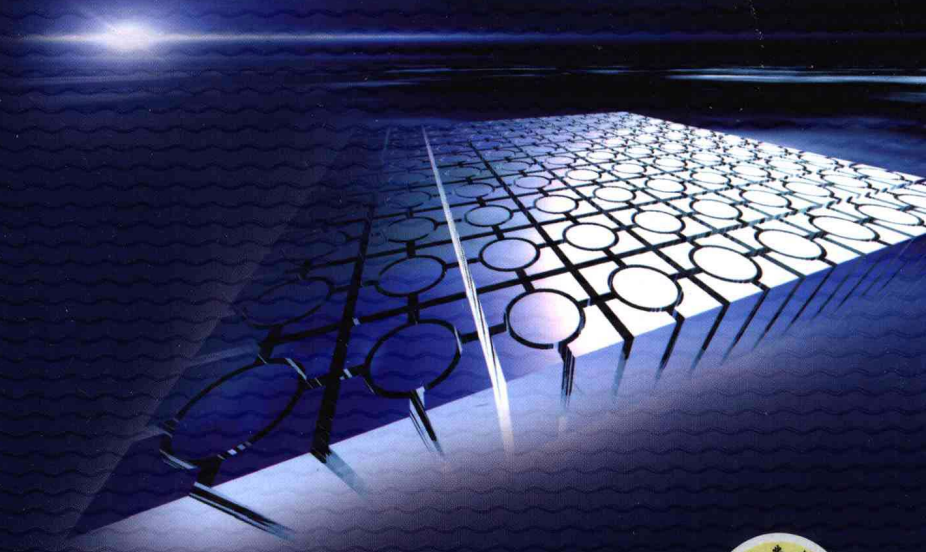
高等院校规划教材
计算机科学与技术系列

网络安全技术及应用实践教程

贾铁军　主　编
王　坚　副主编
沈学东　苏庆刚　王小刚　参　编



机械工业出版社
CHINA MACHINE PRESS

网络安全技术及应用实践教程

高等院校规划教材·计算机科学与技术系列

网络安全技术及应用实践教程

贾铁军　主　编
王　坚　副主编
沈学东　苏庆刚　王小刚　参　编

机械工业出版社

本书主要内容包括：网络安全技术基础实验；无线网安全技术、网络安全管理技术、黑客攻防与入侵检测技术、身份认证与访问控制技术、密码与加密技术、病毒及恶意软件防护技术、防火墙技术、操作系统与站点安全技术、数据与数据库安全技术、电子商务网站安全技术及应用实践等，以及包括“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等技术实验。

书中的知识要点、实验、案例分析、练习测试等，便于师生进行实践教学、课外延伸学习和网络安全综合解决方案实践练习。另外，还提供了选做实验和不同的任务项目，可供不同专业的学生选择使用。

本书可以作为《网络安全技术及应用》配套的辅助教材，也可以单独使用。

本书可作为本科院校计算机类、信息类、电子商务类和管理类专业的信息安全相关课程的教材，也可作为培训教材及参考用书，还可作为高职院校相关专业选修教材。

图书在版编目（CIP）数据

网络安全技术及应用实践教程 / 贾铁军主编. —北京：机械工业出版社，2009.2

（高等院校规划教材·计算机科学与技术系列）

ISBN 978-7-111-25929-9

Ⅰ. 网… Ⅱ. 贾… Ⅲ. 计算机网络－安全技术－高等学校－教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2009）第 010392 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

