21世纪 高等学校信息安全专业规划教材

信息安全基础

李拴保　主编

清华大学出版社

21世纪高等学校信息安全专业规划教材

信息安全基础

李拴保　主编

清华大学出版社
北京

内 容 简 介

信息安全是一门涉及通信工程、计算机科学与技术、电子信息工程、数学、物理学、管理学、法学等领域的新兴交叉学科，本书用通俗易懂的语言阐述了信息安全面临的威胁以及所涉及的关键技术。

本书内容面向市场，简单易学，全面、专业。全书共9章，主要包括信息安全概述、物理安全、密码学基础与应用、网络攻击与安全防范、网络安全技术、信息系统安全、信息内容安全、云计算与云安全、信息安全管理。

本书配有习题和实训，可作为应用型本科、独立学院和高职高专院校信息安全、网络工程、计算机网络技术等相关专业教材，也可作为计算机科学与技术、软件工程、电子商务、信息管理与信息系统等专业的选修课教材。

图书在版编目(CIP)数据

信息安全基础/李拴保主编. —北京：清华大学出版社，2014
21世纪高等学校信息安全专业规划教材
ISBN 978-7-302-37034-5

Ⅰ. ①信… Ⅱ. ①李… Ⅲ. ①信息系统－安全技术－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2014)第143057号

责任编辑：郑寅堃　赵晓宁
封面设计：杨　兮
责任校对：白　蕾
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：16.25　　**字　　数**：396千字
版　　次：2014年9月第1版　　**印　　次**：2014年9月第1次印刷
印　　数：1～2000
定　　价：32.00元

产品编号：057015-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

（3）实施精品战略，突出重点。规划教材建设把重点放在专业核心（基础）课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

（4）支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

（5）依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21 世纪高等学校信息安全专业规划教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

前　言

21世纪是信息的时代。信息已经成为一种重要的战略资源，以 Internet 为代表的计算机网络正引起社会和经济的深刻变革，极大地改变了人们的生活和工作方式，是人们生活和工作不可分割的组成部分。因此，确保网络与信息安全已经成为全球关注的重要问题和信息技术领域的研究热点。

本书融入了作者最近几年从事计算机网络与信息安全教学、科研的成果。全书内容面向市场需求，简单易学，全面、专业，所有软件实训方案均由 Windows Server 2003 真实验证，所有硬件实训方案均可在神州数码网络安全设备实现。

本书编写的方法是尊重人类认识事物的基本规律，即从简单到复杂、从具体到抽象、从特殊到一般，以实践为基础；认识信息安全的基本规律、信息安全面临的威胁、解决威胁的主要技术，硬件设备的安全和操作系统的安全是信息安全的基础，密码技术、网络安全技术是关键技术，遵循这一主线，阐述物理安全、密码技术、网络安全等主要防御机制。

全书共 9 章，第 1 章介绍信息安全的根源、意义、含义和方向；第 2 章阐述物理安全；第 3 章引入密码学基础与应用；第 4 章论述网络攻击与安全防范；第 5 章介绍网络安全技术；第 6 章阐述信息系统安全；第 7 章探讨信息内容安全；第 8 章介绍云计算与云安全；第 9 章引入信息安全管理。内容编排符合认识规律，逻辑性强；案例贯穿于每一章，内容讲解清晰透彻，重要知识技能引入实训。

读者最好具有计算机与通信系统的基本知识，包括数据结构、操作系统、计算机原理、计算机网络和现代通信原理。作为应用型教材，网络安全技能知识可以作为一门课程独立开设。作者主编的《网络安全技术》(清华大学出版社出版)是一本很不错的教材。对于信息安全专业的学生，可选修“信息安全数学基础”和“现代密码学”等相关课程。

本书由李拴保主编。建议学时数为 64～72 学时。对于网络实训设备不够的学校，建议采用思科模拟器 Packet Tracer 5.3 进行实训。

本书配有习题、素材和实训，相关内容可从清华大学出版社网站下载，对本书的建议可发送至邮箱：shbli@126.com。

本书的出版得到了清华大学出版社的鼎力支持和帮助，在此致以衷心的感谢！

限于笔者学识，不足之处恳请同行专家批评指正。

编　者

2014 年 6 月

目　录

第1章　信息安全概述

信息作为一种重要的战略资源，信息的获取、处理和安全保障能力成为一个国家综合国力的重要组成部分。信息安全事关国家安全、事关社会稳定。信息安全问题已威胁到国家的政治、经济、文化和意识形态等领域，成为社会稳定安全的必要前提条件。本章简要介绍信息安全问题产生需要掌握的一些基本概念，重点介绍网络空间的黑客攻击、信息安全的基本内涵、信息安全的发展历程、信息安全威胁、信息安全技术和信息安全管理。

