普通高等教育“十一五”国家级规划教材
教育部普通高等教育精品教材
中央网信办暨教育部评选的**国家网络安全优秀教材奖**

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

网络空间安全重点规划丛书

顾问委员会主任：沈昌祥　编委会主任：封化民

网络安全
——技术与实践（第3版）

刘建伟 王育民 编著

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材
教育部普通高等教育精品教材
中央网信办暨教育部评选的**国家网络安全优秀教材奖**

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

网络空间安全重点规划丛书

网络安全
——技术与实践（第3版）

刘建伟 王育民 编著

清华大学出版社
北京

内 容 简 介

全书共分 3 篇 15 章。第 1 篇为网络安全基础，共 3 章，主要讨论网络安全的基础知识；第 2 篇为密码学基础，共 5 章，详细讨论各种密码算法和技术，特别深入地介绍我国已公布的标准密码算法；第 3 篇为网络安全技术与应用，共 7 章，深入介绍网络实践中常用的一些网络安全技术及产品。

本书内容丰富，概念清楚，语言精练。在网络安全基本知识和密码学理论的阐述上，力求深入浅出，通俗易懂；在网络安全技术与产品的讲解上，力求理论联系实际，面向具体应用。本书在每章的后面提供了思考题和练习题，以便于读者巩固所学的知识点；在书末也提供了大量的参考文献，便于有兴趣的读者继续深入学习有关内容。

本书可作为信息安全、信息对抗技术、密码学等专业的本科生教材，也可以用作网络空间安全一级学科的研究生教材。对于广大网络安全工程师、网络管理员和 IT 从业人员来说，本书也是很好的参考书和培训教材。

图书在版编目（CIP）数据

网络安全：技术与实践/刘建伟，王育民编著. —3 版. —北京：清华大学出版社，2017
（网络空间安全重点规划丛书）
ISBN 978-7-302-46758-8

Ⅰ. ①网… Ⅱ. ①刘… ②王… Ⅲ. ①计算机网络–网络安全–研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2017）第 042441 号

责任编辑：张　民
封面设计：常雪影
责任校对：白　蕾
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　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
课 件 下 载：http://www.tup.com.cn,010-62795954
印 刷 者：三河市君旺印务有限公司
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**30.5　　**字　　数：**696 千字
版　　次：2005 年 6 月第 1 版　　2017 年 5 月第 3 版　　**印　　次：**2017 年 5 月第 1 次印刷
印　　数：1～2000
定　　价：59.50 元

产品编号：070984-01

网络空间安全重点规划丛书

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，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，又批准了多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。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。系列教材的作者都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

该系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到系列教材中，以进一步满足大家对外版书的需求。“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会

暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办,清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006年教育部给武汉大学下达了"信息安全专业指导性专业规范研制"的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下,项目组团结一致,努力工作,克服困难,历时5年,制定出我国第一个信息安全专业指导性专业规范,于2012年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审,并且已经得到武汉大学等许多高校的实际使用。2013年,新一届"教育部高等学校信息安全专业教学指导委员会"成立。经组织审查和研究决定,2014年以"教育部高等学校信息安全专业教学指导委员会"的名义正式发布《高等学校信息安全专业指导性专业规范》(由清华大学出版社正式出版)。

2015年6月,国务院学位委员会、教育部出台增设"网络空间安全"为一级学科的决定,将高校培养网络空间安全人才提到新的高度。2016年6月,中央网络安全和信息化领导小组办公室(下文简称中央网信办)、国家发展和改革委员会、教育部、科学技术部、工业和信息化部及人力资源和社会保障部六大部门联合发布《关于加强网络安全学科建设和人才培养的意见》(中网办发文[2016]4号)。为贯彻落实《关于加强网络安全学科建设和人才培养的意见》,进一步深化高等教育教学改革,促进网络安全学科专业建设和人才培养,促进网络空间安全相关核心课程和教材建设,在教育部高等学校信息安全专业教学指导委员会和中央网信办资助的网络空间安全教材建设课题组的指导下,启动了"网络空间安全重点规划丛书"的工作,由教育部高等学校信息安全专业教学指导委员会秘书长封化民校长担任编委会主任。本规划丛书基于"高等院校信息安全专业系列教材"坚实的工作基础和成果、阵容强大的编审委员会和优秀的作者队伍,目前已经有多本图书获得教育部和中央网信办等机构评选的"普通高等教育本科国家级规划教材"、"普通高等教育精品教材"、"中国大学出版社图书奖"和"国家网络安全优秀教材奖"等多个奖项。

