21世纪高职高专计算机系列规划教材

根据教育部最新高职高专教育教学大纲要求编写

计算机网络

安全技术

余成波　胡顺仁　蒋西明　王培容　张　莲　编著

北京工业大学出版社

21世纪高职高专计算机系列规划教材

计算机网络安全技术

余成波　胡顺仁　蒋西明　王培容　张　莲　编著

北京工业大学出版社

内 容 提 要

本书叙述力求由浅入深，利用通俗的语言阐述了网络所涉及的安全问题，并介绍了网络安全的新技术。本书主要以培养技术应用能力为主线，突出应用性和针对性，强化实践能力的培养。全书共9章，主要内容包括：网络安全概述、网络安全体系结构、操作系统的安全机制、网络数据安全、入侵检测系统、访问控制与防火墙技术、计算机病毒及预防、黑客攻击及其防范、网络安全策略等。

本书内容全面而实用，适用面广，不仅可以作为高校信息安全等高职高专专业教材，也可作广大从事信息安全开发与应用的工程技术人员的自学用书。

图书在版编目（CIP）数据

计算机网络安全技术／余成波等编著. —北京：北京工业大学出版社，2005.7
ISBN 7-5639-1532-X

Ⅰ.计… Ⅱ.余… 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075195号

计算机网络安全技术

余成波 胡顺仁 蒋西明 王培容 张 莲 编著

※

北京工业大学出版社出版发行

邮编：100022 电话：（010）67392308

各地新华书店总经销

徐水宏远印刷厂印刷

※

2005年8月第1版 2005年8月第1次印刷

787 mm×1 092 mm 16开本 13.5印张 336千字

印数：1~3 000册

ISBN 7-5639-1532-X/T·266

定价：18.00元

序

进入21世纪以来，随着国民经济发展水平的提高和教育改革的不断深入，我国的职业教育发展迅速，进入了一个新的历史阶段。社会主义现代化建设需要大量高素质的专业人才，而作为我国高等教育重要组成部分的高等职业教育，正肩负着前所未有的使命，为社会主义现代化建设培养大量高素质的劳动者。

区别于传统的本科教育，高等职业教育以培养应用型的人才为主。正是基于发展我国高等职业教育的需要，通过大量调研、反复讨论和修改，我们组织了一批长期工作在教学第一线的教师编写了这套《21世纪高职高专计算机系列规划教材》。

本套教材在编写上具有以下特点：

1. 具有鲜明的高职高专的特点。教材的策划和编写紧密地围绕培养技术应用性专门人才展开，体现了教育部“以应用为目的，以必需、够用为度，以讲清概念、强化应用为教学重点”的教育方针。本套书的作者都是长期从事高职高专教学工作的教师，有着丰富的教学经验，对高职高专学生的认知规律有深入的了解。本套教材适合高等职业学校、高等专科学校、以及本科院校举办的二级职业技术学院和民办职业高校使用。

2. 理论联系实际，强化应用。本套教材章后配有习题和实验题，突出实践技能和动手能力的培养。对于传统的教材，一般按照“提出概念→解释概念→举例说明”这样一种方法，先抽象后具体；本套教材采用“提出问题→解决问题→归纳总结”的方法，先具体后抽象。显而易见，后者更适合高职高专的教学模式，更能培养出具有较强综合职业能力，能够在生产、服务、技术和管理第一线工作的高素质的职业技术专门人才。

3. 适应行业技术发展，体现教学内容的先进性和前瞻性。在教材中注意突出本专业领域的新知识、新技术、新软件，尽可能实现专业教学基础性与先进性的统一。

为了方便教师教学，我们免费为使用本套教材的师生提供电子教学参考资料包：

- PowerPoint 多媒体课件
- 习题参考答案
- 教材中的程序源代码
- 教材中涉及的实例制作的各类素材

有需要的教师可以登录教学支持网站免费下载。在教材使用中有什么意见或建议也可以直接和我们联系，电子邮件地址：scqcwh@163.com。

希望本套教材，在教学实践的过程中，能够得到教师和学生的欢迎，同时期待得到更多的建议和帮助，以便提高本套教材的质量，更好地为培养社会主义现代化建设的高素质人才服务。

