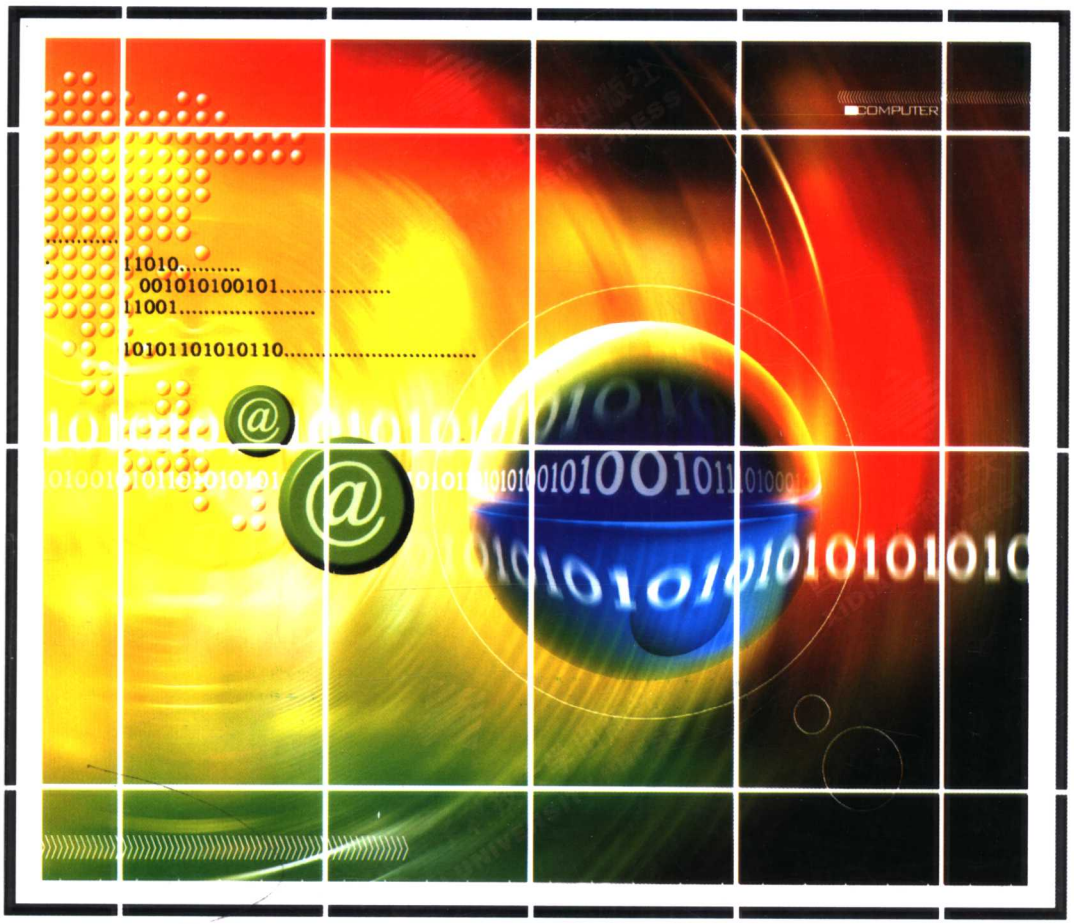
普通高等教育“十一五”国家级规划教材

计算机系统安全

（第二版）

马建峰　郭渊博　编著



西安电子科技大学出版社
http://www.xduph.com

普通高等教育“十一五”国家级规划教材

计算机系统安全

(第 二 版)

马建峰　郭渊博　编著

西安电子科技大学出版社
2007

内 容 简 介

本书详细论述了计算机系统的安全需求、安全对策、安全模型以及安全系统构建理论，系统介绍了安全策略与安全模型在可信操作系统设计、通用操作系统保护、数据库安全设计等方面的相关实践问题。书中对与计算机系统安全相关的常用密码学技术与密码协议理论做了详细介绍和分析。另外，本书还从计算机系统对抗的角度出发，系统讨论了计算机病毒原理及其防治、计算机病毒检测与标识的基本理论、入侵检测的方法与技术以及计算机网络系统可生存性等方面的内容。

本书可作为计算机、信息安全、信息对抗等专业高年级本科生或研究生的教学用书，也可作为相关领域的研究人员和工程技术人员的参考用书。

图书在版编目(CIP)数据

计算机系统安全/马建峰，郭渊博编著. —2 版.
—西安：西安电子科技大学出版社，2007.8
普通高等教育“十一五”国家级规划教材
ISBN 978-7-5606-1867-8

