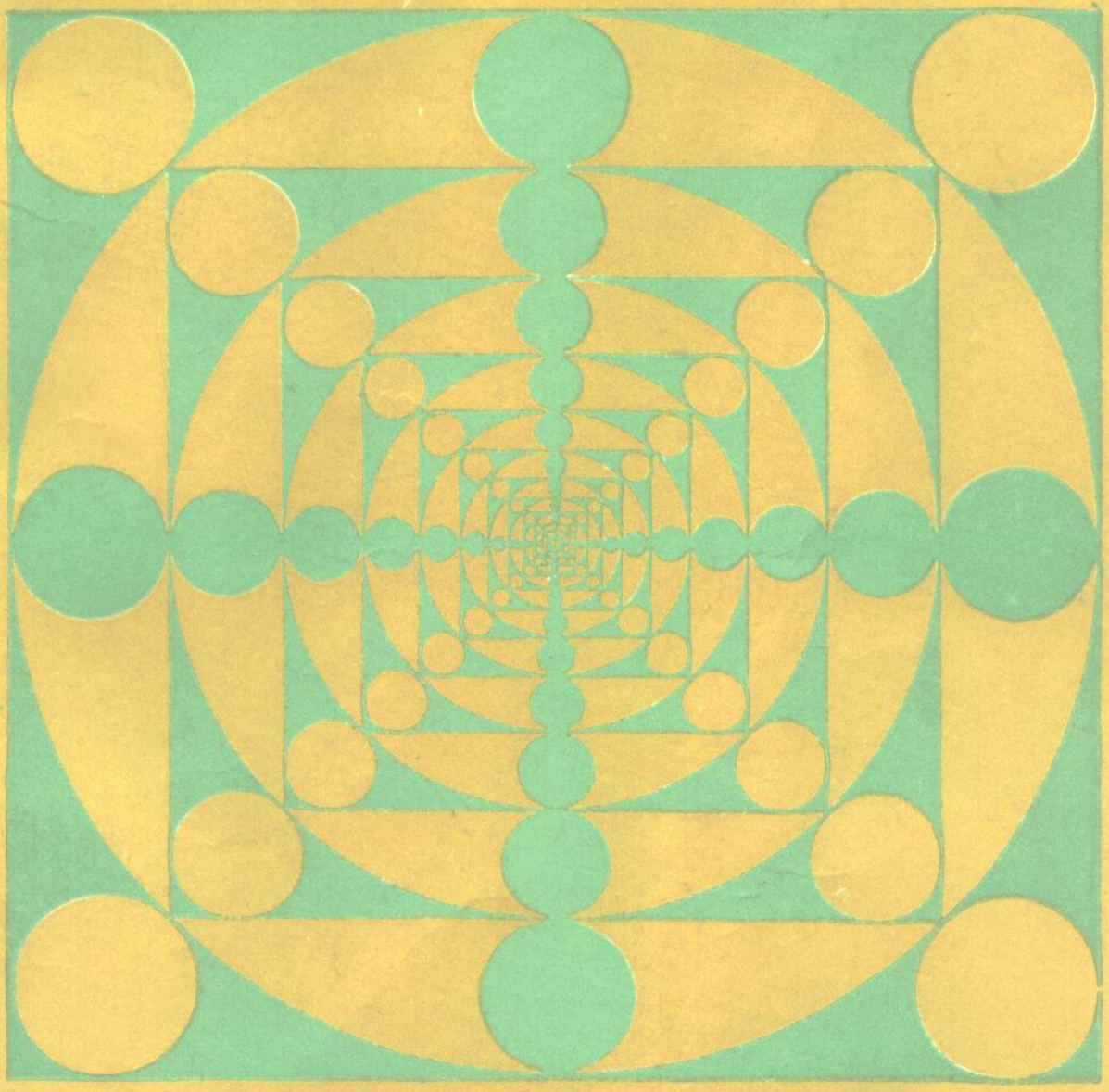
电子计算机应用系列教材

计算机安全保密原理与技术

王化文　张德向　吴　亮　张能胜　李　立　编著



科学出版社

电子计算机应用系列教材

计算机安全保密原理与技术

王化文　张德向
吴　亮　张能胜　李　立　编著

科学出版社

1993

(京)新登字 092 号

内 容 简 介

本书是电子计算机应用系列教材之一. 书中全面阐述了计算机安全保密的基本原理与技术. 全书共八章,主要内容包括:概述;密码术;数据加密标准;存储介质防复制技术;磁盘文件加密;加密文件防破译;网络通信安全保密技术;数据库安全与保密等. 本书的主要特点是理论密切联系实际、实用性强. 书中列有大量的程序范例,便于读者学习、掌握和运用.

本书可作为在职科技人员计算机应用中级培训教材,也可供计算机专业的研究生和大专院校计算机专业高年级学生和有关专业人员参考.

