可下载教学资料

http://www.tup.tsinghua.edu.cn

高等学校教材

计算机科学与技术

信息安全原理与技术

郭亚军 宋建华 李 莉 编著

清华大学出版社

高等学校教材

计算机科学与技术

信息安全原理与技术

郭亚军 宋建华 李 莉 编著

清华大学出版社

北京

内 容 简 介

本书系统地介绍了信息安全的基本原理和基本技术。全书共10章，包括信息安全的数学基础、对称加密技术、公钥加密技术、消息认证与数字签名、身份认证与访问控制、网络安全协议、公钥基础设施、防火墙和入侵检测等内容。

本书体现以读者为中心的思想。为了让读者充分理解每一章节内容以及它们之间的联系，每一章附有本章导读，并用大量的事例帮助读者理解重点知识和难点知识。

本书可作为计算机、信息安全、通信等专业的本科生以及低年级的研究生的教材，也可供从事信息安全相关专业的教学、科研和工程技术人员参考。

图书在版编目(CIP)数据

信息安全原理与技术/郭亚军，宋建华，李莉编著. —北京：清华大学出版社，2008.9
(高等学校教材·计算机科学与技术)
ISBN 978-7-302-17765-4

Ⅰ. 信… Ⅱ. ①郭… ②宋… ③李… Ⅲ. 信息系统－安全技术－高等学校－教材 Ⅳ. TP309

中国版本图书馆CIP数据核字(2008)第104955号

责任编辑：魏江江　王冰飞
责任校对：李建庄
责任印制：孟凡玉
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：185×260　**印　张**：16.75　**字　数**：400千字
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：25.00元

高等学校教材系列

已出版教材

ISBN：9787302115816　C 语言程序设计教程(王敬华　等编著)
ISBN：9787302124412　C 语言程序设计教程习题解答与实验指导(王敬华　等编著)
ISBN：9787302135074　C++语言程序设计教程(杨进才　等编著)
ISBN：9787302140962　C++语言程序设计教程习题解答与实验指导(杨进才　等编著)
ISBN：9787302129066　软件工程(叶俊民　编著)
ISBN：9787302141006　人工智能教程(金聪　等编著)
ISBN：9787302130666　离散数学(李俊锋　等编著)
ISBN：9787302137801　计算机控制——基于 MATLAB 实现(肖诗松　等编著)
ISBN：9787302132042　数字信号处理——原理与算法实现(刘明　等编著)
ISBN：9787302143338　计算机网络技术及应用教程(杨青　等编著)
ISBN：9787302160694　大学计算机基础教程(杨青　等编著)
ISBN：9787302167327　微机组成与组装技术及应用教程(崔建群　等编著)
ISBN：9787302167334　高级语言程序设计与应用教程(陈静　等编著)
ISBN：9787302168119　数字媒体技术导论(刘清堂　等编著)
ISBN：9787302170655　信息工程科技英语导论(瞿少成　等编著)

即将出版教材

数据结构(C 语言版)(魏开平　等编著)
数据结构教学辅导与实验(魏开平　等编著)
操作系统原理(叶俊民　编著)
软件体系结构教程(叶俊民　编著)
非线性编辑原理与技术(左明章　等编著)
多媒体技术原理与应用(刘清堂　等编著)
单片机原理及接口技术(彭文辉　等编著)
计算机组成原理(陈利　等编著)

更详细的教材介绍请登录清华大学出版社网站 http://www.tup.com.cn 查询。
联系人：魏江江　E-mail：weijj@tup.tsinghua.edu.cn　电话：010-62770175-4604

高等学校教材·计算机科学与技术

编审委员会成员

（按地区排序）

清华大学	周立柱　教授
	覃　征　教授
	王建民　教授
	刘　强　副教授
	冯建华　副教授
北京大学	杨冬青　教授
	陈　钟　教授
	陈立军　副教授
北京航空航天大学	马殿富　教授
	吴超英　副教授
	姚淑珍　教授
中国人民大学	王　珊　教授
	孟小峰　教授
	陈　红　教授
北京师范大学	周明全　教授
北京交通大学	阮秋琦　教授
北京信息工程学院	孟庆昌　教授
北京科技大学	杨炳儒　教授
石油大学	陈　明　教授
天津大学	艾德才　教授
复旦大学	吴立德　教授
	吴百锋　教授
	杨卫东　副教授
华东理工大学	邵志清　教授
华东师范大学	杨宗源　教授
	应吉康　教授
东华大学	乐嘉锦　教授
上海第二工业大学	蒋川群　教授
浙江大学	吴朝晖　教授
	李善平　教授
南京大学	骆　斌　教授
南京航空航天大学	秦小麟　教授
南京理工大学	张功萱　教授