Ⅰ. 计… Ⅱ. ①马… ②郭… Ⅲ. 电子计算机—安全技术—高等学校—教材
Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2007)第 115089 号

策　　划　臧延新
责任编辑　阎　彬　臧延新
出版发行　西安电子科技大学出版社(西安市太白南路 2 号)
电　　话　(029)88242885　88201467　　邮　编　710071
http://www.xduph.com　　E-mail：xdupfxb@pub.xaonline.com
经　　销　新华书店
印刷单位　陕西天意印务有限责任公司
版　　次　2007 年 8 月第 2 版　　2007 年 8 月第 2 次印刷
开　　本　787 毫米×1092 毫米　1/16　印张 22.875
字　　数　540 千字
印　　数　4001～8000 册
定　　价　30.00 元

ISBN 7-5606-1867-8/TP·0972
XDUP 2159002-2

前　言

计算机系统安全是信息安全领域的重要基础，也是其核心内容之一。本教材系统阐述了计算机系统安全的基本理论、技术和方法。

针对计算机系统安全技术的发展和应用水平的提高，我们在第一版的基础上增加了一些新内容，但仍保持了第一版的以讲述计算机系统安全的基本概念、基本理论和基本技术为主的特点。增加的主要内容包括：

(1) 为了反映计算机系统安全技术的发展，增加了两章新的内容："数据库安全模型与机制"和"计算机网络系统的可生存性"，全面介绍了数据库系统的安全需求、安全模型与安全策略、安全机制等方面的内容；同时结合我们的研究，对计算机网络系统可生存性的总体发展轮廓、体系结构和设计方法，以及可生存性的形式化描述和评估等做了阐述。

(2) 对第一版"密码学基本理论"中流密码的部分内容，如反馈移位寄存器等的概念和方法做了适度的拓宽和加深，还加入了对两个重要的流密码算法——A5 和 SEAL 的深入分析，以使读者对流密码算法有进一步的认识。

本书共 14 章。第 1 章的目的在于使读者对计算机系统安全问题有一个概括的了解，其内容包括计算机安全的定义及计算机安全的重要性，计算机系统安全的对策及相关技术，计算机系统安全的内容层次以及专业层次等；第 2～8 章重点介绍了计算机系统安全策略、安全模型以及安全系统构建的相关理论，随后介绍了安全策略与安全模型在可信操作系统设计、通用操作系统保护、安全数据库设计等方面的相关实践问题；第 9 章和第 10 章对与计算机系统安全相关的常用密码学技术与密码协议理论做了简单介绍与概括；第 11～13 章的内容则包括了计算机病毒基本知识、计算机病毒的防治、计算机病毒检测与标识的基本理论以及入侵检测的方法与技术等；第 14 章阐述了计算机网络系统可生存性的体系结构和设计方法、可生存性的形式化描述和评估等。

在本次修订过程中，王卫东老师改正了一版中的一些错误，卢贤玲老师、王超博士和王巍博士参与了第二版增补内容的写作，在此向他(她)们表示衷心的感谢！

本书得到了国家自然科学基金项目(No. 60503012、No. 60573036)的支持，在此表示感谢！

计算机系统安全的特点是综合性强、涉及面广、技术发展快，而我们的学识和水平有限，因此书中难免出现错误和不足之处，敬请读者指正。

作　者

2007 年 6 月

第一版前言

随着计算机在社会各个领域的广泛应用，以计算机为核心的信息系统安全保密的问题显得越来越突出，计算机系统安全已经成为评估计算机系统必不可少的重要指标。计算机安全保密的问题很复杂，涉及面也很广，涉及到密码学、物理环境、硬件、软件、数据传输等各个方面。除了传统的安全保密理论和技术外，计算机信息系统安全还包含更多的内容和独立的体系。当前，国内外信息安全方面的研究已经在经历了信息和数据的保密传输以及信息系统的安全这两个阶段之后，进入了第三个发展阶段，即信息保障/信息可生存性的阶段。在这个阶段，信息安全的主要理论与技术包括密码技术、容忍入侵、访问控制、防火墙和入侵检测技术等。但是，需要指出的是，这个阶段的理论与技术仍然很不完善，许多方面有待突破。对于信息的存储和处理而言，计算机系统发挥了最基本和最核心的作用。实现信息空间安全的关键是保障计算机系统的安全。因此，计算机系统安全是信息保障/信息可生存性的基础。

