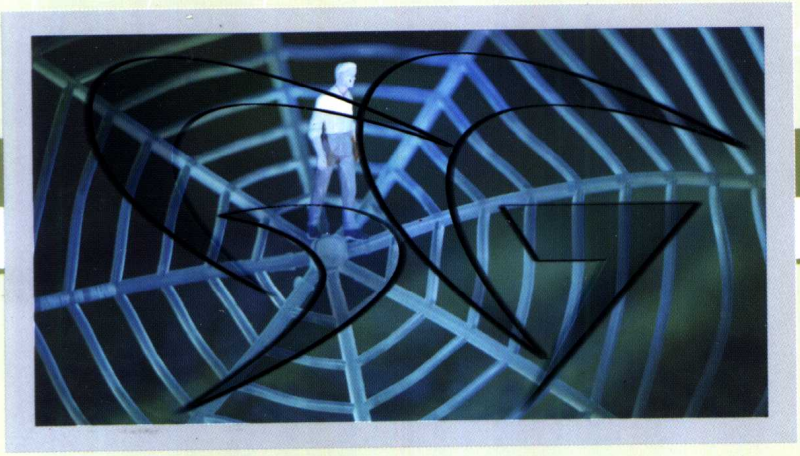
高职高专计算机系列教材

双高系列教材

计算机网络安全

顾巧论 蔡振山 贾春福 编著



科学出版社
www.sciencep.com

内 容 简 介

网络安全是一门涉及计算机科学、网络技术、通信技术、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性学科。网络安全问题在许多国家已经引起了普遍关注，成为当今网络技术的一个重要研究课题。

本书利用通俗的语言阐述了网络所涉及的安全问题，主要内容包括：网络安全基础知识、操作系统安全、网络通信安全、Web 安全、数据安全、病毒及其预防、黑客攻击与防范、防火墙技术，还介绍了几种网络安全产品及有关网络安全的法律法规。

本书不仅适合高职高专学生使用，同时也适合于任何对网络安全感兴趣的读者。

图书在版编目（CIP）数据

计算机网络安全/顾巧论，蔡振山，贾春福编著. —北京：科学出版社，2003

（高职高专计算机系列教材）

ISBN 7-03-010929-5

Ⅰ.计… Ⅱ.①顾…②蔡…③贾… 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 084906 号

责任编辑：鞠丽娜 丁 波/责任校对：都 岚

责任印制：吕春珉 /封面设计：王 浩

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

*

2003 年 1 月第 一 版 开本：B5（720×1000）

2003 年 1 月第一次印刷 印张：15 3/4

印数：1—5 000 字数：297 000

定价：23.00 元

（如有印装质量问题，我社负责调换〈路通〉）

高职高专计算机系列教材编写委员会

序

21 世纪计算机基础教育的发展是以高职高专应用型与专业理论型教育并存、共同发展为特征的教育模式。本科的教学往往是偏重理论教育，学生实践能力普遍偏弱，与生产实践脱离较远，而专科又是本科的浓缩。因此，解决现阶段出现的教育现状与社会需求严重脱节问题的最好的办法是大力发展高等职业教育。高职高专教育是高等教育的重要组成部分，具有高等教育和职业教育的双重属性，其教学目的是使学生既掌握所学专业的基础知识和基本理论，又掌握该专业应具备的职业技能，并具有运用所学知识分析和解决实际问题的综合能力，从而成为各行业的中高级专门人才。国家已经认识到发展高等职业教育对我国建设的重要性，并加大力度重点发展高等职业教育，这主要体现在：

（1）重点发展高职，新扩招的学生主要是高职；

（2）原来的大专逐步向高职发展；

（3）成人教育也要办成高职类型。

高职教育将和全日制普通高等教育并列成为我国重要的高等教育形式。目前我国已有高职高专学校 5000 多所，现正在逐步向本科和研究生层次发展。高职教育的蓬勃发展使计算机应用教育面临如下问题：1）知识更新快；2）每节课需传递的信息量增大；3）实践性强，实验教学占主要地位；4）现有的高校教学经验不适合高职的教学要求；5）师资的知识结构还要改变和更新；6）现阶段没有既定的、完善的教学大纲和教材。

