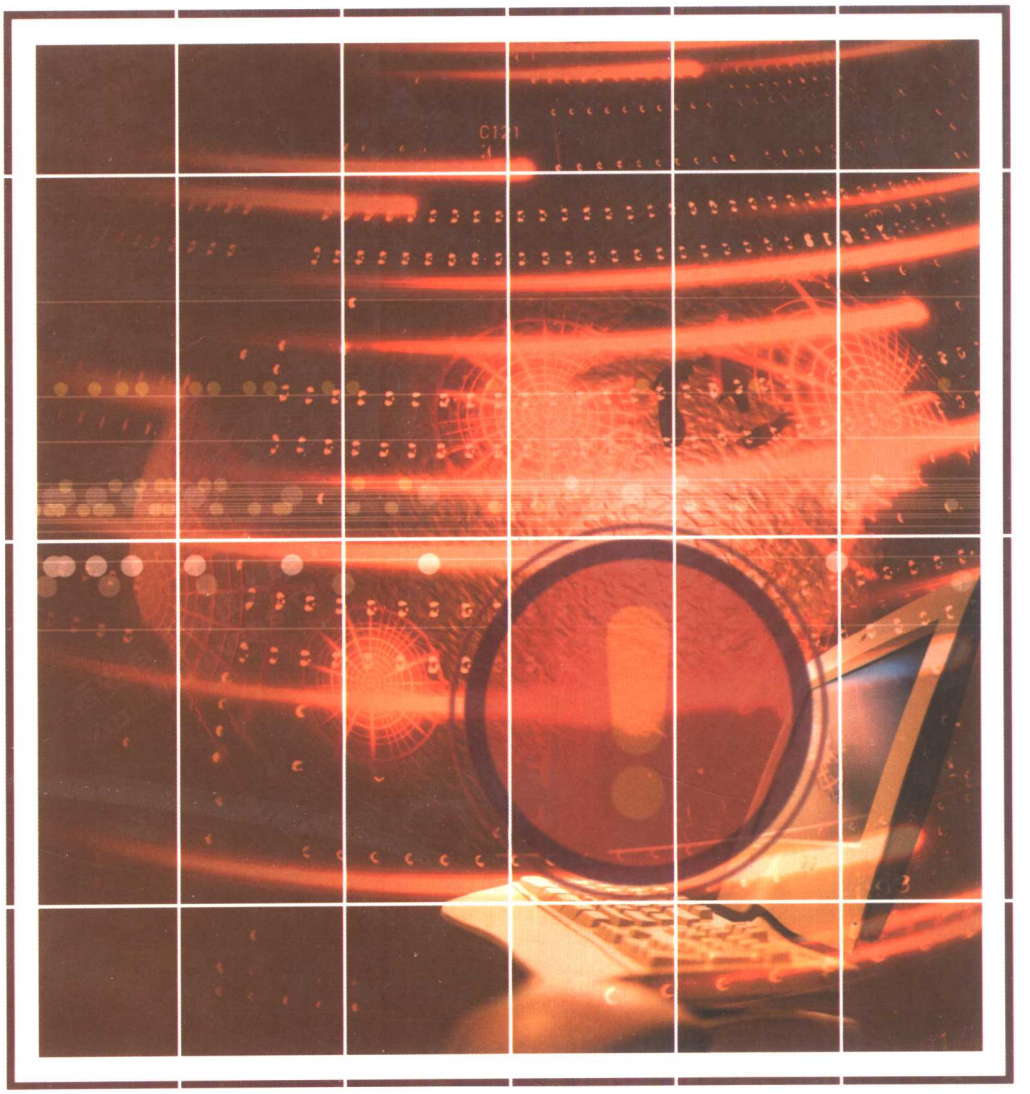
新世纪计算机类本科系列教材



计算机系统安全

马建峰　郭渊博　编著

西安电子科技大学出版社
http://www.xduph.com

新世纪计算机类本科系列教材

计算机系统安全

马建峰　郭渊博　编著

西安电子科技大学出版社

2005

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与通用操作系统保护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以及入侵检测的方法与技术等问题。