本书从基本理论和基本技术的角度出发，针对计算机系统的安全需求，系统介绍了安全计算机系统所涉及的模型、框架、方法、技术和相关实现方法等。其特点是广泛关注国内外这一领域的最新进展，并结合实际工作中的研究与设计经验，将计算机安全理论和技术融于计算机安全系统的实际设计与应用之中，旨在让从事计算机安全理论研究的学者了解具体需求，以使其研究更加实用、更加广泛；同时也让从事计算机系统安全工程设计的人员了解计算机系统安全中的关键理论和技术，以设计出更好、更安全的系统。与国内同类著作相比，本书最大的特点就是具有很好的系统性，而不是像大多数教材那样仅偏重于密码学方面的理论或是网络攻防方面的技术。而且，本书将理论与实践有机地融合在一起，具有很好的可读性和适用性。本书可作为计算机、信息安全、信息对抗等专业高年级本科生或研究生的教学用书，也可作为相关领域的研究和工程技术人员的参考用书。

本书共分为 12 章。

第 1 章的内容可使读者对计算机系统安全问题有一个概括的了解，其中包括计算机安全的定义及其重要性，计算机系统安全的对策及相关技术，计算机系统安全的内容层次以及专业层次等；第 2～7 章重点介绍了计算机系统安全策略、安全模型以及安全系统构建的相关理论，并介绍了安全策略与安全模型

在可信操作系统设计与通用操作系统保护等方面的相关实践问题；第 8 章和第 9 章对与计算机系统安全相关的常用密码学技术与密码协议理论做了简单介绍与概括；第 10～12 章的内容则包括了计算机病毒的基本知识、计算机病毒的防治、计算机病毒检测与标识的基本理论以及入侵检测的方法与技术等。

在本书的编写过程中，王巍、张红斌、杨延庆、张光、李灵玲等参与了部分资料的整理工作；宋峰、周彦利、张倩等参与了部分内容的文字录入和校订工作。作者在这里向他们表示衷心的感谢。同时，本书还参阅了国内外同行的大量文献，在此也向这些文献的作者表示衷心的感谢！

本书得到了国家自然科学基金重大计划(No. 90204012)、国家 863 计划(2002AA143021)、教育部优秀青年骨干教师资助计划、教育部科学技术重点研究项目的支持。在此表示感谢！

由于计算机系统安全涉及面很广，限于篇幅，有些基础理论和基本技术未能在本书中全部展开，为此作者表示遗憾和歉意。另外，由于作者的学识和水平有限，书中难免出现错误，敬请读者批评指正。

作　者

2004 年 11 月

欢迎选购西安电子科技大学出版社教材类图书

~~~~~国家级、部级重点教材~~~~~

计算机系统结构（第四版）（李学干） 25.00
离散数学(第三版)（乔维声） 16.00
雷达对抗原理（赵国庆） 15.00
雷达原理（第三版）（丁鹭飞） 23.00
通信网的安全——理论与技术（王育民） 42.00
模拟电子线路基础（傅丰林） 16.00
移动通信（第四版）（李建东） 30.00
智能控制理论和方法（李人厚） 18.00

~~全国信息技术水平考试指定教材~~~

计算机网络信息安全理论与实践教程 32.00
网页设计与网站开发基础教程 54.00
中小学校园网络管理基础教程 19.00
中小学校园网络管理实验教程 25.00

~~~~~~~计算机提高普及类~~~~~~~

计算机应用基础（第三版）（丁爱萍） 22.00
计算机文化基础（第二版）（丁爱萍） 24.00
计算机组装与维护（高职）（杜飞明） 22.00
计算机组装与维护实用教程（第二版）（高职） 29.00
计算机应用基础（Windows 2000 &Office 2002）（教育部高职） 23.00
计算机应用基础实践技能训练与案例分析（教育部高职） 11.00
计算机综合能力实训教程（高职）（孔祥春） 10.00
办公自动化技术及应用教程（赵元哲） 22.00
办公自动化设备的使用和维护（第二版）（高职） 18.00
网络办公自动化技术与应用（高职）（李平） 21.00

~~~~~~~~计算机网络类~~~~~~~~

计算机网络安全（高职）（杨晨光） 15.00
计算机网络管理（雷震甲） 20.00
网络安全技术（高职）（李卓玲） 17.00
网络安全与保密（胡建伟） 28.00
网络信息安全技术（周明全） 17.00
网络信息安全（徐明） 11.00
动态网页设计实用教程（蒋理） 30.00
网站建设与维护（崔良海） 18.00
Windows网络程序设计（夏靖波） 26.00
嵌入式系统原理与开发（夏靖波） 21.00
通信网理论与技术（夏靖波） 25.00
局域网的组建、管理与维护（高职）(雷育春) 20.00
综合布线技术（高职）（于鹏） 18.00
计算机网络技术导论（王宣政） 16.00
计算机网络（第二版）（袁家政） 26.00
计算机网络技术（刘敏涵） 21.00
计算机网络（第二版）（蔡皖东） 26.00
计算机网络工程（石美红） 20.00
计算机网络实验教程（雷震甲） 14.00
计算机组网实验教程（王宣政） 23.00
计算机网络学习辅导及习题详解（权义宁） 23.00
网络工程设计与实践（夏靖波） 31.00
网络应用程序设计（方敏） 21.00
现代网络技术（第二版）(陆楠) 32.00
网络计算（黄健斌） 19.00

