计算机信息系统安全培训教材

计算机信息系统安全管理与法规相关基础知识

公安部计算机管理监察司编著

群众出版社

计算机信息系统安全培训教材

计算机信息系统安全管理与法规相关基础知识

[redacted]

[redacted]

计算机信息系统安全培训教材

计算机信息系统安全管理与法规相关基础知识

公安部计算机管理监察司　编著

群众出版社
一九九八年·北京

图书在版编目（CIP）数据

安全管理与法律法规相关基础知识/公安部计算机管理监察司编著. -北京：群众出版社，1998
计算机信息系统安全培训教材
ISBN 7-5014-1753-9

Ⅰ.安… Ⅱ.公… Ⅲ.电子计算机-信息系统-安全-法规-中国-教材 Ⅳ.D922.17

中国版本图书馆 CIP 数据核字(98)第 11211 号

计算机信息系统安全培训教材

计算机信息系统安全管理与法规相关基础知识

公安部计算机管理监察司 编著

群众出版社出版、发行 新华书店经销
京安印刷厂印刷
787×1092 毫米 16 开本 9 印张 208 千字
1998 年 6 月第 1 版 1998 年 6 月第 1 次印刷

ISBN 7-5014-1753-9/TP・6 定价：13.50 元
印数：0001—70000 册

序　言

计算机信息系统是国家信息化的重要组成部分。“国家信息化”是指在国家的统一规划和组织下，在农业、工业、科学技术、国防及社会生活各个方面应用现代信息技术，深入开发、广泛利用信息资源，加速实现国家现代化的进程。要确保国家现代化进程的顺利、健康实施，以及国家信息化快、好、省的持续发展，首先要抓好计算机信息系统的安全保护工作。

当前计算机应用已经遍布到社会的方方面面，其安全问题，已经成为社会的公共安全问题。随着计算机应用的进一步的普及与发展，以及计算机信息系统安全问题的日益社会化、严重化，国家有必要运用行政管理杠杆，来进行有效的管理，维护社会的稳定与发展。由公安部主管全国计算机信息系统安全保护工作，是从社会公共安全的角度，加强计算机信息系统的安全保护工作的体现。

抓好计算机信息系统安全保护工作不仅包括加强行政管理、法规制定和安全保护技术的研究，而且还包括加强计算机信息系统安全教育，增强全民族的计算机信息系统安全意识这项重要工作。加强信息安全教育、增强信息安全意识的培养是贯彻《中华人民共和国计算机信息系统安全保护条例》的重要保障，是加强计算机信息系统安全保护的基础。

“计算机信息系统安全培训教材”的编撰发行，作为进行计算机信息系统安全保护培训的统一教材，有助于提高和强化计算机信息系统安全观念和防范意识，促进计算机信息系统安全技术的普及推广。相信该教材在计算机信息系统安全保护的实践中，定能够不断地得到充实、完善和提高。

让我们共同为国家信息化构筑起安全保护的“万里长城”。

（公安部党委委员、部长助理）

编者的话

伴随着我国国民经济信息化进程的推进和信息技术的普及，计算机信息系统的安全显得越来越重要，其中安全教育尤为关键。为适应各地计算机安全培训工作的需要，为各部门、各行业计算机安全提供培训教材，也为各计算机应用单位的领导、计算机从业人员和信息工程人员提供业务学习的读物，公安部计算机管理监察司组织编写了这套计算机信息系统安全培训教材。

全套教材分为三册：《计算机信息系统安全管理与法规相关基础知识》、《计算机信息系统安全技术》和《计算机信息系统安全法规汇编》（修订本）。撰稿人（以姓氏笔画为序）为王春和、王锡林、刘凤昌、张林、张健、张书强、张双桥、罗仁东、段保平、曹隆业、滑建忠。初稿经王锡林、刘凤昌统一修改后，由正、副主编审核定稿。

本套教材在编写过程中，参考了有关的资料和教材。初稿完成后征求了有关部门和专家、领导的意见。卿斯汉、马秋枫、缪道期、崔书昆、吴亚飞、夏锦尧、鹿居正等同志对初稿提出了诸多宝贵的意见，在此一并深表谢意。

