高职高专立体化教材计算机系列

网络安全管理与维护

WANGLUOANQUAN GUANLI YU WEIHU

付忠勇 主 编
赵振洲 副主编

赠送电子课件及
其他立体化资源

清华大学出版社

网络安全管理与维护

高职高专立体化教材　计算机系列

网络安全管理与维护

付忠勇　　主　编
赵振洲　　副主编

清华大学出版社
北　京

内 容 简 介

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方法，并尽量跟踪网络安全技术的最新成果与发展方向。全书共分 12 章，分别讲述网络安全的基本概念、数据加密和认证、常见网络攻击方法与防护、病毒分析与防御、防火墙技术、入侵检测技术、操作系统安全、因特网安全技术、无线网络安全、网络安全管理、安全审计与风险分析和实训方案等。各方面知识内容所占比例为：网络安全理论知识占 40%，操作系统安全知识占 10%，网络安全配置管理、操作维护方面的知识占 50%。

本书内容涵盖了网络安全的基础知识及其管理和维护的基本技能。本书既可以作为高职院校网络安全、信息安全等相关专业的课程教材，也可作为各种培训班的培训教材。

图书在版编目(CIP)数据

网络安全管理与维护/付忠勇主编；赵振洲副主编. —北京：清华大学出版社，2009.6
(高职高专立体化教材　计算机系列)
ISBN 978-7-302-20046-8

Ⅰ. 网…　Ⅱ. ①付…　②赵…　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(2009)第 064684 号

责任编辑：刘天飞　桑任松
封面设计：山鹰工作室
版式设计：杨玉兰
责任校对：李玉萍
责任印制：李红英
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：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京市世界知识印刷厂
装 订 者：三河市李旗庄少明装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：21.75　**字　数**：526 千字
版　　次：2009 年 6 月第 1 版　　**印　　次**：2009 年 6 月第1 次印刷
印　　数：1～4000
定　　价：33.00 元

《高职高专立体化教材计算机系列》丛书序

一、编写目的

关于立体化教材，国内外有多种说法，有的叫“立体化教材”，有的叫“一体化教材”，有的叫“多元化教材”，其目的是一样的，就是要为学校提供一种教学资源的整体解决方案，最大限度地满足教学需要，满足教育市场需求，促进教学改革。我们这里所讲的立体化教材，其内容、形式、服务都是建立在当前技术水平和条件基础上的。

立体化教材是一个“一揽子”式的，包括主教材、教师参考书、学习指导书、试题库在内的完整体系。主教材讲究的是“精品”意识，既要具备指导性和示范性，也要具有一定的适用性，喜新不厌旧，内容愈编愈多，本子愈编愈厚的低水平重复建设在“立体化”的世界中将被扫地出门。和以往不同，“立体化教材”中的教师参考书可不是千人一面的，教师参考书不只是提供答案和注释，而是含有与主教材配套的大量参考资料，使得老师在教学中能做到“个性化教学”。学习指导书更像一本明晰的地图册，难点、重点、学习方法一目了然。试题库或习题集则要完成对教学效果进行测试与评价的任务。这些组成部分采用不同的编写方式，把教材的精华从各个角度呈现给师生，既有重复、强调，又有交叉和补充，相互配合，形成一个教学资源有机的整体。

除了内容上的扩充，立体化教材的最大突破还在于在表现形式上走出了“书本”这一平面媒介的局限，如果说音像制品让平面书本实现了第一次“突围”，那么电子和网络技术的大量运用就让躺在书桌上的教材真正“活”了起来。用 PowerPoint 开发的电子教案不仅大大减少了教师案头备课的时间，而且也让学生的课后复习更加有的放矢。电子图书通过数字化使得教材的内容得以无限扩张，使平面教材更能发挥其提纲挈领的作用。

CAI 课件把动画、仿真等技术引入了课堂，让课程的难点和重点一目了然，通过生动的表达方式达到深入浅出的目的。在科学指标体系控制之下的试题库既可以轻而易举地制作标准化试卷，也能让学生进行模拟实战的在线测试，提高了教学质量评价的客观性和及时性。网络课程更厉害，它使教学突破了空间和时间的限制，彻底发挥了立体化教材本身的潜力，轻轻敲击几下键盘，你就能在任何时候得到有关课程的全部信息。

