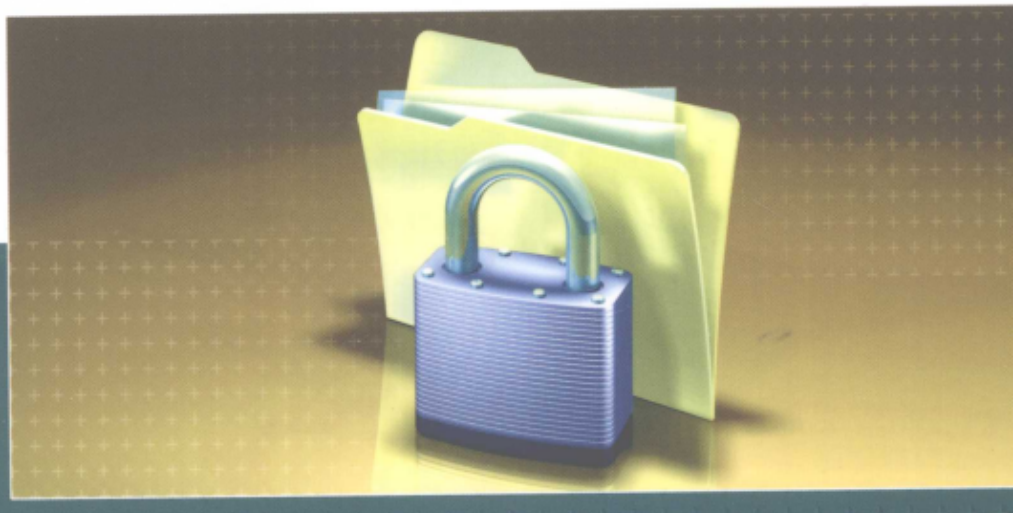
高职高专院校实践类系列规划教材

信息安全技术

Information Security Technology

周 苏 黄林国 王 文 编著



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

高职高专院校实践类系列规划教材

- 操作系统
- 数据结构
- 汇编语言程序设计
- 软件工程
- IT项目管理
- 多媒体技术
- 人机界面设计
- 信息安全技术
- 网络管理技术
- 电子商务概论
- 网页设计与网站建设
- Web程序设计
- 网站开发技术

责任编辑：翟玉峰　**封面设计**：付　巍　**封面制作**：白　雪

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

中国铁道出版社 计算机图书批销部
地址：北京市宣武区右安门西街8号
邮编：100054

网址：http://edu.tqbooks.net
读者热线电话：(010) 63583215
销售服务电话：(010) 83550290/91　83550580

ISBN 978-7-113-10236-4/TP·3406　定价：24.00 元

ISBN 978-7-113-10236-4
9 787113 102364 >

高职高专院校实践类系列规划教材

信息安全技术

周　苏　黄林国　王　文　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书是为高等职业院校和高等专科学校相关专业“信息安全技术”课程编写的以实训为主线开展教学的教材。全书通过一系列在网络环境下学习和实践的实训练习，把信息安全技术的概念、理论知识与技术融入到实践当中，从而加深对该课程的认识和理解。教学内容和实训练习包含了信息安全技术知识的各个方面，涉及熟悉信息安全技术、数据备份技术、加密与认证技术、防火墙与网络隔离技术、安全检测技术、访问控制与审计技术、病毒防范技术、虚拟专用网络技术以及信息安全管理与灾难恢复等，全书包括可供选择的20个实训和1个课程实训总结。

本书适合作为高职高专院校计算机相关专业的教材，也可作为培训教材或自学的参考书。

图书在版编目（CIP）数据

信息安全技术/周苏，黄林国，王文编著. —北京：中国铁道出版社，2009.6
（高职高专院校实践类系列规划教材）
ISBN 978-7-113-10236-4

Ⅰ.信… Ⅱ.①周…②黄…③王… Ⅲ.信息系统－安全技术－高等学校：技术学校－教材 Ⅳ.TP309

中国版本图书馆CIP数据核字（2009）第109329号

书　　名：信息安全技术
作　　者：周　苏　黄林国　王　文　编著

策划编辑：翟玉峰　王春霞
责任编辑：翟玉峰　　**编辑部电话：**（010）63583215
编辑助理：陈　文
封面设计：付　巍　　**封面制作：白　雪**
版式设计：郑少云　　**责任印制：李　佳**

