【内容简介】 本书是为高职高专计算机及相关专业编写的网络安全与管理课程的教材，全书系统全面地介绍了网络安全与管理方面的有关内容，主要包括网络安全概述、局域网的安全、因特网安全协议、防火墙技术、密码技术、入侵检测、病毒防护、网络安全管理协议和网络管理软件等内容。在每章的最后安排了实例解析，并在最后一章安排了实训内容，旨在使读者能够综合运用书中所讲授的知识进行网络安全与管理方面的实践。

本书既可作为高职高专院校的教材，也可供计算机网络技术及管理人员参考。

图书在版编目（CIP）数据

网络安全与管理/王建平主编．—西安：西北工业大学出版社，2008.4
高职高专“十一五”规划教材·计算机系列
ISBN 978-7-5612-2358-1

Ⅰ.网… Ⅱ.王… 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 025939 号

出版发行：西北工业大学出版社
通信地址：西安市友谊西路 127 号 邮编：710072
电 话：(029)88493844 88491757
网 址：www.nwpup.com
印 刷 者：陕西向阳印务有限公司
开 本：787 mm×1 092 mm 1/16
印 张：16
字 数：408 千字
版 次：2008 年 4 月第 1 版 2008 年 4 月第 1 次印刷
定 价：27.00 元

高职高专“十一五”规划教材·计算机系列

编审委员会

出版说明

高职高专教育作为我国高等教育的重要组成部分，承担着培养高素质技术、技能型人才的重任。近年来，在国家和社会的支持下，我国的高职高专教育取得了不小的成就，但随着我国经济的腾飞，高技能人才的缺乏越来越成为影响我国经济进一步快速健康发展的瓶颈。这一现状对于我国高职高专教育的改革和发展而言，既是挑战，更是机遇。

要加快高职高专教育改革和发展的步伐，就必须对课程体系和教学模式等问题进行探索。在这个过程中，教材的建设与改革无疑起着至关重要的基础性作用，高质量的教材是培养高素质人才的保证。高职高专教材作为体现高职高专教育特色的知识载体和教学的基本工具，直接关系到高职高专教育能否为社会培养并输送符合要求的高技能人才。

为促进高职高专教育的发展，加强教材建设，教育部在《关于全面提高高等职业教育教学质量的若干意见》中，提出了“重点建设好 3 000 种左右国家规划教材”的建议和要求，并对高职高专教材的修订提出了一定的标准。为了顺应当前我国高职高专教育的发展潮流，推动高职高专教材的建设，我们精心组织了一批具有丰富教学和科研经验的人员成立了高职高专“十一五”规划教材编审委员会。

编审委员会依据教育部高教司制定的《高职高专教育基础课程教学基本要求》和《高职高专教育专业人才培养目标及规格》，调研了百余所具有代表性的高等职业技术学院和高等专科学校，广泛而深入地了解了高职高专的专业和课程设置，系统地研究了课程的体系结构，同时充分汲取各院校在探索培养应用型人才方面取得的成功经验，并在教材出版的各个环节设置专业的审定人员进行严格审查，从而确保了整套教材“突出行业需求，突出职业的核心能力”的特色。

本套教材的编写遵循以下原则：

（1）成立教材编审委员会，由编审委员会进行教材的规划与评审。

（2）按照人才培养方案以及教学大纲的需要，严格遵循高职高专院校各学科的专业规范，同时最大程度地体现高职高专教育的特点及时代发展的要求。因此，本套教材非常注重培养学生的实践技能，力避传统教材“全而深”的教学模式，将“教、学、做”有机地融为一体，在教给学生知识的同时，强化了对学生实际操作能力的培养。

（3）教材的定位更加强调“以就业为导向”，因此也更为科学。教育部对我国的高职高专教育提出了“以应用为目的，以必需、够用为度”的原则。根据这一原则，本套教材在编写过程中，力求从实际应用的需要出发，尽量减少枯燥、实用性不强的理论灌输，充分体现出“以行业为向导，以能力为本，以学生为中心”的风格，从而使本套教材更具实用性和前瞻性，与就业市场结合也更为紧密。

（4）采用“以案例导入教学”的编写模式。本套教材力图突破陈旧的教育理念，在讲解的过程中，援引大量鲜明实用的案例进行分析，紧密结合实际，以达到编写实训教材的目标。这些精心设计的案例不但可以方便教师授课，同时又可以启发学生思考，加快对学生实践能力的

