“十三五”国家重点出版物出版规划项目

上海市普通高等院校优秀教材奖
上海市普通高校精品课程特色教材

高等教育网络空间安全规划教材

网络安全技术及应用

第3版

主编　贾铁军　陶卫东

立体化·新形态教材

双色印刷、二维码

http://www.cmpedu.com

电子课件　教学视频　教学大纲　同步实验

机械工业出版社
CHINA MACHINE PRESS

“十三五”国家重点出版物出版规划项目
上海市普通高等院校优秀教材奖
上海市普通高校精品课程特色教材
核心产品立体化配套建设工程
高等教育网络空间安全规划教材

网络安全技术及应用

第3版·立体化教材

主　编　贾铁军　陶卫东
副主编　俞小怡　罗宜元　彭　浩　王　坚

机械工业出版社

本书主要内容包括：网络安全基础、网络安全技术基础、网络安全体系及管理、黑客攻防与检测防御、密码与加密技术、身份认证与访问控制、计算机及手机病毒防范、防火墙应用技术、操作系统及站点安全、数据库及数据安全、电子商务安全、网络安全新技术及解决方案等。包括“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基本理论和实用技术。本书为“十三五”国家重点出版物出版规划项目暨上海市普通高校精品课程特色教材，**体现“教、学、练、做、用一体化和立体化”，突出“实用、特色、新颖、操作性”。**

本书由上海市高校精品课程网站提供多媒体课件、动画视频、教学大纲及教案、同步实验，以及课程设计指导及练习等资源，并有配套的学习与实践指导。

本书可作为高等院校计算机类、信息类、电子商务类、工程和管理类专业的网络安全相关课程的教材，也可作为培训及参考用书。高职院校可对“*”内容选用。

本书配套授课电子课件，需要的教师可登录 www.cmpedu.com 免费注册，审核通过后下载，或联系编辑索取。QQ：2850823885，电话：010-88379739。

图书在版编目（CIP）数据

网络安全技术及应用 / 贾铁军，陶卫东主编. —3 版. —北京：机械工业出版社，2017.6

高等教育网络空间安全规划教材

ISBN 978-7-111-57135-3

Ⅰ. ①网… Ⅱ. ①贾… ②陶… Ⅲ. ①计算机网络－网络安全－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2017）第 125553 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：郝建伟 责任校对：张艳霞

责任印制：李 昂

三河市宏达印刷有限公司印刷

2017 年 7 月第 3 版 • 第 1 次印刷

184mm×260mm • 21.25 印张 • 515 千字

0001－3000 册

标准书号：ISBN 978-7-111-57135-3

定价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务

服务咨询热线：（010）88379833

读者购书热线：（010）88379649

网络服务

机 工 官 网：www.cmpbook.com

机 工 官 博：weibo.com/cmp1952

教育服务网：www.cmpedu.com

金 书 网：www.golden-book.com

高等教育网络空间安全规划教材
编委会成员名单

前　言

进入 21 世纪，随着信息化建设和 IT 技术的快速发展，各种网络技术的应用更加广泛深入，同时也出现了很多网络安全问题，致使网络安全技术的重要性更加突出，网络安全已经成为各国关注的焦点，不仅关系到机构和个人用户的信息资源和资产风险，也关系到国家安全和社会稳定，已成为热门研究和人才需求的新领域。因此，必须在法律、管理、技术和道德各方面采取切实可行的有效措施，才能确保网络建设与应用“又好又快”地稳定发展。

网络空间已经逐步发展成为继陆、海、空、天之后的第五大战略空间，是影响国家安全、社会稳定、经济发展和文化传播的核心、关键和基础。网络空间具有开放性、异构性、移动性、动态性和安全性等特性，不断演化出下一代互联网、5G 移动通信网络、移动互联网及物联网等新型网络形式，以及云计算、大数据和社交网络等众多新型的服务模式。

网络安全已经成为世界热门研究课题之一，并引起社会广泛关注。网络安全是一个系统工程，已经成为信息化建设和应用的首要任务。网络安全技术涉及法律法规、政策、策略、规范、标准、机制、措施、管理和技术等诸多方面，是网络安全的重要保障。