计算机信息系统安全是一个正在发展的新领域，许多概念尚在探讨之中。另外，由于时间短促，资料不足，加之我们水平有限，不足之处在所难免，恳请读者指正。

公安部计算机管理监察司

1998 年 2 月 20 日

目　录

第一章　计算机信息系统安全概述

自本世纪40年代计算机在美国诞生以来，计算机应用已逐渐普及社会的各个领域。80年代中、后期，随着计算机网络技术的成熟，计算机网络应用迅速普及，从而宣告了第三次工业革命浪潮的到来。第三次工业革命就是以通过计算机与通信系统实现信息快速传输和共享为标志的信息技术革命。伴随着我国国民经济信息化进程的推进和信息技术的普及，我国各行各业对计算机网络的依赖程度越来越高，这种高度依赖性将使社会变得十分“脆弱”。一旦计算机网络受到攻击，不能正常工作，甚至全部瘫痪时，就会使整个社会陷入危机。尤其Internet应用发展以来，已经涉及到国家安全与主权的重大问题。在为高技术带来巨大经济利益而欣喜的同时，必须居安思危。

安全法规、安全技术和安全管理，是计算机信息系统安全保护的三大组成部分，相辅相成，互补相通。制订法规的根本目的或作用，在于引导、规范及制约社会成员的行为。安全法规以其公正性、权威性、规范性、强制性，成为实施社会计算机安全管理的准绳和依据；有效的计算机安全技术，是确实维护计算机信息系统安全的有力保障。安全保护的直接目标，是保障计算机信息系统的安全。

据国内外大量的调查统计表明，因人为或自然灾害所造成的计算机信息系统的损失中，因管理不善所占的比例高达70%以上。安全法规的贯彻、技术措施的实施都离不开强有力的管理。增强管理意识，强化管理措施，是做好计算机信息系统安全保护工作的有力保障。安全管理的关键因素，是人。

同时，计算机信息系统安全又是动态的。攻击与反攻击、威胁与反威胁是一对永恒的矛盾，水涨船高，安全是相对的，没有一劳永逸的安全防范措施，计算机信息系统安全管理工作必须常抓不懈，警钟常鸣。

信息是人类社会的宝贵资源。功能强大的信息系统，是推动社会发展前进的加速剂和倍增器，它日益成为社会各部门的不可缺少的生产和管理手段。信息与信息系统的安全，已经成为崭新的学术技术领域；信息与信息系统的安全管理，亦已成为社会公共安全工作的重要组成部分。

第一节　计算机信息系统安全概念

为了深刻理解以后计算机信息系统及其安全保护的有关内容，本节首先介绍有关计算机信息系统及其安全的基本概念。

一、计算机信息系统

所谓计算机信息系统是指“由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机

系统”。

信息是客观事物运动状态及运动方式的表征，能使我们由未知变为已知。信息按其内容的有用价值，大体上可分为三类：消息、资料和知识。消息可理解为单条信息的记录，例如报纸上的消息报导；资料可理解为相关信息记录的集合，具有相对较大的参考价值，例如报刊文摘、统计报表；而知识则为在大量资料的基础上，经过分析研究所总结出来的客观规律或法则，这显然是人类文明进步的精华结晶，来之不易，例如论文、论著等。1996 年联合国教科文组织的“信息化与教育”会议，把信息化社会的知识结构，表述为图 1-1-1 所示的知识结构金字塔。

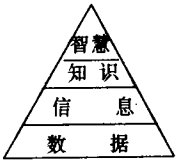

图 1-1-1　知识结构

在这知识结构的金字塔中，数据（Data），是信息的原材料，是一堆数字或符号的总括；信息（Information），是以某种目的组织起来，经加工处理并具有一定结构的数据的总括；知识（Knowledge），是经过整理、分析、评论和验证的信息；智慧（Intelligence），是经历客观现实验证而得到充实的知识，是金字塔的顶端。

