21st CENTURY
规划教材

面向21世纪高职高专计算机系列规划教材

COURSES FOR VOCATIONAL HIGHER EDUCATION: COMPUTER

计算机网络安全技术

NETWORK SECURITY TECHNOLOGIES

马晓绛 主 编

科学出版社
www.sciencep.com

面向21世纪高职高专计算机系列规划教材
COURSES FOR VOCATIONAL HIGHER EDUCATION: COMPUTER

计算机网络安全技术

马晓绛　主编

科学出版社
北京

内 容 简 介

本书从计算机网络安全技术概述入手，逐步介绍面向网络节点和用户、面向网络边界、面向单一网络和 Internet 的安全技术，介绍了计算机网络的攻击、防御和病毒防治技术，并在每章后均配有思考与练习题。

本书适合作为高等院校和高职院校培养计算机类应用性人才的教材或教参，或相关培训用书，也适合于从事计算机网络程序设计、安全技术应用和对此感兴趣的其他人员阅读。

图书在版编目(CIP)数据

计算机网络安全技术/马晓绛主编. —北京：科学出版社，2004
（面向 21 世纪高职高专计算机系列规划教材）
ISBN 7-03-014208-X

Ⅰ.计… Ⅱ.马… 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(2004)第 084329 号

责任编辑：李佩乾 陈砺川/责任校对：柏连海
责任印制：吕春珉/封面设计：飞天创意

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

新蕾印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2004 年 9 月第 一 版 开本：787×1092 1/16
2004 年 9 月第一次印刷 印张：12 1/4
印数：1－3 000 字数：261 000

定价：17.00 元

（如有印装质量问题，我社负责调换〈路通〉）

面向21世纪高职高专规划教材专家委员会

主　任　李宗尧

副主任（按姓氏笔画排序）

丁桂芝　叶小明　张和平　林　鹏

黄　藤　谢培苏

委　员　（略）

信息技术系列教材编委会

主　任　丁桂芝

副主任（按姓氏笔画排序）

万金保　方风波　徐　红　鲍　泓

委　员（按姓氏笔画排序）

于晓平　马国光　仁英才　王东红　王正洪

王　玉　王兴宝　王金库　王海春　王爱梅

邓　凯　付百文　史宝会　本柏忠　田　原

申　勇　任益夫　刘成章　刘克敏　刘甫迎

刘经玮　刘海军　刘敏涵　安志远　许殿生

何瑞麟　佘少华　吴春英　吴家碚　吴瑞萍

宋士银　宋锦河　张红斌　张环中　张海鹏

张蒲生　张德实　李云程　李文森　李　洛

李德家　杨永生　杨　闯　杨得新　肖石明

肖洪生　陈　愚　周子亮　周云静　胡秀琴

赵从军　赵长旭　赵动庆　郝　梅　唐铸文

徐洪祥　徐晓明　袁德明　郭庚麒　高延武

高爱国　康桂花　戚长政　曹文济　黄小鸥

彭丽英　董振珂　蒋金丹　韩银峰　魏雪英

出版前言

随着世界经济的发展，人们越来越深刻地认识到经济发展需要的人才是多元化、多层次的，既需要大批优秀的理论性、研究性的人才，也需要大批应用性人才。然而，我国传统的教育模式主要是培养理论性、研究性的人才。教育界在社会对应用性人才需求的推动下，专门研究了国外应用性人才教育的成功经验，结合国情大力度地改革我国的“高等职业教育”，制定了一系列的方针政策。联合国教科文组织 1997 年公布的教育分类中将这种教育称之为“高等技术与职业教育”，也就是我们通常所说的“高职高专”教育。

我国经济建设需要大批应用性人才，呼唤高职高专教育的崛起和成熟，寄希望于高职高专教育尽快向国家输送高质量的紧缺人才。近几年，高职高专教育发展迅速。目前，各类高职高专学校已占全国高等院校的近 1/2，约有 600 所之多。教育部针对高职高专教育出台的一系列政策和改革方案主要体现在以下几个方面：