信息、物资和能源已经成为人类社会赖以生存与发展的三大支柱和重要保障，信息技术的快速发展为人类社会带来了深刻的变革。随着计算机网络技术的快速发展，我国在网络化建设方面取得了令人瞩目的成就，电子银行、电子商务和电子政务的广泛应用，使计算机网络已经深入到国家的政治、经济、文化和国防建设等各个领域，遍布现代信息化社会工作和生活的每个层面，“数字化经济”和全球电子交易一体化正在形成。网络安全不仅关系到国计民生，还与国家安全密切相关，不仅涉及国家政治、军事和经济各个方面，甚至影响到国家的安全和主权。随着信息化和网络技术的广泛应用，网络安全的重要性尤为突出。因此，网络技术中最关键也最容易被忽视的安全问题正在危及网络的健康发展和应用，网络安全技术及应用越来越受到世界的关注。

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、计算数学、密码技术和信息论等多学科的综合性交叉学科，是计算机与信息科学的重要组成部分，也是近 20 年发展起来的新兴学科。其综合信息安全、网络技术与管理、分布式计算，以及人工智能等多个领域知识和研究成果，概念、理论和技术正在不断发展完善之中。

随着信息技术的快速发展与广泛应用，网络安全的内涵也在不断扩展，从最初的信息保密性发展到信息的完整性、可用性、可控性和可审查性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基本理论和实施技术。

为满足高校计算机、信息、电子商务、工程及管理类本科生、研究生等高级人才培养的需要，本书在 2014 年获得“上海市普通高校精品课程特色教材”和 2015 年获得“上海市普通高等院校优秀教材奖”，并在 2016 年入选国家新闻出版广电总局的“‘十三五’国家重点出版物出版规划项目”，而且在前两版很受欢迎、多次重印的基础上，对教材进行了再

版。主编和编著者多年来在高校从事计算机网络与安全等领域的教学、科研及学科专业建设与管理工作，特别是多次主持过计算机网络安全方面的科研项目研究，积累了大量的宝贵实践经验，谨以此书献给广大师生和其他读者。

本书主要内容共分 12 章，包括“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基本理论和实用技术。书中内容包括很多经过多年的实践总结出来的案例及研究成果，以便于实际应用。书中带“*”的部分为选学内容。

本书重点介绍最新网络安全技术、成果、方法和实际应用，其特点如下。

1. 内容先进，结构新颖。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。“教学练做用一体化”，注重科学性、先进性和操作性。图文并茂、学以致用。

2. 注重实用性和特色。坚持“实用、特色、规范”原则，突出实用及素质能力培养，增加了大量案例和同步实验，以及课程设计指导，将理论知识与实际应用有机结合在一起。

3. 资源丰富，便于教学。通过上海市高校精品课程网站 http://jiatj.sdju.edu.cn/webanq/，提供多媒体课件、教学大纲和计划、电子教案、动画视频、同步实验，以及复习与测试演练系统等教学资源，便于实践教学、课外延伸和综合应用等。并有“十三五”国家重点出版规划项目、上海市高校精品课程配套教材《网络安全技术及应用实践教程》，包含知识要点、案例分析、知识拓展、练习与复习、丰富的同步实验指导和课程设计指导等。

读者可以使用移动设备的相关软件（如微信、QQ）中的“扫一扫”功能扫描书中提供的二维码，在线查看相关资源（音频建议用耳机收听）。如果“扫一扫”后在微信端无法打开相关资源，请选择用手机浏览器直接打开。

本书由贾铁军教授（上海电机学院）、陶卫东副教授（辽宁警察学院）任主编，俞小怡副教授（大连理工大学）、罗宜元副教授（上海电机学院）、彭浩副教授（浙江师范大学）、王坚（辽宁对外经贸学院）任副主编。其中，贾铁军编著第 1、2、3、6、9、12 章，陶卫东编著第 10 章，俞小怡编著第 11 章，彭浩编著第 4 章，罗宜元编著第 5、8 章，王坚编著第 7 章。参与本书编写工作的还有：陈国秦、宋少婷。有多位同仁和研究生对全书的文字和图表进行了校对、编排及查阅资料，并完成了部分课件的制作。

非常感谢对本书编著过程中给予大力支持和帮助的院校及各界同仁。对编著过程中所参阅的大量重要文献资料难以完全准确注明，在此深表诚挚谢意！

由于网络安全技术涉及的内容比较庞杂，而且有关技术方法及应用发展快、知识更新迅速，另外，编著时间比较仓促，编著者水平及时间有限，书中难免存在不妥之处，敬请广大读者海涵见谅，欢迎提出宝贵意见和建议，并指正交流，主编邮箱：jiatj@163.com。

