KH 北京科海 25年·IT技术出版专家

国家“十一五”高等院校计算机应用型规划教材

名家系列

# 信息安全技术及应用实验（第2版）

北京科海 总策划

蔡红柳　刘海燕　主　编

- 以信息安全理论与技术为基础，全面介绍信息安全的基本原理、技术及应用
- 由著名军事学院长期从事信息安全教学理论与实践研究的信息安全专家策划和编写
- “理论与实践”相结合，提供多个有针对性的实验，全面提升综合应用能力
- 内容全面，通俗易懂，紧追时代前沿

科学出版社

国家“十一五”高等院校计算机应用型规划教材

# 信息安全技术及应用实验

（第2版）

蔡红柳　刘海燕　主　编

李　彤　霍景河　编　委

张占军　杨建康

科学出版社

## 内 容 提 要

本书以信息安全理论与技术为基础，全面介绍信息安全的基本原理、技术及应用。主要内容包括信息加密技术、认证技术、密钥管理与公钥基础设施、访问控制与网络隔离技术、Internet的数据安全技术、信息系统安全检测技术、恶意程序及防范技术、网络攻击与防范技术等。

本书注重理论与实践相结合，在介绍概念、原理与技术的同时，给出代表性运行方案和应用实例。每章都配有实验和习题，所有实验均给出了具体的操作过程，目的是让读者在理解、掌握基本原理和技术的基础上，巩固所学知识并快速掌握其实际应用。

本书可作为信息管理与信息系统、计算机科学、通信工程、信息工程等专业信息安全课程的教材，也可作为计算机培训学校的教材以及信息安全技术人员和自学者的参考书。

**图书在版编目（CIP）数据**

信息安全技术及应用实验/蔡红柳，刘海燕主编. —2 版. —北京：科学出版社，2009

ISBN 978-7-03-024960-9

I. 信… II. ①蔡…②刘… III. 信息系统—安全技术—教材 IV. TP309

中国版本图书馆 CIP 数据核字（2009）第 113621 号

责任编辑：周晓娟 / 责任校对：刘雪连

责任印制：科 海 / 封面设计：林 陶

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京市艺辉印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2009 年 9 月 第 一 版 开本：16 开

2009 年 9 月第一次印刷 印张：23.25

印数：0 001~3 000 字数：565 000

**定价：38.00 元**

**（如有印装质量问题，我社负责调换）**

# 丛书序

计算机教材建设是计算机专业教学工作的重要组成部分，高质量的教材是培养高素质人才的基本保证，是体现教育特色的知识载体和教学的基本工具，直接关系到计算机专业教育能否为一线岗位培养符合要求的高级应用型人才。教育部也把教材建设作为衡量高等院校深化教育教学改革的重要指标，作为检验各院校人才培养工作的标准。近年来，许多院校都十分重视计算机专业教材建设工作，编写和出版了一批质量较高的精品教材，但仍然远远满足不了应用型教育发展的需要，所以我们组织了由全国高校计算机专业的专家教授组成的国家“十一五”高等院校计算机应用型规划教材课题研究组，通过对应用型本科院校和高职高专院校计算机应用技术专业全面、细致的调研和讨论，并结合我国当前的教学现状，编写了本丛书。丛书突出系统性、科学性和实践性，以培养社会需求的计算机应用型专门人才为宗旨。

## 丛书特色

### ☑ 课程体系的系统性：注重教学内容和体系的创新

本丛书根据教育部颁布的应用型专门人才培养目标来编写，适合应用型本科院校和高职高专院校的教学需求和教学特色。基础理论型课程体现以应用为目的，以必需、够用为度，以讲清概念、强化应用为教学重点；专业技术型课程强调实用性，以满足社会需求为目标，以强化实践操作为教学重点。

### ☑ 教学方法的先进性：加强全方位的教学配套资源建设

本丛书针对计算机专业教学工作量大、课时多、讲授课程种类全的特点，注重资源和手段的改革，并逐步建立专门的论坛网站，为计算机专业教学提供一个现代化的平台，包括教材推荐和评论、学生提问和教师答疑、教师课程教学博客、教学论文发表、教学实验基地信息发布等功能。

### ☑ 教学内容的多样性：力求介绍最新的技术和方法

先进性和时代性是教材的生命，计算机应用技术专业的教学具有更新快、内容多的特点，本丛书在体例安排和实际讲述过程中都力求介绍最新的技术和方法，并注重拓宽学生的知识面，激发他们的学习热情和创新欲望。