最后还有资料库，它把教学资料以知识点为单位，通过文字、图形、图像、音频、视频、动画等各种形式，按科学的存储策略组织起来，大大方便了教师在备课、开发电子教案和网络课程时的教学工作。如此一来，教材就“活”了。学生和书本之间的关系不再像领导与被领导那样呆板，而是真正有了互动。教材不再只为老师们规定什么重要什么不重要，而是成为教师实现其教学理念的最佳拍档。在建设观念上，从提供和出版单一纸质教材转向提供和出版较完整的教学解决方案；在建设目标上，以最大限度满足教学要求为根本出发点；在建设方式上，不单纯以现有教材为核心，简单地配套电子音像出版物，而是

以课程为核心，整合已有资源并聚拢新资源。

网络化、立体化教材的出版是我社下一阶段教材建设的重中之重，作为以计算机教材出版为龙头的清华大学出版社确立了“改变思想观念，调整工作模式，构建立体化教材体系，大幅度提高教材服务”的发展目标。并提出了首先以建设“高职高专计算机立体化教材”为重点的教材出版规划，希望通过邀请全国范围内的高职高专院校的优秀教师，在2008年共同策划、编写这一套高职高专立体化教材，利用网络等现代技术手段实现课程立体化教材的资源共享，解决国内教材建设工作中存在教材内容的更新滞后于学科发展的状况。把各种相互作用、相互联系的媒体和资源有机地整合，形成立体化教材，把教学资料以知识点为单位，通过文字、图形、图像、音频、视频、动画等各种形式，按科学的存储策略组织起来，为高职高专教学提供一整套解决方案。

二、教材特点

在编写思想上，以适应高职高专教学改革的需要为目标，以企业需求为导向，充分吸收国外经典教材及国内优秀教材的优点，结合中国高校计算机教育的教学现状，打造立体化精品教材。

在内容安排上，充分体现先进性、科学性和实用性，尽可能选取最新、最实用的技术，并依照学生接受知识的一般规律，通过设计详细的可实施的项目化案例(而不仅仅是功能性的小例子)，帮助学生掌握要求的知识点。

在教材形式上，利用网络等现代技术手段实现立体化的资源共享，为教材创建专门的网站，并提供题库、素材、录像、CAI 课件、案例分析，实现教师和学生在更大范围内的教与学互动，及时解决教学过程中遇到的问题。

本系列教材采用案例式的教学方法，以实际应用为主，理论够用为度。教程中每一个知识点的结构模式为“案例(任务)提出→案例关键点分析→具体操作步骤→相关知识(技术)介绍(理论总结、功能介绍、方法和技巧等)”。

该系列教材将提供全方位、立体化的服务。网上提供电子教案、文字或图片素材、源代码、在线题库、模拟试卷、习题答案、案例动画演示、专题拓展、教学指导方案等。

在为教学服务方面，主要是通过教学服务专用网站在网络上为教师和学生提供交流的场所，每个学科、每门课程，甚至每本教材都建立网络上的交流环境。可以为广大教师信息交流、学术讨论、专家咨询提供服务，也可以让教师发表对教材建设的意见，甚至通过网络授课。对学生来说，则在教学支撑平台上所提供的自主学习空间来实现学习、答疑、作业、讨论和测试，当然也可以对教材建设提出意见。这样，在编辑、作者、专家、教师、学生之间建立起一个以网络为纽带、以数据库为基础、以网站为门户的立体化教材建设与实践的体系，用快捷的信息反馈机制和优质的教学服务促进教学改革。

