

《计算机网络安全基础(第4版)(普通高等教育“十一五”国家级规划教材)》

书籍信息

版次：4

页数：

字数：

印刷时间：2013年07月11日

开本：16开

纸张：胶版纸

包装：平装

是否套装：否

国际标准书号ISBN：9787115315113

丛书名：普通高等学校计算机教育“十二五”规划教材

编辑推荐

本书以教材的形式进行编写，内容由浅入深，通俗易懂，每章附有小结和习题，并有相关的实验。本书是目前我国*早出版的网络安全方面的教材，因此应扩大其优势和影响力。

本教材具有如下特色：

1. 通俗易懂

本书的作者具有多年计算机网络安全和计算机网络相关的教学经验和工作经历，并且使用原有的教材已经过多次教学的循环，故能克服原书中的不足并发挥原书中的优点。这样写出的教材语言简练，叙述简洁，可以用于课堂教学和自学。同时还将很多复杂、艰涩的数学公式简化，这样学习者的数学水平不需要很高也可以学好有关安全的知识，扩大了读者群。原教材已经达到了这个目的，并且在教学中已经取得了良好的效果。

2. 丰富的习题和练习

本教材在编写过程中，非常注重读者动手进行练习和习题训练，每道题都经过专门的挑选，并有相应的答案。通过章后的习题可以达到复习所学内容的目的。为了进行本课程编程的训练，作者还编写了相应的教材《计算机网络与安全实用编程》一书，已由人民邮电出版社出版。该书有大量的程序原代码适合学生在学习中提高编程的能力。

3. 实验简单易行

在本书后附有很多网络安全相关的实验，使学生在实验过程中，掌握有关的基本概念和理论，达到对所学内容的巩固和理解。实验时也不需要很多的仪器和设备，克服了网络安全实验需要贵重设备的缺点。

4. 便于课堂教学

本书内容由浅入深，便于学习。同时随书还附有对应章节的电子教案以及相应的教学大纲，这样可以便于教师灵活教学和学生主动学习。

5. 内容丰富

本教材涵盖了当今有关计算机网络安全的重要的、必备的内容，每章节都选取成熟和典型的内容进行教学，同时也让读者了解当今**的安全知识。通过学习本书的内容，学生可以学到有关安全领域里的重点内容，增加在安全领域的工作经验，有利于其就业。

6. 参考文献和网站众多

[显示全部信息](#)

内容简介

计算机网络安全是全社会都关注并亟待解决的一个大问题。本书主要介绍如何保护自己的网络以及网络系统中的数据不被破坏和丢失，如何保证数据在传输过程中的安全，如何避免数据被篡改以及维护数据的真实性等。本书重点进述与计算机系统安全有关的一

些基础知识，如安全级别、访问控制、数据加密、网络安全和数据安全等。本书可作为高等院校计算机专业教材，也可作为计算机网络的系统管理人员、安全技术人员的相关培训教材或参考书。

目录

第1章 网络基础知识与因特网

1.1 网络参考模型

1.1.1 分层通信

1.1.2 信息格式

1.2 网络互连设备

1.2.1 中继器和集线器

1.2.2 网桥

1.2.3 路由器

1.2.4 网关

1.3 局域网技术

1.3.1 以太网和IEEE 802.3

1.3.2 令牌环网和IEEE 802.5

1.3.3 光纤分布式数据接口

1.4 广域网技术

第2章 网络安全概述
2.1 网络安全基础知识
2.1.1 网络安全的含义
2.1.2 网络安全的特征
2.1.3 网络安全的威胁
2.1.4 网络安全的关键技术
2.1.5 网络安全策略
2.2 威胁网络安全的因素
2.2.1 威胁网络安全的主要因素
2.2.2 各种外部威胁
2.2.3 防范措施
2.3 网络安全分类
2.4 网络安全解决方案
2.4.1 网络信息安全模型
2.4.2 安全策略设计依据
2.4.3 网络安全解决方案
2.4.4 网络安全性措施
2.4.5 因特网安全管理
2.4.6 网络安全的评估
2.5 小结习题

