高职高专计算机精品课程系列规划教材

Securities and Solutions of Computer Networks

# 计算机网络安全技术与解决方案

主　编　周小华
副主编　廖伟国　陈　茜
翟懿奎　周平安

浙江大学出版社
ZHEJIANG UNIVERSITY PRESS

Technologies and Solutions of Computer Network Security

# 计算机网络安全技术与解决方案

高职高专计算机精品课程系列规划教材

# 计算机网络安全技术与解决方案

周小华　主　编

廖伟国　陈茜　翟懿奎　周平安　副主编

浙江大學出版社

图书在版编目（CIP）数据

计算机网络安全技术与解决方案／周小华主编.
—杭州：浙江大学出版社，2008.10
ISBN 978-7-308-06214-5

Ⅰ.计… Ⅱ.周… 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 154293 号

**计算机网络安全技术与解决方案**

周小华 主 编
廖伟国 陈茜 翟懿奎 周平安 副主编

策 划 希 言 冯 骏
责任编辑 陈晓嘉
文字编辑 冯 骏
封面设计 陈 辉
出版发行 浙江大学出版社
（杭州天目山路 148 号 邮政编码 310028）
（E-mail：zupress@mail.hz.zj.cn）
（网址：http://www.zjupress.com
http://www.press.zju.edu.cn）
电话：0571—88925592，88273066（传真）
排 版 杭州中大图文设计有限公司
印 刷 德清县第二印刷厂
开 本 787mm×1092mm 1/16
印 张 19.5
字 数 462 千
版 印 次 2008 年 10 月第 1 版 2008 年 10 月第 1 次印刷
书 号 ISBN 978-7-308-06214-5
定 价 28.00 元

# 高职高专计算机精品课程系列
# 规划教材专家指导委员会

# 序

高等职业教育作为高等教育发展中的一个类型，肩负着培养面向生产、建设、服务和管理第一线需要的高级职业技术型人才的使命，在我国加快推进社会主义现代化建设进程中具有不可替代的作用。经过数年的探索和实践，我国的高等职业教育已为现代化建设培养了一批高素质的技能型专门人才，对高等教育大众化作出了重要贡献；也丰富了高等教育体系结构，形成了高等职业教育的体系框架，顺应了国民经济各部门、企事业单位对应用型和技能型人才的不同需求。

精品课程是高等职业教育课程建设的重要组成部分，也是高等职业教育教学质量与教学改革的示范。浙江大学出版社在省级精品课程和国家“十一五”规划教材课程基础上组织出版的“高职高专计算机精品课程系列规划教材”，是由在高职高专教学第一线有丰富教学经验的教师编写的。整套教材从选题到内容的组织，都着力贯彻了实用性的原则；明确提出了与行业接轨，以就业为导向的编写要求；强调从计算机应用需求出发，构造适应技能型人才培养的教学内容体系，强调理论教学与实验实训密切结合，尤其突出实践体系与技术应用能力的实训环节。教材编写力求内容新颖、结构合理、概念清楚、实用性强，语言通俗易懂、前后相关课程有较好的衔接。据悉，浙江大学出版社还将在此基础上，陆续征集出版后续教材，力争在3到5年内完成一套完整的高职高专计算机专业教材，以满足高职院校计算机教育发展的需求。

本系列教材主要面向高职高专院校，同时也适用于同等学历的职业教育和继续教育。我们希望，通过本系列教材的编写和推广应用，对交流和提高高职院校计算机专业教学的整体水平，促进高等装业技术教育课程体系和教学培训方法的改革，完善高职高专精品课程建设带来新的活力。

温　涛

---

温涛　大连东软信息学院院长、教育部高等学校高职高专计算机类专业教学指导委员会主任

# 前　言

近年来，随着中国经济的发展，中国“世界工厂”地位的确立，社会对产业技术工人的需求量大大增加。职业技能教育就是在这样的环境下蓬勃发展的。高职高专教育以就业为导向，以技术应用型人才为培养目标，担负着为国家经济高速发展输送一线高素质技术应用人才的重任。但中国职业教育的发展受到传统教育模式的影响，职业教育质量不高，集中体现在：具有实践又具有理论的双师型教师缺乏；职业教育的教材还是以理论入主，缺乏实际应用和技术系统性。这些问题都制约着职业教育的发展。目前，我国接受过职业教育的人不少，但高级应用型人才紧缺，这就要求职业教育必须改革。

