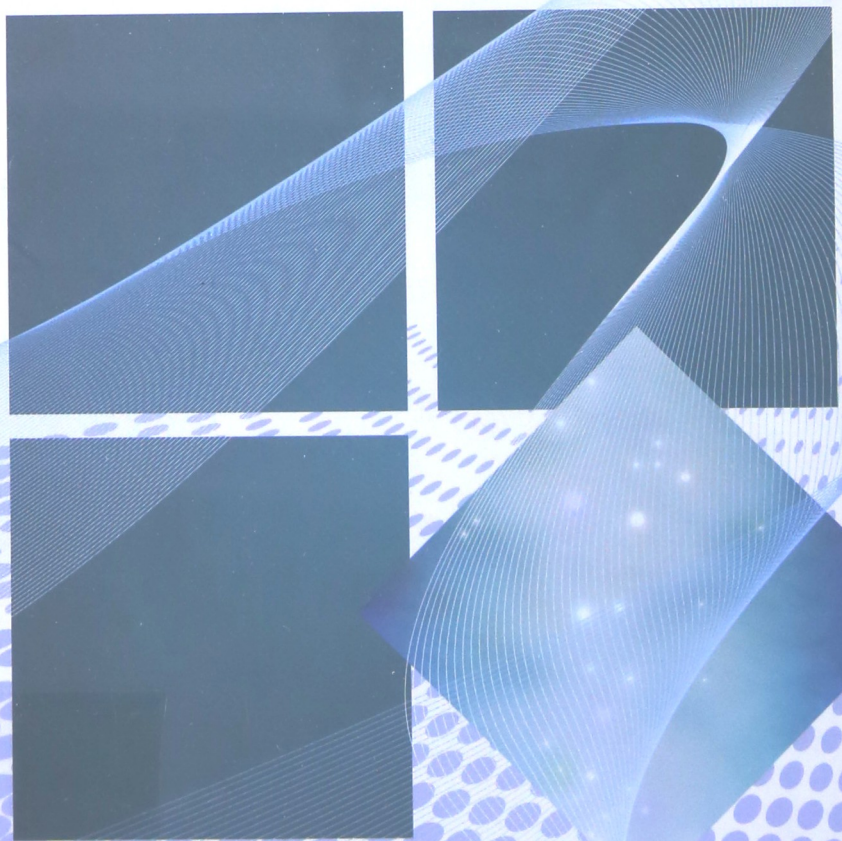
高等学校“十二五”规划教材
上海市精品课程配套教材
上海市教育高地建设项目

网络安全技术及应用学习与实践指导

贾铁军 主编



中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

高等学校“十二五”规划教材

上海市精品课程
上海市教育高地建设项目

网络安全技术及应用

学习与实践指导

贾铁军　主　编
陈国秦　宋少婷　副主编

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书是上海市精品课程“网络安全技术”的配套教材。全书结合最新网络安全技术及应用，介绍网络安全技术相关的基本知识、新技术、新应用方面的知识要点与实践指导，并附有练习题、复习题和模拟测试题等。全书共分三部分：第一篇，知识要点与学习指导，包括本章重点、难点、关键、教学目标，（各节）学习要求、知识要点及学习指导等；第二篇，实验与课程设计指导，包括同步实验指导（最新实验可选做任务）和课程设计综合应用指导；第三篇，习题与模拟测试，包括复习与练习题（含练习与实践应用题等多种题型及参考答案）、典型案例解析、模拟及自测题等。

本书提供实验课件，下载地址为 http://www.hxedu.com.cn。此外，上海市精品课程网站提供动画演练及教学视频、教学大纲、教案等资源，以及典型案例、应用程序、学习与交流样例、实验及课程设计指导、实践与练习题、复习及自测系统与试卷和答案等。

本书可作为高校计算机及信息类、电子商务类和管理类等专业本科生相关课程的教材，也可供高职院校选用，还可作为培训及其他参考用书。

图书在版编目 (CIP) 数据

网络安全技术及应用学习与实践指导/贾铁军主编. —北京：电子工业出版社，2015.4

高等学校“十二五”规划教材

ISBN 978-7-121-25647-9

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 045358 号

策划编辑：王晓庆

责任编辑：谭海平

印　　刷：三河市双峰印刷装订有限公司

装　　订：三河市双峰印刷装订有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱　　邮编：100036

开　　本：787×1 092　1/16　印张：18.5　　字数：473 千字

版　　次：2015 年 4 月第 1 版

印　　次：2015 年 4 月第 1 次印刷

定　　价：39.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010)88258888。

前　言

网络安全已成为21世纪世界热门课题之一，引起了社会的广泛关注。网络安全是个系统工程，已成为网络建设和发展的首要任务。网络安全技术涉及法律法规、政策、策略、规范、标准、机制、措施和管理等方面，它们是网络安全的重要保障。

