信息安全专业系列教材

信息安全概论

（第2版）

Xinxi Anquan Gailun

牛少彰　崔宝江　李剑　编著

北京邮电大学出版社
www.buptpress.com

信息安全专业系列教材

信息安全概论

（第 2 版）

牛少彰　崔宝江　李　剑　编著

北京邮电大学出版社
·北京·

内 容 简 介

本书在第1版的基础上进行了修改和完善，并补充了一些信息安全近几年的研究成果，全书内容更加翔实和新颖。本书全面介绍了信息安全的基本概念、原理和知识体系，主要内容包括信息保密技术、信息认证技术、PKI与PMI认证技术、密钥管理技术、访问控制技术、网络的攻击与防范、系统安全、网络安全技术和信息安全管理等内容。

本书内容全面，既有信息安全的理论知识，又有信息安全的实用技术。文字流畅，表述严谨，并包括信息安全方面的一些最新成果。本书可作为高等院校信息安全相关专业的本科生、研究生的教材或参考书，也可供从事信息处理、通信保密及与信息安全有关的科研人员、工程技术人员和技术管理人员参考。

图书在版编目(CIP)数据

信息安全概论/牛少彰，崔宝江，李剑编著. —2版. —北京：北京邮电大学出版社，2007
ISBN 978-7-5635-1486-1

Ⅰ.信… Ⅱ.①牛…②崔…③李… Ⅲ.信息系统—安全技术 Ⅳ.TP309

中国版本图书馆CIP数据核字(2007)第116573号

书　　名：信息安全概论(第2版)
作　　者：牛少彰　崔宝江　李　剑
责任编辑：张珊珊
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路10号(邮编：100876)
北方营销中心：电话：010-62282185　传真：010-62283578
南方营销中心：电话：010-62282902　传真：010-62282735
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京市梦宇印务有限公司
开　　本：787 mm×960 mm　1/16
印　　张：17.25
字　　数：370千字
印　　数：1—5 000册
版　　次：2004年4月第1版　2007年9月第2版　2007年9月第1次印刷

ISBN 978-7-5635-1486-1/TN·509　　定　价：28.00元

信息安全专业系列教材（第2版）

编 委 会

第 2 版总序

发展 21 世纪中国信息安全要靠教育，而搞好信息安全教育就需要好的教材。2004 年，北京邮电大学信息安全中心完成了第一套信息安全专业本科系列教材，该套教材被评为“北京市高等教育精品教材立项项目”，而后又被教育部列入“普通高等教育‘十五’国家级规划教材”。至今，三年多的时间过去了，这套教材在信息安全专业的教学中发挥了重要的作用，起到了较好的教学效果，受到教师和学生的好评。

在这三年中，我们始终致力于包括专业建设、课程建设、师资建设、教材建设、实训基地建设、实验室建设及校企就业（创业）平台建设等在内的信息安全本科专业的全面建设。2005 年，作为组长单位，我们完成了教育部“信息安全专业规范研究”和“信息安全学科专业发展战略研究”课题；召开了“全国高校本科‘信息安全专业规范与发展战略研究’成果发布与研讨会”；在国内第一次制定了信息安全专业规范，从知识领域、知识单元和知识点三个层次构建学科专业教学的知识体系；由通识教育内容、专业教育内容和综合教育内容三大部分构建课程参考体系；采用顶层设计的方法构建了带有实践性环节的教学体系；在国内第一次较全面地提出信息安全学科专业教学改革与创新研究的发展思路和政策建议，成果提交教育部教学指导委员会，对于引导高等学校信息安全学科专业教学改革与建设，指导信息安全学科专业评估，促进信息安全学科专业教学规范建设与管理，提高专业教育质量和水平有重要的作用。多所举办信息安全专业的高校都参照课题成果调整了自己的教学计划、课程体系和实验方案。

积极搭建信息安全专业校际交流平台。组织成立了“全国信息安全本科教材编写委员会”和“全国信息安全本科专业师资交流与培训互助组”。主持召开了“全国信息安全专业教学经验交流和师资培训研讨会”及“全国信息安全专业实验室建设和实验课程教学经验交流研讨会”。在四川绵阳建设了占地两万六千多平方米的全国信息安全专业本科生实习实训基地，接收了来自全国近 30 所高校的本科生进入该基地参加丰富多彩的实训。

