计算机安全技术

沈学利　张美金　刘玉珍　编著

NEUPRESS
东北大学出版社

计算机安全技术

沈学利　张美金　刘玉珍　编著

东北大学出版社

内容简介

本书从我国实际情况出发，结合高等学校教学的实际情况，简明扼要地介绍了计算机系统的环境安全、实体安全、软件安全技术、计算机病毒分析与防治、操作系统的安全、密码技术、数据库的安全、网络安全、运行安全等内容。

该书适合于作为大中专院校计算机科学与技术、信息工程、经济信息管理等专业的教材，也可作为计算机系统的开发、使用、维护及管理人员的相关培训教材或参考书。

图书在版编目(CIP)数据

计算机安全技术/沈学利，张美金，刘玉珍编著．—沈阳：东北大学出版社，2002.8

ISBN 7-81054-499-3

Ⅰ.计… Ⅱ.①沈… ②张… ③刘… Ⅲ.电子计算机-安全技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2002)第 057077 号

出 版 者：东北大学出版社
（邮编：110004 地址：沈阳市和平区文化路 3 号巷 11 号）
出 版 人：李鎏兴
印 刷 者：沈阳农业大学印刷厂
发 行 者：东北大学出版社
开 本：787mm×1092mm 1/16
字 数：500 千字
印 张：19.25
出版时间：2002 年 8 月第 1 版
印刷时间：2002 年 8 月第 1 次印刷
责任编辑：王兆元
责任出版：杨华宁
封面设计：唐敏智

定 价：29.50 元

垂询电话：024—83680267（社务办） 024—83680265（传 真）
83687331（市场部） 83687332（出版部）
E-mail：neuph@neupress.com WebSite：http://www.neupress.com

前　言

在当今信息社会中，随着计算机和 Internet 的应用领域不断扩大和深入，计算机病毒也在不断产生和传播，计算机网络不断地被非法入侵，造成的损失非常巨大。因此，计算机系统的安全已成为人们十分关切的重要课题。

对计算机系统的威胁和攻击主要有两类：一类是对计算机系统实体的威胁和攻击，另一类是对信息的威胁和攻击。计算机系统实体所面临的威胁和攻击主要指各种自然灾害、场地和环境因素的影响、战争破坏和损失、设备故障、人为破坏、各种媒体设备的损坏和丢失。对实体的威胁和攻击，不仅造成国家财产的严重损失，而且会造成信息的泄露和破坏。因此，对计算机系统实体的安全保护是防止对信息威胁和攻击的有力措施。对信息的威胁和攻击，主要有两种方式：一是信息泄漏，二是信息破坏。信息泄漏是指故意或偶然地侦收、截获、窃取、分析、收集系统中的信息，特别是机密信息和敏感信息，造成泄密事件。信息的破坏是指由于偶然事故或人为因素破坏信息的完整性、正确性和可用性，如各种硬、软件的偶然故障、环境和自然因素的影响以及操作失误造成的信息破坏，尤其是计算机黑客和计算机病毒造成信息的修改、删除或破坏，使系统资源被盗、被非法使用或使系统瘫痪。为了保证计算机系统的安全性，必须系统、深入地研究计算机系统的安全技术与方法。

目前，国内计算机安全方面的书籍大多从某个侧面介绍计算机系统的安全技术，或者是纯理论的阐述，缺乏实用性。为了解决教学急需，我们参阅大量国内外文献资料，在多年教学与科研实践的基础上编写了此书，旨在使计算机系统的开发、使用、维护及管理人员和大中专院校计算机科学技术专业、信息工程专业和经济信息管理专业的师生重视计算机系统的安全问题，更多地了解和掌握这门学科的基本原理、方法、技术和工具，了解本学科研究的范围和内容，使自己开发、使用、维护和管理的信息系统更加安全、可靠。

全书共分 10 章，比较全面、系统地介绍了计算机系统的安全概论、环境安全、实体安全、软件安全技术、计算机病毒分析与防治、操作系统的安全、密码技术、数据库的安全、网络安全、运行安全等内容。本书内容广泛，深入浅出，简明实用。