信息技术的快速发展给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，我国在网络信息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等方面的广泛应用，使计算机网络已深入国家政治、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每个层面，“数字化经济”和全球电子交易一体化逐步形成。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、军事和经济等各个方面，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**。

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**，不仅关系到用户的信息和资产风险，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。只有在相关的法律、管理、技术、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。

我国非常重视网络安全工作。2014年2月，国家主席、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。指出：**网络安全和信息化是事关国家安全和发展，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。会议审议通过了《中央网络安全和信息化领导小组工作规则》、《中央网络安全和信息化领导小组办公室工作细则》、《中央网络安全和信息化领导小组2014年重点工作》，并研究了近期工作。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。

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、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之中。

为满足高校计算机、信息、通信、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，我们编著了这套规划教材。多年来，编著者一直从事计算机网络与安全等领域

的教学、研发及学科专业建设和管理工作，特别是多次主持过计算机网络安全方面的“上海市精品课程”建设及教学科研项目研究，积累了大量且宝贵的实践经验。

本书**主要内容**分三部分。第一篇，知识要点与学习指导，从知识内容体系结构方面包括：本章重点、难点、关键、教学目标，（各节）学习要求、知识要点、典型案例等；从知识、技术、方法及实际应用方面包括：网络安全的“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等基本理论和新实用技术学习与实践指导的知识要点构成的层次结构体系，主要结合新一代网络 IPv6、无线网安全、VPN 技术、Windows Server 2012、SQL Server 2012 和网络安全技术应用等知识要点进行指导帮助，包括：网络安全概述，网络安全技术基础，网络安全管理技术，密码与加密技术，黑客攻防、入侵检测与防御技术，身份认证与访问控制、电子证据与安全审计，操作系统与站点安全，网络安全与数据安全，计算机病毒防范技术，防火墙技术，网银及电子商务安全，网络安全新技术及解决方案等。第二篇，实验与课程设计指导，包括同步实验指导（最新实验任务 1-2 可选做）和课程设计综合应用指导。第三篇，习题与模拟测试，包括复习与练习题（含练习与实践应用题等多种题型及参考答案）、典型案例解析、模拟及自测题等。

书中内容包括经过多年实践总结的典型案例及成果，便于实际应用。书中带“*”部分为选学内容。**重点**介绍最新的网络安全技术、成果、方法和实际应用，其**特点**如下：

1．内容先进，结构新颖。本书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，图文并茂、学以致用。

2．突出实用及素质能力培养，增加大量案例和同步实验，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。提供多媒体实验课件和上海市精品课程“立体化”教学网站资源，便于自主学习和使用。教学资源主要包括：动画模拟实验演练视频、教学大纲与教案、教学视频、习题集、试题库与自测练习、辅导答疑、学习与新技术交流、典型案例、知识拓展等。以上资源可自上海市精品课程资源网站http://jiatj.sdju.edu.cn/webanq/访问，多媒体实验课件免费下载地址为 http://www.hxedu.com.cn。

本书由贾铁军教授任主编并编写第 1～9 章、第 12～14 章和第 16～17 章，陈国秦（腾讯控股有限公司）编写第 10～11 章，宋少婷（大连信源网络有限公司）编写第 15 章并制作部分课件等，多位老师参加了本书编写大纲的讨论、编著审校等工作。邹佳芹女士多次对全书的文字、图表进行了校对、编排及查阅资料，并完成了部分课件制作。

感谢对本书编写给予大力支持和帮助的院校及各界同仁。编著过程中参阅的大量重要文献资料难以完全准确注明，在此深表谢意！

由于网络安全技术涉及的内容比较庞杂，而且发展快、知识更新迅速，加之编著时间比较仓促及编著者水平有限，书中难免存在不妥之处，敬请海涵！欢迎提出宝贵意见和建议以便于改进，主编邮箱 jiatj@163.com。

