高职高专计算机技能型紧缺人才培养规划教材

计算机网络技术专业

网络安全技术与实训

杨文虎　樊静淳　主编

免费提供教学相关资料

人民邮电出版社
POSTS & TELECOM PRESS

高职高专计算机技能型紧缺人才培养规划教材
计算机网络技术专业

网络安全技术与实训

杨文虎　樊静淳　主　编

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全技术与实训/杨文虎，樊静淳主编. —北京：人民邮电出版社，2007.10
高职高专计算机技能型紧缺人才培养规划教材. 计算机网络技术专业
ISBN 978-7-115-16498-8

Ⅰ. 网… Ⅱ. ①杨…②樊… 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（2007）第 139628 号

内 容 提 要

本书首先围绕网络安全的定义、标准、模型以及常见的网络安全威胁进行系统介绍和分析，然后从网络管理与安全防护入手，详细讲述和分析入侵检测、数据加密、身份验证、防火墙以及无线网安全等多方面的理论与技术，同时结合现场工程应用，有机地将网络安全管理技术与主流系统软硬件结合，突出实践能力培养。本书安排了 13 个实训指导课题，从实用和现场的角度介绍企业网络安全管理与防护的应用。

本书适合作为高职高专院校计算机网络技术专业、信息安全技术专业、计算机应用技术专业等的教材，也可作为广大网络管理人员及技术人员学习网络安全知识的参考书。

高职高专计算机技能型紧缺人才培养规划教材
计算机网络技术专业
网络安全技术与实训

◆ 主　　编　杨文虎　樊静淳
责任编辑　赵慧君

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：13.5
字数：321 千字　　2007 年 10 月第 1 版
印数：1–3 000 册　　2007 年 10 月北京第 1 次印刷

ISBN 978-7-115-16498-8/TP

定价：20.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223

高职高专计算机技能型紧缺人才培养

规划教材编委会

丛书出版前言

目前，人才问题是制约我国软件产业发展的关键。为加大软件人才培养力度和提高软件人才培养质量，教育部继在2003年确定北京信息职业技术学院等35所高职院校试办示范性软件职业技术学院后，又同时根据《教育部等六部门关于实施职业院校制造业和现代服务业技能型紧缺人才培养培训工程的通知》（教职成［2003］5号）的要求，组织制定了《两年制高等职业教育计算机应用与软件技术专业领域技能型紧缺人才培养指导方案》。示范性软件职业技术学院与计算机应用与软件技术专业领域技能型紧缺人才培养工作，均要求在较短的时间内培养出符合企业需要、具有核心技能的软件技术人才，因此，对目前高等职业教育的办学模式和人才培养方案等做较大的改进和全新的探索已经成为学校的当务之急。

据此，我们认为做一套符合上述一系列要求的切合学校实际的教学方案尤为重要。遵照教育部提出的以就业为导向，高等职业教育从专业本位向职业岗位和就业为本转变的指导思想，根据目前高等职业教育院校日益重视学生将来的就业岗位，注重培养毕业生的职业能力的现状，我们联合北京信息职业技术学院等几十所高职院校和普拉内特计算机技术（北京）有限公司、福建星网锐捷网络有限公司、北京索浪计算机有限公司等软件企业共同组建了计算机应用与软件技术专业领域技能型紧缺人才培养教学方案研究小组（以下简称研究小组）。研究小组对承担计算机应用与软件技术专业领域技能型紧缺人才培养培训工作的79所院校的专业设置情况做了细致的调研，并调查了几十所高职院校计算机相关专业的学生就业情况以及目前软件企业的人才市场需求状况，确定首批开发目前在高职院校开设比较普遍的计算机软件技术、计算机网络技术、计算机多媒体技术和计算机应用技术4个专业方向的教学方案。

同时，为贯彻教育部提出的要与软件企业合作开展计算机应用与软件技术专业领域技能型紧缺人才培养培训工作的精神，使高等职业教育培养出的软件技术人才符合企业的需求，研究小组与许多软件企业的专家们进行了反复研讨，了解到目前高职院校的毕业生的实际动手能力和综合应用知识方面较弱，他们和企业需求的软件人才有着较大的差距，到企业后不能很快独当一面，企业需要投入一定的成本和时间进行项目培训。针对这种情况，研究小组在教学方案中增加了“综合项目实训”模块，以求强化学生的实际动手能力和综合应用前期所学知识的能力，探索将企业的岗前培训内容前移到学校的教学中的实验之路，以此增强毕业生的就业竞争力。

