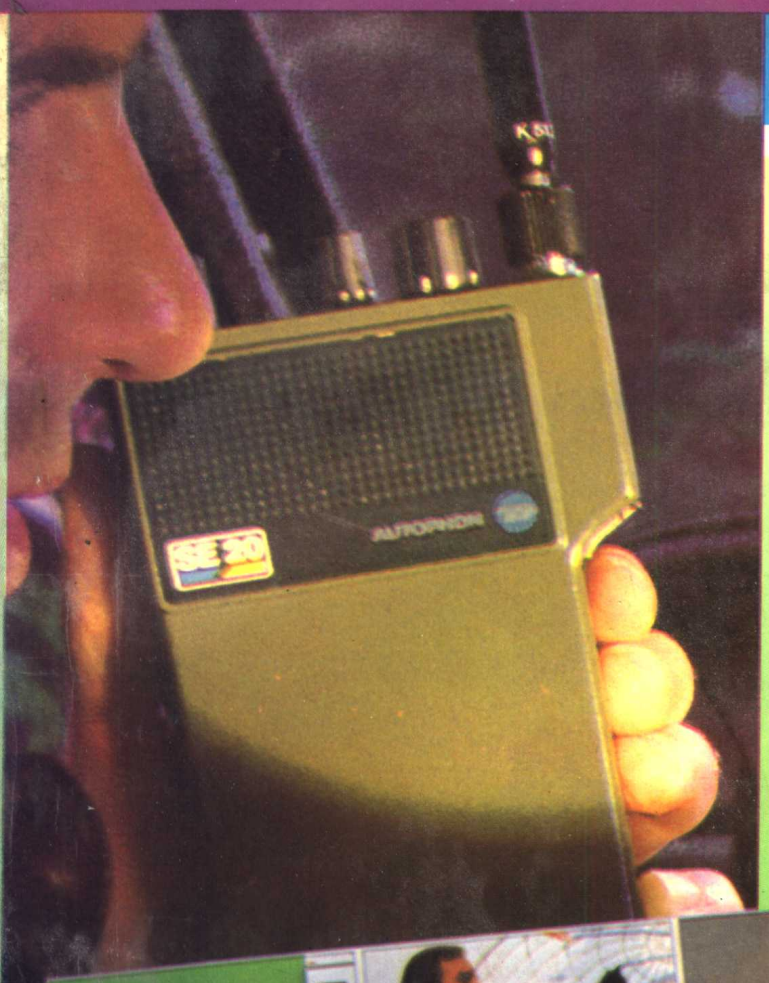
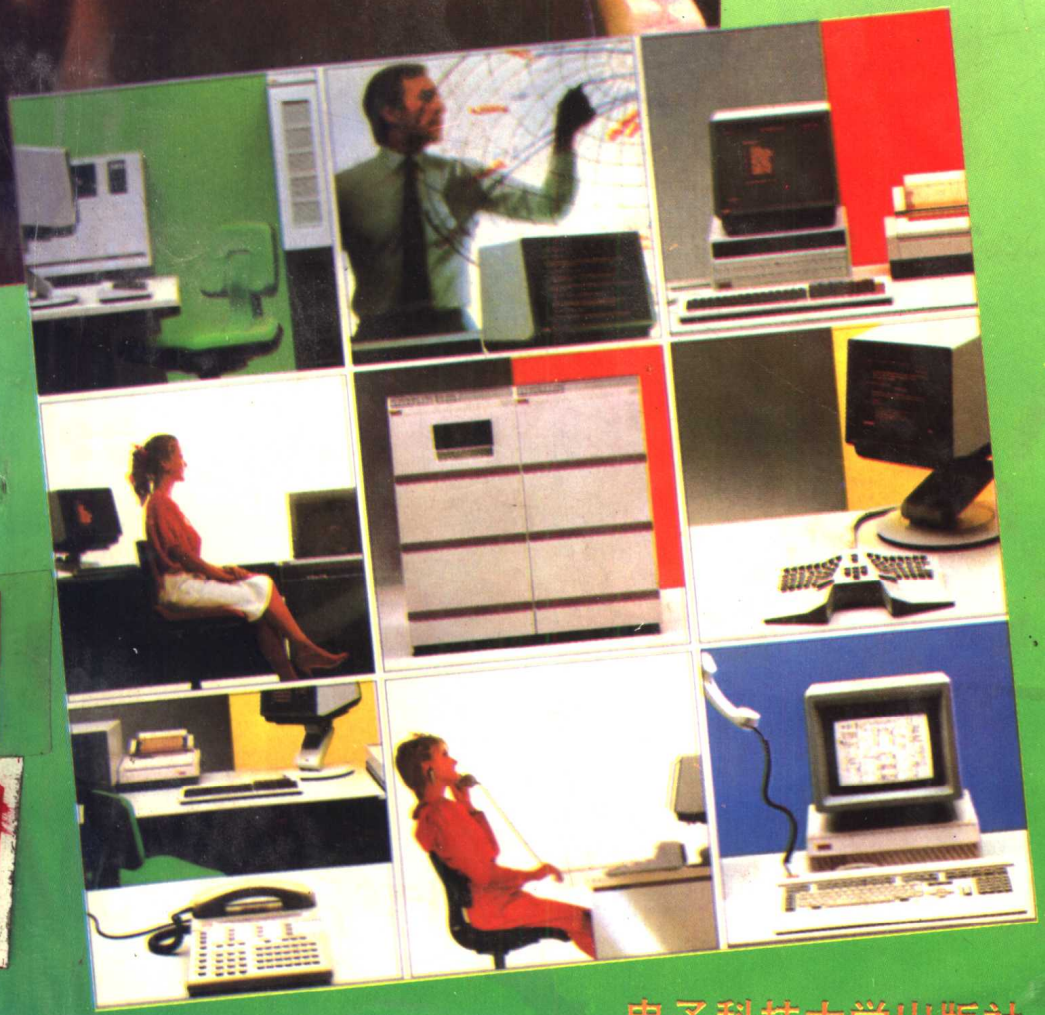
21 世纪通信技术丛书