编　者

目　录

第 1 章　网络安全基础

进入 21 世纪现代信息化社会，随着网络技术的快速发展和广泛应用，网络安全问题不断出现，网络安全的重要性和紧迫性更加突出，不仅关系到国家安全和社会稳定，也关系到信息化建设的健康发展，以及用户资产和信息资源的安全。网络安全已经引起世界各国的高度重视，并成为一项热门研究和人才需求的新领域。

教学目标

- 理解网络安全面临的威胁及发展态势
- 掌握网络安全的基本概念、目标和内容
- 掌握网络安全技术的相关概念、种类和模型
- 理解构建虚拟局域网 VLAN 的过程及方法

1.1　网络空间安全威胁及态势

【案例 1-1】 我国网络遭受攻击近况。根据国家互联网应急中心 CNCERT 抽样监测结果和国家信息安全漏洞共享平台 CNVD 发布的数据，2017 年 3 月国内被篡改网站数量为 5252 个；国内被植入后门的网站数量为 5422 个；针对国内网站的仿冒页面数量为 3198 个。国内被篡改政府网站数量为 215 个；国内被植入后门的政府网站数量为 207 个。国内感染网络病毒的终端数为 128 万个，信息系统漏洞数为 1066 个，其中高危漏洞有 420 个，可被利用来实施远程攻击的漏洞有 964 个。

教学课件
第 1 章　课件资源

1.1.1　网络空间安全威胁及现状分析

网络空间已经逐步发展成为继陆、海、空、天之后的第五大战略空间，是影响国家安全、社会稳定、经济发展和文化传播的核心、关键和基础，其安全至关重要，现存在一些急需解决的重大问题。

1. 法律法规、安全管理和意识欠缺

世界各国在网络空间安全保护方面制定的各种法律法规和管理政策等相对滞后、不完善且更新不及时。很多机构和个人用户对网络风险和隐患不重视、重技术轻管理、网络安全意识薄弱以及管理措施不到位，甚至出现监守自盗等案件。一些机构对网络安全的投入不足，其投入经费也时常被挪用

微视频
第 1 章　授课视频

或挤占。

2. 网络安全规范和标准不统一

网络安全是一个系统工程，需要统一规范和标准。美国等发达国家网络技术先进且对网络安全相对重视，但也同样存在着网络安全规范和标准等问题。西欧国家则另有一套安全标准，在原理和结构上也有很多不同之处。国内外一直存在不同的规范和标准等问题。

3. 政府与企业的侧重点及要求不一致

政府注重信息资源及网络安全的可管性和可控性，企业则注重其经济效益、可用性和可靠性。事实上，一些政府倡导的网络协议或安全措施，因难以实现、不受企业欢迎而无法推广。

4. 网络系统的安全威胁及隐患

进入21世纪现代信息化社会，电子商务、电子政务、网络银行、办公自动化和其他各种业务的应用对网络的依赖程度更大，而且由于计算机及手机网络的开放性、交互性和分散性等特点，以及网络系统从设计到实现自身存在的缺陷、安全漏洞和隐患，致使网络存在巨大的威胁和风险，时常受到侵扰和攻击。各种计算机病毒、垃圾邮件、广告和恶意软件等也影响了正常的网络应用和服务。

【案例1-2】 随着互联网技术和应用的快速发展，全球互联网用户数量和隐患急剧增加。据估计，到2020年，全球网络用户将上升至50亿，移动用户将上升至100亿。中国的互联网用户数量急剧增加，网民规模、宽带网民数和国家顶级域名注册量3项指标仍居世界第一。各种操作系统及应用程序的漏洞隐患不断出现，相比发达国家，网络用户安全防范能力和意识较为薄弱，极易成为国内外攻击利用的主要目标。

5. 网络技术和手段滞后

据统计，全世界平均不足20s就发生一次黑客严重入侵事件，全球每年因黑客入侵造成的经济损失达几千亿美元。网络安全问题已成为世界各国共同关注的焦点。网络安全技术手段研发及更新滞后于出现的需要解决的安全问题。网络技术不断快速发展，相应的网络安全技术手段相对滞后，更新时常不及时、不完善。

