普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类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

顾问委员会主任：沈昌祥 编委会主任：肖国镇

网络安全——技术与实践（第2版）

刘建伟 王育民 编著
寇卫东 审

http://www.tup.com.cn

Information Security

根据教育部高等学校信息安全类专业教学指导委员会制订的《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

高等院校信息安全专业系列教材

教育部高等学校信息安全类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

顾问委员会主任：沈昌祥 编委会主任：肖国镇

网络安全——技术与实践

（第2版）

刘建伟 王育民 编著
寇卫东 审

http://www.tup.com.cn

根据教育部高等学校信息安全类专业教学指导委员会制订的
《信息安全专业指导性专业规范》组织编写

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，主要讨论了与网络安全有关的基础知识；第 2 篇为密码学基础，共 5 章，详细地讨论了网络安全中所涉及的各种密码技术；第 3 篇为网络安全技术与应用，共 7 章，深入介绍了在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保密学理论的阐述上，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，具有很强的实用性。本书在每章的后面提供了大量思考题和练习题，以便于读者巩固课堂上所学的知识；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、密码学等专业的本科生和研究生的网络安全课程教材，也可以作为网络安全工程师、网络管理员和计算机用户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. —2 版. —北京：清华大学出版社，2011.6
ISBN 978-7-302-25721-9

Ⅰ. ①网…　Ⅱ. ①刘…　②王…　Ⅲ. ①计算机网络－安全技术　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 107437 号

责任编辑：张　民　薛　阳
责任校对：焦丽丽
责任印制：何　芊

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：010-62795954，jsjjc@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**：28.5　　**字　　数**：653 千字
版　　次：2011 年 6 月第 2 版　　**印　　次**：2011 年 6 月第 1 次印刷
印　　数：1～4000
定　　价：43.00 元

产品编号：039291-01

高等院校信息安全专业系列教材

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，共同指导“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。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数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。

本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。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。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本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

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将起到重要的指导和推动作用。“高等院校信息安全专业系列教材”将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下，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，并随着我国信息安全学科的发展不断修订和完善。

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

清华大学出版社

前言

随着各种网络技术的飞速发展和网络应用的普及，网络安全问题日益突出，社会对网络安全人才的需求也日益增长。许多大学都开设了信息安全或信息对抗专业，以培养信息安全和信息对抗方面的专业人才；一些从事网络安全产品开发的工程师，也迫切需要掌握网络安全方面的专业知识；对于计算机用户和网管人员来说，他们除了需要系统地学习网络安全方面的基础知识外，还需要深入了解网络安全技术和产品。因此，无论是大学教师还是网络安全工程师，都迫切需要一本理论联系实践的好书。

作者作为教育部高等学校信息安全类专业教学指导委员会委员和中国密码学会理事，参与编写了教育部的《信息安全类专业课程设置规范》。本教材所涉及的网络安全知识体系和知识点，是根据研究型大学《信息安全类专业课程设置规范》而定的。此外，作者长期从事网络安全的教学、科研和产品开发，积累了比较丰富的网络安全教学、科研和实践经验。作者想通过此书，把这些经验与读者分享。

本书共分 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，以及网络低层协议和高层协议的安全性。第 2 篇为密码学基础，共 5 章，主要介绍网络安全中所涉及的密码技术。第 3 篇为网络安全技术与应用，共 7 章，主要介绍一些常用的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。在本教材中，作者尽量避免使用烦琐的语言描述晦涩难懂的理论知识，而是借助大量的图表来阐述深奥的理论。

（2）内容翔实，重点突出。本书既简要介绍了密码学的主要内容，又重点阐述了网络安全的理论、技术与应用。在网络安全知识体系和知识点的选择上，充分参考了教育部高等学校信息安全类专业教学指导委员会制定的《信息安全类专业课程设置规范》。

（3）理论与实践相结合。针对某些网络安全技术和产品，本教材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，以提高读者在未来的网络安全实践中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）本书后面列出了大量的参考文献。这些参考文献为信息安全或信息对抗专业的本科生、研究生和其他技术人员提供了深入研究相关专题的途径和资料。

在本书的编写中，作者对第1版中的部分内容进行了修正，并增补了近年来密码学和网络安全领域出现的一些新理论和新技术。

本书可作为信息安全、信息对抗、密码学等专业的本科生和研究生的教材，也可以作为广大网络安全工程师、网管员和计算机用户的参考书和网络安全培训教材。

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

特别感谢北京航空航天大学张其善教授在各方面给予作者的关怀、支持与帮助。张教授无论在做人还是在做事方面，都是作者学习的楷模。在此，作者想由衷地表达对张其善教授深深的敬意。

感谢张斯芸、袁延荣、张雨霏等同学对第2版书稿进行了仔细的整理和校对，感谢尚涛老师、毛剑老师、修春娣老师、魏凌波博士后给予的支持与帮助，感谢杨友福、邱修峰、刘建华、陈杰、刘哲等博士生，感谢刘书明、王冠、田园、李为宇、孙钰、韩庆同、张薇、宋璐、刘靖、陈庆余、赵朋川、徐先栋、张斯芸、袁延荣、周炼赤、王世帅、樊勇、张雨霏、马妍等硕士生在第2版书稿的整理过程中给予的帮助。感谢朱云茂硕士对参考文献和图表进行了认真的整理和校对。

感谢王琼副译审对全书的文字进行了校对，为提高本书的出版质量做出了贡献。

感谢北京航空航天大学电子信息工程学院的全体老师和朋友们多年来给予作者的关心、支持和帮助。

作　者

2011年6月

于北京

目录

第 1 篇　网络安全基础

第 2 篇 密码学基础