电子计算机应用系列教材

计算机安全保密原理与技术

王化文 张德向
吴 亮 张能胜 李 立 编著

责任编辑 范铁夫

科学出版社出版
北京东黄城根北街16号
邮政编码:100717

北京市华星计算机公司激光照排
国防科工委印刷厂印刷

1993年1月第 一 版 开本:787×1092 1/16
1993年1月第一次印刷 印张:14½
印数:0001—5100 字数:329000

ISBN7-03-001343-3/TP·81

定价:12.40元

电子计算机应用系列教材主持、组织编著单位

主持编著单位：

国务院电子信息系统推广应用办公室

组织编著单位：

广东、广西、上海、山东、山西、天津、云南、内蒙古、
四川、辽宁、北京、江苏、甘肃、宁夏、江西、安徽、
河北、河南、贵州、浙江、湖北、湖南、黑龙江、福建、
新疆、广州、大连、宁波、西安、沈阳、武汉、青岛、
重庆、哈尔滨、南京等35省、市、自治区、计划单列市

电子振兴
计 算 机 领导小组办公室
科技工作

电子计算机应用系列教材联合编审委员会名单

（以姓氏笔画为序）

主 编 审 委 员：

王长胤* 苏世生 何守才 陈有祺 陈莘萌* 邹海明* 郑天健
殷志鹤 童 频 赖翔飞 （有"*"者为常务主编）

常务编审委员：

于占涛 王一良 冯锡祺 刘大昕 朱维华 陈火旺 陈洪陶 余 俊
李 祥 苏锦祥 佟震亚 张广华 张少润 张吉生 张志浩 张建荣
钟伯刚 胡秉光 高树森 徐洁盘 曹大铸 谢王光 谢育先 韩兆轩
韩培尧 董继润 程慧霞

编审委员：

王升亮 王伦津 王树人 王振宇 王继青 王翰虎 毛培法 叶以丰
冯鉴生 刘开瑛 刘尚威 刘国靖 刘晓融 刘德镇 孙令举 孙其梅
孙耕田 朱泳岭 许震宇 何文兴 陈凤枝 陈兴业 陈启泉 陈时锦
邱玉辉 吴宇尧 吴意生 李克洪 李迪义 李忠民 迟忠先 沈林兴
肖金声 苏松基 杨润生 闵福德 张志弘 张银明 张 勤 张福源
张翼鹏 郑玉林 郑 重 郑桂林 孟昭光 林俊伯 林钧海 周俊林
赵振玉 赵惠溥 姚卿达 段银田 钟维明 袁玉馨 唐肖光 唐楷全
徐国平 徐拾义 康继昌 高登芳 黄友谦 黄 侃 程锦松 楼朝城
潘正运 潘庆荣

秘 书 组：

秘 书 长：胡茂生
副秘书长：何兴能 林茂荃 易 勤 黄雄才

序

当代新技术革命的蓬勃发展，带来社会生产力新的飞跃、引起整个社会的巨大变革．电子计算机技术是新技术革命中最活跃的核心技术，在工农业生产、流通领域、国防建设和科学研究方面得到越来越广泛的应用．

党的十一届三中全会以来，我国计算机应用事业的发展是相当迅速的．到目前为止，全国装机量已突破三十万台、十六位以下微型计算机开始形成产业和市场规模，全国从事计算机科研、开发、生产、应用、经营、服务和教学的科技人员已达十多万人，与1980年相比，增长了近八倍．他们在工业、农业、商业、城建、金融、科技、文教、卫生、公安等广阔的领域中积极开发应用计算机技术，取得了优异的成绩，创造了显著的经济效益和社会效益，为开拓计算机应用的新局面作出了重要贡献．实践证明，人才是计算机开发应用的中心环节．我们必须把计算机应用人才的开发与培养放在计算机应用事业的首位，要坚持不懈地抓住人才培养这个关键．

从目前来看，我国计算机应用人才队伍虽然有了很大的发展，但是这支队伍的数量和质量还远不适应计算机应用事业发展的客观需要，复合型人才的培养与教育还没有走上规范化、制度化轨道，教材建设仍显薄弱，培训质量不高．因此，在国务院电子信息系统推广应用办公室领导、支持下，全国三十五个省、市、自治区、计划单列市计算机应用主管部门共同组织118所大学和科研单位的400多位专家、教授编写了全国第一部《电子计算机应用人才培训大纲》以及与之配套使用的电子计算机应用系列教材，在人才培训和开发方面做了一件很有意义的工作，对实现培训工作规范化、制度化将起到很好的推动作用．

《电子计算机应用人才培训大纲》和电子计算机应用系列教材贯穿了从应用出发、为应用服务，大力培养高质量、多层次、复合型 应用人才这样一条主线．大纲总结了近几年各地计算机技术培训正反两方面的经验，提出了计算机应用人才的层次结构、不同层次人才的素质要求和培养途径，制定了一套必须遵循的层次化培训办学规范，编制了适应办学规范的“课程教学大纲”．这部大纲为各地方、各部门、各单位制定人才培养规划和工作计划提供了原则依据，为科技人员、管理人员以及其他人员学习计算机技术指出了努力方向和步骤，为社会提供了考核计算机应用人才的客观尺度．“电子计算机应用系列教材”是培训大纲在教学内容上的展开与体现，是我国目前规模最大的一套计算机应用教材．教材的体系为树型结构，模块化与系统性、连贯性、完整性相兼容，教学内容注重实用性、工程性、科学性，并具有简明清晰、通俗易懂、方便教学、易于自学等特点，是一套很好的系列教材．

