“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

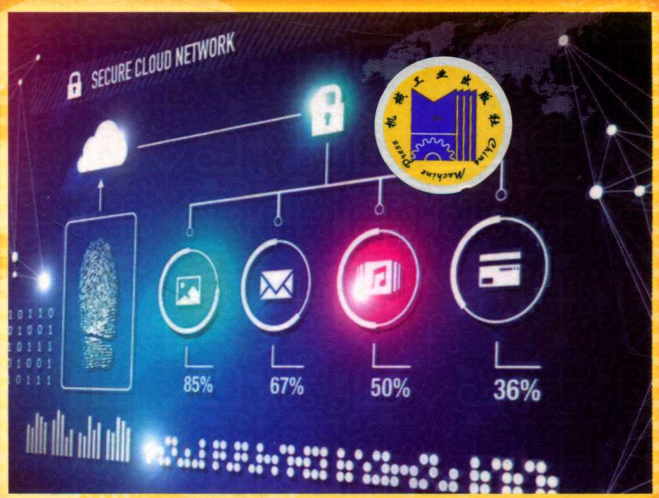
高等教育网络空间安全规划教材

# 网络安全技术及应用实践教程

第3版

主编　贾铁军　蒋建军

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
高等教育网络空间安全规划教材

# 网络安全技术及应用实践教程

## 第3版　立体化教材

主编　贾铁军　蒋建军
副主编　古乐声　杨德全　罗宜元　刘巧红
参编　王小刚　王　坚



机械工业出版社

本书内容为常用网络安全基本知识和技术要点，以及同步实验与综合课程设计指导，包括网络安全基础，网络安全技术基础，网络安全体系与管理、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；数据库与数据安全；电子商务安全、网络安全新技术及解决方案等，涉及“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等。本书为“十三五”国家重点出版物出版规划项目暨上海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”。

本书提供授课及实验动画视频、教学大纲及教案、同步实验和课程设计指导、练习及复习、编码等资源，并有配套学习与实践指导。

本书可作为院校计算机类、信息类、电子商务类、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。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实践教程 / 贾铁军，蒋建军主编 . —3 版 . —北京：机械工业出版社，2018.5

“十三五”国家重点出版物出版规划项目 高等教育网络空间安全规划教材

ISBN 978-7-111-60188-3

Ⅰ. ①网… Ⅱ. ①贾… ②蒋… 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（2018）第 126515 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：张 博

三河市国英印务有限公司印刷

2018 年 7 月第 3 版 · 第 1 次印刷

184mm×260mm · 23 印张 · 565 千字

0001-3000 册

标准书号：ISBN 978-7-111-60188-3

定价：69.00 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

随着信息化建设和网络技术的快速发展，各种信息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，不仅关系到国家安全和社会稳定，也关系到机构和个人用户的信息资源和资产风险，已成为热门研究和人才需求的新领域。因此，需要在法律、管理、技术、道德各方面采取切实可行的措施，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、动态性及安全性等特性，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给人类社会带来了深刻变革，特别是在网络化建设方面取得了巨大成就；电子商务、网银和电子政务的广泛应用，使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，遍布人们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，涉及国家政治、军事和经济各个领域，而且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。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。

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，在获得“上海市普通高校精品课程”和“上海市普通高等院校优秀教材奖”后，入选“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，再版了这本教材。主编和编著者多年来在高校从事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，特别是多次主持过网络安全方面的研究项目，积累了大量的宝贵实

践经验，谨以此书奉献给广大师生和其他读者。

**本书主要内容**共分 13 章，**重点**介绍了常用的网络安全基本知识和技术要点，以及同步实验与综合课程设计指导，主要包括网络安全基础，网络安全技术基础，网络安全体系与管理、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，数据库与数据安全，电子商务安全、网络安全新技术及解决方案等，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 3 版）配套的辅助教材，又可以单独使用。

**体系结构**：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。

**本书重点**介绍了最新网络安全技术、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、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，增加大量案例、同步实验及课程设计指导，将理论知识与实际应用有机结合。

3）资源丰富，便于教学。在出版社和上海市高校精品课程网站，提供多媒体课件、教学大纲和授课计划、电子教案、动画视频、同步实验、考证就业与深造、习题库，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。

