信息安全专业系列教材

网络安全

（第2版）

Wangluo Anquan

徐国爱　张　淼　彭俊好　编著

北京邮电大学出版社
www.buptpress.com

信息安全专业系列教材

网络安全

（第2版）

徐国爱　张　森　彭俊好　编著

北京邮电大学出版社
·北京·

内 容 简 介

本书作为信息安全系列教材之——《网络安全》的再版，在广泛吸纳读者意见和建议的基础上，不仅仍定位于对网络安全基本原理、主流技术和相关应用的讲解，还从内容安排和内容选取方面做了全面的优化。和第1版相比，本书的内容更为系统、内容组织更为精致，并适当加入了网络安全相关技术最近几年发展的内容。

全书内容分为4个部分，第一部分在指出网络安全基本概念的基础上，对以TCP/IP为基础的网络体系结构做了深入分析，这是讲解网络安全知识的基础，内容涉及第1、2章；第二部分是第3章，这部分以网络安全威胁的性质不同为主线，系统对网络安全威胁进行了分析，但其中并未讨论相应的防范技术；第三部分从身份认证、访问控制、安全通信和入侵检测等几个方面系统介绍网络安全最经典的方法技术，内容包括第4～7章；第四部分包括全书的最后两章，内容涉及网络安全的两个热点——无线网络安全和网络安全管理。每章后面配有习题以巩固相关知识，另外配有大量的参考文献。

本书可作为高等院校计算机、通信、信息等专业研究生和高年级本科生的教材，也可作为计算机、通信、信息等领域研究人员和专业技术人员的参考书。

图书在版编目(CIP)数据

网络安全/徐国爱，张淼，彭俊好编著. —2版. —北京：北京邮电大学出版社，2007
ISBN 978-7-5635-1414-4

Ⅰ.网… Ⅱ.①徐…②张…③彭… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2007)第129641号

书　　名：网络安全(第2版)
作　　者：徐国爱　张　淼　彭俊好
责任编辑：方　瑜
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：北京忠信诚胶印厂
开　　本：787 mm×960 mm　1/16
印　　张：18.5
字　　数：404千字
印　　数：1—5 000册
版　　次：2007年9月第2版　2007年9月第1次印刷

ISBN 978-7-5635-1414-4/TP·284　　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

前　言

随着网络技术应用在社会政治、经济、文化、生产等领域的普及，社会信息化建设已初具规模，这给我国经济发展和社会进步带来了前所未有的机遇。然而，问题的另外一面，信息安全问题不仅阻碍网络技术应用的进一步普及，而且还影响现有的应用，直接给国家和人民带来经济或名誉的损害，网络和相关信息系统价值的进一步挖掘更是受到制约，信息安全已成为制约社会信息化发展的瓶颈。网络安全作为信息安全的一个主要方面，已受到业内专家和学者的广泛关注。提高全社会的网络安全意识，已成为保障我国信息化建设长期稳定健康发展的关键工作之一。

北京邮电大学信息安全中心从 1984 年以来，一直专注于信息安全领域的理论和应用研究，中心先后承担过数项国家级信息安全相关课题的研究，并成功地将其中的大部分成果实现商业转化，为国家信息化建设做出了一定的贡献。信息安全系列是我们专为信息安全教学和科研推出的一款系列书籍，内容涵盖信息安全领域的方方面面。系列教材既可作为高等院校信息安全及相关专业研究生和高年级本科生的教材用，也可作为相关专业人员全面参考的系列手册。

本书作为信息安全系列教材之——《网络安全》的再版，在广泛吸纳读者意见和建议的基础上，不仅仍定位于对网络安全基本原理、主流技术和相关应用的讲解，还从内容安排和内容选取上做了全面的优化。和第 1 版相比，本书的内容更为系统、内容组织更为精致，并适当加入了网络安全相关技术最近几年发展的内容。全书内容分为 4 个部分，第一部分在指出网络安全基本概念的基础上，对以 TCP/IP 为基础的网络体系结构做了深入分析，这是讲解网络安全知识的基础，内容涉及第 1、2 章；第二部分是第 3 章，这部分以网络安全威胁的性质不同为主线，系统对网络安全威胁进行了分析，但其中并未讨论相应的防范技术；第三部分从身份认证、访问控制、安全通信和入侵检测等几个方面系统介绍网络安全最经典的方法技术，内容包括第 4～7 章；第四部分包括全书的最后两章，内容涉及网络安全的两个热点——无线网络安全和网络安全管理。

本书由北京邮电大学信息安全中心组织编写。孙学磊参与了第 2、3 章的编写，刘凡凡参与了第 4、5 章的编写，陈爱国参与了第 6、7 章的编写，赵凯参与了第 8 章的编写；陈

思璐、梁婕、冯博、笋大伟、陈晓光、何景根、张明剑、骆春山等共同参与了资料收集、整理工作；全书由徐国爱统稿，张淼、彭俊好协助。此外，本书得到了胡正名教授、杨义先教授、钮心忻教授和罗群副教授等的大力支持和指导，他们对书中的内容提出了宝贵的意见，在此一并表示衷心的感谢。本书在编写过程中，除引用了作者自身的研究内容和成果之外，还大量参考了众多国内外优秀论文、书籍以及互联网上公布的相关资料，尽量在书后面的参考文献中列出，但由于互联网上资料数量众多、出处杂乱，可能无法将所有文献一一注明出处，对这些资料的作者表示由衷的感谢，同时声明，原文版权属于原作者。

本书作为教材，教师在讲授时可以根据学时安排做出一些取舍。本书全部讲授建议40学时；如果只有34学时，建议将第1章或第8章作为选讲内容。

网络安全是一门应用性很强的学科，在网络大规模普及的今天已得到了长足的发展，本书尝试对此领域的理论和技术做一些归纳，以期有益于读者。由于作者的水平有限，书中难免有一些缺点和错误，真诚希望读者不吝赐教，以期再版修订。

作 者

目　录

第 4 章 网络身份认证

第1章

绪　论

本章概要介绍网络安全基本概念、威胁形式和相关技术的发展状况，作为全书的引子。

1.1　网络安全概述

网络安全有许多“别名”，信息安全、信息网络安全、网络信息安全、网络安全威胁、网络安全攻防、网络安全服务和网络安全技术等都是在不同应用场合和不同用户对象中对网络安全的说法。在不引起错误理解的情况下，为描述问题方便，本书在不同章节可能会引用其中任何一种说法。网络安全包括一切解决或缓解计算机网络技术应用过程中存在的安全威胁的技术手段或管理手段，也包括这些安全威胁本身及相关的活动。网络安全的不同“别名”代表网络安全不同角度和不同层面的含义，网络安全威胁和网络安全技术是网络安全含义最基本的表现。

网络安全威胁是指计算机和网络系统所面临的、来自已经发生的安全事件或潜在安全事件的负面影响，这两种情况通常又分别称为现实威胁和潜在威胁。网络安全威胁的种类繁多，对计算机和网络系统带来的负面影响各不相同，网络安全威胁的原因也形形色色。

解决或缓解网络安全威胁的手段和方法就是网络安全技术，网络安全技术应用具备的安全功能称为网络安全服务，有时也称为网络安全特性。机密性、完整性、可用性是基本的网络安全特性，可认证性、可核查性和可靠性是基本安全特性在当前应用中突出和延伸的重要特性。各特性基本含义如下：

- 机密性：信息不泄露给非授权的用户、实体或过程，或供其利用的特性。
- 完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中不被修改、不被破坏和丢失的特性。