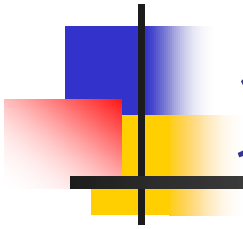
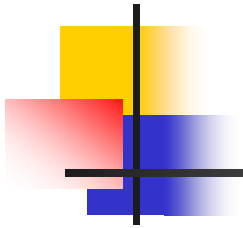


第1章 计算机网络安全概述

1 网络安全基础知识

2 网络安全机制与标准



第1章 信息系统安全概论

1.1 历史与现状

1.2 安全是什么

2.1 安全机制和安全政策

2.2 一些基本概念

2.3 安全标准

本章学习目标

（1）了解信息安全的现状、面临的威胁。

（2）明确安全的基本概念以及安全的需求，以及从经济学角度定义安全。

（3）了解安全机制和安全政策。

（4）了解密码学基本概念、攻击、恶意代码。

（5）了解安全标准及我国的信息安全标准化工作。

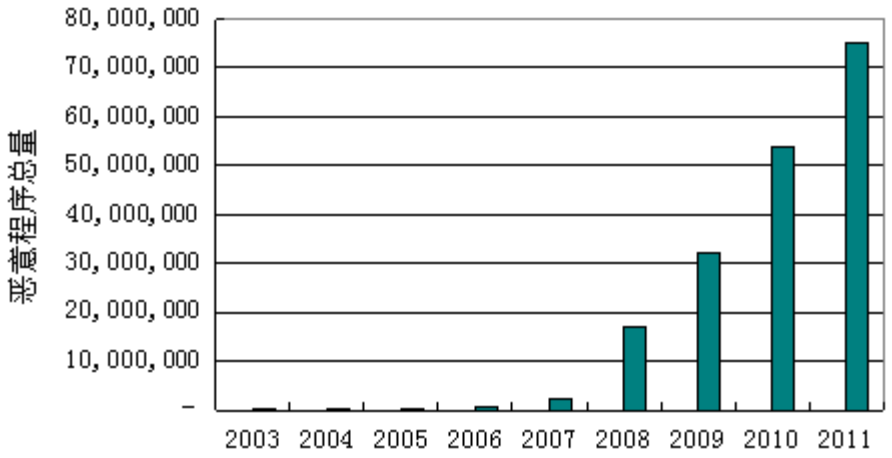
1. 网络安全基础知识

1.1 历史与现状

- Internet 起源于1969年初建立的ARPANET（Advanced Research Projects Agency Network）：一个非常小，独立封闭的，监管严格的网络。它是美国国防部高级研究计划管理局为准军事目的而建立的，开始只有4台主机，这就是只有4个节点的“网络之父”。
- 1972年公开展示时，由于一些学术研究和政府机构的加入，ARPANET网络已经连接了50所大学和研究机构的主机。
- 到1982年，ARPANET实现了与其他多种异构网络的互联，从而形成了以它为主干网的互联网。
- 1988年，莫里斯蠕虫病毒（Morris Worm）

名称	日期	影响
莫里斯（Morris）蠕虫	1988年	与Internet连接的10%的计算机当机
梅丽莎（Melissa）	1999年5月	一周内感染超过100000台计算机，造成损失约15亿美元
爱虫（I Love You）病毒	2000年5月	约87亿美元的经济影响
红色代码（Red Code）蠕虫	2001年7月	14小时内感染超过359000台计算机被感染
尼姆达（Nimda）蠕虫	2001年9月	高峰时160000台计算机被感染，超过15亿美元的经济影响
求职信（Klez）	2002年	7.5亿美元的经济影响
冲击波（Blaster）	2003年	约8亿美元的经济影响
震荡波（Sasser）	2004年5月	破坏能力和影响超过冲击波
极速波（Zobot）蠕虫	2005年8月	具有像“冲击波”和“震荡波”一样的传播能力的恶意蠕虫，而且对反病毒厂商提出了公开挑战
熊猫烧香	2006年	约80亿人民币的经济损失
灰鸽子2007	2005~2007年	国内后门的集大成者，连续三次位列年度十大病毒，
俄格网络战争	2008年	俄罗斯与格鲁吉亚的冲突中，双方利用互联网进行攻击。开启了信息战争的先河。
Conficker蠕虫	2009年	感染了超过千万的计算机