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。

图书在版编目(CIP)数据

计算机系统安全/马建峰等编著. —西安：西安电子科技大学出版社，2005.2
(新世纪计算机类本科系列教材)
ISBN 7-5606-1489-2

Ⅰ.计… Ⅱ.马… 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(2005)第 002582 号

策　　划　臧延新
责任编辑　阎　彬　张　友　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　陕西省乾兴印刷厂
版　　次　2005 年 2 月第 1 版　2005 年 2 月第 1 次印刷
开　　本　787 毫米×1092 毫米　1/16　印张 19.5
字　　数　461 千字
印　　数　1～4000 册
定　　价　22.00 元
ISBN 7-5606-1489-2/TP·0791(课)
XDUP 1760001-1

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

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，也就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制裁等。

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，人们在其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，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的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。包括环境、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。包括电源、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，不仅会造成国家财产的重大损失，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。

对信息进行人为的故意破坏或窃取称之为攻击。根据攻击方法的不同，可分为被动攻击和主动攻击两类。

(1) 被动攻击：是指一切窃密的攻击。它在不干扰系统正常工作的情况下侦收、截获、窃取系统信息，以便破译分析；利用观察信息、控制信息的内容来获得目标系统的位置和身份；利用研究机密信息的长度和传递的频度获得信息的性质。被动攻击不容易被用户察觉出来，因此它的攻击持续性和危害性都很大。

被动攻击的主要方法有：

① 直接侦收。利用电磁传感器或隐藏的收发信息设备直接侦收或搭线侦收信息系统的中央处理机、外围设备、终端设备、通信设备或线路上的信息。

② 截获信息。系统及设备在运行时，散射的寄生信号容易被截获。如离计算机显示终端(CRT)百米左右的辐射信息强度可达 30 dB/V 以上，因此可以在那里接收到稳定、清晰可辨的信息图像。此外，短波、超短波、微波和卫星等无线电通信设备有相当大的辐射量，市话线路、长途架空明线等电磁辐射也相当严重，因此可利用系统设备的电磁辐射截获信息。

③ 合法窃取。利用合法用户身份，设法窃取未被授权的信息。例如，在统计数据库中，利用多次查询数据的合法操作，推导出不该了解的机密信息。

④ 破译分析。对于已经加密的机要信息，利用各种破译分析手段，获得机密信息。

⑤ 从遗弃的媒体中分析获取信息。如从信息中心遗弃的打印纸、各种记录和统计报表、窃取或丢失的软盘片中获得有用信息。

(2) 主动攻击：是指篡改信息的攻击。它不仅能窃密，而且还威胁到信息的完整性和可靠性。它以各种各样的方式，有选择地修改、删除、添加、伪造和重排信息内容，造成信息破坏。

主动攻击的主要方法有：

① 窃取并干扰通信线路中的信息。

② 返回渗透。有选择地截获系统中央处理机的通信，然后将伪信息返回系统用户。

③ 线间插入。当合法用户已占用信道，但是终端设备还没有动作时，插入信息进行窃听或信息破坏活动。

④ 非法冒充。采取非常规的方法和手段，窃取合法用户的标识符，冒充合法用户进行窃取或信息破坏。

⑤ 系统人员的窃密和毁坏系统数据、信息的活动等。

有意威胁(攻击)的主要目的有以下几种：

① 企图获得系统中的机密信息，为其国家或组织所利用。

② 企图修改、添加、伪造用户的机密信息，以便从中得到好处。

③ 企图修改、删除或破坏系统中的信息，达到不可告人的目的。

④ 获得任意使用数据通信系统或信息处理系统的自由。

3. 计算机犯罪

计算机犯罪是利用暴力和非暴力形式，故意泄露或破坏系统内的机密信息，危害系统实体和信息安全的不法行为。暴力形式是对计算机设备和设施进行物理破坏，如使用武器摧毁计算机设备，炸毁计算机中心建筑等。而非暴力形式是利用计算机技术及其他技术进

行犯罪活动，它通常采用下列技术手段：

（1）线路窃收：将数据线与计算机通信线相连或搭线窃听。当合法用户发送口令时，捕获口令。

（2）信息捕获：利用窃收器拦截几公里之外的计算机信号。例如，冒充电话公司的修理工进入计算机房，在线路上安装窃收器或在计算机内事先安装窃收器，或利用电磁泄露捕获有用信息。

