全国高校出版社优秀畅销书

高等学校计算机科学与技术教材

- 原理与技术的完美结合
- 教学与科研的最新成果
- 语言精炼，实例丰富
- 可操作性强，实用性突出

计算机网络安全教程

（修订本）

□ 石志国　薛为民　尹　浩　编著

清华大学出版社　●　北京交通大学出版社

TP393.08
179
2004

全国高校出版社优秀畅销书
高等学校计算机科学与技术教材

计算机网络安全教程

(修订本)

石志国　薛为民　尹　浩　编著

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

本书是《计算机网络安全教程》的修订本，在原书基础上做了大量修整和扩充，使之更加适合高校教学和自学的需要。利用大量的实例讲解知识点，将安全理论、安全工具与安全编程三方面内容有机地结合到一起。每章最后都配有大量的习题，用来检查教学和学习的进度。

全书从网络安全体系上分成四部分。第一部分：计算机网络安全基础，介绍网络安全的基本概念、实验环境配置、网络协议基础及网络安全编程基础。第二部分：网络安全攻击技术，详细介绍攻击技术“五部曲”及恶意代码的发展和原理。第三部分：网络安全防御技术，介绍安全操作系统相关原理、加密与解密技术的应用、防火墙、入侵检测技术及 IP 和 Web 安全相关理论。第四部分：网络安全综合解决方案，从工程的角度介绍网络安全工程方案的编写。

本书可以作为高校及各类培训机构相关课程的教材或者参考书。

本书中的源代码、所涉及的软件和授课幻灯片等教学支持信息可以从图书支持网站 http://www.gettop.net 下载，也可以从出版社网站 http://press.bjtu.edu.cn 的下载栏目中下载。

版权所有，翻印必究。举报电话：010－62782989　13501256678　13801310933

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。

本书防伪标签采用特殊防伪技术，用户可通过在图案表面涂抹清水，图案消失，水干后图案复现；或将表面膜揭下，放在白纸上用彩笔涂抹，图案在白纸上再现的方法识别真伪。

图书在版编目(CIP)数据

计算机网络安全教程/石志国，薛为民，尹浩编著．—修订本．—北京：清华大学出版社；北京交通大学出版社，2007.1

（高等学校计算机科学与技术教材）

ISBN 978－7－81082－249－7

Ⅰ．计…　Ⅱ．①石…　②薛…　③尹…　Ⅲ．计算机网络－安全技术－高等学校－教材　Ⅳ．TP393.08

中国版本图书馆 CIP 数据核字（2006）第 126904 号

责任编辑：谭文芳

出版发行：清华大学出版社　邮编：100084　电话：010－62776969　http://www.tup.com.cn

北京交通大学出版社　邮编：100044　电话：010－51686414　http://press.bjtu.edu.cn

印 刷 者：北京东光印刷厂

经　　销：全国新华书店

开　　本：185×260　印张：21.5　字数：550 千字

版　　次：2004 年 2 月第 1 版　2007 年 1 月第 1 次修订　2007 年 2 月第 8 次印刷

书　　号：ISBN 978－7－81082－249－7/TP·101

印　　数：35 001～45 000 册　定价：31.00 元

本书如有质量问题，请向北京交通大学出版社质监组反映。对您的意见和批评，我们表示欢迎和感谢。

投诉电话：010－51686043、51686008；传真：010－62225406；E-mail：press@center.bjtu.edu.cn。

修订本前言

修订本在原书基础上做了大量修整和扩充，使之更加适合高校教学和自学的需要。本书利用大量的实例讲解知识点，将安全理论、安全工具与安全编程三方面内容有机地结合到一起，每章最后都配有大量的习题，用来检查教学和学习的进度。

与第一版比较

2004 年初《计算机网络安全教程》出版，目的是为了满足网络安全技术教学的迫切需要。该书综合了作者在北京大学计算机研究所部分研究内容、清华大学计算机系部分教学内容及网络信息安全国际认证考试的部分内容，在写作过程中还得到了三院院士王选老师的支持和指导。

原书出版以来，受到了老师、同学及广大读者的认可和欢迎，同时，很多读者也提出了很多改进意见。当前，网络安全是计算机相关领域中的一门重要学科，很多高校和研究机构都设置了网络信息安全本科专业及网络信息安全方向的硕士点和博士点。这次花了大量的时间对原书做了一次全面的更新，希望能更好的帮助广大读者学习好网络安全的相关知识。

