上海普通高校优秀教材奖
上海市精品课程特色教材

免费提供
电子教案

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 第2版

主　编　贾铁军

机械工业出版社
CHINA MACHINE PRESS

上海普通高校优秀教材奖
上海市精品课程特色教材
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

第2版

主　编　贾铁军
副主编　贾欣歌　曾　刚　王　冠
参　编　王　坚　王小刚

机械工业出版社

本书主要内容为网络安全基本知识和应用技术要点，详尽的同步实验与综合课程设计指导，主要包括：网络安全的现状及态势、有关概念内容和方法；网络协议安全及 IPv6 安全、网络安全体系结构及管理、无线网络安全；入侵检测与防御技术、黑客的攻击与防范；身份认证与访问控制技术、安全审计；密码及实用加密技术；数据与数据库安全技术；计算机病毒防范；防火墙应用技术；操作系统与站点安全技术；电子商务及网站安全实用技术、网络安全解决方案等，涉及“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等。

本书提供教学目标、知识要点、案例分析、知识拓展、要点小结、同步实验及课程设计指导、练习与实践等，并提供了选择性实验和任务。还配套提供上海市精品课程网站的课件、视频、实验及案例等丰富资源。

本书既可作为高等院校计算机类、信息类、电子商务、工程和管理类各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。

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．—2 版．—北京：机械工业出版社，2016.1
高等院校规划教材．计算机科学与技术系列
ISBN 978-7-111-52560-8

Ⅰ.①网… Ⅱ.①贾… Ⅲ.①计算机网络-安全技术-高等学校-教材
Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 309449 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
策划编辑：郝建伟　　责任编辑：郝建伟
责任校对：张艳霞　　责任印制：李　洋
高教社（天津）印务有限公司印刷
2016 年 1 月第 2 版·第 1 次印刷
184mm×260mm ·21.5 印张·534 千字
0001-3000 册
标准书号：ISBN 978-7-111-52560-8
定价：49.90 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	网络服务
服务咨询热线：(010)88379833	机 工 官 网：www.cmpbook.com
读者购书热线：(010)88379649	机 工 官 博：weibo.com/cmp1952
	教育服务网：www.cmpedu.com
封面无防伪标均为盗版	金　书　网：www.golden-book.com

出 版 说 明

计算机技术在科学研究、生产制造、文化传媒、社交网络等领域的广泛应用，极大地促进了现代科学技术的发展，加速了社会发展的进程，同时带动了社会对计算机专业应用人才的需求持续升温。高等院校为顺应这一需求变化，纷纷加大了对计算机专业应用型人才的培养力度，并深入开展了教学改革研究。

为了进一步满足高等院校计算机教学的需求，机械工业出版社聘请多所高校的计算机专家、教师及教务部门针对计算机教材建设进行了充分的研讨，达成了许多共识，并由此形成了教材的体系架构与编写原则，策划开发了“高等院校规划教材”。

