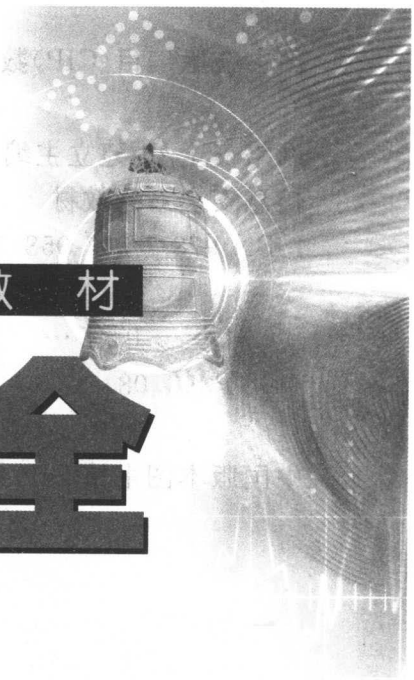
信息安全系列教材

网络安全

主　编　丁建立
副主编　江荣安　许　峰　崔　鸿
　　牛丹梅　王小军　黄淑宽

WUHAN UNIVERSITY PRESS
武汉大学出版社



信息安全系列教材

网络安全

主　编　丁建立
副主编　江荣安　许　峰　崔　鸿
　　牛丹梅　王小军　黄淑宽

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

网络安全/丁建立主编．—武汉：武汉大学出版社，2007.9
信息安全系列教材
ISBN 978-7-307-05847-7

Ⅰ.网… Ⅱ.丁… 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(2007)第 147393 号

责任编辑：黄金文　史　敏　　责任校对：程小宜　　版式设计：支　笛

出版发行：**武汉大学出版社**　(430072　武昌　珞珈山)
(电子邮件：wdp4@whu.edu.cn 网址：www.wdp.com.cn)
印刷：湖北金海印务公司
开本：787×1092　1/16　印张：20.375　字数：487 千字
版次：2007 年 9 月第 1 版　2007 年 9 月第 1 次印刷
ISBN 978-7-307-05847-7/TP・277　定价：30.00 元

前 言

随着信息技术空前繁荣，人们对计算机和网络的依赖性越来越大，信息被暴露和非法使用、网络受到攻击的可能性大大增加。经济全球化、互联网应用的普及、国家信息化建设的深入，使得信息安全已经成为国家安全保障体系的核心组成部分。一个国家的信息获取能力和信息安全保障能力是21世纪综合国力、经济竞争能力和生存能力的重要组成部分，信息安全事故的频发已成为信息社会十分突出的问题。

从本质上来讲，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是网络安全的研究领域。从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，对用户资源进行破坏。从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现"陷门"、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须进行控制。

本书主要从网络安全的基本原理和实践技术两个角度出发，分析目前常见的各种安全威胁，指出问题根源，提出网络安全的任务。内容基本涵盖目前主要的网络安全技术，既注重基本原理的阐述，又关注网络安全的新动向，并适时增加了实践的新技术，每章均安排有习题，重要内容安排了典型案例。

全书共分14章。第1章是网络安全概述，在分析常见的安全威胁与攻击、 安全问题根源基础上，给出网络信息安全的内涵。第2章是安全框架与评估标准，介绍了ISO/OSI安全体系结构和动态的自适应网络安全模型，给出了国际安全评价标准和我国计算机安全等级划分与相关标准。第3章是身份认证，阐述了身份认证的基本原理，分别介绍了单机状态下的身份认证、网络环境下的身份认证以及Windows NT安全子系统。第4章是授权与访问控制，在阐述了基本概念、基本原理、常用实现方法和访问控制策略基础上，给出了一个Windows NT提供的安全访问控制手段的实例。第5章是系统平台安全，分别介绍了UNIX系统安全、Windows NT安全以及网络应用安全平台。第6章是IP的安全，在分析IP安全体系结构基础上，给出了Windows 2000对于IPSec的支持实例。第7章是电子邮件的安全，分析了S/MIME和垃圾邮件， 实例介绍PGP软件的使用。第8章是Web与电子商务的安全，介绍了Web安全防护技术和电子商务的安全，重点阐述了SSL和主页防修改技术。第9章是防火墙技术，