- 截至2011年6月底，中国网民数量达到 5.6亿；2011年上半年，有59.2%的网民遇到过病毒或木马攻击；有30.9%的网民账号或密码被盗过。
- 2011年12月，CSDN 600万用户密码泄露；2015年11月，免费邮箱 密码泄露，网盘账号无法登录
- 盗号木马 用户网游账号、网银账号，发送到黑客控制的服务器，具有极其明显的经济利益特征。



- 根本原因—信息的作用：表征和控制

  货币、股票、水电、武器、成绩等，信息系统，如银行证券、电力水务、作战部署、教务，物流
- 信息的特性：可重用性，复制、转换等成本低
- 面临的威胁：窃取、篡改、破坏，攻击—控制、载体**DoS**
- 威胁的严重性：攻击成本低，隐蔽性，瞬时性，受害面广（病毒蠕虫），风险小（分散）

网络安全国际化

- 随着全球信息化进程的加快，信息网络已深入应用到全球各国政治、经济、军事、科技、文化等多个领域。与此同时，网络安全威胁不断推陈出新，病毒传播、木马窃密、网络攻击等网络违法犯罪活动日益猖獗，趋利化特征明显，黑客攻击破坏活动越来越具有全球化特征，跨境网络违法犯罪给各国政府维护网络安全带来严峻挑战。
- 面对日益严峻复杂的国内外网络安全形势，美国、欧盟、日本等主要国家和地区高度重视网络安全立法，一方面加快出台网络安全基本法，另一方面强化政府信息安全、信息监控与内容安全、数据保护、关键基础设施保护等多方面立法，为网络安全保护各项措施的具体实施提供法律依据。

各国的行动

- 美国2014年通过了《国家网络安全保护法》，强化了国土安全部的国家网络安全和通信集成中心在联邦部门和私营部门共享网络安全信息方面的重要作用，为立足国家层面部署和加强公共和私营部门网络安全信息共享提供了法律依据。
- 俄罗斯、加拿大分别出台《联邦信息、信息化和数据保护法》、《信息安全法》，作为保护本国网络与信息安全的基本法律。
- 日本2014年颁布《网络安全基本法》，明确设立“网络安全战略本部”以统一协调各部门的网络安全政策，并对电力、金融等基础设施运营方落实网络安全相关措施提出了要求。
- 中国2015年《国家网络安全法》（草案）正式发布，作为我国网络安全领域具有最高效力的法律，《国家网络安全法》共七章六十八条，从网络运行安全、关键信息基础设施安全、网络信息安全、法律责任等方面进行了明确规定，将等级保护、网络产品与服务安全、网络安全信息共享、个人信息保护等多项工作纳入法律轨道，为保障国家网络安全、促进我国信息化健康发展提供了高层次的法律依据。

1.2 安全是什么

1.2.1 真正的安全

实体—人、计算机、进程， 能做**or**不能做

网络安全是指网络系统的硬、软件及其系统中的数据受到保护，不会由于偶然或恶意的原因而遭到破坏、更改、泄露等。

安全需求：

- 信息安全—保密性（加密）、完整性（签名，校验）
- 实体身份认证 人（外貌、声音、证件），信息系统（口令，**IC**卡、指纹、虹膜等）
- 访问控制 – 规则模型
- 行为审计、抗抵赖、可控性
- 可用性 **DoS**（拒绝服务）