### ☑ 理论与实践并重：阐明基础理论，强调实践应用

理论是实践的基础，实践是理论的升华；不能有效指导实践的理论是空头理论，没有理论指导的实践是盲目的实践。对于时代呼唤的信息化人才而言，二者缺一不可。本丛书以知识点为主线，穿插演示性案例于理论讲解之中，使枯燥的理论变得更易于理解、易于接受；此外，还在每一章的最后提供大量的练习题和综合示例，以提高学生综合利用所学知识解决实际问题的能力。

### ☑ 易教易学：创新体例，合理布局，通俗易懂

本丛书结构清晰，内容系统翔实，布局合理，语言精炼实用（不讲深奥的原理），实例难度适中；力求把握各门课程的核心，通俗易懂，便于教学的展开，也便于学生融会贯通，熟练掌握所学知识。

### ☑ 版式设计：简洁大方

精心设计的版式简洁、大方和实用。对于标题、正文、注释、技巧等都设计了醒目的字体，读者阅读起来会感到轻松愉快。

## 涵盖领域

本丛书涵盖了计算机各个应用领域，包括：

- 计算机操作基础
- 计算机硬件基础
- 程序设计技术
- 数据库应用技术
- 信息安全
- 计算机网页设计与制作
- 计算机网络技术
- 图形图像
- 软件工程

## 丛书编委会



## 教学服务与支持

本丛书的出版者和作者竭诚为读者提供服务。网络支持与服务网址为 http://www.khp.com.cn。包括：

- 提供实用的相关资源与最新信息，读者可以方便地下载本丛书的实例源代码及相关教学素材。
- 作者和专家邮件答疑（E-mail：khservice@khp.com.cn），将努力高效快捷地解决读者在图书使用和学习中遇到的疑难问题。
- 免费为教师提供的 PowerPoint 演示文档，该文档可将书中的内容及图片以幻灯片的形式呈现在学生面前，在很大程度上减轻了教师的备课负担，所以深受广大教师的欢迎。请用书教师致电：010-82896438 或发 E-mail：feedback@khp.com.cn 获取电子教案。

## 编者寄语

教学改革是教育工作不变的主题。要紧跟教学改革，不断创新，编写出真正满足新形势下教学需求的教材，还需要我们不断地努力实践、探索和完善。本丛书的作者和出版者虽然竭尽全力进行细致的编写与校订，仍难免有疏漏和不足，我们真诚希望使用本丛书的教师和学生提出宝贵的意见和建议，以便能不断改进和日臻完善。

本丛书出版者的电子邮件：feedback@khp.com.cn

丛书编委会

2009 年 1 月

# 前　言

信息与信息系统安全已成为信息化建设关注的焦点和重要的研究课题。本书针对高等院校相关专业本科生所开设的信息安全课程，结合教育目标、学时和教学特点设计章节内容，介绍信息与信息系统安全所涉及的理论与技术。通过信息安全课程的学习，使学生理解信息及信息系统所面临的各种威胁及信息安全的重要性；掌握信息安全的概念、理论和技术；具备运用信息安全技术构建信息安全系统和处理信息安全相关问题的能力。

本书主要涉及两个方面：在信息安全技术方面，主要介绍信息加密技术、认证技术、密钥管理与公钥基础设施、Internet 的数据安全技术；在系统安全技术方面，主要介绍访问控制与网络隔离技术、信息系统安全检测技术、恶意程序及防范技术、网络攻击与防范技术。

## 本书内容

本书为第 2 版。作者在第 1 版的基础上进行了更新，把近几年积累的教学新成果和一些有效的案例引入到第 2 版中，并根据最新教学标准，对旧版内容进行了修订。

全书共 9 章，主要涉及对称密钥密码算法、非对称密钥密码算法、信息加密传输、消息认证、认证协议、数字签名、身份认证、密钥管理、公钥基础设施、Windows 2000 的 PKI、访问控制技术、防火墙技术、物理隔离技术、IPSec 与网络层安全、SSL 与传输层安全、Kerberos 认证系统、PGP 与电子邮件安全、入侵检测技术、漏洞检测技术、审计追踪、恶意程序、病毒、蠕虫、木马、常见的网络攻击技术、网络攻击技术的演变等内容。