本套教材具有以下特点：

1）涵盖面广，包括计算机教育的多个学科领域。

2）融合高校先进教学理念，包含计算机领域的核心理论与最新应用技术。

3）符合高等院校计算机及相关专业人才培养目标及课程体系的设置，注重理论与实践相结合。

4）实现教材“立体化”建设，为主干课程配备电子教案、素材和实验实训项目等内容，并及时吸纳新兴课程和特色课程教材。

5）可作为高等院校计算机及相关专业的教材，也可作为从事信息类工作人员的参考书。

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。衷心感谢广大读者的支持与帮助！

机械工业出版社

第2版前言

21世纪进入现代信息化时代，信息已经成为国家的重要战略资源，世界各国对于网络信息的安全更加重视，并将网络安全技术和产品作为国家优先发展战略之一。网络安全不仅关系到国家的安全和稳定，而且对于国家政治、经济、国防、科技和文化等方面的安全极为重要。世界各国都极为重视网络安全，不惜投入巨资和大量人力物力，利用最先进的技术，构建最安全可靠的网络系统。信息化时代，网络安全主导国家信息安全且决定国家的信息主权安危。强国推行信息强权和信息垄断，依仗信息优势控制弱国的信息技术。一旦信息弱国却步，又缺乏自主创新的网络安全策略和手段，国家的信息主权就有可能被葬送。正如美国未来学家托尔勒所说："谁掌握了信息，谁控制了网络，谁就将拥有整个世界"。知识经济时代，竞争首先表现为科技竞争，其重点是对信息技术制高点的争夺。网络安全已经成为影响国家政治命脉、经济发展、军事强弱、社会稳定，以及民族与文化复兴等方面的关键因素。

在现代信息化社会，随着信息化建设和IT技术的快速发展，计算机网络技术的应用更加广泛深入，网络安全问题不断出现，致使网络安全技术的重要性更加突出，**网络安全已经成为世界各国关注的焦点**，并成为热门研究和人才需求的新领域。只有在法律、管理、技术和道德各方面采取有效措施，才能确保网络建设与应用"安全稳定"地发展。

我国极为重视网络安全工作。2014年2月27日，中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长习近平主持召开中央网络安全和信息化领导小组第一次会议并发表重要讲话。他强调，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。习近平强调，网络安全和信息化对一个国家很多领域都是牵一发而动全身的，要认清我们面临的形势和任务，充分认识做好工作的重要性和紧迫性，因势而谋，应势而动，顺势而为。网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业。

网络安全已经成为21世纪世界热门课题之一，引起社会广泛关注。网络安全是一个系统工程，并已经成为网络信息化建设的重要任务。网络安全技术涉及法律法规、政策、策略、规范、标准、机制、措施和管理等方面，是网络安全的重要保障。

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，电子银行、电子商务和电子政务等方面的广泛应用，计算机网络已经深入到国家的政治、经济、文化和国防建设等各个领域，遍布现代信息化社会的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，不仅涉及国家政治、军事和经济各个方面，而且影响到国家的安全和稳定等

方面。随着计算机及通信网络的广泛应用，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。

网络安全的内涵随着信息技术的快速发展与广泛应用也在不断扩展，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。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。需要综合信息安全、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，其理论和技术正在不断发展完善之中。

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，我们编著了这套教材。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，谨以此书奉献给广大师生。

主要内容：本书共分为13章，重点介绍了常用的计算机网络安全基本知识、基本原理及其应用技术要点，以及同步实验与综合课程设计指导，主要包括：计算机网络安全的现状及态势；网络安全技术有关概念、内容、体系结构和方法；网络协议安全及IPv6安全、网络安全体系结构及管理、无线网络安全技术及应用；入侵检测与防御技术、黑客的攻击与防范；身份认证与访问控制技术、安全审计；密码及实用加密技术；数据与数据库安全技术；计算机病毒及恶意软件的防范技术；防火墙技术及应用；操作系统与站点安全技术；电子商务及网站安全实用技术、网络安全解决方案等，涉及“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等。本书既可作为《网络安全技术及应用》第2版配套的辅助教材，也可单独使用。

体系结构：包括教学目标、知识要点、案例分析、知识拓展、要点小结、同步实验指导、练习与实践，以及课程设计指导等，便于实践教学、课外延伸学习和网络安全综合实践练习，并提供了选择性实验和任务，可根据专业选用。书中带“*”部分为选学内容。

特色及资源：本书是上海市精品课程暨上海市高校获奖特色教材，突出“教学练做用一体化”和“实用、特色、新颖、操作性、资源丰富”，重点介绍了最新的网络安全技术、成果、方法和实际应用。通过上海市精品课程网站提供教学大纲、授课计划、课件、视频、实验及案例、模拟测试复习与考试系统、知识拓展等丰富资源。本书还提供了配套的同步实验指导、实践与练习习题，以及部分答案等。上海市高校获奖特色教材及上海市精品课程特色教材资源网址：**http://jiatj.sdju.edu.cn/webanq/**。