本书第 1，2，3 章及第 4 章的 1～3 节由张美金编写；第 5，7，9 章由沈学利编写；第 4 章的 4～7 节及第 6，8，10 章由刘玉珍编写。全部书稿由辽宁工程技术大学电子与信息工程系孙劲光教授审阅。

由于编写时间仓促，编著者水平所限，书中一定会有诸多不当之处，敬请各位读者批评指正。书中引用了同行们的一些研究成果，在此表示深深的谢意，同时向对本书的编写和出版给予支持、帮助的领导和同事表示感谢。

编著者

2002 年 5 月

目　　录

第1章 绪 论

1.1 计算机系统面临的威胁和攻击

随着科学技术的不断发展，人类已进入了信息化社会。面对信息化社会汪洋大海般的信息，信息系统已成为信息处理必不可少的强有力工具。所谓信息系统，是指由人、机和软件组成的，能自动进行信息收集、传输、存储、加工处理、分发和利用的系统。它由实体和信息两大部分组成。实体是指实施信息收集、传输、存储、加工处理、分发和利用的计算机及其外部设备和网络；信息是指存储于计算机及其外部设备上的程序和数据。由于计算机系统涉及到有关国家安全的政治、经济和军事情况以及一些工商企业单位与私人的机密及敏感信息，因此它已成为国家和某些部门的宝贵财富，同时也成为敌对国家和组织以及一些非法用户、别有用心者威胁和攻击的主要对象。所以，计算机系统的安全越来越受到人们的广泛重视。

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。

1.1.1 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。这些因素所造成的损失姑且不论，单就设备故障所造成的损失已令人们触目惊心。

• 1962 年 6 月，美国宇航局发往金星的宇宙探测器“水手 1 号”，由于计算机系统的一个故障，在其发射后不久就坠毁了，数亿美元的设备顷刻间化为灰烬。

• 1979 年，新西兰航空公司的一架客机，因计算机控制的飞行系统出错而撞在 Erebus 山上，机上 257 名乘客和机组人员全部遇难身亡。

• 在英阿马岛战争中，英国一艘驱逐舰因舰上计算机控制的防御系统出故障，将飞来的导弹误认为是友军武器，没有将它击落，结果被导弹击沉。

• 1980 年 6 月 2 日，北美战略防空司令部因计算机中的一个元件故障，误发“苏联发起核进攻”的战争警报，造成北美战略防空司令部和美国国防部的极大惊慌。

• 1981 年 7 月 4 日，日本兵库县川门崎重工公司因计算机发生故障，而发生机器人杀人的事件。

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。

1.1.2 对信息的威胁和攻击

对信息的威胁和攻击主要有两种：一种是信息的泄露，另一种是信息的破坏。

1. 信息泄露

所谓信息泄露，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，造成泄露事件。信息泄露的事件是很多的，兹举例如下。

• 1988 年，德国汉诺威大学计算机系 24 岁的学生马蒂亚斯·斯佩尔将自己的计算机同美国军方和军工承包商的 30 台计算机进行网络连接，在两年时间内收集了美国国防部的大量机密信息。其中有美国"星球大战"计划、北美战略防空司令部核武器和通信卫星等方面的资料，震惊了美国国防部和联邦调查局。

• 1989 年 10 月，英国一个名叫哈卡的青年利用截获的泄漏电磁波取得的密码进行计算机犯罪，给社会带来极大震动。

• 1990 年 1 月 19 日，美国三名工作人员利用政府的计算机窃取军事机密情报，窃取了大量军事文件和联邦调查局关于菲律宾总统马科斯及其密友的敏感信息。

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，造成大量信息丢失或被破坏、修改。

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。

偶然事故有以下几种可能：

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，造成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。

信息破坏方面的例子屡见不鲜，造成的损失是很大的。

• 1970 年，在牙买加的昆斯，5 名诈骗犯利用计算机把存储的支票非法修改为现金存储，获得了现金取回权，诈取北美国家银行现金 90 万美元。那张无价值的支票原存在纽约一家银行，等银行弄清楚后，现金已被提取。

• 1987 年 1 月 1 日，美国马萨诸塞州技术学院一名学生在使用 PDP-11 计算机时，连入了政府机构的数据网。该网与麻省理工学院的计算机相连，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。