另外，本书坚持理论与实践并重，提供了多个有针对性的实验。例如，加/解密算法实现、安装和配置证书服务、简易防火墙配置、SQL Server 2000 的安全管理、入侵检测系统 Snort 配置、创建 Kerberos 服务、利用 SSL 加密 HTTP 通道、PGP 的应用、配置 VPN 连接等。

## 本书特点

- “基础与前沿”相结合。书中在阐述信息安全理论及基本概念时注重科学、严谨，同时结合信息安全技术发展，做到内容全面，通俗易懂，紧追时代前沿。
- “理论与实践”相结合。立足于“看得懂、学得会、用得上”，原理、技术、应用并重，每章都配有应用实验，结合实验使学生能够更好地理解原理和技术，掌握信息安全技术在实际生活中的应用。
- “教学与自修”相结合。结合信息安全课程学时数和培养目标，设计了一套完整的教学实施方案。全书共配有 200 余道习题，对于每章节，习题的选择以必需、够

用为原则，有利于学生学以致用，巩固所学知识，便于自修人员进行自我考核。

## 本书编者

本书由著名军事学院长期从事信息安全教学理论与实践研究的信息安全专家编写，他们有着多年的授课经验，为学院信息安全学科带头人。

## 增值服务

为方便教学，本书还配有电子教案以及相关程序的源代码。用书教师请致电（010）82896438或发送电子邮件至feedback@khp.com.cn免费获取教学资源包。

## 编者寄语

在编写本书的过程中，参考了国内外有关信息安全方面的著作（包括网站内容），从中得到了很大帮助，在此表示衷心的感谢。

信息安全是一门内容广泛、发展迅速的学科，本书是在此领域教学工作的一次努力尝试，由于作者的学识水平有限，尽管做了最大努力，但是难免存在疏漏和不足，敬请读者批评指正。

编　者

2009年5月

# 目　录

# 第 1 章

# 概 述

CHAPTER 01

## 本章学习目标

本章介绍信息安全的基本概念，分析信息系统所面临的威胁、脆弱性及原因。具体包括信息安全研究的内容和发展过程、安全体系、安全策略与安全原则、安全体系与评估标准等。

通过本章的学习，应该掌握以下内容：

- 明确信息安全的概念、内涵、属性。
- 了解信息系统所面临的威胁及构成威胁的原因。
- 理解保证信息系统安全的重要性和必要性；了解信息安全发展的过程。
- 了解信息安全技术的研究内容。
- 理解信息安全防御策略、安全原则。
- 理解信息安全体系、安全服务、安全机制和评估标准。

所谓信息，一般描述为“客观世界中各种事物的变化和特征的最新反映，是客观事物之间联系的表征，也是客观事物状态经过传递后的再现”。在信息社会里，人类的一切活动都离不开对信息的获取与处理，信息作为一种无形资产已经成为人们最宝贵的财富。

## 1.1 信息安全概述

信息安全是一个涉及计算机技术、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合学科。

### 1.1.1 信息安全的概念

#### 1. 信息安全的内涵

信息安全是指信息在产生、传输、处理和存储过程中不被泄漏或破坏，确保信息的可用性、保密性、完整性和不可否认性，并保证信息系统的可靠性和可控性。信息安全包含以下 3 层含义。

（1）系统安全，即实体安全和运行安全。

① 实体安全。保护计算机设备、设施（含网络）以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施、过程。特别是避免由于电磁泄漏产生信息泄漏，从而干扰他人或受他人干扰。实体安全包括环境安全、设备安全和介质安全3方面。

② 运行安全。为保障系统功能的安全实现，提供一套安全措施（如风险分析、审计跟踪、备份与恢复、应急等）来保护信息处理过程的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失。

风险分析是指为了使计算机信息系统能安全地运行，首先了解影响计算机信息系统安全运行的诸多因素和存在的风险，从而进行风险分析，找出克服这些风险的方法。

审计跟踪是利用计算机信息系统所提供的审计跟踪工具，对计算机信息系统的工作过程进行详尽的跟踪记录，同时保存好审计记录和审计日志，保证计算机信息系统安全可靠地运行。这就要求系统管理员要认真负责，切实保存、维护和管理审计日志。

应急措施和备份恢复应同时考虑。首先要根据所用信息系统的功能特性和灾难特点制定包括应急反应、备份操作、恢复措施3方面内容的应急计划，一旦发生灾害事件，就可按计划方案最大限度地恢复计算机系统的正常运行。