责任编辑：唐德凯

责任印制：邓 博

北京四季青印刷厂印刷 （三河市兴旺装订厂装订）

2009 年 2 月·第 1 版第 1 次印刷

184mm×260mm·17.25 印张·421 千字

0001－3000 册

标准书号：ISBN 978-7-111-25929-9

定价：28.00 元

凡购本书，如有缺页，倒页，脱页，由本社发行部调换

销售服务热线电话：（010）68326294 68993821

购书热线电话：（010）88379639 88379641 88379643

编辑热线电话：（010）88379753 88379739

出 版 说 明

计算机技术的发展极大地促进了现代科学技术的发展，明显地加快了社会发展的进程。因此，各国都非常重视计算机教育。

近年来，随着我国信息化建设的全面推进和高等教育的蓬勃发展，高等院校的计算机教育模式也在不断改革，计算机学科的课程体系和教学内容趋于更加科学和合理，计算机教材建设逐渐成熟。在“十五”期间，机械工业出版社组织出版了大量计算机教材，包括“21 世纪高等院校计算机教材系列”、“21 世纪重点大学规划教材”、“高等院校计算机科学与技术‘十五’规划教材”、“21 世纪高等院校应用型规划教材”等，均取得了可喜成果，其中多个品种的教材被评为国家级、省部级的精品教材。

为了进一步满足计算机教育的需求，机械工业出版社策划开发了“高等院校规划教材”。这套教材是在总结我社以往计算机教材出版经验的基础上策划的，同时借鉴了其他出版社同类教材的优点，对我社已有的计算机教材资源进行整合，旨在大幅提高教材质量。我们邀请多所高校的计算机专家、教师及教务部门针对此次计算机教材建设进行了充分的研讨，达成了许多共识，并由此形成了“高等院校规划教材”的体系架构与编写原则，以保证本套教材与各高等院校的办学层次、学科设置和人才培养模式等相匹配，满足其计算机教学的需要。

本套教材包括计算机科学与技术、软件工程、网络工程、信息管理与信息系统、计算机应用技术以及计算机基础教育等教材系列。其中，计算机科学与技术系列、软件工程系列、网络工程系列和信息管理与信息系统系列是针对高校相应专业方向的课程设置而组织编写的，体系完整，讲解透彻；计算机应用技术系列是针对计算机应用类课程而组织编写的，着重培养学生利用计算机技术解决实际问题的能力；计算机基础教育系列是为大学公共基础课层面的计算机基础教学而设计的，采用通俗易懂的方法讲解计算机的基础理论、常用技术及应用。

本套教材的内容源自致力于教学与科研一线的骨干教师与资深专家的实践经验和研究成果，融合了先进的教学理念，涵盖了计算机领域的核心理论和最新的应用技术，真正在教材体系、内容和方法上做到了创新。同时本套教材根据实际需要配有电子教案、实验指导或多媒体光盘等教学资源，实现了教材的“立体化”建设。本套教材将随着计算机技术的进步和计算机应用领域的扩展而及时改版，并及时吸纳新兴课程和特色课程的教材。我们将努力把这套教材打造成为国家级或省部级精品教材，为高等院校的计算机教育提供更好的服务。

对于本套教材的组织出版工作，希望计算机教育界的专家和老师能提出宝贵的意见和建议。衷心感谢计算机教育工作者和广大读者的支持与帮助！

机械工业出版社

前　言

随着计算机网络技术的快速发展和电子银行、电子商务、电子政务的广泛应用，计算机网络已经深入到国家的政治、经济、文化和国防建设的各个领域，遍布现代信息化社会工作和生活的各个层面，“数字化经济”和全球电子交易一体化正在形成。计算机网络安全不仅关系到国计民生，还与国家安全密切相关，不仅涉及到国家政治、军事和经济各个方面，而且影响到国家的安全和主权。随着计算机网络的广泛应用和网络数据传输量的急剧增大，网络安全的重要性更为突出。

随着信息技术的发展与应用，网络安全的内涵不断地延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。网络安全是一个综合与交叉的学科领域，要综合利用数学、物理、通信和计算机等诸多学科的长期知识积累和最新技术成果，不断发展和完善。为满足高校应用型人才培养的需要，我们编写了本书。本书主要作者20多年来，在高校从事计算机网络与安全等领域的教学、科研和学科专业管理工作，特别是在公安院校多次主持过计算机网络安全方面的科研项目研究，积累了大量宝贵的实践经验。

本书既可以作为与《网络安全技术及应用》配套的辅助教材，也可以单独使用。书中的知识要点（内容提要与学习指导）、实验、案例分析、练习测试等，便于师生的实践教学、课外延伸学习和网络安全综合解决方案练习。另外，还提供了选做实验和不同的任务项目，可供不同专业的学生选择使用。书中带“*”部分为选学内容。