1.1　网络空间的黑客攻击

随着计算机网络、移动互联网、物联网和云计算在商业领域的普及应用，社会对网络空间的信息共享资源依赖性越来越强。企业和个人利用移动通信网络感知、处理、传递和存储一些机密数据，使其免受未经授权人员的窃取、伪造、篡改和破坏等极端行为的威胁。

近年来，“黑客”攻击已成为危害计算机网络、移动智能终端、云计算服务和信息安全的多发性事件，下面列出一些经典的真实案例。

2009年12月，某国武装分子使用标价仅为25.95美元的黑客软件，成功侵入美国中央情报局(CIA)的“捕食者”无人机攻击系统。单价2000万美元的“捕食者”无人机上搭载有“地狱火”导弹，经常在伊拉克、阿富汗以及巴基斯坦境内对武装分子发动攻击。

2010年9月，Stuxnet蠕虫入侵伊朗Bushehr核电站电网和工业控制计算机系统，远程控制一些核心计算机信息系统，造成核电站大规模运行故障。

2014年1月，我国免费DNSPON解析服务器遭受不明来源的流量攻击，导致全国出现大范围DNS故障，包括baidu.com、qq.com、sina.com等使用顶级域名的网站解析出现异常，域名访问请求被跳转到几个没有响应的美国IP上，不同省份的用户均出现不同程度的网络故障。

以上只是少数案例，实际上还有更多案例未被报道。

信息安全的威胁，总体上可以分为两大类。

1. 自然因素

自然因素是指地震、水灾、火灾、飓风、雷电等人类不可抗拒力量导致信息本身或访问通道遭到破坏。例如，在数据传输的过程中，闪电、鼠灾、电气设备老化等会造成传输时的信号干扰、衰减与数据完整性改变等问题。

2. 人为因素

人为因素是指黑客企图攻破信息系统的安全访问控制，从中获取不当的利益。特别是由于云计算的移动性、共享性和服务性，网民在享受Internet带来的无穷乐趣的同时，黑客利用掌握的专业知识不断探测云计算系统的漏洞，非法盗取计算机资源，破坏计算机系统的

正常运行机制。信息安全的目的主要是保护所有信息系统内的资源，包括机密数据、计算机软件资源、计算机硬件资源及网络通信设备。计算机系统的长期运行，会造成物理硬件的疲劳和损坏，致使存储系统重要数据丢失和运算错误。因此，经常性保养硬件系统安全，是信息安全管理的重要课题。

1.2 信息安全的基本内涵

从信息安全的发展过程来看，在计算机出现以前，通信安全以保密为主，密码学是信息安全的基础和核心；随着计算机的出现，计算机系统安全保密成为现代信息安全的重要内容；网络普及和云计算的出现，使得分布式跨平台的信息系统的安全保密成为信息安全的主要内容。

信息安全之所以引起人们的普遍关注，是由于信息安全问题目前已经涉及人们日常生活学习工作的各个方面。以电子商务网络交易为例，2009 年 11 月 11 日（双十一，“光棍节”），淘宝网销售额为 0.5 亿元；2010 年，销售额提高到 9 亿元；2011 年，销售额已跃升到 33 亿元；2012 年，交易额实现飞速增长，达到 191 亿元；2013 年，总交易额突破 350 亿元。漂亮的数字背后，电子商务交易必须遵循客观事实：交易双方都是谁？信息在传输过程中是否被篡改（信息的完整性）？信息在传送途中是否会被外人看到（信息的保密性）？网上支付后，对方是否会不认账（不可抵赖性）？因此，商家、银行、个人对电子交易安全的担忧是必然的，电子商务的安全问题已经成为阻碍现代服务业发展的瓶颈。推动信息安全技术不断发展和普及，是信息服务产业的重要使命。