培养，改革人才的培养模式。

本套教材涵盖了公共基础课系列、计算机系列、财经管理系列和机电系列的主要课程。目前已经规划的教材系列名称如下：

公共基础课系列

- 公共基础课

机电系列

- 机械类
- 数控类
- 电子信息类

计算机系列

- 计算机公共基础课
- 计算机专业基础课
- 计算机网络技术专业
- 计算机软件技术专业
- 计算机应用技术专业

对于教材出版及使用过程中遇到的各种问题，欢迎您通过电子邮件及时与我们取得联系（联系方式详见“教师服务登记表”）。同时，我们希望有更多经验丰富的教师加入到我们的行列当中，编写出更多符合高职高专教学需要的高质量教材，为我国的高职高专教育做出积极的贡献。

高职高专“十一五”规划教材编审委员会

序

21 世纪是科技和经济高速发展的重要时期。随着我国经济的持续快速健康发展，各行各业对高技能专业型人才的需求量迅速增加，对人才素质的要求也越来越高。高职高专教育作为我国高等教育的重要组成部分，在加快培养高技能专业型人才方面发挥着重要的作用。

与国外相比，我国高职高专教育起步时间短，这种状况与我国经济发展对人才大量需求的现状是很不协调的。因此，必须加快高职高专教育的发展步伐，提高应用型人才的培养水平。

高职高专教育水平的提高，离不开课程体系的完善。相关领域人才的培养需要一批兼具前瞻性和实践性的优秀教材。教育部高教司针对高职高专教育人才培养模式提出了“以就业为导向”的指导思想，这也正是本套高职高专教材的编写宗旨和依据。

如何使高职高专教材既突出行业的需求特点，又突出职业的核心能力？这是教材编写的过程中必须首先解决的问题。本系列教材编委会深入研究了高职高专教育的课程和专业设置，并对以往的教材进行了详细分析和认真考察，力图在不破坏教材系统性的前提下，加强教材的创新和实践性内容，从而确保学生在学习专业知识的同时多动手，增强自己的实践能力，以加强“知”与“行”的结合。

同时，本系列教材在编写过程中还充分重视群体和类别的差异性，面对不同学校和不同专业方向的定位差异，精心设计了与其相配套的辅助实验指南及相关的习题解答等。通过这些栏目的设计，使本系列教材内容更加丰富，条理更为清晰，为老师的讲授和学生的学习都提供了很大的便利。

经过编委会的辛勤努力，本套教材终于顺利出版了，相信本套教材一定能够很好地适应现代高职高专教育的教学需求，也一定能够在高职高专教育计算机课程的改革中发挥积极的推动作用，为社会培养更多优秀的应用型人才。

全国计算机基础教育研究会副秘书长 

前　言

计算机网络的发展，特别是互联网的普及，使人们的学习、工作和生活方式发生了很大的变化，与计算机网络的联系也越来越密切。计算机网络系统提供了丰富的资源以便用户共享，提高了系统的灵活性和便捷性，但也正是这些特点，增加了网络系统的脆弱性、网络受威胁和攻击的可能性以及网络安全的复杂性。

网络安全是一门涉及计算机科学、通信技术、网络技术、密码技术、信息安全技术、数论、信息论等多种学科的综合性科学。从本质上来说，网络安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或恶意的影响而遭到破坏、更改、泄露，系统连续可靠地正常运行，网络服务不中断。从广义上来说，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领域。网络安全涉及的内容既有技术方面的问题又有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于防范外部非法用户的攻击，管理方面侧重于人为因素的管理。

本书以培养应用型和技能型人才为根本，通过认识、实践、总结和提高这样一个认知过程，精心组织内容，力求重点突出，要点讲明，难点讲透，通俗易懂。全书共分为 10 章，内容包括网络安全概述、局域网的安全、因特网安全协议、防火墙技术、密码技术、入侵检测、病毒防护、网络安全管理协议、网络管理软件和网络安全实训。

本书由王建平任主编，方贤进、李克东任副主编，全书由王建平定稿。

本书可作为高等专科院校、高等职业院校、成人高等学校以及应用型本科院校计算机及相关专业教材。通过对本书的学习可培养学生的实际动手能力，使学生更加适合用人单位的技能要求。