本书由上海市高校优秀教材奖获得者及主持上海市精品课程的贾铁军教授任主编并编著第1章、第3~6章、第11~12章，贾欣歌（上海电机学院）任副主编并编著第2章，曾刚（辽宁警察学院）任副主编并编著第7章，王冠（辽宁警察学院）任副主编编著第8章，王坚（辽宁对外经贸学院）编著第9章，王小刚（上海电机学院）编著第10章，另外，部分老师也参加了本书编写大纲的讨论、编著审校等工作，并多次对全书的文字、图表进行了校

对、编排及查阅资料，完成了部分实验课件及视频制作等工作。

非常感谢机械工业出版社和有关院校，提供了许多重要帮助、指导意见和参考资料，并提出很好的修改意见和建议。同时，非常感谢对本书编著过程中给予大力支持和帮助的各界同仁。对编著过程中参阅的大量重要文献资料难以完全准确注明，在此表示诚挚的谢意！

由于网络安全技术涉及的内容比较庞杂，而且网络安全技术发展快、知识更新迅速，另外，编著时间比较仓促，编著者水平所限，书中难免存在不妥之处，敬请海涵见谅！欢迎广大读者提出宝贵意见和建议，发送至主编邮箱 jiatj@163.com。

编　者

2015.7 于上海

第1版前言

信息技术的快速发展为人类社会带来了深刻的变革，信息、物资和能源已经成为人类赖以生存和发展的重要保障。随着计算机网络技术的快速发展，电子银行、电子商务和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的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，网络安全的重要性尤为突出。

随着信息技术的发展与应用，网络安全的内涵也在不断地延伸，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、交叉学科领域，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发展成果，不断发展和完善。为满足高校应用型人才培养的需要，我们编著了这套教材。主编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，积累了大量的宝贵实践经验，谨以此书奉献给广大师生。

本书既可以作为《网络安全技术及应用》配套的辅助教材，也可以单独使用。**体系结构：**知识要点（内容提要与学习指导）、实验教学、实验报告、练习测试和课程设计等，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，本书还提供了选择性实验和不同的任务项目，可根据不同专业选择使用。书中带“*”部分为选学内容。

本书共分为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、黑客的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压缩技术实验；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，以便于实际应用。

编著本书旨在重点介绍最新成果、防范技术、处理技术、方法和实际应用。本套教材主要是专门针对应用型人才培养编写的，其**特点**如下。

1. 内容先进，结构新颖。编著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，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，提供电子教案和教学大纲。还提供了同步实验、学习指导和练习测试等资源，可以进行选用。

本书由贾铁军教授任主编、统稿并完成第1～6、11、12章的编著工作。王坚任副主编并编著第8章、全书练习测试及解答和课件制作等，王小刚编著第7章、苏庆刚编著第9

章、沈学东编著第10章，部分老师也参与了本书大纲的讨论、编著审校等工作，并对全书的文字、图表进行了校对、编排及查阅资料等。

非常感谢机械工业出版社为本书的编著提供了许多重要帮助、指导意见和参考资料。同时，感谢对本书编著给予大力支持和帮助的上海电机学院的有关领导和同仁。对编著过程中参阅的大量重要文献资料难以完全准确注明，在此表示诚挚的谢意！

由于编者学识水平有限，内容庞杂、更新迅速及时间仓促，书中难免存在不妥之处，敬请见谅！欢迎广大读者提出宝贵意见和建议。E－mail：jiatj@163.com

编　者

2009.2

目　录

第1章　网络安全概述

在现代信息化社会中，计算机网络技术得到了快速发展和广泛应用，给人们的工作、文化和生活带来极大便利，同时网络安全问题也不断显现。当前，网络安全已经成为世界关注的热点问题之一，其重要性更加突出，不仅关系到国家安全和社会稳定，也涉及信息化建设的顺利发展，以及用户资产和信息资源的安全，并成为热门研究和人才需求的新领域。

