISBN 7-302-05636-6

I. 计… II. 袁… 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(2002)第 045426 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.tsinghua.edu.cn>

责任编辑: 徐跃进

印 刷 者: 北京市人民文学印刷厂

发 行 者: 新华书店总店北京发行所

开 本: 787×1092 1/16 **印张:** 24.25 **字数:** 559 千字

版 次: 2002 年 8 月第 1 版 2002 年 8 月第 1 次印刷

书 号: ISBN 7-302-05636-6/TP·3322

印 数: 0001~8000

定 价: 30.00 元

序

1999年10月,教育部高教司主持召开了全国高职高专教材工作会议,会议要求尽快组织规划和编写一批高质量的、具有高职高专特色的基础和专业教材。根据会议精神,在清华大学出版社的支持下,于2000年1月在上海召开了由来自全国各地的部分高职、高专、成人教育及本科院校的代表参加的“高职高专计算机专业培养目标和课程设置体系研讨会”。与会的专家和教师一致认为,在当前教材建设严重滞后同高职教育迅速发展的矛盾十分突出的情况下,编写一套适应高等职业教育培养技术应用性人才要求的、真正具有高职特色的、体系完整的计算机专业系列教材十分必要而且迫切。会议成立了高职高专计算机专业系列教材编审委员会,明确了高职计算机专业的培养目标,即掌握计算机专业有关的基本理论、基本知识和基本技能,尤其要求具有对应用系统的操作使用、维护维修、管理和初步开发的能力。

根据上述目标,编委会拟定了本套教材的编写原则。在教材内容安排上,以培养计算机应用能力为主线,构造该专业的课程设置体系和教学内容体系;从计算机应用需求出发进行理论教学,强调理论教学与实验实训密切结合,尤其突出实践体系与技术应用能力的实训环节的教学;教材编写力求内容新颖、结构合理、概念清楚、实用性强、通俗易懂、前后相关课程有较好的衔接。与本科教材相比,本套教材在培养学生的应用技能上更有特色。

根据目前各高职高专院校计算机专业的课程设置情况,编委会确定了首批出版的十几本教材。这些教材的作者多是在高职高专院校或本科院校的职业技术学院任教的、具有多年教学经验的教师,每本书均由计算机专业的资深教授或专家主审把关。我们还将在此基础上,陆续征集出版第二、三批教材,力争在3到5年内完成一套完整的高职高专计算机专业教材。

应当说明的是,凡是高等职业教育、高等专科学校教育和成人高等院校的计算机及其相关专业均可使用本套教材。各学校可以根据实际需要,在教学中适当增删一些内容、实训项目和练习题,从而更有针对性地帮助学生掌握计算机专业知识,并形成相关的应用能力。

由于各地区各学校在教学水平、培养目标理解等方面有所不同,加上这套教材编写时间仓促,难免会出现这样或那样的错误,敬请各学校在使用过

程中及时将修改意见或好的建议返回给教材编审委员会,以便我们及时修订、改版,使该系列教材日趋完善。

我们恳切地希望高职高专院校任课的专业教师和专家对后续教材的编写提出建设性的意见,并真诚地希望各位教师参与我们的工作。

高职高专计算机专业
系列教材编审委员会

2000年5月

前言

随着计算机网络技术的发展,网络安全问题越来越受关注。网络技术已被广泛应用于社会生活直至国防等各个方面,网络安全已超越其本身而达到国家安全问题的高度,因此非常必要在高校开设计算机网络安全课程教学。

