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

信息安全原理及应用

熊　平　主　编

朱天清　副主编

清华大学出版社

高等学校教材

计算机科学与技术

信息安全原理及应用

熊　平　主编

朱天清　副主编

清华大学出版社

北京

内 容 简 介

本书共15章。第1章介绍信息安全的基本概念、目标和研究内容；第2章介绍密码学的基本概念，是信息安全的基础理论；第3～4章介绍两种重要的密码实现体制，即对称密码体制和公钥密码体制；第5～7章介绍了密码学理论的应用机制，分别是消息认证、身份认证与数字签名、密钥管理；第8章介绍访问控制技术；第9～10章从安全技术人员的角度介绍网络攻击技术和恶意代码分析；第11～12章介绍两种应用广泛的安全防护系统，即防火墙和入侵检测系统；第13章从网络体系结构上分别介绍网络层、传输层及应用层的安全协议；第14章介绍评估信息系统安全的国内外标准；第15章编制了8个信息安全实验，使读者通过实际操作加深对基础理论与技术的理解。

本书可作为信息安全、计算机应用、信息管理等相关专业本科生或研究生的教材和参考书，也可供从事安全技术和管理工作人员参考。

图书在版编目(CIP)数据

信息安全原理及应用/熊平主编. —北京：清华大学出版社，2009.5
(高等学校教材·计算机科学与技术)
ISBN 978-7-302-19107-0

Ⅰ. 信…　Ⅱ. 熊…　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197113号

责任编辑：丁　岭　李玮琪
责任校对：李建庄
责任印制：王秀菊
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 刷 者：北京市世界知识印刷厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：20.75　**字　数**：499千字
版　　次：2009年5月第1版　　**印　　次**：2009年5月第1次印刷
印　　数：1～3000
定　　价：36.00元

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

当今时代是信息的时代，信息成为社会发展的重要战略资源。信息的安全交换、存储和保障能力成为综合国力和经济竞争力的重要组成部分。我国政府把信息安全技术与产业列为今后一段时期的优先发展领域。

信息安全教育在我国高等教育中正在逐步展开。教育部继2001年批准在武汉大学开设信息安全本科专业之后，又先后批准了几十所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。另外，教育部2005年7号文件出台了“关于进一步加强信息安全学科、专业建设和人才培养工作的意见”，并将建立国家网络信息安全保障体系确定为国家发展的基本战略目标之一。

目前有关信息安全的书籍很多，其中不乏精品。然而，由于信息安全所涵盖的内容非常广泛，要想在一部教材中介绍信息安全的方方面面是不切实际的，在内容安排上都会做适当的取舍。笔者在实际教学过程中发现，正是这种取舍造成目前信息安全基础教材普遍存在两个方面的缺憾。其一，对密码学基础理论缺乏比较系统的介绍。密码学是信息安全的基石，信息安全理论与技术大多建立在密码学基础之上，但遗憾的是，目前信息安全基础教材大多突出密码学的应用，而忽视了对基础知识的介绍。其二，没有与信息安全理论相应的实验内容。实验教学是信息安全基础教学中不可缺少的内容，但目前的信息安全基础教材要么没有实验内容，要么有实验内容但对实验环境要求较高，在实际教学中没有可操作性。因此，在本书的内容编排上，力求理论与实践相结合，包含了密码学基础理论、密码学应用机制、实用安全技术及相关实验内容，使读者更清晰地从信息安全体系的层面掌握信息安全的基础理论和应用技术。

本书内容共分为15章。

第1章介绍信息安全的基本概念、发展历史、实现的目标以及主要的研究内容。

第2～4章介绍密码学基础理论：第2章对密码学进行综述，介绍了密码学的基本概念、密码系统及其分类，并对经典密码学的基本方法进行了阐述；第3章介绍对称密码体制，包括分组密码和序列密码，并对代表性的对称密码DES、AES、RC4等进行了阐述；第4章对公钥密码体制进行了介绍，包括数论基础、公钥密码体制的基本原理，并对代表性的RSA密码及其他公钥密码进行了阐述。

第5～7章介绍密码学应用机制：第5章介绍了用于解决信息安全完整性的消息

认证机制，重点包括消息认证码和 Hash 函数；第 6 章介绍了身份认证与数字签名技术，其中，身份认证是实现访问控制的基本前提，而数字签名则用于解决信息安全的抗否认性。第 7 章介绍了密钥管理机制，包括对称密码体制下的密钥管理和公钥密码体制下的密钥管理，重点是公钥证书的管理及 PKI。

第 8～12 章介绍安全保障技术：第 8 章介绍访问控制技术，包括访问控制策略和常用的网络访问控制方法；第 9 章介绍了常用的网络攻击技术和相应的防范方法；第 10 章介绍了恶意代码分析技术，根据对恶意代码的分类，逐一介绍了各类恶意代码及其防范方法；第 11 章介绍了防火墙系统，包括防火墙的原理与分类、基本技术，以及在实际部署中的体系结构；第 12 章介绍了入侵检测系统，包括入侵检测系统的分类和主要检测方法，并以 Snort 为例阐述了入侵检测系统的基本结构。

第 13 章介绍安全协议，对 TCP/IP 体系结构进行了安全分析，并从网络体系结构上分别介绍了网络层、传输层及应用层的安全协议 IPSec、SSL 和 SET。