**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（上海剑桥学院）任主编并编著第 1、2、11、12、13 章，蒋建军副教授（上海电机学院）任主编并编著第 3 章，杨德全（北京理工大学）任副主编并编著第 6、7 章，古乐声副教授（河南科技学院）任副主编并编著第 9、10 章，罗宜元副教授（上海电机学院）任副主编并编著第 8 章、刘巧红（上海健康医学院）任副主编并编著第 4、5 章，王小刚、王坚参与了本书编写工作。多位同仁和研究生对全书的文字、图表进行了校对、编排及查阅资料。

非常感谢机械工业出版社计算机分社的郝建伟主任，为本书的编著提供了许多重要帮助、指导意见和参考资料，并提出了很好的重要修改意见和建议，同时，非常感谢对本书编著过程中给予大力支持和帮助的院校及各界同仁。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。欢迎指正交流，主编邮箱：jiatj@163.com。

编　者

2018 年 6 月于上海

# 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，网络安全问题日益突出，已经引起世界各国的高度重视，并成为一个热门研究和人才需求的新领域。网络空间安全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、用户资产和信息资源的安全，其重要性和紧迫性更加突出。

**教学目标**

- 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
- 理解网络安全面临的威胁及发展态势
- 了解网络实体安全、隔离技术及应用
- 理解构建和设置虚拟局域网VLAN的方法

**教学课件**

第1章　课件资源

## 1.1　知识要点

【案例1-1】2016年，近70%网友曾遭遇电信网络诈骗。2016年，山东女大学生被骗近万元学费导致猝死、清华大学教授被骗上千万元等案件，使电信网络诈骗案件成为备受瞩目的社会热点之一。公安等相关部门为破解这个多年顽疾进行了重点整治。2016年前10个月，全国共破获电信诈骗案件9.3万起，收缴赃款赃物价值人民币23.8亿元，为群众挽回经济损失48.7亿元。2015年，全国共发生电信网络诈骗案59万余起，被骗222亿元。

**教学视频**

第1章　微视频

### 1.1.1　网络安全的概念和内容

**1. 网络安全的相关概念、目标和特征**

（1）网络安全与网络空间安全相关概念

信息安全（Information Security）是指系统的硬件、软件及其信息受到保护，并持续正常地运行和服务。**信息安全的实质**是保护信息系统和信息资源免受各种威胁、干扰和破坏，即保证信息的安全性；主要**目标**是防止信息被非授权泄露、更改、破坏，或被非法的系统辨识与控制，确保信息的保密性、完整性、可用性、可控性和可审查性（信息安全五大特

征)。在《计算机信息系统安全保护条例》中指出，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。

**国际标准化组织（ISO）对于信息安全给出的定义**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、数据不因偶然及恶意的原因而遭到破坏、更改和泄漏。

知识拓展
信息安全内涵的变化

网络安全（Network Security）是指利用网络技术、管理和控制等措施，保证网络系统和信息的保密性、完整性、可用性、可控性和可审查性。即保证网络系统及数据资源得到安全保护，不受干扰破坏和非授权使用。ISO/IEC27032：2012 中**网络安全**的定义则是指对网络的设计、实施和运营等过程中的信息及其相关系统的安全保护。

**注意**：网络安全不局限于计算机网络安全，还包括手机网络安全等。实际上，网络安全是一个相对的概念，世界上不存在绝对的安全，过分提高网络的安全性可能会降低网络传输速度，浪费资源和增加成本。

特别理解
网络安全概念的内涵

网络空间安全（Cyberspace Security）是研究网络空间中的信息在产生、传输、存储及处理等环节中所面临的威胁和防御措施，以及网络和系统本身的威胁和防护机制。不仅包括传统信息安全所研究的信息的保密性、完整性和可用性，还包括构成网络空间基础设施的安全和可信。首先需要明确信息安全、网络安全及网络空间安全这 3 个概念的异同，三者均属于非传统安全，均聚焦于信息安全问题。网络安全及网络空间安全的核心是信息安全，只是出发点和侧重点有所差别。

（2）网络安全的目标及特征

**网络安全的目标**是指在网络的信息传输、存储与处理的整个过程中，提高物理上、逻辑上的防护、监控、反应恢复和对抗的要求。网络安全的**主要目标**是通过各种技术与管理等手段，实现网络信息的保密性、完整性、可用性、可控性和可审查性（网络信息安全五大特征）。其中保密性、完整性和可用性是网络安全的**基本要求**。