南京邮电学院	朱秀昌	教授
苏州大学	龚声蓉	教授
江苏大学	宋余庆	教授
武汉大学	何炎祥	教授
华中科技大学	刘乐善	教授
中南财经政法大学	刘腾红	教授
华中师范大学	王林平	副教授
	魏开平	副教授
	叶俊民	教授
国防科技大学	赵克佳	教授
	肖　侬	副教授
中南大学	陈松乔	教授
	刘卫国	教授
湖南大学	林亚平	教授
	邹北骥	教授
西安交通大学	沈钧毅	教授
	齐　勇	教授
长安大学	巨永峰	教授
西安石油学院	方　明	教授
西安邮电学院	陈莉君	教授
哈尔滨工业大学	郭茂祖	教授
吉林大学	徐一平	教授
	毕　强	教授
长春工程学院	沙胜贤	教授
山东大学	孟祥旭	教授
	郝兴伟	教授
山东科技大学	郑永果	教授
中山大学	潘小轰	教授
厦门大学	冯少荣	教授
福州大学	林世平	副教授
云南大学	刘惟一	教授
重庆邮电学院	王国胤	教授
西南交通大学	杨　燕	副教授

出版说明

改革开放以来，特别是党的十五大以来，我国教育事业取得了举世瞩目的辉煌成就，高等教育实现了历史性的跨越，已由精英教育阶段进入国际公认的大众化教育阶段。在质量不断提高的基础上，高等教育规模取得如此快速的发展，创造了世界教育发展史上的奇迹。当前，教育工作既面临着千载难逢的良好机遇，同时也面临着前所未有的严峻挑战。社会不断增长的高等教育需求同教育供给特别是优质教育供给不足的矛盾，是现阶段教育发展面临的基本矛盾。

教育部一直十分重视高等教育质量工作。2001 年 8 月，教育部下发了《关于加强高等学校本科教学工作，提高教学质量的若干意见》，提出了十二条加强本科教学工作提高教学质量的措施和意见。2003 年 6 月和 2004 年 2 月，教育部分别下发了《关于启动高等学校教学质量与教学改革工程精品课程建设工作的通知》和《教育部实施精品课程建设提高高校教学质量和人才培养质量》文件，指出“高等学校教学质量和教学改革工程”是教育部正在制定的《2003—2007 年教育振兴行动计划》的重要组成部分，精品课程建设是“质量工程”的重要内容之一。教育部计划用五年时间（2003—2007 年）建设 1500 门国家级精品课程，利用现代化的教育信息技术手段将精品课程的相关内容上网并免费开放，以实现优质教学资源共享，提高高等学校教学质量和人才培养质量。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展、顺应并符合新世纪教学发展的规律、代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻

性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。首批推出的特色精品教材包括:

(1) 高等学校教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2) 高等学校教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 高等学校教材·电子信息——高等学校电子信息相关专业的教材。

(4) 高等学校教材·软件工程——高等学校软件工程相关专业的教材。

(5) 高等学校教材·信息管理与信息系统。

(6) 高等学校教材·财经管理与计算机应用。

清华大学出版社经过20多年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

E-mail: dingl@tup.tsinghua.edu.cn

前言

信息安全涉及的知识面很广，本书的目标是力图向读者系统地介绍信息安全的基本原理与技术。全书主要由下面几个部分组成。

第一部分：信息安全的数学基础。这一部分介绍了信息安全所需要的数学知识，包括数论、代数基础、计算复杂性理论和单向函数等。

第二部分：信息安全的基本理论与技术。包括密码技术、认证、数字签名和访问控制等。

第三部分：信息安全技术在网络安全上的应用。这一部分重点介绍了 PKI 技术、网络安全协议。

第四部分：系统安全技术这一部分简单介绍了保障系统安全的防火墙技术和入侵检测技术。

信息安全涉及许多复杂的概念和技术。为了处理这种复杂性，本书从两个方面让读者“看透”信息安全基本技术。一是从整体上让读者了解其外貌，从全局的角度向读者揭示信息安全研究的基本内容和基本技术，本书的章节安排体现了这一点；二是在局部方面向读者展示每一章应该学些什么以及它们的作用等(如导读部分)。