知识拓展
网络安全技术的缺陷

6. 网络安全威胁新变化，黑客利益产业链惊人

移动安全、大数据、云安全、社交网络和物联网等成为新的攻击点。黑客产业链和针对性攻击普遍，攻击力度和数量也呈现上升趋势，且被用于军事或利益集团。云端数据保护压力增大，攻击目标向离线设备延伸，利用终端及网络在脱网状态下远程控制等。

【案例1-3】 中国黑客利益产业链严重。据调查显示，2010年中国的木马产业链一年收入达上百亿元。湖北某地警方破获了一起制造传播具有远程控制功能的木马病毒网络犯罪案件，是国内破获的首个上下游产业链完整的木马犯罪案件。嫌疑人杨某等编写并贩卖木马程序。原本互不相识的几位犯罪嫌疑人，在不到半年的时间就非法获利近200万元。木马程序灰鸽子产业链如图1-1所示。

图1-1　黑客木马程序灰鸽子产业链

1.1.2 网络安全威胁的种类及途径

1. 网络安全威胁的主要种类

网络安全面临的主要威胁有人为因素、系统和运行环境，其中包括网络系统问题和网络数据（信息）的威胁和隐患。网络安全威胁主要表现为：非法授权访问、窃听、黑客入侵、假冒合法用户、病毒破坏、干扰系统正常运行、篡改或破坏数据等。这些威胁性攻击大致可分为主动攻击和被动攻击两大类。

【案例 1-4】 美国网络间谍活动公诸于世。2013 年曾参加美国安全局网络监控项目的斯诺登曝光“棱镜事件”，公开美国多次秘密利用超级软件监控包括其盟友政要在内的网络用户和电话。谷歌、雅虎、微软、苹果、Facebook、美国在线、PalTalk、Skype 和 YouTube 等公司还帮助其提供漏洞参数、开放服务器等，使其轻易监控有关国家机构或上百万网民的邮件、即时通话及相关数据。

网络安全面临的威胁的主要种类如表 1-1 所示。

表 1-1 网络安全威胁的主要种类

威胁类型	主要威胁
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
窃听	窃听网络传输信息
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
伪造	将伪造的信息发送给他人
窃取	盗取系统重要的软件或硬件、信息和资料
截获/修改	数据在网络系统传输中被截获、删除、修改、替换或破坏
病毒木马	利用木马病毒及恶意软件进行破坏或恶意控制他人系统
行为否认	通信实体否认已经发生的行为
拒绝服务攻击	黑客以某种方式使系统响应减慢或瘫痪，阻止用户获得服务
截获	黑客从有关设备发出的无线射频或其他电磁辐射中获取信息
人为疏忽	已授权人为了利益或由于疏忽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	对终端、部件或网络进行破坏，或绕过物理控制非法入侵
讹传	攻击者获得某些非正常信息后，发送给他人
旁路控制	利用系统的缺陷或安全脆弱性的非正常控制
服务欺骗	欺骗合法用户或系统，骗取他人信任以便牟取私利
冒名顶替	假冒他人或系统用户进行活动
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，达到信任并非法侵权目的
陷阱门	协调陷阱“机关”系统或部件，骗取特定数据以违反安全策略
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	为了国家或集团利益，通过网络严重干扰破坏或恐怖袭击

2. 网络安全威胁的主要途径

世界上各种计算机网络、手机网络或电视机网络被入侵攻击的事件频发，其途径种类

各异且变化多端。目前，大量网络系统的功能、网络资源和应用服务等已经成为黑客攻击的主要目标。目前，网络的主要应用包括电子商务、网上银行、股票、证券、即时通信、邮件、网游和下载文件等，都存在大量安全隐患。

【案例 1-5】 中国已成为被监控的重要目标，脱网也会被攻击。美国《纽约时报》2014 年 1 月曝光了美国国家安全局“量子”项目，美国国家安全局（National Security Agency，NSA）可以将一种秘密技术植入脱网的计算机，并对其数据进行更改。2008 年以来一直使用，主要用安装在计算机内的微电路板和 USB 连线发送秘密无线电波实现监视，已经在全球 10 万台计算机上植入其软件。美国专家以“肆无忌惮”来评价 NSA 的行为，称“白宫曾义正词严地批评中国黑客盗取我们的军事、商业机密，原来我们一直在对中国做同样的事情”。

