21世纪

中国高等职业技术教育研究会推荐
高职高专计算机专业规划教材

计算机网络安全基础与技能训练

主　编　吴献文
主　审　李卓玲

西安电子科技大学出版社
http://www.xduph.com

□ 中国高等职业技术教育研究会推荐

高职高专计算机专业规划教材

计算机网络安全基础与技能训练

主　编　吴献文

副主编　刘志成　毛春丽　龚　娟

主　审　李卓玲

西安电子科技大学出版社

2008

内 容 简 介

本书介绍了计算机网络安全的基础知识和常用的安全技术、安全策略，适应“以学生为中心”的教育思想，遵循学生的认知规律，由浅入深，由基础到专业、到实践，层层深入，并结合高职教育的特点，增强了实践动手的内容，弱化了理论部分，让学生在“学中做”，在“做中学”，更加适应学生自主学习和能力的培养。

本书共分为七个章节。

第 1 章是整本书的基础部分，从网络的脆弱性入手，介绍了网络安全的概念、策略、标准、基本模型、体系结构、安全机制与技术和网络安全法律法规等理论基础知识。

第 2～7 章分别介绍了病毒技术、黑客技术、加密技术、数字签名技术、防火墙技术和入侵检测技术等各项安全领域的专业技术，通过实例操作的方式详细阐述了每一种技术的应用。

本书可作为高职高专院校计算机专业的教材，也可供计算机爱好者参考借鉴。

★ 本书配有电子教案，有需要的老师可与出版社联系，免费提供。

图书在版编目(CIP)数据

计算机网络安全基础与技能训练/吴献文主编. —西安：西安电子科技大学出版社，2008.7

中国高等职业技术教育研究会推荐. 高职高专计算机专业规划教材

ISBN 978-7-5606-2043-5

Ⅰ. 计… Ⅱ. 吴… 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(2008)第 067546 号

策　　划　杨　璠

责任编辑　杨　璠

出版发行　西安电子科技大学出版社(西安市太白南路 2 号)

电　　话　(029)88242885　88201467　　邮　编　710071

http: //www.xduph.comE-mail: xdupfxb001@163.com

经　　销　新华书店

印刷单位　陕西光大印务有限责任公司

版　　次　2008 年 7 月第 1 版　2008 年 7 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　印　张　14.5

字　　数　333 千字

印　　数　1～4000 册

定　　价　21.00 元

ISBN 978-7-5606-2043-5/TP・1054

XDUP 2335001-1

序

进入21世纪以来，高等职业教育呈现出快速发展的形势。高等职业教育的发展，丰富了高等教育的体系结构，突出了高等职业教育的类型特色，顺应了人民群众接受高等教育的强烈需求，为现代化建设培养了大量高素质技能型专门人才，对高等教育大众化作出了重要贡献。目前，高等职业教育在我国社会主义现代化建设事业中发挥着越来越重要的作用。

教育部2006年下发了《关于全面提高高等职业教育教学质量的若干意见》，其中提出了深化教育教学改革，重视内涵建设，促进“工学结合”人才培养模式改革，推进整体办学水平提升，形成结构合理、功能完善、质量优良、特色鲜明的高等职业教育体系的任务要求。

根据新的发展要求，高等职业院校积极与行业企业合作开发课程，根据技术领域和职业岗位群任职要求，参照相关职业资格标准，改革课程体系和教学内容，建立突出职业能力培养的课程标准，规范课程教学的基本要求，提高课程教学质量，不断更新教学内容，而实施具有工学结合特色的教材建设是推进高等职业教育改革发展的重要任务。

为配合教育部实施质量工程，解决当前高职高专精品教材不足的问题，西安电子科技大学出版社与中国高等职业技术教育研究会在前三轮联合策划、组织编写“计算机、通信电子、机电及汽车类专业”系列高职高专教材共160余种的基础上，又联合策划、组织编写了新一轮“计算机、通信、电子类”专业系列高职高专教材共120余种。这些教材的选题是在全国范围内近30所高职高专院校中，对教学计划和课程设置进行充分调研的基础上策划产生的。教材的编写采取在教育部精品专业或示范性专业的高职高专院校中公开招标的形式，以吸收尽可能多的优秀作者参与投标和编写。在此基础上，召开系列教材专家编委会，评审教材编写大纲，并对中标大纲提出修改、完善意见，确定主编、主审人选。该系列教材以满足职业岗位需求为目标，以培养学生的应用技能为着力点，在教材的编写中结合任务驱动、项目导向的教学方式，力求在新颖性、实用性、可读性三个方面有所突破，体现高职高专教材的特点。已出版的第一轮教材共36种，2001年全部出齐，从使用情况看，比较适合高等职业院校的需要，普遍受到各学校的欢迎，一再重印，其中《互联网实用技术与网页制作》在短短两年多的时间里先后重印6次，并获教育部2002年普通高校优秀教材奖。第二轮教材共60余种，在2004年已全部出齐，有的教材出版一年多的时间里就重印4次，反映了市场对优秀专业教材的需求。前两轮教材中有十几种入选国家“十一五”规划教材。第三轮教材2007年8月之前全部出齐。本轮教材预计2008年全部出齐，相信也会成为系列精品教材。