计算机系统的出现，是人类历史上相当重要的一次信息革命。它从 1946 年诞生至今，经历了科学计算、过程控制、数据加工、信息处理、人工智能等应用发展过程，功能逐步完善，现已进入普及应用的阶段。

计算机信息系统是一个人机系统，其基本组成是：计算机实体、信息和人。

所谓计算机系统实体，是指计算机系统的硬件部分，应包括计算机本身的硬件和各种接口，也应包含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和线路、信道。

在计算机信息系统中，信息的主要形式有操作系统、数据库、网络功能及各种功能的应用程序。计算机系统实体之有用，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。

计算机信息系统的发展也是有一个过程的。70 年代以来，大体上是计算机网络的开发、应用和发展阶段。网络技术的应用，使得在空间、时间上原先分散、单立的信息，形成为相关密切的庞大的统计信息资源系统，网络资源的共享，无可估量地提高了信息系统中信息的有效使用价值。

90 年代以来，多媒体技术蓬勃发展，这大大地拓宽了计算机系统所处理的信息的范畴，为计算机信息系统在各行各业、包括日常生活领域在内的广泛应用，展现了令人鼓舞的前景。

二、计算机信息系统安全

计算机信息系统安全包括实体安全、信息安全、运行安全和人员的安全等几个部分。人的安全主要是指计算机使用人员的安全意识、法律意识、安全技能等，这在有关安全教

育章节中论述。下面就其他几个方面的内容作简单的说明。

（一）计算机信息系统实体安全

在计算机信息系统中，计算机及其相关的设备、设施（含网络）统称为计算机信息系统的“实体”，“实体安全”是指保护计算机设备、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。实体安全包括环境安全、设备安全和媒体安全三个方面。

对计算机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漏和破坏。因此，对计算机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。

（二）计算机信息系统运行安全

计算机信息系统的运行安全包括：系统风险管理、审计跟踪、备份与恢复、应急四个方面的内容。系统的运行安全是计算机信息系统安全的重要环节，是为保障系统功能的安全实现，提供一套安全措施来保护信息处理过程的安全，其目标是保证系统能连续、正常地运行。

（三）计算机信息系统信息安全

所谓计算机信息系统的信息安全是指防止信息财产被故意的或偶然的非法授权泄漏、更改、破坏或使信息被非法系统辨识、控制。即确保信息的保密性、完整性、可用性、可控性。针对计算机信息系统中信息存在形式和运行特点，则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、加密与鉴别七个方面。

下面的列表，指出了对信息安全构成威胁的一些行为。

·对可用性的威胁

－破坏、损耗或者污染

－否认、拒绝或延迟使用或者访问

·对完整性的威胁

－输入、使用或生成错误数据

－修改、替换或重排序

－歪曲（misrepresent）

－否认（当成不真实的而拒绝）

－误用或没有按要求使用

·对保密性的威胁

－访问

－泄露

－监视或监听

－拷贝

－偷盗

为了帮助读者领会信息安全要素，下面列举了几个信息安全性遭到破坏的案例。

1．可用性遭到破坏。用户的一个数据文件被别有用心的人移到了这个用户的另一个文件子目录中。该计算机用户在运行其应用程序时，由于程序指定的子目录里数据文件已不存在，系统肯定要出错。

在这个事件中，信息的可用性被破坏了，而信息的其他安全性要素都没有遭到破坏，这个数据文件的完整性、保密性在该情况中没有被改变。

2．破坏信息的完整性。一个软件公司为了按期交货，将一个没有包含重要计账控制机制的应用程序提供给了一家客户，而该软件技术说明书里有这个控制机制。客户将该软件用在了生产线上。然而，客户公司里的一名会计发现：这一应用软件中并没有计账控制，该会计利用了这一疏漏并参与了一次巨大的可付帐的公款盗用，客户公司蒙受了巨大的经济损失。