- “就业导向”成为高职高专教育的共识。高职高专院校在办学过程中充分考虑市场需求，用“就业导向”的思想制定招生和培养计划。
- 加快“双师型”教师队伍建设。已建立 12 个国家高职高专学生和教师的实训基地。
- 对学生实行“双认证”教育。学历文凭和职业资格“双认证”教育是高职高专教育特色之一。
- 高职高专教育以 2 年学制为主。从学制入手，加快高职高专教学方向的改革，充分办出高职高专教育特色，尽快完成紧缺人才的培养。
- 开展精品专业和精品教材建设。已建立科学的高职高专教育评估体系和评估专家队伍，指导、敦促不同层次、不同类型的学校办出一流的教育。

在教育部关于“高职高专”教育思想和方针指导下，科学出版社积极参与到高职高专教材的建设中去。在组织教材过程中采取了“请进来，走出去”的工作方法，即由教育界的专家、领导和一线的教师，以及企事业从事人力资源工作的人员组成顾问班子，充分分析我国各地区的经济发展、产业结构以及人才需求现状，研究培养国家紧缺人才的关键要素，寻求切实可行的教学方法、手段和途径。

通过研讨认识到，我国幅员辽阔，各地区的产业结构有明显的差异，经济发展也不平衡，各地区对人才的实际需求也有所不同。相应地，对相同专业和相近专业，不同地区的教学单位在培养目标和培养内容上也各有自己的定位。鉴于此，适应教育现状的教材建设应该具有多层次的设计。

为了使教材的编写能针对受教育者的培养目标，出版社的编辑分不同地区逐所学校拜访校长、系主任和老师，深入到高职高专学校及相关企事业，广泛、深入地和教学第

一线的老师、用人单位交流，掌握了不同地区、不同类型的高职高专院校的教师、学生和教学设施情况，清楚了各学校所设专业的培养目标和办学特点，明确了用人单位的需求条件。各区域编辑对采集的数据进行统计分析，在相互交流的基础上找出各地区、各学校之间的共性和个性，有的放矢地制定选题项目，并进一步向老师、教育管理者征询意见，在获得明确指导性意见后完成“高职高专规划教材”策划及教材的组织工作：

- 第一批“高职高专规划教材”包括三个学科大系：经济管理、信息技术、建筑。
- 第一批“高职高专规划教材”在注意学科建设完整性的同时，十分关注具有区域人才培养特色的教材。
- 第一批“高职高专规划教材”组织过程正值高职高专学制从3年制向2年制转轨，教材编写将其作为考虑因素，要求提示不同学制的讲授内容。
- 第一批“高职高专规划教材”编写强调
  - 以就业岗位对知识和技能需求下的教材体系的系统性、科学性和实用性。
  - 教材以实例为先，应用为目的，围绕应用讲理论，取舍适度，不追求理论的完整性。
  - 提出问题→解决问题→归纳问题的教、学法，培养学生触类旁通的实际工作能力。
  - 课后作业和练习（或实训）真正具有培养学生实践能力的作用。

在“高职高专规划教材”编委的总体指导下，第一批各科教材基本是由系主任，或从教学一线中遴选的骨干教师执笔撰写。在每本书主编的严格审读及监控下，在各位老师的辛勤编撰下，这套凝聚了所有作者及参与研讨的老师们的经验、智慧和资源，涉及三个大的学科近200种的高职高专教材即将面世。我们希望经过近一年的努力，奉献给读者的这套书是他们渴望已久的适用教材。同时，我们也清醒地认识到，“高职高专”是正在探索中的教育，加之我们的水平和经验有限，教材的选题和编辑出版会存在一些不尽人意的地方，真诚地希望得到老师和学生的批评、建议，以利今后改进，为繁荣我国的高职高专教育不懈努力。

科学出版社

2004年6月1日

前　言

计算机网络安全已引起世界各国的关注，我国近几年才逐渐开始在高等教育中渗透计算机网络安全方面的基础知识和网络安全技术应用知识。随着网络高新技术的不断发展，社会经济建设与发展越来越依赖于计算机网络，与此同时，网络安全对国民经济的威胁、甚至对国家和地区的威胁也越来越严重。加快培养网络安全方面的应用性人才、广泛普及网络安全知识和掌握网络安全技术突显重要和迫在眉睫。