修订本在保证原书整体结构的情况下，对内容进行了全面的扩充和修正，一个主要的特点是理论性的增强，主要做了如下 6 方面的调整。

(1) 增强了理论性并全面阐述了网络安全两个重要的概念：恶意代码和 Web 安全。添加了两章，分别为恶意代码分析与防治和 IP 安全与 Web 安全(修订本第 11 章)，将全书扩充为 12 章。

(2) 修正并解决了部分内容不规范、图表不清楚的问题。

(3) 全面扩充了拒绝服务攻击及分布式拒绝服务攻击的分类和原理。

(4) 增加了安全操作系统的机制与原理。

(5) 增加了数字签名、数字水印和公钥基础设施 PKI 的相关内容。

(6) 为了检查教学及自学的效果，每章都重新设计了课后习题的内容，并给出了相关参考答案。

本书结构

修订本在每一章前面精心设计了“本章要点”，因为每一章内容都比较庞杂，所以要注意本章要点，重点掌握提及的内容。每一章后面都精心设计了适量的习题，主要是针对本章重点、难点进行训练。附录还提供了选择题和填空题的答案，可以对照检查自己的学习效果。对于简答题，均可以在书上找到答案。

本书导读

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。本书从计算机网络安全理论、网络安全攻防工具

和网络安全编程三个角度介绍计算机网络安全技术，这三方面内容均来自工程和课堂教学的实践，并通过网络安全攻防体系结合在一起。从网络安全攻防体系上，全书分成四部分，共12章。

第一部分：计算机网络安全基础

第1章　网络安全概述与环境配置。介绍信息安全和网络安全的研究体系、研究网络安全的意义、评价网络安全的标准及实验环境的配置。

第2章　网络安全协议基础。介绍OSI参考模型和TCP/IP协议族，实际分析IP、TCP、UDP、ICMP协议的结构及工作原理、网络服务和网络命令。

第3章　网络安全编程基础。介绍网络安全编程的基础知识、C语言发展的四个阶段，以及网络安全编程的常用技术：Socket编程、注册表编程及驻留编程，等等。

第二部分：网络安全的攻击技术

第4章　网络扫描与网络监听。介绍黑客及黑客攻击的基本概念，如何利用工具实现网络踩点、网络扫描和网络监听。

第5章　网络入侵。介绍常用的网络入侵技术：社会工程学攻击、物理攻击、暴力攻击、漏洞攻击及缓冲区溢出攻击等。

第6章　网络后门与网络隐身。介绍网络后门和木马的基本概念，并利用四种方法实现网络后门；介绍利用工具实现网络跳板和网络隐身。

第7章　恶意代码分析与防治。介绍恶意代码的发展史，恶意代码长期存在的原因，介绍恶意代码实现机理、定义及攻击方法等。

第三部分：网络安全的防御技术

第8章　安全操作系统基础。介绍UNIX、Linux和Windows的特点，着重介绍安全操作系统的原理，介绍Windows操作系统的安全配置方案。

第9章　密码学与信息加密。介绍密码学的基本概念，DES加密算法的概念及如何利用程序实现，RSA加密算法的概念及实现算法，PGP加密的原理和实现。

第10章　防火墙与入侵检测。介绍防火墙的基本概念、分类、实现模型，以及如何利用软件实现防火墙的规则集；介绍入侵检测系统的概念、原理，以及如何利用程序实现简单的入侵系统。

第11章　IP安全与Web安全。介绍IPSec的必要性，IPSec中的AH协议和ESP协议、密钥交换协议IKE和VPN的解决方案等。

第四部分：网络安全综合解决方案

第12章　网络安全方案设计。从网络安全工程的角度介绍网络安全方案编写的注意点及评价标准。

致谢

在编写过程中，得到众多老师的指导和帮助。感谢中科院软件所卿斯汉研究员、梁洪亮博士、商青华博士、周启明博士、张宏博士和金洁华工程师。感谢清华大学计算机系林闯主任。感谢北京科技大学王志良教授、徐正光教授、解仑副教授和王莉副教授。感谢中央广播电视大学崔林教授，徐孝凯教授、田萧老师和王春凤老师。感谢中国软件行业协会邱钦伦高级工程师。感谢他们为本书提供了大量并且详尽的编程资料，并为本书解决了很多编程方面的问题。尤其要感谢的是北京交通大学出版社编辑谭文芳老师，她的支持是本书能顺利出版的关键。

