上海市精品课程教材

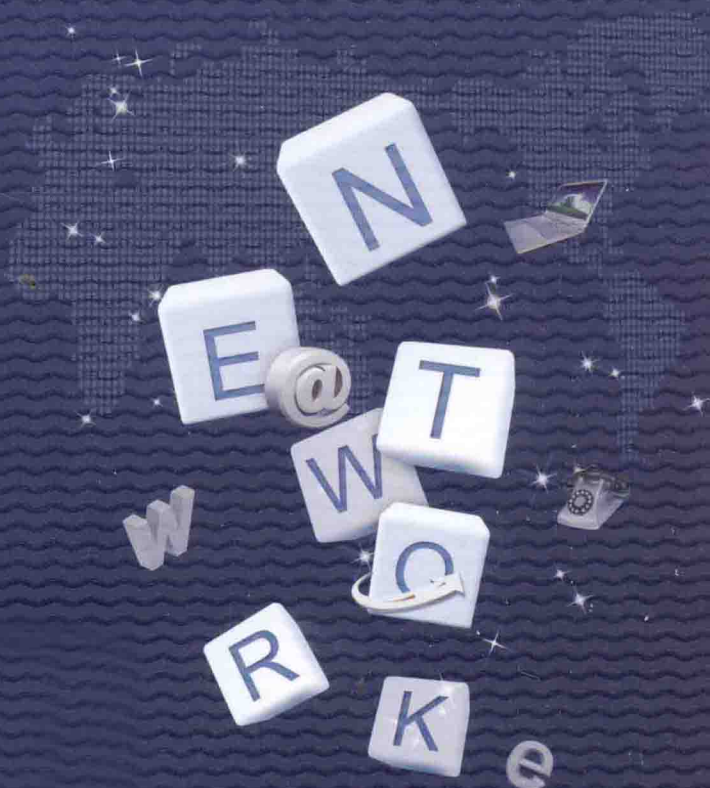
免费提供
电子教案

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

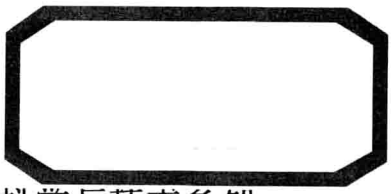
第2版

主　编　贾铁军



机械工业出版社
CHINA MACHINE PRESS

上海市精品课程教材
上海市教育高地建设项目
上海市重点课程建设项目
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

第2版

主编　贾铁军
副主编　陈国秦　苏庆刚　沈学东
参　编　王　坚　王小刚　宋少婷

机械工业出版社

本书内容包括网络安全技术基础知识、网络安全体系结构、无线网络安全技术、网络安全管理、黑客攻防技术、入侵检测与防御技术、身份认证与访问控制技术、密码及加密技术、数据库安全技术、计算机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、电子商务安全技术、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）”等多方面的基础理论和实用技术。本书着重突出“实用、特色、新颖、操作性”的特点，力求技术先进、实用性强。

本书通过上海市精品课程网站提供多媒体课件、动画视频、同步实验等教学资源，便于师生实践教学、课外延伸学习和网络安全综合解决方案练习。

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各专业的网络安全相关课程的教材（高职院校也可选用），也可作为培训及参考用书。

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：2966938356，电话：010 - 88379739）。

图书在版编目（CIP）数据

网络安全技术及应用/贾铁军主编．—2 版．—北京：机械工业出版社，2014. 8
高等院校规划教材·计算机科学与技术系列
ISBN 978-7-111-46983-4

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（2014）第 122187 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 吴超莉 责任校对：张艳霞
责任印制：李 洋

北京宝昌彩色印刷有限公司印刷

2014 年 9 月第 2 版·第 1 次印刷
184mm × 260mm · 22. 75 印张 · 565 千字
0001 - 3000 册
标准书号：ISBN 978-7-111-46983-4
定价：49. 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	网络服务
社 服 务 中 心：（010）88361066	教 材 网：http：//www. cmpedu. com
销 售 一 部：（010）68326294	机工官网：http://www. cmpbook. com
销 售 二 部：（010）88379649	机工官博：http://weibo. com/cmp1952
读者购书热线：（010）88379203	**封面无防伪标均为盗版**