计算机系统、数据库系统和通信网络的安全与保密

SECURITY OF COMPUTER SYSTEMS DATABASE AND COMMUNICATIONS NETWORKS

蒋继洪　黄月江　编著





电子科技大学出版社

21 世纪通信技术丛书

计算机系统、数据库系统和通信网络的安全与保密

蒋继洪　黄月江　编著

电子科技大学出版社
· 1995 ·

[川] 新登字 016 号

21 世纪通信技术丛书

计算机系统、数据库系统和通信网络的安全与保密

蒋继洪　黄月江　编著

*

电子科技大学出版社出版

（成都建设北路二段四号）　邮编 610054

四川石油管理局印刷厂胶印

四川省新华书店经销

*

开本 787×1092　1/16　印张 24.75　　字数 601 千字

版次 1995 年 6 月第一版　印次 1995 年 6 月第一次印刷

印数 1—4000 册

ISBN 7—81043—203—6/TP・63

定价：28. 00 元

《21世纪通信技术丛书》编辑委员会

前　言

计算机系统、网络系统和数据库系统可以说是三种主要的计算系统；本书尽管以讨论它们的安全问题为主线，而实际讨论的却是一般计算设备（或系统）中的安全问题。其基本原理适用于包含CPU芯片、软件和硬件的各种设备。

随着社会的日益信息化，联成网络的计算机系统（往往包含大型数据库）在银行系统、商业系统、管理部门（如大的航空港的管理）、政府和军事领域的应用越来越广泛。其中的安全问题也日渐突出，稍有不慎常常带来灾难性后果。不论在西方还是在我国，计算中的安全问题都已成为社会各界关注的焦点；信息高速公路的规划和实施对于这一问题无异于火上浇油，必然引发更大的研究热潮。本书就是应此之需而组织编写的。