出版发行：中国铁道出版社（北京市宣武区右安门西街8号　　邮政编码：100054）
印　　刷：北京市彩桥印刷有限责任公司
版　　次：2009年8月第1版　　2009年8月第1次印刷
开　　本：787mm×1092mm　1/16　**印张：**15.25　**字数：**383千
印　　数：4 000册
书　　号：ISBN 978-7-113-10236-4/TP・3406
定　　价：24.00元

FOREWORD

前言

在长期的教学实践中，我们体会到，“因材施教”是教育教学的重要原则之一，把实训实践环节与理论教学相融合，抓实训实践教学促进学科理论知识的学习，是有效地提高高职高专相关专业教学效果和教学水平的重要方法之一。随着教改研究的不断深入，我们已经逐渐发展了一系列以实训实践方法为主体开展教学活动的，具有鲜明特色的课程主教材，相关的数十篇教改研究论文也赢得了普遍的好评，并多次获得教学优秀成果奖。这套“高职高专院校实践类系列规划教材”所涉及的内容包括操作系统原理、汇编语言程序设计、数据结构与算法、数据库技术、软件工程、项目管理、网页设计与网站建设、多媒体技术、信息安全技术、人机界面设计、数字艺术设计、艺术欣赏概论、信息资源管理、电子商务概论、管理信息系统、网络管理技术和面向对象程序设计等课程。

本丛书的编写原则是：依据课程教学大纲，充分学习和理解课程的大多数主教材和教学成果，遵循课程教学的规律和节奏，充分体现实训实践的可操作性，既可以与课程的其他教材辅助配套，也可以作为具有应用和实践特色的课程主教材，还可以是自学的实践教材。本书旨在很好地推动本课程的教学发展，辅助老师教，帮助学生学，帮助用户切实把握本课程的知识内涵和理论与实践的水平。

本书是为高职高专院校相关专业“信息安全技术”(计算机信息安全)课程开发的具有实践特色的新型教材，通过一系列在网络环境下学习和熟悉信息安全技术知识的实训练习，把信息安全技术的概念、理论知识与技术融入到实践当中，从而加深对信息安全技术知识的认识和理解。

每个实训均设有“实训总结”和“实训评价”部分；全部实训完成之后的实训总结部分还设计了“课程学习能力测评”等内容。希望以此方便师生进行交流，对学科知识、实训内容的理解与体会，以及对学生学习情况进行必要的评估。

本书的编著得到了浙江大学城市学院、台州科技职业学院、浙江商业职业技术学院等多所院校师生的支持，在此一并表示感谢！本书中的实训素材可以从中国铁道出版社网站(http://edu.tqbooks.net)的下载区下载。欢迎教师索取为本书教学配套的相关资料并与我们进行交流。E-mail：zs@mail.hz.zj.cn；QQ：81505050；教学网站：www.zhousu.net；博客http://blog.sina.com.cn /zhousu58。

编　者

2009年仲夏于西子湖畔

GUIDE

读者指南

本书是为高等职业院校和高等专科院校相关专业“信息安全技术”课程编写的应用型、实践型教材，目的是通过一系列在网络环境下学习和实践的实训练习，把信息安全技术的概念、理论知识与技术融入到实践当中，从而加深对该课程的认识和理解。

读者对象

高职高专院校相关专业的学生可以把此书作为课程学习的主教材、实训辅助教材或自学读物。教学实践证明，在主要强调实践性、应用性的相关课程中，本书是一本实用和优良的课程主教材。对于已经具备计算机应用基础知识，并希望通过进一步学习得到提高的读者来说，本书也是一本继续教育的良好读物。本书将有助于“信息安全技术”课程的教与学，有助于读者理解、掌握和应用本课程内容，并建立起足够的信心和兴趣。

实训内容

本书的教学内容和实训练习包含了信息安全技术知识的各个方面，包括可供选择的 20 个实训、1 个课程实训总结，可帮助读者加深对教材中所介绍概念的理解，掌握主流工具的基本使用方法等。

第 1 章：熟悉信息安全技术。包括信息安全技术的计算环境、信息系统的物理安全以及 Windows 系统管理与安全设置等方面。通过学习和实训，了解信息安全技术的基本概念和基本内容。通过对因特网进行的专题搜索与浏览，了解网络环境中主流的信息安全技术网站，掌握通过专业网站不断丰富信息安全技术最新知识的学习方法，尝试通过专业网站的辅助与支持来开展信息安全技术应用实践；熟悉物理安全技术的基本概念和基本内容；通过学习使用 Windows 系统管理工具，熟悉 Windows 系统工具的内容，由此进一步熟悉 Windows 操作系统的应用环境。通过使用和设置 Windows XP 的安全机制，回顾和加深了解现代操作系统的安全机制，熟悉 Windows 网络安全特性和 Windows 提供的安全措施。