编著者

2015 年 2 月于上海

目　录

第一篇　知识要点与学习指导

第二篇　实验与课程设计指导

第三篇 习题与模拟测试

第一篇

知识要点与学习指导

第 1 章　网络安全概述

为了更好地学习“网络安全技术”课程的基础知识、基本技术和基本方法，提高自主学习的能力和学习效率，并将所学到的网络安全知识、技术、方法和内容的体系结构系统化，同时便于更好地进行系统复习、总结和深化提高，有利于提高知识、素质和能力，对各章的知识要点与学习指导进行了系统概述。本章的网络安全及网络安全技术等相关概念和内容，对后续学习极为重要。

重点	信息安全、网络安全和网络安全技术等基本概念 网络安全的目标和内容，网络安全技术的种类和模型
难点	网络安全的目标和内容 网络安全技术的种类和模型
关键	网络安全和网络安全技术的基本概念 网络安全的目标和内容 网络安全技术的种类
教学目标	掌握网络安全的概念、目标和内容 理解网络安全面临的威胁及脆弱性 掌握网络安全技术的概念、种类和模型 理解网络安全研究现状与趋势 了解物理（实体安全）与隔离技术

1.1　网络安全概念及内容

1.1.1　学习要求

（1）熟悉信息安全和网络安全的概念。
（2）掌握网络安全的目标及特征。
（3）掌握网络安全涉及的内容及侧重点。

1.1.2　知识要点

1. 信息安全和网络安全的概念

国际标准化组织（ISO）对**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和管理的安全保护，保护计算机硬件、软件、数据不因偶然及恶意的原因而遭到破坏、更改和泄露。

我国《计算机信息系统安全保护条例》将**信息安全**定义为：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，确保信息的完整性、

保密性、可用性和可控性。主要涉及物理（实体）安全、运行（系统）安全与信息（数据）安全三个层面。

计算机网络安全（Computer Network Security）简称**网络安全**，是指利用计算机网络技术、管理、控制和措施，保证网络系统及数据（信息）的保密性、完整性、网络服务可用性、可控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数据（信息）资源不受有害因素的威胁和危害。广义上，凡是涉及计算机网络信息安全属性特征（保密性、完整性、可用性、可控性、可审查性）的相关知识、技术、管理、理论和方法等，都是网络安全的研究领域。

2．网络安全的目标及特征

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（数据）安全，而网络安全的最终目标和关键是保护网络的信息（数据）安全。

网络安全的目标是指计算机网络在信息的采集、存储、处理与传输的整个过程中，根据安全需求，达到相应的物理上及逻辑上的安全防护、监控、反应恢复和对抗的能力。网络安全的最终目标就是通过各种技术与管理手段，实现网络信息系统的保密性、完整性、可用性、可控性和可审查性。其中保密性、完整性、可用性是网络安全的基本要求。**网络信息安全的 5 大要素**，反映了网络安全的特征和目标要求。

（1）保密性。也称机密性，指将信息不泄露或提供给非授权用户、实体和过程。强调网络中信息只被授权用户使用的特征。

（2）完整性。指网络信息未经授权不可改变的特性，即信息在存储或传输过程中保持不被修改及破坏或丢失的特性。也是网络安全最基本的安全特征。

（3）可用性。也称有效性，指网络信息系统和信息资源可以被授权用户按照规定要求正常使用或在非正常情况下可恢复使用的特性。

（4）可控性。指对信息的传播及内容的管理控制能力，可以控制授权范围内的信息流向及行为方式。

（5）可审查性。可审查性又称不可否认性、抗抵赖性或拒绝否认性，指网络通信双方在信息传输交互过程中，确信发送方身份和所提供的信息真实同一性。

网络安全目标俗称要求达到“五不”：进不来、看不了、改不成、拿不走、跑不掉。

3．网络安全涉及的内容及侧重点

（1）网络安全涉及的主要内容

网络安全涉及的内容包括：操作系统安全、数据库安全、网络站点安全、病毒与防护、访问控制、加密与鉴别等。

从层次结构上，也可以将**网络安全所涉及的内容**概括如下：

① 物理安全。也称实体安全，指保护硬件系统和软件系统，即计算机网络设备、设施及其他媒介，免遭破坏的措施及过程。包括环境安全、设备安全和媒体安全三个方面。

② 运行安全。主要指为了网络系统正常运行和服务，所采取的各种安全措施。包括计算机网络及系统运行安全和网络访问控制的安全。

③ 系统安全。主要指为了确保整个系统的安全，所采取的各种安全举措。主要包括操作系统安全、数据库系统安全和网络系统安全。

④ 应用安全。主要指确保各种用户实际应用和服务的安全的措施。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。