本书是在广泛调研和充分论证的基础上，结合人们普遍关心的热点问题，并经过教学实践而形成的一本社会广泛需求的，特别是适合职业教育发展特点和具有广泛普及性的教材。

本书利用14项任务驱动把网络安全技术知识组织在一起，突出应用性和技能性。改变了过于注重知识传授的倾向，强调形成积极主动的学习态度获得基础知识与基本技能的过程，就是学会学习和形成正确价值观的过程；改变了过于强调系统性和学科本位的现状，课程结构具有综合性和灵活性；改变了过于注重书本知识的现状，加强了课程内容与现代社会和科技发展的联系，精选终身学习必备的基础知识和技能；改变了过于强调接受学习、机械训练的现状，倡导学生自主学习、自主探索和主动参与教学，培养学生的实践动手能力、获取新知识的能力、分析和解决问题的能力以及交流与合作的能力。

全书共分7章。第1章是计算机网络安全技术概述，主要介绍了网络安全技术中的基本知识、技术方法和发展趋势。第2章是面向节点和用户的安全技术，主要介绍访问控制、身份鉴别、安全审计和数据安全存储等安全技术知识。第3章是面向网络边界的安全技术，主要介绍了网络边界的概念、安全防火墙和入侵检测等技术内容。第4章是面向单一网络的安全技术，主要介绍了VLAN、VPN、密钥管理和分配等基本知识。第5章是网络攻击与防御技术，主要介绍了黑客的概念、主要攻击手段、防御攻击的主要方法和特洛伊木马的检测防御问题。第6章是计算机病毒防治技术，主要介绍了计算机病毒的基本概念、防治方法和常用杀毒工具的使用等知识。第7章是Internet安全技术问题，主要介绍了CA认证、IP安全、FTP安全、电子邮件安全和Web安全等相关内容。

全书由马晓绛负责主编和统稿，第1章由马晓绛执笔，第2～4章由陆祥翠执笔，第5～7章由王琛执笔。由于时间仓促，加之编者水平有限，书中难免有错漏之处，希望广大读者批评指正。

作者E-mail：yj@xzcat.edu.cn。

作　者

2004年7月于徐州

目　录

第 1 章　计算机网络安全技术概述

任务 1：计算机网络安全技术主要涉及的内容

- 实体硬件安全。
- 软件系统安全。
- 网络安全防护。
- 数据信息安全。
- 病毒防治技术。
- 网络站点安全。

任务 2：检查网络安全级别

检查方法：

- 准备一套关于计算机信息系统安全等级标准的文献。
- 参照软硬件技术说明书，检查网络的软硬件配置和安全认证情况。
- 对照信息系统安全等级标准，检查网络满足哪个安全等级标准。
- 确定安全级别后，检查相应级别的安全保证和文档要求。分析判别网络是否满足要求。

计算机网络日益受到人们的注目，并得到广泛应用。众所周知，利用计算机网络环境进行信息交流已成为时代发展的必然趋势，人们可以利用网络方便快捷地进行各种信息处理，例如，网上办公、电子商务、分布式数据处理等。但是，网络也存在不容忽视的安全问题，例如，用户的数据被篡改、合法用户被冒充、通信被中断等。所以，如何在一个开放式的计算机网络物理环境中构造一个封闭的逻辑环境来保障敏感信息和保密数据不受到各种主动和被动的人为攻击，已成为必须考虑的实际问题。

同以前的计算机安全保密相比，计算机网络安全技术的问题要多得多，也复杂得多，它涉及到物理环境、硬件、软件、数据、传输、体系结构等各个方面。计算机网络安全技术包括了计算机安全、通信安全、操作安全、访问控制、实体安全、系统平台及网络站点的安全，以及安全管理和法律制裁等诸多内容，并逐渐形成独立的学科体系。

1.1 计算机网络安全

1.1.1 基本概念

1. 计算机网络安全的定义

从狭义的保护角度来看,计算机网络安全是指计算机及其网络资源和信息资源不受到人为有害因素的威胁和危害,即指计算机、网络系统的硬件、软件及其系统中的数据受到保护,不因偶然的或者恶意的原因而遭到破坏、更改、泄露,确保系统能连续可靠地正常运行,使网络服务不中断。计算机网络安全从其本质上来讲就是系统上的信息安全。计算机网络安全是一门涉及计算机科学、网络技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合科学。