第 2 章：数据备份技术。包括优化 Windows XP 磁盘子系统和数据存储解决方案等方面。通过学习和实训，熟悉 Windows XP 的 NTFS 文件系统，掌握优化 Windows XP 磁盘子系统的基本方法和理解现代操作系统的文件和磁盘管理知识；熟悉数据备份技术的基本概念和基本内容。通过案例分析深入领会备份的真正含义及其意义，通过案例了解备份技术的学习和获取途径。

第 3 章：加密与认证技术。包括加密技术与 DES 加解密算法、电子邮件加密软件 PGP 和认证技术、个人数字证书。通过学习和实训，了解《电子签名法》及其关于电子认证服务的相关规定，熟悉数字认证的基本原理和作用，掌握数字认证的申请和使用过程，熟悉加密技术的基本概念和基本内容，熟悉认证技术的基本概念和基本内容；掌握 PGP 和 MiniPGP 软件的使用来实现对邮件、文件等的加密与传输，掌握 PGP 的基本功能。

第 4 章：防火墙与网络隔离技术。包括防火墙技术及 Windows 防火墙配置和网络隔离技术与网闸应用等方面。通过学习和实训，熟悉防火墙技术的基本概念和基本内容，掌握通过专业网站不断丰富防火墙技术最新知识的学习方法，并在 Windows XP 中学习配置简易防火墙（IP 筛选器）的操作；熟悉网络隔离技术的基本概念、工作原理和基本内容，熟悉隔离网闸的基本概念和工作原理，了解网闸产品及其应用。

第 5 章：安全检测技术。包括入侵检测技术与网络入侵检测系统产品、漏洞检测技术和微软系统漏洞检测工具 MBSA 等方面。通过学习和实训，了解入侵检测技术的基本概念和基本内容；了解漏洞检测技术的基本概念和基本内容，学习在 Windows 环境中安装和使用 MBSA 软件。

第 6 章：访问控制与审计技术。包括访问控制技术与 Windows 访问控制和审计追踪技术与 Windows 安全审计功能等方面。通过学习和实训，熟悉访问控制技术的基本概念、工作原理和基本内容，学习配置安全的 Windows 操作系统，掌握 Windows 的访问控制功能；熟悉安全审计技术的基本概念和基本内容，通过应用 Windows 的审计追踪功能，加深理解安全审计技术。

第 7 章：病毒防范技术。包括病毒防范技术与杀病毒软件和解析计算机蠕虫病毒、反垃圾邮件技术等方面。通过学习和实训，熟悉计算机病毒防范技术的基本概念，掌握计算机蠕虫病毒的查杀和防范措施，尝试通过专业网站的辅助与支持来开展计算机病毒防范技术的应用实践；了解反垃圾邮件技术的概念、原理及其基本内容。

第 8 章：虚拟专用网络技术。通过学习和实训，熟悉虚拟专用网络技术的基本概念和基本内容，尝试通过专业网站的辅助与支持来开展 VPN 技术应用实践。

第 9 章：信息安全管理与灾难恢复。包括信息安全管理与工程和信息灾难恢复规划等方面。通过学习和实训，熟悉信息安全管理的基本概念和内容，通过学习某金融单位的“计算机安全管理规定”，提高对信息安全管理工作的认识，理解信息安全管理工作的方法；熟悉数据容灾技术和信息灾难及其恢复计划的概念、内容及其意义；通过案例更好地理解灾难恢复规划的概念。

实训要求

尽管全部实训有 20 个，但并不一定都要完成。教师可以根据不同的教学安排和要求，实际情况、条件以及需要，从中选取部分实训必须完成，部分实训作为作业完成等。个别实训可能也需要占用课后时间才能全部完成。

致教师

现有的“信息安全技术”教材大都有理论性很强，而实践与应用性偏弱的特点，对教学活动的开展，尤其是对强调教学型、应用型的高等院校相关课程教学的开展带来了一定的困难。但是，信息安全技术活动本身却具有鲜明的应用性，因此我们应该充分重视这门课程的实训环节，以实训与实践教学来促进理论知识的学习。本书以一系列与网络学习密切相关的实训练习作为主线，来组织对信息安全技术课程的教学，以求掌握信息安全技术知识在实践中的应用。