（2）系统中的信息安全。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，即通过对用户权限的控制、利用数据加密等技术确保信息不被非授权者获取和篡改。防止信息被故意地或偶然地非授权泄漏、更改、破坏或使信息被非法的系统辨识以及控制，即确保信息的完整性、保密性、可用性和可控性。信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与认证等方面。

（3）管理安全，即用综合手段对信息资源和系统安全运行进行有效管理。

总之，信息安全的目的是在安全法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理措施，维护计算机信息安全。信息安全应当保障计算机及其相关的设备、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的安全运行。

### 2. 信息安全的基本属性

不论攻击者怀有什么样的目的、采用什么手段，都要通过攻击信息的以下几种安全属性来达到目的。所谓“信息安全”，在技术层次上的含义是保证在客观上杜绝对信息安全属性的威胁，使信息的主人在主观上对其信息的本源性放心。信息安全的基本属性有以下几项。

（1）保密性（Confidentiality）

保密性是指严密控制各个可能泄密的环节，使信息在产生、传输、处理和存储的各个环节中不泄漏给非授权的个人和实体，或供其使用的特性。军事信息的安全尤其注重信息的保密性。

（2）完整性（Integrity）

完整性是指信息在存储或传输过程中保持不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性，保证真实的信息从真实的信源无失真地到达真实的信宿，并且能

够判断信息或进程是否已被篡改。对于军事信息来说，完整性被破坏可能意味着接收到不正确的命令，导致延误战机、误伤或闲置战斗力。破坏信息的完整性是对信息安全发动攻击的重要目的之一。

（3）可用性（Availability）

可用性是指保证信息和相关资源可以持续有效，即保证合法用户可以访问和使用信息的特性，当在需要时可以使用所需信息。防止由于主客观因素造成信息系统拒绝服务，防止因系统故障或误操作等使信息丢失或妨碍对信息的使用。网络可用性还包括在某些不正常条件下继续运行的能力。

（4）可认证性（Authentication）

可认证性是指可识别、可验证的特性，识别是“辨认是谁”，而验证却要“证明是谁”。在信息系统中，它们可能合二为一，成为一个步骤，即通过授权方法赋予用户一定权限，而通过用户所有、所知和个人特征来识别、证明用户是否为合法的授权用户。

（5）抗否认性（Non-reputation）

抗否认性是指保证信息方不能否认自己行为的特性，是面向通信双方（人、实体或进程）信息真实同一的安全要求，包括收、发双方均不可否认。

（6）可控性（Controllability）

可控性是指信息和信息系统时刻处于合法所有者或使用者的有效掌握与控制之下。例如，对越权利用网络资源的行为进行控制；对企图入侵内部网的非法用户进行有效的监控和抵制；必要时可依法对网络中流通与存储的信息进行监视。

（7）可靠性（Reliability）

可靠性是指信息系统能在一定质量水平上持续运行的状态，使信息用户得到认可的质量连续服务于用户的特性。它要求运用容错和多机备份技术，还要精心考虑信息系统场所的设计（防火、防水、防盗、防静电、防电磁干扰等）。

### 1.1.2 信息系统面临的威胁及原因

信息系统是复杂系统中与信息有关的小系统。将信息系统涉及的功能与范围加以界定，可大体将信息系统分为广义的信息系统和狭义的信息系统。前者包括各种处理信息的系统，包括社会组织、人和各种人造系统；后者仅指基于计算机的系统，是人、规程、数据库、软件、硬件等各种设备、工具的有机结合，它突出的是计算机、网络通信、信息处理等技术的应用。

#### 1. 信息系统面临的威胁

由于信息系统是信息采集、存储、加工、分析和传输的工具，目前，被用于军事、政务、金融、贸易和企业等各个领域，它在给人们带来极大方便的同时，也面临着巨大的威胁，各种对信息系统的攻击和网络犯罪活动已经存在，直接影响了信息系统的使用。归纳信息系统所面临的威胁，可分为以下几类。

（1）信息通信过程中的威胁

信息系统的用户在进行通信的过程中，常常受到两方面的攻击。一是主动攻击，攻击

者通过网络线路将虚假信息或计算机病毒传入信息系统内部，破坏信息的真实性、完整性及系统服务的可用性，即通过中断、伪造、篡改和重放信息内容造成信息破坏，使系统无法正常运行，严重的甚至使系统处于瘫痪；二是被动攻击，攻击者非法截获、窃取通信线路中的信息，使信息保密性遭到破坏，信息泄漏而无法察觉，给用户带来巨大的损失。下面介绍如图1-1所示的几种攻击。

