全国工程硕士专业学位教育指导委员会推荐教材

计算机网络安全

——协议、技术与应用

黄　河 编著　李伟琴 审核

http://www.tup.com.cn

清华大学出版社

全国工程硕士专业学位教育指导委员会推荐教材

计算机网络安全
——协议、技术与应用

黄　河　编著　李伟琴　审核

清华大学出版社
北京

内 容 简 介

本书以 TCP/IP 网络安全协议为核心，全面、系统地论述计算机网络安全的协议、技术与应用等问题。全书共分为三个部分：网络安全基础部分，包括网络安全概述、密码学基础、数字认证技术和公钥基础设施等；网络安全协议部分，分层描述计算机网络各层的安全协议及其应用，包括网络层的 IPSec，传输层的 SSL/TLS，应用层的 S/MIME、PGP、SSH、DNSSEC、TSIG、SNMPv3 等；网络安全技术与应用部分，详细讲解防火墙、VPN、访问控制、入侵检测、系统审计等较为成熟的网络安全技术，同时还介绍了移动 IP 安全、无线网络安全、Web Service 安全等网络安全新技术。

本书可作为通信、计算机等相关专业的大学本科生和研究生教材，也可作为从事计算机网络与信息安全工作的工程技术人员和广大爱好者的参考书。

图书在版编目(CIP)数据

计算机网络安全——协议、技术与应用/黄河编著. —北京：清华大学出版社，2008.9
(全国工程硕士专业学位教育指导委员会推荐教材)
ISBN 978-7-302-18057-9

Ⅰ. 计…　Ⅱ. 黄…　Ⅲ. 计算机网络－安全技术－研究生－教材　Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 098217 号

责任编辑：丁　岭　赵晓宁
责任校对：梁　毅
责任印制：李红英
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185×230　**印　张**：25.5　**字　数**：551 千字
版　　次：2008 年 9 月第 1 版　　**印　　次**：2008 年 9 月第1次印刷
印　　数：1～3000
定　　价：49.00 元

序

软件质量具有功能性、可靠性、易用性、效率性、维护性和可移植性6个特性，可从软件的内部质量、外部质量和使用质量三个视角去考量。软件质量保证就是要求把质量嵌入到软件开发的生命周期全过程中，以保证软件的“生产”质量；软件测试是软件质量保证的一个关键手段，又是软件产品发布前的最终检验；对软件产品质量的评价是以量化的方式来说明软件质量的程度的。因此，软件质量保证、测试与评价三方面的内容是一个相互关联的体系。鉴于此，在上海实施了“软件质量专业技术职业资格”的培训与资格考试专家组的工作基础上，由于杨根兴教授长期从事软件质量保证、测试与评价研究和实践工作，因此，以他为主编写此书确可担当。该书主要特点如下。

1. 创新与继承相结合

软件质量随着软件工程学科的不断发展而推陈出新，该书内容既论述了行之有效的质量保证方法和技术，也在实践经验基础上总结出了一些重要内容，如风险管理、软件缺陷管理、测试用例的复用和面向应用的测试等。

2. 规范与整体相结合

通过对GB/T 16260、8566、17544、CMU/SEI CMMI等国家和国际标准的学习和研究，运用了这些标准中相关概念和过程的规范描述。既具有标准的依从性，又有从软件质量保证和软件测试两个方面较为深入和详细的阐述，形成了一个较为完整的体系。

3. 技术与管理相结合

软件质量保证的实践活动大多需要在软件企业中进行，虽然技术十分重要，而管理也非常重要。该书内容既论述技术和方法，也阐述了软件测试管理的内容和方法。在软件质量保证中，管理同样会出效益，也会出质量。

4. 理论与实践相结合

任何理论的存在，必有其实践背景。软件质量从重要性来讲，实践经验是第一位的。该

Preface

书从不同的侧面反映了我国在软件质量方面的研究成果和实践经验，使之理论和实践均能兼顾和融合。

以我毕生研究软件质量的经验，软件质量的保证、测试与评价是一大难题，特别是要提出一套符合中国文化理念的方法有待时日，尚需不断努力。因此，我们必须培养更多的软件质量保证和软件测试人才，共同努力，为中国软件产业的发展作出积极的贡献。

该书的出版，将会有益于读者掌握一门重要的技艺，有益于推动软件质量保证与测试的研究、教学、实践的进一步发展，有益于助推我国软件产业的发展。

朱三元

2007 年 9 月于上海

前言

本书为全国工程硕士研究生教育核心教材，同时得到“北京市精品教材”项目的资助。本书由北京航空航天大学的黄河博士编著，李伟琴教授审核。

网络安全既有丰富的理论基础，又是实践性较强的一门学科。本书主要讲述网络环境下的信息安全技术，对于传统信息安全中的密码算法和密码协议等理论内容只做了简要介绍，着重描述了计算机网络安全的理论和实践知识，对于密码学的应用则贯穿在网络安全协议和技术中进行描述。为了使内容的组织具有系统性并便于读者理解，将教材内容划分为网络安全协议、技术和应用等不同层次进行论述。其中，网络安全协议部分是教材的核心内容，力争系统、全面地讲解 TCP/IP 网络安全协议，协议部分尽量结合其应用背景、实例和方法等加以论述；网络安全技术重点讲述防火墙、虚拟专用网、访问控制、入侵检测和系统审计等网络安全防御技术，同时也介绍了网络安全方面新的研究方向和技术。