书中列举的安全问题的背景材料主要来自美国。本书共分十五章，主要涉及下列几方面的内容：

第一～五章：一般的安全问题；加密算法；安全协议及其应用；程序的安全。

第六～七章：操作系统的安全性要求和设计，是本书的重点。

第八～九章：数据库的安全及个人计算机的安全问题。

第十～十一章：计算机网络和通信系统中的安全问题。

第十二～十三章：物理保护、风险分析、安全规划。大型工程的规划管理人员应该对此感兴趣。

第十四～十五章：计算机安全的社会方面：安全立法、安全道德等。

本书适合于计算机、通信、信息管理等有关专业的大学本科、研究生及专业工作者参考，也可作为有关专业的教学参考书。

本书是集体编写的，其中：

黄月江　编写第一、第五、第十二和第十三章；

黄月江　编写第一、第五、第十二和第十三章；

关义章　编写第二、第十、第十一章；

蒋继洪　编写第四章的4.3～4.4、第六章、第七章、第八章、第九章的9.1；

龚奇敏、杨旭　编写第三章；

周安民　编写第四章的4.1～4.2；

雷利民　编写第九章的9.2～9.5；

于增贵　编写第十四章；

杨　新　编写第十五章

最后，由蒋继洪对全部书稿作了第一遍审校；由蒋继洪、黄月江又分别作了第二遍审校。

在本书的出版过程中，吴世忠同志负责组织工作，付出了大量的劳动。

由于题材较新，时间和水平有限，不当之处望读者批评指正。

编　者

内 容 简 要

计算机系统、网络系统和数据库系统可以说是三种主要的计算系统。本书尽管以讨论他们的安全问题为主体，而实际上讨论的却是一般计算设备(或系统)中的安全问题。其基本原理适用于包含 CPU 芯片、软件和硬件的各种设备。本书主要内容包括：一般的安全问题、加密算法、安全协议及其应用、程序的安全、操作系统的安全性要求和设计、数据库的安全及个人计算机、计算机网络和通信系统中的安全问题、物理保护、风险分析、安全规划、计算机安全的立法、道德等。

本书适合于计算机、通信、信息管理等有关专业的大学本科、研究生及专业工作者参考，也可作为有关专业的教学参考书。

ter Systems

etworks

目　录

第一章　计算设备中的一般安全问题

目前我国的计算机网络系统还没有西方国家那么发达，银行计算机系统正开始普及。研究发达国家在这方面走过的道路很有启发作用。现在，在西方发达国家如美国人们已经很少听到银行抢窃案了。在野蛮的西部时代，银行除金银外，还拥有大量难以追踪的现钞。通信和交通设施落后，一件抢窃案发生后，法律当局要数小时才能得知消息，赶到犯罪现场要花几天的功夫，但抢窃犯早已溜之大吉了。夜里派一个守卫也仅起有限的作用。窃贼需要知道一点普通常识以及几天的时间来分析情况，但不需要更复杂的训练；某些人在学道期间就已懂行。所有这些因素都使天平向罪犯一方倾斜，因此银行窃贼那时是受益匪浅。

然而在今天，发达的技术条件使得许多因素都与潜在的罪犯不利。无论有人无人，复杂的警报系统都在静静地护卫着银行。侦察罪犯的技术已变得非常有效，因而可通过指纹、噪音、拼图、弹痕或其他难以掩盖的特征来识别出一个人。因为大多数银行的生意现在都通过支票来进行，许多银行支行用来周转的现金比某些大的零售商店还少。那些储备大量现金或现钞的地方都具有多个层次的安全保护：多层物理系统、复杂的锁，需要两个人一致同意才允许访问的双关系统，以及许多型式的其他的系统。现代化的交通工具和通信手段使得警察可以在几分钟内抵达现场，并且在几秒钟内告知同行注意监视嫌疑犯。抢窃银行要冒很大的风险并需要复杂的技术，因而一般的罪犯通常都转向比银行更容易的目标。

本书讨论的是计算系统而不是银行的安全。现在考察一下计算系统与银行的不同之处。

·大小和可携带性。计算的物理装置是如此之小，价值数千元的计算机可以很舒服地装入一个手提箱，而价值上万元的计算机可以很轻松地用两手搬走。

·避免物理接触的能力。电子资金转移常见于银行间的金钱转移。例如，私人公司付雇员工资就直接用计算机过户而不用支票。公用事业公司、保险公司和抵押公司都自动地处理从其客户帐户扣钱的事务。银行的顾客甚至在家里就可以与银行打交道，将资金从一个户头转移到另外的户头，通过电话访问计算机而安排取钱的事务。

·财产的价值。存储在计算机里的信息的价值也是非常高的。一些计算机存有有关个人的纳税、投资、医疗历史或教育方面的秘密信息；另一些计算机存有关于新的生产线、销售数字、市场战略，或军事目标、部队调动、武器杀伤能力等等非常敏感的信息。