教材建设是高职高专院校教学基本建设的一项重要工作。多年来，高职高专院校十分重视教材建设，组织教师参加教材编写，为高职高专教材从无到有，从有到优、到特而辛勤工作。但高职高专教材的建设起步时间不长，还需要与行业企业合作，通过共同努力，出版一大批符合培养高素质技能型专门人才要求的特色教材。

我们殷切希望广大从事高职高专教育的教师，面向市场，服务需求，为形成具有中国特色和高职教育特点的高职高专教材体系作出积极的贡献。

中国高等职业技术教育研究会会长 [illegible]

2007年6月

高职高专计算机专业规划教材
编审专家委员会

前　言

计算机技术的飞速发展促进了网络的发展。网络已经普遍存在于我们的生活、学习和工作环境中。计算机网络的安全是网络可靠、稳定运行的保证，因此必须掌握网络的安全基础知识，学会如何安全使用，如何有效地保证、维护网络的安全，才能建立和维护一个有效的、满足要求的、安全的网络系统。

本书介绍了计算机网络安全的基础知识和常用的安全技术、安全策略，适应“以学生为中心”的教育思想，遵循学生的认知规律，由浅入深，由基础到专业、到实践，层层深入，并结合高职教育的特点，增强了实践动手的内容，弱化了理论部分，让学生在“学中做”，在“做中学”，更加适应学生自主学习和能力的培养。

编者总结多年的“计算机网络安全技术”课程教学经验，以安全技术案例为核心，采用引入、讲述、应用、疑难解析、知识拓展的模式，由浅入深，围绕实际案例展开对安全技术知识的介绍。本书遵循“项目驱动 + 案例教学”的教学模式，在案例的支持下展开对知识点的介绍。

本书在编写过程中十分注意教材内容的取舍和安排，具有以下主要特点：

第一，教材内容以应用为中心。采用“项目驱动”的编写方式，以实际项目引出相关的原理和概念；在实训过程中融入知识点，并通过实训思考、实训总结进行分析归纳，解决实训中出现的问题，提高学生动手能力以及发现问题、分析问题、解决问题的能力。

第二，教材内容以实用为目标。不追求面面俱到，力求突出重点。

第三，采用“层次化”策略。在项目驱动下，采用由浅入深、层次递进的方式，兼顾不同层次学生的需求，设有基本掌握部分和拓展部分。

第四，“模块化”教学。教材编写时采用“模块化”思想，由基础知识和实训内容组成一个知识模块，真正实现“一体化教学”，边讲边练、讲练结合，而且学习节奏紧凑，老师讲完某一项技能或知识点，学生马上就练，练中出现了问题再看原理和知识点，然后再练，形成一个“讲—练—发现问题—再讲—再练—解决问题”的小循环，有利于学生自主学习能力的培养，增强学生学习的成就感，提高学习兴趣。

第五，面向课堂教学全过程设置教学环节，将知识讲解、技能训练和能力的提高有机结合起来。除了第一章外，其余每一章都设有知识讲解与示范、实例、疑难解析、知识拓展、本章小结、思考与习题、实训等环节。

参与本书编写工作的人员都是长期从事计算机网络技术和计算机网络安全技术课程教学的一线教授和长期从事网络安全管理和维护的网络工程师，具有丰富的教学经验和实践经验。本书由湖南铁道职业技术学院吴献文任主编，刘志成、毛春丽、龚娟任副主编。第 1 章由龚娟编写，第 2 章由谢树新编写，第 3 章由言海燕编写，第 4 章由吴献文编写，第 5 章由薛志良编写，第 6 章由毛春丽编写，第 7 章由刘志成编写。另外，张杰、颜谦和、周

进等也参与了本书的校对、整理和修改工作，并提出了许多宝贵意见。本书写作过程中也得到了西安电子科技大学出版社杨璠编辑的大力支持和帮助，在此一并表示感谢。

由于作者水平有限，书中难免有不足之处，恳请读者批评指正。

主编 E-mail：wxw_422lxh@126.com。

编　者

2008 年 3 月

目　录

第 1 章　网络安全基础

随着网络技术的不断发展，网络在人们的生活中已经占有越来越重要的位置，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，成为当今网络技术研究的一个重要课题。