这部大纲和系列教材的诞生是各方面团结合作、群策群力的结果，它的公开出版和发行，对计算机应用人才的培训工作将起到积极的推动作用．希望全国各地区、各部门、各单位广泛运用这套系列教材，发挥它应有的作用，并在实践中检验、修改、补充和完善它．

通过培训教材的建设，把培训工作与贯彻国家既定的成人教育、函授教育、电视教育

和科技人员继续工程教育等制度相结合，逐步把计算机应用人才的培训工作引向规范化、制度化轨道，为培养和造就大批高素质、多层次、复合型计算机应用人才而努力奋斗，更好地推动计算机应用事业向深度和广度发展.

李祥林

1988年10月17日

前　言

随着计算机在各个领域的广泛应用，需要对大量被传输和存取的信息进行保护，这样，计算机安全保密就成了计算机科学中的一个重要的研究课题，特别是在70年代以后，由于出现了强有力的基于加密的协议，并开辟了新的应用领域，密码学得到了迅速的发展. 1977年1月15日，美国国家标准局采纳了一种加密算法作为联邦的标准——数据加密标准(DES)，从而成为密码研究和设计方面的一个新的里程碑. 1980年12月，美国国家标准协会采纳这个算法作为美国的商用加密算法，随后人们又提出了公开密钥密码的新思想，这种密码目前还在研究之中. 人们研究密码术，不仅将它应用于网络通信中的数据加密，还将它应用于存储介质的文件加密等方面，因此，进行计算机安全保密的研究对于保护政治、经济、军事和其他部门的信息具有极为重要的意义. 为了满足广大读者了解和掌握数据安全保密的原理和方法的需要，我们编写了这本书.

本书是电子计算机应用系列教材之一. 全书共分八章，主要介绍计算机安全保密的发展情况和立法情况，阐述密码术的基本原理，讨论常用的加密算法，并以存储介质和通信网络的安全保密为重点，讨论实施计算机安全保密的技术和方法，如存储介质的防复制技术、软件加密、加密系统和加密程序的防跟踪破译措施、网络通信的信息加密，以及微机数据库安全与保密等. 全书各章尽可能结合 IBM PC 微型计算机，列举大量已运行通过的程序实例，以供读者进一步研究时参考. 本教材适用于中级计算机应用科技人员的研修学习，也可作为大专院校高年级学生和研究生以及其他有关专业人员的参考书.

使用本教材时应注意除课堂讲授以外，必须上机实习(可参考教材中列举的实例)，在作习题的基础上开展一些专题讨论和研究工作. 本教材的重点是讲述存储介质和通信网络的安全保密原理及实施技术. 学习本课程要求具备汇编语言程序设计、计算机网络、数据库和操作系统等方面的知识.

本教材由王化文编写第四章和第七章，张德向编写第五章和第六章，吴亮编写第一章和第八章，张能胜编写第二章和第三章，李立参加了第四章和第五章的部分编写工作，由王化文统编全稿. 本书由河北机电学院赵惠溥副教授担任主审，在此谨向他表示诚挚的谢意. 由于编著者水平有限，书中难免还存在一些缺点和错误，殷切希望广大读者指正.

编著者

目　录

第一章 概 述

自1946年第一台电子数字计算机问世以来，至今已有40多年的发展历史. 今天的计算机已经不仅仅是用于科学计算的快速工具，而是几乎用于各个领域的信息储存和处理的工具. 政府机关、大型企业、银行、军事机关等国家的重要部门都使用计算机建立了信息系统，大量的政治、经济、军事信息都转换为数据存放在计算机里进行处理. 而且，随着计算机性能的不断提高，设备的规模日益增大，许多信息系统已经联成了世界性的计算机网络系统. 例如，全世界已有二千多家银行联成了计算机网络，组成了电子汇兑系统. 通过这个电子汇兑系统，可以自动完成异地各银行之间转帐、现金和支票的结算，以及银行的清算轧帐等等. 计算机应用的普及和深入已经使得社会的生产方式发生了重大变化，而且对现代社会的生活也产生了重大影响，使得现代社会成为信息化的社会. 计算机应用的普及，虽然对现代社会的发展起到很大的推动作用，使得各方面都越来越依赖于计算机提高工作质量和效率，但也随之带来了新的问题——计算机的信息安全问题.

1.1 计算机安全与保密研究的内容和意义

计算机安全技术是随着计算机应用的深入而逐步提出来的. 因为，随着国家的政府机关、大型企业、银行、军事机关等部门大量使用计算机，并建立了庞大的信息系统，大量的国家机密，以及国家要害部门的政治、经济、军事等系统的重要数据都存放在计算机的数据库系统中，利用计算机进行信息处理，而且现代计算机还能联成世界性的庞大的计算机网络，网上的每一台计算机都可以相互存取信息. 显然，这就给窃取其它国家的信息机密提供了机会. 因此，随着计算机应用的普及和深入，出现了利用计算机进行犯罪和窃密，而且越来越严重. 因为破坏某个国家的政府机构所建立的信息系统，就意味着使其政府的一部分职能丧失，甚至导致整个国家机器都运转失灵. 另外，把计算机系统中的数据破坏或者篡改，也会使飞机、轮船偏离航向，或者使火车失事，达到谋害某个重要人物的目的. 例如，国外曾报道，某国驻外大使曾因导航计算机数据出现误差，险些机毁人亡. 还有一些国家，利用出口计算机来进行间谍活动和经济讹诈，如在出口的计算机系统中暗藏程序，窃取信息或进行破坏，使其在使用的某个时候出错，或者是利用出口计算机的零配件，或配套软件要挟买主国. 所以，对于依赖进口计算机的国家来说，计算机的安全和信息保密问题更为重要.