本书是由教育部和清华大学联合策划和出版的高职《计算机网络安全与应用技术》教材,是作者长期从事计算机网络教学的经验和多年网络设计及实践的总结。

作为高等职业教育的教材,本书在介绍网络安全理论及其基础知识的同时,突出计算机网络安全方面的管理、配置及维护的实际操作手法和手段,并尽量跟踪网络安全技术的最新成果与发展方向。全书主要内容包括网络安全的基本概念、密码技术、防火墙技术、Windows 98/NT/2000 系统的安全、黑客技术与防范措施、网络病毒技术、Internet/Intranet 的安全性和实训问题等,总共分 9 章。各方面知识内容所占比例为:网络安全理论知识 30%;网络系统(主要指 Windows 98/NT/2000、Internet/Intranet)的安全技术特点 20%;网络安全配置、操作维护和安全应用方面的知识 50%。本书的教学内容大约需要 64 课时,最好另外安排 32 小时的实训。书中以 * 标记的少量选读内容由各校教师酌情确定是否讲授。

计算机网络安全主要包括网络系统的安全和网络信息的安全,一般通过密码技术和访问控制技术实现。鉴于此,本书的主要内容安排如下所示。

第一部分(第 1~3 章)主要介绍了计算机网络安全基础知识和网络安全的理论知识。第 1 章具体介绍计算机网络安全的相关基础知识,网络安全存在的问题,黑客、密码技术、数字签名和访问控制技术等基本概念,网络安全的体系结构,网络安全的策略防范问题和网络安全的发展方向;第 2 章介绍了网络安全中的密码技术,包括传统的加密方法、DES 加密标准、公开密钥体制和数字签名等技术;第 3 章介绍了访问控制技术中的防火墙的技术,包括防火墙的原理、种类和实现策略等。

第二部分(第 4、5 章)是计算机网络系统的安全性问题。第 4 章主要介绍网络系统的安全等级,Windows 98 的安全机制、安全漏洞和防范措施;第 5 章详细介绍了流行的计算机网络系统 Windows NT/2000 的网络机制、网

络安全模型、密码技术和访问控制技术、安全漏洞和防范措施等方面的知识。

第三部分(第6章)介绍黑客技术与防范措施。主要讲述常见的黑客技术,如网络监听、端口扫描、口令破解和木马等,同时以 Windows NT/2000 为实例介绍了黑客攻击网络系统的主要步骤和防范措施。

第四部分(第7章)讲述网络病毒原理与防范。主要介绍了病毒的原理、病毒的类型和计算机网络病毒,同时介绍了几种影响较大的网络病毒,如 CIH 病毒、Word 宏病毒、Nimda 病毒和红色代码病毒等,并且讲述了病毒的清除及防护措施。

第五部分(第8章)是 Internet/Intranet 的安全性问题。主要介绍 Internet/Intranet 的脆弱性和提供的信息服务的安全缺陷,并介绍了 IE 浏览器中 Cookies 技术、Java 技术和 ActiveX 技术带来的安全问题,以及电子邮件的安全和 IIS Web 服务器的安全问题及配置方法。

第六部分(第9章)主要是有关网络安全的实训问题。其中囊括了与本书全部内容相关的实训,针对密码技术、防火墙技术、Windows 98/NT/2000、IE 浏览器、Outlook Express 和 IIS 等知识及安全性安排了十几个实训。

通过对该书的学习,读者可掌握计算机网络安全的基本原理和当今流行的网络系统 Windows 98/NT/2000 系统安全设置、安全漏洞、管理及维护,同时对 Unix/Linux 及 Internet/Intranet 等系统的安全有一定的了解,并且能够胜任一般网络安全、防火墙的策略与实现、黑客原理与防范及简单网络安全应用策略程序的开发。

全书主要由北京联合大学信息学院袁家政策划和主编,付百文、赵淑红和张翼编写了部分内容,在编写过程中参考并摘录了大量国内外计算机网络安全书籍中的部分内容,并从 Internet 网络中下载了大量计算机网络安全、黑客技术与防范措施的资料。由于计算机网络安全技术发展迅速,作者的学识有限,加上时间仓促,书中难免有所疏漏,敬请广大读者批评指正。来信地址:jzyuan@sohu.com。