【本章学习要求】

1. 知识技能目标

(1) 了解计算机网络系统的脆弱性；
(2) 了解网络安全的现状及所涉及的领域；
(3) 掌握网络安全的概念；
(4) 熟悉实现网络安全的策略；
(5) 熟悉网络安全的体系结构；
(6) 了解常用的网络安全机制与技术；
(7) 熟悉常见的网络安全法规。

2. 要点内容

(1) 本章重点：网络安全的概念，网络安全的实现策略，网络安全的体系结构；
(2) 本章难点：网络安全的体系结构，网络安全机制与技术。

3. 能力目标

(1) 培养学生的自主学习能力和知识应用能力；
(2) 培养学生勤于思考、认真做事的良好作风；
(3) 培养学生具有良好的职业道德和较强的工作责任心。

1.1　网络安全概述

1.1.1　计算机网络系统的脆弱性分析

随着计算机技术的迅速发展，人类社会已经进入信息时代，或称网络化时代。互联网、计算机网和各种通信网的飞速发展，使得网络已经成为人们新的社会生活空间，信息和网络已经成为社会发展的重要保证。

网络最重要的作用是资源共享，但资源共享和信息安全是一对矛盾。随着网络资源共享的加强，随之而来的信息安全问题也日益突出，网络安全已成为一个值得关注的重要问题。各种计算机病毒和网上黑客(Hackers)对互联网的攻击越来越激烈，许多网站遭受破坏的事例不胜枚举。国家计算机网络应急技术处理协调中心(简称 CNCERT/CC)在其 2006 年网络安全工作年报中指出:“CNCERT/CC 在 2006 年接收和自主发现的网络安全事件与 2005 年同期相比有了大幅度的增加，其中涉及国内政府机构和重要信息系统部门的网页篡改类事件、涉及国内外商业机构的网络仿冒类事件和针对互联网企业的拒绝服务攻击类事件的影响最为严重，僵尸网络和木马的威胁依然非常严重，攻击者谋求非法利益的目的更加明确，行为更加嚣张，黑客地下产业链基本形成。”

信息系统安全漏洞是各种安全威胁的主要根源之一。2006 年 CNCERT/CC 共整理发布和我国用户密切相关的漏洞公告 87 个，同比 2005 年增长了 16%；其中的部分漏洞严重威胁互联网的运行安全，更多的漏洞则对广大互联网用户的系统造成严重威胁。2006 年与安全漏洞关系密切的零日攻击现象在互联网上显著增多。“零日攻击”是指漏洞公布当天就出现相应的攻击手段，例如 2006 年出现的“魔波蠕虫”(利用 MS06-040 漏洞)以及利用微软 Word 漏洞(MS06--011 漏洞)进行的木马攻击等。

此外，恶意代码成为黑客入侵用户主机、构建僵尸网络，进而窃取用户重要信息并控制受害计算机发动大规模攻击的重要手段。2006 年，仅 CNCERT/CC 每天通过分布式蜜网所捕获的新的漏洞攻击型恶意代码数量就达到 96 个，平均每天捕获次数高达 3069 次。除此以外，互联网上还充斥着大量通过网页、邮件、聊天攻击、P2P 传播的恶意代码，令人防不胜防。

总体来看，我国的公共互联网网络安全状况令人堪忧，在利益的驱动下网络安全事件更加频繁、隐蔽和复杂，需要政府、产业界、运营商、网络用户等各方给以高度重视并加强合作，采取切实有效的措施加以应对。

1. 国内外典型的安全事件

2000 年 3 月，英国出现了历史上最为严重的公司计算机系统入侵案。在英国的一伙骇客侵入了至少 12 家跨国公司的系统，盗走了机密文件，事后索要 1000 万英镑的赎金。

2005 年 4 月，深圳市某人才交流服务网站因受到来历不明的 DDoS(即分布式拒绝服务，这是一种目前黑客经常采用而难以防范的攻击手段)攻击，导致该网站无法正常访问，损失严重。

2006 年 5 月 9 日，广州市物价局官方网站被链接到某成人网站。

2006 年 1 月份，熊猫烧香(武汉男生，Worm.WhBoy)病毒以近乎完美的传播方式引发病毒狂潮。该病毒通过多种方式进行传播，并将感染的所有程序文件改成熊猫举着三根香的模样，同时该病毒还具有盗取用户游戏账号、QQ 账号等功能。该病毒传播速度快，危害范围广，短时间内已有上百万个人用户、网吧及企业局域网用户遭受感染和破坏，引起社会各界高度关注。熊猫烧香病毒利用的传播方式囊括了漏洞攻击、感染文件、移动存储介质、局域网传播、网页浏览、社会工程学欺骗等种种可能的手法。