除了这种利用各种手段，进行非法地窃取国家机密，或是窃取单位及个人的秘密的计算机犯罪以外，还有的就是采用暴力手段进攻和炸毁计算机设备，非法破坏和清除重要的计算机程序和数据，造成计算机系统的重大失误或瘫痪. 据报道，70年代初就曾在某些国家发生过暴力袭击计算中心的事件. 因此，计算机机房的实体安全防护措施也具有重要意义. 它不仅可以防止敌人的进攻，而且对于抵抗自然灾害或意外事故，如火灾、水灾等也是

非常必要的. 其次,利用计算机进行诈骗活动,也是计算机犯罪的一种常见案例. 罪犯通过计算机修改银行或公司帐目,把别人在计算机户头上储存的金钱改在自己的户头上,或是为自己增加工资金额,达到骗取金钱的目的. 甚至有些罪犯还盗用计算机进行工程设计或算题,偷用以后又不缴纳上机费,以获取额外收入. 还有一些计算机系统,由于安全保护措施不力,用户在使用过程中很容易侵入系统程序,造成系统信息破坏,致使整个系统运转出错. 据国外杂志报道,某计算机系统就是由于有几个中学生上机实习时出于好奇心修改了系统文件的某些信息,造成了系统运行时发生错误.

显然,计算机犯罪或事故所造成的损失是相当严重的. 有关资料表明,美国每年因计算机犯罪或事故造成的损失达到几十亿美元. 实际数字可能还要大,因为计算机犯罪是在广泛深入使用计算机的形势下出现的,从事计算机犯罪活动的人往往不被察觉,也未留下什么痕迹. 近年来,据美国联邦调查局估计,实际发生的计算机犯罪案件仅有1%能被发现,且发现以后也难以侦破. 所以,进行计算机信息安全与保密的研究,意义是非常重要的. 实施计算机安全措施,不仅能够保护国家的机密,以及政府和单位、个人的秘密,也可避免造成巨大的经济损失,杜绝计算机犯罪的发生,使得计算机的应用更加深入发展,促进现代社会的不断发展,使计算机为人类的幸福与和平事业发挥效益,真正成为人类实现现代化的有效工具.

那么,计算机信息安全到底要研究哪些内容呢? 从目前对计算机安全的要求来看,其主要研究包括以下四个方面:

1. 计算机实体安全

所谓计算机的实体安全,就是保证计算机系统的各种设备,包括机房设备的安全. 计算机实体的安全,是保证计算机正常运行,确保信息系统安全的前提.

计算机在实际运行时,可能会遇到一些人为的或自然的因素所造成的计算机实体的破坏,使得信息系统遭受破坏. 因此,对计算机安放的位置,地理环境等都要慎重选择,要考虑战争和暴力袭击的影响,其次,还要考虑地震和水灾等自然因素的影响,这对计算机的防火、防漏、防尘、防磁都是十分重要的,甚至空气成分对计算机设备也会产生影响. 据报道,IBM公司的3330磁盘机常常出错,有可能是空气中的有机锡造成的. 所以计算机的实体安全有许多值得研究的课题.

2. 计算机防电磁波辐射

计算机系统电磁波安全问题包含两个方面,一是计算机系统受到外界电磁场的干扰,使得计算机系统不能正常工作. 例如美国曾经有一台计算机安装在几个商业广播电台和雷达站附近,造成计算机运算时常常出错. 测量发现,电磁场强度太大,于是把机房进行金属屏蔽,计算机才得以正常运行.

二是计算机系统本身向外界所产生的电磁波,造成信息泄漏,为攻击者提供了电磁窃取的可能性. 这种情况往往不受计算机专业人员和保卫人员的重视,他们常常认为计算机工作时所产生的电磁波辐射很微弱,可以忽略. 其实不然,计算机工作时系统运行的高频电脉冲会不断向外界空间辐射电磁波. 这样,通过无线电接收机就可接收到辐射的信息. 如果人为地在计算机内装上发射电波的装置,使高频电波发射功率增大,就会使计算机运

行时辐射的电磁信号更容易被接收. 很显然,这种利用计算机向外泄漏电磁波,接收以后再加以还原的作法是现代电磁窃听技术的新手段,既非常隐蔽,又不易被察觉. 从事间谍活动的人,用一台接收机,接收到计算机系统辐射的电磁波信号后,就可通过卫星发回本国的情报中心,再利用计算机解译出所需要的信息来. 因为计算机的显示器、打印机等往返扫描式的设备,工作时电波规律性明显,其窃听到的电磁波信息解译出来是比较容易的. 例如,国外在1985年就报道过,一位荷兰的无线电技术人员,用一台稍加改装的黑白电视机,在1公里的距离内,接收了计算机显示终端上的辐射信息,并在黑白电视机的荧幕上复原出来,可以看到和计算机显示屏上相同的内容. 我国也有人做过同样的试验,也证明了能把计算机显示屏辐射电波的信息复原出来.

