高等院校信息安全专业系列教材

网络安全——技术与实践

刘建伟摇王育民摇编著
寇卫东摇审

清 华 大 学 出 版 社
北　京

内 容 简 介

全书共分 猿篇 员缘章。第 员篇为网络安全基础，共 猿章，主要讨论了网络安全的基础知识，并从网络协议安全性的角度出发，阐述了当今计算机网络中存在的安全威胁 第 圆篇为保密学基础，共 缘章，较详细地讨论了网络安全中涉及的各种密码技术 第 猿篇为网络安全实践，共 苑章，主要介绍了网络安全实践中一些比较重要的产品及其技术应用。

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方面，力求深入浅出，通俗易懂 在网络安全产品方面，力求理论与实践相结合，具有很强的实用性。特别是在每章的后面提供了很多习题，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地学习有关内容。

本书可以作为高等院校信息安全、通信、计算机等专业的研究生和本科生教材，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用书，或作为网络安全培训教材。

图书在版编目（悦陨孕）数据

网络安全：技术与实践 刘建伟，王育民编著 郾—北京：清华大学出版社，圆园园缘
（高等院校信息安全专业系列教材）
陨杂月晕 苑原猿园圆原员园远缘园原缘

Ⅰ郾网… 摇Ⅱ郾①刘… ②王… 摇Ⅲ郾计算机网络 原安全技术 原高等学校 原教材摇Ⅳ郾栽孕猿怨猿郾园愿

中国版本图书馆 悦陨孕数据核字（圆园园缘）第 园愿怨缘愿怨号

出 版 者：清华大学出版社
澡贼贼责：鄄鄄憎憎憎郾贼怎责郾糟燥皂郾糟灶
社 总 机：园员园原远圆苑苑园员苑缘
地 址：北京清华大学学研大厦
邮 编：员园园园愿源
客户服务：园员园原远圆苑苑远怨远怨
组稿编辑：张摇民
文稿编辑：霍志国
印 刷 者：清华大学印刷厂
装 订 者：北京市密云县京文制本装订厂
发 行 者：新华书店总店北京发行所
开 本：员愿缘伊圆远园摇印张：猿愿摇字数：苑圆员千字
版 次：圆园园缘年 远月第 员版摇圆园园缘年 远月第 员次印刷
书 号：陨杂月晕 苑原猿园圆原员园远缘园原缘辕栽孕· 苑员怨愿
印 数：员~ 猿园园园
定 价：源愿郾园园元

高等院校信息安全专业系列教材

编审委员会

序

摇摇在社会信息化的进程中，信息已成为社会发展的重要资源，信息安全也成为21世纪国际竞争的重要战场。为了保护国家的政治利益和经济利益，各国政府都非常重视信息和网络安全，信息安全已成为一个世纪性、全球性的研究课题。

我国的信息安全事业正在蓬勃发展，国家领导高度重视，各部门通力合作、统筹规划，大大加快了我国信息安全产业发展的步伐。随着信息安全产业的快速发展，社会对信息安全人才的需求在不断增加，在高等教育领域大力推进信息安全的专业化教育，将是国家在信息安全领域掌握自主权、占领先机的重要举措。

目前，许多大学和科研院所已设办了信息安全专业或是开设了相关课程。很高兴中国计算机学会教育专业委员会和清华大学出版社在近期联合组织了一系列信息安全专业的研讨活动。他们以严谨负责的态度，认真组织全国各高校和科研院所的专家、学者，共同研讨信息安全专业的教育方法和课程体系，并在进行大量前瞻性研究工作的基础上，启动了“高等院校信息安全专业系列教材”的编写工作。这套教材将是我国信息安全专业的第一套完整、权威的教材，相信可以对全国的高等院校信息安全专业的建设起到很好的促进作用。

希望中国计算机学会教育专业委员会和清华大学出版社能够将这个研究课题一直做下去，也希望这套教材能够取得成功并不断完善，以促进各高等院校培养出更多、更好的信息安全专门人才，为我国的信息安全事业作出更大的贡献。