第 14 章介绍了评估信息系统安全的国内外标准，包括 TCSEC、CC 及国内标准。

第 15 章是实验部分，由 8 个实验组成，包括数据加密、认证和签名、访问控制、网络扫描、协议分析、远程控制、防火墙及入侵检测系统的配置等内容。

本书由熊平担任主编，朱天清参与了各章内容的讨论、安排与编写工作。

由于作者自身水平有限，本书定有不妥甚至错误之处，恳请读者及专家提出宝贵意见。

编　者

2009 年 2 月

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室　　计算机与信息分社营销室　收
邮编：100084　　电子邮件：jsjjc@tup. tsinghua. edu. cn
电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：信息安全原理及应用
ISBN：978-7-302-19107-0

个人资料

姓名：_____　年龄：_____所在院校/专业：_____

文化程度：_____　通信地址：_____

联系电话：_____　电子信箱：_____

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：

□很满意 □满意 □一般 □不满意　改进建议_____

您对本书印刷质量的满意度：

□很满意 □满意 □一般 □不满意　改进建议_____

您对本书的总体满意度：

从语言质量角度看　□很满意 □满意 □一般 □不满意

从科技含量角度看　□很满意 □满意 □一般 □不满意

本书最令您满意的是：

□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？(可附页)

_____

_____

您希望本书在哪些方面进行改进？(可附页)

_____

_____

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至jsjjc@tup. tsinghua. edu. cn 咨询，也可以到清华大学出版社主页（http://www. tup. com. cn 或 http://www. tup. tsinghua. edu. cn）上查询。

高等学校教材·计算机科学与技术
系列书目

书　号	书　名	作　者
9787302103400	C++程序设计与应用开发	朱振元等
9787302135074	C++语言程序设计教程	杨进才等
9787302140962	C++语言程序设计教程习题解答与实验指导	杨进才等
9787302124412	C语言程序设计教程习题解答与实验指导	王敬华等
9787302162452	Delphi程序设计教程(第2版)	杨长春
9787302091301	Java面向对象程序设计教程	李发致
9787302159148	Java程序设计基础	张晓龙等
9787302158004	Java程序设计教程与实验	温秀梅等
9787302133957	Visual C#.NET程序设计教程	邱锦伦等
9787302118565	Visual C++面向对象程序设计教程与实验	温秀梅等
9787302112952	Windows系统安全原理与技术	薛质
9787302133940	奔腾计算机体系结构	杨厚俊等
9787302098409	操作系统实验指导——基于Linux内核	徐虹等
9787302118343	Linux操作系统原理与应用	陈莉君等
9787302148807	单片机技术及系统设计	周美娟等
9787302097648	程序设计方法解析——Java描述	沈军等
9787302086451	汇编语言程序设计教程	卜艳萍等
9787302147640	汇编语言程序设计教程(第2版)	卜艳萍等
9787302147626	计算机操作系统教程——核心与设计原理	范策等
9787302092568	计算机导论	袁方等
9787302137801	计算机控制——基于MATLAB实现	肖诗松等
9787302116134	计算机图形学原理及算法教程(Visual C++版)	和青芳
9787302137108	计算机网络——原理、应用和实现	王卫亚等
9787302126539	计算机网络安全	刘远生等
9787302116790	计算机网络实验	杨金生
9787302153511	计算机网络实验教程	李馥娟等
9787302143093	计算机网络实验指导	崔鑫等
9787302118664	计算机网络基础教程	康辉
9787302139201	计算机系统结构	周立等
9787302134398	计算机原理简明教程	王铁峰等
9787302111467	计算机组成原理教程	张代远
9787302130666	离散数学	李俊锋等
9787302104292	人工智能(AI)程序设计(面向对象语言)	雷英杰等
9787302141006	人工智能教程	金聪等
9787302136064	人工智能与专家系统导论	马鸣远
9787302093442	人机交互技术——原理与应用	孟祥旭等
9787302129066	软件工程	叶俊民

书　　号	书　　名	作　　者
9787302162315	软件体系结构设计	李千目等
9787302117186	数据结构——Java 语言描述	朱战立
9787302093589	数据结构(C 语言描述)	徐孝凯等
9787302093596	数据结构(C 语言描述)学习指导与习题解答	徐孝凯等
9787302079606	数据结构(面向对象语言描述)	朱振元等
9787302099840	数据结构教程	李春葆
9787302108269	数据结构教程上机实验指导	李春葆
9787302108634	数据结构教程学习指导	李春葆
9787302112518	数据库系统与应用(SQL Server)	赵致格
9787302149699	数据库管理与编程技术	何玉洁
9787302155409	数据库技术——设计与应用实例	岳昆
9787302160151	数据库系统教程	苑森淼等
9787302106319	数据挖掘原理与算法	毛国君
9787302126492	数字图像处理与分析	龚声蓉
9787302146032	数字图像处理	李俊山等
9787302146032	数字图像处理	李俊山等
9787302124375	算法设计与分析	吕国英
9787302103653	算法与数据结构	陈媛
9787302150343	UNIX 系统应用编程	姜建国等
9787302136767	网络编程技术及应用	谭献海
9787302150503	网络存储导论	姜宁康等
9787302148845	网络设备配置与管理	甘刚等
9787302071310	微处理器(CPU)的结构与性能	易建勋
9787302109013	微机原理、汇编与接口技术	朱定华
9787302140689	微机原理、汇编与接口技术学习指导	朱定华
9787302145257	微机原理、汇编与接口技术实验教程	朱定华
9787302128250	微机原理与接口技术	郭兰英
9787302084471	信息安全数学基础	陈恭亮
9787302128793	信息对抗与网络安全	贺雪晨
9787302112358	组合理论及其应用	李凡长
9787302154211	离散数学	吴晟 等

目 录