高职高专现代信息技术系列教材

计算机信息安全

李成大　张京　龚茗茗　编

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

计算机信息安全/李成大，张京，龚茗茗编. —北京：人民邮电出版社，2004.5
（高职高专现代信息技术系列教材）
ISBN 7-115-12064-1

I. **计**… II. **①李**… **②张**… **③龚**… III. **电子计算机—安全技术—高等学校：技术学校—教材** IV. TP309

中国版本图书馆 CIP **数据核字（**2004**）第** 024606 **号**

内 容 提 要

本书在回顾信息安全发展的基础上，总结了信息安全的特征，全面介绍信息安全的概念、原理和知识体系，主要包括实体安全与防护、计算机软件安全技术、备份技术、密码技术、认证与数字签名、网络安全技术、防火墙及入侵检测技术、操作系统与网站安全、E-mail **安全与网络加密、数据库系统安全、计算机病毒及防治以及实训等方面的内容。**

本书讲述力求深入浅出，通俗易懂，注重科学性与实用性，并配有精选实例、习题和实训，便于教学和自学。

本书可作为高职高专计算机类、信息技术类等专业的教材，也可供从事信息处理、通信保密、军事指挥等专业工程技术人员和管理人员阅读，同时也可作为网络管理员和个人因特网用户的参考书。

高职高专现代信息技术系列教材

计算机信息安全

◆ **编** **李成大 张京 龚茗茗**
责任编辑

◆ **人民邮电出版社出版发行** **北京市崇文区夕照寺街** 14 **号**
邮编 100061 **电子函件** 315@ptpress.com.cn
网址 http://www. ptpress.com.cn
读者热线：010-67194092
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ **开本：**787×1092 1/16
印张：17.25
字数：413 **千字** 2004 **年** 3 **月第** 1 **版**
印数：1 – 000 **册** 2004 **年** 3 **月北京第** 1 **次印刷**

ISBN 7-115-12064-9/ TP · 3821

定价： .00 **元**

编者的话

信息已成为社会发展的重要战略资源、决策资源，信息化水平已成为衡量一个国家现代化程度和综合国力的重要指标。抢占信息资源已经成为国际竞争的重要内容。

在信息化社会中，计算机和通信网络已经广泛应用于各个领域。以此为基础建立的各种信息系统，给人们的生活、工作带来了巨大变化。然而，人们在享受网络信息所带来的利益的同时，也面临着信息安全的严峻考验，信息安全的重要性有目共睹。以 Internet 为代表的全球性信息化浪潮日益高涨，信息网络技术的应用正日益普及和广泛，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展。伴随网络的普及，安全日益成为影响信息系统性能的重要问题，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求。

本书着重从实用角度讲解计算机信息安全的基本概念、基本原理和技术方法，同时也注意了该书的系统型和先进性。

全书共 14 章。第 1 章介绍计算机信息安全的定义、特征、含义和分类，着重讲述了计算机信息系统面临的威胁及安全对策。第 2 章讲述实体安全与防护技术，包括影响实体安全的主要因素，实体安全的内容，计算机机房场地环境的安全防护，实体访问控制的基本任务，记录媒体的保护与管理，计算机电磁泄漏及防护。第 3 章主要介绍软件防拷贝技术，防静态和动态分析技术，软件保护及工具。第 4 章讲述有关备份的基础知识，包括备份的内容、层次、方式以及意义等，介绍一些常用的软硬件备份及网络备份方法。第 5 章讨论加密系统的基本组成及常用加密算法，包括 DES 加密算法、IDEA 加密算法以及 RSA 公开密钥密码算法。第 6 章阐述信息认证技术，报文摘要，数字签名，数字证书，最后还介绍了公钥基础设施 PKI。第 7 章详细讲述网络存在的威胁、网络安全技术分类、黑客的历史与现状，网络攻击的分类及一般步骤，扫描、监听与嗅探，口令破解、后门和特洛伊木马，最后介绍几种常见的入侵攻击方法。第 8 章描述防火墙基本理论和实践背景，逐节阐述防火墙的含义、功能和局限性，介绍防火墙的分类、常见体系结构、主要技术形式及实现方式，设置防火墙的要素，防火墙安全技术分析，防火墙的设计准则，防火墙功能指标，防火墙的选择，在本章的最后展示了当今主要流行的几种防火墙产品。第 9 章讲述入侵检测系统的发展历史、作用、功能、分类，入侵检测原理及系统通用模型，讨论入侵检测系统的局限及面临的挑战，介绍入侵检测系统的发展趋势及产品。第 10 章主要介绍 Windows 2000 操作系统安全特性、功能、工具及防范对策，Linux 系统安全及网络安全，IIS Web 服务器安全和 Apache Web 服务器安全。第 11 章讲述 E-mail 工作原理、安全漏洞及保护 E-mail 的方法，并介绍了邮件加密软件 PGP，最后讨论了网络加密与密钥管理。第 12 章阐述数据库系统安全的含义、特性，基本安全架构，数据库加密，数据库的故障类型，数据库的备份与恢复。第 13 章介绍计算机病毒的定义、分类、特点、破坏行为、入侵途径、作用机制，重点讲述网络计算机病毒的特点、检测、防止及感染病毒后的修复，并对反病毒软件的原理及常用产品进行了介绍。第 14 章主要是有关信息安全的实训问题。其中囊括了与本书内容相关的实训，针对软件安全、备份软件、