本书在编写过程中得到了清华大学出版社的大力支持,在此深表感谢。

编 者

2002 年 8 月

目 录

第 1 章 计算机网络安全的基础知识	1
1.1 计算机网络基础知识	1
1.1.1 计算机网络体系结构	2
1.1.2 Internet 网络	6
1.2 计算机网络存在的安全问题	14
1.2.1 什么使网络通信不安全	14
1.2.2 影响计算机网络安全因素	15
1.2.3 Internet 网络存在的安全缺陷	17
1.3 网络安全体系结构	20
1.3.1 网络安全系统的功能	20
1.3.2 安全功能在 OSI 模型中的位置	21
1.4 网络安全技术	26
1.4.1 什么是黑客	26
1.4.2 常用的网络安全技术	27
1.4.3 密码技术	28
1.4.4 数字签名	30
1.4.5 访问控制技术	31
1.5 实现网络安全的策略问题	34
1.5.1 网络安全的特征	34
1.5.2 网络安全策略与安全机制	34
1.5.3 网络安全的实现	36
1.6 计算机网络安全立法	38
1.6.1 计算机网络安全立法的必要性和立法原则	39
1.6.2 国外主要的计算机安全立法	39
1.6.3 我国计算机信息系统安全法规简介	40
1.7 网络安全的发展方向	42
1.8 本章小结	44
练习题	44

第 2 章 密码技术	45
2.1 概述	45
2.2 传统的加密方法	46
2.2.1 替代密码	46
2.2.2 换位密码	50
2.3 数据加密标准 DES 与 IDEA	52
2.3.1 数据加密标准 DES 思想	52
*2.3.2 DES 详细算法	53
2.3.3 IDEA 算法	60
2.4 公开密钥加密算法	61
*2.5 RSA 密码系统	63
2.5.1 RSA 公开密钥密码系统	63
2.5.2 RSA 的安全性	64
2.5.3 RSA 的实用考虑	65
2.6 计算机网络加密技术	66
2.6.1 链路加密	66
2.6.2 节点加密	68
2.6.3 端-端加密	68
2.7 报文鉴别和 MD5 算法	70
2.7.1 报文鉴别	70
*2.7.2 MD5 算法	71
2.8 密钥管理与分配	71
2.9 密码技术的应用实例	73
2.9.1 口令加密技术的应用	73
*2.9.2 电子邮件 PGP 加密系统	76
2.10 本章小结	78
练习题	78
 第 3 章 防火墙技术	 80
3.1 防火墙的基本概述	80
3.1.1 什么是防火墙	80
3.1.2 防火墙的功能	81
3.2 防火墙的作用	82
3.2.1 配置防火墙的目的	82
3.2.2 防火墙的优点	83

3.2.3	防火墙的特性	84
3.2.4	防火墙的缺点	84
3.3	防火墙的分类	85
3.3.1	包过滤路由器	85
3.3.2	应用型防火墙	86
3.3.3	主机屏蔽防火墙	87
3.3.4	子网屏蔽防火墙	88
3.4	防火墙的安全标准	88
3.5	在网络中配置防火墙	89
3.5.1	包过滤路由器的配置与实现	89
3.5.2	应用型防火墙的配置与实现	90
3.5.3	主机屏蔽防火墙的配置与实现	91
3.5.4	子网屏蔽防火墙的配置与实现	92
3.5.5	防火墙与 Web 服务器之间的配置策略	92
3.6	防火墙的访问控制策略	94
3.7	防火墙的选择原则	95
3.7.1	防火墙自身安全性的考虑	95
3.7.2	防火墙应考虑的特殊需求	96
3.7.3	防火墙选择须知	96
3.8	防火墙技术的展望	97
3.8.1	防火墙发展趋势	98
3.8.2	防火墙需求的变化	98
* 3.9	防火墙实例——天网防火墙简介	98
3.9.1	天网防火墙简介	98
3.9.2	天网防火墙下载安装	99
3.9.3	天网防火墙运行	100
3.9.4	使用天网防火墙	101
3.10	本章小结	108
	练习题	108
第 4 章	计算机及网络系统的安全性	110
4.1	计算机系统的安全保护机制	110
4.1.1	用户的识别和验证	111
4.1.2	决定用户访问权限	112
4.2	计算机系统的安全等级	112
4.2.1	非保护级	112