教学目标

- 掌握网络安全的概念、特征、目标及内容
- 了解网络安全面临的威胁及其因素分析
- 掌握网络安全模型、网络安全体系和常用网络安全技术
- 了解实体安全技术的概念、内容、措施和隔离技术
- 理解构建设置虚拟局域网的同步实验

1.1　知识要点

【案例1-1】中国网络因遭受攻击而“瘫痪”，涉事IP指向美国公司。据环球时报2014年1月报道，中国互联网部分用户21日遭遇大范围的极为严重的“瘫痪”性攻击现象，国内通用顶级根域名服务器解析出现异常，部分国内用户无法访问.cn或.com等域名网站。全国约有2/3的网站和几十亿企事业单位或个人用户访问受到极大影响，绝大多数网站无法打开浏览，导致系统处于瘫痪状态。网络系统故障发生后，一些用户访问时都会被跳转到一个位于美国Dynamic Internet Technology公司，曾是“自由门”翻墙软件的开发者的IP地址。

1.1.1　网络安全的概念、特征和内容

1. 信息安全及网络安全的概念

国际标准化组织（ISO）提出**信息安全**（Information Security）的定义是：为数据处理系统建立和采取的技术及管理保护，保护计算机硬件、软件及数据不因偶然及恶意的原因而遭到破坏、更改和泄漏。

我国《计算机信息系统安全保护条例》定义**信息安全**为：计算机信息系统的安全保护，应当保障计算机及其相关的配套设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统安全运行。主要防止信息被非授权泄露、更改、破坏或使信息被非法的系统辨识与控制，确保信息的机密性、完整性、可用性、可控性和可审查性（称为**信息安全属性特征**）。

信息安全的发展经历了通信保密、信息安全（以保密性、完整性和可用性为目标）和信息保障3个阶段。信息安全的内涵也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）”等多方面的基础理论和实施技术。

网络安全（Network Security）以计算机网络安全为主，是指利用计算机及通信网络管理控制和技术措施，保证网络系统及数据的保密性、完整性、网络服务可用性和可审查性受到保护，即保证网络系统的硬件、软件及系统中的数据资源得到完整、准确、连续运行与服务不受干扰破坏和非授权使用。**狭义上**，网络安全是指计算机及其网络系统资源和信息资源不受有害因素的威胁和危害。**广义上**，凡是涉及计算机及通信网络信息安全属性特征的相关技术和理论，都是网络安全的研究领域。实际上，**网络安全问题**包括两方面的内容，一是网络的系统安全，二是网络的信息安全，而网络安全的最终目标和关键是保护网络的信息安全。

拓展阅读：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。需要综合信息安全、网络技术与管理、分布式计算、人工智能等多个领域的知识和研究成果，其概念、理论和技术正在不断发展完善。

2. 网络安全的特征及目标

网络安全定义中的保密性、完整性、可用性、可控性和可审查性，反映了网络信息安全的**基本特征和要求**。反映了网络安全的**基本属性**、**要素**与技术方面的**重要特征**。

1）**保密性**。也称**机密性**，是指网络信息按规定要求不泄漏给非授权用户、实体或过程，即保护有用信息不泄漏给非授权个人或实体，强调有用信息只被授权对象使用的特征。

2）**完整性**。是指网络数据在传输、交换、存储和处理过程保持非修改、非破坏和非丢失的特性，即保持信息原样性，使信息能正确生成、存储和传输，是最基本的安全特征。