在上述工作的基础上，研究小组于2004年多次组织召开了包括企业专家、教育专家、学校任课教师在内的各种研讨会和方案论证会，对各个专业按照“岗位群→核心技能→知识点→课程设置→各课程应掌握的技能→各教材的内容”一步步进行了认真的分析和研讨：

- 列出各专业的岗位群及核心技能。针对教育部提出的以就业为导向，根据目前高职高专院校日益关心学生将来的就业岗位的现状，在前期大量调研的基础上，首先提炼各个专业的岗位群。如对某专业的岗位群进行研究时，首先罗列此专业的各个岗位，以便能正确了解

每个岗位的职业能力，再根据职业能力进行有意义的合并，形成各个专业的岗位群，再对每个岗位群总结和归纳出其核心技能。

- 根据岗位群及核心技能做出教学方案。在岗位群及核心技能明确的前提下，列出此岗位应该掌握的知识点，再依据这些知识点推出应该学习的课程、学时数、课程之间的联系、开课顺序并进行必要的整合，最终形成一套科学完整的教学方案。

为配合学校对技能型紧缺人才的培养工作，在研究小组开发上述 4 个专业的教学方案的基础上，我们组织编写了这套包含计算机软件技术、计算机网络技术、计算机多媒体技术及计算机应用技术 4 个专业的教材。本套教材具有以下特点：

- 注重专业整体策划的内涵。对各专业系列教材按照“岗位群→核心技能→知识点→课程设置→各课程应掌握的技能→各教材的内容”的思路组织开发教材。
- 按照“理论够用为度”的原则，对各个专业的基础课进行了按需重新整合。
- 各专业教材突出了实训的比例，注重案例教学。每本教材都配备了实验、实训的内容，部分专业的教材配备了综合项目实训，使学生通过模拟具体的软件开发项目了解软件企业的运行环境，体验软件的规范化、标准化、专业化和规模化的开发流程。

为了方便教学，我们免费为选用本套教材的老师提供部分专业的整体教学方案及教学相关资料。

- 所有教材的电子教案。
- 部分教材的习题答案。
- 部分教材中实例制作过程中用到的素材。
- 部分教材中实例的制作效果以及一些源程序代码。

本套教材以各个专业的岗位群为出发点，注重专业整体策划，试图通过对系列教材的整体构架，探索一条培养技能型紧缺人才的有效途径。

经过近两年的艰苦探索和工作，本套教材终于正式出版了，我们衷心希望，各位关心高等职业教育的读者能够对本套教材的不当之处给予批评指正，提出修改意见，也热切盼望从事高等职业教育的教师以及软件企业的技术专家和我们联系，共同探讨计算机应用与软件技术专业的教学方案和教材编写等相关问题。来信请发至 panchunyan@ptpress.com.cn。

编 者 的 话

人类已步入21世纪这一信息网络时代，计算机网络应用已日益普及。然而随着网络的不断发展，网络应用也日益复杂化，在不断满足人们对于信息的大量需求的同时，大量网络故障及网络病毒冲击着我们的网络与终端用户，计算机网络的安全性成为信息化建设的一个核心问题。

近年来，高等职业技术教育得到了飞速的发展，企业网络发展迅速，因此高职学院和企业技术人员均急需适合职业教育特点的结合实际应用的实用型教材，减少枯燥难懂的理论，取而代之的是设备应用、防护技术等实际操作应用能力的培养与训练。本书就是根据这种现状而编写的。

全书围绕网络涉及的安全问题，系统地讲述了常见的网络攻击、拒绝服务、网络病毒与木马等安全威胁以及所应采取的措施，同时着重介绍了网络防护的主要手段和设备应用。本书结合当前主流的网络防护技术，有机地将网络管理、安全防护、VPN应用、加密等技术与主流软硬件设备相结合，充分体现了理论与实践结合、教学与现场结合的特点，力求突出教材的系统性、先进性和实用性。

本书根据网络安全管理与防护的内容，共分为9章，同时设置13个实训指导课题。由杨文虎、樊静淳任主编，平寒、葛伟任副主编，杨文虎负责全书的构思及编写大纲，并编写第5章、第6章、第7章、第8章，樊静淳编写第1章、第2章，平寒编写第3章，葛伟编写第9章，刘志杰编写第4章，吴鹏编写实训1、3、13等实训内容。全书由杨文虎统稿、定稿。