为了适应当前高职高专的教学需要，我们编写了这套教材，并将这套教材奉献给读者，希望在教学中能起到抛砖引玉的作用。

本套计算机教材有以下特点：

（1）以实用为主兼顾最基本的理论知识。本套教材拟涵盖计算机的网络专业、多媒体专业、信息管理专业、电脑艺术设计专业、会计电算化专业和电子商务专业等多个专业的计算机用书。

（2）本套教材的基础部分以公共课为主要讲述内容，专业部分以实用技术为主，并以实例贯穿全书进行讲述。对个别实用性极强的内容，采用以实例教学的方式阐述，用实例讲解该技术的具体操作方法。

（3）每本书的编写，均遵循“深入浅出”和“言简意明”的原则论述基本原理与使用方法，以实例分析的方式阐述具体的操作过程，使读者对从一般理论知识到实际应用有一个全面的认识过程。

（4）为了便于多媒体教学，每本教材配有电子教案和源程序代码。有教学需求的教师可到科学出版社网站上下载（网址：www.sciencep.com）。

（5）为了方便学生使用，每本教材都有习题解答和上机指导。

（6）书中每章都有：1）要点与难点提要；2）本章的要求：熟练掌握的内容和了解的内容；3）小结。

（7）每章中使用大量的例题说明应用的关键和难点所在。每章都配有较多数量的思考题或练习题。

（8）每本书包括：1）课程的主要内容；2）实验（或上机）指导；3）习题解答；4）电子教案。

本套教材是根据高职高专发展的需要以及全国高等教育计算机基础教学研究会的教学指导思想编写的。在此，我们对关心、支持以及参与本套教材的研究、写作和发行的领导、专家和朋友们表示衷心的感谢！

计算机应用型人才教育的研究是一项具有深远意义的改革探索课题。我们愿意与从事计算机应用型人才教育的广大教师合作，为培养高质量的应用型人才共同努力。

《高职高专计算机系列教材》编委会

2002 年 10 月 27 日

前　言

目前，网络安全问题已经在许多国家引起了普遍关注，成为当今网络技术的一个重要研究课题。

从技术上讲，网络安全是一门涉及计算机科学、网络技术、通信技术、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全性学科。网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，从而确保系统能连续、可靠、正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及到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网络安全的研究领域。

影响计算机网络安全的因素很多，除了信息的不安全以外，层出不穷的电脑病毒也给网络安全带来了威胁。另外，黑客对于网络安全的威胁也日趋严重。网络所面临的威胁很多，其中包括：物理威胁（偷窃、废物搜寻、间谍行为、身份识别错误）、系统漏洞（乘虚而入、不安全服务、配置和初始化）、身份鉴别威胁（口令圈套、口令破解、算法考虑不周、编辑口令）、线缆连接威胁（窃听、拨号进入、冒名顶替）、有害程序（病毒、代码炸弹）。

当然，网络安全不仅是一个技术问题，也是一个社会问题和法律问题。要解决信息网络的安全问题，必须采取技术和立法等多种手段进行综合治理。

本书作为高职高专教材，采用通俗易懂的语言，围绕网络所涉及的安全问题，讲述了各种相关的安全技术，各章内容如下：

第 1 章是网络安全概述，包括网络安全简介、网络安全面临的威胁、网络出现安全威胁的原因、网络安全机制。

第 2 章介绍操作系统安全，包括安全等级标准、漏洞和后门、NetWare 系统安全、Windows NT 系统安全、UNIX 系统的安全、Windows 2000 的安全。