问题：有没有*通用的方法*保证真正的安全？

安全的前提限制

1.2.2 从经济学角度定义安全

从投资角度理解适度的安全 100 200 -60 90 10 40

风险－投资效果图

风险评估模型

风险＝威胁x漏洞数目x可能受攻击的资产

威胁＝暴露的时间x（对手实施攻击的概率及水平）

暴露的时间＝检测到攻击的时间＋响应时间-入侵所需时间

2 安全机制和安全政策

2.1 安全机制

保护、检测、容忍、响应、取证、反击

2.2 安全政策

与安全管理模式相关的政策

集中式和分布式、所有者和管理员

访问控制相关的政策（模型）

最小特权、最大共享、开放和封闭

基于名字（属性）、基于内容、基于访问类型、上下文

与控制信息流动方向相关的政策

自主访问控制、多层分级控制、强制访问控制（高级不得传给低级）- 设计数学模型

2.3 一些基本概念

2.3.1 密码学基本概念

- 对称密码算法与非对称密码算法
- 数字签名 网络购物
- 哈希函数 **128b 160b**
- 零知识认证

  零知识洞穴（**Quisquater-Guillou**） 概率**1/2^n**

  零知识与美国国防部事件 **1986.7.9**美国专利申请

  Feige-Fiat-Shamir 零知识身份识别协议

  1987.1.6 禁令，两天后取消

2.3.2 攻击

被动攻击 包括嗅探、信息收集、通信量分析等， 数据的合法用户对这种活动一点也不会觉察到。

主动攻击 包括拒绝服务攻击、信息篡改、资源使用、欺骗、入侵、恶意代码、破坏数据完整性等

邻近攻击 物理接近网络、系统或设备

内部人员攻击 恶意、非恶意，难于检测和防范（顶替）间谍建立连接秘密通道

分发攻击 软硬件开发出来之后和安装之前（生产线上）修改配置

2.3.3 恶意代码

- 特洛伊木马
- 病毒
- 蠕虫
- 陷门（后门）2016年2月，苹果与FBI关于iPhone解密问题
- 逻辑炸弹 特定条件，如特定时间，启动
- 僵尸 DoS用途

2.4 安全标准

标准-规范-产业，产品，安全防范

1 国际标准化组织

2 国际电报和电话咨询委员会

3 电气和电子工程师学会

4 Internet体系结构委员会

5 美国国家标准局与美国商业部国家技术标准研究所

6 美国国防部及国家计算机安全中心

7 我国的信息安全标准化工作

8 其他有关密码的协议

国际标准化组织（ISO）信息技术安全标准

- SC17 ID卡和信用卡安全
- ISO/IEC JTC1/SC27 信息技术安全
- ISO/TC46 信息系统安全
- ISO/TC68/SC2 银行操作和规程（有关信息安全的标准）
- ISO/TC65 要害保险系统安全
- ISO/TC154 电子数据交换EDI安全

安全服务、安全机制

国际电报和电话咨询委员会

- 国际电报电话咨询委员会(CCITT)是国际电信联盟(ITU)的一个组成部分
- X.400：（Message Handling Service Protocol）— 信息处理服务协议，是由 ITU-T 和 ISO 定义用于电子邮件传输的信息处理服务协议。
- X.509被广泛使用的数字证书标准，是由国际电联电信委员会（ITU-T）为单点登录（SSO-Single Sign-on）和授权管理基础设施（PMI-Privilege Management Infrastructure）制定的PKI标准。
- 作为ITU X.500目录服务标准的一部分。它设定了一系列严格的证书授权CA分级体系来颁发数字证书。和其他网络信任模型（譬如PGP)对比，除了特定的CA，任何人可以签发并验证其他密钥证书的有效性。

电气和电子工程师学会

- IEEE即国际电气与电子工程师学会（The Institute of Electrical and Electronics Engineers）该组织在太空、计算机、电信、生物医学、电力及消费性电子产品等领域中都是主要的权威。在电气及电子工程、计算机及控制技术领域中，IEEE 发表的文献占了全球将近百分之三十。
- IEEE被国际标准化组织授权为可以制定标准的组织，设有专门的标准工作委员会，有30000义务工作者参与标准的研究和制定工作，每年制定和修订800多个技术标准。
- IEEE的标准制定内容有：电气与电子设备、试验方法、原器件、符号、定义以及测试方法等。
- IEEE P1363公钥密码体制，密钥管理，密钥签名，加密 Diffie-Hellman离散对数，椭圆曲线，DSA ，RSA

Internet体系结构委员会

- IETF(Internet工程任务组)等。IETF标准制定的具体工作由各个工作组承担。Internet工程任务组分成8个工作组，分别负责Internet路由、传输、应用等8个领域，TCP/IP协议，其著名的IKE和IPSec都在征求意见草案RFC系列之中，还有电子邮件、网络认证和密码及其他安全协议标准。