前　言

计算机网络是一门发展迅速、知识密集的综合性学科及高新信息科学技术，它涉及计算机、通信、电子、自动化、光电子和多媒体等诸多学科及信息技术。它是多种信息科学技术相互渗透和结合的产物，是建设信息高速公路和实现现代化信息社会的物质和技术基础。目前，已进入计算机发展的网络时代（信息化社会）。计算机网络已遍及世界 240 多个国家和地区，它在政治、军事、外交、经济、交通、电信、文教等方面的作用日益增大。社会对计算机网络的依赖程度也日益增强，尤其是计算机技术和通信技术相结合所形成的信息基础设施已经成为反映信息社会特征最重要的基础设施。人们建立了各种各样完备的信息系统，使得人类社会的一些机密和财富高度集中于计算机中。随着全球信息化的迅猛发展，国家的信息安全和信息主权已成为越来越突出的重要战略问题，它关系到国家的稳定与发展。网络的安全问题正在引起国家、信息界乃至社会公众的注意和重视，网络安全技术已经成为世界各国研究的热门课题。

本书系受《电脑报》委托，根据高校网络安全课程的基本要求，吸收近年来各高校的教学经验，在编写过程中力求内容丰富、全面、新颖，叙述由浅入深，具有一定的实用和参考价值。本教材以“培养技术应用能力为主线”，突出应用性和针对性，强化实践能力的培养。同时，在编写过程中，注意了补充反映新技术的内容，力求使读者了解前沿学科。

全书共 9 章，其主要内容包括：网络安全概述、网络安全体系结构、操作系统的安全机制、网络数据安全、入侵检测系统、访问控制与防火墙技术、计算机病毒及预防、黑客攻击及其防范、网络安全策略等。

本书由余成波、胡顺仁、张莲、王培容、蒋西明等编著，全书由余成波统稿。其中：第 1 章由张莲、余成波编写。第 2、5、6 章由胡顺仁编写。第 3 章由张莲编写。第 4 章由余成波编写。第 7 章由王培容编写。第 8、9 章及习题由蒋西明编写。

本书在编写过程中得到了《电脑报》有关领导和同志自始至终的大力支持和帮助，并获得了许多宝贵的意见。许多兄弟院校也为本书的编写提供了帮助。陶红艳、姜宏、刘东等同志为本书出版做了大量的工作，在此，一并表示衷心的感谢。

本书内容全面而实用，适用面广，不仅可以作为高校信息安全等高职高专专业教材，也可作为广大从事信息安全开发与应用的工程技术人员的自学用书。

由于时间比较仓促，错漏之处在所难免，热忱地期望各位读者和同仁对本书的错误和不足提出指正和建议。

编　者

2005 年 7 月

目　录

第 1 章　网络安全概述

计算机网络是一门发展迅速、知识密集的综合性学科及高新信息科学技术，它涉及计算机、通信、电子、自动化、光电子和多媒体等诸多学科及信息技术。它是多种信息科学技术相互渗透和结合的产物，是建设信息高速公路和实现现代化信息社会的物质和技术基础。目前，已进入计算机发展的网络时代（信息化社会）。计算机网络已遍及世界 240 多个国家和地区，它在政治、军事、外交、经济、交通、电信、文教等方面的作用日益增大。社会对计算机网络的依赖也日益增强，尤其是计算机技术和通信技术相结合所形成的信息基础设施已经成为反映信息社会特征最重要的基础设施。人们建立了各种各样完备的信息系统，使得人类社会的一些机密和财富高度集中于计算机中。但是这些信息系统都要依靠计算机网络接收和处理信息，实现其相互间的联系和对目标管理与控制。以网络方式获得信息和交流信息已成为现代信息社会的一个重要特征。随着全球信息化的迅猛发展，国家的信息安全和信息主权已成为越来越突出的重要战略问题，关系到国家的稳定与发展。就企业而言，网络信息对于在日益激烈的市场竞争中是否取胜非常关键，因此，网络的安全问题正在引起国家、信息界乃至社会公众的注意和重视，网络安全技术已经成为世界各国研究的热门课题。

1.1　计算机网络安全的定义及内容

1.1.1　计算机网络安全的定义

网络安全从其本质上来讲就是网络上的信息安全。它涉及的领域相当广泛。这是因为在目前的公用通信网络中存在各种各样的安全漏洞和威胁。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，都是网络安全所要研究的领域。下面给出网络安全的一个通用定义。

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，不因偶然或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段对用户的利益和隐私造成损害和侵犯，同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