为方便教师对课程实训环节的组织，我们在实训内容的选择、实训步骤的设计和实训文档的组织等诸方面都做了精心的考虑和安排。任课教师不需要作为专家来自己设计练习，相反，教师和学生都可以通过本书提供的实训练习来研究概念的实现。

本书的全部实训，都经过了教学实践的检验，取得了良好的教学效果。根据经验，虽然大部分实训确实能够在一次实训课的时间内完成，但学生普遍存在着两个方面的问题：

① 常常会忽视对教学内容的阅读和理解，而急功近利，只求完成实训步骤。

② 在实训步骤完成之后，没有投入时间对实训内容进行消化，从而不能很好地进行相关的实训总结。

因此，为了保证实训的质量，建议教师重视对教学实践环节的组织，例如：

① 在实训之前要求学生对教学和实训内容进行预习。实训指导老师在实训开始时应该对学生的预习情况进行检查，并计入实训成绩。

② 明确要求学生重视对实训内容的理解和体会，认真完成“实训总结”、“单元学习评价”等环节，并把这些内容作为实训成绩的主要评价成分，以激励学生对所学知识进行积极和深度的思考。

③ 考虑到多数学校教学和实训环境的实际情况，本书所设计的实训主要以单机方式进行，一般不考虑服务器环境。对于有条件的学校，建议可以在信息安全技术的服务器应用方面再设计一些可行的实训练习项目。

如果需要，教师还可以在现有实训的基础上，在应用实践方面做出一些要求、指导和布置，以进一步发挥学生的潜能和激发学习的主动性和积极性。

每个实训均留有“实训总结”和“实训评价”部分；每个单元设计了“单元学习评价”；全部实训完成之后的实训总结部分还设计了“课程学习能力测评”等内容。希望以此方便师生交流对学科知识、实训内容的理解与体会，以及对学生学习情况进行必要的评估。如果有更多需要，请任课老师加以补充。

关于实训的评分标准

合适的评分标准有助于促进实训的有效完成。在实践中，我们摸索出了如下评分安排，即对于每个实训以 5 分计算，其中阅读教学内容（要求学生用彩笔标注，留下阅读记号）占 1 分，完成全部实训步骤占 2 分（完成了但质量不高则只给 1 分），认真撰写“实训总结”占 2 分（写了但质量不高则只给 1 分）。以此强调对课文的阅读和强调通过撰写“实训总结”来强化实训效果。

致学生

对于 IT 及其相关专业的学生来说，信息安全技术肯定是需要掌握的重要知识之一。但是，单凭课堂教学和一般作业，要真正领会信息安全技术课程所介绍的概念、原理、方法和技巧等，是很困难的。而经验表明，学习尤其是真正体会和掌握信息安全技术知识的最好方式是理论联系实际，进行充分的应用实践。

本书为读者提供了一个研究信息安全技术知识的学习方法，因此可以由此来学习和体验信息安全技术的知识及其应用。

下面两点对于提高读者的实训效果非常重要：

(1) 在开始每一个实训之前，请务必预习各章的教学内容，其中包含本课程知识的主体，也和实训内容有着密切的联系。

(2) 实训完成后，请认真撰写“实训总结”，认真撰写每个单元的“单元学习评价”和最后的课程实训总结，完成“课程学习能力测评”等内容，把感受、认识和意见建议等表达出来，这能起到“画龙点睛”的作用，也可以此和老师进行积极的交流，以及对自己的学习情况进行必要的评估。

另一方面，可能仅靠书本所提供的实训还不够。如果需要，可以在这些实训的基础上，结合应用项目，来进一步实践信息安全技术知识，以发挥自己的潜能和激发学习的主动性与积极性。

关于 Windows 系统的兼容性

本书各实训的操作平台都采用主流操作系统 Windows XP Professional。Windows 各版本的一致性和兼容性，使本书的各个实训在 Windows 环境下具有普遍的适用性。但即使这样，为避免可能存在的问题，仍然建议读者在实训室和自己的计算机上安装 Windows XP Professional 来完成实训。当然，我们相信，当把本书的实训在其他 Windows 环境中进行时，也一定会得到很大的收获。

实训设备

个人计算机在学生，尤其是专业学生中的普及，使得我们有机会把实训任务分别利用课内和课外时间来完成，以获得更多的锻炼。这样，对实训室和个人计算机的配置就有不同的要求。

实训室设备与环境

大多数用于信息安全技术实训的工具软件都基于 Windows 环境，用来开展信息安全技术实训的实训室计算机，其操作系统建议安装 Windows XP Professional。