⑤ 管理安全。也称为安全管理，主要指对相关人员及网络系统进行安全管理的各种法律、法规、政策、策略、规范、标准、技术手段、机制和措施等内容。

图 1-1 网络安全的层次结构

从层次结构上，**网络安全所涉及的主要内容及其关系**如图 1-1 所示。在网络信息安全法律法规的基础上，以安全管理和运行安全为保障，贯穿整个实体（物理）安全、操作系统安全、网络安全和应用安全的全过程，确保网络运行与服务安全平稳有序。

从体系结构方面，网络信息安全的主要内容及其相互关系，如图 1-2 所示。

从网络安全攻防体系方面，可以将网络安全研究的主要内容概括成两个体系：攻击技术和防御技术。该体系研究内容以后将陆续介绍，如图 1-3 所示。

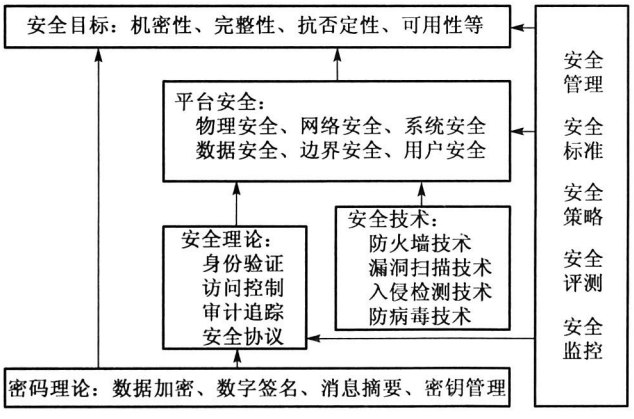


图 1-2 网络信息安全的内容及关系

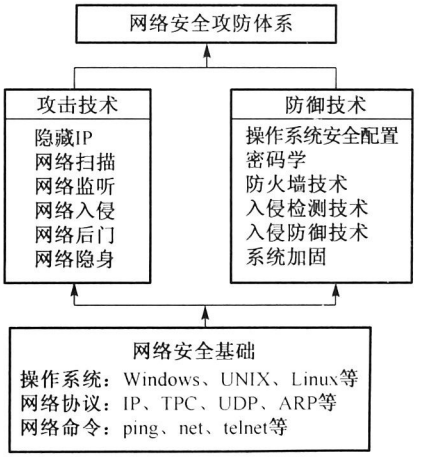


图 1-3 网络安全攻防体系

（2）网络安全保护范畴及重点

实际上，**网络安全涉及的内容**对不同人员或部门各有**侧重点**。

① 网络安全研究人员。关注从理论上采用数学等方法精确描述安全问题的属性特征，之后通过安全模型等进行具体解决。

② 网络安全工程师。主要侧重网络安全工程技术和方法，经常从实际应用角度出发，更注重成熟的网络安全解决方案和新型网络安全产品，注重网络安全工程建设开发与管理、安全防范工具、操作系统防护技术和安全应急处理措施等。

③ 网络安全评估人员。一般关注的是网络安全评价标准与准则、安全等级划分、网络安全风险评估、安全产品测评方法与工具、网络问题的评价、网络信息采集与分析等。

④ 网络安全管理员或主管。主要注重与网络安全管理有关的策略、机制、身份认证、访问控制、入侵检测、系统加固与防御措施、网络安全审计、网络安全应急响应和计算机病毒防治等安全管理技术与举措。

⑤ 安全保密监察人员。必须掌握网络信息泄露、窃听、检测和过滤等各种技术手段，确保涉及国家政治、军事、经济等重要机密信息的安全；检测和过滤威胁国家安全的不良信息传播，以免给国家安全和稳定带来不利的影响。

⑥ 军事国防相关人员。注重信息对抗、信息加密、安全通信协议、无线网络安全、入侵攻击与防范、应急处理和网络病毒传播等网络安全新技术、新方法，设法取得网络信息优势，扰乱敌方指挥系统，摧毁敌方网络基础设施，打赢未来信息战争。