4.2.2	自主保护级	113
4.2.3	强制安全保护级	114
4.2.4	验证安全保护级	115
4.3	计算机的开机口令验证机制	115
4.3.1	BIOS 的口令机制	116
4.3.2	BIOS 的口令破解与防范措施	117
4.4	Windows 95/98/ME 的安全保护机制	122
4.4.1	Windows 98 的登录机制	122
4.4.2	Windows 98 的屏幕保护机制	124
4.4.3	Windows 98 共享资源和远程管理机制	124
4.4.4	Windows 98 注册表的机制	130
4.5	利用注册表提高 Windows 95/98/ME 的安全性	131
4.6	Windows 98 系统安全策略编辑器	133
4.6.1	安全策略编辑器的安装	133
4.6.2	系统策略编辑器的使用	134
4.6.3	防止非法用户的进入	137
4.7	Windows 95/98/ME 的缺陷和防范措施	139
4.7.1	Windows 95/98/ME 密码的破解	139
4.7.2	Windows 的漏洞问题	144
4.8	计算机文档的保密问题	149
4.8.1	办公软件密码	149
4.8.2	办公软件密码解密	151
4.9	本章小结	152
	练习题	153
第 5 章	Windows NT/2000 的安全与保护措施	154
5.1	Windows NT/2000 系统的安全基础	154
5.1.1	Windows NT 系统的安全基础概念	155
5.1.2	Windows 2000 系统的安全概述	162
5.2	Windows NT/2000 的安全模型	166
5.2.1	Windows NT/2000 的用户登录管理	167
5.2.2	Windows NT/2000 的资源访问控制机制	168
5.3	Windows NT/2000 用户登录与账户管理	169
5.3.1	Windows NT/2000 的登录机制	169
5.3.2	Windows NT 的用户账户管理	170
5.3.3	Windows NT 用户的配置	173

5.4	用活动目录管理 Windows 2000 的账户	175
5.4.1	Windows 2000 的有关账户的基本概念	175
5.4.2	Windows 2000 用户账户的管理	178
5.5	Windows NT/2000 系统的访问控制与权限	186
5.5.1	Windows NT 的安全性	186
5.5.2	Windows NT 文件/目录的权限设置	190
5.5.3	Windows 2000 安全访问控制	194
5.6	Windows NT/2000 系统数据保护措施	203
5.6.1	Windows NT 的容错技术	203
5.6.2	Windows NT 系统的恢复与修复	207
5.6.3	Windows 2000 系统的诊断与修复	210
* 5.7	Windows NT/2000 系统的缺陷	218
5.7.1	Windows NT 系统的缺陷	218
5.7.2	Windows 2000 系统的缺陷	220
* 5.8	常见破解 Windows NT/2000 密码的方法及防范措施	225
5.8.1	几种常见破解 Windows NT/2000 密码的方法	225
5.8.2	防御保密字猜测	227
5.9	Windows NT/2000 的安全管理	229
5.9.1	安全问题的产生	229
5.9.2	安全防范措施	229
5.10	利用输入法漏洞本地入侵 Windows 2000 的防范	231
5.11	本章小结	235
	练习题	236
第 6 章	黑客原理与防范措施	237
6.1	计算机网络系统的缺陷与漏洞	237
6.1.1	计算机网络的设计缺陷	237
6.1.2	计算机网络系统的漏洞及漏洞等级	240
6.2	网络监听	243
6.2.1	网络监听 Sniffer 的工作原理	244
6.2.2	怎样在一个网络上发现一个 Sniffer	245
6.2.3	怎样防止被 Sniffer	245
6.3	端口扫描	246
6.3.1	什么是端口扫描	247
6.3.2	手工扫描	247
6.3.3	使用端口软件扫描	249