网络安全威胁的主要途径可以很直观地用如图 1-2 所示的方式来表示。

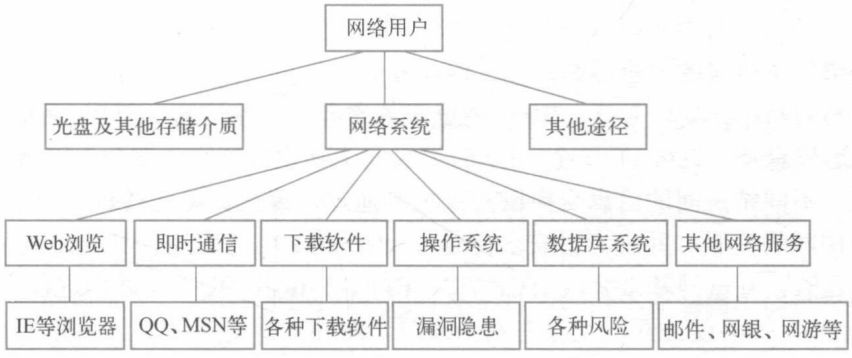

图 1-2　网络安全威胁主要及途径

1.1.3　网络安全的威胁及风险分析

网络安全的风险及脆弱性涉及网络设计、结构、层次、范畴和管理机制等方面，要做好网络安全防范，必须进行认真深入的分析，研究网络系统的安全风险及隐患。

1. 网络系统安全威胁及风险

（1）网络系统面临的威胁和风险

互联网创建初期只用于计算和科学研究，其设计及技术基础并不安全。现代互联网的快速发展和广泛应用使其具有开放性、国际性和自由性等特点，也出现了一些网络系统的安全风险和隐患，主要因素包括下述 7 个方面。

1）网络开放性隐患多。通过计算机和手机网络的开放端口，都可登录浏览互联网的各种信息资源，其开放端口及网络协议等增加了网络系统的风险和隐患，极易受到网络侵入和攻击，且站点主机数量剧增，致使网络监控难以准确、及时、有效。

2）网络共享风险大。网络资源共享增加了开放端口，为系统安全带来了更大风险，并为黑客借机破坏提供了极大便利。网络资源共享和网络快速发展与更新，致使相关的法律法规、分布式管理、运行及技术保障等各个方面很难及时有效地解决各类出现的问题。

3）系统结构复杂有漏洞。主机系统和网络协议的结构复杂，以及一些软件设计和实现

过程中难以避免的疏忽及漏洞隐患，致使网络系统安全与防范非常繁杂困难，难以有效彻底解决问题。

4）身份认证难。实际上，网络系统的身份认证环节、技术、机制、方式和方法等比较薄弱，常用的静态口令极易被破译，此外，通过越权访问还可借用管理员的网络检测信道，窃取用户密码等。

5）边界难确定。网络升级与维护的可扩展性致使其边界难以确定，网络资源共享访问也使其安全边界容易被破坏，导致网络安全受到严重威胁。

6）传输路径与结点隐患多。网络用户通过网络互相传输的路径很多，一个报文从发送端到目的端需要经过多个中间结点，所以，起止端的安全保密性根本无法解决中间结点的安全问题。

7）信息高度聚集，易受攻击。当信息量少且分散时，其价值往往并不被注意。当大量相关信息聚集以后，显示出其重要价值。网络聚集大量敏感信息后，很容易受到分析性等方式的攻击。

（2）网络服务协议的安全威胁

常用的互联网服务安全包括：Web 浏览服务安全、文件传输（FTP）服务安全、E-mail 服务安全、远程登录（Telnet）安全、DNS 域名安全和设备的实体安全。网络的运行机制依赖网络协议，不同结点间的信息交换以约定机制通过协议数据单元实现。TCP/IP 在设计初期只注重异构网的互联，并没考虑安全问题，Internet 的广泛应用使其安全威胁对系统安全产生了极大风险。互联网基础协议 TCP /IP、FTP、E-mail、RPC（远程进程调用）和 NFS（网络文件系统）等不仅公开，且存在安全漏洞。此外，网络管理人员没有足够时间和精力专注于全程网络安全监控，而且由于操作系统的复杂性，难以检测并解决所有的安全漏洞和隐患，致使连接网络的终端受到入侵威胁。

知识拓展
网络协议本身缺陷

2. 操作系统的漏洞及隐患

操作系统安全（Operation System Secure）是指操作系统本身及运行的安全，通过其对系统软硬件资源的整体有效控制，并对所管理的资源提供安全保护。操作系统是网络系统中最基本、最重要的系统软件，在设计与开发时由于疏忽而留下漏洞和隐患。