此为试读，需要完整PDF请访问：www.ertongbook.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

前　言

进入21世纪，随着全球互联网和计算机网络技术的快速发展，世界各国和行业机构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等得到了广泛应用，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，不仅涉及国家政治、军事和经济各个方面，而且影响到国家的安全、主权和社会稳定。随着计算机网络的广泛应用和网络之间数据传输量的急剧增大，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，正在危及网络的发展和应用，而且已经成为各国关注的焦点，也成为研究热点和人才需求的新领域。

随着信息技术的发展与应用，网络安全的内涵在不断地延伸。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，作者编写了这本教材，同时配备了配套教材《网络安全技术及应用实践教程》。这次再版《网络安全技术及应用》，从新知识、新技术、新方法、新成果和新应用等方面都作了重大更新、修改和完善，并在每章增加了相应的同步实验指导、新的典型案例和新应用实例等。本书的主要作者30多年来，在公安和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。

本书为上海市教育高地暨特色专业建设项目、上海市重点课程建设项目成果之一。

本书共分12章，主要介绍了计算机网络安全常用的新技术和新应用，基本知识、基本理论、新技术和新方法，主要包括：计算机网络安全概论、网络面临的威胁及隐患和学习网络安全的必要性、网络安全研究现状及趋势、物理安全与隔离技术等；网络协议安全及IPv6的安全性、虚拟专用网（VPN）技术、无线网络安全技术及应用和常用网络安全管理命令等；网络安全体系结构、网络安全管理技术、安全服务与安全机制、网络安全法律法规、网络安全管理规范、评估准则及方法，网络安全管理的原则、制度、策略和规划等；入侵检测与防御技术、黑客的攻击与防范技术；身份认证与访问控制技术；网络安全中的密码与加密技术；计算机病毒及恶意软件的防护技术；防火墙技术及应用；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、网络安全解决方案和综合应用实例等。书中增加了很多生动的典型案例，以及作者经过多年的实践总结出来的知识体系、企事业应用实例和研究成果。书中带“*”部分为选学内容。

本书重点介绍了最新成果、防范技术、处理技术、方法和实际应用。本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。书中吸收了国内外大量的新知识、新技术、新应用、新成果、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，突出实用及素质能力培养，在内容安排上，通过大量案例将理论知识与网络安全技术的实际应用有机结合，并配有同步实验。

3）资源配套，便于教学。上海市精品课程网站配有动画模拟演练视频、教学视频、实验交流实例、实用程序及代码、课件、习题集、试卷库、知识拓展等，便于资源共享。为了方便师生教学，本书配有电子教案，并在配套的《网络安全技术及应用实践教程》提供更为详尽的同步实验指导、学习指导、练习测试等资源，可以根据需要进行选用。

上海市精品课程“网络安全技术”资源网站：http:jiatj. sdju. edu. cn/webanq/。

本书由贾铁军教授任主编、统稿并编写了1、2、4、5、6、11、12章。陈国秦（腾讯公司）任副主编并编著第3章，苏庆刚（上海电机学院）任副主编并编著第9章，沈学东（上海电机学院）任副主编并编著第10章，王坚（辽宁对外经贸学院）编著第7章，王小刚及宋少婷编著第8章，同时完成了部分习题解答和课件制作。于森参加本书大纲的讨论、编著审校等工作，邹佳芹对全书的文字、图表进行了校对编排并完成了查阅资料等工作。

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。

因作者水平所限，书中难免存在不妥之处，欢迎广大读者提出宝贵意见和建议。

编　者

第1版前言

随着计算机网络技术的快速发展，我国在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之间数据传输量的急剧增大，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，正在危及网络的发展和应用，现在已经成为各国关注的焦点，也成为研究热点和人才需求的新领域。