本系列教材专题网站：http://www.lth.wenyuan.com.cn。

前　言

随着信息社会的到来以及 Internet 的迅猛发展，网络已经影响到社会生活的各个领域，给人类的生活方式带来了巨大的变革。人们在利用网络实现资源共享、进行电子商务等社会活动，享受网络给我们带来便利的同时，安全问题也变得日益突出。黑客入侵，网络病毒肆虐，网络系统损坏或瘫痪，重要数据被窃取或毁坏等，给政府、企业以及个人带来了巨大的经济损失，也为网络的健康发展造成了巨大的障碍。网络信息安全问题已成为网络技术领域的重要研究课题，它已经成为一个组织生死存亡或贸易盈亏成败的决定性因素之一，因此信息安全逐渐成为人们关注的焦点。世界范围内的各个国家、机构、组织、个人都在探寻如何保障信息安全的问题，各相关部门和研究机构也纷纷投入相当多的人力、物力和资金来试图解决信息安全问题。

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方法，并尽量跟踪网络安全技术的最新成果与发展方向。全书网络安全理论知识占 40%、操作系统安全知识占 10%、网络安全配置管理、操作维护方面的知识占 50%。本书的教学内容大约需要 48 课时，实训需 32 课时。部分内容可由各校教师酌情确定是否讲授。

本书特点主要体现在以下三个方面。首先是通俗易懂，计算机网络的技术性很强，网络安全技术本身也比较晦涩难懂，本书力求以通俗的语言和清晰的叙述方式，向读者介绍计算机网络安全的基本理论、基本知识和实用技术。其次是突出实用，通过阅读本书，读者可掌握计算机网络安全的基础知识，并了解设计和维护网络及其应用系统安全的基本手段和方法。本书在编写形式上突出了应用的需求，每一章的理论内容都力求结合实际案例进行教学，第 12 章还设计了与前述章节内容配套的实训方案，从而为教学和自主学习提供了方便。第三是选材新颖，计算机应用技术和网络技术的发展是非常迅速的，本书在内容组织上力图靠近新知识、新技术的前沿，以使本书能较好地反映新理论和新技术。

参加本书编写的教师都长期工作在教学的第一线，具有丰富的教学经验。其中第 1 章和第 10 章由付忠勇执笔，第 2 章和第 6 章由乔明秋执笔，第 3 章由李星华执笔，第 4 章和第 7 章由赵振洲执笔，第 5 章和第 8 章由胡守国执笔，第 9 章和第 11 章由郑宝昆执笔，第 12 章由上述 6 位老师共同完成。付忠勇、赵振洲负责内容的组织、统稿和审定。

由于水平所限，疏漏与谬误之处在所难免，恳请专家、同仁及广大读者批评指教。

编　者

目　录

第 1 章　网络安全概述

本章要点

- 网络安全现状及面临的威胁
- 网络攻击的类别
- 网络安全的特点、属性及主要安全技术

近年来，计算机信息技术的发展，使网络成为全球信息传递、信息交互的主要途径，并在政治、经济、军事、文化、教育等社会生活的各个领域产生了巨大的影响，迅速改变着人们的生产和生活方式。然而，信息网络的发达，同时也伴随着巨大的风险。事实上，网络安全已经成为关系国家主权和国家安全、经济繁荣和社会稳定、文化传承和教育进步的重大问题，并且随着全球化步伐的加快而愈显其重要。因此，我们在利用网络信息资源的同时，必须加强网络信息安全技术的研究和开发。

网络安全已经成为网络发展的瓶颈，阻碍着网络应用在各个领域的纵深发展。面对网络安全的严峻形势，我们应当持辩证、客观的态度，一方面不能因噎废食，拒绝先进的网络技术和文化；另一方面要对网络的安全威胁给予充分的重视。政府对网络安全技术的研发给予积极支持，普通网络使用者和网络提供商也应该充分认识到网络安全及网络管理的重要性，保护好个人、集体和国家利益不受侵害。

构筑信息网络安全防线事关重大，刻不容缓。

1.1　网络安全现状

1.1.1　网络的发展

20 世纪末信息技术领域内最使人振奋的重大事件是互联网的发展，它已遍及 180 多个国家和地区。无论你身在办公室、家里、工地、野外、大街，或是正在旅途中、海边，都可以与互联网亲密接触！无论是在工作、学习、玩游戏、炒股，你都需要互联网！