3）**可用性**。指网络信息可被授权实体正常使用或在非正常情况下能应急恢复使用的特征。是衡量网络信息系统面向用户的一种安全性能。

4）**可控性**。指在网络系统中的信息传播及具体内容能够实现有效控制的特性，即网络系统中的任何信息要在一定传输范围和存放空间内可控。

5）**可审查性**。又称**不可否认性**，指网络通信双方在信息交互过程中，确信参与者本身，以及参与者所提供的信息的真实同一性，即所有参与者都不可能否认或抵赖本人的真实身份，以及提供信息的原样性和完成的操作与承诺。

网络安全研究的目标是：在信息输入、传输、存储、处理和输出的整个过程中，提供物理和逻辑上的防护、监控、反应恢复和对抗能力，以保护网络信息的保密性、完整性、可用性、可控性和可审查性。网络安全的**最终目标**是保障网络上的信息安全。

3. 网络安全涉及的主要内容

可以从不同角度划分网络安全研究的主要内容。

从层次结构上，也可将**网络安全所涉及的内容**概括为以下5个方面。

1）**实体安全**（Physical Security）。也称**物理安全**，指保护计算机网络设备、设施及其他媒介免遭地震、水灾、火灾、有害气体、盗窃和其他环境事故破坏的措施及过程。包括环境安全、设备安全和媒体安全3个方面。实体安全是信息系统安全的基础。

2）**运行安全**（Operation Security）。包括网络运行和访问控制安全，如设置防火墙实现内外网隔离、备份系统实现系统的恢复等。运行安全包括：内外网的隔离机制、应急处置机制和配套服务、网络系统安全性监测、网络安全产品运行监测、定期检查和评估、系统升级

和补丁处理、跟踪安全漏洞、灾难恢复机制与预防、安全审计、系统改造，以及网络安全咨询等。

3）**系统安全**(System Security)。主要包括操作系统安全、数据库系统安全和网络系统安全。以网络系统的特点、实际条件和管理要求为依据，通过针对性地为系统提供安全策略机制、保障措施、应急修复方法、安全建议和安全管理规范等，确保整个网络系统安全运行。

4）**应用安全**(Application Security)。由应用软件开发平台的安全和应用系统的数据安全两部分组成。包括：业务应用软件的安全性测试分析、业务数据的安全检测与审计、数据资源访问控制验证测试、实体身份鉴别检测、业务现场的备份与恢复机制检查、数据唯一性/一致性/防冲突检测、数据的保密性测试，以及系统的可靠性测试和系统的可用性测试等。

5）**管理安全**(Management Security)。也称**安全管理**，主要指对人员及网络系统安全管理的各种法律、法规、政策、策略、规范、标准、技术手段、机制和措施等。主要管理：法律法规、政策策略、规范标准、相关人员、应用系统使用、软件及设备、文档、数据、操作、运营、机房，以及安全培训等。

4. 网络安全内容的相互关系

网络安全所涉及的主要相关内容及其关系如图 1-1 所示。在网络信息安全法律法规的基础上，以安全管理为保障，实体运行安全为基础，以系统安全、运行安全和应用安全确保网络正常运行与服务。网络安全与信息安全相关内容及其相互关系如图 1-2 所示。