努力建设精品课程。召开了“全国高校信息安全专业精品课程建设经验交流会议”，来自全国各地高校的专家齐聚北邮，介绍与交流了精品课程建设的经验。组织建设了全国第一批信息安全实验室，并且编写出版了信息安全实验指导教材，2007 年，我们的《现代密码学》课程申报了北京市精品课程，已经被专家评审通过，目前正在申报 2007 年度“国家精品课程”。

三年多的时间过去了，信息安全的教育和产业都取得了丰硕的成果，随着信息安全向更高层次的发展，其趋势已经从基础的网络层建设开始向内容层建设过渡。为适应信息安全教育的发展需要，积极探索培养创新型高素质人才，我们按照制定的学科发展战略和专业规范的精神，结合近几年的教学实践，对原信息安全专业本科系列教材进行了全面修订。这次修订不仅对原来的系列教材在第1版的基础上进行修改和完善，还补充了信息安全最新的研究成果，使教材的内容更加翔实和新颖。同时，在原有体系的基础上又增加了一些新的课程教材。在新修订的系列教材中，目前有《信息安全概论(第2版)》、《现代密码学及其应用》、《网络安全(第2版)》、《信息安全管理》、《计算机病毒原理与防治(第2版)》、《数字版权管理》、《计算机系统安全》、《网络安全实验教程》、《信息安全专业科技英语》、《防火墙、入侵检测与VPN》、《对称密码学及其应用》、《信息安全导论》等12本教材。随着信息安全专业教学的需要，今后还将不断有新的教材补充进来。希望通过对内容的精心组织和设计能促进信息安全课程的建设，同时涌现出更多的信息安全精品课程。

在这次修订中，我们组织了强大的师资队伍，将多次讲授相关课程的教师充实到本次修订队伍中。经过反复研讨，本着理论与实际相结合的原则，对原来的系列教材进行了较大的修改和扩充，我们希望这套新修订的系列教材能够满足国内各类高校信息安全本科专业以及相关方向的不同需求。

虽然我们在这次修订中投入了很大精力，但是由于水平有限，时间仓促，且信息安全专业的发展速度非常快，不足之处和错误在所难免，我们衷心期望使用和关心该系列教材的师生，继续对新的系列教材提出宝贵意见和建议。

本系列教材也是国家重点基础研究发展计划(973)(课题编号：2007CB310704 和2007CB311203)资助的成果，并在积极申报“普通高等教育‘十一五’国家级规划教材”。

在本系列教材的修订过程中，得到了北京邮电大学出版社的大力支持，同时也得到了北京邮电大学信息安全中心成员的支持与配合，在此一并表示感谢。

教授、博士生导师、全国政协委员

杨义先

第 1 版前言

随着信息社会的到来，人们在享受信息资源所带来的巨大的利益的同时，也面临着信息安全的严峻考验。信息安全已经成为世界性的现实问题，信息安全问题已威胁到国家的政治、经济、军事、文化、意识形态等领域，同时，信息安全问题也是人们能否保护自己个人隐私的关键。信息安全是社会稳定安全的必要前提条件。本书全面介绍了信息安全的基本概念、原理和知识体系，主要内容包括信息保密技术、信息认证技术、访问控制技术、密钥管理技术、数据库安全、网络安全技术、信息安全标准和信息安全管理等内容。

本书内容全面，既有信息安全的理论知识，又有信息安全的实用技术，并包括信息安全方面的一些最新成果。本书可作为高等院校信息安全相关专业的本科生、研究生的教材或参考书，也可供从事信息处理、通信保密及与信息安全有关的科研人员、工程技术人员和技术管理人员参考。本书的教学时数约为 34 学时，每章后面均有小结并配有习题。

在本书编写的过程中，赵义斌参加了第 2 章和第 3 章初稿的编写，李志虎参加了第 7 章的编写，刘歆编写了第 9 章，郭春碌参加了第 6 章的编写，翟军华参加了第 8 章的编写，张晓芬、邓雁城、郭延龄、谢正程参加了书稿的讨论。此外，刘歆还在本书的整理和校对方面做了许多工作。