除记帐控制疏漏了之外，软件应用程序如期完成了。然而因为程序是不完善的，该产品缺少了完整性，而不是可靠性。在这种情况中，保密性没有被影响。

3．保密性破坏情况。某用户的一份秘密文件被人拷贝，因而他的秘密被侵犯了。

在保密性的破坏（案例）中，可用性、完整性没有被影响。虽然用户信息的独占性被丢失了，但他仍然掌握和拥有这些信息。

思考题

1．何为信息？计算机信息系统中信息的主要存在形式和运行方式有哪些？

2．计算机信息系统安全保护的概念是什么？

3．计算机信息系统安全保护的直接目标是什么？有哪些内容？

4．试述计算机信息系统安全性的主要目标。

5．有哪些危害计算机信息系统的误用行为？

6．计算机信息系统安全保护的功能行为及其目的有哪些？

第二节　计算机信息系统面临的威胁及其脆弱性

信息社会化与社会的信息化，广为应用的计算机信息系统在推动社会发展前进的同时，也面临着形形色色的威胁和攻击。外因是条件，内因是根据，外因必须通过内因才能起作用。计算机信息系统本身，无论是在存取运行的基本原理上，或者是系统本身的设计、技术、结构、工艺等等方面都存在着亟待完善的缺陷。或者说，计算机信息系统本身的脆弱性，成为了被攻击的目标或利用为有效的攻击途径。这是本节的主要内容。

一、计算机信息系统面临的威胁

计算机信息系统面临的威胁主要来自自然灾害构成的威胁、人为或偶然事故构成的威胁、计算机犯罪的威胁、计算机病毒构成的威胁以及信息战的威胁等几个方面，下面逐一简单介绍。

（一）自然灾害构成的威胁

主要是指火灾、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。

据有关方面调查，我国不少计算机房，没有防震、防火、防水、避雷、防电磁泄漏或干扰等措施，接地系统疏于周到考虑，抵御自然灾害和意外事故的能力较差，事故不断，因断电而设备损坏、数据丢失的现象也屡见不鲜。

（二）人为或偶然事故构成的威胁

常见的事故有：

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，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，电源突然掉电或冲击造成系统信息出错、丢失或破坏。

（三）计算机犯罪的威胁

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中的机密信息，以及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知识及其他技术进行犯罪活动。1997 年 3 月 14 日我国颁布的《中华人民共和国刑法》对计算机犯罪作了明确的定义，从新刑法的描述看计算机犯罪有两类形式，一是利用计算机技术知识进行犯罪活动（见《刑法》第二百八十七条），计算机信息系统被作为犯罪的工具，如同枪支、交通工具一样。另一类是针对计算机信息系统的犯罪（见《刑法》第二百八十五条、第二百八十六条），这种犯罪行为是将计算机信息系统作为犯罪的对象。

1．计算机犯罪的类型。人为地利用计算机实施危害及犯罪活动，始于 60 年代末，70 年代迅速增长，80 年代形成威胁，成为发达国家和发展中国家不得不予以关注的社会公共安全问题。主要的犯罪形式有：

（1）计算机滥用。

（2）非法入侵计算机信息系统。利用窃取口令等手段，渗入计算机系统，用以干扰、篡改、窃取或破坏。

（3）利用计算机传播反动和色情等有害信息。

（4）侵权。主要是针对电子出版物和计算机软件。

（5）利用计算机实施贪污、盗窃、诈骗和金融犯罪等活动。

（6）破坏计算机系统。

2．计算机违法犯罪的特点及发展趋势。计算机犯罪通常采用下列技术手段：

（1）数据欺骗：非法篡改数据或输入假数据。

（2）特洛伊木马术：非法装入秘密指令或程序，由计算机实施犯罪活动。

（3）香肠术：利用计算机从金融信息系统中一点一点地窃取存款，如窃取各户头上的利息尾数，积少成多。

（4）逻辑炸弹：输入犯罪指令，以便在指定的时间或条件下抹除数据文件或破坏系统的功能。

（5）陷阱术：采用程序中为便于调试、修改或扩充功能而特设的断点，插入犯罪指令或在硬件中相应地方增设供犯罪用的装置。总之，是利用计算机硬、软件的某些断点或接口插入犯罪指令或装置。