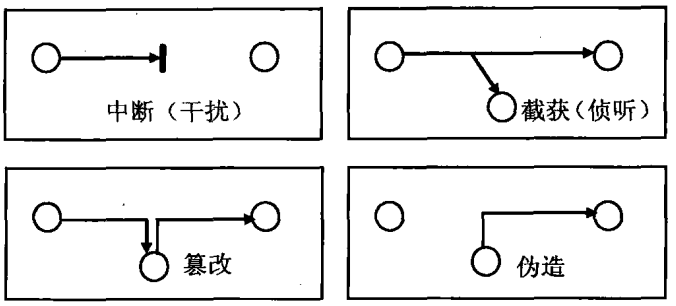


图1-1 4种攻击类型

① 中断（interruption）。中断是指威胁源使系统的资源受损或不能使用，从而暂停数据的流动或服务，属于主动攻击。

② 截获（interception）。截获是指某个威胁源未经允许而获得了对一个资源的访问，并从中盗窃了有用的信息或服务，属于被动攻击。

③ 篡改（modification）。篡改是指某个威胁源未经许可却成功地访问并改动了某项资源，因而篡改了所提供的信息服务，属于主动攻击。

④ 伪造（fabrication）。伪造是指某个威胁源未经许可而在系统中制造出了假消息源、虚假的信息或服务，属于主动攻击。

（2）信息存储过程中的威胁

存储于计算机系统中的信息，易受到与通信线路同样的威胁。非法用户在获取系统访问控制权后，可以浏览存储介质上的保密数据或专利软件，并且对有价值的信息进行统计分析，推断出所有的数据，这样就使信息的保密性、真实性、完整性遭到破坏。

（3）信息加工处理中的威胁

信息系统一般都具有对信息进行加工分析的处理功能，而信息在进行处理过程中，通常都是以源码出现，加密保护对处理中的信息不起作用。因此，有意攻击和意外操作都极易使系统遭受破坏，造成损失。除此之外，信息系统还会因为计算机硬件的缺陷、软件的脆弱、电磁辐射和客观环境等原因造成损害，威胁计算机信息系统的安全。

**2. 威胁表现和构成因素**

（1）表现形式

信息系统中的信息和网络中的设备所面临的威胁具体表现形式有以下几种。

① 伪装。某个具有合法身份的威胁源成功地假扮成另一个实体（用户或程序），随后滥用后者的权利。这时的威胁源可以是用户，也可以是程序，受威胁对象与此类同。

② 非法连接。威胁源以非法手段形成合法身份，使网络实体（用户或连接）与网络

资源之间建立了非法连接。威胁源可以是用户，也可以是程序，受威胁对象则是各种网络资源。

③ 非授权访问。非授权实体非法访问信息系统资源，或授权实体超越权限访问信息系统资源。例如，有意避开系统访问控制机制，对信息设备及资源进行非法操作或运行；擅自扩大权限，越权访问信息系统资源。非法访问主要有假冒和盗用合法用户身份攻击、非法进入网络系统进行违法操作、合法用户以未授权的方式进行操作等形式。

④ 拒绝服务。攻击者通过对系统进行非法的、根本无法成功的访问尝试而产生过量的系统负载，从而导致系统的资源对合法用户的服务能力下降或丧失；或是由于信息系统或其组件在物理上或逻辑上受到破坏而中断服务。威胁源可以是用户，也可以是程序；受威胁对象与此类同。

⑤ 否认。网络用户虚假地否认提交过信息或接收到信息。威胁源可以是用户，也可以是程序，受威胁对象是用户。

⑥ 信息泄漏。信息泄漏指敏感数据在有意或无意中被泄漏、丢失或透露给某个未授权的实体。通常情况下是信息在传输中被丢失或泄漏，如利用电磁泄漏或搭线窃听等方式可截获保密信息。威胁源可以是用户，也可以是程序，受威胁对象是信息系统中传输的信息或数据库中的信息。

