普通高等教育“十一五”国家级规划教材

普通高校本科计算机专业特色教材精选·网络与通信

计算机网络安全与应用技术
(第二版)

袁家政　印　平　主编
商新娜　廖礼萍　编著

清华大学出版社

普通高等教育“十一五”国家级规划教材

普通高校本科计算机专业特色教材精选·网络与通信

计算机网络安全与应用技术（第二版）

袁家政　印　平　主编
商新娜　廖礼萍　编著

清华大学出版社
北京

内 容 简 介

本书主要从网络的基本知识、密码技术、防火墙技术、Windows XP/ 2003/ 2008 操作系统的安全、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。书中提供了大量网络安全与对抗的实例，并从实例引出概念，然后进行归纳总结，帮助读者掌握计算机网络的基本原理，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。

本书是作者长期从事计算机网络教学和网络设计的经验总结，是一本面向本科、高职、高专和成人高等教育的教材，适合于广大在校学生学习，也可供有关工程技术人员阅读。

图书在版编目（CIP）数据

计算机网络安全与应用技术/袁家政，印平主编；商新娜，廖礼萍，编著．--2 版.--北京：清华大学出版社，2011.6
（普通高校本科计算机专业特色教材精选·网络与通信）
ISBN 978-7-302-26125-4

Ⅰ．①计…　Ⅱ．①袁…②印…③商…④廖…　Ⅲ．①计算机网络－安全技术－高等学校－教材　Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 122627 号

责任编辑：谢　琛　薛　阳
责任校对：白　蕾
责任印制：何　芊

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　　总　　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010 62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京市清华园胶印厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185×260　　**印　　张**：21.5　　**字　　数**：522 千字
版　　次：2011 年 6 月第 2 版　　**印　　次**：2011 年 6 月第 1 次印刷
印　　数：1～4000
定　　价：33.00 元

产品编号：026301 01

出版说明

我国高等学校计算机教育近年来迅猛发展，应用所学计算机知识解决实际问题，已经成为当代大学生的必备能力。

随着时代的进步与社会的发展，对高等学校计算机教育的质量提出了更高、更新的要求。现在，很多高等学校都在积极探索符合自身特点的教学模式，涌现出一大批非常优秀的精品课程。

为了适应社会的需求，满足计算机教育的发展需要，清华大学出版社在进行大量调查研究的基础上，组织编写了《高等学校计算机专业教材精选》。本套教材从全国各高校的优秀计算机教材中精挑细选了一批很有代表性且特色鲜明的计算机精品教材，把作者们对各自所授计算机课程的独特理解和先进经验推荐给全国师生。

本系列教材特点如下。

(1) 编写目的明确。本套教材主要面向广大高校的计算机专业学生，使学生通过本套教材，学习计算机科学与技术方面的基本理论和基本知识，接受应用计算机解决实际问题的基本训练。

(2) 注重编写理念。本套教材作者群为各校相应课程的主讲，有一定经验积累，且编写思路清晰，有独特的教学思路和指导思想，其教学经验具有推广价值。本套教材中不乏各类精品课配套教材，并力图努力把不同学校的教学特点反映到每本教材中。

(3) 理论知识与实践相结合。本套教材贯彻从实践中来到实践中去的原则，书中的许多必须掌握的理论都将结合实例来讲，同时注重培养学生分析、解决问题的能力，满足社会用人要求。

(4) 易教易用，合理适当。本套教材编写时注重结合教学实际的课时数，把握教材的篇幅。同时，对一些知识点按教育部教学指导委员会的最新精神进行合理取舍与难易控制。

(5) 注重教材的立体化配套。大多数教材都将配套教师用课件、习题及其解答，学生上机实验指导、教学网站等辅助教学资源，方便教学。

随着本套教材的陆续出版，相信能够得到广大读者的认可和支持，为我国计算机教材建设及计算机教学水平的提高，为计算机教育事业的发展作出应有的贡献。

清华大学出版社

前　言

本书是普通高等教育“十一五”国家级规划教材，是2002年出版的《计算机网络安全与应用技术》教材的修订版。

本书第1版是2002年由教育部和清华大学出版社联合策划出版，第1版出版以来得到了广大读者的认可，被许多高校选为教材，受到了多所院校广大师生的好评，并且于2005年被评为北京市精品教材。