何德全

中国工程院院士

高等院校信息安全专业系列教材编审委员会名誉主编

出版说明

摇摇圆员世纪是信息时代，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，国家对信息安全人才的需求量不断增加，但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，以满足社会的需求。为此，教育部继 圆园园员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、通信工程、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何德全院士担任名誉主编，著名学者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，确定了编写教材的作者，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作出更大的贡献。

我们的 [illegible] 地址是：[illegible] 联系人：张民。

中国计算机学会教育专业委员会
清华大学出版社

本书序

摇摇随着网络技术的迅猛发展，国家在网络化建设方面取得了令人欣慰的进展。网络已经深入到国家的政治、经济、文化及国防建设的各个领域，遍布社会生活的每个角落。近年来电子商务及电子政务应用的普及更加提高了网络在国计民生中的地位，网络已经直接关系到现代社会的运行和发展。另一方面，网络中的安全问题正在危及网络的各种应用，从而严重影响网络的进一步发展。网络安全问题已经成为人们高度关注的焦点问题。

“危机”：有危就有机。网络安全的危机为研究网络安全问题和开发网络安全产品的人们带来了机遇。刘建伟博士和王育民教授两位学者通过自己的行动把“危”转化成了“机”。他们的《网络安全——技术与实践》是一本为满足国家网络安全人才培养和技术研究的迫切需求而编写的教材。

全书整体结构合理，层次清晰，结合当前网络安全的最新发展深入浅出地系统介绍了网络安全的有关知识，有利于读者理解和学习。本书从介绍网络安全的基本概念开始，进而介绍网络安全中所涉及的密码技术，最后介绍了网络安全实践中常见的一些技术和产品。作者在本书中不但写进了网络安全理论研究的成果，同时注重对网络安全实践的有关问题进行讨论，此外还收入并且讨论了网络安全领域近年来出现的新技术。

我认为本书对高等院校、科研院所的师生，对从事网络安全的工程师、网管员和计算机用户都是一本不可多得的好书。这是因为网络安全专业的研究生、本科生可以从本书中系统全面地学习到网络安全理论和实践两方面的知识；从事网络安全产品开发的工程师可以从本书中掌握他们迫切需要的网络安全方面的专业知识；计算机用户和网管人员可以从本书中系统地了解他们需要的网络安全方面的基础知识。特别要提到的是本书精心安排的习题，读者可以通过回答这些习题迅速熟练地掌握每章的基本内容和方法。这些习题不仅有利于帮助读者加深对每章内容的理解，也是对每章重点内容的再次总结。另外，本书列出的大量参考文献为有兴趣的读者提供了深入研究相关专题的途径和资料。

本书的作者都是网络安全领域的专家，一位是网络安全领域的资深教授，一位

是网络安全公司的老总。特别是王育民教授，他是国内最早从事信息和网络安全研究的资深大家之一。我有幸在 圆猿世纪 愿园年代成为他和肖国镇以及王新梅等老师组织的密码学讨论班的学生，几位大师的教诲，使我终身受益。不论是十多年的海外留学生涯的漂流奋斗，还是如今的“海归”时代的为国贡献，只要在这个领域工作，就一定会回想起 愿园年代初的那个密码学讨论班。

现在为老师的著作写序，一方面深感荣幸，另一方面也心存忧虑，害怕自己在一页纸的序言中很难将这样一本无论是在内容上还是组织上都堪称网络安全领域的优秀之作总结归纳给读者。但我相信，只要读者自己用心去读，就会了解和欣赏它。我也相信本书的出版必将对网络安全领域的人才培养和网络安全技术的不断创新产生深远的影响。