这些都说明计算机系统本身的电磁辐射问题是危及计算机信息安全的一个重要方面. 由此出现了一项专门的技术——TEMPEST技术. TEMPEST技术,简要地讲就是研究控制和抑制信息处理设备工作时所散射的寄生电信号(Spurious Electronic Signals). 显然,TEMPEST技术的研究,实际上就是对计算机电磁波安全问题的研究. 现在TEMPEST技术的研究已受到国内外的高度重视.

3. 计算机数据操作安全

现代的计算机系统大都是庞大的信息处理系统,如经济信息系统、金融信息系统、军事信息系统等等,它们不再是独立的使用,而是利用各种数据库来储存大量的信息,而且为了提高信息的使用率,数据库中存放的信息往往是共享的,即信息可以为许多用户所共用. 数据库中的数据有的允许任何人使用,有的则只允许某些机关部门的专门人员使用,还有的只限于本部门中一定级别的专门人员使用. 否则,任何人对数据库的数据都可以进行任何操作,数据安全就无法保证.

因此,对数据操作安全的研究就包括了对计算机操作系统安全,以及数据库安全的研究. 这两个方面的研究内容是非常广泛的. 首先是存取控制,即采用授权控制,也就是规定哪些用户可以使用哪些信息? 可以对数据进行哪些操作? (如只读或只写,不允许修改等),可以在什么时候进行操作? 在什么地方进行操作? 以及用户为什么要进行这一操作等等. 根据这些规定,计算机的操作系统或数据的存取控制机构就可以在用户进行数据操作时,检查用户身份和使用权限,防止非授权者的侵入. 如果有非授权者绕过存取控制机构的检查,非法侵入进行数据操作时,操作系统或数据库的保护机构还要能够追踪非法侵入者,记下侵入者窃密的踪迹,以供侦破使用.

存取控制是保证数据操作安全的重要一环. 其中重要的一步是检查用户代码和口令(暗号),这些代码和口令通常由字母数字串组成,是比较容易被人冒名顶替的. 例如,美国曾发生这样一起计算机案例,几名少年,长期在终端上猜测口令,最终试出一套口令,通过学校的那台终端进入了美国-加拿大的计算机网络, 使得加拿大20多家数据系统受到干扰. 因此,通常要对口令加密.

还有一个例子是,美国一家银行职员,非法侵入操作系统,篡改银行的出纳程序,把储户计利息时不足一分的零头都转记到这个职员的名下,时间一长就可达到相当可观的数目.

另外,数据库中除了存取控制来保护数据的安全外,还要对一些机密数据进行编码加

密，使机密数据用密码存放，防止机密数据泄漏．所以，进行作操系统安全和数据库安全的研究，对于实现数据操作安全、建立安全的计算机系统具有重大意义．

4．计算机数据通信安全

现代计算机系统不仅形成庞大的数据库系统，还组成了世界性的计算机网络，为世界各地进行大量的信息交流提供了巨大的便利，同时这种世界性的计算机网络在进行数据通信时，将对数据安全产生严重的威胁．例如，美国同欧洲之间有两家银行通过计算机网络进行转帐，结果被人们在通信线路上安装了窃听器，不仅监听了他们传递资金的情况，还造成资金传送方向的改变，使得本来转到欧洲某家银行帐上的资金反而转送到了另一家银行的帐户上了．由于在计算机网上通信受到窃密和攻击，不仅在经济上造成重大损失，往往还影响国家之间的关系．所以，计算机网络通信的安全，一直受到人们的高度重视．因为，自从世界上出现电子通信以来，信息通信网历来都是受攻击和截获情报的重点对象．计算机网只不过是现代电子通信网络的一种延伸和发展．因此，计算机网的安全可以利用通信网络的一些防护措施，如使用古老的密码术，对所需传输的数据进行加密，接收者接收以后再脱密还原．这样即使在网络传输过程中被截取，因为是密码，在一段时间内破译不了就可起到一定的保护作用．因此，在计算机数据通信安全的研究中，密码技术的研究是一项重要的内容．特别是用于计算机通信网上的加密、解密技术，以及各种适合于计算机系统的密码变换方法都是通信安全中要研究的内容．除此而外，还要研究计算机网的特殊问题，如何防止利用计算机网窃取网上数据库中的数据，或防止修改网络操作系统的程序等等．通常对通信网的窃听有两种情况：一是被动的单纯式窃听，即只是窃听传送信息的内容，并不改变传送信息的内容；二是主动的更改式窃听，即除了截收传送的信息以外，还要更改部分信息，然后继续传送出去，使接收者接收错误的信息．