全书共分12章，重点介绍了计算机网络安全技术基础实验；无线网络安全技术及应用；入侵检测技术实验、黑客攻击与防范技术实验；身份认证与访问控制技术实验；网络安全中的密码与加密技术实验；病毒及恶意软件的防护技术实验；防火墙技术及应用实验；操作系统与站点安全技术实验、数据与数据库安全技术实验；电子商务网站安全技术及应用等实验。书中还增加了大量的案例分析及有关研究成果，以便于教学和实际应用。

本书重点介绍了最新成果、防范技术、处理技术及方法和实际应用。其特点如下：

1）内容先进，结构新颖。书中吸收了国内外大量的新知识、新技术、新方法和国际通用准则，注重科学性、先进性、操作性。

2）注重实用性和特色。坚持“实用、特色、规范”原则，突出实用及学生的素质能力培养。在内容安排上将理论知识与实际应用有机结合。

3）资源配套，便于教学。为了方便师生教学，本书提供了同步实验、学习指导、练习测试等。

本书由贾铁军任主编，统稿并编写第1～6、11、12章，王坚任副主编并编写第8章、全书练习测试及解答和课件制作，王小刚编写第7章、苏庆刚编写第9章，沈学东编写第10章。邹飞和于淼参加了本书大纲的讨论、审校等工作。邹佳芹对全书的文字、图表进行了校对编

排、并查阅、整理了大量的资料。

非常感谢对本书编著给予大力支持和帮助的上海电机学院有关领导和同仁。对编著过程中参阅的大量重要文献资料的作者，在此深表谢意。

由于作者水平有限，书中难免存在不妥之处，敬请读者批评指正。

编　者

目　录

第 1 章　网络安全概论

计算机网络安全不仅关系到国计民生，还与国家安全密切相关，不仅涉及到国家政治、军事和经济各个方面，而且影响到国家的安全和主权。因此，现代网络技术中最关键也最容易被忽视的安全性问题，现在已经成为各国关注的焦点，也成为热门研究和人才需求的新领域。只有在法律、管理、技术、道德各个方面采取切实可行的有效措施，共同努力，才能确保实现网络安全。

本章要点

- 网络安全的概念、技术特征、研究目标及内容要点
- 网络面临的威胁及其分析
- 网络安全模型、网络安全保障体系和关键技术
- 安全技术评估标准和准则
- 网络安全设计与建设的原则和步骤
- 构建虚拟局域网与虚拟机实验及本章练习测试

1.1　知识要点

信息安全（Information Security）是指防止信息财产被故意或偶然的非授权泄露、更改、破坏或使信息被非法的系统辨识与控制，确保信息的完整性、保密性、可用性和可控性。信息安全是计算机、通信工程、数学等领域的交叉学科。

信息安全技术（Information Security Technology）是指在信息系统的物理层、应用层，以及对信息自身的保护（数据层）及攻击的层面上，所反映出的对信息自身与信息系统在可用性、机密性与真实性方面的保护与攻击的技术。

信息安全技术在发展过程中经历了通信保密、信息安全、信息保障 3 个阶段。

1.1.1　网络安全概述

1．网络安全的概念及技术特征

（1）网络安全的概念

计算机网络安全（Computer Network Security）简称网络安全，是指利用网络管理控制和技术措施，保证在网络环境中数据的机密性、完整性、网络服务可用性和可审查性受到保护。保证网络系统的硬件、软件及其系统中的数据资源得到完整、准确、连续运行和服务不受到干扰破坏和非授权使用。网络安全问题实际上包括网络的系统安全和信息安全，而保护网络的信息安全是网络安全的最终目标和关键，因此，网络安全的实质是网络的信息安全。