密码技术、安全漏洞扫描、监听与嗅探，防火墙、网络入侵检测系统、Windows 2000 的权限配置与安全审核、IIS Web 服务器安全、E-mail 安全等知识和安全性安排了十几个实训。

本书内容新颖翔实、覆盖面广、实例丰富，语言文字通俗易懂；各章重点、难点突出，原理、技术和方法的阐述融于丰富的实例之中；各章均配有习题和实训，便于教学和自学。本书可作为高职高专“信息安全”课程的教材或教学参考书，也可供从事信息安全的工程技术人员和管理人员阅读参考。

本书的第 1、3、6、7、8、9、14 章由李成大副教授编写，第 2 章和第 10、11、12 章由张京副教授编写，第 4、5、13 章由龚茗茗老师编写，李成大老师负责统稿全书。

由于编者水平有限，时间仓促，书中错误之处在所难免，恳请读者批评指正。

编　者

2004 年 3 月

目　录

第 1 章　绪论

目前，计算机和通信网络已经广泛应用于社会的各个领域，以此为基础建立的各种信息系统，给人们的生活、工作带来了巨变。

然而，人们在享受网络信息所带来的巨大利益的同时，也面临着信息安全的严峻考验。信息安全已成为世界性的现实问题，信息安全与国家安全、民族兴衰和战争胜负息息相关。

本章将学习以下主要内容。

1．计算机信息安全的定义、特征以及含义。

2．计算机信息系统面临的威胁，包括恶意攻击及系统安全缺陷等。

3．信息安全分类及关键技术，系统安全级别。

4．计算机信息系统的安全对策。

1.1　计算机信息安全概述

1.1.1　计算机信息安全的定义

人们对信息安全的认识，是一个由浅入深、由此及彼、由表及里的深化过程。20 世纪 60 年代的通信保密（COMSEC）时代，人们认为信息安全就是通信保密，采用的保障措施就是加密和基于计算机规则的访问控制。到了 20 世纪 80 年代，人们的认识加深了，大家逐步意识到数字化信息除了有保密性的需要外，还有信息的完整性、信息和信息系统的可用性需求，因此明确提出了信息安全就是要保证信息的保密性、完整性和可用性，这就进入了信息安全（INFOSEC）时代。其后由于社会管理以及电子商务、电子政务等网上应用的开展，人们又逐步认识还要关注可控性和不可否认性（真实性）。1993 年 6 月，美国政府同加拿大及欧共体共同起草通用安全评价准则（简称 CC 标准）并将其推进到国际标准（ISO 15408），把所有的安全问题定义为信息系统或者安全产品的安全策略、安全功能、管理、开发、维护、检测、恢复和安全评测等概念的简称。

信息安全的概念是与时俱进的，过去是通信保密（COMSEC）或信息安全（INFOSEC），而今天以至于今后是信息保障（IA- Information Assurance）。

信息安全主要涉及到信息存储的安全、信息传输的安全以及对网络传输信息内容的审计三方面。它研究计算机系统和通信网络内信息的保护方法。

从广义来说，凡是涉及到信息的完整性、保密性、真实性、可用性和可控性的相关技术

和理论都是信息安全所要研究的领域。下面给出信息安全的一般定义：计算机信息安全是指计算机信息系统的硬件、软件、网络及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

1.1.2 计算机信息安全的特征

计算机信息安全具有以下五方面的特征。

1．保密性

保密性是信息不被泄露给非授权的用户、实体或过程，或供其利用的特性，即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。

2．完整性

完整性是信息未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。影响网络信息完整性的主要因素有设备故障、误码、人为攻击及计算机病毒等。

3．真实性

真实性也称作不可否认性。在信息系统的信息交互过程中，确信参与者的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收到信息。