信息安全涉及的领域相当广泛，人们对信息财产的使用主要通过计算机网络来实现，信息的处理在计算机和网络上是以数据的形式进行的。从这个角度来说，信息就是数据，信息安全可以分为数据安全和系统安全。因此，信息安全可以从两个层次来看。

从消息的层次，包括信息的完整性（Integrity），即保证消息的来源、去向、内容真实无误；保密性（Confidientiality），即保证消息不会被非法泄露扩散；不可否认性（Non-repudiation），也称为不可抵赖性，即保证消息的发送者和接收者无法否认自己所做过的操作行为等。从网络层次，包括可用性（Availability），即保证网络和信息随时可用，运行过程中不出现故障，若遇意外打击尽可能减少损失并尽快恢复正常；可控性（Controllability），即对网络信息的传播及内容具有控制能力的特性。信息安全的基本属性主要表现在以下五个方面。

1. 完整性

完整性是指未经授权不能修改数据的内容，保证数据的一致性。在网络传输和存储过程中，系统必须保证数据不被篡改、破坏和丢失。因此，网络系统有必要采用某种安全机制确认数据在此过程中没有被修改。

2. 保密性

保密性是指由于网络系统无法确认是否有未经授权的用户截取数据或非法使用数据，这就要求使用某种手段对数据进行保密处理。数据保密可分为网络传输保密和数据存储保

密。对机密敏感的数据使用加密技术，将明文转化为密文，只有经过授权的合法用户才能利用密钥将密文还原成明文。反之，未经授权的用户无法获得所需信息。这就是数据的保密性。

3. 可用性

可用性是指信息可被授权者访问并按需求使用的特性，即保证合法用户对信息和资源的使用不会被不合理地拒绝。对可用性的攻击就是阻断信息的合理使用，例如，破坏系统的正常运行就属于这种类型的攻击。

4. 不可否认性

不可否认性是指建立有效的责任机制，防止网络系统中合法用户否认其行为，这一点在电子商务中是极其重要的。抗否认包含两个方面：数据来源的抗否认，为数据接收者 B 提供数据的来源证据，使发送者 A 不能否认其发送过这些数据或不能否认发送数据的内容；数据接收的抗否认，为数据的发送者 A 提供数据的交付证据，使接收者 B 不能否认其接收过这些数据或不能否认接收数据的内容。

5. 可控性

可控性是指对信息的传播及内容具有控制能力的特性。授权机构可以随时控制信息的机密性，能够对信息实施安全监控。

1.3　信息安全的发展历程

信息安全自古以来就受到人们的持续关注，但在不同的发展时期，信息安全的侧重点和控制方式是不同的。需要全面理解信息安全的发展历程，粗略地讲，可把信息安全分成三个基本阶段。

1. 通信安全

早期，所有的资产是物理的，重要的信息也是物理的，如古代把文字刻在骨头上即甲骨文，到后来把文字写在纸上。信息传递通常由信使完成，如果信使被敌人武力劫持，报文的信息就会被敌人知悉，因此就产生了通信安全的问题，可见物理安全是存在缺陷的。

第二次世界大战期间，德国人发明了一种称为 Enigma 的机器来加密报文（图 1-1 所示），用于军队，当时他们认为 Enigma 是不可破译的。确实是这样，如果使用恰当，要破译它非常困难。但经过一段时间发现，由于某些操作员的使用差错，Enigma 被破译了。

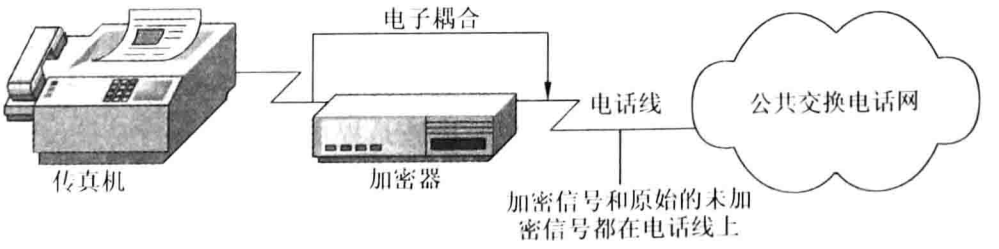

图 1-1　Enigma 加密报文

军事通信也使用编码技术，将每个字编码后放入报文传输。在战争期间，日本人曾用编码后的字通信，即使美国人截获了这些编码也难以识别该报文。在准备 Midway 之战时，日本人曾传送编码后的报文，使日美之间在编码和破译之间展开了一场有关通信安全的对抗。