美国

- 美国国家标准与技术研究院（**National Institute of Standards and Technology，NIST**）原名美国国家标准局（**NBS**），直属美国商务部，从事物理、生物和工程方面的基础和应用研究，以及测量技术和测试方法方面的研究，提供标准、标准参考数据及有关服务，
- **DES**，云计算及安全标准的制定
- 《关键基础设施网络安全框架》
- 美国国家安全局（**National Security Agency**，简写为**NSA**），隶属于美国国防部，又称国家保密局。由于过于神秘，甚至完全不为美国政府的其他部门所了解，所以它的缩写**NSA**经常被戏称为“**No Such Agency**（没有这个局）”。

- **NSA密钥**

  所谓**NSA**密钥，是指**1998**年有人发现**Windows**操作系统中存在用途等详情不清的第二把密钥。**1999**年**8**月，加拿大**Cryotonym**公司的首席科学家**Andrew Fernandes**宣布，他发现这第二把密钥叫做**NSAkey**，而**NSA**就是美国国家安全局的简称，也就是说，微软公司在每一份**Windows**操作系统中都安装了一个程序上的“后门”，专供**NSA**在需要时进入全世界**Windows**用户的电脑。

- 棱镜门

  棱镜计划（英文名称：**Prism**）一项由美国国家安全局自**2007**年起开始实施的计划。该计划的正式名称为“**US-984XN**”。

  据美国中情局前职员爱德华·斯诺登爆料：“棱镜”窃听计划，始于**2007**年的小布什时期，美国情报机构一直在九家美国互联网公司中进行数据挖掘工作，从音频、视频、图片、邮件、文档以及连接信息中分析个人的联系方式与行动。监控的类型有**10**类：信息电邮，即时消息，视频，照片，存储数据，语音聊天，文件传输，视频会议，登录时间，社交网络资料的细节，其中包括两个秘密监视项目，一是监视、监听民众电话的通话记录，二是监视民众的网络活动。**2013**年**7**月**1**日晚，维基解密网站披露，美国“棱镜门”事件泄密者爱德华·斯诺登**(Edward Snowden)**在向厄瓜多尔和冰岛申请庇护后，又向**19**个国家寻求政治庇护。

中国的信息安全标准

- 《信息安全标准体系》是全国信息安全标准化技术委员会的技术文件，用于指导信息安全标准制定和信息安全标准实施。
- **2005**年，《国家信息安全标准体系》**v1.0**
- **2012**年，《国家信息安全标准体系》**v2.0**
- 近年来信息安全国家标准研究与制定情况，对现有信息安全国家标准进行了归类和整理而提出的。
- 该标准体系编制原则：既能保持与国际接轨，又能体现全国信息安全标准化技术委员会的工作特点；既能反映标准体系的共性，又能体现信息安全标准化的特征。
- 我国的信息安全标准命名格式：