编者收集整理了大量的资料，同时参考了很多优秀的教材和论文，结合自己的研究，撰写了本书。在此对本书中所引用的所有文献的作者表示衷心的感谢。

由于编者水平所限，书中难免存在错误和不妥之处，恳请读者提出宝贵意见，以便再版时及时修正。联系的E-mail地址是ywh_0001@163.com。

编 者

2007年7月

目　录

第 1 章

网络安全基础

本章学习要点

- 掌握网络安全的概念及安全模型
- 掌握安全服务及安全标准
- 了解我国计算机网络安全等级标准
- 掌握常见的安全威胁和攻击
- 了解网络安全的现状与发展趋势

1.1 引　　言

在社会日益信息化的今天，信息已成为一种重要的战略资源，信息的应用也从原来的军事、科技、文化和商业渗透到当今社会的各个领域，其在社会生产、生活中的作用日益显著。传播、共享和增值是信息的固有属性，与此同时，又要求信息的传播是可控的，共享是授权的，增值是确认的，因此信息的安全和可靠在任何状况下都是必须要保证的。

计算机网络是信息社会的基础，已经进入社会的各个角落。经济、文化、军事和社会生活越来越多地依赖计算机网络。然而，网络本身的开放性在给人们带来巨大便利的同时，也带来了一些不容忽视的问题，计算机网络的安全性成为信息化建设的一个核心问题。

许多在计算机网络中存储、传输和处理的信息是政府宏观调控决策、商业经济信息、银行资金转账、股票证券、科研数据等重要信息，其中很多是敏感信息甚至是国家机密。由于网络安全的漏洞，导致敏感信息泄露、信息篡改、数据破坏、恶意信息发布、计算机病毒发作等，由此造成的经济损失和社会不良影响难以估计。全世界计算机犯罪正以每年大于 100% 的速度增长，网络的黑客攻击事件也以每年 10 倍的速度递增。首例计算机病毒自 1988 年发现以来，计算机病毒种类的数量正在呈几何级数的速度增长。利用计算机实施金融犯罪已经渗透到了我国金融行业的各项业务。近几年已经掌握和破获 100 多起金融犯罪，涉及金额几个亿。据有关部门统计，国内 90%以上的电子商务网站存在着严重的安全漏洞，网络的安全问题正面临着日益严重的威胁。

1.2 网络安全概念

国际标准化组织（ISO）7498-2 安全体系结构文献定义了安全就是最小化资产和资源的漏洞。资产可以指任何事物。漏洞是指任何可以造成破坏系统或信息的弱点。

网络安全（Network Security）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。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，不受偶然的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。

从内容上看，网络安全大致包括以下 4 个方面的内容。

- 网络实体安全——如计算机硬件、附属设备及网络传输线路的安装及配置。
- 软件安全——如保护网络系统不被非法侵入，软件不被非法篡改，不受病毒侵害等。
- 数据安全——保护数据不被非法存取，确保其完整性、一致性、机密性等。
- 安全管理——运行时突发事件的安全处理等，包括采取计算机安全技术、建立安全制度、进行风险分析等。

从特征上看，网络安全包括 5 个基本要素。

- 机密性——确保信息不泄露给非授权的用户、实体。
- 完整性——信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。
- 可用性——得到授权的实体可获得服务，攻击者不能占用所有的资源而阻碍授权者的工作。
- 可控性——对信息的传播及内容具有控制能力。
- 可审查性——对出现的安全问题提供调查的依据和手段。