从网络运行和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络“黑客”的攻击。

对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防

堵，避免其通过网络泄露，避免由于这类信息的泄密对社会产生危害，对国家造成巨大的经济损失。

从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

因此，网络安全在不同的环境和应用会得到不同的解释。

（1）运行系统安全，即保证信息处理和传输系统的安全。包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。它侧重于保证系统正常的运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄露，产生信息泄露，干扰他人（或受他人干扰），本质上是保护系统的合法操作和正常运行。

（2）网络上系统信息的安全。包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密。

（3）网络上信息传播的安全，即信息传播后果的安全。包括信息过滤，不良信息的过滤等。它侧重于防止和控制非法、有害的信息进行传播后的后果。避免公用通信网络上大量自由传输的信息失控。本质上是维护道德、法律或国家利益。

（4）网络上信息内容的安全，即我们讨论的狭义的“信息安全”。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。本质上是保护用户的利益和隐私。

显而易见，网络安全与其所保护的信息对象有关。本质是在信息的安全期内保证其在网络上流动时或者静态存放时不被非授权用户非法访问，但授权用户却可以访问。显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。下面给出本书所研究和讨论的网络安全的含义。

网络安全的含义是通过各种计算机、网络、密码技术和信息安全技术，保护在公用通信网络中传输、交换和存储的信息的机密性、完整性和真实性，并对信息的传播及内容具有控制能力。网络安全的结构层次包括：物理安全、安全控制和安全服务。

1.1.2 物理安全

网络安全首先要保障网络上信息的物理安全。物理安全是指在物理介质层次上对存储和传输的信息的安全保护。目前，常见的不安全因素（安全威胁或安全风险）包括四大类：

（1）自然灾害（如雷电、地震、火灾、水灾等），物理损坏（如硬盘损坏、设备使用寿命到期、外力破损等），设备故障（如停电断电、电磁干扰等）和意外事故。

特点是：突发性，自然因素性，非针对性。这种安全威胁只破坏信息的完整性和可用性（无损信息的秘密性）。

解决方案是：防护措施，安全制度，数据备份等。

（2）电磁泄漏（如侦听微机操作过程），产生信息泄漏，干扰他人或受他人干扰，乘机而入（如进入安全进程后半途离开）和痕迹泄露（如口令密钥等保管不善，易于被人发现）。

特点是：难以察觉性，人为实施的故意性，信息的无意泄露性。这种安全威胁只破坏信息的秘密性（无损信息的完整性和可用性）。

解决方案是：辐射防护，屏幕口令，隐藏销毁等。

（3）操作失误（如删除文件、格式化硬盘、线路拆除等）和意外疏漏（如系统掉电、“死机”等系统崩溃）。

特点是：人为实施的无意性，非针对性。这种安全威胁只破坏信息的完整性和可用性（无损信息的秘密性）。

解决方案是：状态检测，报警确认，应急恢复等。

（4）计算机系统机房环境的安全。

特点是：可控性强，损失也大，管理性强。

解决方案：加强机房管理，运行管理，安全组织和人事管理。

物理安全是信息安全的最基本保障，是不可缺少和忽视的组成部分。一方面，研制生产计算机和通信系统的厂商应该在各种软件和硬件系统中充分考虑到系统所受的安全威胁和相应的防护措施，提高系统的可靠性；另一方面，也应该通过安全意识的提高，安全制度的完善，安全操作的提倡等方式使用户和管理维护人员在系统和物理层次上实现信息的保护。

1.1.3　安全控制

安全控制是指在微机操作系统和网络通信设备上对存储和传输的信息的操作和进程进行控制和管理。主要是在信息处理层次上对信息进行的初步的安全保护。可以分为三个层次。

（1）微机操作系统的安全控制。如用户开机键入的口令（但目前某些微机主板有“万能口令”），对文件的读写存取的控制（如 UNIX 系统的文件属性控制机制）。主要用于保护存储在硬盘上的信息和数据。

（2）网络接口模块的安全控制。在网络环境下对来自其他机器的网络通信进程进行安全控制。主要包括：身份认证、客户权限设置与判别、审计日志等，如 UNIX、Windows95/NT 的网络安全措施。

（3）网络互联设备的安全控制。对整个子网内的所有主机的传输信息和运行状态进行安全监测和控制。主要通过网管软件或路由器配置实现。

可见，安全控制主要是通过现有的操作系统或网管软件、路由器配置等实现。安全控制只提供了初步的安全功能和信息保护，仍然存在着很多漏洞和问题。但由于实际情况的限制，很难对此进行弥补和更改。