计算机网络安全是一门涉及计算机科学、网络技术、信息安全技术、通信技术、应用数学、密码技术和信息论等多学科的综合性学科，是信息安全学科的重要组成部分。

随着信息技术的发展与应用，信息安全的内涵在不断地延伸和变化，从最初的信息保密

性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。

网络安全需求定义包括网络安全硬件、软件和服务。其中，用于保护计算机信息系统安全的专用硬件和软件属于计算机信息系统安全专用产品。

（2）网络安全的技术特征

网络安全定义中的机密性、完整性、可用性、可控性、不可否认性，反映了信息安全的基本特征和目标，其中前 3 个为信息安全的基本要求。保证信息安全，最根本的就是保证信息安全的基本特征发挥作用。因此，网络信息安全的特征也反映了网络安全的基本属性、要素与技术方面的重要特征。

2．网络安全的研究目标及内容

（1）网络安全研究的目标

网络安全研究的目标是：在计算机和通信领域的信息传输、存储与处理的整个过程中，提供物理上、逻辑上的防护、监控、反应恢复和对抗的能力，以保护网络信息资源的保密性、完整性、可控性和抗抵赖性。网络安全的最终目标是保障网络上的信息安全。解决网络安全问题需要安全技术、管理、法制、教育并举，从安全技术方面解决信息网络安全问题是最基本的方法。

（2）网络安全的内容

网络信息安全包括：操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别等 7 个方面。网络安全所涉及的内容可以概括为实体安全、运行安全、系统安全、应用安全和管理安全 5 个方面。

3．网络安全的威胁

（1）网络安全威胁的现状

网络系统自身的脆弱性、复杂性和开发性等特点，在为其带来发展机遇的同时，也必将带来巨大的风险。人们普遍缺乏网络安全意识，甚至根本没有意识到网络安全的重要性。因而，导致网络存在着先天性的安全漏洞、隐患和威胁。国际上也一直存在着信息安全管理规范和标准不统一的问题。

在网络安全技术的发展过程中，企业和政府对其要求也有差异。企业注重信息和网络安全的可靠性，而政府则更注重信息和网络安全的可管性和可控性。

由于网络安全技术的快速发展，在国内，网络安全产品被夸大和误解的现象在一定程度上普遍存在，防火墙似乎成了网络安全的全部。其中重技术、轻管理和网络安全知识不够普及是主要的问题。据国家计算机网络应急技术处理协调中心 2007 年上半年统计显示，我国被植入木马的主机 IP 超过 2006 年全年，增幅达 50%以上。

【案例 1-1】2008 年元旦期间，一种名为“木马下载器 20480”的病毒在网上现身，这种病毒会下载大量盗号程序，给用户的系统安全和财产带来威胁。另外，国家计算机病毒应急处理中心也曾发出预报，2007 年 12 月 31 日至 2008 年 1 月 6 日将定期发作“求职信”（Worm_Klez.E）病毒，属于电子邮件蠕虫病毒类型。目前，全球的计算机病毒已超过 10 万种，几乎每天都有几种新病毒或病毒变种出现。

【案例 1-2】2007 年底，著名互联网安全公司赛门铁克评出 10 大互联网安全事件：

1）数据窃取。超过 9400 万名用户的 Visa 和 MasterCard 信用卡信息被黑客窃取。

2）Windows Vista 安全问题。微软公司在 2008 年为 Windows Vista 推出了 16 款安全补丁，将来更多的恶意软件会把目光集中在 Vista 身上。