2. 当前网络安全事件的特点

(1) 入侵者难以追踪。有经验的入侵者往往不直接攻击目标，而是利用所掌握的分散在

不同网络运营商、不同国家或地区的跳板机发起攻击，使得对真正入侵者的追踪变得十分困难。

(2) 拒绝服务攻击频繁发生。入侵目标主机需要一定的技术和运气，因此很多攻击者选择了使用分布式拒绝服务的攻击方法(攻击者使用虚假的源地址，因此很难定位攻击者的位置)，严重干扰目标的网络服务。

(3) 攻击者需要的技术水平逐渐降低，但危害逐渐增大。由于在网络上很容易下载到攻击工具，而且一个新的操作系统漏洞被公布后，相应的攻击方法一般在两个月内就会被发布到互联网上。

(4) 攻击手段更加灵活，联合攻击急剧增多。网络蠕虫逐渐发展成为传统病毒、蠕虫和黑客攻击技术的结合体，不仅具有隐蔽性、传染性和破坏性，还具有不依赖于人为操作的自主攻击能力。新一代网络蠕虫的攻击能力更强，并且和黑客攻击、计算机病毒之间的界限越来越模糊，带来更为严重的多方面危害。

(5) 系统漏洞发现加快，攻击爆发时间变短。近年来，新的计算机系统安全漏洞不断被发现。据统计，2002 年新发现漏洞的数目比 2001 年增加了 82%。网络攻击者热衷于攻击新发现的漏洞，在所有新攻击方法中，64%的攻击针对一年之内发现的漏洞，最短的大规模攻击距相应漏洞被公布的时间仅为 28 天，以致于很多网络管理员还来不及给系统打补丁。

(6) 垃圾邮件问题严重。在垃圾邮件中不仅有毫无用处的信息，还有病毒和恶意代码。从传播的范围和速度来说，垃圾邮件是蠕虫病毒的“最佳搭档”。调查显示，蠕虫病毒制造的邮件已经占全球电子邮件通信量的 20%～30%，造成了严重的网络拥塞。

(7) 间谍软件、恶意软件威胁安全。间谍软件在用户不知情的情况下监控用户的网络连接，收集并发送有关用户访问的网址、IP 地址、用户计算机存储的信息。间谍软件一般隐藏在其他的应用软件中，用户在网上下载实用程序、游戏、媒体播放器和计费软件时，这些间谍软件就随之在用户的计算机留驻，收集、监控并发送有关用户计算机的信息。另外，广告软件、密码窃听程序、恶意脚本程序等有害软件，通过不同方式盗取用户的信息，威胁用户安全。

(8) 无线网络、移动手机渐成安全重灾区。在无线网络中被传输的信息没有加密或者加密很弱，很容易被窃取、修改和插入，存在较严重的安全漏洞。另外，手机病毒利用普通短信、彩信、上网浏览、下载软件与铃声等方式传播，还将攻击范围扩大到移动网关、WAP 服务器或其他的网络设备。

3. 网络容易袭击的原因

(1) 网络使用者过分“信任”网络。如最初设计网络时，只考虑防御从网络设施以外来的攻击力量(如攻击网络的有形线路或计算机)，而没考虑来自于网络内部的攻击(使用网络的人对网络进行的攻击)。

(2) 破坏程序简单易行。

(3) 追踪作案者困难，袭击者本身风险很小。袭击者运用“IP 伪装”技术伪造其身份及网络位置。另外，袭击者可跨越多个地理和法律区域，这也为追捕和审理工作增添了额外的司法困难。

1.1.2　网络安全的概念

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科学。网络安全是一个系统性概念，不仅包括网络信息的存储安全，还涉及信息的产生、传输和使用过程中的安全，应该说网络节点处的安全和通信链路上的安全共同构成了网络系统的安全体系。国际标准化组织(ISO)在ISO 7498-2 文献中指出："安全就是最大程度地减少数据和资源被攻击的可能性。"那么，什么是网络安全？

从狭义的角度来看，计算机网络安全是指计算机及其网络系统资源和信息资源不受自然和人为有害因素的威胁和危害，确保计算机和计算机网络系统的硬件、软件及其系统中的数据不因偶然的或者恶意的原因而遭到破坏、更改、泄露，保证系统能连续、可靠、正常地运行，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的信息安全。