据《第 20 次中国互联网络发展状况统计报告》统计，截至 2007 年 6 月，中国网民人数已经达到 1.62 亿，如图 1-1 所示，仅次于美国 2.11 亿的网民规模，位居世界第二。这比 2006 年年末新增了 2500 万网民，与 2006 年同期相比，网民数 1 年内增加了 3900 万人。中国网民年增长率达到 31.7%，步入新一轮的快速增长阶段。

目前中国的互联网普及率已经达到 12.3%，比 2006 年同期 9.4%的互联网普及率提高了接近 3 个百分点，如图 1-2 所示。互联网在中国的应用正逐步广泛化，越来越多的人接触到互联网，并从互联网世界获益。根据 CNNIC 统计，接触过互联网的人中，99%都会继续上网。

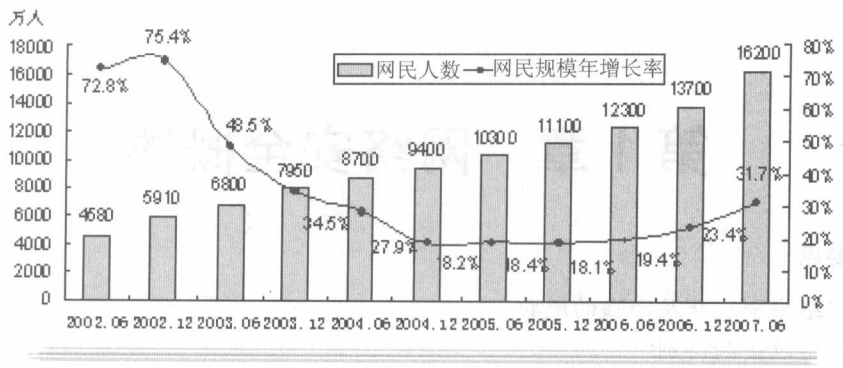

图 1-1　中国网民规模和年增长率

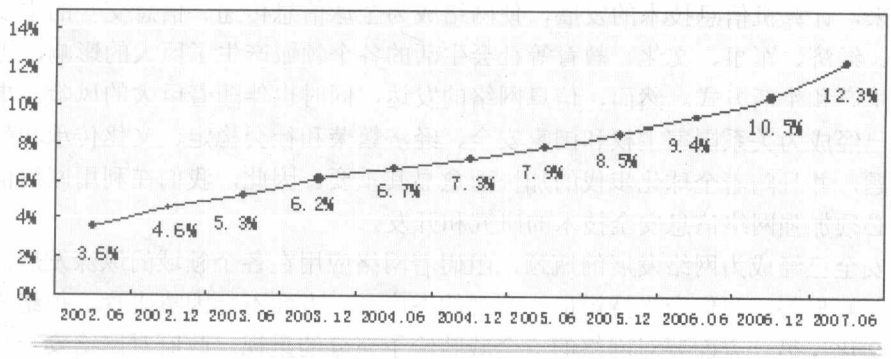

图 1-2　中国互联网普及率

1.1.2　网络安全概念

与能源、物源一样，信息资源同样具有价值，在有些情况下，价值更高。具有价值的信息必然存在安全问题。

网络安全是指保护网络系统中的软件、硬件及信息资源，使之免受偶然或恶意的破坏、篡改和泄露，保证网络的正常运行，以及网络服务不中断。

网络安全包括网络软、硬件资源和信息资源的安全性。

从广义上讲，凡是涉及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问题。

网络安全涉及的内容有技术方面的问题，也有管理方面的问题，两者相辅相成，缺一不可。

1.1.3　网络安全现状

互联网的飞速发展，使社会政治、经济、文化、教育等各个领域的网络应用蓬勃兴起。与此同时，“信息垃圾”、“邮件炸弹”、“电脑病毒”等也开始在网上肆意横行，不仅造成了难以估量的社会资源的损失，也给网络发展中投下了巨大的阴影，产生了巨大的阻力。

目前，全球范围内，平均每 20 秒就会发生一起主机入侵事件，有高达 75%的网站抵御不了黑客的攻击。全球已发现病毒及其变种 5 万多个，而病毒所造成的损失占到网络经济损失的 76%。