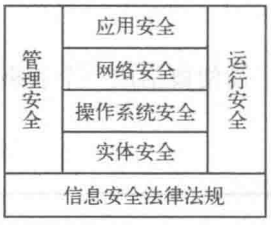

图 1-1　网络安全主要内容

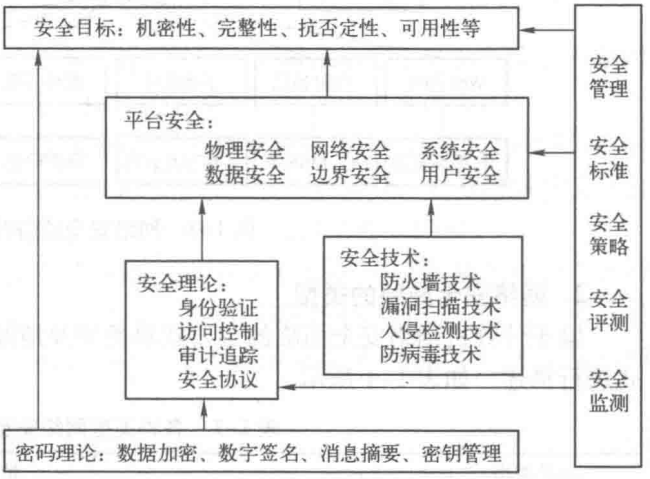

图 1-2　网络安全与信息安全相关内容

1.1.2　网络安全的威胁和风险

【案例 1-2】 美国网络间谍活动公诸于世。2013 年 6 月曾经参加美国安全局网络监控项目的斯诺登披露“棱镜事件”曝光，在香港公开爆料美国多次秘密利用超级软件监控包括其盟友在内的网络用户和电话记录，包括谷歌、雅虎、微软、苹果、Facebook、美国在线、PalTalk、Skype 和 YouTube 等九大公司帮助提供漏洞参数、开放服务器等，使其轻而易举地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。据称，思科参与了中国几乎所有大型网络项目的建设，涉及政府、军警、金融、海关、民航和医疗等要害部门。

1. 网络安全的威胁及其途径

掌握网络安全威胁的现状及途径，有利于更好地掌握网络安全的重要性、必要性和重要的现实意义，有助于深入讨论和强化网络安全。

【案例 1-3】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，2015 年 6 月 22 日至 28 日一周内被篡改网站数量为 4386 个，其中政府网站数量 132 个；境内被植入后门的网站数量为 1615 个；针对境内网站的仿冒页面数量为 3881 个；针对境内网站的仿冒页面涉及域名 259 个；一周境内感染网络病毒的主机数量约为 92.9 万个。新增信息安全漏洞 143 个，其中高危漏洞 39 个。其中大部分的攻击来自国外。

目前，随着信息技术的快速发展和广泛应用，国内外网络被攻击或受病毒侵扰等威胁的状况呈现出上升的态势，威胁的类型及途径变化多端。一些网络系统及操作系统、数据库系统、网络资源和应用服务都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、网游、下载软件或流媒体等，它们都存在大量安全隐患。主要**威胁的途径**如图 1-3 所示。

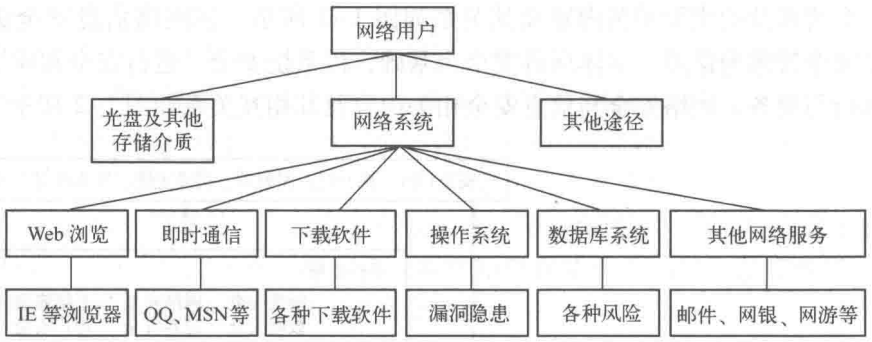

图 1-3　网络安全威胁的主要途径

2. 网络安全威胁的类型

鉴于计算机网络安全面临的主要威胁类型及情况比较复杂，为了简便概括成一个表格形式进行描述，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
网络窃听	网络传输信息被窃听
窃取资源	盗取系统重要的软件或硬件、信息和资料等资源
讹传信息	攻击者获得某些信息后，发送给他人
伪造信息	攻击者将伪造的信息发送给他人
篡改发送	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	以某种方式使系统响应减慢甚至瘫痪，使网络难以正常服务
行为抵赖	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
截获信息	从有关设备发出的无线射频或其他电磁辐射中提取信息