在安全方面，计算领域非常近似于西部时代。在某些计算站中，计算机及其数据被认为是非常宝贵而脆弱的资源，受到适当的保护；而某些计算站的安全措施却极其缺乏。但是，与"西部时代"银行家不一样，某些计算专家和管理人员甚至还未认识到他们所使用或控制的资源的价值。

更糟的是，在一项犯罪事件发生后，某些公司不调查也不分析，因为害怕损害他们的公众形象。例如，当一家银行刚刚因为计算机被盗用而损失五百万美元之后，在这家银行存款会感到安全吗？事实上，那家银行刚刚痛苦地了解到了他安全上的弱点。该银行也许会有效

地增强他的安全，因而可能比未蒙受损失的银行还要安全一些。

不认为电磁信号是财产的状态妨碍了犯罪调查和起诉。新闻界将最近由一伙年青人进行的计算机入侵事件描绘成其严重性还不如搞坏一个室外设施的恶作剧。

显然，计算安全是一个非常重大的问题，这是一个值得计算机专家、管理人员甚至用户研究的领域。本书就是为此而写的。通过学习本书，将了解计算中的安全问题是什么以及采用什么方法来处理这些问题。许多情况即使在西方发达国家也仍然存在，在我国或者已经存在，或者将来也会碰到。

本书的目的是要考察计算安全方面的危险，考虑合适的防护措施，并指出还需做更多工作的领域。本章首先考察哪些计算系统易于产生哪类弱点，然后研究这些弱点是如何被利用的，即可能进行的各种攻击。第三，要看是谁造成了计算中的安全问题。最后，将介绍控制——防止系统攻击的方式。

1.1 计算机入侵的特征

计算机犯罪的目标可以是任何计算系统。计算系统是一个组织用来完成计算任务的硬件、软件、存储介质、数据以及人员的集合。银行窃贼的明显目标是现金，而存款者的姓名和地址表对于相互竞争的银行是很有价值的。这张表可以印在纸上，也可以记录在磁介质中，存储在计算机的内部存储器上，或者通过如像电话线之类的介质用电子方法进行传输。目标的多样性使得计算机安全的实现相当困难。

在任何安全系统中，最易受到攻击的地方就是最弱的地方。当窃贼要从屋里偷什么东西时，如果窗户最容易进入，他决不会去弄穿几寸厚的金属墙。一个复杂的环形物理安全系统不能防止简单地利用电话线和调制解调器进行的无戒备的访问。“最弱点”的概念可以重新阐述为下列原则：

最易穿透原则(Principle of Easiest Penetration)

一个入侵者可以使用任何现有的穿透手段，这种手段不见得是最明显的，也不必是用来对付最坚固防护的手段。

这个原则说明，计算机安全专家必须考虑所有可能的穿透手段，因为加强对一种手段的防护必然使另一种手段更加吸引入侵者。现在考察到底有一些什么样的穿透手段。

1.2 对资源安全性的四类威胁

在安全中，暴露(Exposure)是指对计算系统可能引起的某种形式的损失和损害；暴露的例子有未经许可地泄露数据，更改数据，或者拒绝对计算的合法访问。弱点(Vulnerability)就是在安全系统中可被利用并引起损失和损害的薄弱之处。人们可利用弱点对系统发起攻击(Attack)。对计算系统的威胁(Threats)是有可能引起损失或损害的事件。人发起的攻击是威

胁的一个例子，其他的还有自然灾害，非故意的人员出错，以及内部的硬件或软件缺陷。最后，控制(Control)是能减少弱点的一种防护措施——一个行动，设备，过程或技术。

计算机系统的主要资源(Assets)是硬件、软件和数据。对计算系统安全的威胁有四种类型：中断(Interruption)、窃取(Interception)、更改(Modification)和伪造(Fabrication)。这四种威胁都是利用计算系统资源的弱点产生的，如图 1.1 所示。