• 1989 年，一个名叫哈巴特的青年利用计算机窃取了美国军用部门和电报电话公司贝尔实验室人工智能软件，价值 120 万美元。另外，还破坏了电报电话公司的文件，造成 17.4 万美元的经济损失。

对信息的人为故意威胁称之为攻击。就攻击的方法而言，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位置、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 30dBV 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,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:

- 企图获得系统中的机密信息,为其他国家或组织所利用。
- 企图修改、添加、伪造用户的机密信息,以便从中得到好处。
- 企图修改、删除或破坏系统中信息,达到不可告人的目的。
- 获得任意使用数据通信系统或信息处理系统的自由。

1.1.3 计算机犯罪

1. 计算机犯罪的手段

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。它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) 特洛伊木马技术。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儿一点儿地窃取存款,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。

近二十年来出现的计算机犯罪,严重地威胁和危害到信息系统的安全,造成许多重大损失,现已成为严重的社会问题。下面,仅从有关资料上反映的部分案例,说明计算机犯罪所造成的经济损失。

美国:

• 1973 年,纽约联合迪梅储蓄所的一名出纳员用银行计算机篡改账目,从该银行储蓄中非法窃取 150 万美元。为了不被人察觉,他又在计算机中输入了假信息。

• 1980 年 3 月 17 日,马萨诸塞州配给中心的一名计算机操作员利用计算机掩盖一起 100 万美元的药物盗窃案。

• 1985 年 2 月 25 日,布鲁克大学医院的一名系统分析员将一份价值 30 万美元的 IBM 公司的病人管理信息系统非法复制,转卖给费城一家医疗中心。

• 平准基金保险公司有人利用计算机制造假保险案,诈骗 2700 万美元;太平洋安全银行计算机顾问利用计算机盗领 1000 万美元;艾克森石油公司计算机操作员窃取 2000 万美元的石油;某股票经纪人利用计算机假造资料,骗取了 300 万美元;新泽西州一家银行被人从计算机中窃取 12.8 万美元。

德国:

• 1985 年 5 月,前联邦德国的四名罪犯利用计算机改变信用卡上的磁带密码,骗取了 10 万马克。

哥伦比亚:

• 1983 年 5 月 12 日,哥伦比亚中央银行一名犯罪分子,利用计算机将 1350 万美元几经周折从该银行转移到巴拿马的一家银行,后来又将这笔款转移到欧洲。

日本:

• 三和银行计算机操作员与外部人员勾结,假造存款 1.8 亿日元,并非法提取了 1.3 亿日元。

中国:

• 香港税务局一名职员利用计算机资料制造假储税券,骗取公款 20 万港币。

• 1988 年,某市银行营业部一名微机操作员利用职务之便制造假账户,趁晚上机房无人之机,利用计算机向假账户输入 87 万元,并修改程序,使总账虚平。

• 1989年,某市支行储蓄所微机管理员利用自己知道终端操作员密码之便,在机内凭空开设一假账户,将某一用户的3万元作销户处理,转入自己的账上,又篡改自己活期账户余额。两起作案,从该储蓄所共盗领资金9万元。

据统计,目前全世界每年被计算机犯罪盗走的资金达200多亿美元,其中美国、德国各50亿美元,英国25亿英镑,法国100亿法郎。美国平均每起案件损失45万美元。计算机犯罪的损失金额是常规犯罪的几十倍到几百倍。日本的计算机犯罪也在成倍地增长。

2. 计算机犯罪的特征

计算机犯罪具有以下明显特征。

(1) 犯罪方法新。由于信息系统包括众多的设备和子系统,它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、电子跟踪等技术用来进行犯罪活动。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或几十分之一秒,有的甚至几千分之一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,你还认为他在工作,一般难以发现。美国对计算机犯罪的破案率不到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,甚至通过计算机网络搭线或侦听,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。