6.3.4	预防端口扫描·····	250
6.4	口令破解·····	250
6.4.1	用户的登录口令认证机制·····	250
6.4.2	口令破解的方法·····	251
6.4.3	口令破解器·····	251
6.4.4	口令破解器是怎样工作的·····	252
6.4.5	注册码破解实例·····	253
6.4.6	防止口令的破解·····	254
6.5	特洛伊木马·····	256
6.5.1	特洛伊木马简介·····	256
6.5.2	几种著名特洛伊木马·····	261
6.6	缓冲区溢出及其攻击·····	266
6.7	黑客攻击的一般步骤及防范措施·····	268
6.7.1	黑客攻击的一般步骤·····	268
6.7.2	对付黑客入侵的措施·····	270
6.8	入侵 Windows NT 的实例·····	272
6.8.1	通过 NetBIOS 入侵·····	272
6.8.2	口令破解·····	276
6.8.3	后门·····	277
6.8.4	本地攻击·····	279
6.9	远程入侵 Windows 2000·····	280
6.10	本章小结·····	284
	练习题·····	284
第 7 章	网络病毒与防治·····	286
7.1	计算机病毒概述·····	286
7.1.1	病毒的定义·····	286
7.1.2	计算机病毒的发展历史·····	287
7.2	计算机病毒的工作原理·····	288
7.2.1	计算机病毒的主要特征·····	288
7.2.2	病毒与黑客软件的异同·····	290
7.2.3	计算机病毒破坏行为·····	290
7.2.4	计算机病毒的结构·····	291
7.3	病毒分类·····	291
7.3.1	引导型病毒·····	291
7.3.2	文件型病毒·····	298

7.3.3	混合型病毒	304
7.3.4	Internet 病毒	304
7.4	计算机网络病毒的发展	304
7.5	计算机网络病毒的检测、清除与防范	305
7.5.1	计算机网络病毒的检测	305
7.5.2	计算机网络病毒的防范	307
7.5.3	病毒防治新产品	308
7.6	网络病毒实例	309
7.6.1	CIH 病毒机制及防护	309
7.6.2	宏病毒机制及防护	311
7.6.3	其他著名的网络病毒:“红色代码”和“尼姆达”	316
7.7	本章小结	321
	练习题	322
第 8 章	Internet 的安全性	323
8.1	Internet/Intranet 的安全概述	323
8.1.1	Internet 的脆弱性	323
8.1.2	Internet 提供的服务中的安全问题	324
8.1.3	Intranet 的安全性	328
8.2	网页中的新技术与 IE 的安全性	329
8.2.1	浏览器中 Cookie 的安全	329
8.2.2	ActiveX 的安全问题	333
8.2.3	Java 语言的使用与安全	338
8.3	电子邮件与 Outlook Express 的安全	343
8.3.1	E-mail 工作原理及安全漏洞	344
8.3.2	Outlook Express 的安全	346
8.4	IIS 服务器的安全	353
8.4.1	微软的 Internet 信息服务器 IIS	353
8.4.2	IIS 的安全基础	354
8.4.3	IIS 的安全设置	355
8.4.4	Web 服务器的安全性	359
8.4.5	FTP 与 Gopher 服务器安全性	360
8.5	本章小结	361
	练习题	361
第 9 章	计算机网络安全实训问题	362
9.1	实训说明	362
9.2	实训问题	363

*实训一	使用费杰尔算法进行编程	363
实训二	BIOS 密码和计算机开机密码的配置	363
实训三	Windows 98 的相关密码设置	364
实训四	配置天网个人防火墙	365
实训五	Windows NT/2000 的权限配置与安全审核	366
*实训六	本地入侵 Windows NT 系统	367
*实训七	网络监听获取 Windows NT 普通用户密码	368
*实训八	远程攻击 Windows 2000 系统	369
实训九	Windows NT/2000 的诊断与修复操作	369
实训十	杀毒软件的使用	370
实训十一	IE 浏览器安全配置	370
实训十二	Outlook Express 安全配置	371
实训十三	IIS 的安全配置	372
参考文献		373