由于大多数实训都需要因特网环境的支持，因此用来进行信息安全技术实训的实训室环境，应该具有良好的上网条件。

个人实训设备与环境

用于信息安全技术实训的个人计算机环境，建议安装 Windows XP Professional 操作系统。需要为实训准备足够的硬盘存储空间，以方便实训软件的安装和实训数据的保存。

在利用个人计算机完成实训时，要重视理解在操作中系统所显示的提示甚至警告信息，注意保护自己数据和计算环境的安全，做好必要的数据备份工作，以免产生不必要的损失。

没有设备时如何使用本书

如果本书的读者由于某些客观原因无法获得必要的实训设备时，也不用失望，我们相信您仍将从本书中受益。全书以循序渐进的方式介绍了课程知识和实训任务，读者通过认真阅读和仔细分析实训的操作步骤，相信也能在一定程度上有所收获。

Web 站点资源

几乎所有软件工具的生产厂商都对其产品的用户提供了足够的因特网支持，用户可利用这些网络来修改错误、升级系统，并获得更为详尽和丰富的技术资料。由于网络资料的日新月异，我们不便在本书中一一罗列，有要求的读者可以上网利用谷歌、百度等搜索工具即时进行检索。

本书中的实训素材可以从中国铁道出版社网站（http://edu.tqbooks.net）的下载区下载，或者从网站 www.zhousu.net 下载。其中包含了在本书各个实训中用到的所有程序的源代码。这些源程序均通过调试运行，希望有助于提高实训的效率。下载资料中还包含了与本书内容相配套的教学课件，可帮助教师做一点基础的备课准备，有助于学生在课堂上更好地集中听课的注意力，也方便了课前课后的预习和复习。

CONTENTS

目录

第 1 章 熟悉信息安全技术 1
1.1 信息安全技术的计算环境 1
1.1.1 信息安全的目标 1
1.1.2 信息安全技术发展的四大趋势 2
1.1.3 因特网选择的几种安全模式 3
1.1.4 安全防卫的技术手段 3
1.1.5 实训与思考：信息安全技术基础 5
1.1.6 阅读与思考：丹·布朗及其《数字城堡》 11
1.2 信息系统的物理安全 12
1.2.1 物理安全的内容 12
1.2.2 环境安全技术 13
1.2.3 电源系统安全技术 14
1.2.4 电磁防护与设备安全技术 15
1.2.5 通信线路安全技术 16
1.2.6 实训与思考：物理安全技术 16
1.2.7 阅读与思考：基本物理安全 17
1.3 Windows 系统管理与安全设置 19
1.3.1 Windows 系统管理 19
1.3.2 Windows 安全特性 20
1.3.3 账户和组的安全性 21
1.3.4 域的安全性 22
1.3.5 文件系统的安全性 22
1.3.6 IP 安全性管理 22
1.3.7 实训与思考：Windows 安全设置 22
1.3.8 阅读与思考：信息安全技术正从被动转向主动 29
第 2 章 数据备份技术 30
2.1 优化 Windows XP 磁盘子系统 30
2.1.1 选择文件系统 30
2.1.2 EFS 加密文件系统 31
2.1.3 压缩 31
2.1.4 磁盘配额 32
2.1.5 实训与思考：Windows 文件管理 32

2.1.6 阅读与思考：信息安全已成为信息社会文明的重要内容 39
2.2 数据存储解决方案 40
2.2.1 数据备份的概念 40
2.2.2 常用的备份方式 41
2.2.3 直连方式存储（DAS） 41
2.2.4 网络连接存储（NAS） 42
2.2.5 存储区域网络（SAN） 42
2.2.6 主流备份技术 43
2.2.7 备份的误区 44
2.2.8 实训与思考：了解数据备份技术 45
2.2.9 阅读与思考：信息安全技术专业 48
第 3 章 加密与认证技术 49
3.1 加密技术与 DES 加解密算法 49
3.1.1 密码学的基础知识 50
3.1.2 古典密码算法 51
3.1.3 单钥加密算法 52
3.1.4 数据加密标准 DES 算法 53
3.1.5 实训与思考：了解加密技术 54
3.1.6 阅读与思考：手掌静脉识别技术 57
3.2 电子邮件加密软件 PGP 58
3.2.1 PGP 的工作原理 59
3.2.2 PGP 的主要功能 60
3.2.3 PGP 的安全性 61
3.2.4 实训与思考：加密软件的功能与应用 62
3.2.5 阅读与思考：加密技术存在重大漏洞 67
3.3 加密算法与认证技术 67
3.3.1 RSA 算法 68
3.3.2 认证技术 70
3.3.3 个人数字证书 73
3.3.4 实训与思考：加密算法与认证技术 73
3.3.5 阅读与思考：认证技术之争 78
第 4 章 防火墙与网络隔离技术 80
4.1 防火墙技术及 Windows 防火墙配置 80
4.1.1 防火墙技术 80
4.1.2 防火墙的功能指标 83
4.1.3 防火墙技术的发展 84
4.1.4 Windows 防火墙 84
4.1.5 实训与思考：了解防火墙技术 85