  GB/T nnnnn.x-y(nnnnn表示分类编号，**x**表示部分系数，**y**表示年份**)**

  GB/T 25069-2010 信息安全技术 术语

  GB/T 29829-2013 信息安全技术 可信计算密码支撑平台功能与接口规范

  GJB 国家军用标准

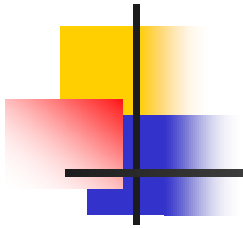
国家信息安全标准体系介绍

信息安全技术标准从总体上可划分为七大类：

- 基础标准
- 技术与机制标准
- 管理标准
- 测评标准
- 密码标准
- 保密标准
- 通信安全标准

其他有关密码的协议

- **PKCS The Public-Key Cryptography Standards (PKCS)**是由美国**RSA**数据安全公司及其合作伙伴制定的一组公钥密码学标准，其中包括证书申请、证书更新、证书作废表发布、扩展证书内容以及数字签名、数字信封的格式等方面的一系列相关协议。
- **HTTPS**（全称：**Hyper Text Transfer Protocol over Secure Socket Layer**），**HTTP**下加入**SSL**层，采用不同于**HTTP**的默认端口及一个加密/身份验证层（在**HTTP**与**TCP**之间）。这个系统的最初研发由网景公司**(Netscape)**进行，并内置于其浏览器**Netscape Navigator**中，提供了身份验证与加密通讯方法。现在被广泛用于各种浏览器上进行安全敏感的通讯，例如交易支付方面。
- **SET** 安全电子交易协议**(Secure Electronic Transaction)** 由**VISA**、**MasterCard**国际组织创建，结合**IBM**、**Microsoft**、**Netscape**、**GTE**等公司制定的电子商务中安全电子交易的一个国际标准。通过**SET**协议可以实现电子商务交易中的加密、认证、密钥管理机制等，保证了在因特网上使用信用卡进行在线购物的安全。



网络安全与电子商务

- 电子商务是以Internet为基础进行的商务活动，它通过Internet进行包括政府、商业、教育、保健和娱乐等活动。
- 下面是一个日常网上购物（电子商务）活动的案例。一个持有信用卡的消费者进行网上购物的流程如下：