由于编者水平有限，书中不足之处在所难免，恳请读者批评指正。

编　者

目　　录

第 1 章　网络安全概述

本章要点

- ◆ 网络安全目标
- ◆ 网络安全模型
- ◆ 网络安全策略
- ◆ 网络安全类别
- ◆ 网络安全威胁
- ◆ 网络安全标准

网络安全是指保持网络中的软、硬件资源不受非法访问、获取、篡改、破坏而使用的计算机网络维护技术，它是保障网络稳定、正常运行的重要方面。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领域。由此看来，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。

1.1　网络安全组成

网络信息安全主要是指保护网络信息系统。下面从网络安全目标、网络安全模型和网络安全策略三个方面来了解网络安全的概念。

1.1.1　网络安全目标

网络安全的目标主要表现在系统的可靠性、可用性、保密性、完整性、不可抵赖性和可控性等方面。

1. 可靠性

可靠性是网络信息系统能够在规定条件下和规定时间内实现规定功能的特性。可靠性是系统安全的最基本要求之一，是所有网络信息系统的建设和运行目标。可靠性用于保证系统在人为或者随机性破坏下的安全程度。

2. 可用性

可用性是网络信息可被授权实体访问并按需求使用的特性。可用性是网络信息系统面向用户的安全性能。可用性应满足身份识别与确认、访问控制、业务流控制、路由选择控制、审计跟踪等要求。

3. 保密性

保密性是网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。也就是说，防止信息泄漏给非授权的个人或实体，信息只为授权用户使用。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，它是在可靠性和可用性的基础之上，保障网络信息安全的重要手段。

4. 完整性

完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、存储和传输。

5. 不可抵赖性

不可抵赖性也称作不可否认性，在网络信息系统的信息交互过程中，确信参与者的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据防止发信方不真实地否认已发送信息，利用递交接收证据防止收信方事后否认已经接收的信息。

6. 可控性

可控性是对网络信息的传播及内容具有控制能力的特性。保障系统依据授权提供服务，使系统在任何时候都不被非授权人使用，对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等采取防范措施。

思考：对网络用户的操作事件进行记录，属于网络安全目标的哪个方面？

1.1.2 网络安全模型

网络安全模型是动态网络安全过程的抽象描述。通过对安全模型的研究，了解安全动态过程的构成因素，是构建合理而实用的安全策略体系的前提之一。为了达到安全防范的目标，须要建立合理的网络安全模型，以指导网络安全工作的部署和管理。目前，在网络安全领域存在较多的网络安全模型，下面介绍常见的 PDRR 模型和 PPDR 模型。

1. PDRR 安全模型

PDRR 是美国国防部提出的常见安全模型。它概括了网络安全的整个环节，即防护(Protection)、检测(Detection)、响应(Reaction)、恢复(Restore)。这 4 个部分构成了一个动态的信息安全周期，如图 1-1 所示。

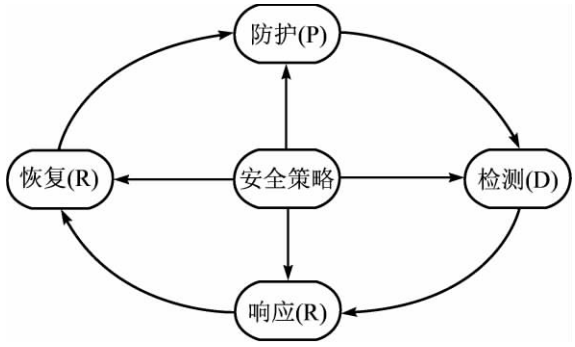

图 1-1 PDRR 安全模型

(1)防护。防护是 PDRR 模型最重要的部分。防护是预先阻止攻击可能发生的条件产生，让攻击者无法顺利地入侵。防护可以抵御大多数的入侵事件，它包括缺陷扫描、访问控制及防火墙、数据加密、鉴别等。

(2)检测。检测是 PDRR 模型的第二个环节。通常采用入侵检测系统(IDS)来检测系统漏洞和缺陷，增加系统的安全性能，从而消除攻击和入侵的条件。检测根据入侵事件的特征进行。

(3)响应。响应是 PDRR 模型的第三个环节。响应就是已知一个入侵事件发生之后进行的处理过程。通过针对入侵事件的警报进行响应通告,从而采取一定的措施来实现安全系统的补救过程。