1.1.4 计算机病毒

计算机病毒是利用程序干扰或破坏系统正常工作的一种手段,它的产生和蔓延给信息系统的可靠性和安全性带来严重威胁和巨大的损失。自美国1989年首先发现计算机病毒以来,世界上许多国家和地区都发生了计算机病毒的侵扰,我国也不例外。据不完全统计,至今已发现了5000多种计算机病毒,每年造成的损失超过10亿美元。仅1989年一年,美国就有9万台计算机受病毒感染,仅11月份一个月就造成1亿多美元的损失。实践表明,计算机病毒已成为威胁计算机及信息系统安全的最危险的因素。这些病毒,有的只干扰屏幕,有的则封锁键盘或打印机,有的修改或破坏硬盘、软盘上的数据,有的封锁软盘驱动器,有的破坏磁盘的引导扇区、硬盘引导扇区和文件分配表,有的驻留内存、修改中断向量表或格式化硬盘,有的则大量占用磁盘空间,降低系统运行效率或使系统瘫痪。计算机病毒的发展和蔓延,造成许多恶性事件,使国家和人民深受其害。

• 1989年,美国军方一架由计算机控制的隐形战斗机,由于受计算机病毒的攻击而坠毁,造成重大损失。

• 1987 年 12 月，美国 IBM 公司邮电通信网中的数万台计算机因感染圣诞树"蠕虫"病毒而瘫痪，35 万台终端因被圣诞树"蠕虫"病毒堵塞而被迫关闭。

• 1988 年 11 月 2 日，美国康奈尔大学计算机系研究生罗伯特·莫里斯的一项病毒程序试验，竟使美国国防部远景规划署的 ARPANET 网上的 6000 多台电子计算机突然停止工作。该网连接着全国 300 所大学、研究中心、军事基地和国防部科研机构及私人公司，东起麻省理工学院、哈佛大学、马里兰海军实验室，西到加利福尼亚大学、斯坦福大学国家研究所以及费古尼亚的太空总署研究中心和兰德研究中心。整个网络瘫痪了 24 个小时，造成的直接经济损失接近 1000 万美元。

有人预言，今后在现代化战争中可以利用传染病毒来破坏对方的军事指挥通信系统，使其处于瘫痪状态。因而，对计算机病毒的危害决不能掉以轻心。

大量事实表明，来自内部的和外部的威胁和攻击，已成为计算机系统发展和应用的极大障碍，成为一个亟待解决的社会问题，必须深入研究并采取切实措施。

1.2 计算机系统的脆弱性

计算机系统本身因为存在着一些脆弱性，常被非授权用户不断利用。他们对计算机系统进行非法访问，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。

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。兹举例说明。

• 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。

• 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因电磁辐射而造成信息泄露。

• 通信线路：通信线路上的信息容易被截获，线路容易被破坏或盗窃。

• 软件：操作系统、数据库系统和程序容易被修改或破坏。

• 输出部分：输出信息的设备容易造成信息泄露或被窃取。

• 存取控制部分：系统的安全存取控制功能还比较薄弱。

不安全因素按其造成的原因可分成三类：

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 偶然无意构成的威胁。如硬件设备故障、突然断电或电源波动大、检测不到的软件错误或缺陷。

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，使计算机系统表现出种种脆弱性。

计算机系统的脆弱性主要表现在 以下几个方面。

1. 存储密度高

在一张磁盘或一条磁带中可以存储大量信息，而一块软盘很容易放在口袋中带走。这些存储介质也很容易受到意外损坏。不管哪种情况，都会造成大量信息的丢失。

2. 数据可访问性

数据信息可以很容易地被拷贝下来而不留任何痕迹。一台远程终端上的用户可以通过计算机网络连到信息中心的计算机上。在一定条件下,终端用户可以访问到系统中的所有数据,并可以按他的需要将其拷贝、删改或破坏掉。

3. 信息聚生性

当信息以分离的小块形式出现时,它的价值往往不大,但当将大量相关信息聚集在一起时,则显出它的重要性。信息系统的特点之一,就是能将大量信息收集在一起,进行自动、高效的处理,产生很有价值的结果。信息的这种聚生性与其安全密切相关。

4. 保密困难性

计算机系统内的数据都是可用的,尽管可以利用许多方法在软件内设置一些关卡,但对一个熟悉的人来说,下些功夫就可能突破这些关卡,因此要保密很困难。

5. 介质的剩磁效应

存储介质中的信息有时是擦除不干净或不能完擦除掉的,会留下可读信息的痕迹,一旦被利用,就会泄密。另外,在大多数的信息系统中,删除文件仅仅是将文件的文件名删除,并相应地释放存储空间,而文件的真正内容还原封不动地保留在存储介质上。利用这一特性,可以窃取机密信息。