阐述了防火墙的基本概念、类型、体系结构，介绍了防火墙的基本技术与附加功能、防火墙技术的几个新方向、常见的防火墙产品。第 10 章是网闸技术，介绍了网闸的基本概念、结构与特点，阐述了网闸的配置，并进行网闸典型案例剖析。第 11 章是 VPN 技术，在阐述了 VPN 的基本原理、应用领域及关键安全技术，分析了 VPN 的实现方法，介绍了 VPN 产品与解决方案。第 12 章是无线网络安全技术，介绍了常见无线网络攻击与无线网络安全对策，分析了无线通信安全与无线 VPN 安全。第 13 章是网络侦查与取证技术，介绍了网络扫描技术与工具，分析了网络监听、口令破译、蜜罐技术，给出了网络取证的原则与步骤。第 14 章是入侵检测技术，介绍了入侵检测系统的分类、系统结构、分析方法以及入侵检测的发展方向，并对典型入侵检测系统进行了介绍。

在武汉大学出版社的组织下，中国民航大学丁建立教授担任本书主编，担任本书副主编的有：大连理工大学江荣安、河海大学许峰、中国民航大学崔鸿、杭州电子科技大学王小军、河南科技大学牛丹梅、福州大学黄淑宽。具体分工是：丁建立主持编写第 1~2 章，江荣安主持编写第 3~4 章，黄淑宽主持编写第 5~6 章，许峰主持编写第 7~8 章，牛丹梅主持编写第 9~10 章，崔鸿主持编写第 11~12 章，王小军主持编写第 13~14 章。本书由崔鸿补充习题，丁建立负责统稿。

在本书的编写过程中，中国民航大学计算机科学与技术学院的硕士研究生计金玲参与了部分资料的收集与整理，王新茹为本书的排版做了部分工作。在此对所有参与本书编写工作的老师和同学们表示衷心感谢。在此要特别感谢武汉大学张焕国教授、武汉大学王丽娜教授，武汉大学出版社黄金文副编审对教材所给予的建议与帮助。

由于作者水平有限，书中难免有不妥和错误之处，恳请读者与同行批评指正。

编者

2007 年 7 月

信息安全系列教材

编　委　会

内 容 摘 要

本书主要从网络安全的基本原理和实践技术两个角度出发，分析目前常见的各种安全威胁，指出问题根源，提出网络安全的任务。全书共分 14 章，从安全框架与评估标准出发，分别介绍了身份认证、授权与访问控制、系统平台安全、IP 的安全、电子邮件的安全、Web 与电子商务的安全、防火墙技术、网闸技术、VPN 技术、无线网络安全技术、网络侦查与取证技术、入侵检测技术等。内容基本涵盖目前主要的安全技术，既注重基本原理的阐述，又关注网络安全的新动向，适时增加了实践的新技术，每章均安排有习题，重要内容均安排了典型案例。

本书重点突出，难易适当，实例丰富，实用性强。可作为各高等院校开设的信息安全相关专业的本科教材，也可供初学、准备从事相关研究的研究生参考，对从事网络安全研究和网络安全管理等领域的人员有参考价值。

序 言

21 世纪是信息的时代，信息成为一种重要的战略资源，信息的安全保障能力成为一个国家综合国力的重要组成部分。一方面，信息科学和技术正处于空前繁荣的阶段，信息产业成为世界第一大产业。另一方面，危害信息安全的事件不断发生，信息安全的形势是严峻的。

信息安全事关国家安全，事关社会稳定，必须采取措施确保我国的信息安全。

我国政府高度重视信息安全技术与产业的发展，先后在成都、上海和武汉建立了信息安全产业基地。

发展信息安全技术和产业，人才是关键。人才培养，教育是根本。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准，武汉大学又建立了信息安全的硕士点、博士点和企业博士后产业基地。自此以后，我国的信息安全专业得到迅速的发展。到目前为止，全国设立信息安全专业的高等院校已达 50 多所。我国的信息安全人才培养进入蓬勃发展阶段。

为了给信息安全专业的大学生提供一套适用的教材，武汉大学出版社组织全国 40 多所高校，联合编写出版了这套《信息安全系列教材》。该套教材涵盖了信息安全的主要专业领域，既有基础课教材，又有专业课教材，既有理论课教材，又有实验课教材。

这套书的特点是内容全面，技术新颖，理论联系实际。教材结构合理，内容翔实，通俗易懂，重点突出，便于讲解和学习。它的出版发行，一定会推动我国信息安全人才培养事业的发展。

诚恳希望读者对本系列教材的缺点和不足提出宝贵的意见。

编委会

2006 年 9 月 19 日

目 录