~~~~~~~~计算机技术类~~~~~~~~

计算机系统结构（陈智勇） 26.00
计算机系统设计——概念与技术（洪龙） 18.00
计算机组成原理与系统结构实验教程（杨小龙） 12.00
计算机系统安全（马建峰） 22.00
实用计算机类毕业设计指导（聂琨坤） 18.00
计算机原理课程设计（陈智勇） 10.00
电子商务概论（宋沛军）（高职） 20.00
电子商务基础与应用（第五版）（含盘） 39.00
电子商务基础与实务（第二版）（高职） 16.00
《数据结构》算法实现及解析（含光盘）（第二版）（高一凡） 35.00
数据结构—使用C++语言（第二版）（朱战立） 23.00
数据结构（高职）（周岳山） 15.00
计算方法与实习（高职）（田祥宏） 11.00
算法设计与分析(霍红卫) 15.00

编译原理教程（第二版）（胡元义） 18.00
《编译原理教程（第二版）》
习题解析与上机指导（胡元义） 18.00
离散数学（蔡英） 21.00
《离散数学》学习指导书（蔡英） 16.00
离散数学（马光思） 22.00
离散数学——精讲·精解·精练 (黄健斌) 24.00
软件工程（第二版）(邓良松) 22.00
软件工程与数据库概论 (陈春玲) 16.00
信息系统分析与设计（高职）（卫红春） 20.00
信息系统分析与设计（第二版）（陈圣国） 15.00
人工智能技术导论 （第二版）(廉师友) 21.00

～～～～～～计算机辅助技术类～～～～～～

电子工程制图 (含习题集) (高职) (童幸生) 25.00
机械制图与计算机绘图 (含习题集) (高职) 40.00
计算机绘图（第二版）(许社教) 25.00
DSP应用技术（高职）(赵明忠) 25.00
现代DSP技术 (潘松) 22.00
电子电路CAD程序及其应用 (高职) (王源) 16.00
电子线路 CAD 实用教程 (潘永雄) (第二版) 26.00
AUTOCAD 基础教程 (高职) (石高峰) 15.00
电子工艺与电子 CAD（高职）(朱旭平) 14.00
EDA 技术及应用（第二版）(谭会生) 27.00
EDA 技术综合应用实例与分析 (谭会生) 22.00
数字电路 EDA 设计（高职）(顾斌) 19.00

～～～～～～操 作 系 统 类～～～～～～

计算机操作系统（第二版）（颜彬）（高职） 19.00
计算机操作系统（修订版）（汤） 24.00
《计算机操作系统》学习指导与题解 16.00
计算机操作系统（方敏） 28.00
Linux 操作系统实用教程（高职）(梁广民) 20.00
Linux实训指导教程（高职）(陆虹) 13.00

～～～～～～图 形 处 理 类～～～～～～

多媒体技术及应用 (高职) (王坤) 21.00
多媒体软件设计技术（第二版）(陈启安) 20.00
多媒体技术与应用（第二版）（傅献祯） 18.00
多媒体技术基础与应用（曾广雄） 20.00
多媒体技术教程（杨安琪） 20.00
计算机图形学（丁爱玲） 14.00
计算机图形学（研究生系列）（璩柏青） 26.00
计算机图形学——图形的计算与显示原理 22.00
数字图像处理 (何东建) 23.00
3DS MAX 6.0实用教程（高职）(范永富) 23.00