知识拓展
网络空间安全与网络安全的关系

网络安全包括两个方面，一个是网络系统的安全，另一个是网络信息（数据）的安全。网络安全的**最终目标和关键**是保护网络信息的安全。**网络信息安全的特征**反映了网络安全的具体目标要求。

1）保密性（Confidentiality）。也称机密性，是指不将有用信息泄漏给非授权用户的特性。可以通过信息加密、身份认证、访问控制和安全通信协议等技术实现。信息加密是防止信息非法泄露的最基本手段，主要强调有用信息只被授权对象使用的特征。

2）完整性（Integrity）。是指信息在传输、交换、存储和处理过程中，保持信息不被破坏或修改、不丢失，以及信息未经授权不能改变的特性，也是最基本的安全特征。

3）可用性。也称有效性（Availability），是指信息资源可被授权实体按要求访问、正

常使用或在非正常情况下能恢复使用的特性（系统面向用户服务的安全特性）。在系统运行时，正确存取所需信息；当系统遭受意外攻击或破坏时，可以迅速恢复并能投入使用。可用性是衡量网络信息系统面向用户的一种安全性能，保障为用户提供服务。

4）可控性（Controllability）。是指网络系统和信息在传输范围和存放空间内的可控程度，是对网络系统和信息传输的控制能力特性。

5）可审查性。又称拒绝否认性（No-repudiation）、抗抵赖性或不可否认性，是指网络通信双方在信息交互过程中，确信参与者本身和所提供信息的真实同一性，即所有参与者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。

**2. 网络安全的内容及侧重点**

（1）网络安全涉及的内容

通常，网络安全的内容包括操作系统安全、数据库安全、网络及站点安全、病毒与防护、访问控制、加密与鉴别等方面，具体内容将在后续章节中分别进行详细介绍。也可从层次结构上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。也称物理安全，是指保护网络设备、设施及其他媒介免遭地震、水灾、火灾、有害气体和其他环境事故破坏的措施及过程。具体参见 1.3 节的介绍。

2）**系统安全**。主要包括网络系统安全（含应用系统）、操作系统安全和数据库系统安全。主要以网络系统的特点、条件和管理要求为依据，通过有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、安全要求和管理规范等，确保整个网络系统安全。

3）**运行安全**。包括相关系统的运行安全和访问控制安全，如用防火墙进行内外网隔离、访问控制和系统恢复。运行安全包括内外网隔离机制、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、跟踪最新安全漏洞、灾难恢复机制与预防、安全审计、系统改造、网络安全咨询等。

4）**应用安全**。由应用软件平台安全和应用数据安全两部分组成。应用安全包括业务应用软件的程序安全性测试分析、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、业务数据备份与恢复机制检查、数据唯一性或一致性、防冲突检测、数据保密性测试、系统可靠性测试和系统可用性测试等。

5）管理安全。也称安全管理，主要是指对人员、网络系统和应用与服务等要素的安全管理，涉及各种法律、法规、政策、策略、机制、规范、标准、技术手段和措施等内容。主要包括法律法规管理、政策策略管理、规范标准管理、人员管理、应用系统管理、软件管理、设备管理、文档管理、数据管理、操作管理、运营管理、机房管理和安全培训管理等。

广义网络安全的主要内容如图 1-1 所示。依据网络信息安全法律法规，以实体安全为基础，以管理和运行安全保障操作系统安全、网络安全（狭义）和应用安全及正常运行与服务。网络安全的相关内容及其相互关系如图 1-2 所示。📖