随着信息技术的发展与应用，网络安全的内涵在不断地延伸。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，要综合利用计算机、通信、数学和管理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，我们编著了本书，同时配备了配套教材《网络安全技术及应用实践教程》。本书的主要作者30多年来，在高校一直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。

本书共分12章，重点介绍了计算机网络安全的基本知识、原理及其应用技术，主要内容包括：计算机网络安全概述和基本安全问题；网络安全技术的基本概念、内容和方法；网络协议安全、安全体系结构、网络安全管理技术、安全服务与安全机制、无线网络安全技术及应用；入侵检测技术、黑客的攻击与防范技术；身份认证与访问控制技术；网络安全中的密码与压缩技术；病毒及恶意软件的防护技术；防火墙技术及应用；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等。书中给出了很多实例，以及作者经过多年的实践总结出来的案例及研究成果。书中带“*”部分为选学内容。

本书重点介绍了最新成果、防范技术、处理技术、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，突出实用及素质能力培养，在内容安排上，通过实例将理论知识与实际应用有机结合。

（3）资源配套，便于教学。为了方便教学，本书配有多媒体课件、电子教案、动画演练视频、常用软件等，并在配套的教材《网络安全技术及应用实践教程》中提供了同步实验、学习要点与指导、练习测试与复习等内容，供师生选用。

本书由贾铁军教授任主编、统稿并编写1~6、8、11、12章，上海理工大学叶春明教授对全书进行了审阅。沈学东副教授任副主编并编写了第10章、苏庆刚任副主编并编写了第9章、王小刚及王坚编写了第7章，完成了部分习题解答和课件制作。于森参加本书大纲的

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完成了查阅资料等工作，在此一并表示感谢。

感谢对本书编著给予大力支持和帮助的有关领导和同仁，也对编著过程中参阅的大量重要文献资料的作者深表谢意。

因作者水平所限，书中难免存在不妥之处，欢迎广大读者提出宝贵意见和建议。

编　者

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第 1 章　网络安全概论

随着 21 世纪信息技术的快速发展和广泛应用，信息资源共享给人们的工作和生活带来了极大的便利，同时网络安全问题更加突出。现在，网络安全问题已经成为世界热点问题之一，其重要性更加突出，不仅关系到企事业的顺利发展及用户资产和信息资源的风险，也关系到国家安全和社会稳定，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　网络安全的概念、特征和内容

【案例 1-1】 网络安全的威胁触目惊心。21 世纪是信息时代，信息成为国家的重要战略资源。世界各国都不惜巨资，优先发展和强化网络安全。强国推行信息垄断和强权，依仗信息优势控制弱国的信息技术。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。"科技竞争的重点是对信息技术这一制高点的争夺。据 2013 年 6 月日本《外交学者》报道，即使美国监控各国网络信息的"棱镜"事件已经引起世界轰动，印度政府仍在进行类似的项目。信息、资本、人才和商品的流向逐渐呈现出以信息为中心的竞争新格局。网络安全成为决定国家政治命脉、经济发展、军事强弱和文化复兴的关键因素。

1.1.1　网络安全的概念及特征

1. 信息安全及网络安全的概念

目前，国内外对信息安全尚无统一确切的定义。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、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》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，确保信息的完整性、保密性、可用性和可控性。

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：

1）通信保密阶段（Communication Security）。20世纪初期，对安全理论和技术的研究只侧重于密码学，这一阶段的信息安全可以简单称为通信安全。

2）信息安全阶段（Information Security）。20世纪60年代后，人类将信息安全的关注扩展为以保密性、完整性和可用性为目标的信息安全阶段。

3）信息保障阶段（Information Assurance）。20世纪90年代，也称网络信息系统安全阶段，信息安全的焦点衍生出可控性、可审查性、真实性等其他的原则和目标，信息安全也转化为从整体角度考虑其体系建设的信息保障阶段。