～～～～～～～～微机与控制类～～～～～～～～

微型计算机原理与应用（第二版）（本科） 33.00
《微型原理及应用》（第二版）学习指导 8.00
微型计算机原理（第四版） 29.00
《微型计算机原理》（第四版）学习指导书 14.00
《微型计算机原理》学习与实验指导 18.00
微型计算机原理及接口技术（裘雪红） 25.00
80X86 微机原理与接口技术 (喻宗泉) 26.00
单片机原理及接口技术（余锡存） 15.00
单片机原理与应用技术 (喻宗泉) 19.00
新编单片机原理与应用（潘永雄） 22.00
可编程序控制器原理及应用(第二版) 24.00
计算机控制技术（高职）（温希东） 12.00
微机外围设备的使用与维护 (高职) (王伟) 19.00
微机结构组成与外部设备(第二版) (高职) 17.00

～～～～～数据库及计算机语言类～～～～～

数据库原理（第二版）（郭盈发） 16.00
C程序设计（第二版）（荣政） 20.00
Visual FoxPro 6.0数据库原理与应用（高职） 21.00
基于VFP和SQL的数据库技术及应用 18.00
SQL Server 2000应用基础与实训教程(高职) 22.00
Oracle数据库SQL和PL/SQL实例教程(高职) 17.00
数据库技术及应用（高职）(丁爱萍) 16.00
网络数据库技术及应用（高职）(范剑波) 24.00
C++程序设计语言 (揣锦华) 20.00
《C++程序设计语言》经典题解与实验指导 13.00
Visual C++基础教程（郭文平） 29.00
汇编语言程序设计（第二版）（韩海） 18.00
汇编语言程序设计（李强） 23.00
微型计算机汇编语言程序设计（龚尚福） 23.00
面向对象程序设计与VC++实践(揣锦华) 22.00
面向对象程序设计与C++语言（第二版） 18.00
面向对象程序设计——JAVA（第二版） 32.00

工程材料与热加工技术（高职）（程晓宇）	20.00	电火花加工实训教程（高职）（贾立新）	10.00
先进制造技术（高职）（赵云龙）	14.00	机电一体化技术（高职）(邱士安)	17.00
先进制造技术（高职）（孙燕华）	16.00	机床电器与 PLC（高职）（李伟）	14.00
检测与控制技术（高职）（李贵山）	21.00	机床电气与 PLC（高职）(陶维利)	16.00
机械工程基础（李茹）（高职）	26.00	电机及拖动基础（高职）（孟宪芳）	17.00
机械设计基础（张京辉）（高职）	24.00	电机拖动与控制（高职）（刘保录）	25.00
机械设计基础（郭红星）（高职）	20.00	电机与电气控制（高职）（冉文）	23.00
机械基础（周家泽）	17.00	电切削加工技术（高职）（詹华西）	13.00
机械 CAD/CAM 技术（方新）	20.00	金属切削与机床（高职）（聂建武）	22.00
SolidWorks2005 机械设计		金属切削原理与刀具实训教程（黄雨田）	15.00
基础教程 (高职)（蓝汝铭）	18.00	模具制造技术（高职）（刘航）	22.00
机械制图（刘家平）（高职）	35.00	模具设计（高职）（赵伟阁）	30.00
机械制图与计算机绘图（刘家平）（高职）	40.00	模具设计（高职）（曾霞文）	18.00
机械制造工艺装备（高职）（吴新佳）	19.00	液压与气动技术（朱梅）	19.00
机械制造工艺装备（高职）（朱派龙）	22.00	液压传动技术（高职）（简引霞）	23.00
机械制造技术（高职）（邵堃）	24.00	特种加工技术 (高职)（周旭光）	10.00
机械制造技术（高职）（吴慧媛）	25.00	汽车电工电子技术（高职）（黄建华）	20.00
机械制造基础（高职）（郑广花）	21.00	汽车电气设备与维修（高职）（吴涛）	32.00
机械加工技术（高职）（魏康民）	24.00	汽车电气设备与维修（高职）（李春明）	25.00
计算机辅助机械设计（秦汝明）	19.00	汽车车身结构与维修（高职）（吴兴敏）	26.00
数控机床原理与编程（高职）（陈富安）	20.00	汽车空调（高职）（李祥峰）	16.00
数控编程与操作--SINUMERIK 数控系统	15.00	汽车概论（高职）（邓书涛）	20.00
数控加工与编程（高职）(詹华西)	22.00	现代汽车典型电控系统结构原理	
数控加工工艺与编程（高职）（荣瑞芳）	20.00	与故障诊断（高职）（徐生明）	25.00
数控加工工艺（高职）（赵长旭）	24.00	工业机器人技术（高职）（郭洪红）	16.00
数控加工实训教程（高职）（朱岱力）	14.00	互换性与技术测量（高职）（杨好学）	18.00
数控加工技术实训教程（高职）（詹华西）	23.00	车工基本技能训练（高职）（武建荣）	6.00
数控编程与操作（高职）（秦启书）	16.00	钳工基本技能训练（高职）（彭彦）	5.00
数控技术及应用（高职）（马一民）	17.00	钣金基本技能训练（高职）（刘富觉）	10.00
数控机床故障分析与维修 (高职)（潘海丽）	19.00	焊接基本技能训练（高职）（王红英）	6.00
数控机床电气控制（高职）（姚勇刚）	21.00	建筑管道工基本技能训练（高职）(陈斐明）	8.00
现代数控机床（高职）（刘瑞已）	25.00	铣工基本技能训练（高职）（韩振武）	4.00
数控应用专业英语（高职）（黄海）	17.00	Pro/ENGINEER应用教程（高职）(朱玉红）	23.00
数控原理与系统（高职）（苏宏志）	14.00	营销管理——创造和传递需求的艺术	30.00