第4章 数据安全技术

4.1 数据完整性简介

4.1.1 数据完整性

4.1.2 提高数据完整性的办法

4.2 容错与网络冗余

4.2.1 容错技术的产生及发展

4.2.2 容错系统的分类

4.2.3 容错系统的实现方法

4.2.4 网络冗余

4.3 网络备份系统

4.3.1 备份与恢复

4.3.2 网络备份系统的组成

4.3.3 备份的设备与介质

4.3.4 磁带轮换

4.3.5 备份系统的设计

4.4 数据库安全概述

4.4.1 简介

4.4.2 数据库的特性

4.4.3 数据库安全系统特性

4.4.4 数据库管理系统

4.5 数据库安全的威胁

4.6 数据库的数据保护

4.6.1 数据库的故障类型

4.6.2 数据库的数据保护

4.7 数据库备份与恢复

4.7.1 数据库备份的评估

4.7.2 数据库备份的性能

4.7.3 系统和网络完整性

4.7.4 制定备份的策略

4.7.5 数据库的恢复

4.7.6 MySQL数据库备份与恢复

4.8 小结习题

第6章 数据加密与认证技术

6.1 数据加密概述

6.1.1 密码学的发展

6.1.2 数据加密

6.1.3 基本概念

6.2 传统密码技术

6.2.1 数据表示方法

6.2.2 替代密码

6.2.3 换位密码

6.2.4 简单异或

6.2.5 一次密码

6.3 对称密钥密码技术

6.3.1 Feistel密码结构

6.3.2 数据加密标准

6.3.3

国际数据加密算法6.3.4 Blowfish算法6.3.5 GOST算法6.3.6 PKZIP算法6.3.7 RC5算法6.4
公钥密码体制6.4.1 公钥加密原理6.4.2 Diffie-Hellman密钥交换算法6.4.3 RSA密码系统6.4.4
数字信封技术6.5 数字签名技术6.5.1 基本概念6.5.2 安全Hash函数6.5.3
直接方式的数字签名技术6.5.4 数字签名算法6.5.5 其他数字签名技术6.6 验证技术6.6.1
信息的验证6.6.2 认证授权6.6.3 CA证书6.6.4 PKI系统6.6.5 Kerberos系统6.7 加密软件PGP6.8
小结习题

第8章 网络站点的安全8.1 因特网的安全8.1.1 因特网服务的安全隐患8.1.2 因特网的脆弱性
8.2 Web站点安全8.2.1 Web技术简介8.2.2 Web安全体系的建立8.2.3
Web服务器设备和软件安全8.2.4 建立安全的Web网站8.2.5 Web网站的安全管理8.3
口令安全8.3.1 口令的破解8.3.2 安全口令的设置8.4 无线网络安全8.4.1
无线局域网安全技术8.4.2 无线网络的常见攻击8.4.3 无线网络安全设置8.5 网络监听8.5.1
监听的原理8.5.2 监听的工具8.5.3 监听的实现8.5.4 监听的检测与防范8.6 扫描器8.6.1
什么是扫描器8.6.2 端口扫描8.6.3 扫描工具8.7 E-mail的安全8.7.1 E-
mail工作原理及安全漏洞8.7.2 匿名转发8.7.3 E-mail欺骗8.7.4 E-mail轰炸和炸弹8.7.5 保护E-
mail8.8 IP电子欺骗8.8.1 IP电子欺骗的实现原理8.8.2 IP电子欺骗的方式和特征8.8.3
IP欺骗的对象及实施8.8.4 IP欺骗攻击的防备8.9 DNS的安全性8.9.1
目前DNS存在的安全威胁8.9.2 Windows下的DNS欺骗8.10 小结习题

附录附录一 优秀网络安全站点附录二 英文缩写词

[显示全部信息](#)

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

[更多资源请访问www.tushupdf.com](http://www.tushupdf.com)