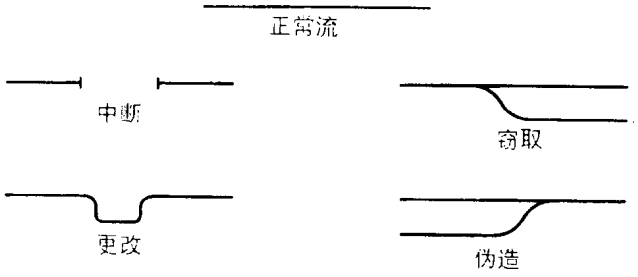


图 1.1　破坏安全的四种类型

1. 在中断时，系统的资源受损，不见或不能使用。这方面的例子有：恶意地毁坏硬件设备，擦除程序或数据文件，或者是一操作系统的文件管理器出现故障，因而他不能找到一个特定的磁盘文件。

2. 窃取意味着某个未经许可的部件获得了对一个资源的访问。这个外部部件可以是一个人，一个程序，或者一个计算系统。这类破坏的例子是非法拷贝程序或数据文件，或者通过窃听的方法从网络中获得数据。它造成的损失可以相当快地发现，但沉默的窃取者却可能不留踪迹。因而不容易检测出窃取的发生。

3. 如果未经许可的当事人不仅访问而且损坏一项资源，这种损坏就是更改。例如，某个人可能更改数据中的值，修改一个程序以便完成一项附加的计算，或者更改电子传送中的数据。甚至还有可能更改硬件。某些情形的更改可以用简单的措施检测出来，而其他一些更精妙的更改却几乎是不可能检测出来的。

4. 最后要说的是，一未经许可的当事人可以在一计算系统中伪造假目标。入侵者可能希望在网络通信系统上加上假的交易，或者在现有的数据库中增加记录。某些时候，这些增加的东西可作为伪造物而检测出来；但如果伪造技艺纯熟的话，几乎会达到以假乱真的地步。