欢迎来函索取本社最新书目和教材介绍，欢迎投稿！

通信地址：西安市太白南路2号　　西安电子科技大学出版社发行部　　邮　编：710071

邮购业务电话：（029）88276697 88201467　　传　真：（029）88213675

目　录

第 1 章　计算机安全引论

信息安全是一个具有悠久历史的话题。自 20 世纪 40 年代以来，计算机的出现和迅速普及使人类社会步入了信息时代，信息安全问题越来越显现出其重要性，也促使信息安全技术更加普及，发展更快。

随着计算机在社会各个领域的广泛应用，以计算机为核心的信息系统安全保密的问题越来越突出。同计算机出现前的信息安全保密相比，计算机安全保密的问题要多得多，也复杂得多，它涉及到物理环境，计算机的硬件、软件及数据传输等各个方面。除了传统的安全保密理论和技术外，计算机信息系统安全具有更多的内容和独立的体系。

20 世纪 70 年代以来，在计算机应用和普及的基础上，以计算机网络为主体的信息处理系统得到了迅速的发展，计算机应用也逐渐向网络发展。网络化的信息系统是集通信、计算机和信息处理于一体的、连接广大区域(甚至全球)的系统，是现代社会不可缺少的基础设施之一 。网络信息安全保密的问题与单纯的计算机安全问题不同，不仅有单机的问题，而且还有大量环境、传输、体系结构等问题，因此，系统安全的问题包括了计算机安全、通信安全、操作安全、访问控制、实体安全、电磁安全以及安全管理和法律等方面的问题。

计算机应用发展到网络阶段后，信息安全技术得到了迅速发展，给原有的计算机安全问题增加了许多新的内容。当前，人们在日常生活中对计算机系统的依赖性越来越大。由于对计算机的种种危害直接威胁到了各行各业的发展和国家的机密、财产的安全，因此，计算机系统安全已经成为评估计算机系统性能的必不可少的重要指标，计算机安全学也正在形成一个独立的学科体系。

迄今为止，信息安全的发展经历了三个主要阶段。在第一个阶段，信息安全的主要任务是实现机密数据的保密传输，使用的主要技术是密码技术。而在第二个阶段，信息安全的主要任务是实现信息和信息系统的安全，但并没有更多地考虑信息的可用性和有效性问题。在这个阶段，信息安全的主要技术包括密码学、防火墙和入侵检测等。目前可以认为，信息安全已经进入了第三个发展阶段：信息保障/信息可生存性的阶段。在这个阶段，信息安全的基本目的是：不仅要实现信息的安全性和保密性，同时还要保障信息的可用性和有效性，实现信息保障或者信息可生存性，保障信息空间更高层次的安全。在这个阶段，信息安全的主要理论与技术包括密码技术、容忍入侵、访问控制、防火墙和入侵检测技术等。但需要指出的是，这个阶段的理论与技术仍然很不完善，许多方面有待突破。对于信息的存储和处理而言，计算机系统发挥了最基本和最核心的作用。所以，实现信息空间安全的关键是保障计算机系统的安全，计算机安全是信息系统安全的基础。随着信息系统的广泛建立和各种网络的互连，安全逐渐扩展到了系统和体系，成为全方位的安全问题。