（6）寄生术：用某种方式紧跟享有特权的用户打入系统或在系统中装入“寄生虫”。

（7）超级冲杀：用共享程序突破系统防护，进行非法存取或破坏数据及系统功能。

（8）异步攻击：将犯罪指令掺杂在正常作业程序中，以获取数据文件。

（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。

3．计算机犯罪与传统的犯罪行为相比有如下特点：

(1) 危害巨大，发生率的上升势头前所未有。据有关方面统计，由于计算机犯罪而遭受的损失，目前美国每年超过百亿美元；联邦德国约 50 亿美元；英国约 30 亿；法国约 100 亿法朗。

我国的计算机犯罪，近几年发展也很快，上升幅度也较大。

(2) 危害领域不断扩大。当初，危害领域主要是金融系统。现在，则已发展到邮电、科研、卫生、生产等几乎所有使用计算机的领域。受害的，往往是整个地区、行业系统、社会或国家，以致被称为公害。

(3) 计算机违法犯罪社会化。原先，主要是内部计算机专业技术人员作案；现在，则是非计算机专业技术人员和熟悉部门业务及其他外部人员作案增多。作案过程中，也并非完全使用高技术手段，且多为内外勾结，共谋作案。

(4) 计算机危害的国际化。过去作案，主要在一个国家内；现在，则通过国际联网或计算机技术产品和媒体等，跨国作案，成功率很高，屡见不鲜，势头看增。

(5) 危害目的多样化。计算机信息系统，已日益成为各个行业系统、各个地区国家的核心机密的集散部位。信息系统运行的正常与干扰，信息的保护与窃取，历来是异常激烈的看不见的战线。以前作案，多以获取钱财为目的；现在，各政治经济集团、敌对势力之间，则纷纷利用各种计算机危害手段，来达到各自的目的。国外甚至有人声称，计算机战争的威胁，远比核武器的大，包括计算机病毒在内的各种危害手段，正受到国外军方与日俱增的高度重视。

(6) 计算机犯罪者年轻化，转化为恶性案件的增多。

(7) 危害手段更趋隐蔽复杂。

(8) 能不留痕迹地瞬间作案。

计算机犯罪的高技术，使许多犯罪的实施，可在瞬间完成，往往不留痕迹。现有的规章制度、法规和不少人的观念，难以对他们进行制约、界定和制裁。这也是计算机危害日趋严重的重要原因之一。因此，法规的制定刻不容缓，安全管理必须加强，安全技术措施应当跟上，计算机安全教育和职业道德教育势在必上，这已成为国内外专家学者、有识之士及深受其害的广大用户的共识。

(四) 计算机病毒对计算机信息系统构成的威胁

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

计算机病毒是通过连接来扩散的。计算机病毒就像其他程序一样是一种计算机程序，因为这些程序的很多特征是模仿疾病病毒，所以我们使用“病毒”一词。这些特征包括潜伏与自我复制能力。计算机病毒程序把自己附着在其他程序上，等这些程序运行时，病毒进入到系统中。再是扩散能力，第三是制造损害，一台计算机感染上病毒后，轻则系统运行效率下降，部分文件丢失，重则造成系统死机。正是因为计算机病毒有如此大的危害性，恐怖主义者用计算机病毒制造破坏，一些国家的军事和国家安全部门将计算机病毒作为重要的信息战武器来研究。

研制、传播计算机病毒的客观效果，是危害或破坏计算机系统的资源，中断或干扰计

算机系统的正常运行。计算机病毒是危害计算机的最新手段，防不胜防。

据不完全统计，美国在1988年里，约有9万台计算机被病毒感染；仅在11月份里，病毒感染造成的损失就超过了1亿美元。

一份市场调查报告表明，当前我国约有90%的局域网用户，曾遭到病毒的侵袭，其中的大部分因此而受到损失，这比西方国家的约50%的病毒感染率要高出了许多。例如1996年夏，武汉证券机构的Net Ware网络环境，因“夜贼”（Byrglar）DOS型病毒的侵袭，病毒首先影响了双向卫星通信，接着造成网络瘫痪，使得当天的直接经济损失就达500多万元。