2. 计算机安全

1938 年，德国人康拉德·楚泽发明了运行二进制数据的计算机；1985 年，美国微软公司开发出了 Windows 操作系统。从此，计算机系统以指数的速度发展，互联网普及率迅速提升，大部分信息资产以电子形式移植到计算机上，人们用交互会话的方式访问计算机系统。

20 世纪 70 年代，David Bell 和 Leonard La Padula 开发了一个安全计算机的操作模型，该模型基于政府概念的各种级别分类信息（一般、秘密、机密、绝密）和各种许可级别。如果主体的许可级别高于文件（客体）的分类级别，则主体能访问客体。如果主体的许可级别低于文件（客体）的分类级别，则主体不能访问客体。这个模型的概念进一步发展，1983 年，美国国防部发布了橘皮书标准 500.28——可信计算机系统评估准则（the Trusted Computing System Evaluation Criteria，TCSEC）。

TCSEC 共分为四类七级：①D 级，安全保护欠缺级；②C1 级，自主安全保护级；③C2 级，受控存取保护级；④B1 级，标记安全保护级；⑤B2 级，结构化保护级；⑥B3 级，安全域保护级；⑦A1 级，验证设计级。

橘皮书对每一级定义了功能要求和保证要求，也就是说要符合某一安全级要求，必须既满足功能要求，又满足保证要求。为了使计算机系统达到相应的安全要求，计算机厂商要花费很长时间和很多资金。有时当产品通过级别论证时，该产品已经过时了。计算机技术发展得如此之迅速，当老的系统取得安全认证之前新版的操作系统和硬件已经出现。

1999 年，我国发布了计算机信息系统安全保护等级划分准则（Classified Criteria for Security Protection of Computer Information System）的国家标准，序号为 GB 17859—1999，评估准则的制定为我们评估、开发、研究计算机系统的安全提供了指导准则。

3. 信息安全保障

通信安全解决的是远距离点到点长途通信的安全问题。随着 Internet 的发展及其普及应用，如何解决开放网络环境下局域网、城域网的安全问题便成为迫切需要解决的问题。

橘皮书不解决联网计算机的安全问题。为此，1987 年，美国国防部制定了 TCSEC 的可信网络解释 TNI，又称红皮书。除了满足橘皮书的要求外，红皮书还企图解决计算机的联网环境的安全问题。红皮书主要说明联网环境的安全功能要求，较少阐述保证要求。

通信安全的主要目的是解决数据传输的安全问题，主要的措施是密码技术。计算机安全的主要目的是解决计算机信息载体及其运行的安全问题，主要措施是根据主、客体的安全级别，正确实施主体对客体的访问控制。信息安全保障的主要目的是解决分布网络环境中对信息载体及其运行提供的安全保护问题，主要措施是提供完整的信息安全保障体系，包括防护、检测、响应、恢复。

随着信息技术的发展与应用，信息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。信息安全逐渐演变

成一个综合、交叉的学科领域，不再仅仅限于对传统意义上的网络和计算机技术进行研究，必须要综合利用数学、物理、通信、计算机以及经济学等诸多学科的长期知识积累和最新发展成果，进行自主创新研究，并提出系统的、完整的、协同的解决方案。例如，防电磁辐射、密码技术、数字签名、信息安全成本和收益等方面的研究都分别涉及并综合了计算机、物理学、数学以及经济学上的一些原理。信息安全保障体系，就是由信息系统、信息安全技术、人、管理、操作等元素有机结合，能够对信息系统进行综合防护，保障信息系统安全可靠运行、保障信息的“保密性、完整性、可用性、可控性、抗抵赖性”的具有“WPDRR”能力的综合性信息系统防护体系。1995 年，美国国防部提出了“保护—监测—响应”的动态模型，即 PDR 模型，后来增加了恢复，成为 PDR2(Protection，Detection，Reaction，Restore)模型，再后来又增加了政策(Policy)，即 P2DR2，如图 1-2 所示。