现代的计算机网不仅承担着传送信息的任务，而且使用计算机网就像使用电话网一样普遍和方便；任何人，任何时间，在任何地方，只要计算机终端联在网络上就可以使用计算机网进行数据通信，因此给信息的相互交流和数据的共享带来了极大的方便．但是，不容忽视的是，它也给计算机的数据通信安全提出了许多值得研究的课题．

总之，计算机信息安全与保密所要研究的内容是十分广泛的，它是包括计算机的硬件结构设计、软件系统设计、电磁辐射、密码学、电子学、计算机管理、社会学和法律学等多方面的综合性的研究．实际上计算机安全是一门自然科学和社会科学等多学科交叉的综合性学科．而且，计算机安全不仅仅是一项科学研究，它还将对现代社会产生重大影响，并且涉及到国家的政治、经济和军事等重要部门．因此，计算机安全的研究应当受到社会各方面的重视和支持．

1.2 计算机安全与保密的发展概况

图 1.1 描述了计算机保密与安全的关系．在计算机应用的早期，即 50 年代到 60 年代，计算机保密只是限于军事方面．因为那时计算机应用的范围很有限，外界接触计算机系统的机会也不多，加上军事计算机系统往往是封闭的系统，所以计算机安全的问题还不突出．而且当时计算机系统本身的性能也较低，计算机应用软件的开发水平也不高，计算

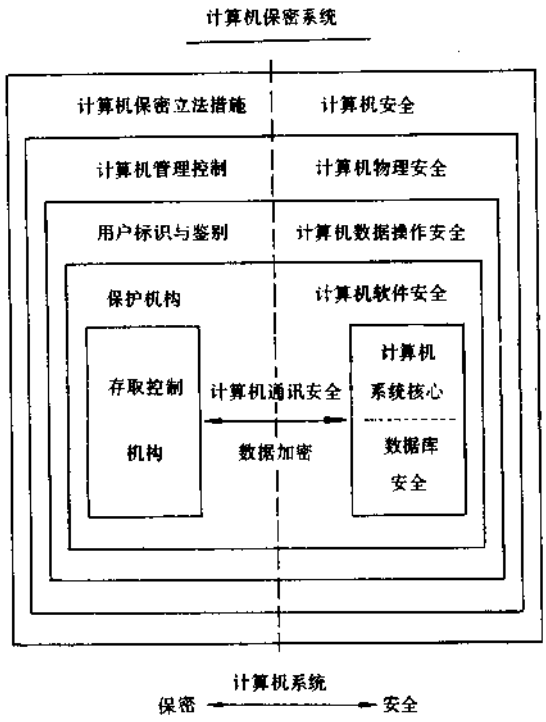


图 1.1 计算机保密与安全的关系

机主要应用是科学计算. 因此,人们的主要精力是放在如何提高计算机系统的性能,研究高级的软件开发工具等,对计算机信息安全问题还来不及考虑. 到了 60 年代末,随着计算机系统性能的提高,计算机系统的操作方式上有了很大改进,出现了许多高级语言,如 FORTRAN,ALGOL,PL/1,PASCAL 等等,并提出了计算机的操作系统概念. 它是以多道程序运行和分时操作为其特征的计算机系统,是现代计算机的标志. 众所周知,现在,计算机的发展已经历了四代,正向新一代更高性能的智能计算机发展. 现代的计算机已具有完善的操作系统,而在当时,操作系统出现的初期,要实现多道程序运行和分时操作,操作系统必须管理好各种计算机资源的使用,如内存管理,作业管理与控制,进程管理以及设备管理等. 特别是内存管理,由于实现了多道程序运行,多个作业要同时装入内存并运行,而且要求相互之间又不能发生干扰或者相互侵入甚至有意破坏. 因此,操作系统的设计者们开始认识到信息保护的必要性,并着手研究信息保护的措施和手段. 这一时期(60 年代末到 70 年代初)是计算机安全与保密发展的第一阶段. 它的主要特点是:采用程序的方法实现信息保护,通常是由计算机的操作系统来完成信息保护的功能.

进入 70 年代后,由于大规模集成电路的出现,使计算机迅速进入第四代,计算机的硬件和软件都有了很大的发展,计算机的应用也日益广泛,随之计算机犯罪案件也时有发生. 据有关资料记载,1973 年美国因计算机信息系统中文件被盗所造成的损失达到国民总收入的 1%. 因此,计算机安全问题马上受到了有关部门的高度重视,计算机安全系统的研制者们也在想方设法制造出具有信息保护功能的产品. 因为现有的计算机系统,如

OS/360 虽能对非法接触信息告警，但并不能防止犯罪分子接触信息，其信息保护功能并不强. 所以随后又出现了 MULTIC 操作系统、SDC 公司研制的 ADFPT-50 系统，以及马萨诸塞工艺学院和几家公司共同研制的资源安全系统等等. 这些系统除了具有原来 OS/360 系统的保护功能外，还采用了分密级的数据结构，按不同密级控制进入相应数据区，采用口令暗语和对用户受权的存取控制方法，以实现用户和系统的隔离，以及用户访问完后清除残留内存的信息等等措施，来增强计算机系统的安全性. 但是，无论怎样改善操作系统，还是不能达到可靠地保证信息安全的目的，罪犯还是可能通过猜口令、修改密级和受权级别等非法手段绕过各种保护装置，接触保密信息，因为从事计算机犯罪的罪犯大都是计算机方面的专业人员. 因此，为了保证操作系统的保护装置能够对外实现控制，提出了计算机安全核心的概念，这就是保护系统要求采用统一的设备和程序的综合措施. 这是计算机安全技术发展的第二阶段.