4.1.6 阅读与思考：防火墙知识问答 96
4.2 网络隔离技术与网闸应用 97
4.2.1 网络隔离的技术原理 98
4.2.2 网络隔离的技术分类 100
4.2.3 网络隔离的安全要点 100
4.2.4 隔离网闸 101
4.2.5 实训与思考：了解网络隔离技术 103
4.2.6 阅读与思考：加密狗 105
第 5 章 安全检测技术 107
5.1 入侵检测技术与网络入侵检测系统产品 107
5.1.1 IDS 分类 108
5.1.2 IDS 的基本原理 109
5.1.3 入侵检测系统的结构 110
5.1.4 入侵检测的基本方法 112
5.1.5 实训与思考：了解入侵检测技术 113
5.1.6 阅读与思考：八大信息安全技术的创新点 115
5.2 漏洞检测技术和微软系统漏洞检测工具 MBSA 117
5.2.1 入侵攻击可利用的系统漏洞类型 118
5.2.2 漏洞检测技术分类 119
5.2.3 漏洞检测的基本要点 120
5.2.4 微软系统漏洞检测工具 MBSA 120
5.2.5 实训与思考：漏洞检测工具 MBSA 121
5.2.6 阅读与思考：前黑客提出的个人计算机安全十大建议 128
第 6 章 访问控制与审计技术 130
6.1 访问控制技术与 Windows 访问控制 130
6.1.1 访问控制的基本概念 130
6.1.2 Windows XP 的访问控制 132
6.1.3 实训与思考：Windows 访问控制功能 133
6.1.4 阅读与思考：信息安全管理滞后 企业数据失窃严重 138
6.2 审计追踪技术与 Windows 安全审计功能 138
6.2.1 审计内容 139
6.2.2 安全审计的目标 139
6.2.3 安全审计系统 139
6.2.4 实训与思考：Windows 安全审计功能 141
6.2.5 阅读与思考：网络管理技术的亮点与发展 146
第 7 章 病毒防范技术 150
7.1 病毒防范技术与杀病毒软件 150

7.1.1 计算机病毒的概念 150
7.1.2 计算机病毒的特征 152
7.1.3 计算机病毒的分类 153
7.1.4 病毒的传播 154
7.1.5 病毒的结构 154
7.1.6 反病毒技术 154
7.1.7 实训与思考：计算机病毒防范技术 156
7.1.8 阅读与思考：全球信息安全技术“教父”——尤金·卡巴斯基 159
7.2 解析计算机蠕虫病毒 160
7.2.1 蠕虫病毒的定义 160
7.2.2 网络蠕虫病毒分析和防范 162
7.2.3 实训与思考：蠕虫病毒的查杀与防范 162
7.2.4 阅读与思考：木马 167
7.3 反垃圾邮件技术 169
7.3.1 垃圾邮件的概念 169
7.3.2 反垃圾邮件技术 170
7.3.3 实训与思考：熟悉反垃圾邮件技术 171
7.3.4 阅读与思考：全球向垃圾电邮开战 175
第 8 章 虚拟专用网络技术 177
8.1 VPN 的安全性 177
8.2 因特网的安全协议 IPSec 178
8.2.1 IPSec 的体系结构 179
8.2.2 安全关联 180
8.2.3 传输模式与隧道模式 180
8.2.4 AH 协议 180
8.2.5 ESP 协议 181
8.2.6 安全管理 182
8.2.7 密钥管理 182
8.3 VPN 应用 182
8.3.1 通过因特网实现远程用户访问 182
8.3.2 通过因特网实现网络互连 183
8.3.3 连接企业内部网络计算机 184
8.4 实训与思考：Windows VPN 设置 184
8.5 阅读与思考：杭州建成四网融合无线城市 188
第 9 章 信息安全管理与灾难恢复 190
9.1 信息安全管理与工程 190
9.1.1 信息安全管理策略 190
9.1.2 信息安全机构和队伍 191