从广义的角度来讲，凡是涉及到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，如场地环境保护、防火措施、静电防护、防水防潮措施、电源保护、空调设备、计算机辐射等。

1.1.3　网络安全面临的主要威胁

网络系统的安全威胁主要表现在主机可能会受到非法入侵者的攻击，网络中的敏感数据有可能泄露或被修改，从内部网向公共网传送的信息可能被他人窃听、篡改等。表 1-1 列出了典型的网络安全威胁类型。

表 1-1　典型的网络安全威胁

威　胁	描　　述
窃听	网络中传输的敏感信息被窃听
重传	攻击者事先获得部分或全部信息，以后将此信息发送给接收者
伪造	攻击者将伪造的信息发送给接收者
篡改	攻击者对合法用户之间的通信信息进行修改、删除、插入，再发送给接收者
非授权访问	通过假冒、身份攻击、系统漏洞等手段获取系统访问权，从而使非法用户进入网络系统读取、删除、修改、插入信息等
拒绝服务攻击	攻击者通过某种方法使系统响应减慢甚至瘫痪，阻止合法用户获得服务
行为否认	通信实体否认已经发生的行为
旁路控制	攻击者发掘系统的缺陷或安全脆弱性
电磁/射频截获	攻击者从电子或机电设备所发出的无线射频或其他电磁辐射中提取信息
人员疏忽	已授权人为了自己的利益或由于粗心将信息泄漏给未授权人

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。影响计算机网络安全的因素大体可分为两种：一是对网络中信息的威胁，二是对网络中设备的威胁。影响计算机网络安全的因素来自于多方面，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，还有可能是外来黑客对网络系统资源的非法使用。归结起来，网络安全面临的威胁主要有以下 4 个方面。

1. 网络硬件设备和线路的安全问题

Internet 的脆弱性，系统的易欺骗性和易被监控性，加上薄弱的认证环节以及局域网服务的缺陷和系统主机的复杂设置与控制，使得计算机网络容易遭受到威胁和攻击。

(1) 电磁泄露：网络端口、传输线路和处理机都有可能因屏蔽不严或未屏蔽而造成电磁泄露。目前，大多数机房屏蔽和防辐射措施都不健全，通信线路也同样容易出现信息泄露。

(2) 搭线窃听：随着信息传递量的不断增加，传递数据的密级也在不断提高，犯罪分子为了获取大量情报，可能会监听通信线路，非法接收信息。

(3) 非法终端：有可能在现有终端上并接一个终端，当合法用户从网上断开时，非法用户乘机接入，并操纵该计算机通信接口；或由于某种原因使信息传到非法终端。

(4) 非法入侵：非法分子通过技术渗透或利用电话线侵入网络，非法使用、破坏或获取数据或系统资源。目前的网络系统大都采用口令验证机制来防止非法访问，一旦口令被窃，就无安全可言。

(5) 注入非法信息：通过电话线有预谋地注入非法信息，截获所传信息，再删除原有信息或注入非法信息后再发出，使接收者接收到错误信息。

(6) 线路干扰：当公共转接载波设备陈旧或通信线路质量低劣时，会产生线路干扰。如调制解调器的错误会随着传输速率的上升迅速增加。

(7) 意外原因：包括人为地对网络设备进行破坏、设备偶然出现故障。如在处理非预期中断过程中，通信方式留在内存中，或未被保护的信息段在通信方式意外出错时被传到别的终端上。

(8) 病毒入侵：计算机病毒能以多种方式侵入计算机网络，并不断繁殖，然后扩散到网上的计算机来破坏系统。轻者使系统出错，重者可使整个系统瘫痪或崩溃。

(9) 黑客攻击：黑客采用种种手段，对网络及其计算机系统进行攻击，侵占系统资源或对网络和计算机设备进行破坏，窃取或破坏数据和信息。从攻击者与计算机系统的距离来划分，攻击可分超距攻击、远距攻击和近距攻击。超距攻击是利用互联网进行攻击，具有极大的隐蔽性，特别要警惕外国情报机关利用这种方式进行窃密和破坏；远距攻击是通过电话线进入网络，注册登录到国内某一主机，进行非法存取；近距攻击是同一单位的人利用合法身份越权存取数据或干扰其他用户使用。

2. 网络系统和软件的安全问题

(1) 网络软件的漏洞及缺陷被人利用，使网络遭到入侵和破坏。

(2) 网络软件功能不健全或被安装了“特洛伊木马”软件。

(3) 应加安全措施的软件可能未给予标识和保护；要害的程序可能没有安全措施，使软件非法使用，破坏或产生错误结果。