1.1.4　安全服务

安全服务是指在应用层对信息的保密性、完整性和来源真实性进行保护和鉴别，满足用户的安全需求，防止和抵御各种安全威胁和攻击手段。这是对现有操作系统和通信网络的安全漏洞和问题的弥补和完善。

安全服务的主要内容包括：安全机制、安全链接、安全协议和安全策略。

1．安全机制

安全机制是利用密码算法对重要而敏感的信息进行处理。包括：加密/解密（保护信息的保密性），数字签名/签名验证（确认信息来源的真实性和合法性），信息认证（保护信息的

完整性，防止和检测数据的修改、插入、删除和改变）。安全机制是安全服务乃至整个安全系统的核心和关键。现代密码学的理论和技术在安全机制的设计中具有重要的作用。

2. 安全链接

安全链接是在安全处理前与网络通信方之间的链接过程，为安全处理进行必要的准备工作。主要包括：会话密钥的分配和生成及身份验证（保护进行信息处理和操作的对等双方身份的真实性和合法性）。

3. 安全协议

协议是多个使用方为完成某些任务所采取的一系列的有序步骤。协议的特性是：预先建立、相互同意、非二义性和完整性。安全协议使网络环境下不信任的通信方能够相互配合，并通过安全链接和安全机制的实现来保证通信过程的安全性、可靠性和公平性。

4. 安全策略

安全策略是安全体制、安全链接和安全协议的有机组合方式，是系统安全性的完整的解决方案。安全策略决定了信息安全系统的整体安全性和实用性。不同的通信系统和具体的应用环境决定不同的安全策略。

另外，安全设备是存储密钥、口令、权限、审计记录等安全信息的硬件介质和载体，以及存储和运行安全信息系统的设备，如具有防火墙功能的路由器，具有密钥分配和认证功能的安全服务器等。安全设备自身的安全防护也是必不可少的。

1.1.5 网络安全的内容

网络安全的内容大致上包括：网络实体安全、软件安全、数据安全和网络安全管理 4 个方面，如图 1-1 所示。

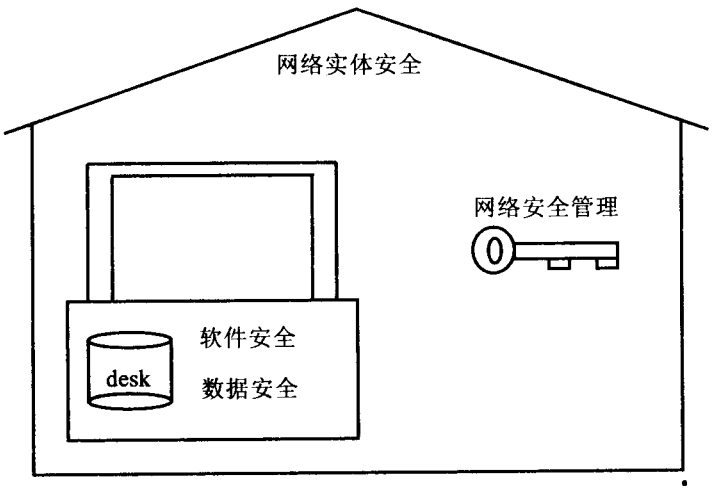

图 1-1 网络安全的内容

1. 网络实体安全

如计算机机房的物理条件、物理环境及设施的安全，计算机硬件、附属设备及网络传输线路的安装及配置等。

2．软件安全

如保护网络系统不被非法侵入，系统软件与应用软件不被非法复制、不受病毒的侵害等。

3．网络中的数据安全

如保护网络信息数据的安全、数据库系统的安全，保护其不被非法存取，保证其完整、一致等。

4．网络安全管理

如运行时突发事件的安全处理等，包括采取计算机安全技术，建立安全管理制度，开展安全审计，进行风险分析等内容。

1.2　计算机网络安全的主要威胁及隐患

1.2.1　网络安全的主要威胁

计算机网络的发展，使信息共享应用日益广泛与深入。但是信息在公共通信网络上存储、共享和传输，会被非法窃听、截取、篡改或毁坏而导致不可估量的损失。尤其是银行系统、商业系统、管理部门、政府或军事领域对公共通信网络中存储与传输的数据安全问题更为关注。如果因为安全因素使得信息不敢放进 Internet 这样的公共网络，那么办公效率及资源的利用率都会受到影响，甚至使人们丧失了对 Internet 及信息高速公路的信赖。