本章的主要内容包括计算机安全的定义、计算机系统安全的重要性、计算机系统的安全对策、计算机系统的安全技术和计算机安全的专业层次。

本章内容是全书的基础，对深入学习和掌握以后各章的内容非常重要。

1.1 计算机安全

1.1.1 计算机安全的定义

所谓计算机安全，是指为计算机系统建立和采取的技术与管理的安全保护措施，这些安全保护措施可以保护计算机系统中的硬件、软件及数据，防止因偶然或恶意的原因而使系统或信息遭到破坏、更改或泄露。信息系统安全的内容包括计算机安全技术、安全管理、安全评价和安全产品、计算机犯罪与侦察、计算机安全法律、安全监察以及计算机安全理论与策略。概括起来，计算机系统的安全性问题被分为三大类，即技术安全类、管理安全类和政策法律类。技术安全是指计算机系统本身采用具有一定安全性质的硬件、软件来实现对于数据或信息的安全保护，在无意和恶意的软件或硬件攻击下仍能使得系统内的数据或信息不增加、不丢失、不泄露。除技术安全之外的，诸如硬件意外故障、场地的意外事故、管理不善导致的数据介质的物理丢失等安全问题，被视为管理安全。而政策法律类则指有关政府部门建立的一系列与计算机犯罪有关的法令、法规。本书将集中讨论技术安全类问题。

国际标准化组织(ISO)曾建议将“计算机安全”定义为：为数据处理系统建立和采取的技术与管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露。

为了帮助计算机用户区分和解决计算机安全问题，美国国防部公布了“桔皮书”(orange book，正式名称为“可信计算机系统标准评估准则”)，对多用户计算机系统安全级别的划分进行了规定。

桔皮书将计算机安全由低到高分为四类七级：D1、C1、C2、B1、B2、B3、A1。其中，D1 级是不具备最低安全限度的等级，C1 和 C2 级是具备最低安全限度的等级，B1 和 B2 级是具有中等安全保护能力的等级，B3 和 A1 属于最高安全等级。

D1 级：计算机安全的最低一级。D1 级不要求用户进行用户登录和密码保护，任何人都可以使用，整个系统是不可信任的，其硬件、软件都易被侵袭。

C1 级：自主安全保护级。C1 级要求硬件有一定的安全级(如计算机带锁)，用户必须通过登录认证方可使用系统，并建立了访问许可权限机制。

C2 级：受控存取保护级。C2 级比 C1 级增加了几个特性：引进了受控访问环境，进一步限制用户执行某些系统指令；授权分级使系统管理员给用户分组，授予他们访问某些程序和分级目录的权限；采用系统审计，跟踪记录所有安全事件及系统管理员工作。

B1 级：标记安全保护级。B1 级对网络上的每个对象都实施保护；支持多级安全，对网络、应用程序工作站实施不同的安全策略；对象必须在访问控制之下，不允许拥有者自己改变所属资源的权限。

B2 级：结构化保护级。B2 级对网络和计算机系统中所有对象都加以定义，给一个标签；为工作站、终端等设备分配不同的安全级别；按最小特权原则取消权力无限大的特权用户。

B3 级：安全域级。B3 级要求用户工作站或终端必须通过信任的途径连接到网络系统内部的主机上；采用硬件来保护系统的数据存储区；根据最小特权原则，增加了系统安全员，将系统管理员、系统操作员和系统安全员的职责分离，将人为因素对计算机安全的威胁减至最小。

A1 级：验证设计级。A1 级是计算机安全级中的最高一级，它包括了以上各级别的所有措施，并附加了一个安全系统的受监视设计；合格的个体必须经过分析并通过这一设计；所有构成系统的部件来源都必须有安全保证；还规定了将安全计算机系统运送到现场安装所必须遵守的程序。

在具体设计过程中，应根据计算机系统规划中提出的各项技术规范、设备类型、性能要求以及经费等综合考虑，以确定一个比较合理、性能较高的计算机系统安全级别，从而实现计算机系统的安全性和可靠性。

我国公安部提出的计算机安全的概念为：计算机系统的硬件、软件、数据受到保护，不因偶然的或恶意的原因而遭到破坏、更改、泄露，系统连续正常运行。

上述定义中所说的计算机系统，指的是信息系统赖以存在的实体和依赖于计算机实体所生成及运行的信息系统。

所谓计算机系统实体，应包括计算机本身的硬件、软件、数据和各种接口，也应包括各种相应的外部设备，还应包括形成计算机网络时应有的通信设备、线路和信道。计算机系统之所以有用，是在形成了计算机信息系统之后。计算机系统实体本身再昂贵也是有价的；而信息系统则是无价的，它的损害往往是无法弥补、难以挽回的。