"网络空间安全重点规划丛书"将根据《高等学校信息安全专业指导性专业规范》(及后续版本)和相关教材建设课题组的研究成果不断更新和扩展,进一步体现科学性、系统性和新颖性,及时反映教学改革和课程建设的新成果,并随着我国网络空间安全学科的发展不断完善,力争为我国网络空间安全相关学科专业的本科和研究生教材建设、学术出版与人才培养做出更大的贡献。

我们的E-mail地址是:zhangm@tup.tsinghua.edu.cn,联系人:张民。

"网络空间安全重点规划丛书"编审委员会

前言

为了加强网络空间安全专业人才的培养，教育部已正式批准在 29 所大学设立网络空间安全一级学科博士点，全国已有 128 所高校相继设立了信息安全或信息对抗本科专业。为了提高网络空间安全人才培养质量，急需编写出版一批高水平的网络空间安全优秀教材。

作者作为教育部高等学校信息安全专业教学指导委员会委员和中国密码学会理事，参与编写了教育部高等学校信息安全专业教学指导委员会编制的《高等学校信息安全专业指导性专业规范》。在本书的编写过程中，力求使本教材的知识体系和知识点符合《高等学校信息安全专业指导性专业规范》的要求，并加入了对国产密码算法的阐述。

全书共分 3 篇 15 章。第 1 篇为网络安全基础，共 3 章，主要介绍网络安全的基本概念、计算机网络的基础知识，以及 TCP/IP 协议族的安全性。第 2 篇为密码学基础，共 5 章，主要介绍密码学中的各种密码算法和协议。第 3 篇为网络安全技术与应用，共 7 章，主要介绍 PKI/CA、密钥管理、无线网络安全，以及防火墙、VPN、IDS 和身份认证等网络安全技术与应用。

本书主要有以下特色：

（1）基本概念清晰，表述深入浅出。在基本概念的阐述上，力求准确而精练；在语言的运用上，力求顺畅而自然。作者尽量避免使用晦涩难懂的语言描述深奥的理论和技术知识，而是借助大量的图表进行阐述。

（2）内容全面，涵盖密码学和网络安全技术。本书既介绍了现代密码学的知识，又阐述了网络安全的理论与技术，特别适合于将密码学和网络安全合并为一门课进行授课的高校。

（3）理论与实践相结合。针对某些网络安全技术和产品，本书给出相应的网络安全解决方案，从而使读者能够深入而全面地了解网络安全技术的具体应用，以提高读者独立分析问题和解决问题的能力。

（4）每章后面都附有精心斟酌和编排的思考题。通过深入分析和讨论思考题中所列问题，读者可加强对每章所学基本概念和理论的理解，从而进一步巩固所学的知识。

（5）本书详细列出了大量的参考文献。这些参考文献为网络空间安全学科的研究生和密码学、信息安全、信息对抗技术等专业的本科生，以及其他网络安全技术人员提供了深入研究相关专题的途径和资料。

本书可作为密码学、信息安全和信息对抗技术等专业的本科生教材和网络空间安全学科的研究生教材，也可以作为网络安全工程师的参考书和培训教材。

本书由刘建伟主编，刘建伟和王育民对全书进行了审校。第1章由刘建伟编著，第2章由杜瑞颖编著，第3章由杜瑞颖和刘建伟编著，第11～14章由刘建伟编著，第4～10章和第15章由王育民和刘建伟编著。

感谢伍前红教授、尚涛副教授、毛剑老师、关振宇老师、修春娣老师、张宗洋老师给予的支持与帮助。感谢陈杰、刘巍然、毛可飞、周星光、王蒙蒙、何双羽、程东旭、刘哲、李大伟、程昊苏、钟林、王朝、姜勇、周林志等博士研究生，以及宋晨光、苏航、冯伯昂、周修文、陶芮、夏丹枫、樊一康、齐婵、刘懿中、王培人、马寒军、雷奇、李珂、崔键、史福田、杜岗、王沁、梁智等硕士研究生在书稿的整理过程中给予作者的大力支持与帮助。

由于作者水平所限，书中难免会存在错误和不妥之处。敬请广大读者朋友批评指正。

作　者

于北京

目 录

第 1 篇　网络安全基础

第 2 篇 密码学基础

第3篇　网络安全技术与应用