6. 电磁泄漏性

计算机设备工作时能够辐射出电磁波,任何人都可以借助仪器设备在一定的范围内收到它,尤其是利用高灵敏度仪器可以清晰地看到计算机正在处理的机密信息。

7. 通信网络的弱点

连接信息系统的通信网络有不少弱点:通过未受保护的外部线路可以从外界访问到系统内部的数据;通信线路和网络可能被搭线窃听或破坏。这种威胁增加了通信和网络的不安全性。

计算机系统的这些脆弱性对系统安全构成了潜在的危险。这些脆弱性如果被利用,系统的资源就会受到很大损失。

1.3 影响计算机系统安全的因素

1.3.1 计算机系统安全的重要性

计算机系统的安全之所以重要,其原因在于:

① 计算机系统的重要应用成为威胁和攻击的目标。因为计算机系统存储和处理有关国家安全的政治、经济、军事情况及一些部门、组织的机密信息或个人的敏感信息,因此成为国外敌对国家情报部门和一些组织或个人威胁和攻击的目标。

② 计算机系统本身的脆弱性成为不安全的内在因素。由于计算机系统本身的脆弱性以及硬件和软件的开放性,加之缺乏完善的安全措施,容易给犯罪分子以可乘之机。

③ 随着计算机功能的日益完善和运行速度的不断提高,其系统组成越来越复杂,规模也越来越庞大,所用元器件数量不断增加,装配密度日益加大,其本身存在的隐患就成为不安全因素。另外,随着计算机网络的迅速发展,而且越来越大,更增加了隐患和被攻击的区域及环节。

④ 随着应用的需要，计算机使用的场所逐渐从条件优越的机房转向工业场地、野外、海上、天空、宇宙、核辐射环境，其气候、力学、电磁和辐射等环境条件都比机房恶劣，导致计算机出错概率和故障的增加，其可靠性和安全性便受到影响。

⑤ 随着计算机系统的广泛应用，应用人员队伍不断扩大，各层次的应用人员增多，人为的某些因素，如操作失误的概率增加，会威胁信息系统的安全。

⑥ 安全是针对某种威胁而言的，对计算机系统来说，许多威胁和攻击是隐蔽的，防范对象是广泛的、难以明确的，即潜在的。

⑦ 计算机系统安全涉及到许多学科，既包含自然科学和技术，又包含社会科学。就技术而言，计算机系统安全涉及计算机技术、通信技术、存取控制技术、验证技术、容错技术、诊断技术、加密技术、防病毒技术、抗干扰技术和防泄露技术等，因此它是一个综合性很强的问题，并且其技术、方法和措施还要根据外界不断变化的威胁和攻击情况而不断变化，这就增加了保证计算机系统安全的难度。

1.3.2 影响计算机系统安全的因素

影响计算机系统安全的因素，可以分为两大类：一类是自然因素，一类是人为因素。

1. 自然因素

自然因素是指因自然因素造成的地震、水灾、火灾、风暴、雷击等，它可以破坏计算机系统实体，也可以破坏信息。自然因素可以分为自然灾害、自然损坏、环境干扰等因素。

(1) 自然灾害。各种自然灾害造成的事故和损失如表 1-1 所示。

表 1-1 各种自然灾害造成的事故概率和损失

不安全因素	发生事故的概率	损失范围/万元
失　火	0.50	1～300
地震灾害	0.01	50～300
风暴灾害	0.20	50～300
洪水灾害	0.10	50～300
雷击灾害	0.01	1～100
静　电	0.18	0.2～2

(2) 自然损坏。自然损坏是指因系统本身的脆弱性而造成的威胁。例如，元器件失效、设备(包括计算机、外围设备、通信及网络、供电设备、空调设备等)故障、软件故障(含系统软件和应用软件)、设计不合理、保护功能差和整个系统不协调等。

(3) 环境干扰。环境干扰如高低温冲击、电压降低、过压或过载、振动冲击、电磁波干扰和辐射干扰等因素。环境因素造成事故的概率及其损失如表 1-2 所示。

表 1-2 环境因素干扰造成的事故概率及其损失

不安全因素	发生事故的概率	损失范围/万元
电压降低或断电	0.50	0.1～10
电压波动	0.20	0.1～5.0
振动冲击	0.02	0.1～2.0
高低温冲击	0.10	0.5～3.0
电磁波干扰或辐射	0.03	
过　载	0.15	0.1～2.0