从以上定义中可以看出，计算机安全是指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害。因此，一切影响计算机安全的因素和保障计算机安全的措施都是计算机安全学研究的内容。这些内容主要有：

(1) 设备安全：指系统设备及相关设施运行正常，系统服务适时，涉及环境、建筑、设备、电磁、辐射、数据介质安全及灾害报警等。

(2) 运行安全：指系统资源和信息资源使用合法，涉及电源、空调、人事管理、机房管理、出入控制、数据与介质管理及运行管理等。

(3) 信息安全：指系统拥有的和产生的数据或信息完整、有效，使用合法，不被破坏或泄露，包括输入/输出数据安全、进入识别、访问控制、加密、审计与追踪、备份与恢复。

(4) 软件安全：指软件(网络软件、操作系统、资料)完整，包括软件开发规程、软件安全测试、软件的修改与复制等。

(5) 通信安全：指计算机通信和网络的安全，包括线路、传输、接口、终端与工作站、路由器的安全等。

反过来，计算机的不安全称为计算机危害。对照计算机安全的概念，计算机危害的概念就是：计算机系统的硬件、软件、数据未受到保护，因偶然的或恶意的原因而遭到破坏、更改、泄露，系统不能连续正常运行。

“系统连续正常运行”进一步阐明了信息系统的动态安全，即保证信息系统正常运转，为我所用，发挥应有效益。

“保护”的终极目标是信息系统的安全。为此，必须保护计算机系统实体及其所在的环境。所谓环境，不仅是指机房等物理环境，更重要的是系统所处的社会人文环境。

上述定义既说清了计算机安全的本质和核心，又顾及到了安全所涉及到的方面。

因此，完整的计算机安全体系的定义是由“实体安全”、“运行安全”和“数据安全”三部分组成的。

安全对抗的核心对象是计算机信息系统；安全对抗的核心因素是人。

不言而喻，计算机系统、物理环境和社会人文环境，皆为人控制；各种计算机危害，除了难以预知和抗拒的天灾外，亦为人所致。人是最为活跃、能动的核心因素。惟有依靠人，采取技术的、管理的和法律的得力措施，才能把计算机危害抑制到最低限度。从这个意义上讲，计算机安全治理的核心问题是人的技术和职业道德教育。

1.1.2 计算机系统面临的威胁和攻击

计算机系统所面临的威胁和攻击大体上可以分为两类：一类是对实体的威胁和攻击，另一类是对信息的威胁和攻击。计算机犯罪和计算机病毒则包括了对计算机系统实体和信息两个方面的威胁和攻击。

1. 对实体的威胁和攻击

对实体的威胁和攻击主要指对计算机及其外部设备和网络的威胁和攻击，如各种自然灾害与人为的破坏、设备故障、场地和环境因素的影响、电磁场的干扰或电磁泄露、战争的破坏、各种媒体的被盗和散失等。对信息系统实体的威胁和攻击，不仅会造成设备的严重损坏，而且会使信息系统的机密信息严重泄露和破坏。因此，对信息系统实体的保护是防止对信息威胁和攻击的首要一步，也是防止对信息威胁和攻击的天然屏障。

2. 对计算机系统的威胁和攻击

计算机系统所面临的威胁大体可分为两种：一种是信息泄露，另一种是信息破坏。所谓信息泄露，就是指偶然地或故意地获得(侦收、截获、窃取或分析破译)目标系统中的信息，特别是敏感信息，造成泄露事件。信息破坏是指由于偶然事故或人为破坏，使信息的正确性、完整性和可用性受到破坏，如系统的信息被修改、删除、添加、伪造或非法复制，造成大量信息的破坏、修改或丢失。

影响计算机系统的因素很多，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计算机系统资源的非法使用。

人为破坏有以下几种手段：

(1) 利用系统本身的脆弱性。

(2) 滥用特权身份。

(3) 对系统的非法使用。

(4) 修改或非法复制系统中的数据。

偶然事故有以下几种可能的情况：

(1) 硬、软件的故障引起安全策略失效。

(2) 工作人员的误操作使系统出错，使信息严重被破坏或无意地让别人看到了机密信息。

(3) 自然灾害的破坏，如洪水、地震、风暴、泥石流等使计算机系统受到严重破坏。

(4) 环境因素的突然变化，如高温或低温、各种污染破坏了空气洁净度，电源突然掉电或被冲击造成系统信息出错、丢失或破坏。