70 年代后期到 80 年代，随着计算机应用的普及和深入，使现代社会发展成为信息化的社会，无论是国家决策机关，还是人们的日常生活；无论是银行的金融系统，还是企业的规划管理；无论是商业服务系统，还是交通运输调度管理，几乎是各行各业都越来越依赖计算机. 因为当今世界计算机已是深入到家庭的“细胞”，缺少这一细胞，或者是这一细胞出毛病，都将带来极大的社会问题. 这就是人们常常谈论的计算机化社会的脆弱性. 除此而外，由于计算机技术的不断提高，计算机应用水平也在逐步发展，使用和掌握计算机技术的人越来越多，计算机犯罪和滥用案件不断发生，计算机的安全已受到严重威胁. 由于计算机系统遭到窃密、篡改、破坏和引出故障等造成的损失越来越大，计算机社会的脆弱性表现得更为突出，迫使人们在使用计算机时，不得不用心考虑信息安全的问题. 因此，这一时期计算机安全技术的发展也有了很大的进步，许多信息系统都采用了各种安全保护措施. 如复杂口令、实时口令和应答会话协定，或是应用动态程序等身份鉴别的手段进行存取控制和授权控制；还有的通过硬件装置检查磁卡或标志；甚至有的系统要检验语音波形、指纹、手形和面部形状的几何特征等才能进入. 只要计算机系统在运行，就会在硬件、软件和数据三个层次都实施保护措施. 而且，这一阶段已经不单是从计算机技术一方面考虑信息安全问题，而是把计算机的实体安全技术、存取控制软件、数据的加密和解密、TEMPEST 技术、计算机安全审计技术，以及计算机立法和其它安全管理方法都结合在一起，形成一套综合性的安全措施和信息保护机构. 这种综合性的安全保护方法涉及到许多方面，必须由各方面的技术人员共同合作研究，而且国家还要制定相应政策和法律来加以保证，才能取得好的效果.

计算机安全的综合性保护机构和措施之间的层次联系可用图 1.2 来加以说明. 从图 1.2 可以看到，具体的保护方法，一方面是由安全技术的研究来实现的；另一方面则是由社会的环境，即人们所确定的某些活动来保证的. 按照层次结构的观点，光是从物理设备上具备有实体安全防护措施，以及利用硬设备进行存取控制和身份鉴别仅是最基本的手段；更进一步是要从逻辑上来进行验证，即使有人利用非法手段突破物理层的保护，在逻辑层还可再次核实其存取数据的合法性以及检查其密钥是否正确等；其三是人事层，在计算机安全保护诸因素中，人是最重要的因素，无论你在物理层和逻辑层设置安全措施有多少，在实施之前，就有可能人为地把输入数据加以改变，因此在组织上保证计算机安全是一项重要而艰巨的任务. 另外，计算机的安全管理也是实现计算机安全保护措施的有力保

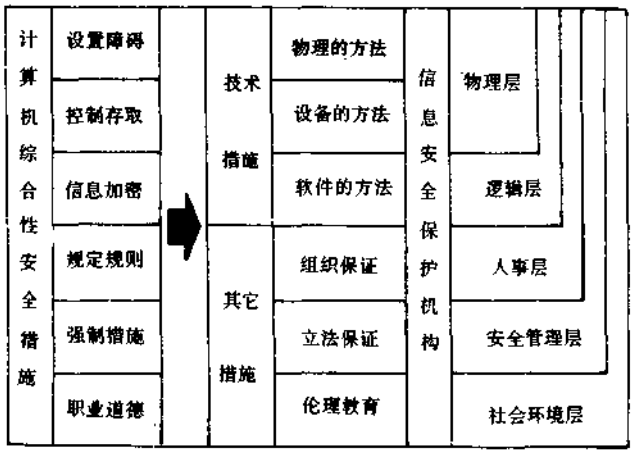


图 1.2 计算机综合性安全系统的层次图

证，从政策制定上、信息保护的法律上给予保证. 最后是对全社会的计算机安全宣传和对专业人员的职业道德教育等，以期全社会都能正确认识和重视这一问题，以形成良好的计算机安全的社会环境.