随着计算机网络技术的发展，网络的安全问题越来越受到关注。网络技术已被广泛应用于社会生活甚至国防等各个方面，网络安全已超越其本身而达到国家安全的高度，因此非常有必要在高校开设计算机网络安全的课程。

作为应用型教材，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 Server 2003/2008系统的安全与保护措施、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，总共分为9章。各方面知识内容所占比例为：网络安全理论和知识30%；网络系统（主要指Windows Server 2003、Windows Server 2008 Internet/Intranet）的安全技术特点20%；网络安全配置、操作维护和安全方面的知识50%。本书的教学内容大约需要64课时，最好另外安排32课时的实训。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技术实现。鉴于此，本书的主要内容安排如下。

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基础知识。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、访问控制技术、入侵检测和蜜罐技术等基本概念，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章介绍了网络中的密码技术，包括传统的加密方法、DES加密标准、AES算法、公开密钥体制和其他加密高新技术及其发展；第3章介绍了访问控制技术中防火墙的技术，包括防火墙的原理、种类、选择原则和实现策略等。

第二部分（第4、5章）主要介绍计算机系统及网络操作系统的安全性问题。第4章介绍了网络系统的安全等级，无线局域网和虚拟专用网（VPN）的安全性问题，Windows XP和Windows 7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 2003/ 2008操作系统的网络机制、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 XP操作系统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、宏病毒、熊猫烧香病毒、“尼姆达”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）介绍 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、IIS Web 服务器的安全问题、电子商务的安全问题及配置方法。

第六部分（第 9 章）主要讲述与本书全部内容相对应的网络安全的实训问题。分别是针对密码技术、防火墙技术、Windows XP/2003/2008 操作系统、IE 浏览器、Outlook Express 和 IIS 等知识及安全性所安排的 13 个实训。

通过对该书的学习，读者可以掌握计算机网络安全的基本原理和当前流行的网络系统 Windows XP/2003/2008 系统的安全设置、安全漏洞、管理及维护，同时对 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计算机技术研究所袁家政、印平策划和主编，袁家政、商新娜、廖礼萍、印平编写了部分内容，此外，山西省大同大学的刘春贵副教授也参与了编写。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。

作　者

2011 年 3 月

目　录

第 1 章　计算机网络安全的基础知识

随着计算机技术的飞速发展，信息网络已经成为社会发展的重要保证。信息网络涉及国家的政府、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重要的政府宏观调控决策、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、数据修改、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的安全、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各种资源设施，随时存储和传输大量的数据，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：

- 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。

1.1　计算机网络基础知识

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，用一句简单的话概括即："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距离，且每台计算机系统能独立工作，能够自我处理数据，而无须其他系统帮助。例如：具有通信功能的单机系统，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，但它不属于两个计算

机系统互连在一起，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，由物理介质来和通信设备实现。它们可以是铜线、光纤等“有线”介质，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。

从以上3个方面，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

计算机网络中不同系统的两实体间只有在通信的基础上，才有可能相互交换信息，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的集合。简单说，协议就是通信双方的约定。更进一步讲，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，主要承担通信子网的信息传输和转接的作用；另一类是访问节点，是资源子网中的计算机或终端，主要是信息资源的来源和发送信息的目的地。

不同类型的网络，其通信子网的物理组成各不相同。局域网最简单，它的通信子网由物理传媒介质和主机网络接板（网卡）组成。而广域网，除物理传媒介质和主机网络接板（网卡）外，必须靠通信子网的转接节点传递信息。

对于通信子网的设计，如果从通信信道类型分类有两种类型：点对点通信方式和广播式通信子网。

（1）点对点通信，如图1-1所示。在该种类型网中，任何一段物理链路，都唯一连接一对节点。如果不在同一段物理链路的一对节点要通信，必须通过其他节点转接。采用点对点通信的基本拓扑结构有：星形、树形、环形及不规则形和全部互连等。