病毒的泛滥危害，已是公认的危害社会的一大公害，这在一定的意义上，揭示了计算机系统本身及其社会环境在安全方面的薄弱环节。

（五）信息战的严重威胁

所谓的信息战，就是为了国家的军事战略而取得信息优势，并干扰敌方的信息和信息系统，同时保卫自己的信息和信息系统所采取的行动。这种对抗形式的目标在于，不是集中打击敌方的人员或战斗技术装备，而是集中打击敌方的计算机信息系统，瘫痪其神经中枢似的指挥系统。

某些发达国家已经指望，借助现代信息技术，作为信息武器，成为对敌方施加军事、政治压力的有力手段，把恫吓的概念，提高到一个崭新的水平，在枪响之前就能取得胜利。信息技术将根本改变进行战争的方法，就像坦克的运用引起了第一次世界大战战争艺术的变革一样。继原子武器、生物武器、化学武器之后，信息武器已被列为第四类战略武器。据有关媒介报导，发达国家，特别是美国，每年用于信息安全研究的费用高达150亿美元。在其军队中，已经有了毕业于美国国防大学的以信息战为主要职业的军官。

信息武器大体分三类：

1．具有特定骚扰或破坏功能的功能程序。计算机病毒就是典型的例子，这大概是某超级大国国防部高价征集高性能病毒的原因。

2．具有扰乱或迷惑性能的数据信号。

3．具有针对性信息擦除或干扰运行的噪声信号。

在海湾战争中，作为信息武器用于实战的首例，伊拉克的指挥系统就吃了美国的大亏，仅仅是在伊拉克购买的智能打印机中，塞进一片带有病毒的集成电路芯片，加上其他的因素，最终导致系统崩溃，指挥失灵，几十万人被几万人俘虏。美国的维和部队，还利用国际卫星组织的全球计算机网络，为其建立军事目的的全球数据电视系统服务。在波黑，也成了美国信息战的试验场。

二、计算机信息系统受到的攻击

以上从五个主要方面介绍了计算机信息系统所面临的威胁。对信息的人为故意威胁称之为攻击。以下介绍的就是计算机信息系统被攻击的主要方式和方法。

（一）威胁和攻击的对象

按被威胁和攻击的对象划分，可分为两类：一类是对计算机信息系统实体的威胁和攻击；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漏、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漏和破坏。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．对信息的威胁和攻击。对信息的威胁和攻击主要有两种：一种是信息的泄漏；另一种是信息的破坏。

（1）信息泄漏。所谓信息泄漏，就是偶然地或故意地获得（侦收、截获、窃取或分析破译）目标系统中信息，特别是敏感信息，造成泄漏事件。

（2）信息破坏。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，使得系统的信息被修改、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。

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不合法地使用；

④修改或非法复制系统中的数据。

信息破坏方面的例子屡见不鲜，造成的损失是很大的，例如，1987 年 1 月 1 日，美国马萨诸塞州技术学院一学生在使用 PDP 一 11 计算机时，联入了政府机构的数据网。该网与麻省理工学院的计算机相联，使得该生侵入到政府的几个信息系统中，非法复制了北美战略防空司令部和美国空军司令部的大量机密信息，并造成政府数据网阻塞，导致系统崩溃。

（二）主动攻击与被动攻击

就攻击的方式而言，可归纳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。它是在不干扰系统正常工作的情况下进行侦收、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设置、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，辐射信息强度可达 30DBUV 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面，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。它不仅是窃密，而且威胁到信息的完整性和可靠性。它是以各种各样的方式，有选择地修改、删除、添加、伪造和复制信息内容，造成信息破坏。

主动攻击的主要方法有：

(1) 窃取并干扰通信线中的信息。

(2) 返回渗透。有选择地截取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而终端设备还没有动作时，插入信道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。

三、计算机信息系统的脆弱性

如上所述，计算机信息系统面临着种种威胁，而计算机系统本身因为存在着一些脆弱性，抵御攻击的能力很弱，自身的一些缺陷常被非授权用户不断利用。这种非法访问使系统中存储的信息完整性受到威胁，使信息被修改或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；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。