本书作者具有多年 IT 行业工程经验，具有 Microsoft、Cisco、3Com 工程师认证，并有多年职业技能教育经验。为了配合高职高专院校的学制改革和教材建设，华南农业大学珠江学院教学改革和教材建设，在信息工程系的指导下，组织了一批工作在高等职业教育第一线的资深教师和相关行业的优秀工程师，编写了适应新教学要求的计算机系列高职高专教材——《计算机网络安全技术与解决方案》。

《计算机网络安全技术与解决方案》主要面向高等职业教育，遵循“以就业为导向、懂理论精实践”的原则，根据企业的实际需求来进行课程体系设置和教材内容选取。根据教材所对应的专业，以实用为基础，理论上避免繁琐，实践上注重和提高案例教学的比重，突出培养人才的应用能力和实际问题解决能力，满足高等职业教育“学校评估”和“社会评估”的双重教学特征。

本教材的内容均由“理论”和“产品与方案”两个互为联系和支持的部分组成，“理论”部分介绍学生必须掌握或了解的基础知识。“产品与方案”用于强化学生的计算机应用能力和解决实际问题的能力。本书分两部共有 12 章，第一部分是安全技术介绍，包括 1 至 10 章，主要讲网络安全基础、加密、认证、访问控制、病毒、防火墙、IDS 等技术，技术全面简介。第二部分是完整的安全解决方案，包括第 12 章，案例准确典型。每章后面有配套的练习题和实验题，练习题重点在于培养学生运用理论思考、掌握基本理论知识，实验题重在培养学生独立自主完成和解决实际问题的能力。本书第 1 章至第 2 章由翟懿奎老师编写，第 3 至第 4 章由陈茜老师编写，第 5 章至第 6 章由周平安老师编写，第 7 章至第 12 章由周小华编写。

本书中提到的网络安全完整方案以及实验软件，可以到 http://www.2004edu.com 网站上下载。同时，本站对本书提供长期全面的技术运行，读者在使用过程中遇到了疑惑或困难，可以在本站上留言或者直接和本书的作者以及相应的技术人员联系（E-mail:

zhousir09288@163.com QQ：343367021，649003159）

本书可以作为职业院校本、专科教材，也可以作为普通本科院校和IT人员实践教材。由于本书编写时间仓促，难免有不正之处，请读者指正。

周小华

2008年7月于广州

# 目　录

第 1 章

# 网络安全概述

随着 Internet 技术的迅猛发展和网络社会化的到来，网络已经无所不在地影响着社会的政治、经济、文化、军事和社会生活等各个方面。同时，在全球范围内，针对重要信息资源和网络基础设施的入侵行为和企图入侵行为的数量在持续增加，这都对国家安全、经济发展和社会生活造成了极大的威胁。因此，网络安全已成为世界各国当今共同关注的焦点。网络安全就是为防范计算机网络硬件、软件、数据被偶然或蓄意破坏、篡改、窃听、假冒、泄露、非法访问和保护网络系统持续有效工作的措施总和。随着网络应用的普及，人们对网络的依赖与日俱增，确保信息安全和发展网络安全技术已经是全球范围内的难题和重点。

## 1.1 网络安全产生的原因

网络安全技术得以发展的很重要的原因是网络风险的存在、网络攻击技术的提升以及危害网络信息安全的手段、工具的增多。

### 1.1.1 网络自身的安全缺陷

#### 1. 软件漏洞

软件漏洞(flaw)是指在设计与编制软件时没有考虑对非正常输入进行处理或错误代码造成的安全隐患，也称为软件脆弱性(vulnerability)或软件隐错(bug)。软件漏洞产生的主要原因是软件设计人员不可能将所有输入都考虑周全，因此软件漏洞是任何软件都存在的客观事实。随着软件产业的发展，软件越来越复杂，软件的漏洞也越来越多，这就给黑客的入侵创造了条件(如图 1-1 所示)。软件产品在正式发布之前，一般都要相继发布多个版本供反复测试使用，目的就是为了尽可能减少软件漏洞。常见的漏洞有以下几种形式：

(1) 操作系统漏洞。操作系统是计算机上最主要的软件，没有操作系统作支撑，任何应用软件都无法使用，近几年操作系统的发展非常快，系统的漏洞也越来越多。如 Windows