1.2.1 安全模型

通信双方想要传递某个信息，需建立一个逻辑上的信息通道。通信主体可以采取适当的安全机制，包括以下两个部分。

- 对被传送的信息进行与安全相关的转换，包括对消息的加密和认证。
- 两个通信主体共享不希望对手知道的秘密信息，如密钥等。

图 1.1 所示为网络安全的基本模型。

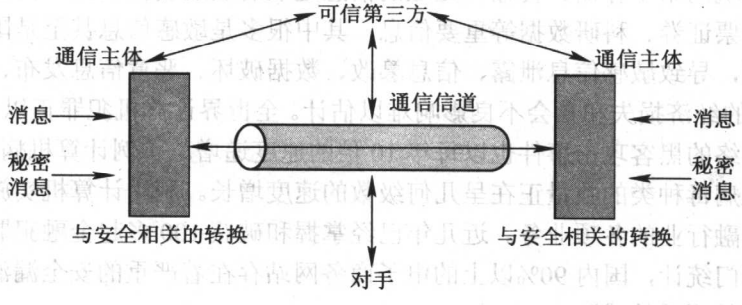

图 1.1 网络安全的基本模型

为了获得消息的安全传输，还需要一个可信的第三方，其作用是负责向通信双方分发秘密消息或者在通信双方有争议时进行仲裁。

并非所有的同安全相关的情形都可以用上述安全模型来描述。比如，目前万维网（WWW）的安全模型就应当另当别论。由于其通信方式大都采用客户服务器方式来实现，由客户端向

服务器发送信息请求，然后服务器对客户端进行身份认证，根据客户端的相应权限来为客户端提供特定的服务，因此，其安全模型可以采用如图 1.2 所示的安全模型来描述。其侧重点在于如何有效地保护客户端对服务器的安全访问，以及如何有效地保护服务器的安全性。

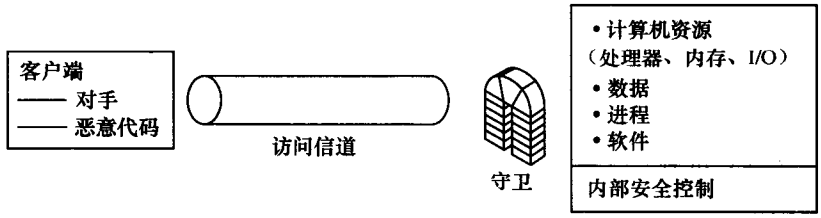

图 1.2　网络安全访问模型

这种安全模型同现实中的黑客入侵相吻合，客户端本身就可以是对手或者敌人，他可以利用大量的网络攻击技术来对服务器系统构成安全威胁，这些攻击可以利用网络服务的安全缺陷、通信协议的安全缺陷、应用程序或者网络设备本身的安全漏洞来实施。

为了有效地保护模型中信息系统的各种资源以及对付各种网络攻击，在模型中加入了守卫（Guard）功能。守卫可以有效地利用安全技术对信息流进行控制，如对客户端进行身份认证、对客户端对服务器的请求信息进行过滤、对服务器的资源进行监视审计等，从而可以抵御大部分的安全攻击。

1.2.2　安全体系

ISO（国际标准化组织）1989 年制定的 ISO/IEC 7498-2，给出了 ISO/OSI 参考模型的安全体系结构，在 OSI 参考模型中增设了安全服务、安全机制和安全管理，并给出了 OSI 网络层次、安全服务和安全机制之间的逻辑关系，定义了 5 大类安全服务，提供这些服务的 8 大类安全机制以及相应的与开放系统互联的安全管理。

1. 安全服务

针对网络系统受到的威胁，为了确保系统的安全保密性，ISO 安全体系结构定义了 5 种类型的安全服务，并在物理层、网络层、传输层和应用层上配置安全服务。

- 鉴别服务——它的目的在于保证信息的可靠性。实现身份认证的主要方法包括口令、数字证书、基于生物特征（比如指纹、声音等）的认证等。
- 访问控制服务——确定一个用户或服务可能用到什么样的系统资源，是查看还是改变。一旦一个用户通过认证，操作系统上的访问控制服务确定此用户将能做些什么。
- 数据完整性服务——指网络信息未经授权不能进行改变的特性，它要求保持信息的原样，即信息的正确生成、正确存储和正确传输。完整性与保密性不同，保密性要求信息不被泄漏给未授权的人，而完整性则要求信息不受到各种原因的破坏。
- 数据保密服务——指保护数据只被授权用户使用。根据发布信息的内容不同，可以使用几个不同的保护级别。保密性的另一方面是保护通信流，以防止被分析。数据保密性实现的手段包括物理加密、防窃听、防辐射、信息加密等。
- 抗抵赖性服务——指防止发送方或接收方否认消息的发送或接收。当消息发出时，接收方可以证实消息确实是从声明的发送方发出。与此类似，当接收到消息时，发送方也能证实消息确实由声明的接收方接收了。实现抗抵赖性的主要手段有数字签名等方法。

2. 安全机制

安全服务依赖于安全机制的支持。ISO 安全体系结构提出了 8 种基本的安全机制，将一个或多个安全机制配置在适当层次上以实现安全服务。

- 加密机制。
- 数字签名机制。
- 访问控制机制。
- 数据完整性机制。
- 认证（鉴别）机制。
- 通信业务填充机制。
- 路由选择控制机制。
- 公证机制。