从广义来说,凡是涉及计算机网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是计算机网络安全的研究领域。所以,广义的计算机网络安全还包括信息设备的物理安全性,诸如场地环境保护、防火措施、防水措施、静电防护、电源保护、空调设备、计算机辐射和计算机病毒等。

2. 计算机网络安全的重要性

计算机网络安全之所以重要,其主要原因在于:

1) 计算机存储和处理的是有关国家安全的政治、经济、军事、国防的情况及一些部门、机构、组织的机密信息或是个人的敏感信息、隐私,因此成为敌对势力、不法分子的攻击目标。

2) 随着计算机系统功能的日益完善和速度的不断提高,系统组成越来越复杂、系统规模越来越大,特别是 Internet 的迅速发展,存取控制、逻辑连接数量不断增加,软件规模空前膨胀,任何隐含的缺陷、失误都能造成巨大损失。

3) 人们对计算机系统的需求在不断扩大,这类需求在许多方面都是不可逆转和替代的,而计算机系统使用的场所正在转向工业、农业、野外、天空、海上、宇宙空间、核辐射环境等,这些环境都比机房恶劣,出错率和故障的增多必将导致可靠性和安全性的降低。

4) 随着计算机系统的广泛应用,各类应用人员队伍迅速发展壮大,操作人员、编程人员和系统分析员的失误或缺乏经验都会造成系统的安全功能不足。

5) 计算机网络安全问题涉及许多学科领域,既包括自然科学,又包括社会科学。就计算机系统的应用而言,安全技术涉及计算机技术、通信技术、存取控制技术、检验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术、防泄露技术等,因此是一个非常复杂的综合问题,并且其技术、方法和措施都要随着系统应用环境的变化而不断变化。

学习计算机网络安全技术的目的不是要把计算机网络系统武装到百分百安全,而是使之达到相当高的水平,使入侵者的非法行为变得极为困难、危险、耗资巨大,获得的价

值远不及付出的代价高。

1.1.2　计算机网络面临的主要威胁

随着计算机网络的不断发展，全球信息化已成为人类发展的大趋势。但计算机网络系统迅猛发展的同时，也面临着各种各样的威胁。

根据国际标准化组织定义的计算机网络面临的威胁，是指对计算机网络安全性的潜在破坏。一个系统可能遭受到各种各样的威胁，只有知道系统受到的威胁以后，才能对其进行有效的防范。

1. 计算机所面临威胁的类型

计算机网络所面临的威胁可分为两大类型：主动威胁和被动威胁。主动威胁是指威胁者对计算机网络信息进行修改、删除等非法操作；被动威胁是指威胁者通过非法手段获取信息，分析信息，而不修改它。如果按威胁的对象、性质则可以分为以下四类。

(1) 对硬件实体的威胁和攻击

这类威胁和攻击是对计算机本身和外部设备乃至网络和通信线路而言的，如各种自然灾害、人为破坏、操作失误、设备故障、电磁干扰、被盗和各种不同类型的不安全因素所致的物质财产损失、数据资料损失等。

(2) 对信息的威胁和攻击

这类威胁和攻击是指计算机系统处理所涉及的国家、部门、各类组织团体和个人的机密、重要及敏感信息。由于种种原因，这些信息往往成为敌对势力、不法分子和黑客攻击的重要对象。无论是无意的泄露，或是有意的窃取，都会造成直接或间接的经济损失或社会重大损失。

(3) 同时攻击软、硬件系统

这类情况除了战争攻击、武力破坏以外，最典型的就是病毒的危害。

(4) 计算机犯罪

计算机犯罪是指一切借助计算机技术或利用暴力、非暴力手段攻击、破坏计算机及网络系统的不法行为。计算机犯罪的损失异常惊人，近年来，我国大陆地区的计算机犯罪也在成倍增长。