（3）偷看：进入计算机中心或终端所在区域，观察显示屏上的重要信息，或通过高倍望远镜在附近的建筑物内观察显示屏上的信息。

（4）欺骗：假冒合法用户通过电话向系统管理员询问口令，或通过贿赂手段获取口令，然后侵入系统。使用口令词典，猜中用户的口令，偷窃系统的重要数据和信息。

（5）尾随：紧跟在授权用户之后，通过转动门或其他障碍，绕过物理访问控制措施，入侵系统，实施犯罪。

（6）线间进入：当授权用户吃午饭或进洗手间时，乘机接管一个已注册的终端或 PC 机，对系统信息进行窃取、修改或破坏。

（7）采取手段，扩大授权：利用技术手段，扩大系统的授权，进行非法活功。通常进行扩大授权的内容主要有：在系统屏幕或终端上浏览，延长响应时间，察看存储器的最新使用情况，窃取重要信息等。

（8）人工干预系统：使用实用的人工干预程序，侵犯系统安全，实施犯罪。例如，美国一州立银行计算机操作员利用人工干预程序修改了账号，从一个客户的账目中盗走了12.8万美元。

（9）废品利用：从废弃资料、磁盘、磁带中提取有用信息或进一步分析系统密码等。

（10）伪造证件：伪造他人信用卡、磁卡、存折等。

近些年来出现的计算机犯罪，严重威胁并危害到了信息系统的安全，造成了许多重大损失，已成为严重的社会问题。

计算机犯罪具有以下明显特征：

（1）犯罪方法新。信息系统包括众多的设备和子系统，从而为计算机犯罪提供了较多的目标、途径和方法。其作案的方式主要有逻辑炸弹、特洛伊木马、意大利香肠等。近年来，许多犯罪分子已把先进的电子扫描、电子跟踪等技术用于犯罪活动。这些都是传统犯罪方法所少见的。

（2）作案时间短。传统犯罪时间得花上几分钟、几小时，乃至几天时间来完成，而计算机犯罪只需几分之一秒或几十分之一秒，有的甚至只需几千分之一秒或几万分之一秒就可以完成，速度快，获益高，危害大。这一特征强烈地刺激和诱发着犯罪。

（3）不留痕迹。作案后销证容易，不留痕迹，不容易被人发现，不容易侦破。即便是罪犯正在作案，你可能还认为他正在工作，因此一般难以发现。例如美国的破案率不到10%。

（4）内部工作人员犯罪的比例在增加。外部犯罪和内部犯罪的可能性都很大，特别是系统内部工作人员犯罪的比例在增加。他们熟悉系统的功能，具有娴熟的作案技巧、方法和智谋，同时具有合法身份，有许多便利条件。统计资料表明，在内部人员中，非技术人员犯罪的比例在上升，其中女性的比例在日益增加。

(5) 犯罪区域广。计算机犯罪可以通过终端，甚至通过计算机网搭线或侦听，从远端进行威胁和攻击，因此涉及的范围极广，影响极大。计算机犯罪研究专家帕克(Donn. B. Parker)曾经指出："计算机犯罪是一个世界问题。凡是有计算机的地方，都会发生计算机犯罪，对此我们不能掉以轻心。"

(6) 利用保密制度不健全和存取控制机制不严的漏洞作案。

欲使计算机系统正常运行，必须努力避免各种非人为的灾害，最大限度地抑制和杜绝形形色色的人为危害。

1.1.3 计算机系统的脆弱性

1. 造成不安全因素的原因

造成计算机系统不安全的因素按其原因可分成三类：

(1) 自然灾害构成的威胁，如火灾、水灾、风暴、地震等破坏以及环境(温度、湿度、振动、冲击、污染)的影响。

(2) 偶然和无意构成的威胁，如硬件设备故障、突然断电或电源波动大、测不到的软件错误或缺陷等。

(3) 人为攻击的威胁，如国外间谍窃取机密情报、内部工作人员的非法访问、用户的渎职行为以及利用计算机技术进行犯罪等。

这些不安全因素，如果结合并充分利用计算机系统本身所具有的种种脆弱性，就可能对计算机系统的安全性带来严重威胁。

2. 系统的脆弱性

针对计算机系统的各种攻击之所以能够成功，很关键的原因是计算机系统本身存在着这样或那样的脆弱性，而且这些弱点往往隐藏在计算机系统所具有的优越的特征之中，因此常常会被非授权用户不断利用。攻击者正是以这些弱点作为突破口来发起攻击，从而对计算机系统进行非法访问的。这种非法访问使系统中存储信息的完整性受到威胁，使信息被修改或被破坏而不能继续使用，更为严重的是，系统中有价值的信息被非法篡改、伪造、窃取或删除而不留任何痕迹。然而，若去掉这些弱点，那么计算机系统的好多优点也就不复存在或者大打折扣了。另外，计算机还易受各种自然灾害和各种误操作的破坏。认识计算机系统的这种脆弱性，可以找出有效的措施保证计算机系统的安全。