教材中每章的实验部分列出了编者认为与教材内容配套的实验名称，其具体实验内容和方法读者可以根据需要自己选取。

教材的编写过程中得到诸多老师、同事及同学的帮助。北京航空航天大学的李伟琴教授对全书进行了审核并提出了许多宝贵的修改意见。北京航空航天大学软件学院的研究生周由胜、张凡、马心意和王隽竹，北京交通大学的研究生顾成杰，中国电力国际发展有限公司的陆路，路透中国科技有限公司的郑久丹，中国移动研究院的张鑫等同志也参与了本书的编写，在此表示诚挚的谢意。

由于作者水平所限，书中难免存在一些疏漏和错误，敬请广大读者批评指正。

编　者

2008 年 5 月

Foreword

目录

第一部分　网络安全基础

Contents

第三部分 网络安全技术与应用

第一部分

网络安全基础

第1章

网络安全概述

1.1 网络安全的概念及目标

网络安全是指对网络系统的硬件、软件及其中的数据实施保护，使网络信息不因偶然或恶意攻击而遭到破坏、更改或泄露，并且保证网络系统连续、可靠、正常地运行，保证网络服务不中断。

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、数论和信息论等多种学科的综合性学科。

如图 1.1 所示，网络信息安全包括以下三个目标。

- 机密性(confidentiality)：指计算机系统的资源应该仅能由授权实体读取。
- 完整性(integrity)：指资源只能由授权实体修改。
- 可用性(availability)：指一旦用户得到访问某一资源的权限，该资源就应该能够随时为其使用。

图 1.1 网络信息安全目标

国际电信联盟(international telecommunication union，ITU)将网络安全定义为攻击、安全机制和安全服务三个部分。

其中，攻击(attack)是指损害机构所拥有信息的安全的行为；安全机制(security mechanism)是指设计用于检测、预防安全攻击或者恢复系统的方法；安全服务(security service)是指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统安全和信息传输安全的能力。安全机制和安全服务将在 1.3 节详述，下面简单分析针对网络和信息的攻击。

从攻击的动机和危害性上看，可以将网络攻击分为被动攻击和主动攻击两类。其中，被

动攻击是指进行网络窃听，截取数据包并进行分析，从中窃取敏感信息。被动攻击不会导致对系统中所含信息的任何改动，而且系统的操作和状态也不被改变，因此被动攻击主要威胁信息的机密性，被动攻击不易被检测。主动攻击是指意在篡改系统中所含信息或者改变系统的状态及操作，例如冒充、篡改、抵赖、非授权访问、非法登录、信息或网络服务破坏等，主动攻击可以被网络系统检测到。

从信息流的角度上看，网络中的数据受到四个方面的威胁，包括中断威胁、侦听威胁、修改威胁和伪造威胁。设信息是从源地址流向目的地址，那么正常的信息流向如图 1.2 所示。

(1) 中断威胁：如图 1.3 所示，中断威胁使得信息在传输过程中被阻断，无法正确到达目的地，导致正在使用的信息系统毁坏或不能正常使用，破坏系统的可用性。中断威胁的攻击手段包括切断网络通信线路、损坏网络服务和使文件系统瘫痪等。

图 1.2 正常信息流

图 1.3 受中断威胁的信息流

(2) 侦听威胁：如图 1.4 所示，在侦听威胁中，一个非授权方进入系统并获取资源，破坏系统的机密性。非授权方可以是一个人、一个程序或一台主机。侦听威胁的攻击手段包括搭线窃听，文件或程序的不正当复制等。

(3) 修改威胁：如图 1.5 所示，在修改威胁中，一个非授权方不仅介入系统而且对系统中的信息进行了修改，破坏系统的完整性。修改威胁包括改变数据文件、改变程序使之不能正确执行、修改报文内容等。

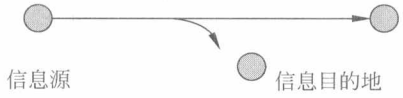

图 1.4 受侦听威胁的信息流

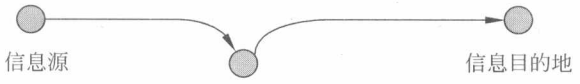

图 1.5 受修改威胁的信息流

(4) 伪造威胁：如图 1.6 所示，在伪造威胁中，一个非授权方将伪造的客体插入到系统中，破坏信息的真实性。伪造威胁包括在网络中插入虚假信息，或者在文件中追加记录等。

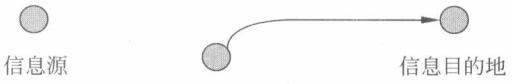

图 1.6 受伪造威胁的信息流

对应以上安全威胁，针对网络系统的攻击有多种，例如：

- 冒充攻击。指一个实体伪装成另一个实体，使网络中的信息遭受修改威胁和伪造威胁。例如，攻击者可以通过密码嗅探和猜测等方式获取合法用户的密码，然后冒充