（1）体系结构和研发漏洞

【案例 1-6】 网络系统的威胁主要来自操作系统的漏洞。操作系统的程序不仅有研发疏忽漏洞，其 I/O 驱动程序和系统服务可通过打“补丁”的方式动态链接，如操作系统版本升级。其动态链接方法容易被黑客利用，成为计算机病毒入侵的环境。另外，操作系统的一些功能也具有不安全因素，如支持在网络上传输可以执行的文件映像、网络加载程序等。系统漏洞造成的威胁主要包括初始化错误、不安全服务及配置，以及从漏洞乘虚而入。

（2）创建进程的隐患

支持进程的远程创建与激活、所创建的进程继承原进程的权限，其机制也时常给黑客提供远端服务器安装“间谍软件”的可乘之机。如将木马病毒以打补丁的方式“补”在一个合法用户或特权用户上，就可以使系统进程与作业的监视程序失效。此外，为设计编程和维护人员而设置的网络系统隐秘通道容易成为黑客入侵的通道。

（3）服务及设置的风险

【案例 1-7】 操作系统的部分服务程序有可能绕过防火墙、查杀病毒等安全系统，互联网蠕虫具有 3 个可以绕过 UNIX 系统的机制。网上浏览 IE、文件传送、E-mail、远程登录和即时通信 QQ 等网络服务，如果不注意安全选项设置与安全防范，很容易出现信息资源被窃取、网络攻击和感染病毒等问题。

（4）配置和初始化错误

网络系统一旦出现严重故障，必须关掉某台服务器维护其某个子系统，之后再重新启动服务器时，可能会发现个别文件丢失或被篡改的现象。这可能就是在系统进行重新初始化时，安全系统没有被正确初始化，从而留下了安全漏洞被黑客所利用，类似地，在木马程序修改系统的安全配置文件时也可能会出现此情况。

3. 防火墙的局限性及风险

防火墙能够较好地阻止外网基于 IP 包头的攻击和非信任地址的访问，却无法阻止基于数据内容的黑客攻击和病毒入侵，也无法控制内网之间的攻击行为。其安全局限性还需要入侵检测系统、入侵防御系统、统一威胁管理（Unified Threat Management, UTM）等技术进行弥补，应对各种网络攻击，以扩展系统管理员的防范能力（包括安全审计、监视、进攻识别和响应）。从网络系统中的一些关键点收集并分析有关信息，可检查出违反安全策略的异常行为或遭到攻击的迹象。入侵防御和检测系统被认为是继防火墙后的第二道安全闸门，在不影响网络性能的情况下，需要及时对网络进行异常行为的防御和监测，提供对网络内部攻击、外部攻击和误操作的实时保护。

防火墙安全技术和方法的具体内容将在第 8 章进行介绍。

4. 网络数据库的安全风险

知识拓展
网络数据库安全性

数据库技术是信息资源管理和数据处理的核心技术，也是各种应用系统处理业务数据的关键，是信息化建设的重要组成部分。网络系统需要在数据库中存取并调用大量重要数据共享，数据库技术的核心是数据库管理系统（DBMS），主要用于集中管理数据资源信息，解决数据资源共享、减少数据冗余，确保系统数据的保密性、完整性和可靠性，各类应用系统都以其为支撑平台。数据库安全不仅包括数据库系统本身的安全，还包括最核心和关键的数据（信息）安全，需要确保数据的安全可靠和正确有效，确保数据的安全性、完整性和并发控制。数据库存在的不安全因素包括非法用户窃取信息资源，以及授权用户超出权限进行数据访问、更改和破坏等。

数据库安全技术和应用的具体内容将在第 10 章进行介绍。

5. 网络安全管理及其他问题

网络安全是一项系统工程，需要各方面协同管理。安全管理产生的漏洞和疏忽属于人为因素，如果缺乏完善的相关法律法规、管理技术规范和安全管理组织及人员，缺少定期的安全检查、测试和实时有效的安全监控，将是网络安全的最大问题。

【案例 1-8】 中国是网络攻击最大受害国之一。国家互联网应急中心（CNCERT）监测的数据显示，中国遭受国外网络攻击的情况日趋严重。CNCERT 抽样监测发现，2013