📖 知识拓展

网络安全层次结构的其他特点


图1-1　网络安全的主要内容

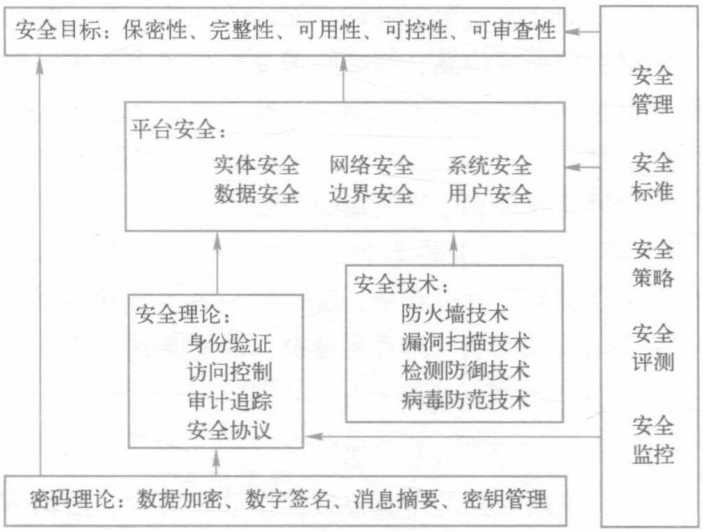



图1-2　网络安全的相关内容及其相互关系

（2）网络安全保护范畴及侧重点

【案例1-2】国家网络与信息安全中心紧急通报：2017年5月12日20时左右，新型“蠕虫”式勒索病毒爆发，很快就有100多个国家和地区的数万台计算机感染了该勒索病毒，我国部分Windows操作系统用户已经被感染。有关安全机构提醒广大计算机用户尽快升级并安装补丁，相关用户可打开并启用Windows防火墙，进入“高级设置”，禁用“文件和打印机共享”设置；或启用个人防火墙关闭445、135、137、138及139等高风险端口。

**网络安全涉及的内容**包括技术和管理等多个方面，需要相互补充、综合协同防范。技术方面主要侧重于防范外部非法攻击，管理方面则侧重于内部人为因素的管理。如何更有效地保护重要数据、提高网络系统的安全性，已经成为必须解决的一个重要问题。

**网络安全的关键及核心**是确保网络系统中的信息安全，凡涉及网络信息的可靠性、保密性、完整性、有效性、可控性和可审查性的理论、技术与管理，都属于网络安全的研究范畴，不同人员或部门对网络安全内容的侧重点有所不同。

1）网络安全工程人员。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。

特别理解
网络安全保护的范畴

2）网络安全研究人员。注重从理论上采用数学等方法精确描述安全问题的特征，之后通过安全模型等解决具体的网络安全问题。

3）网络安全评估人员。主要关注网络安全评价标准与准则、安全等级划分、安全产品测评方法与工具、网络信息采集、网络攻击及防御技术和采取的有效措施等。

4）网络管理员或安全管理员。主要侧重网络安全管理策略、身份认证、访问控制、入侵检测、防御与加固、网络安全审计、应急响应和计算机病毒防治等安全技术和措施。主要职责是配置与维护网络，在保护授权用户方便、快捷地访问网络资源的同时，必须防范

非法访问、病毒感染、黑客攻击、服务中断和垃圾邮件等各种威胁，一旦系统遭到破坏，使数据或文件破坏或丢失，可以采取相应的应急响应和恢复等措施。

5）国家安全保密人员。注重网络信息泄露、窃听和过滤的各种技术手段，以避免涉及国家政治、军事及经济等重要机密信息的无意或有意泄露；抑制和过滤威胁国家安全的暴力与邪教等信息的传播，以免给国家的稳定带来不利影响，甚至危害国家安全。

知识拓展
公共安全机构的要求

6）国防军事相关人员。更关心信息对抗、信息加密、安全通信协议、无线网络安全、入侵攻击、应急处理和网络病毒传播等网络安全综合技术，以此夺取网络信息优势、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。

注意：所有网络用户都应关心网络安全问题，注意保护个人隐私和商业信息不被窃取、篡改、破坏和非法存取，确保网络信息的保密性、完整性、有效性和可审查性。

## 1.1.2　网络安全技术概述

### 1. 网络安全技术的概念和通用技术

（1）网络安全技术相关概念

网络安全技术（Network Security Technology）是指为解决网络安全问题进行有效监控和管理，保障数据及系统安全的技术手段。主要包括实体安全技术、网络系统安全技术、数据安全、密码及加密技术、身份认证、访问控制、防恶意代码、检测防御、管理与运行安全技术等，以及确保安全服务和安全机制的策略等。