此为试读，需要完整PDF请访问：www.ertongbook.com

感谢众多老师和同学们的支持，他们的每一个问题，都是本书要强调并解决的知识点，他们的认可是我最大的动力，本书献给你们，献给最广大的读者。

图书支持

本书可以作为高校及各类培训机构相关课程的教材或者教学参考书，网络安全自学人员和网络安全开发人员的参考书。本书提供完整的教学幻灯片、书中的所有软件和源代码及相关学习资源，将在 http://www.gettop.net 或者 http://press.bjtu.edu.cn 下载栏目中发布，欢迎访问和下载。

由于作者水平和时间有限，难免出现错误，对于本书的任何问题请使用E-mail发送到作者邮箱：shizhiguo@tom.com。

石志国

2007 年 1 月

目　录

第一部分　计算机网络安全基础

第二部分 网络安全的攻击技术

第三部分 网络安全的防御技术

此为试读，需要完整PDF请访问：www.ertongbook.com

第四部分 网络安全综合解决方案

第一部分 计算机网络安全基础

本部分包括：

★第 1 章　网络安全概述与环境配置

- ☑ 网络安全研究的体系、研究网络安全的必要性
- ☑ 研究网络安全的社会意义，与网络安全有关的法规
- ☑ 评价一个系统或者应用软件的安全等级
- ☑ 较为详细地介绍实验环境的配置

★第 2 章　网络安全协议基础

- ☑ OSI 七层网络模型、TCP/IP 协议族
- ☑ IP 协议、TCP 协议、UDP 协议和 ICMP 协议
- ☑ 常用的网络服务：FIP 服务、Telnet 服务等
- ☑ 常用的网络服务端口和常用的网络命令

★第 3 章　网络安全编程基础

- ☑ 操作系统编程中的 C 和 C++ 语言
- ☑ C 语言的 4 个发展阶段
- ☑ Socket 编程、注册表编程
- ☑ 定时器编程、驻留程序编程和多线程编程

第 1 章　网络安全概述与环境配置

本章要点

- ☑ 介绍网络安全研究的体系、研究网络安全的必要性
- ☑ 研究网络安全的社会意义，目前与计算机网络安全有关的法规
- ☑ 评价一个系统或者应用软件的安全等级
- ☑ 详细介绍实验环境的配置

1.1　信息安全概述

网络安全是信息安全学科的重要组成部分。信息安全是一门交叉学科，广义上讲，信息安全涉及多方面的理论和应用知识，除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学。狭义上讲，也就是通常说的信息安全，只是从自然科学的角度介绍信息安全的研究内容。信息安全各部分研究内容及相互关系如图 1-1 所示。

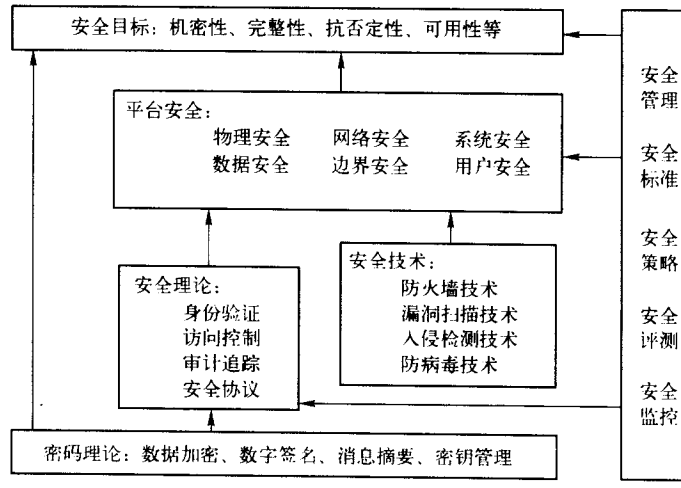

图 1-1　信息安全研究内容及关系

信息安全研究大致可以分为基础理论研究、应用技术研究、安全管理研究等。基础研究包括密码研究、安全理论研究；应用技术研究则包括安全实现技术、安全平台技术研究；安全管理研究包括安全标准、安全策略、安全测评等。

1.1.1　信息安全研究层次

信息安全从总体上可以分成 5 个层次：安全的密码算法、安全协议、网络安全、系统安全和

此为试读，需要完整PDF请访问：www.ertongbook.com