目前，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。

计算机网络安全（Computer Network Security）简称**网络安全**（Network Security），是指利用计算机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：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知识和研究成果，其概念、理论和技术正在不断发展完善中。

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、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

保密性也称**机密性**，是指网络信息按规定要求不泄露给非授权的个人、实体或过程，或提供其利用的特性，即保护有用信息不泄露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

完整性是指网络数据在传输、交换、存储和处理过程中保持非修改、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、传输，是最基本的安全特征。

（3）可用性

可用性是指网络信息可被授权实体正确访问，并按要求能正常使用或在非正常情况下能恢复使用的特征，即在系统运行时能正确存取所需信息，当系统遭受攻击或破坏时，能迅速恢复并投入使用。可用性是衡量网络信息系统面向用户的一种安全性能。

（4）可控性

可控性是指对流通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。除了采用常规的传播站点和传播内容监控这种形式外，最典型的如密码的托管政策，当加密算法交由第三方管理时，必须严格按规定可控执行。

（5）可审查性

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。

1.1.2 网络安全涉及的主要内容及相互关系

1. 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。

通常，网络安全的内容从技术方面包括：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、加密与鉴别等几个方面。具体内容将在以后章节中分别进行详细介绍。**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

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，包括：机房安全、场地安全、机房环境（温度、湿度、电磁、噪声、防尘、静电及振动等）、建筑安全（防火、防雷、围墙及门禁安全）、设施安全、设备可靠性、通信线路安全性、辐射控制与防泄露、动力、电源/空调、灾难预防与恢复等。

（2）运行安全

运行安全（Operation Security）包括计算机网络运行和网络访问控制的安全，如设置防火墙实现内外网的隔离、备份系统实现系统的恢复。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。

（3）系统安全

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。主要以网络系统的特点、实际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、安全建议和安全管理规范等，确保整个网络系统的安全运行。

（4）应用安全

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。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、实体的身份鉴别检测、业务现场的备份与恢复机制检查、数据的唯一性/一致性/防冲突检测、数据的保密性测试、系统的可靠性测试和系统的可用性测试等。

（5）管理安全

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、机制和措施等内容。管理安全包括：法律法规管理、政策策略管理、规范标准管理、人员管理、应用系统使用管理、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、安全培训管理等。

2. 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，以管理安全为保障，实体安全为基础，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。

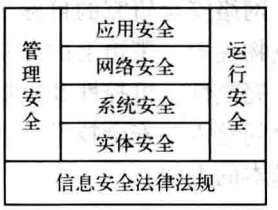


图 1-1　网络安全主要内容

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。

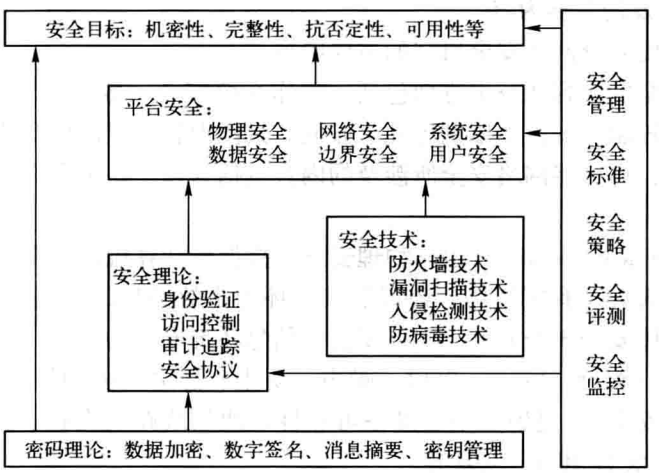


图 1-2　网络安全与信息安全相关内容

讨论思考：

1）网络安全的概念和主要特征是什么？

2）网络安全研究的目标是什么？

3）网络安全研究的主要内容有哪些？

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”，在中国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政要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、YouTube 等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

此为试读，需要完整PDF请访问：www.ertongbook.com