(一) 信息处理环节中存在的不安全因素

计算机信息系统的脆弱性可从几个角度来分析。首先从信息处理的各个环节看，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自电磁辐射而造成信息泄漏。

3. 数据传输。通信线路上的信息容易被截获，线路容易被破坏或盗窃。

4. 软件。操作系统、数据库系统和程序容易被修改或破坏。

5. 输出部分。输出信息的设备容易造成信息泄漏或被窃取。

6. 存取控制部分。系统的安全存取控制功能还比较薄弱。

(二) 计算机信息系统自身的脆弱性

从计算机信息系统自身的体系结构方面分析，也存在着先天的不足，而这些缺陷在短时间内是无法解决的。其中包括：

1. 计算机操作系统的脆弱性。计算机操作系统的不安全是信息系统不安全的重要原

因。

（1）操作系统不安全的首要原因是操作系统结构体制造成的，操作系统的程序是可以动态连接的，包括 I/O 的驱动程序与系统服务，都可以用打补丁的方式进行动态连接。虽然做这些操作需要被授予特权。许多 UNIX 操作系统的版本进化开发，都是采用打补丁的方式进行开发的。这种方法厂商可用，“黑客”也可用。这种动态连接也是计算机病毒产生的环境。一个靠渗透与打补丁开发的操作系统是不可能从根本上解决安全问题的。然而，操作系统支持程序动态连接与数据动态交换是现代系统集成和系统扩展的需要，很显然，系统集成与系统安全是矛盾的。

（2）操作系统支持在网络上传输文件，包括可以执行的文件映象，即在网络上加载程序。

（3）操作系统不安全的原因还在于可以创建进程，甚至支持在网络的结点上进行远程进程的创建与激活，更为重要的是被创建的进程还继承创建进程的权力。本条与上一条结合起来，构成在远程服务器上安装“间谍”软件的条件。再加上第一条，还可以把这种“间谍”软件以打补丁的方式打在一个合法的用户上，尤其打在一个特权用户上，可以做到系统进程与作业的监视程序都看不到它的存在。

（4）操作系统通常都提供 DAEMON 的软件，这种软件实际上都是一些系统进程，它们总在等待一些条件的出现，一旦条件出现，程序便可以运行下去。这些软件通常都是“黑客”利用的手段。问题不在于有没有 DAEMON，而在于这种 DAEMON 在 UNIX、WINDOWSNT 操作系统上具有与其他操作系统核心层软件同等的权力。

（5）操作系统提供远程过程调用（RPC）服务。操作系统提供 NFS 服务。NFS 系统是基于 RPC 网络文件系统的。

（6）操作系统的 Debug 与 Wizard。许多搞系统软件的人员，他们的基本技能就是 patching + 系统 Debug，有了这两样技术，几乎可以搞“黑客”的所有事情。

（7）操作系统安排的无口令人口，实际上它是为系统开发人员提供的便捷入口。另外，操作系系统还有隐蔽信道。

（8）其他。

2. 计算机网络系统的脆弱性。ISO7498 网络协议形成的当初，基本上就没有顾及到安全的问题，只是后来，才加进了五种安全服务和八种安全机制，形成了 ISO7498 - 2 开放系统互联安全体系结构。

国际互联网的 TCP/IP 也存在着类似的问题。

网络层 IP 对来自物理层的数据包，并没有对发送顺序和内容是否正确进行必要的确认，因此，IP 数据包是不可靠的。

高层的 TCP 和 UDP 服务在接收数据包时，通常总是默认数据包中的源地址是有效的，这给源主机造成了能够随意填写冒名顶替的机会。

UDP 与 TCP 位于同一层，它对包顺序的错误不作修正，对包丢失也不要求重传，而 UDP 又没有建立初始化的连接，因此，UDP 包更容易受到欺骗。

由于 Internet/intranet 出现，网络的安全问题更加严重。可以说，TCP/IP 协议的网络提供的 FTP、TELNET、E - MAIL、NFS、RPC 等都包含许多不安全的因素，存在着许多漏洞。