1. 全球范围的网络安全事件

据美国“世界日报”1993 年 10 月报道，由于高技术犯罪，利用侦读器拦截卫星通信电话的用户号码，再转手复制出笼，1992 年美国就有 20 亿美元的国际电话费转帐混乱，给公司造成严重损失。

2000 年 2 月包括 Yahoo 在内的若干世界最大的网站都遭受了黑客攻击而停止服务。

2002 年 10 月，黑客入侵微软公司一台托管 Windows 测试网络的服务器，这个服务器是为 2000 多位 Windows 用户提供测试正在开发中的软件的服务器。

2003 年 2 月 18 日，美国 3 大信用卡集团——万事达(MasterCard)、维萨(Visa)和美国运通(American Express)被一个“未经授权的入侵者”成功通过电脑网络安全漏洞进入信用卡网络。

据美国联邦调查局的报告，计算机犯罪是商业犯罪中最大的犯罪类型之一，每笔犯罪的平均金额超过 45000 美元，每年因犯罪造成的经济损失达百亿美元，以后还将上升。

美国《防务新闻》2003 年 5 月 12 日报道如下。

据国防部计算机网络作战联合特遣部队统计，1999—2002 年发生在美国国防部网络的入侵企图次数如下所示。

- 1999 年：22000 次。
- 2000 年：24000 次。
- 2001 年：40000 次。
- 2002 年：45000 次。

据国防信息系统局统计，2002 年国防部网络的信息安全事故的类型及次数如下所示。

- 拒绝服务，即拒绝合法使用：36 次。
- 资源误用：39 次。
- 网址毁损：46 次。
- 个人帐户的未经授权使用：111 次。
- 机构帐户的未经授权使用：125 次。
- 病毒、蠕虫、特洛伊木马和其他恶毒代码：265 次。
- 其他：1268 次。
- 侦察：488000 次。

据 CERT 协调中心统计，1999—2002 年美国商业和学术界网络信息安全事故数量如下所示。

- 1998 年：4952 次。
- 1999 年：9859 次。
- 2000 年：21756 次。
- 2001 年：52658 次。

- 2002 年：82094 次。
- 2003 年：第一季度为 42586 次，预计全年将达 170000～180000 次。

美国 21 世纪国家安全委员会在 1999 年发表的《新世纪国家安全报告》中，已首次将网络攻击武器定义为大规模破坏性武器，并将其与专指核、生化武器的大规模毁灭性武器相提并论。

2．国内网络安全事件

近几年来，我国网络受黑客侵犯事件也屡屡发生，数量每年呈明显上升趋势，所以更应加强对网络安全的防护。

据有关部门统计，全国公安机关 2002 年共受理各类信息网络违法犯罪案件 6633 起，比 2001 年增长 45.9%，其中利用计算机实施的违法犯罪案件 5301 起，占案件总数的近 80%。如 1997 年 12 月 19 日至 1999 年 8 月 18 日，有人先后 19 次入侵某证券公司上海分公司的电脑数据库，非法操作股票价格，累计挪用金额 1290 万元；1999 年 4 月 16 日，黑客入侵中亚信托投资公司上海某证券营业部，造成 340 万元的损失。

中国的银行每年也损失数亿元人民币。以前有个钓鱼网站的网址及界面都与某正式的银行网站类似，如图 1-3 所示。

图 1-3　某钓鱼网站的页面

利用计算机网络进行的各类违法行为在中国以每年 30% 的速度递增，而已发现的黑客攻击案只占总数的 30%。

同时，网络安全人才的需求暴涨，中国对网络安全人才的需求在今后几年内将超过 100 万，但专业的网络与信息安全机构在国内却屈指可数。

网络信息安全已经初步形成一个产业，根据权威职业调查机构的预测表明，网络信息安全人才必将成为信息时代最热门的抢手人才。

1.2 网络安全威胁

网络安全威胁是指对网络信息的机密性、完整性、可用性在合法使用时可能造成的危害。主要有以下几个方面。

1. 不良信息的入侵和污染

Internet 是一个开放的世界，很多国家和地区的经营商在利益的驱动下，开放淫秽网站，大量制作色情网页。

2. 计算机犯罪

对计算机及网络的攻击活动每年正在以 10 倍的速度增长。例如：破坏程序、修改网页、转移金额、窃取密码、进行电子邮件骚扰、阻塞用户等。

3. 网络病毒

活体病毒已达 50000 多种。发作时，计算机系统陷于瘫痪。

4. 协议安全漏洞

TCP/IP 协议是一个开放式协议，其本身很不安全。黑客可以使用如 Sniffer、Tcpdump 或 Snoop 等类似软件，看到一台计算机登录到另外一台计算机的全过程，同时可以获取口令和明文。