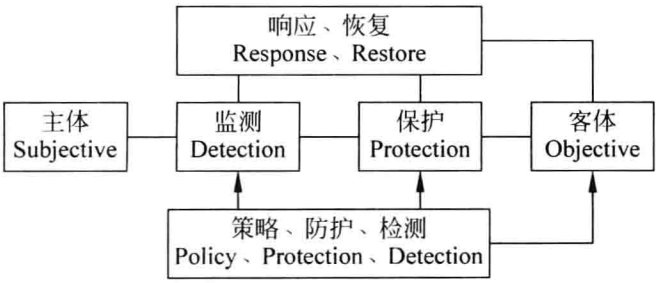

图 1-2　P2DR2 动态安全模型

1.4　信息安全威胁

熟悉了信息安全的发展历史，对进一步全面系统认识信息系统的安全分析打下了基础，首先了解信息安全的威胁以及产生威胁的根源。信息安全威胁是指某个人、物、事件或概念对信息资源的保密性、完整性、可用性或合法使用的危害。攻击是对安全威胁的具体体现，根本原因就是利用网络的脆弱性，入侵系统的有价值信息资产。

网络脆弱性(Network Vulnerability)主要体现在以下三个方面。

1. 开放的网络环境

互联网是一个无中心的、地位对等的自由网络，你和每个人都能互相连接，可怕之处在于每个人都能和你互相连接。

2. 协议本身的缺陷

网络传输离不开 TCP/IP 通信协议栈，每一层都有不同的漏洞，针对协议漏洞的攻击非常多。

3. 操作系统的漏洞

Windows、Linux、UNIX 等多种类型网络操作系统都不可避免地存在诸多安全隐患，如非法存取、远程控制、缓冲区溢出以及系统后门等称为操作系统漏洞。微软报告显示，2013 年 Windows XP、Windows 7 和 Windows 8 的漏洞为 350 多个，Windows 7 漏洞为 102 个，Windows XP 漏洞为 99 个，Windows 8 漏洞则高达 156 个，这一数字相较于 2012 年翻了一

番。2012 年 Windows 7 漏洞为 50 个，Windows XP 漏洞为 49 个。

利用开放的网络环境、协议缺陷和操作系统漏洞，许多人为因素和非人为因素可以对信息系统构成威胁，但是尽心设计的人为攻击威胁最大。针对信息系统，常见的威胁有以下几类。

(1) 物理安全威胁：是指对系统所用设备的威胁。物理设备安全是信息系统安全的首要问题。物理安全威胁主要有：自然灾害(地震、水灾、火灾等)造成整个系统毁灭；电源故障造成设备断电以致操作系统引导失败或数据库信息丢失；设备被盗、被毁造成数据丢失或信息泄露。计算机存储的数据价值远远超过计算机本身，必须采取严格的防范措施以确保不会被入侵者窃取。

(2) 通信链路安全威胁：网络入侵者可能在传输线路上安装窃听装置，窃听网上传输的信号，再通过一些技术手段读出数据信息，造成信息泄露；或对通信链路进行干扰，破坏数据的完整性。

(3) 操作系统安全威胁：操作系统安全是信息系统安全的基础。系统平台最危险的是在系统软件或硬件芯片中植入威胁，如“木马”或“陷阱门”。操作系统的安全漏洞通常是由开发者有意设置的，这样他们就能在用户失去了对系统的所有访问权后仍能进入系统。

(4) 应用系统安全威胁：是指对于网络服务或用户业务系统安全的威胁。应用系统对应用安全的需求有足够的保障能力。应用系统也受到“木马”和“陷阱门”的威胁。

(5) 管理系统安全威胁：不管是什么样的网络系统都离不开人员的管理，必须从人员管理上杜绝安全漏洞。再先进的安全技术也不能完全防范由于人员不慎造成的信息泄露，管理安全是信息安全有效的前提。

(6) 网络安全威胁：计算机网络的使用对数据造成了新的安全威胁，由于在网络上存在电子窃听，分布式计算机的特征是各个独立的计算机通过一些媒介相互通信。当内部网络和国际互联网相接时，由于互联网的开放性、国际性和无安全关联性，对内部网络形成严重的安全威胁。