我们知道，TCP/IP 刚出现时，协议设计者对网络安全方面考虑较少。随着因特网的快速发展，它的各种安全脆弱性逐步体现出来，但是又不能设计一种全新的协议来取代 TCP/IP，因此，相对于 ISO/OSI 的网络安全体系结构，因特网的安全体系结构有点类似于打补丁，它是在各个层次上加上相应的安全协议来进行处理的，如表 1.1 所示。

表 1.1　　因特网安全体系结构

层　次	安全协议
应用层	MOSS　PEM　PGP　S/MIME　SSH　SHTTP　Kerberos
传输层	TCP　SSL
网络层	UDP　IPv6　IPSec　ISAKMP

因特网各层与 ISO/OSI 安全服务的对应关系如表 1.2 所示。

表 1.2　　TCP/IP 各层与 ISO/OSI 安全服务的对应关系

层　次	安全协议	鉴　别	访问控制	机密性	完整性	抗抵赖性
网络层	IPSec	Y	–	Y	Y	–
传输层	SSL	Y	–	Y	Y	–
应用层	PEM	Y	–	Y	Y	–
	MOSS	Y	–	Y	Y	Y
	PGP	Y	–	Y	Y	Y
	S/MIME	Y	–	Y	Y	Y
	SHTTP	Y	–	Y	Y	Y
	SSH	Y	–	Y	Y	–
	Kerberos	Y	Y	Y	Y	Y
	SNMP	Y	–	Y	Y	–

注：Y=提供 -=不提供

1.2.3 安全标准

安全标准按照制定的组织和实施的国家不同存在多种标准，一般有 OSI 安全体系技术标准、可信任计算机标准评估准则（TCSEC）和我国的计算机网络安全等级标准。OSI 安全体系技术标准属于国际标准；可信任计算机标准评估准则是由美国制定的为实现对网络安全的

定性评价，该标准认为要使系统免受攻击，对应不同的安全级别，硬件、软件和存储的信息应实施不同的安全保护，而安全级别对不同类型的物理安全、用户身份验证、操作系统软件的可信任性和用户应用程序进行了安全描述。

TCSEC 将网络安全性等级划分为 A、B、C、D 这 4 类共 7 级，如表 1.3 所示，其中，A 类安全等级最高，D 类安全等级最低。

表 1.3　　TCSEC 安全等级

类　别	名　称	描　述	举　例
D1	最小保护	该标准规定整个系统都是不可信任的。对硬件来说，没有任何保护；操作系统容易受到损害；对存储在计算机上信息的访问权限没有身份认证	MS-DOS、MS-Windows 3.1、Macintosh System 7.X
C1	选择安全保护	确定每个用户对程序和信息拥有什么样的访问权限	早期的 UNIX 系统
C2	访问控制保护	进一步限制用户执行某些命令或访问某些文件的能力。这不仅基于许可权限，而且基于身份验证级别。另外，这种安全级别要求对系统加以审核	UNIX、XENIX、Novell 3.X 及 Windows NT
B1	标签安全保护	除 C2 的保护外，把用户隔离成各个单元以提高进一步保护	AT&T System V
B2	结构保护	要求计算机系统中所有对象都加标签，而且给设备分配单个或多个安全级别	XENIX、Honeywell MULTICS
B3	安全域级别	使用安装硬件的办法来加强域管理	Honeywell、Federal
A	验证设计	包含了一个严格的设计、控制和验证过程。与前面提到的各级别一样，这一级包含了较低级别的所有特性。其设计必须是从数学上经过验证的，而且必须进行对秘密通道和可信任分布的分析	Honeywell SCOMP

由公安部主持制定、国家质量技术监督局发布的中华人民共和国国家标准 GB17895-1999《计算机信息系统安全保护等级划分准则》已经正式颁布，并于 2001 年 1 月 1 日起实施。该准则将信息系统安全分为如下 5 个等级。

- 自主保护级。
- 系统审计保护级。
- 安全标记保护级。
- 结构化保护级。
- 访问验证保护级。

主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计、隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径和可信恢复等，这些指标涵盖了不同级别的安全要求。

1.2.4　安全目标

保障网络安全的基本目标就是要能够具备安全保护能力、隐患发现能力、应急反应能力和信息对抗能力。

- 安全保护能力——采取积极的防御措施，保护网络免受攻击、损害；具有容侵能力，使得网络在即使遭受入侵的情况下也能够提供安全、稳定、可靠的服务。
- 隐患发现能力——能够及时、准确、自动地发现各种安全隐患，特别是系统漏洞，并及时消除安全隐患。
- 应急反应能力——当出现网络崩溃或其他安全问题，能够以最短的时间、最小的代价