(4)恢复。恢复是 PDRR 模型中的最后一个环节。恢复是指事件发生后进行初始化恢复的过程。通常,用户通过系统的备份和还原来进行恢复,然后安装系统对应的补丁程序,实现安全漏洞的修复等。

2. PPDR 安全模型

PPDR 是美国国际互联网安全系统公司(ISS)提出的可适应网络安全模型,它包括策略(Policy)、保护(Protection)、检测(Detection)、响应(Response)4 个部分。PPDR 模型如图 1-2所示。

(1)策略。PPDR 安全模型的核心是安全策略,所有的防护、检测、响应都是依据安全策略实施的,安全策略为安全管理提供管理方向和支持手段。策略体系的建立包括安全策略的制定、评估、执行等。

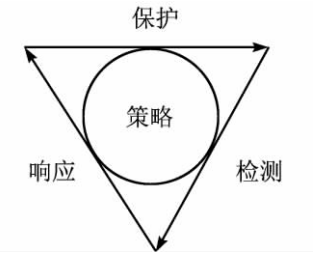

图 1-2　PPDR 安全模型

(2)保护。保护就是采用一切手段保护信息系统的保密性、完整性、可用性、可控性和不可抵赖性,应该依据不同等级的系统安全要求来完善系统的安全功能、安全机制。保护通常采用身份认证、防火墙、客户端软件、加密等传统的安全技术来实现。

(3)检测。检测是 PPDR 模型中非常重要的环节,检测是进行动态响应和动态保护的依据,同时强制网络落实安全策略,检测设备不间断地检测、监控网络和系统,及时发现网络中的威胁和存在的弱点,通过循环的反馈来及时做出响应。网络的安全风险是无时不在的,检测的对象主要针对系统自身的脆弱性及外部威胁。

(4)响应。响应是指在系统检测到安全漏洞后做出的处理方法,它在 PPDR 安全系统中占有重要的位置,是解决潜在安全问题最有效的方法。

思考:PDRR 模型和 PPDR 模型的核心是否相同?

1.1.3　网络安全策略

1. 安全层次设计

网络安全策略主要考虑安全对象和安全机制,安全对象主要有网络安全、系统安全、数据库安全、信息安全、设备安全、信息介质安全和计算机病毒防治等。网络安全贯穿于整个 OSI 网络模型。针对 TCP/IP 协议,网络安全应贯穿于信息系统的 4 个层次。图 1-3 所示的为网络安全体系层次模型。

(1)物理层。物理层是面向硬件的层次,它的作用是提供原始比特流的传输。物理层信息安全主要是防止物理通路的损坏、窃听、干扰等。

(2)数据链路层。数据链路层的主要作用是组织数据链路,在该层实现差错控制和流量控制。运行在该层的安全措施有编码、加密、虚拟局域网等技术。

(3)网络层。网络层的主要作用是根据 IP 地址进行路由选择。在本层中,需要通过认证头等方式提供授权服务,通过安全的路由协议保证路由的强壮性。

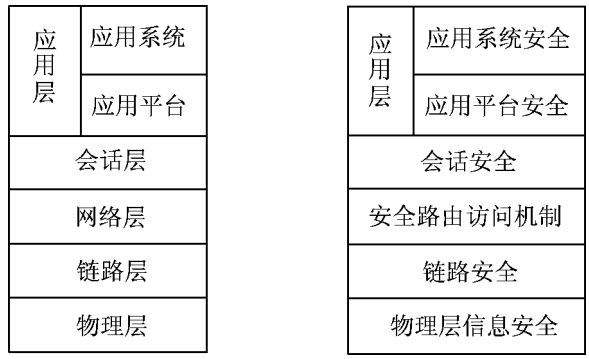

图 1-3 安全体系层次模型

(4)会话层。会话层保证系统会话的正常进行,在系统的操作中通常采用会话原语来实现。原语指的是不可分割的操作序列,它本身不可中断,要么全做,要么不做,这就是其原子性。会话层通过对会话原语的维持来保证会话安全。

(5)应用层。应用层是面向系统用户的高层,所有的服务都在该层体现,在应用层的服务中,最基本的是应用平台的安全性,即操作系统安全,在此基础上实现的是应用系统的安全。对于各种不同的应用系统,其脆弱性各不相同。在 TCP/IP 体系结构中,服务系统分为基于 TCP 的可靠服务系统和基于 UDP 的不可靠服务系统。对应在应用层,就出现面向连接的认证服务和面向无连接的非认证服务,所以应用层的安全特征必须由不同的服务类型而定。

思考:对网络进行安全路由设置,属于安全体系结构的哪个层次?