本书作者多年从事信息安全课程的教学和研究，了解学生的需要，因此本书始终从读者的角度进行编写的。每一章的导读部分介绍了本章的知识要点、作用以及它们之间的联系。在正文中用大量的事例来帮助读者理解重点知识和难点知识。

为了方便教师授课，我们还专门整理了本书的课件以及本书习题的全部答案。

本书由郭亚军整体规划和统稿，郭亚军编写了第 1、2、3、4 章，宋建华编写了第 6、7、9、10 章，李莉编写了第 5、8 章。本书在编写过程中参考了国内外许多文献和书籍，在此，编者对原作者表示真诚的感谢！

本书的出版得到了中国博士后基金(20070410953)和华中师范大学教学研究项目(2007004)的资助。在本书的编写过程中得到了许多同行的热情帮助和支持，得到了清华大学出版社编辑们的关心和帮助，在此一并表示衷心的谢意。

由于作者水平有限，书中难免有不足之处，敬请读者提出宝贵意见。

作　者

2008 年 7 月

目录

第1章 引 言

本章导读

- 本章主要介绍安全攻击、安全机制、安全服务、安全需求和安全目标，以及它们之间的关系。最后介绍了一般安全模型以及网络安全协议。
- 安全攻击分为被动攻击和主动攻击。被动攻击的目的是获得传输的信息，不对信息作任何改动；主动攻击则意在篡改或者伪造信息。
- 安全机制是阻止安全攻击及恢复系统的机制。
- 安全服务是加强数据处理系统和信息传输的安全性的一种服务，安全服务是利用一种或多种安全机制阻止安全攻击。
- 用户所有的安全要求的实现就达到了用户的安全目标；不同的安全服务的联合能够实现不同的安全需求。
- 安全问题主要存在于网络传输过程中以及对信息系统的访问，本章给出了这两类安全模型。
- TCP/IP 参考模型的安全性是通过在各层增加一些安全协议来实现。

近十年来，信息技术和信息产业得到快速发展，与信息技术相关的各个学科和产业如微电子、通信和计算机科学与工程等受到各国政府、企业界和学术界的高度重视。现代的信息系统形式多种多样，除了我们日常生活必需的信息以外，还包括一些十分重要的信息，如政府或企业高度机密的信息、机构和个人的产权信息等。如果信息系统受到攻击致使系统瘫痪甚至崩溃或者某些重要信息被泄露进而被利用，会造成很大损失。

因特网的发展使用户之间的信息交换越来越方便，同时也使恶意攻击越来越容易。从国家计算机网络应急技术处理协调中心(CNCERT/CC)2006 年的网络安全工作报告中可以发现，每年接收到的安全事件越来越多。2004 年为 4485 件，2005 年为 9112 件，2006 年为 26476 件。事件类型主要有网络仿冒、网页篡改、网页恶意代码、拒绝服务攻击、病毒、木马和蠕虫等。2006 年我国大陆地区约 4.5 万个 IP 地址的主机被植入木马；约 1 千多万个 IP 地址的主机被植入僵尸程序；大陆被篡改网站总数达到 24477 个。现在的攻击具有一些更可怕特征，如发动攻击所需要的技能越来越低，检测攻击越来越复杂，攻击的破坏性也越来越大。因此，需要大量的技术和工具来抵抗这些攻击。

信息安全主要研究能够抵抗各种攻击的技术。在过去的几十年里，信息安全经历了几个阶段，每个阶段的侧重点不同，但本质一致。计算机出现之前，主要靠物理安全和管理政策保护信息的安全性，这个阶段信息安全主要研究如何对信息保密。在计算机出现后，信息安全则主要研究计算机安全，即研究如何用一些工具来保护计算机系统自身的安全，保护计算机中的数据并阻止黑客攻击。国际标准化组织 ISO 将计算机安全定义为数据处理系统建立和采用的技术上和管理上的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。在计算机网络出现以后，信息在传输、处理、存储时都存在安全