网络安全与电子商务

① 消费者在客户机上浏览商家的网站，查看和 浏览在线商品目录及性能等；

② 消费者选择中意的商品（放入购物车）；

③ 消费者填写定单，包括项目列表、单价、数量、金额、运费等；

④ 消费者选择付款方式，如网上支付。此时开始启动安全电子交易（SET）协议；

⑤ 消费者通过网络发送给商家一个完整的定单和要求付款的请求；

网络安全与电子商务

⑥ 商家接到定单后，通过支付网关向消费者信用卡的开户银行请求支付；在银行和发卡机构经检验确认和批准交易后，支付网关给商家返回确认信息；

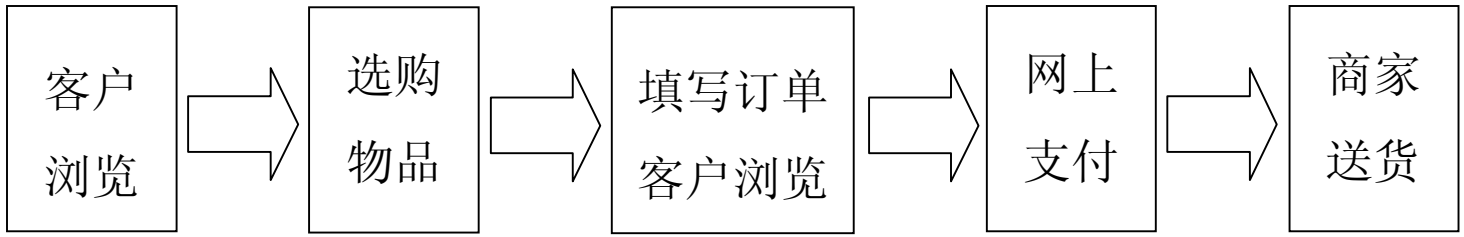
⑦ 商家通过网络给消费者发送定单确认信息；

⑧ 商家请求银行将钱从消费者的信用卡账号中划拨到商家账号；

⑨ 商家为消费者配送货物，完成订购服务。

网络安全与电子商务

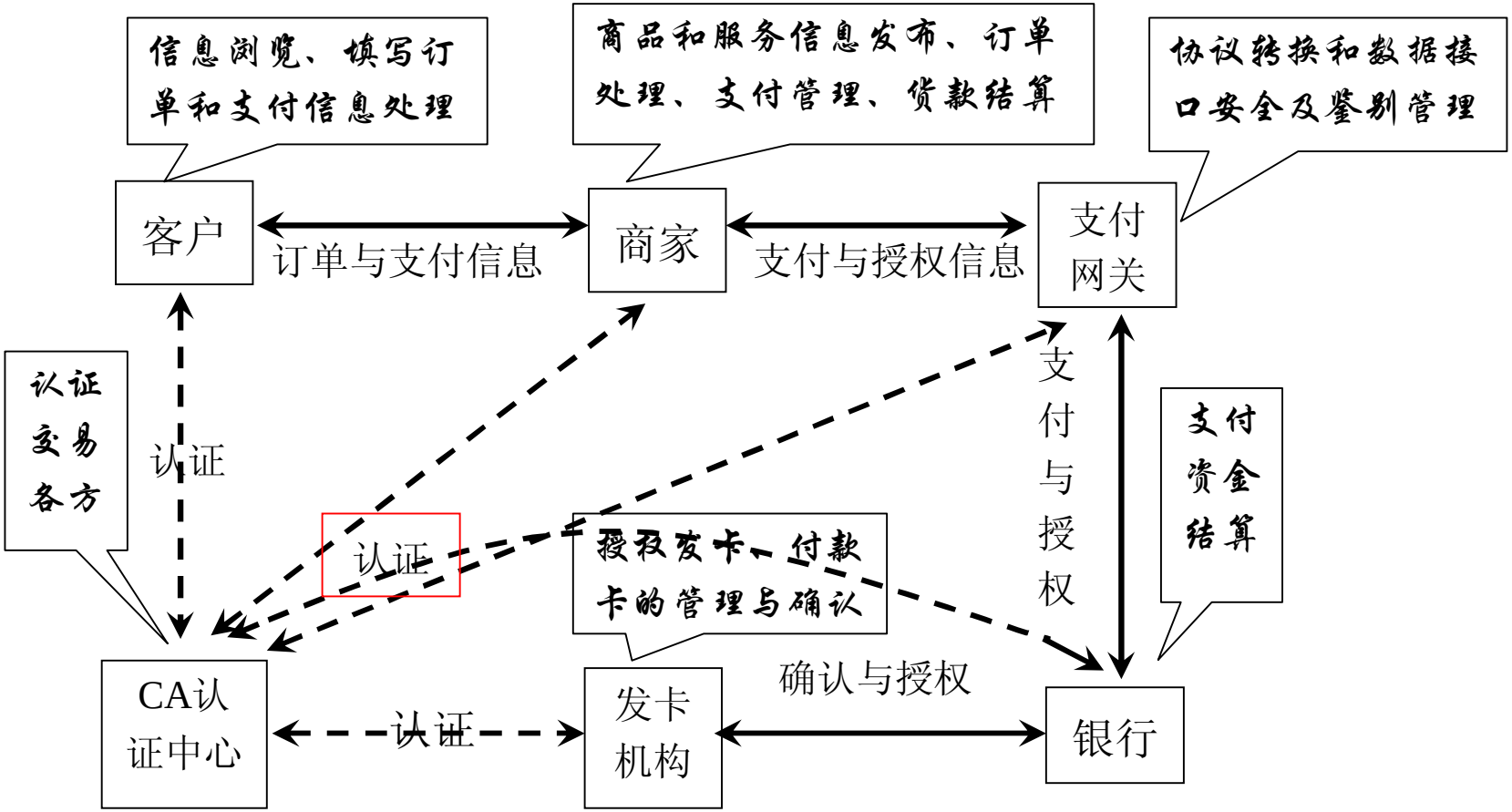
- 至此，一次网上购物过程结束。该过程可以简化为如下图所示五个过程：



简单的网上购物流程

网络安全与电子商务

- 但网上购物涉及的这五个过程中每个过程都包含一些具体操作，甚至是很复杂的具体操作。网上支付过程就涉及上述流程中的第④一第⑧步。网上支付所用的安全电子交易协议SET很复杂，与网上购物涉及的6个实体均有联系，如下图所示。



利用SET协议的网上购物流程

网络安全与电子商务

- 从网上购物流程可见，SET协议流程的许多步骤都涉及到网上交易的各方。还涉及到很复杂的网络安全管理和安全支付问题，如持卡人的数字签名、CA认证、信息的加密和鉴别、数字证书等。
- 由此可见，电子商务活动需要有一个安全的环境基础，以保证数据在网络中存储和传输的保密性和完整性，实现交易各方的身份验证，防止交易中抵赖行为的发生等。

网络安全与电子商务

- 除电子商务应用外，目前很多在Internet和其他网络上的应用也都涉及网络的信息安全技术，如数据加密、身份鉴别、病毒防治、网络数据库安全、访问控制、认证技术等，本课程将在此后各章介绍这些技术原理及其应用。