2. 安全威胁的来源

针对计算机及网络系统的安全威胁的来源主要有三个：不可控制的自然灾害、人为的恶意攻击以及计算机系统本身的原因。其中，人为因素和系统本身问题更具普遍性。

(1) 人为因素

对于人为的威胁因素，往往是由威胁源(入侵者或其入侵程序)利用系统资源中的脆弱环节进行入侵而产生的。主要有四种类型：中断、窃取、更改和伪造。

1) 中断(Interruption)。威胁源使系统的资源受损或不能使用，从而使数据的流动或服务的提供中止。

2) 窃取(Interception)。某个威胁源成功地获取了一个资源的访问，从而成功地盗窃

有用的数据或服务。

3）更改(Modification)。未经授权的某个威胁源，成功地访问，并改动了某些资源，从而篡改了系统所提供的数据或服务。

4）伪造(Fabrication)。未经授权的某个威胁源，成功地在系统中制造假源，从而产生虚假的数据或服务。

（2）系统本身的原因

1）计算机硬件系统的故障。由于生产工艺或制造商的原因，计算机硬件系统本身有故障，如电磁泄漏、短路、断线、接触不良引起系统的不稳定、电压波动的干扰等。

2）软件的“后门”。软件的“后门”是软件公司的程序设计人员预留设置的，主要用于软件调试和进一步开发或远程维护提供了方便，但同时也为非法入侵者提供了通道。这些“后门”一般不为外人所知，一旦“后门”被打开，其后果不堪设想。

3）软件的漏洞。软件不可能是百分百无缺陷和无漏洞的，因而，这些漏洞和缺陷就成了黑客攻击的首选目标，典型的缺陷和漏洞有系统中的 BUGS。

计算机网络安全保障体系应尽量避免自然灾害造成的计算机危害，控制、预防和减少人为以及系统本身原因造成的计算机危害。

3. 威胁的具体表现形式

国际标准化组织对具体的威胁定义如下：

1）伪装：某个具有合法身份的威胁源成功地假扮另一实体，随后滥用这个实体的权力。其威胁源可以是用户，也可以是程序。

2）非法连接：威胁源以非法的手段形成合法的身份，使得网络资源之间建立非法的连接。威胁源可以是用户，也可以是程序。被威胁的对象是各种网络资源。

3）非授权访问：威胁源成功地破坏了访问控制服务（如修改了访问控制文件的内容），实现了越权访问。威胁源可以是用户，也可以是程序。被威胁的对象是网络各种资源。

4）重放：威胁源通过截获信息，然后根据需要将截获的信息再次重放。威胁源主要是用户，被威胁的对象也是用户。

5）拒绝服务：阻止合法的网络用户或其他执行其合法的权限，如妨碍执行服务或信息传递。威胁源可以是用户，也可以是程序。

6）抵赖：使网络用户虚假地否认递交过信息或接受到信息。威胁源可以是用户，也可以是程序。被威胁的对象是用户。

7）信息泄露：未经授权的实体（用户或程序）获取了传递中或存放的信息，造成了失密。威胁源可以是用户，也可以是程序。被威胁的对象是通信系统中的信息或数据库中的数据。

8）业务流量分析：威胁源观察通信协议中的控制信息，或对传送中的信息的长度、频率、源或目的进行分析。威胁源可以是程序，也可以是用户。被威胁的对象是通信系统中的信息。

9）改变信息流：对正确的通信信息序列进行非法修改、删除、重排序或重复。威胁源

可以是用户,也可以是程序。被威胁的对象是通信系统中的信息。

10) 篡改或破坏数据:针对传送的信息或存放的数据进行有意的非法修改或删除。威胁源可以是用户,也可以是程序。被威胁的对象是通信系统汇总的信息或数据库中的数据。

11) 推断或演绎信息:由于统计信息数据含有原始的信息踪迹,非法用户利用公布的统计数据,推导出某个信息源是从何处来的值。威胁源可以是用户,也可以是程序。被威胁的对象是数据库中的数据或通信系统中的信息流。

12) 非法篡改:具有三种形式——病毒、特洛伊木马和蠕虫。它们破坏操作系统、通信软件或应用程序。威胁源可以是程序,也可以是用户。被威胁的对象是程序。

1.2　计算机网络安全技术

1.2.1　基本概念

本节介绍基本的网络安全技术,主要包括身份认证技术、访问控制技术、数据的完整性和数字签名技术以及和安全管理相关的密钥管理和入侵检测技术等。

认证也称鉴别,是指验证一个实体的确是他所声称实体的过程。认证服务几乎是其他所有安全服务的依据,如访问控制、记账、抗抵赖等。认证目前有两种目的:实体身份认证和数据源发认证。实体身份认证一般发生在连接建立阶段,而数据源发认证一般发生在数据传输阶段。