（2）广播式通信，如图1-2所示。在该种通信子网中只有一个公共通信信道，为所有节点共享使用，任一时刻只允许一个节点使用公用信道。当一个节点利用公共通信信道发送数据时，必须携带目的地址，其他节点都能收到数据，只有地址符合的那个节点，才接收数据。

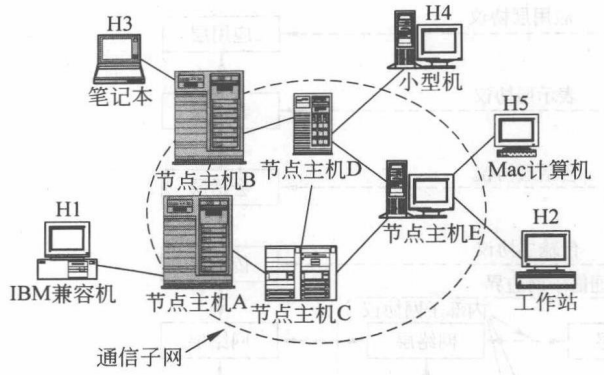

图 1-1　点对点通信方式

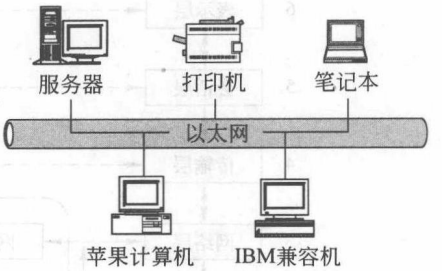

图 1-2　广播式通信方式

4. 计算机网络体系结构

为简化问题、减少协议设计的复杂性，大多数网络都采用一种层次结构，按层或级的方式来组织。因此协议也是分层次的。每一层都建立在下层之上，每一层的目的都是为上层提供一定的服务，并对上层屏蔽其服务的实现细节。各层协议互相协作，构成一个整体，常称之为协议簇(protocol family)或协议套(protocol suite)。

网络分层体系结构模型的概念，为计算机网络协议的设计和实现提供了很大方便。体系结构中最著名的是国际标准化组织(ISO)于 1981 年颁布的开放系统互连参考模型(open system interconnection reference model)，简称 OSI 模型。OSI 定义了异种互联网标准的框架结构，受到计算机和通信行业的极大关注。OSI 不断发展，得到了国际上的承认，成为其他各计算机网络系统结构靠拢的标准，大大地推动了计算机网络和计算机通信的发展。

在这里“系统”是指一台或多台计算机、外部设备、终端、信息传输设备、操作员及相应软件的集合。“开放”是指按照 OSI 参考模式建立的任意两系统之间的连接或操作。当一个系统能按照 OSI 标准与另一个系统进行通信时，就称该系统为开放系统。可见，开放系统要求建立一整套能保证全部级别都能进行通信的标准。

OSI 开放系统互连参考模型，如图 1-3 所示。它采用结构描述方法，即分层描述的方法，将整个网络的通信功能划分成 7 个部分(也叫 7 个层次)，每层各自完成一定的功能。由低层至高层分别称为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。这种划分使每一层都能执行本层所承担的具体任务，且功能相对独立，通过接口与其相邻层连接。这里接口指相邻层之间的连接，依靠各层之间的接口或功能的组合，实现两系统间、各节点间信息的传输。

(1) 物理层(physical layer)

物理层涉及通信在信道上传输的原始比特流，主要处理与物理传输介质有关的机械的、电气的、功能的和规程的接口。物理层与具体设备有关，如光纤及收发器、网卡和集线器等。

(2) 数据链路层(data link layer)

数据链路层的主要任务是加强物理层传输原始比特的功能，使之对网络层显现为一条无差错的链路。它通过将传输的数据增加同步信息、校验信息及地址信息封装成数据帧。同时提供数据帧传输顺序的控制、差错检测与控制和数据流量控制以保证数据的正确性。