特别理解
网络安全技术的内涵

通过对网络系统的扫描、检测和评估，可以预测主体受攻击的可能性，以及风险和威胁。由此可以识别检测对象的系统资源，分析被攻击的可能指数，了解系统的安全风险和隐患，评估所存在的安全风险程度及等级。国防、证券及银行等一些非常重要的网络，安全性的要求最高，不允许受到入侵和破坏，扫描和评估技术标准更为严格。

监控和审计是与网络安全密切相关的技术。主要通过对网络通信过程中可疑、有害信息或异常行为进行记录，为事后处理提供依据，对黑客形成强有力的威慑，提高网络整体安全性。例如，局域网监控可提供内部网异常行为监控机制。

（2）通用的网络安全技术

**通用的网络安全技术**主要可以归纳为三大类。

1）预防保护类。包括身份认证、访问管理、加密、防恶意代码、入侵防御和加固等。

2）检测跟踪类。对网络客体的访问行为需要进行监控、检测和审计跟踪，防止在访问过程中可能产生的安全事故。

3）响应恢复类。网络或数据一旦发生重大安全故障，需要采取应急预案和有效措施，确保在最短的时间内对其事件进行应急响应和备份恢复，尽快将损失和影响降至最低。

【案例1-3】某银行以网络安全业务价值链的概念，将网络安全的技术手段分为预防保护类、检测跟踪类和响应恢复类三大类，如图1-3所示。

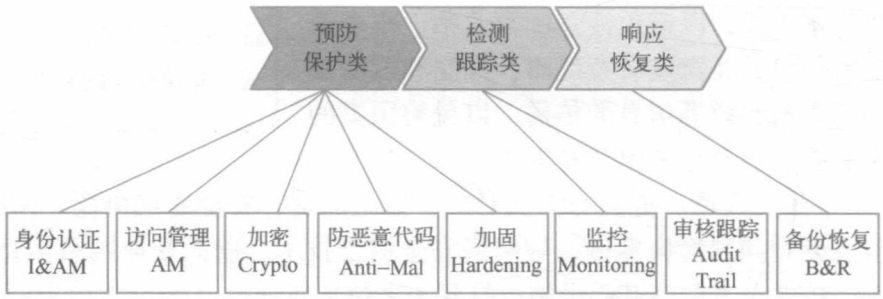



图1-3　常用的网络安全技术

主要的**通用网络安全技术**有8种，分别如下。

1）身份认证（Identity and Authentication）。通过网络身份的一致性确认，保护网络授权用户的正确存储、同步、使用、管理和控制，防止别人冒用或盗用的技术手段。

知识拓展
网络安全技术的缺陷

2）访问管理（Access Management）。保障授权用户在其权限内对授权资源进行正当使用，防止非授权使用的措施。

3）加密（Cryptograghy）。加密技术是最基本的网络安全手段，包括加密算法、密钥长度确定、密钥生命周期（生成、分发、存储、输入/输出、更新、恢复和销毁等）安全措施和管理等。

4）防恶意代码（Anti-Malicode）。建立健全恶意代码（计算机病毒及流氓软件）的预防、检测、隔离和清除机制，预防恶意代码入侵，迅速隔离和查杀已感染病毒，识别并清除网内恶意代码。

5）加固（Hardening）。对系统漏洞及隐患采取必要的安全防范措施，主要包括安全性配置、关闭不必要的服务端口、系统漏洞扫描、渗透性测试、安装或更新安全补丁、增设防御功能和对特定攻击的预防手段等，提高系统自身的安全。

6）监控（Monitoring）。通过监控用户主体的各种访问行为，确保对网络等客体的访问过程中有效地采用合适的安全技术手段。

7）审核跟踪（Audit Trail）。对网络系统异常访问、探测及操作等事件进行及时核查、记录和追踪。利用多项审核跟踪不同活动。

8）备份恢复（Backup and Recovery）。在网络系统出现异常、故障或入侵等意外情况时，及时恢复系统和数据而进行的预先备份等技术方法。备份恢复技术主要包括4个方面：备份技术、容错技术、冗余技术和不间断电源保护。

（3）网络空间安全新技术

网络空间安全新技术主要包括以下几种。

1）智能移动终端恶意代码检测技术。针对智能移动终端恶意代码研发的新型恶意代码检测技术，是在原有PC机已有的恶意代码检测技术的基础上，结合智能移动终端的特点引