在本书的编写过程中，还得到了很多老师同学的关心和帮助。北京邮电大学出版社为本书的出版付出了大量的工作，借此表示衷心感谢。

限于编者水平有限，书中难免有疏漏和错误之处，恳请读者批评指正。

作　者

第 2 版前言

本书第 1 版在使用过程中得到了多方肯定，取得了较好的教学效果。结合近几年的教学实践，我们在第 1 版的基础上进行了修改和完善，并根据信息安全近几年的研究成果进行了补充，使全书内容更加翔实和新颖。全书进一步梳理了信息安全的基础理论部分，增加了对信息安全实际工作的指导，尽可能全面地反映信息安全进几年来的最新理论和技术成果。

本书除了保持第 1 版的内容外，还增加了以下内容和特色：

(1) 除全面介绍了信息安全的基本概念、原理和知识体系外，从信息安全技术、安全管理和政策法规 3 个方面论述了信息安全，并增加信息安全的实施指导，介绍了信息安全的防范原理和主要模型。

(2) 除详细论述了信息安全的核心技术，包括密码技术、信息认证技术、密钥管理技术以及信息安全研究的新领域——信息隐藏——外，对身份认证技术进行了较为详细的介绍，将 PKI 认证技术独立成为一章。

(3) 在网络安全技术部分，除修改原有的访问控制技术、防火墙技术、虚拟专用网技术、入侵检测技术和计算机病毒防治外，还介绍了目前普遍关心的内网安全技术方面的内容。

(4) 将原来的数据库安全技术改为系统安全，除修改原有的数据库存安全外，对整个的系统安全进行了论述。

(5) 为了更好地做好信息安全的防范工作，做到知己知彼，增加了对网络攻击内容的介绍。

(6) 对整个信息安全管理部分进行整合，将原来的信息安全标准合并到信息安全管理部分，介绍了信息安全管理的标准和整个流程。

通过补充和完善，使本书在同类教材中具有内容全面、题材新颖、全面反映近年来的最新成果、理论联系实际等特色。

在本书第 2 版中，第 8 章由崔宝江编写，第 10 章由牛少彰和李剑共同编写，其余各章由牛少彰编写，全书最后由牛少彰统稿。

信息安全概论第 2.版在新版的信息安全专业系列教材中将继续起到承上启下的作

用，对读者继续了解密码学在信息安全中的作用以及进入后续专题的学习进行衔接。同时，本书又自成体系，非信息安全专业可单独使用，用于全面了解信息安全领域的有关理论、概念、技术原理、实际工作指导和最新研究成果。

虽然我们尽力进行修订和创新，但是由于编者水平有限，时间仓促，书中难免有疏漏和错误之处，恳请使用和关心该教材的广大读者批评指正。

作　者

目　录

第 3 章 信息认证技术

第 9 章 网络安全技术

第1章

概　述

随着现代通信技术的迅速发展和普及，特别是随着通信与计算机相结合而诞生的计算机互联网络全面进入千家万户，信息的应用与共享日益广泛，且更为深入。世界范围的信息革命激发了人类历史上最活跃的生产力，人类开始从主要依赖物质和能源的社会步入物质、能源和信息三位一体的社会。各种信息化系统已成为国家基础设施，支撑着电子政务、电子商务、电子金融、科学研究、网络教育、能源、通信、交通和社会保障等方方面面，信息成为人类社会必需的重要资源。

与此同时，信息的安全问题日渐突出，情况也越来越复杂。从大的方面来说，信息安全问题已威胁到国家的政治、经济、军事、文化、意识形态等领域，因此很早就有人提出了“信息战”的概念并将信息武器列为继原子武器、生物武器、化学武器之后的第四大武器。从小的方面来说，信息安全问题也涉及到人们能否保护个人的隐私。

信息安全已成为社会稳定安全的必要前提条件。

信息安全，即关注信息本身的安全，以防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的不可靠或无法处理等问题，使得我们在最大限度地利用信息为我们服务的同时而不招致损失或使损失最小。

1.1　信息的定义、性质和分类

在人类社会的早期，人们对信息的认识比较肤浅和模糊，对信息的含义没有明确的定义。到了20世纪特别是中期以后，科学技术的发展，特别是信息科学技术的发展，对人类社会产生了深刻的影响，迫使人们开始探讨信息的准确含义。

1.1.1　信息的概念

1928年，哈特莱(L. V. R. Hartley)在《贝尔系统技术杂志》(BSTJ)上发表了一篇题