1.2　网络安全的威胁及隐患

1.2.1　学习要求

（1）理解国内外网络安全的现状。

（2）掌握网络安全威胁类型及途径。

1.2.2　知识要点

1. 国内外网络安全的现状

国内外网络安全威胁的现状及主要因由，主要涉及以下 5 个方面。

（1）法律法规和管理不完善。

（2）企业和政府的侧重点不一致。

（3）网络安全规范和标准不统一。

（4）网络安全技术和手段滞后。

（5）网络安全风险和隐患增强。

注意：计算机病毒防范技术、网络防火墙技术和入侵检测技术，常被称为网络安全技术的三大主流。

2. 网络安全的主要威胁及途径

网络安全的主要威胁（见表 1-1）及途径如图 1-4 所示。

表 1-1　网络安全的主要威胁

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
截获/窃听	数据在网络系统传输中被截获、窃听信息
伪造信息	将伪造的信息发送给他人
篡改/修改	对合法用户之间的通信信息篡改/替换/删除或破坏
窃取资源	盗取系统重要的软件或硬件、信息和资料
病毒木马	利用计算机木马病毒及恶意软件进行破坏或恶意控制他人系统
讹传信息	攻击者获得某些非正常信息后，发送给他人
行为否认	通信实体否认已经发生的行为
旁路控制	利用系统的缺陷或安全脆弱性的非正常控制
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
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

（续表）

威胁类型	主要威胁
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
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
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
重发信息	重发某次截获的备份合法数据，达到信任并非法侵权目的
设置陷阱	违反安全策略，设置陷阱“机关”系统或部件，骗取特定数据
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
其他威胁	上述之外的其他各种攻击或威胁

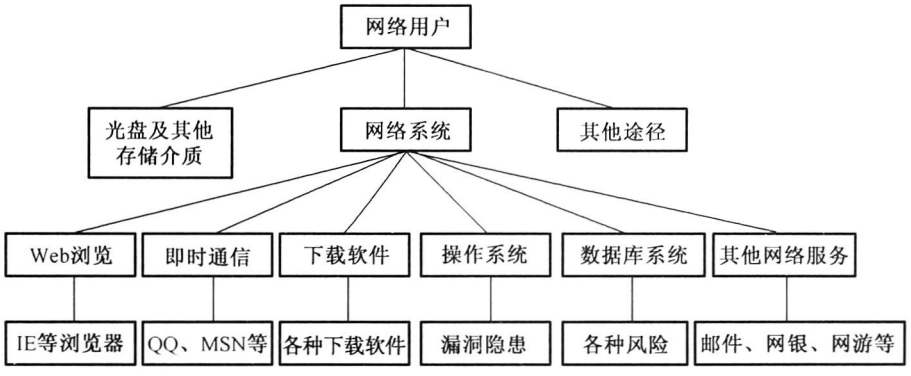


图 1-4 网络安全主要威胁及途径

3. 网络安全的隐患及风险

（1）网络系统安全隐患及风险。网络系统面临的安全隐患主要包括 7 个方面。

① 系统漏洞及复杂性。

② 网络协议及共享性。

③ 网络开放性。

④ 身份认证难。

⑤ 传输路径与节点不安全。

⑥ 信息聚集度高。

⑦ 边界难确定。

（2）操作系统的漏洞及隐患。包括体系结构的漏洞、创建进程的隐患、服务及设置风险、配置和初始化错误。

（3）网络数据库的安全风险。

（4）防火墙的局限性。

（5）网络安全管理及其他问题。

4. 网络安全威胁的发展态势

2015 年网络安全与管理趋势的十大预测，包括 10 个方面。

① 随着社交媒体和移动终端持续升温，大数据冲击时代即将到来。

② 随着混合云模式、大宗商品化软硬定义的数据中心（SDDC）等趋势日益深入，未来的数据中心将发生根本性的变革。
③“物联网”时代带来新挑战。
④“分布式数据”将对消费者带来困扰。
⑤ 针对企业的应用程序商店将得到普及。
⑥ 人们将过分依赖和相信网络应用程序。
⑦ 身份认证将成为主流。
⑧ 网络欺诈者、数据窃取者和网络罪犯将关注社交网络。
⑨ 3D 打印技术将为网络犯罪提供新可能。
⑩ 采取更积极的举措保护私人信息。

1.3　网络安全技术概述

1.3.1　学习要求

（1）熟练掌握网络安全技术相关概念及目标。
（2）掌握常用网络安全关键技术的种类。
（3）理解网络安全的常用模型。

1.3.2　知识要点

1. 网络安全技术概述

（1）网络安全技术相关概念

网络安全技术（Network Security Technology）是指计算机网络系统及其在数据采集、存储、处理和传输过程中，保障网络信息安全属性特征（保密性、完整性、可用性、可控性、可审查性）的各种相关技术和措施。狭义上是指为保障网络系统及数据在采集、存储、处理和传输过程中的安全（最终目标和关键是保护网络的数据安全），所采取的各种技术手段、机制、策略和措施等；广义上是指保护网络安全的各种技术手段、机制、策略和措施等。