第 3 章介绍网络通信安全，包括网络通信的安全性、网络通信存在的安全威胁、调制解调器的安全、不同层的安全、IP 安全等。

第 4 章介绍 Web 安全，包括 Web 技术简介、Web 的安全需求、Web 服务器安全策略、Web 浏览器安全。

第 5 章介绍数据安全，包括数据加密、数据压缩、数据备份。

第 6 章介绍病毒知识，包括计算机病毒简介、网络病毒及其防治、典型病毒介绍、常用杀毒软件介绍。

第 7 章介绍黑客的知识，包括黑客攻击介绍、黑客攻击常用工具、黑客攻击常见的两种形式、黑客攻击的防备。

第 8 章介绍防火墙技术，包括防火墙简介、防火墙的类型、防火墙配置、防火墙系统、防火墙的选购和使用、防火墙产品介绍。

第 9 章介绍几种网络安全产品，包括 ZoneAlarm、NetSwift iGate、MBSA 安全分析器、Dragon 6.0 入侵检测系统。

第 10 章介绍网络安全的法律法规。

本书第 1 章、第 2 章、第 6 章～第 9 章及附录 A 由顾巧论编写；第 3 章由高铁杠、李莉编写；第 4 章、第 10 章及附录 B 由蔡振山编写；第 5 章由贾春福编写；本书由顾巧论统稿。其中，徐伟在第 5 章中做了部分工作，在此表示感谢。

本书在编写过程中，参考了大量书籍，在此对各部书的作者表示感谢。

由于编者水平有限，书中错误和疏漏之处在所难免，望读者和各位专家给予指教。

作　者

目 录

第 1 章　网络安全概述

知识点

- 网络安全的定义
- 网络面临的安全威胁
- 网络出现安全威胁的原因
- 网络的安全机制

难点

- 网络安全威胁是如何产生的

要求

熟练掌握以下内容：

- 网络安全的定义
- 网络面临的各种安全威胁
- 网络的安全机制

了解以下内容：

- 产生网络安全威胁的原因

随着网络技术的不断发展，网络在人们的生活中已经占有一席之地，为人们的生活带来了很大方便。然而，网络也不是完美无缺的，它在给人们带来惊喜的同时，也带来了威胁。计算机犯罪、黑客、有害程序和后门问题等严重威胁着网络的安全。目前，网络安全问题已经在许多国家引起了普遍关注，成为当今网络技术的一个重要研究课题。

1.1　网络安全简介

网络安全是一门涉及计算机科学、网络技术、通信技术、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性学科。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然

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、正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及到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网络安全的研究领域。

保密性：信息不泄露给非授权用户。

完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和不被丢失的特性。

可用性：可被授权实体访问并按需求使用的特性。即当需要时能否存取所需的信息。例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

可控性：对信息的传播及内容具有控制能力。

网络安全包括物理安全、逻辑安全、操作系统安全、联网安全。

1.1.1 物理安全

物理安全是指用来保护计算机硬件和存储介质的装置和工作程序。物理安全包括多方面的内容。

1. 防盗

像其他的物体一样，计算机也是偷窃者的目标，例如盗走硬盘、主板等。计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，因此必须采取严格的防范措施，以确保计算机设备不会丢失。

2. 防火

计算机机房发生火灾一般是由于电气原因、人为事故或外部火灾蔓延引起的。电气设备和线路因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。人为事故是指由于操作人员不慎、吸烟、乱扔烟头等，使充满易燃物质(如纸片、磁带、胶片等)的机房起火，当然也不排除人为故意放火。外部火灾蔓延是指因外部房间或其他建筑物起火而蔓延到机房而引起火灾。

3. 防静电

静电是由物体间的相互摩擦、接触而产生的，计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体内，会有很高的电位(能量不大)，从而产生静电放电火花，造成火灾。还能使大规模集成电路损坏，这种损坏可能是不知不觉造成的。

4. 防雷击

随着科学技术的发展，电子信息设备的广泛应用，对现代闪电保护技术提出了更高、更新的要求。利用传统的常规避雷针，不但已不能满足微电子设备对安全的需求，而且还带来很多弊端。利用引雷机理的传统避雷针防雷，不但增加雷击概率，而且还产生感应雷，而感应雷是电子信息设备被损坏的主要杀手，也是易燃易爆品被引燃起爆的主要原因。

雷击防范的主要措施是：根据电气、微电子设备的不同功能及不同受保护程序和所属保护层确定防护要点作分类保护；根据雷电和操作瞬间过电压危害的可能通道从电源线到数据通信线路都应做多级层保护。