9.1.3 信息安全管理制度 192
9.1.4 信息安全管理标准 193
9.1.5 信息安全的法律保障 193
9.1.6 信息安全工程的设计原则 194
9.1.7 信息安全工程的设计步骤 195
9.1.8 信息安全工程的实施与监理 197
9.1.9 实训与思考：熟悉信息安全管理 197
9.1.10 阅读和思考：信息安全管理的核心是人的尽职意识和警觉 209
9.2 信息灾难恢复规划 210
9.2.1 数据容灾概述 211
9.2.2 数据容灾与数据备份的联系 212
9.2.3 数据容灾等级 213
9.2.4 容灾技术 213
9.2.5 实训与思考：了解信息灾难恢复 215
9.2.6 阅读与思考：M 公司的灾难恢复计划 218
第 10 章 信息安全技术实训总结 223
10.1 实训的基本内容 223
10.2 实训的基本评价 225
10.3 课程学习能力测评 226
10.4 信息安全技术实训总结 226
参考文献 228

第1章 熟悉信息安全技术

信息安全是指信息网络的硬件、软件及系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改或泄露，使系统连续、可靠、正常地运行，信息服务不中断。熟悉信息安全技术，应该了解信息安全技术的网络支持环境、信息系统的物理安全、操作系统的系统管理与安全设置等内容。

1.1 信息安全技术的计算环境

信息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学科。从广义来说，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属于信息安全的研究领域。

如今，基于网络的信息安全技术也是未来信息安全技术发展的重要方向。由于因特网（Internet）是一个全开放的信息系统，窃密和反窃密、破坏与反破坏广泛存在于个人、集团甚至国家之间，资源共享和信息安全一直作为一对矛盾体而存在着，网络资源共享的进一步加强以及随之而来的信息安全问题也日益突出。

1.1.1 信息安全的目标

无论是在计算机上存储、处理和应用，还是在通信网络上传输，信息都可能被非授权访问而导致泄密，被篡改破坏而导致不完整，被冒充替换而导致否认，也有可能被阻塞拦截而导致无法存取。这些破坏可能是有意的，如黑客攻击、病毒感染；也可能是无意的，如误操作、程序错误等。因此，普遍认为，信息安全的目标应该是保护信息的机密性、完整性、可用性、可控性和不可抵赖性（即信息安全的五大特性）。

1. 机密性

机密性是指保证信息不被非授权访问，即使非授权用户得到信息也无法知晓信息的内容，因而不能使用。

2. 完整性

完整性是指维护信息的一致性，即在信息生成、传输、存储和使用过程中不发生人为或非人为的非授权篡改。

3. 可用性

可用性是指授权用户在需要时能不受其他因素的影响，方便地使用所需信息。这一目标对信息系统的总体可靠性要求较高。

4．可控性

可控性是指信息在整个生命周期内部可由合法拥有者加以安全地控制。

5．不可抵赖性

不可抵赖性是指保障用户无法在事后否认曾经对信息进行的生成、签发、接收等行为。

事实上，安全是一种意识，一个过程，而不仅仅是某种技术。进入21世纪后，信息安全的理念发生了巨大的变化，从不惜一切代价把入侵者阻挡在系统之外的防御思想，开始转变为预防—检测—攻击响应—恢复相结合的思想，出现了PDRR(protect/detect/react/restore)等网络动态防御体系模型，如图1-1所示。

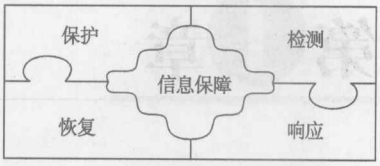


图1-1 信息安全的PDRR模型

PDRR倡导一种综合的安全解决方法，即针对信息的生存周期，以“信息保障”模型作为信息安全的目标，以信息的保护技术、信息使用中的检测技术、信息受影响或攻击时的响应技术和受损后的恢复技术作为系统模型的主要组成元素。在设计信息系统的安全方案时，综合使用多种技术和方法，以取得系统整体的安全性。

PDRR模型强调的是自动故障恢复能力，把信息的安全保护作为基础，将保护视为活动过程，用检测手段来发现安全漏洞，及时更正；同时采用应急响应措施对付各种入侵；在系统被入侵后，采取相应的措施将系统恢复到正常状态，使信息的安全得到全方位的保障。