⑦ 通信流量分析。攻击者观察通信协议中的控制信息，或对传送中的信息的长度、频率、源和目的进行分析。威胁源可以是用户，也可以是程序；受威胁对象是通信系统中的信息。

⑧ 改动信息流。对正确的通信信息序列进行非法的修改、删除、重排序或重放。威胁源可以是用户，也可以是程序；受威胁对象是通信系统中的信息。

⑨ 篡改或破坏数据。以非法手段窃得对信息的管理权，通过未授权的创建、修改、删除或重放等操作而使数据的完整性受到破坏。

⑩ 推断或演绎信息。统计数据含有原始信息的踪迹，非法用户利用公布的统计数据，推导出某个信息的原始值。威胁源可以是用户，也可以是程序；受威胁对象是数据库中的数据或通信系统中的信息流。

⑪ 非法篡改程序。这种威胁具有3种形式：病毒、特洛伊木马和蠕虫。它们会破坏操作系统、通信软件或应用程序。威胁源可以是程序，也可以是用户；受威胁对象是存于库中的程序。

（2）构成因素

影响信息系统的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；还可能是外来黑客对网络系统资源的非法使用。针对信息系统的威胁归结起来，主要有以下3个因素。

① 环境和灾害因素。信息系统易受环境和灾害的影响。温度、湿度、供电、火灾、水灾、地震、静电、灰尘、雷电、强电磁场、电磁脉冲等，均会破坏数据和影响信息系统的正常工作。灾害轻则造成业务工作混乱，重则造成系统中断，甚至造成无法估量的损失。

② 人为因素。可分为有意和无意。有意的是指人为的恶意攻击、违纪、违法和犯罪，这是信息系统所面临的最大威胁。无意的是指人为的无意失误，如操作员安全配置不当造

成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与他人共享等都会对网络安全带来威胁。

人为的无意失误和各种各样的误操作都可能造成严重的不良后果，典型的错误有文件的误删除、输入错误的数据等。

③ 系统自身脆弱性。计算机网络安全保障体系应尽量避免天灾造成的计算机危害，控制、预防、减少人祸以及系统本身原因造成的计算机危害。尽管近年来计算机网络安全技术取得了巨大的进展，但计算机网络系统的安全性比以往任何时候都更加脆弱。主要表现在它极易受到攻击和侵害，它的抗打击力和防护力很弱。其脆弱性主要表现在如下几方面。

- 系统硬件。由于生产工艺或制造商的原因，计算机硬件系统本身有故障而引起系统的不稳定、电压波动干扰等。信息系统在工作时，向外辐射电磁波，易造成敏感信息的泄漏。由于这些问题是固有的，除在管理上强化人工弥补措施外，采用软件程序的方法见效不大。因此在设计硬件或选购硬件时，应尽可能减少或消除这类安全隐患。
- 软件组件。主要安全隐患来源于设计和软件工程中的问题。软件设计中的疏忽可能留下安全漏洞；软件设计中不必要的功能冗余及代码过长，将不可避免地导致软件存在安全脆弱性；软件设计不按信息系统安全等级要求进行模块化设计，导致软件的安全等级不能达到所声称的安全级别；软件工程实现中造成的软件系统内部逻辑混乱，导致垃圾软件，这种软件从安全角度来看，绝对不可用。
- 网络和通信协议。安全问题最多的是基于 TCP/IP 协议栈的 Internet 及其通信协议。TCP/IP 协议最初设计的应用环境是美国国防系统的内部网络，这一网络环境是互相信任的，而且支持 Internet 运行的 TCP/IP 协议栈原本只考虑互联互通和资源共享的问题，并未考虑也无法兼容解决来自网际中的大量安全问题。当其推广到全社会的应用环境之后，信任问题发生了。因此 Internet 充满安全隐患就不难理解了。

总之，系统自身的脆弱和不足是造成信息系统安全问题的内部根源，但系统本身的脆弱性、社会对系统应用的依赖性这一对矛盾又将促进计算机网络安全技术的不断发展和进步。信息系统安全保护工作的重点是维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。

### 1.1.3 信息安全的研究内容

由于信息系统存在着诸多因素的脆弱性和潜在威胁，所以需从确保信息系统的保密性、完整性和可用性等问题入手。一切影响信息系统安全的因素和信息系统安全的措施都是信息安全研究的内容。

#### 1. 实体硬件安全技术

实体硬件安全是指系统设备及相关设施运行正常，系统服务适时，即应保证计算机设备、通信线路及设施、建筑物等的安全；预防地震、水灾、火灾、飓风、雷击；满足设备