5. 防电磁泄漏

电子计算机和其他电子设备一样，工作时要产生电磁发射。电磁发射包括辐射发射和传导发射。这两种电磁发射可被高灵敏度的接收设备接收并进行分析、还原，造成计算机的信息泄露。例如，从20世纪80年代开始，美国市场上出现了一种符合TEMPEST标准的军用通信设备，并逐渐形成商品化、标准化生产。TEMPEST技术是综合性的技术，包括泄露信息的分析、预测、接收、识别、复原、防护、测试、安全评估等项技术，涉及到多个学科领域。

屏蔽是防电磁泄漏的有效措施，屏蔽主要有电屏蔽、磁屏蔽和电磁屏蔽三种类型。

1.1.2 逻辑安全

计算机的逻辑安全需要用口令字、文件许可、查账等方法来实现。防止计算机黑客的入侵主要依赖计算机的逻辑安全。

可以限制登录的次数或对试探操作加上时间限制；可以用软件来保护存储在计算机文件中的信息，该软件限制了其他人存取非自己所有的文件，直到该文件的所有者明确准许其他人可以存取该文件时为止；限制存取的另一种方式是通过硬件完成，在接收到存取要求后，先询问并校核口令，然后访问列于目录中的授权用户标志号。此外，有一些安全软件包也可以跟踪可疑的、未授权的存取企图，例如，多次登录或请求别人的文件。

1.1.3 操作系统安全

操作系统是计算机中最基本、最重要的软件。同一计算机可以安装几种不同的操作系统。如果计算机系统可提供给许多人使用，操作系统必须能区分用户，以便于防止他们相互干扰。例如，多数的多用户操作系统不会允许一个用户删除属于另一个用户的文件，除非第二个用户明确地给予允许。

一些安全性较高、功能较强的操作系统可以为计算机的每一位用户分配账户。通常一个用户一个账户，操作系统不允许一个用户修改由另一个账户产生的数据。

1.1.4 联网安全

联网的安全性只能通过以下两方面的安全服务来达到：

(1) 访问控制服务：用来保护计算机和联网资源不被非授权使用。

(2) 通信安全服务：用来认证数据机要性与完整性，以及各通信的可信赖性。例如，基于互联网或 WWW 的电子商务就必须依赖并广泛采用通信安全服务。

1.2 网络安全面临的威胁

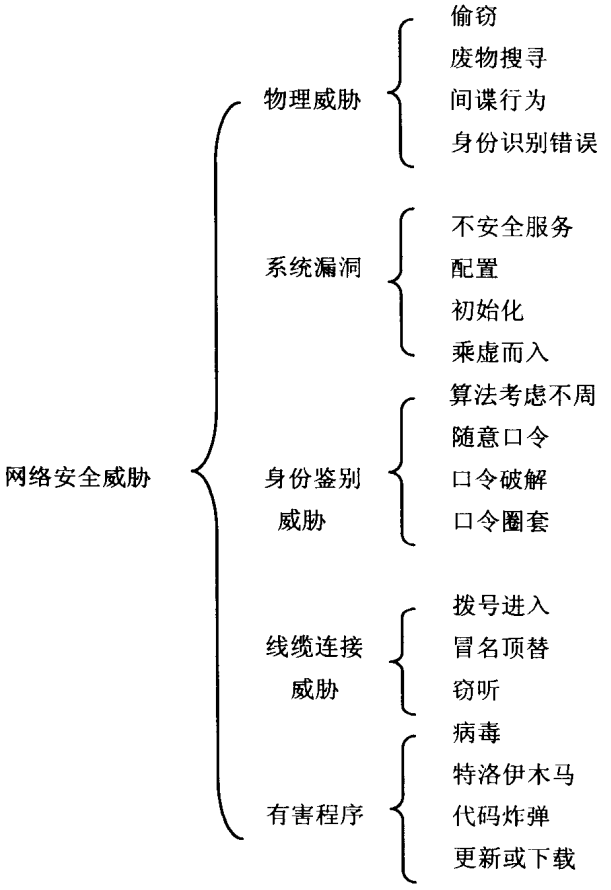


图 1-1 网络安全威胁