寇卫东摇谨识

圆猿园缘年 员月

寇卫东，国际知名电子商务和信息安全专家，现任 阿里巴巴软件集团大中华区普及计算部总架构师、美国马里兰大学兼职教授；曾任综合业务网国家重点实验室主任、西安电子科技大学计算机学院院长，香港大学电子商业研究所首席研究员、副总监，加拿大 阿里巴巴高级研究中心首席研究员等职；曾多次担任电子商务和信息安全领域的国际会议大会主席和程序委员会主席，多个国际学术期刊编委、副主编、客座主编等职；出版了 苑本英文专著，发表了 苑园余篇论文，拥有 猿项美国专利，源项加拿大专利，以及多项美国待批专利。

前言

摇摇随着计算机网络技术的飞速发展，以及电子商务及电子政务应用的普及，网络安全问题日益突出。为了保护网络中传输信息的可靠性、保密性和有效性，许多研究机构、大学和企业都在致力于网络安全的技术研究和产品开发。许多大学都开设了网络安全专业，以培养网络安全方面的专门人才；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络管理员来说，他们除了需要了解某些网络安全产品的具体使用之外，也需要系统地了解网络安全方面的基础知识。因此，人们迫切需要一本理论结合实践的书，深入浅出地系统介绍网络安全的有关知识。然而，目前出版的许多网络安全教材，要么偏重于晦涩难懂的密码学理论的讨论，要么偏重于网络安全技术和产品的一般概念介绍，往往难尽人意。

正是在以上背景下，作者萌生了编写此书的念头。长期以来，作者一直从事网络安全方面的教学、技术研究和产品开发，积累了一些实践经验。作者想通过此书，把这些经验与读者分享。

本书分猿篇，共员缘章。第员篇为网络安全基础，共猿章，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；第圆篇为保密学基础，共缘章，主要介绍网络安全中涉及的密码技术；第猿篇为网络安全实践，共苑章，主要介绍网络安全实践中常见的一些技术和产品。作者编写此书时，力求避免烦琐的理论阐述，尽可能地将理论和实践结合在一起，用很大的篇幅着重于网络安全实践的有关问题的讨论。此外，作者还将近年来网络安全领域出现的一些新的技术，如无线网络安全技术和蜜罐技术等，在书中也进行了讨论。

本书另一个鲜明的特点是列出了大量的参考文献。这些参考文献为网络安全专业的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。

本书可作为高等院校信息安全、计算机、通信等专业的研究生、本科生教材，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用书，或作为网络安全培训教材。

本书由刘建伟博士主编，刘建伟博士和王育民教授对全书进行了审校。

第 员章由刘建伟编著，第 圆~ 猿章由刘建伟和姜斌斌编著，第 源~ 员园章，第 员缘章由王育民和刘建伟编著，第 员员章由屠晓鲲和刘建伟编著，第 员圆章由原涛和刘建伟编著，第 员猿章由王鸿鹏和刘建伟编著，第 员源章由王锋和刘建伟编著。姜斌斌对第 员圆~ 员源章进行了审校。

北京航空航天大学的张其善教授及其博士生为本书的写作提供了许多素材，张其善教授的支持和鼓励也给了作者完成此书的力量和勇气。作者在此致以深切的感谢。

感谢空军工程大学的朱云茂硕士对全书的参考文献和图表进行了详细的校对，他为提高参考文献的准确性进行了艰苦而又细致的工作。

感谢王琼翻译对全书的文字进行了校对，并改正了原稿件中存在的许多语法错误，为提高本书的出版质量做出了贡献。

此外，感谢刘涛、陈四强、杜汇光、文中领对本书的部分内容进行了补充和修改。感谢西安电子科技大学的博士生姜正涛和硕士生袁素春。姜正涛仔细阅读了本书的初稿，并提出不少修改意见，袁素春为本书的编写提供了许多英文资料。

最后，感谢海信集团有限公司的周厚健董事长和于淑珉总裁，以及海信研发中心的领导和北京海信数码科技有限公司的全体员工。没有他们的鼓励和支持，没有海信提供的宽松研究环境和条件，就不可能有此书的诞生。

作摇者

圆园园缘年 员月

目 录

第 员篇摇网络安全基础

第圆篇摇保密学基础