5. 操作系统安全漏洞

Windows、UNIX 等系统都存在一些安全漏洞。厂商在不断升级系统的同时也在生产新的 bug。操作系统厂商不时发布一些补丁程序，但新的程序出来后又有新的 bug。

公理(摩菲定理)：所有的程序都有缺陷。

定理(大程序定理)：大程序的缺陷甚至比它包含的内容还多。

推论：一个安全相关程序有安全性缺陷。

1) UNIX 安全漏洞举例

(1) Arp 命令漏洞。受影响的系统：SunOS 4.1.x。

```
$ arp  -f/dev/kmem | string > mem
```

运行该命令后，会把当前内存的信息写入当前目录下的 mem 文件，通过普通的文本编辑器就可以查看内存的情况。

(2) Sun 的 Java Web 服务器远程命令执行漏洞。受影响的系统：Solaris、使用 Sun Java Web Server 的所有版本的系统。

Sun 的 Java Web 服务器默认配置存在一个漏洞。使用 Java Web 服务器提供的公告示例应用，就有可能在目标机系统上远程执行任何命令。

2) Linux 安全漏洞

(1) RedHat Linux ping 缓冲区溢出漏洞。受影响的系统：RedHat Linux 7.0、6.2。Ping 命令存在两处缓冲区溢出，本地用户有可能利用此漏洞获取 root 权限。

(2) Linux ls-w 参数本地拒绝服务漏洞。受影响的系统：Linux RedHat 6.x、Linux Slackware 7.0。

一些 Linux 系统中的 ls 命令包含一个-w 选项，它可以用来定义显示屏幕的宽度，同时指定一个很大的宽度数值，通过循环执行多次相应的命令，来耗尽系统内存。

3) Windows XP 安全漏洞举例

(1) Microsoft Windows 标准输出系统崩溃漏洞。Windows NT/2000/XP 操作系统的标准输出系统存在安全漏洞，通过发送特定的空格序列，可能导致标准输出系统崩溃。

(2) Windows XP 终端服务 IP 欺骗漏洞。Windows 2000/XP 的终端服务器允许远程攻击者匿名访问该服务。假设某个客户端位于路由器的后面，并且只有内部 IP 地址，如果该客户端与远程终端服务器建立连接的话，那么远程的终端服务器就会记录该客户端的内部 IP 地址，而该地址没有什么意义。

6. 网络硬件设备

由于网络技术发展的客观原因，路由器等网络设备过分依赖国外产品，从而埋下了安全隐患。

7. 数据库漏洞

加密强度不够，存在安全漏洞等。

例 1 Oracle_home 环境变量缓存区溢出漏洞。

受影响的系统：Oracle 8.0、8.1.6、9.0.1 等。

当 Oracle_home 环境包含有 750bytes 或更多的时候，缓存区溢出。

例 2 Oracle 包含一些默认用户/口令组合：Scott/Tiger、Dbsnmp/Dbsnmp、System/Manager 等。

例 3 可以用 TCP/IP 协议从 1521 和 1526 端口访问 Oracle 7.3 和 Oracle 8 等数据库。

8. 安全管理漏洞

例如：路由器配置错误，开放匿名 FTP，TELNET，口令文件缺乏安全保护，防火墙配置不正确，操作失误，缺乏安全知识等。

总之，在没有采取防护措施的网络中，其安全漏洞有上千种。

1.3 网 络 攻 击

1.3.1 潜在的对手

进行网络攻击的潜在对手有以下几种。

(1) 国家：组织精良并得到很好的财政资助。

(2) 黑客：攻击网络和系统，企图探求操作系统的脆弱性或其他缺陷的人(能解密者、