目前还没有统一的方法来对各种威胁进行分类，也没有统一的方法来对各种威胁加以区别。信息安全所面临的威胁与环境密切相关，不同威胁的存在及重要性是随环境的变化而变化的。

1.5 信息安全技术

信息安全学科是研究信息获取、信息存储、信息传输和信息处理领域中信息安全保障问题的一门新兴学科。信息安全学科是计算机、电子、通信、数学、物理、生物、管理、法律和教育等学科交叉融合而形成的一门新型学科。它与这些学科既有紧密的联系，又有本质的不同。信息安全学科已经形成了自己的内涵、理论、技术和应用，并服务于信息社会，从而构成一个独立的学科。信息安全学科包含五大研究方向，分别为密码学、网络安全、信息系统安全、信息内容安全和信息对抗。

密码学由密码编码学和密码分析学组成，其中密码编码学主要研究对信息进行编码以实现信息隐蔽，而密码分析学主要研究通过密文获取对应的明文信息；密码学研究密码理

论、密码算法、密码协议、密码技术和密码应用等。

网络安全的基本思想是在网络的各个层次和范围内采取防护措施，以便能对各种网络安全威胁进行检测和发现，并采取相应的响应措施，确保网络环境的信息安全；网络安全研究网络安全威胁、网络安全理论、网络安全技术和网络安全应用等。

信息系统是信息的载体，是直接面对用户的服务系统。信息系统安全的特点是从系统级的整体上考虑安全威胁与防护；它研究信息系统的安全威胁、信息系统安全的理论、信息系统安全技术和应用。

信息内容安全是信息安全在政治、法律、道德层次上的要求；我们要求信息内容是安全的，就是要求信息内容在政治上是健康的，在法律上是符合国家法律法规的，在道德上是符合中华民族优良的道德规范的。

信息对抗是为削弱、破坏对方电子信息设备和信息的使用效能，保障己方电子信息设备和信息正常发挥效能而采取的综合技术措施，其实质是斗争双方利用电磁波和信息的作用来争夺电磁频谱和信息的有效使用和控制权；信息对抗研究信息对抗的理论、信息对抗技术和应用。

信息安全技术涉及信息传输的安全、信息存储的安全以及对网络传输信息内容的审计三个方面。为了保障数据传输的安全，需要采用数据传输加密技术、数据完整性鉴别技术；为保证信息存储的安全，需要进行数据备份以及灾难恢复和保证终端安全；信息内容审计则是实时地对进出内部网络的信息进行内部审计，以保证防止或追查可能的泄密行为。

1.5.1　信息保密技术

信息保密技术包括信息加密技术和信息隐藏技术。

信息加密是指使有用的信息变为看上去似为无用的乱码，使攻击者无法读懂信息的内容从而保护信息。信息加密是保障信息安全的最基本、最核心的技术理论措施和理论基础，它也是现代密码学的主要组成部分。信息加密过程由形形色色的加密算法来具体实施，它以很小的代价提供很大的安全保护。到目前为止，据不完全统计，已经公开发表的各种加密算法多达数百种。如果按照首发双方密钥是否相同来分类，可以将这些加密算法分为单钥密码算法和公钥密码算法。

当然，在实际应用中，单钥密码和公钥密码结合在一起使用，比如利用 AES 来加密信息，采用 RSA 来传递会话密钥。如果按照每次加密所处理的比特数来分类，可以将加密算法分为序列密码和分组密码。序列密码每次只加密一个比特，而分组密码则先将信息序列分组，每次处理一个组。

加密是网络安全的核心技术。加密技术不仅应用于数据的存储和传输的过程中，而且应用于程序的执行中。

网络中的数据加密，与选择的加密算法密切相关。加密算法可分为对称密钥算法和非对称密钥算法，对称密钥属于私钥体制，即加密密钥和解密密钥相同，典型算法有 DES、AES；非对称密钥属于公钥体制，有两把密钥（公钥加密和私钥解密），典型算法有 RSA，它解决了网络环境中密钥的分发问题，简化了密钥管理。

数据加密主要与选择的加密方式有关，链路层点对点加密、网络层主机对主机加密、传输层进程对进程加密和应用层内容加密。加密算法除了提供信息的保密性之外，与其他技