3）垃圾邮件。垃圾邮件比例创下了历史新高。

4）黑客工具成为赚钱工具。不仅黑客的攻击手段越来越高明，而且还通过出售黑客工具获取利润。

5）“钓鱼”式攻击依然肆虐。

6）可信的知名网站成为黑客攻击目标。

7）僵尸程序。一种偷偷安装在用户计算机上使未经授权的用户能远程控制计算机的程序 Bots，成为黑客窃取受保护信息的主要手段。

8）Web 插件攻击。ActiveX 控件是最易遭受攻击的 Web 插件。

9）黑客在网上拍卖软件漏洞。

10）虚拟机安全问题突出。

（2）网络安全的威胁类型

计算机网络安全面临的主要威胁类型及情形如表 1-1 所示。

表 1-1　各种类型网络安全的主要威胁

威胁类型	情况描述
窃听	网络传输信息被窃听
讹传	攻击者获得某些信息后，发送给他人
伪造	攻击者将伪造的信息发送给他人
篡改	攻击者对合法用户之间的通信信息篡改后，发送给他人
非授权访问	通过口令、密码和系统漏洞等手段获取系统访问权
截获/修改	网络系统传输中数据被截获、删除、修改、替换或破坏
拒绝服务攻击	攻击者以某种方式使系统响应减慢甚至瘫痪，阻止用户获得服务
行为否认	通信实体否认已经发生的行为
旁路控制	攻击者发掘系统的缺陷或安全脆弱性
截获	攻击者从有关设备发出的无线射频或其他电磁辐射中提取信息
人为疏忽	已授权人为了利益或由于粗心将信息泄露给未授权人
信息泄露	信息被泄露或暴露给非授权用户
物理破坏	通过计算机及其网络或部件进行破坏，或绕过物理控制非法访问
病毒木马	利用计算机病毒或木马等恶意软件进行破坏或恶意控制他人系统
窃取	盗取系统重要的软件或硬件、信息和资料
服务欺骗	欺骗合法用户或系统，骗取他人信任以便谋取私利
陷阱门	设置陷阱“机关”系统或部件，骗取特定数据以违反安全策略
资源耗尽	故意超负荷使用某一资源，导致其他用户服务中断
消息重发	重发某次截获的备份合法数据，达到信任非法侵权目的
冒名顶替	假冒他人或系统用户进行活动
媒体废弃物	利用媒体废弃物得到可利用信息，以便非法使用
信息战	为国家或集团利益，通过信息战进行网络干扰破坏或恐怖袭击

（3）网络安全威胁的发展趋势

现代计算机病毒技术与黑客技术的结合对信息安全造成更大的威胁。从发展趋势来看，现在的病毒已经由从前的单一传播、单种行为，变成依赖互联网传播，具有电子邮件、文件传染等多种传播方式，融黑客、木马等多种攻击手段于一身的广义的“新病毒”。今后恶意代码、网络安全威胁和攻击机制的发展将具有以下特点：

1）连通性、扩散性、分布广泛性。

2）黑客技术与病毒传播结合。

3）扩散快且更加具有欺骗性。

4）利用系统漏洞和更新将成为病毒有力的传播方式。

5）无线网络技术的发展使远程网络攻击的可能性加大。

6）信息战及各种境内外情报人员将越来越多地通过网络渠道搜集情报和窃取资料。

7）超级蠕虫病毒的大规模扩散。

8）各种攻击技术的隐蔽性增强，常规手段难以识别。

9）分布式计算技术用于攻击的趋势增强，威胁高强度密码的安全性。

10）威胁范围更广泛，甚至一些政府部门的超级计算机资源将成为攻击者利用的跳板。

11）网络管理安全问题日益突出。

有关专家认为，2008 年开始各种计算机病毒将出现一些更为明显的变化特征和趋势，网络安全将面临新的 5 大威胁。

1）服务器端的变异。

2）客制化加壳技术。

3）特定应用的“点杀”技术。

4）季节性的流行网站攻击。

5）“众包”模式。

1.1.2 网络安全风险分析

网络安全的脆弱性是体制性、多层次、多范畴的，从而导致了网络安全机制和功能的复杂性。

1．网络系统安全分析

（1）网络系统特征安全分析

互联网所具有的开放性、国际性和自由性等特征，也给网络带来了不安全性因素，其主要表现为 6 个方面：网络的共享性、网络的开放性、系统漏洞和复杂性、边界的不确定性、传输路径的不确定性和信息的高度聚集性。

（2）网络服务协议安全分析

互联网使用的基础协议 TCP/IP（传输控制协议/网际协议）、FTP（文件传输协议）、E-mail（电子邮件）、RPC（远程进程调用）和 NFS（网络文件系统）等是公开的，因此，存在许多安全漏洞，如协议本身的缺陷、网络应用层服务存在的安全隐患、IP 层通信存在的易欺骗性、系统和网络具有的易被监视性等。

计算机网络的运行机制基于网络协议，不同结点之间的信息交换按照事先约定的固定机制通过协议数据单元来完成。