随着计算机技术的飞速发展,信息和网络已经成为社会发展的重要保证。信息与网络涉及到国家的政府、军事、文教等诸多领域,在计算机网络中存储、传输和处理的信息有许多是政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要信息,其中有很多是敏感信息甚至是国家机密,所以难免会吸引来自世界各地的各种人为攻击(例如,信息泄漏、信息窃取、数据删除与添加、计算机病毒等)。因此计算机网络安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题,其重要性正随着全球信息化步伐的加快而变得越来越重要。

计算机网络安全主要涉及网络信息的安全和网络系统本身的安全。在计算机网络中存在着各种资源设施,随时存储和传输的大量数据;这些设施可能遭到攻击和破坏,数据在存储和传输过程中可能被盗用、暴露或篡改。另外,计算机网络本身可能存在某些不完善之处,网络软件也有可能遭受恶意程序的攻击而使整个网络陷于瘫痪。同时网络实体还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。

本章介绍计算机网络安全的基本知识,主要包括以下内容:

- 计算机网络基础知识;
- 计算机网络存在的安全问题;
- 网络安全的体系结构;
- 网络安全技术;
- 网络安全的策略及实现;
- 计算机网络安全立法;
- 计算机网络安全的发展方向。

为了更好地学习网络安全知识,掌握网络的攻防策略,学习一些相关的计算机网络基础知识是非常必要的。



1.1.1 计算机网络体系结构

1. 计算机网络

计算机网络,可以用一句简单的话概括:“通过通信线路连接起来的自治的计算机集合”。这句话包括以下 3 个方面的含义。

(1) 必须有两台或两台以上的具有独立功能的计算机系统相互连接起来,以达到共享资源为目的,才能构成网络。这里所指的两台计算机系统的位置要有一定的距离,且每个计算机系统能够独立地工作,能够自行处理数据,而无需其他系统的帮助。例如:具有通信功能的单机系统(即一台主机连接多个终端的系统),因为只有一台主机,就不属于网络。并行机虽然有多个处理器,但它不属于两个具有独立功能的计算机系统互连在一起,因此也不属于网络。

(2) 两台或两台以上的计算机连接,互相通信交换信息,必须有一条通道。这条通道的连接是物理的,由物理介质和通信设备实现。它们可以是铜线、光缆等“有线”介质,也可以是微波、红外线或卫星等“无线”介质。

(3) 计算机系统之间交换信息,必须有某种约定和规则,这就是协议。这些协议可以由硬件或软件来完成。

综合以上 3 个方面的内容,可以把计算机网络归纳为:把分布在不同地点且具有独立功能的多个计算机系统通过通信设备和线路连接起来,在功能完善的网络软件和协议的管理下,以实现网络中资源共享为目标的系统。

2. 计算机网络协议

在计算机网络中不同系统的两个实体之间只有在通信的基础上,才有可能相互交换信息,并共享网络资源。一般来说,实体是能发送和接收信息的任何东西,可以指用户应用程序、文件传送包、数据库管理系统、电子邮件设备和终端等。系统可包含一个或多个实体(如主机和终端等)。两个实体之间若要能通信,就必须能够相互理解,共同遵守有关实体的某种互相能接受的规则。这些规则的集合称为协议。因此协议可被定义为实体之间控制数据交换的规则集合。简单说,协议就是通信双方的约定。一个网络协议主要由以下 3 个要素组成。

- (1) 语法:即数据与控制信息的结构或格式;
- (2) 语义:即需要发出何种控制信息,完成何种动作以及做出何种应答;
- (3) 同步:即实体通信实现顺序的详细说明。

由此可见,网络协议是计算机网络不可缺少的组成部分。

3. 通信子网及子网信道类型

计算机网络主要由计算机系统(包括计算机和终端)、网络节点(通信处理机)和通信链路(通信线路和网络设备)等网络单元组成。从功能上可以将计算机网络分为资源子网和通信子网,网络上的每一个连接称为节点,节点有两类:一类是转接节点,主要承担通信