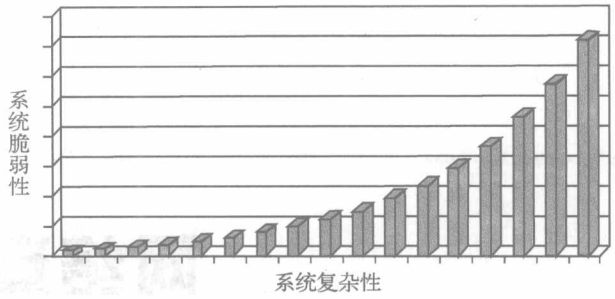


图 1-1 系统漏洞发展趋势

2000 Server 和 Windows Server 2003 上的 Active Directory 实施中的一个秘密报告的漏洞允许远程执行代码或拒绝服务，成功利用此漏洞的攻击者可以完全控制受影响的计算机；Windows Vista 防火墙允许信息泄露漏洞允许未经请求传入的网络流量访问网络接口，利用该漏洞攻击者可以潜在地收集有关受影响主机的信息；Linux Kernel 的 proc 文件系统中存在竞争条件错误，本地攻击者可利用此漏洞获取 root 用户权限。

(2) 数据库漏洞。数据库是系统软件的一种，随着其功能的壮大，漏洞也越来越多。如 IBM DB2 是一个大型的商业关系型数据库系统，其内容管理器在更新文本索引时存在拒绝服务漏洞，用户可以向文本搜索允许的项目类型中导入破坏的 Exel 文件，这样在 NSE 试图索引破坏的文件时，db2fmp 进程就会陷入循环，导致系统性能降低；Oracle 数据库服务器捆绑的 MDSYS.SDO_CS 软件包提供用于系统协作的子程序，该软件包中的 TRANSFORM 函数存在缓冲区溢出漏洞，如果远程攻击者向该函数提交了恶意请求的话，就可能触发这个溢出，导致拒绝服务或执行任意指令。

(3) 通讯协议漏洞。通讯协议是系统软件的一种，协议设计者在设计时由于测试不严格等原因也会留下漏洞。如 Microsoft Windows 的 TCP/IP 协议驱动处理特定畸形的 IP 源路由报文时存在缓冲区溢出漏洞，远程攻击者可以通过发送有“Loose Source and Record Route”选项的特制 ICMP 报文触发这个漏洞，导致 tcpip.sys 或 ntoskrnl.exe 中出现错误而造成拒绝服务或执行任意指令；FreeBSD TCP/IP 协议栈在处理特殊的带 SYN 标志的报文时存在漏洞，远程攻击者可以利用此漏洞影响已经建立的 TCP 连接，如果已创建了连接的计算机接收到设置了 SYN 标记的 TCP 报文的话，就可能延迟 TCP 连接，导致拒绝服务。

(4) 网络设备漏洞。网络设备是软件与硬件的结合，其软件上的漏洞也是难免的。如 3Com OfficeConnect Remote 812 ADSL 路由器的 Telnet 协议不能正确处理超长请求，远程攻击者可以利用这个漏洞对设备进行拒绝服务攻击，使设备挂起或重新启动，需要手工恢复才会正常工作；多个 Cisco 产品在处理 IPSec IKE 消息时存在漏洞，如果收到了特定的畸形报文的话，有漏洞的 Cisco 设备可能重置，导致临时的拒绝服务。

(5) 应用软件漏洞。通常，用户只关心操作系统的漏洞而忽视了应用程序的漏洞，但它又是黑客攻击的热点。如 Include 是编写 PHP 网站时最常用的函数，并且支持相对路径，有很多 PHP 脚本直接把某输入变量作为 Include 的参数，造成任意引用脚本或绝对路径泄露等漏洞；Windows 桌面应用程序处理通过 keybd_event() function 函数发送的键盘事件时存在溢出错误，攻击者可以通过向以更高权限运行的桌面应用程序(如 explorer.exe)发送恶意的键盘事件，使用管理员权限执行任意代码，这一漏洞可以使一个普通用户权限的账户使用

管理员权限对系统进行任意操作。

**2. 通讯过程和通讯技术开放性**

网络通讯双方在通讯时，通讯协议和通讯过程都是开放的，这对造成网络的安全威胁提供了可能，攻击者可以利用协议或者网络的漏洞来攻击网络或者采用 SNIFFER 等形式来窃取数据包。如 TCP/IP 协议中的 DoS 漏洞，黑客只需要下载一个发送 SYN 洪水攻击的软件(如 xflood)就可以对目标发起攻击，对于漏洞的防御的方法也是公开的，这些都为黑客的攻击提供了前提。所以，要保证通讯过程安全，可以采用加密技术和数据认证技术等。