目前，计算机系统安全存在的问题主要表现在如下几个方面：

(1) 操作系统的脆弱性。操作系统不安全是系统不安全的根本原因。绝大部分的攻击都借助了操作系统本身的漏洞。操作系统的弱点主要表现在以下几个方面：

① 操作系统支持系统集成和扩展的能力给系统自身留下了一个漏洞。操作系统的程序允许进行动态链接，I/O 驱动程序与系统服务都可以用动态链接的方式挂接到操作系统上。这种方法虽然给系统的扩展和升级带来了方便，同时也为"黑客"和计算机病毒的产生打开了方便之门。

② 操作系统支持在网络上传输文件，但上传可执行文件有助于病毒和黑客程序的加载。

③ 操作系统支持创建进程，特别是支持在网络的结点上进行远程进程的创建与激活是不安全的另一原因。被创建的进程还能继承创建进程的权力。将此功能与②结合可以实

现黑客程序的远程安装。

④ 操作系统的守护进程具有与操作系统核心层软件同等的权力；另外，操作系统提供的 Debug 与 Wizard 都是黑客可以利用的程序。

⑤ 操作系统提供的远程过程调用(RPC)服务往往缺乏安全验证功能。

⑥ 操作系统为系统开发人员提供的无口令便捷入口或“后门”，也是黑客可以利用的通道。

(2) 计算机网络的脆弱性。计算机网络本身也给数据带来了安全威胁，Internet 的大面积覆盖和广泛应用使得安全问题变得更加严重。网络带来的安全问题主要表现如下：

① 网络的根本是资源共享，而这些资源本身也能为攻击者所共享。

② 构成网络基本单元的局域网采用的是共享传输介质的广播通道，特别如无线局域网采用空间作为信道，这使得消息截获相对较容易。

③ 网络设备存在各种安全隐患，网络设备不安全就意味着整个网络不安全。

④ TCP/IP 协议的不完善，成为攻击者可利用的漏洞。

⑤ 各种应用软件(FTP、E-mail、Web、CGI 等)的缺陷，为攻击者提供了方便。

(3) 数据库管理系统的脆弱性。由于用户的主要信息是存储在数据库中的，因此数据库的安全性将直接对用户的数据造成影响。数据库管理系统的安全与操作系统的安全类似，软件的设计漏洞、数据具有的共享性以及管理人员配置和操作上的错误都会危及数据的安全。

(4) 计算机本身的不安全因素。计算机系统是一个复杂的系统，其各个环节都可能存在不安全因素。例如：

① 数据输入部分：数据通过输入设备进入系统，输入数据容易被篡改或输入假数据。

② 数据处理部分：数据处理部分的硬件容易被破坏或盗窃，并且容易受电磁干扰或电磁辐射的影响而造成信息泄露。

③ 输出部分：输出信息的设备容易造成信息泄露或被窃取。

④ 存取控制部分：系统的安全存取控制功能还比较薄弱。

(5) 缺少安全管理。目前，绝大多数计算机网络系统在安全管理方面存在以下问题：

① 对安全管理的重视程度存在很大差异，许多部门没有采取足够的安全措施。

② 对安全知识的教育和培训不足，安全设备没有充分发挥作用。

③ 缺少安全管理的技术规范。

④ 没有定期的安全测试与检查，缺乏安全监控。

在没有系统安全链的各个环节中，最薄弱的环节是人。进行系统软、硬件设计的是人，进行系统管理的是人，使用系统的也是人。因此，人是整个安全系统中的决定因素。

1.1.4 计算机危害与其他危害的区别

计算机危害是一种崭新的危害形式，与其他危害相比，其突出的区别是技术性和专业性，且易造成严重的危害，因而被界定为犯罪。计算机犯罪有如下特点：

(1) 高技术智能犯罪。计算机犯罪的直接目标，除了有形的计算机及其运行环境外，更多的是无形的电子数据或计算机信息系统。作案时往往运用计算机技术，作案人不少都是掌握计算机技术、从事计算机工作的。