（2）常用网络安全关键技术的种类

网络安全技术分类将网络安全技术分为预防保护类、检测跟踪类和响应恢复类三大类，如图 1-5 所示。

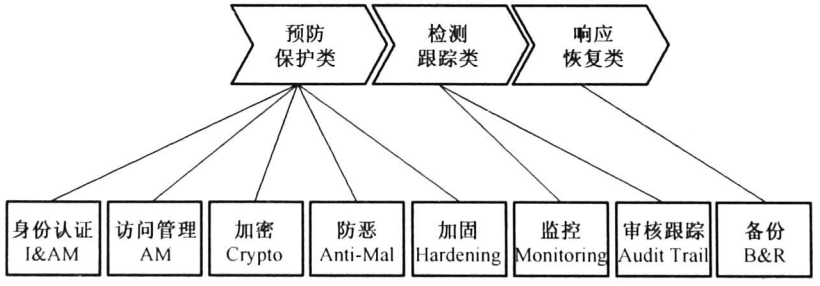


图 1-5　常用网络安全关键技术

常用的网络安全关键技术包括：

① 身份认证。确保网络用户身份的正确存储、同步、使用、管理和一致性确认，防止他人冒用或盗用的技术手段。

② 访问管理。用于确保授权用户在指定时间对授权的资源进行正当的访问，防止未经授权的访问的措施。

③ 加密。以加密技术，确保网络信息的保密性、完整性和可审查性。加密技术包括加密算法、密钥长度的定义和要求等，以及密钥整个生命周期（生成、分发、存储、输入/输出、更新、恢复、销毁等）的技术方法。

④ 防恶意代码。通过建立计算机病毒的预防、检测、隔离和清除机制，预防恶意代码入侵，迅速隔离查杀已感染病毒，识别并清除网内恶意代码。

⑤ 加固。对系统自身弱点采取的一种安全预防手段，主要是通过系统漏洞扫描、渗透性测试、安装安全补丁及入侵防御系统、关闭不必要的服务端口和对特定攻击的预防设置等技术或管理手段，确保并增强系统自身的安全。

⑥ 监控。通过监控主体的各种访问行为，确保对客体的访问过程中安全的技术手段，如安全监控系统、入侵监测系统等。

⑦ 审核跟踪。对出现的异常访问、探测及操作相关事件进行核查、记录和追踪。每个系统可以有多个审核跟踪不同的特定相关活动。

⑧ 备份恢复（Backup and Recovery）。网络出现异常、故障、入侵等意外事故时，确保及时恢复系统和数据而进行的预先备份等技术手段。

2. 网络安全常用模型

（1）网络安全通用模型

网络安全通用模型如图 1-6 所示，其不足是并非所有情况都通用。

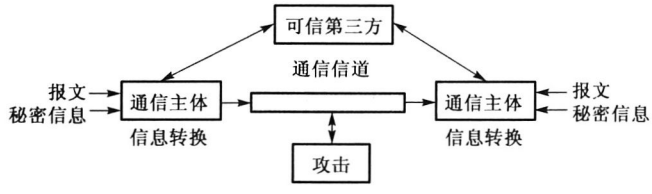


图 1-6 网络安全通用模型

（2）网络安全 PDRR 模型

描述网络安全整个过程和环节的常用网络安全模型为 PDRR 模型：防护（Protection）、检测（Detection）、响应（Reaction）和恢复（Recovery），如图 1-7 所示。

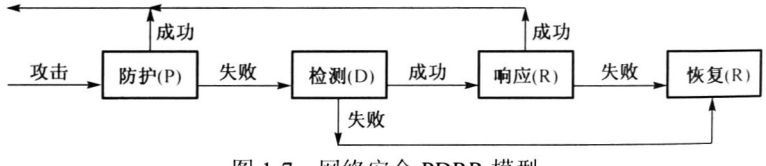


图 1-7 网络安全 PDRR 模型

在此模型的基础上，按照“检查准备、防护加固、检测发现、快速反应、确保恢复、反省改进”的原则，经过改进和完善得到另一个网络系统安全生命周期模型——IPDRRR（Inspection，Protection，Detection，Reaction，Recovery，Reflection）模型，如图 1-8 所示。