经过三个阶段的发展，目前计算机安全技术已经成为一门独立的学科. 许多发达国家还设立了专门的计算机安全技术研究机构，以及有关计算机安全管理和监察的机构，对计算机的产品及其安全性能进行论证和鉴定. 例如，美国国防部在 1981 年就成立了计算机安全中心，集中研究国防部在处理敏感信息时，对计算机系统的安全性所要提出的要求，并于 1983 年公布了国防部对可信计算机等级的评审判据. 它是衡量计算机系统自身安全性能、安全等级的一个标准. 这说明，当前国际上的计算机安全技术和产品的发展，已经趋向标准化，做到技术上可以实现，实用上检测有章可循、方便灵活、费用低且安全可靠. 例如，已经颁布实行的标准有：计算机系统安全评价标准 (TEMPEST 标准、DES 标准等)，国际标准化组织还将在近期制定出有关计算机实体安全、身份识别、操作系统安全、安全通讯、安全审计分析以及电磁波辐射控制等若干计算机安全的标准. 其次，大部分的计算机安全系统都采用了系统隔离技术，也就是把用户同系统隔离起来，使其不能直接访问主系统，而要经过存取控制机构识别和鉴定之后才能进行访问，增强了系统的安全性. 计算机安全技术的最新发展是同计算机技术的进步有密切联系的，如人工智能和模式识别技术，也引进到计算机安全领域里来了. 有些国家正在研制安全控制的专家系统，使其在计算机安全方面能发挥更大的作用.

除计算机安全在技术上的不断进步之外，计算机安全管理和立法也在不断完善，许多国家都制定了相应的数据保护法和有关计算机安全的监察条例，从政策上和法律上给计算机安全以保证，并作广泛的社会宣传和进行计算机安全与保密的教育，以形成一个有利于计算机安全的社会环境.

尽管随着计算机应用的深入发展，计算机安全技术得到了长足的进步，但是，就计算机安全保护方面来说，其安全技术还远远落后于计算机应用的发展水平. 技术和行政的安

全管理，法律制度都还不能满足保证计算机安全的需要，并且由于整个社会计算机化所存在的脆弱性，使犯罪分子或集团仍然对要害部门、国家及整个社会都构成严重威胁．特别是信息系统的发展趋势是分布数据库加上网络，并朝着世界性的网络发展，使得信息系统的经济和政治价值日益增大．系统安全某部分一旦出问题，社会就将产生“多米诺骨牌”效应．因此，国际上现在各种形式的计算机安全学术组织活动频繁，就是为了从理论上探索出新的更好的信息保护方法；从实际应用技术上，寻求新的更为安全可靠的技术措施．

在我国，由于计算机的应用尚处于普及发展阶段，所以计算机安全与保密的工作也处在打基础阶段．但鉴于国际上一些计算机技术应用发达的国家中计算机安全方面的经验教训，计算机安全与保密已经引起了我国有关部门的重视，并成立了计算机管理和监察机构，专门对计算机安全问题进行管理和监督，并制定出有关计算机安全的条例和规范，慎重考虑计算机安全问题，避免走别人失败的老路．目前，主要应采用各种方式进行广泛持久的宣传教育，使人们充分认识到计算机信息系统安全的重要性、迫切性和复杂性，同时加强对有关人员的安全技术训练，并进行计算机安全技术的研究工作，使得在计算机应用系统的设计时就能全面考虑其安全性能．目前，我国已成立了专门的计算机安全与保密学术组织，计算机安全问题已受到专家和有关人员的重视．另外，在我国不断完善法律制度的同时，也能提出适合我国实际情况的计算机安全的法规，使建立起有关计算机安全的严密的、科学的行政管理、技术管理、基本技术规范和法律制度，以促进我国计算机安全技术水平迅速赶上国际先进水平．

1.3 计算机安全与保密的立法情况

计算机技术发展如此迅速，应用如此广泛，大大促进了社会的进步和繁荣，也为将来的社会描绘出一幅美好的前景．但是另一方面，由于计算机技术的迅速发展，对现代社会和家庭产生的影响之大，使得计算机和社会之间还来不及相互适应，造成了计算机易受攻击的脆弱性．同时，人们只看到计算机技术发展给人们带来巨大财富和方便的一面，而忽视了计算机的安全与保密这一面，使得一些计算机技术发达国家，计算机犯罪事件不断发生，特别是经济领域，窃取使用计算机的密码口令和身份证，或利用职务之便把伪造的数据输入计算机，从而盗窃大量钱财的案件不断发生．如日本统计，自动付款机犯罪在近十年间增长了 90 倍，仅 1984 年确认的就是 723 例．又如，1973 年曾揭露了美国证券投资公司轰动一时的重大的计算机犯罪案件．这家公司利用计算机系统掩盖亏损，伪造了多达 21 亿美元的假合同，欺骗顾客达十年之久．直到由一名被解雇而心怀不满的职员告发，才真相大白．1978 年，美国太平洋安全银行雇用的电子计算机技术顾问，假借解决技术问题为由，骗取了计算机系统的口令，然后通过银行计算机网将 1020 万美元转到瑞士的苏黎士某银行的一个帐户上，构成了美国历史上计算机犯罪的最大盗窃案．后来，由于罪犯自我炫耀时才露出马脚得以破案．上述案件固然令人咋舌，但比起国家安全和防御所受到的外部威胁，则是小巫见大巫了．

总之，由于计算机技术对社会各方面的渗透，对社会的发展也产生了深刻的影响．首先是在现代社会中，人们对计算机的依赖与日俱增，无论是在政府机关、军事部门，还是在经济、金融机构，以及科学技术研究部门和大型企业集团，都使用了计算机，国家的政治、