2. 安全设计原则

在进行计算机网络安全设计、规划时,应遵循以下原则:

(1)需求、风险、代价平衡分析的原则。它指的是保护成本与被保护信息的价值必须平衡,如果保护成本高于被保护信息的价值,这种保护策略就是失败的,是不可取的。

(2)综合性、整体性原则。它指的是运用系统工程的观点、方法来分析网络的安全问题,并制定具体措施。

(3)一致性原则。这主要是指网络安全问题应与整个网络的工作周期(或生命周期)同时存在,制定的安全体系结构必须与网络的安全需求相一致。

(4)易操作性原则。要求安全系统容易被掌握和使用,这样在操作安全性和维护成本上都有了保证。

(5)适应性、灵活性原则。安全措施必须具有动态的自适应性,能随着网络性能及安全需求的变化而变化。实际上这一条是比较难做到的,任何网络安全措施都不可能保证网络 100%的可靠,所以网络的自适应性安全措施是目前网络安全研究的重要课题。

1.2 网络安全类别

1.2.1 物理安全

物理安全指网络系统中相关设备的物理保护,以免于破坏、丢失等。通常的物理网络安全

措施是使用物理隔离设备，物理隔离设备的作用是使网络之间无连接的物理途径，这样，内网的信息就不可能外泄。

在确保网络物理安全的措施中，目前比较流行的是采用物理隔离卡。物理隔离卡使用双硬盘物理隔离技术，隔离器与主板之间无数据交换途径，真正实现了网络隔离和数据隔离。内网和外网的切换通过手动物理开关来实现，且只能由用户自己操作，任何通过网络或运行软件的操作方法都无效，不存在软件操作隐患。

另外，在网络管理中建立一套严格的安全制度非常必要，如做好防盗、防火措施。在非常机密的网络环境下做好网络信息的屏蔽工作也非常必要，例如在无线网络环境中，为防止信息的窃取，在网络中安装屏蔽层等。

1.2.2　逻辑安全

逻辑安全指的是通过软操作方式来实现网络安全的措施，通常指的是用户通过安装杀毒软件、系统补丁，关闭服务、端口，加密等多种方式实现网络安全的过程。逻辑安全包括信息保密性、完整性和可用性。保密性是指信息不泄漏给未经授权的人；完整性是指计算机系统能够防止非法修改或删除数据、程序；可用性是指系统能够防止非法独占计算机资源和数据，合法用户的正常请求能及时、正确、安全地得到服务或回应。

1.2.3　操作系统安全

在网络服务中，网络操作系统起着非常重要的组织作用，所以操作系统的安全关系到网络的整体性能。每一种网络操作系统都采用了一些安全策略，并使用了一些常用的安全技术，但是目前很难找到一款安全的网络操作系统。就微软公司的 Windows NT 系列操作系统而言，关注系统的漏洞，升级系统文件，为系统安装补丁程序是非常必要的。

由于 TCP/IP 协议本身的不安全因素，导致网络安全防不胜防。对操作系统安全而言，应该注意以下几个方面：

(1)为操作系统选择一款优秀的杀毒软件和防火墙系统。

(2)设置操作系统管理员账号和密码，并且要保证密码足够“强壮”。

(3)对系统进行分角色管理，严格控制系统用户。

(4)定期进行系统扫描，及时安装系统补丁程序。

(5)对系统进行备份，定期进行磁盘扫描，检测系统是否出现异常。

(6)可以在系统上安装外壳软件或蜜罐系统进行反跟踪。

1.2.4　连网安全

网络按照其工作方式划分为两级体系结构，即把由发送端和接收端组织的网络称为资源子网，把由中间的链路机构成的网络称为通信子网，所以连网的安全性就体现在内部网络安全和外部网络安全两个方面。

内部网络的安全性表现在不向外部网络发送非安全数据，如病毒等，对来自外部网络的攻击有一定的防御能力，保护连网资源不被非授权使用。外部网络安全指的是通过数字加密等方式认证数据机密性与完整性，保证数据通信的可靠性。