2. 人为因素

人为因素分为无意损坏和有意破坏两种。

(1) 无意损坏。无意损坏是过失性的,是因人的疏忽大意造成的。例如,操作失误、错误理解、无意造成的信息泄露或破坏。无意损坏或操作失误造成事故的概率及损失范围如表1-3所示。

表 1-3 无意损坏的概率及损失范围

不安全因素	发生事故的概率	损失范围/万元
设备故障	0.05	0.1~25
软件故障	0.10	1~10
程 序 员	0.15	0.1~2.0
操 作 员	0.15	0.1~1.0
用 户	0.20	0.1~1.5
维护人员	0.20	0.1~1.0
非专业人员	0.15	

(2) 有意破坏。有意破坏是指直接破坏建筑设施或设备、盗窃资料及信息、非法使用资源、施放病毒或使系统功能改变等,这是应该引起特别注意的。这种危害发生的概率及其损失范围如表 1-4 所示。

表 1-4 有意破坏发生的概率及其损失范围

不安全因素	发生事故的概率	损失范围/万元
内部破坏	0.20	1~500
外部破坏	0.10	1~300
贪 污	0.15	1~1000
窃 听	0.15	1~100
资料或信息被盗	0.10	10~200
篡改程序	0.15	0.5~100
施放病毒	0.15	1~数千万元

1.4 计算机系统的安全对策

1.4.1 制定安全对策的一般原则

1. 需求、风险、代价综合平衡原则

一个计算机系统的安全,要根据系统的实际情况(包括系统任务、功能、环节及工作状况等)需求、威胁、风险和代价进行定性和定量相结合的分析,找出薄弱环节,制定规范。具体措施往往是上述因素相互平衡、折衷的结果。

2. 综合性、整体性原则

对计算机系统的安全对策,应该用系统工程的观点进行综合分析,贯彻整体性原则。一个计算机系统包括人、设备、软件、数据、网络以及运行等环节。这些环节在一个系统安全中的地位、作用及影响,只有从系统综合、整体角度去分析,才能对可能采取的措施的有效性、可行性

得出恰当的结论。另外，一种安全技术可以有多种措施，并且可能是多种措施综合使用的结果，而各种措施的代价、效果对不同的系统并不一定相同。因此，综合性、整体性分析是非常需要的。

3. 易操作性原则

计算机系统的许多安全措施要人去完成，如果措施过于复杂，以致对完成安全操作的人要求很高，这样将降低安全性。例如，密钥的使用，如果要求人们进行过多的记忆，则会带来许多问题。

4. 适应性和灵活性原则

计算机系统的安全措施要能比较容易地适应系统的变化(需求变化、威胁与风险变化)，或用较小代价即可适应变化。在安全措施中，一定要考虑出现不安全情况时可采取的措施，例如系统应急措施、快速恢复功能措施、隔离措施等，以限制不安全状态的扩展。

5. 可评估性原则

对计算机系统采取的安全措施应能预先评价，应有相应的评价规范和准则。

1.4.2 安全策略的职能

计算机系统安全的实质就是安全法规、安全管理和安全技术的实施。安全策略的职能可以概括成三个方面：限制、监视和保障。

1. 限　制

限制那些非法的、偶然的和非授权的信息活动，支持正常的信息活动。

2. 监　视

监视系统的运行，发现异常的信息活动或设备(硬件和软件)故障，进行必要的、法律的、行政的或技术的处理。

3. 保　障

保障系统资源(硬件、软件)和各类数据及信息的完整性、可靠性和可用性。

1.4.3 安全策略和措施

从概念上讲，计算机系统的安全包括两方面的含义：一是安全，二是保密。为此，应采取的对策主要包括四个方面：法律保护、行政管理、人员教育和技术措施。

1. 法律保护

有关计算机系统的法规大体上可以分成两类：一类是社会规范，另一类是技术规范。

(1) 社会规范。社会规范是调整信息活动中人与人之间的行为准则。要结合专门的保护要求定义合法的信息实践，不正当的信息活动要受到民法或刑法的限制或惩处。发布阻止任何违反保护要求的禁令，明确用户和系统人员应履行的权力和义务，包括保密法、数据保护法、计算机安全法、计算机犯罪法等。