事物总是辨证的。一方面，网络提供了资源的共享性、用户使用的方便性，通过分布式处理提高了系统效率和可靠性，并且还具有了扩充性。另一方面，正是这些特点增加了网络受攻击的可能性。计算机网络所面临的威胁包括对网络中信息的威胁和对网络中设备的威胁。影响计算机网络的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；还可能是外来黑客对网络系统资源的非法使用等。

人为的无意失误，如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借给他人或与别人共享都会对网络安全带来威胁。

人为的恶意攻击，是计算机面临的最大威胁。敌手的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一种是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄露。

网络软件的漏洞和“后门”，网络软件不可能是百分之百无缺陷和无漏洞的。然而，这些漏洞和缺陷恰恰是黑客经常攻击的首选目标。曾经出现过的黑客攻入网络内部的事件大部分就是因为安全措施不完善所招致的苦果。另外，软件的“后门”都是软件公司的设计编程人员为了方便而设置的，一般不为外人所知，但一旦“后门”打开，其造成的后果将不堪设想。

总的说来，网络安全的主要威胁来自以下几个方面：

（1）自然灾害、意外事故。

（2）计算机犯罪。

（3）人为行为，比如使用不当，安全意识差等。

（4）“黑客”行为，由于黑客的入侵或侵扰，比如非法访问、拒绝服务、计算机病毒、非法链接等。

（5）内部泄密。

（6）外部泄密。

（7）信息丢失。

（8）电子谍报，比如信息流量分析、信息窃取等。

（9）信息战。

（10）网络协议中的缺陷，例如 TCP/IP 协议的安全问题等。

1.2.2 计算机网络安全的技术隐患

计算机网络的安全隐患是多方面的。从网络组成结构上分，有计算机信息系统的，有通信设备、设施的；从内容上分，有技术上的和管理上的；从技术上来看，主要有以下几个方面。

1. 网络系统软件自身的安全问题

网络系统软件的自身安全与否直接关系到网络的安全，网络系统软件的安全功能较少或不全，以及系统设计时的疏忽或考虑不周而留下的“破绽”都等于给危害网络安全的人和事留下许多“后门”。例如，美国微软公司就经常针对已发现的系统“破绽”发布“补丁”程序。同时，在同一系统软件中，低版本的往往比高版本的在安全性能方面差了许多，所以在服务器上要注意尽量使用高版本的操作系统，并应使用系统软件所能提供的最高安全级别。另外，值得注意的是操作系统的许多缺省值都已被黑客们盯上了，往往被用来作为侵入网络的突破口，所以应尽量避免使用系统缺省值。此外，还要注意的有：

（1）操作系统的体系结构造成其本身是不安全的，这也是计算机系统不安全的根本原因之一。操作系统的程序是可以动态连接的，包括 I/O 的驱动程序与系统服务，都可以采用打“补丁”的方式进行动态连接。许多 UNIX 操作系统的版本的升级、开发都是采用打“补丁”的方式进行的。这种方法既然厂商可以使用，那么黑客也可以使用，同时这种动态连接也成为计算机病毒产生的好环境。

（2）操作系统的一些功能，例如，支持在网络上传输文件的功能，包括可以执行的文件映象，即在网络上加载程序等，必然带来一些不安全因素。

（3）操作系统不安全的另一原因在于它可以创建进程，甚至支持在网络的节点上进行远程进程的创建与激活，更重要的是被创建的进程可以继承创建进程的权力。这一点与可在网络上加载程序结合起来就构成了可以在远端服务器上安装“间谍”软件的条件。若再加上把这种间谍软件以打补丁的方式“打”在一个合法的用户上，尤其“打”在一个特权用户上，系统进程与作业监视程序就都无法监测这些黑客和间谍软件的存在。

（4）操作系统运行时一些系统进程总在等待一些条件的出现，一旦有满足要求的条件出现，程序便继续运行下去，这都是黑客可以利用的。

（5）操作系统要安排无口令入口，这原本是为系统开发人员提供的便捷入口，但它也是黑客的通道。另外，操作系统还有隐蔽信道。