访问控制技术用于限制合法用户的操作,根据一定的访问控制政策来保护资源的保密性、完整性或可用性。在操作系统中,一次访问可以用一个三元组(主体、操作、客体)来表示,通常用一个概念性的访问矩阵来表示主体对客体所允许的操作模式(如读、写、执行等)。

散列函数、堆成密钥密码技术和公开密钥密码技术是实现数据传输的完整性、保密性和数字签名的基础。由于公钥密码算法效率较低,常用加密或签名少量的数据,例如会话密钥(Session Key)的协商。

网络安全管理是 OSI 所定义的网络管理的五个功能域之一,OSI 安全体系结构中把安全管理分为系统安全管理、安全服务管理、安全机制管理、管理的安全四个方面的内容。然而目前各种网络管理产品中安全管理的内容很难找到,主要原因是多数网络安全机制或网络安全产品不提供远程管理的手段,各安全系统提供独立的管理手段和管理界面,主要包括用户及口令管理、访问控制规则管理、密钥管理、审计与入侵检测等。

1.2.2　研究的主要内容

由于计算机网络具有连接形式多样性、终端分布不均匀性和网络的开放型、互联性等特征,致使网络易受到黑客、恶意软件和其他不轨的攻击,所以网上信息的安全和保密是一个至关重要的问题。无论是在单机系统、局域网还是在广域网系统中,都存在着自

然和人为等诸多因素的脆弱性和潜在威胁。因此,计算机网络系统的安全措施应是能全方位地针对各种不同的威胁和脆弱性,这样才能确保网络信息的保密性、完整性和可用性。总之,一切影响计算机网络安全的隐私和保障计算机网络安全的措施都是计算机网络安全技术的研究内容。主要涉及以下几个方面。

1. 实体硬件安全

实体硬件安全是指系统设备及相关设施运行正常,系统服务适时。即应保证计算机设备和通信线路及设施、建筑物、构筑物的安全;预防地震、水灾、火灾、飓风、雷击;满足设备正常运行环境的要求,包括电源供电系统,包括机房的温度、湿度、清洁度、电磁屏蔽要求;采取监测、报警和维护技术及相应高可靠、高技术、高安全的产品;防止电磁辐射、泄露的高屏蔽、低辐射的设备,安全管理技术等。

2. 软件系统安全

软件系统安全主要是针对所有计算机程序和文档资料,保证它们免遭破坏和非法拷贝,软件安全技术还包括掌握高安全产品的质量标准,对于自己开发使用的软件建立严格的开放、控制、质量保障机制,保证软件满足安全标准技术标准要求,确保系统安全运行。

3. 网络安全防护

网络安全防护主要是针对计算机网络面临的威胁和网络的脆弱性而采取的防护技术,如安全服务、安全机制及其配置方法、动态网络安全策略、网络安全设计的基本原则等。

4. 数据信息安全

数据信息安全对于系统越来越重要。其安全保密主要是指为保障计算机系统的数据库、数据文件和所有数据信息的完整、有效、使用合法、免遭破坏、修改、泄露和窃取,为防止这些威胁和攻击而采用的一切技术、方法和措施。其中包括备份技术、密码技术与压缩技术、数据库安全技术等。

5. 病毒防治技术

计算机病毒对计算机系统安全的威胁,已成为一个重要的问题。要保证计算机系统的安全运行,除了运行服务安全技术措施外,还有专门设置计算机病毒检测、诊断、杀除设施,并采取成套的、系统的预防方法,以防止病毒的再入侵。计算机病毒的防治涉及计算机硬件实体、计算机软件、数据信息的压缩和加密解密技术。

6. 网络站点安全

网络站点安全是指为了保障计算机系统中网络通信和所有站点的安全而采取的各种技术措施,其中最主要的是防火墙技术。防火墙是介于内部网络或 Web 站点与