4．可用性

可用性是信息可被授权实体访问并按需求使用的特性，即信息服务在需要时，允许授权用户或实体使用的特性，或者是信息系统（包括网络）部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。

5．可控性

可控性是对信息的传播及内容具有控制能力的特性，即指授权机构可以随时控制信息的机密性。美国政府所提倡的“密钥托管”、“密钥恢复”等措施就是实现信息安全可控性的例子。

概括地说，计算机信息安全核心是通过计算机、网络、密码技术和安全技术，保护在信息系统及公用网络中传输、交换和存储的信息的完整性、保密性、真实性、可用性和可控性等。

1.1.3 计算机信息安全的含义

信息安全的具体含义和侧重点会随着观察者角度的变化而变化。

从用户（个人用户或者企业用户）的角度来说，他们最为关心的问题是如何保证他们的涉及个人隐私或商业利益的数据在传输、交换和存储过程中受到保密性、完整性和真实性的保护，避免其他人（特别是其竞争对手）利用窃听、冒充、篡改和抵赖等手段对其利益和隐私造成损害和侵犯，同时用户也希望他保存在某个网络信息系统中的数据不会受其他非授权用户的访问和破坏。

从网络运行和管理者的角度来说，他们最为关心的问题是如何保护和控制其他人对本地网络信息的访问和读写等操作。比如，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用与非法控制等现象，制止和防御网络黑客的攻击。

对安全保密部门和国家行政部门来说，他们最为关心的问题是如何对非法的、有害的或涉及国家机密的信息进行有效过滤和防堵，避免非法泄露。秘密敏感的信息被泄密后将会对社会的安定产生危害，对国家造成巨大的经济损失和政治损失。

从社会教育和意识形态角度来说，人们最为关心的问题是如何杜绝和控制网络上不健康的内容。有害的黄色内容会对社会的稳定和人类的发展造成不良影响。

1.2 计算机信息系统面临的威胁

计算机网络的发展，使信息共享应用日益广泛与深入。但是信息在公共通信网络上存储、共享和传输，会被非法窃听、截取、篡改或毁坏而导致不可估量的损失。尤其是银行系统、商业系统、管理部门、政府或军事领域对公共通信网络中存储与传输的数据安全问题更为关注。

事物总是辩证的。一方面，信息系统的网络化提供了资源的共享性和用户使用的方便性，通过分布式处理提高了系统效率和可靠性，并且还具有可扩充性。另一方面，这些特点增加了网络信息系统的不安全性。本书所讨论的计算机信息系统主要指网络信息系统。

网络信息的安全所面临的威胁来自很多方面，并且随着时间的变化而变化。这些威胁可以宏观地分为人为威胁和自然威胁。自然威胁可能来自于各种自然灾害、恶劣的场地环境、电磁辐射和电磁干扰以及设备自然老化等。这些无目的的事件，有时会直接威胁计算机信息安全，影响信息的存储媒体。本书重点讨论人为威胁。此种威胁，通过攻击系统暴露的要害或弱点，使得网络信息的保密性、完整性、真实性、可控性和可用性等受到伤害，造成不可估量的经济和政治损失。人为威胁又分为两种：一种是以操作失误为代表的无意威胁（偶然事故），另一种是以计算机犯罪为代表的有意威胁（恶意攻击）。虽然人为的偶然事故没有明显的恶意企图和目的，但它会使信息受到严重破坏。最常见的偶然事故有：操作失误（未经允许使用、操作不当和误用存储媒体等）、意外损失（漏电、电焊火花干扰）、编程缺陷（经验不足、检查漏项）和意外丢失（被盗、被非法复制、丢失媒体）。

1.2.1 恶意攻击

恶意攻击是人为的、有目的的破坏，它可以分为主动攻击和被动攻击。主动攻击是指以各种方式有选择地破坏信息（如修改、删除、伪造、添加、重放、乱序、冒充和制造病毒等）。被动攻击是指在不干扰网络信息系统正常工作的情况下，进行侦收、截获、窃取、破译和业

务流量分析及电磁泄露等。

典型的恶意攻击有如下几种类型。

1．窃听

在广播式网络信息系统中，每个节点都能读取网上的数据。对广播网络的基带同轴电缆或双绞线进行搭线窃听是很容易的，安装通信监视器和读取网上的信息也很容易。网络体系结构允许监视器接收网上传输的所有数据帧而不考虑帧的传输目的地址，这种特性使得偷听网上的数据或非授权访问很容易且不易被发现。

2．流量分析

流量分析能通过对网上信息流的观察和分析推断出网上的数据信息，比如有无传输，传输的数量、方向和频率等。因为网络信息系统的所有节点都能访问全网，所以流量的分析易于完成。由于报头信息不能被加密，所以即使对数据进行了加密处理，也可以进行有效的流量分析。