所谓合法的信息实践，是指在一定的人—机环境条件下，符合社会规范和技术规范要求，并满足系统或用户应用目标的信息活动。合法的信息实践受到法律保护，并且遵循如下的原则。

① 合法信息系统原则。要按一定法律程序注册、建立信息系统，对不符合准则的系统不予注册，没有注册登记的系统其安全当然不受法律保护。系统的任何改变，拓朴结构的任何变化，均应修改注册或重新登记注册。

② 合法用户原则。进入系统的用户必须是经过严格技术审查和信息利用目的审查，并登记注册的。

③ 信息公开原则。信息系统中允许收集、扩散、维护有关的和必要的信息，系统对这些信息的常规使用方式对法律公开。

④ 信息利用原则。用户信息按用户确认和系统允许的形式保存在系统中，用户有权查询和复制这些信息，有权修改名称和内容，但对他人和外部泄露则应予以限制和制止。

⑤ 资源限制原则。对系统保持信息的类型应给予适当限制，不允许超出系统合法权益的信息类型，并对信息保持的时限和精确性也给出限制。

(2) 技术规范。技术规范是调整人与自然界之间关系的准则，其内容包括各种技术标准和规程，如计算机安全标准、网络安全标准、操作系统安全标准、数据和信息安全标准、电磁兼容性标准、电磁泄漏极限等。这些法律和标准是保证计算机系统安全的依据和主要的保障。

2. 行政管理

行政管理是安全管理的一般行政措施，是依据系统的实践活动，为维护系统安全而建立和制定的规章制度和职能机构。这些制度主要包括如下内容。

(1) 组织及人员制度。包括机构、人员的安全意识和技术培训及人员选择，严格的操作守则，严格的分工原则。严禁程序设计人员同时担任系统操作员，严格区分系统管理员、终端操作员和系统设计人员，不允许工作交叉。

(2) 运行维护和管理制度。包括设备维护制度、软件维护制度、用户管理制度、密钥管理制度、出入门管理制度、值班守则、操作规程、行政领导定期检查和监督等制度。

(3) 计算机处理的控制与管理制度。包括编程流程及控制、程序和数据的管理，拷贝及移植、存储介质的管理，文件的标准化及通信和网络的管理。

(4) 机房保卫制度。机要机房应规定双人进出的制度，严禁单人在机房操作计算机。下班时机房门可加双锁，且只有两把钥匙同时使用时门才能打开。

(5) 对各种凭证、账表、资料要视同有价证券妥善保管，严格控制。

(6) 记账必须交叉复核，各类人员所掌握的资料要与其身分相适应。例如，终端操作员只能阅读终端操作手册，系统管理员只能阅读和使用系统手册。

(7) 信息处理用机要专机专用，不允许兼作其他用机。终端操作员因事离开终端时，必须将终端退回到登录界面，避免其他人员使用该终端进行非法操作。

重要计算机系统的安全组织机构包括安全审查机构、安全决策机构、安全管理机构和领导机构等。安全管理机构必须由安全、审计、保安、系统分析、软硬件技术人员、通信等有关方面的人员组成。其中安全、审计、保安和系统管理人员的职责是：

① 安全管理人员具体负责本系统区域内的安全策略的实现，保证安全策略的长期有效；负责可信软硬件的安装维护、日常操作监视，应急条件下安全措施的恢复和风险分析等；负责整个系统的安全，对系统修改的授权，对特权和口令的授权，对违章报告、报警记录、控制台记录的审阅和安全人员的培训，遇到重大问题时及时向主管领导报告等。

② 安全审计人员监视系统运行情况，收集对系统资源的各种非法访问事件，并对非法事件进行记录、分析和处理。必要时，要将审计的事件及时上报主管领导。

③ 保安人员主要负责非技术性的常规安全工作，如信息系统场地的警卫、办公室的安全、验证出入管理的手续和各项规章制度的落实。

④ 系统管理人员的主要任务是安装和升级系统，控制系统的操作、维护和管理，使系统处