### 1.1.2 黑客(HACKER)入侵

常见的黑客是指利用互联网的漏洞或系统的漏洞来入侵他人系统窃取数据或破坏系统的计算机高手，随着网络技术的发展，黑客入侵的手段也呈现出多样化，危害程度越来越高，检测难度也越来越大。在 2007 年的网络攻击事件中，脚本入侵比例为 47%，拒绝服务攻击比例为 26%，漏洞利用比例为 13%，暴力猜解比例为 8%，社会工程学比例为 5%，其他方法为 1%(如图 1-2 所示)。黑客入侵的目的大体为以下几种：

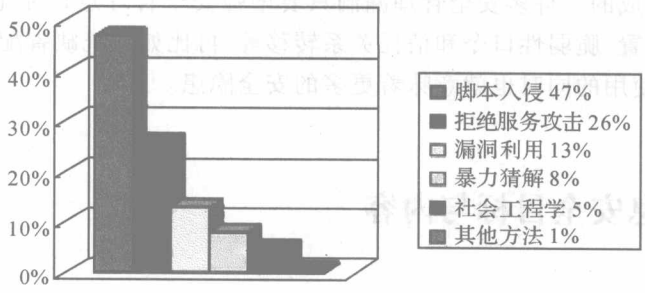


图 1-2 黑客入侵的手段多样化

- 基于政治和经济利益非法入侵：这种入侵一般都是为窃取国家机密信息、企业关键信息、商业机密，以获取政治、经济利益。
- 基于兴趣非法入侵：入侵者一般没有明确的利益目标，只是想证明自己的计算机应用能力，或者出于自己对技术的爱好进行的攻击，一般多为少年黑客。
- 信息战：随着国际政治形式的复杂化加深，国与国的关系越来越复杂，国家间的信息战也在升级，成为国家间接斗争的一种方式。

### 1.1.3 计算机病毒

计算机病毒也是计算机程序，有着生物病毒相似的特性：病毒驻留在受感染的计算机内，并不断传播和感染可连接的系统，在满足触发条件时发作，破坏正常的系统工作，强占系统资源，甚至损坏系统数据。病毒不但具有普通程序存储和运行的特点，还具有传染性、潜伏性、可触发性、破坏性、针对性、隐蔽性和衍生性等特征。随着计算机技术的发展，病毒的

危害由原来的以破坏主机系统为主，发展为破坏计算机网络资源为主，传播手段也发展为以网络传播为主，它是目前威胁网络安全的重要因素。

目前全世界流行的病毒共有20000余种，这个数量还正在以每月300～500种的速度向上飞速膨胀。据ICSA(International Computer Security Association，国际计算机安全协会)2007年对581458台桌面机和12122台应用/文件服务器进行抽样调查的结果显示，几乎所有计算机(大于99%)都有过被计算机病毒感染的经历。虽然有91%的服务器和98%的桌面机都使用了反病毒软件，但病毒感染、发作率是有增无减。同时，随着电子邮件系统的普及，通过Internet电子邮件传播的黑客程序和网络蠕虫等病毒越来越多。与以往主要靠软盘等交换方式传播的病毒相比，现在通过电子邮件传播的病毒(特别是宏病毒)种类越来越多、传播速度越来越快、传播空间大大延伸，呈现无国界的趋势。

### 1.1.4 管理漏洞

网络安全技术只是保证网络安全的基础，网络安全管理才是发挥网络安全技术的根本保证。因此，网络安全问题并不是一个纯技术问题，从网络安全管理角度看，网络安全首先应当是管理问题。目前，大多数网络攻击能够得逞是因为网络管理人员管理策略不严格和管理思想的大意造成的。许多安全管理漏洞只要增强安全管理意识完全可以避免，如改变常见的系统缺省配置、脆弱性口令和信任关系转移等，再比如系统缺省配置主要考虑的是用户友好性，但方便使用的同时也就意味着更多的安全隐患。

## 1.2 网络信息安全目标与内容

### 1.2.1 基本任务

正因为有网络风险威胁网络信息安全，所以才会有网络安全技术的产生与发展，网络安全技术从不同的方面保护计算机系统稳定可靠地运行和网络资源受控合法地使用。

### 1.2.2 网络安全目标

#### 1.保密性

保密性(confidentiality)是指信息系统防止信息非法泄露的特性，信息只限于授权用户使用，保密性主要通过信息加密、身份认证、访问控制、安全通信协议等技术实现，信息加密是防止信息非法泄露的最基本手段。