3．破坏完整性

有意或无意地修改或破坏信息系统，或者在非授权和不能监测的方式下对数据进行修改。

4．重发

重发是重复一份报文或报文的一部分，以便产生一个被授权效果。当节点拷贝发到其他节点的报文并在其后重发它们时，如果不能监测重发，节点依据此报文的内容接收某些操作，例如报文的内容是关闭网络的命令，则将会出现严重的后果。

5．假冒

当一个实体假扮成另一个实体时，就发生了假冒。一个非授权节点，或一个不被信任的、有危险的授权节点都能冒充一个授权节点，而且不会有多大困难。很多网络适配器都允许网帧的源地址由节点自己来选取或改变，这使冒充变得较为容易。

6．拒绝服务

当一个授权实体不能获得对网络资源的访问或当紧急操作被推迟时，就发生了拒绝服务。拒绝服务可能由网络部件的物理损坏而引起，也可能由使用不正确的网络协议而引起（例如传输了错误的信号或在不适当的时候发出了信号），也可能由超载而引起。

7．资源的非授权使用

即与所定义的安全策略不一致的使用。因为常规技术不能限制节点收发信息，也不能限制节点侦听数据，所以一个合法节点能访问网络上的所有数据和资源。

8．干扰

干扰是由一个节点产生数据来扰乱提供给其他节点的服务。干扰也能由一个已经损坏的并还在继续传送报文的节点所引起，或由一个已经被故意改变成具有此效果的节点所引起。频繁的令人讨厌的电子邮件信息是最典型的干扰形式之一。

9．病毒

目前，全世界已经发现了数万种计算机病毒。计算机病毒的数量已有了相当的规模，并且新的病毒还在不断出现。随着计算机技术的不断发展和人们对计算机系统和网络依赖程度的增加，计算机病毒已经构成了对计算机系统和网络的严重威胁。

1.2.2 安全缺陷

假如网络信息系统本身没有任何安全缺陷，那么恶意攻击者即使有天大的本事也不能对网络信息安全构成威胁。但是现在所有的网络信息系统都不可避免地存在着安全缺陷。有些安全缺陷可以通过人为努力加以避免或者改进，但有些安全缺陷则是各种折衷所必须付出的代价。

网络信息系统是计算机技术和通信技术的结合。计算机系统的安全缺陷和通信网络的安全缺陷构成了网络信息系统的潜在安全缺陷。

1.2.2.1 计算机硬件安全缺陷

计算机硬件资源易受自然灾害和人为破坏，计算机硬件工作时的电磁辐射以及硬件的自然失效、外界电磁干扰等均会影响计算机的正常工作。计算机及其外围设备在进行信息处理时会产生电磁泄漏，即电磁辐射。在计算机中，以视频显示器的辐射发射最为严重。由于计算机网络传输媒介的多样性和网内设备分布的广泛性，使得电磁辐射造成信息泄漏的问题变得十分严重。有些先进设备能在一公里以外收集计算机站的电磁辐射信息，并且能区分不同计算机终端的信息。因此，电磁辐射已对计算机信息的安全构成严重威胁。

1.2.2.2 计算机软件安全缺陷

软件资源和数据信息易受计算机病毒的侵扰、非授权用户的复制、篡改和毁坏。由于软件程序的复杂性和编程的多样性，在信息系统的软件中很容易有意或无意地留下一些不易被发现的安全漏洞。软件漏洞显然会影响计算机信息的安全。下面介绍一些有代表性的软件安全漏洞。

1．陷门

陷门是一个程序模块的秘密未记入文档的入口。一般陷门是在程序开发时插入的一小段程序，是用于测试这个模块或是为了连接将来的更改和升级程序或者是为了将来发生故障后，为程序员提供方便等合法用途。通常在程序开发后期去掉这些陷门。但是由于各种有意或无意的原因，陷门也可能被保留下来。陷门一旦被原来的程序员利用，或者被他人发现，将会带来严重的安全后果。比如，可能利用陷门在程序中建立隐蔽通道，甚至植入一些隐蔽的病毒程序等。非法利用陷门可以使原来相互隔离的网络信息形成某种隐蔽的关联，进而可以非法访问网络，达到窃取、更改、伪造和破坏的目的，甚至有可能造成网络信息系统的大面积瘫痪。

2．操作系统的安全漏洞

操作系统是硬件和软件应用程序之间接口的程序模块，它是整个计算机信息系统的核心控制软件。系统的安全体现在整个操作系统之中。对一个设计上不够安全的操作系统，事后