1.1.2 信息安全技术发展的四大趋势

信息安全技术的发展，主要呈现四大趋势，即可信化、网络化、标准化和集成化。

1．可信化

可信化是指从传统计算机安全理念过渡到以可信计算理念为核心的计算机安全。面对愈演愈烈的计算机安全问题，传统安全理念很难有所突破，而可信计算的主要思想是在硬件平台上引入安全芯片，从而将部分或整个计算平台变为“可信”的计算平台。目前，主要研究和探索的问题包括基于TCP的访问控制、基于TCP的安全操作系统、基于TCP的安全中间件、基于TCP的安全应用等。

2．网络化

由网络应用和普及引发的技术和应用模式的变革，正在进一步推动信息安全关键技术的创新发展，并引发新技术和应用模式的出现。如安全中间件、安全管理与安全监控等都是网络化发展所带来的必然的发展方向。网络病毒、垃圾信息防范、网络可生存性、网络信任等都是要继续研究的领域。

3．标准化

安全技术要走向国际，也要走向实际应用，政府、产业界和学术界等必将更加高度重视信息安全标准的研究与制定，如密码算法类标准（例如加密算法、签名算法、密码算法接口）、安全认证与授权类标准（例如PKI、PMI、生物认证）、安全评估类标准（例如安全评估准则、方法、规范）、系统与网络类安全标准（例如安全体系结构、安全操作系统、安全数据库、安全路由器、可信计算平台）、安全管理类标准（例如防信息泄露、质量保证、机房设计）等。

4．集成化

集成化即从单一功能的信息安全技术与产品，向多种功能融于某一个产品，或者是几个功能相结合的集成化产品发展。安全产品呈硬件化/芯片化发展趋势，这将带来更高的安全度与更

高的运算速率，也需要发展更灵活的安全芯片的实现技术，特别是密码芯片的物理防护机制。

1.1.3　因特网选择的几种安全模式

目前，在因特网应用中采取的防卫安全模式归纳起来主要有以下几种：

1．无安全防卫

在因特网应用初期多数采取此方式，安全防卫上不采取任何措施，只使用随机提供的简单安全防卫措施。这种方法是不可取的。

2．模糊安全防卫

采用这种方式的网站总认为自己的站点规模小，对外无足轻重，没人知道；即使知道，黑客也不会对其进行攻击。事实上，许多入侵者并不是瞄准特定目标，只是想闯入尽可能多的机器，虽然它们不会永远驻留在你的站点上，但它们为了掩盖闯入网站的证据，常常会对网站的有关内容进行破坏，从而给网站带来重大损失。为此，各个站点一般要进行必要的登记注册。这样，一旦有人使用服务时，提供服务的人知道它从哪来，但是这种站点防卫信息很容易被发现，例如登记时会有站点的软、硬件以及所用操作系统的信息，黑客就能从这发现安全漏洞，同样在站点与其他站点连机或向别人发送信息时，也很容易被入侵者获得有关信息，因此这种模糊安全防卫方式也是不可取的。

3．主机安全防卫

这可能是最常用的一种防卫方式，即每个用户对自己的机器加强安全防卫，尽可能地避免那些已知的可能影响特定主机安全的问题，这是主机安全防卫的本质。主机安全防卫对小型网站是很合适的，但是由于环境的复杂性和多样性，例如操作系统的版本不同、配置不同以及不同的服务和不同的子系统等都会带来各种安全问题。即使这些安全问题都解决了，主机防卫还要受到软件本身缺陷的影响，有时也缺少有合适功能和安全保障的软件。

4．网络安全防卫

这是目前因特网中各网站所采取的安全防卫方式，包括建立防火墙来保护内部系统和网络、运用各种可靠的认证手段（如一次性密码等），对敏感数据在网络上传输时，采用密码保护的方式进行。

1.1.4　安全防卫的技术手段

在因特网中，信息安全主要是通过计算机安全和信息传输安全这两个技术环节，来保证网络中各种信息的安全。

1．计算机安全技术

① 健壮的操作系统。操作系统是计算机和网络中的工作平台，在选用操作系统时，应注意软件工具齐全和丰富、缩放性强等因素，如果有很多版本可供选择，应选用户群最少的版本，这样使入侵者用各种方法攻击计算机的可能性减少，另外还要有较高访问控制和系统设计等安全功能。

② 容错技术。尽量使计算机具有较强的容错能力，如组件全冗余、没有单点硬件失效、动态系统域、动态重组、错误校正互连；通过错误校正码和奇偶检验的结合保护数据和地址总线；在线增减域或更换系统组件，创建或删除系统域而不干扰系统应用的进行，也可以采取双机备份同步检验方式，保证网络系统在一个系统由于意外而崩溃时，计算机进行自动切换以确保正常运转，保证各项数据信息的完整性和一致性。