干扰计算机行动的四种类型——中断、窃取、更改和伪造——可以描述可能的暴露类型。这些干扰类型的例子见图 1.2，产生的问题在下一节中描述。

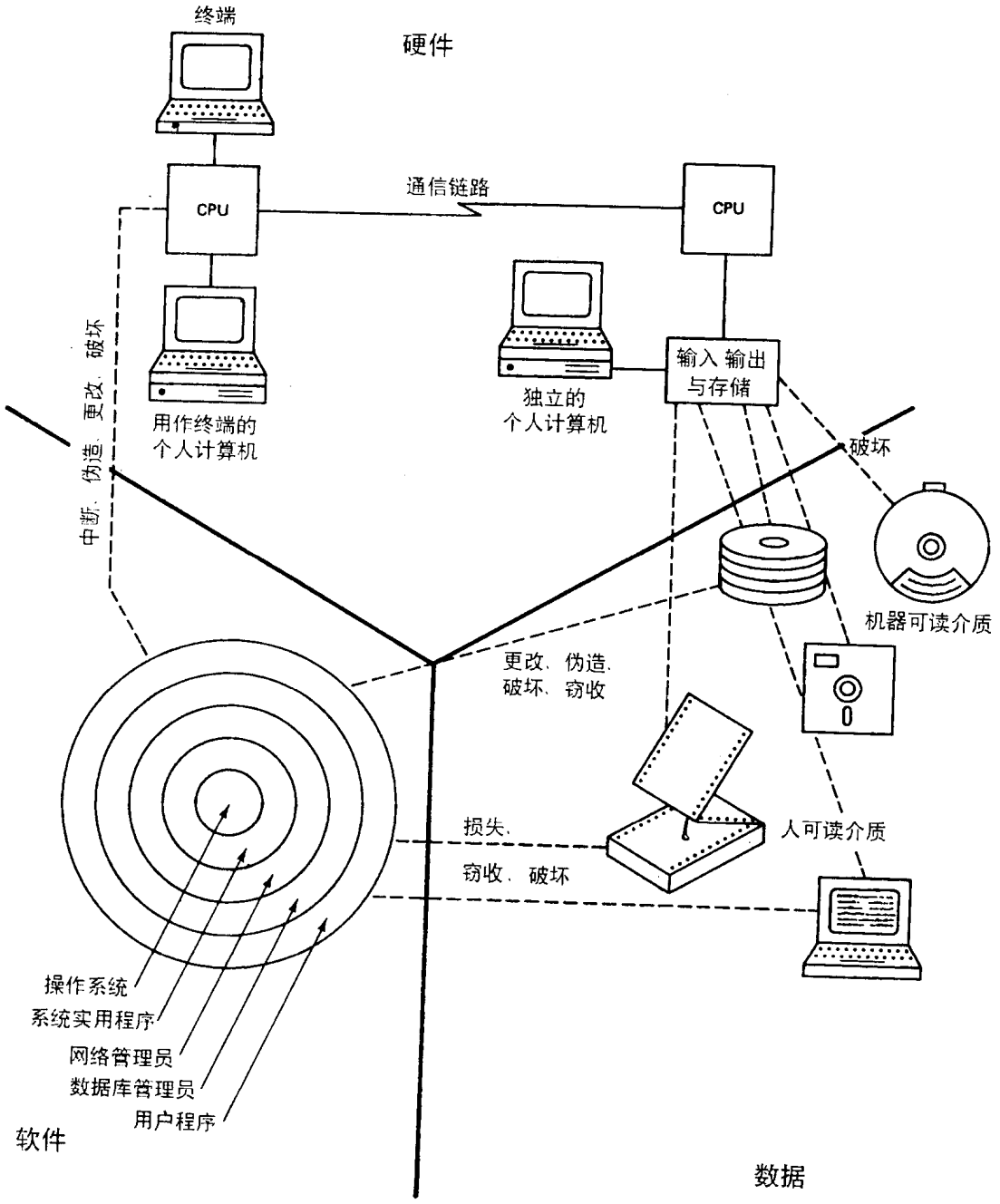


图 1.2　计算机系统中的滥用类型

1.3 安全上的弱点

计算机安全的构成要维持三个特征：保密性、完整性和可获性。

• 保密性(Secrecy)意味着一计算系统的资源只能由许可的当事人访问。这类访问是"读"类型的访问：阅读、观看、打印或者甚至对目标是否存在的了解。

• 完整性(Interity)意味着资源只能由许可的当事人更改。在本文中，更改包括写入，改变内容，改变状态，删除和创建。

• 可获性(Availability)意味着资源只能由许可的当事人使用。对于有合法访问权的经许可的用户，不应当阻止它们访问那些目标。例如，一安全系统可以通过禁止任何人读一个特定的目标而达到完善的保密性，然而，这个系统并未满足对适当的访问具有可获性的要求。

图 1.3 示出了应用于硬件、软件和数据这些资源时的三种安全任务。这三种资源以及它们之间的连接就是所有潜在的安全薄弱之处。

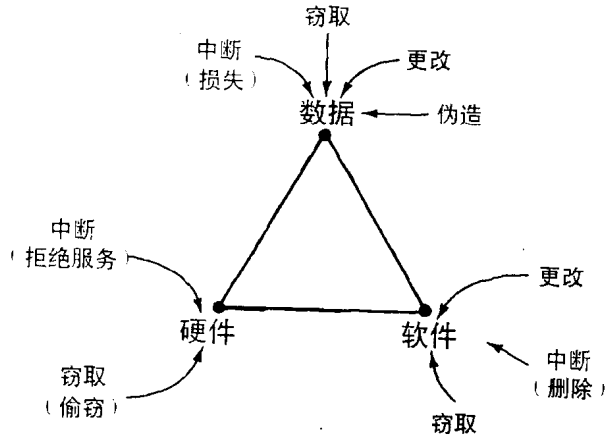


图 1.3 计算系统的弱点

下面几节针对计算系统每一特定的资源讨论其薄弱之处。

一、对硬件的攻击

由于物理设备是可见的，故它是发起攻击的最简单的地方。但幸运的是通常这类地方都装有适当的安全装置。计算机可因为水灾、燃烧、汽体而损坏，也可因雷电，或者其他地方的电源波动而判死刑。人们常常将软饮料、爆米花、蕃茄酱、啤酒及许多其他的食物洒落到计算设备上。老鼠经常把电缆咬穿。灰尘的粒子，尤其是烟雾粒子，威胁着工程精度很高的运动部件。计算机被拳打、脚踢、撞击、震动。所有这些滥用都属于"非志愿的机器杀手"之列：本意并不想引起硬件严重损失的无意行动。

更严重的攻击可称为“志愿的机器杀手”或简称“机器杀手”。在这类攻击中，有人实际上希望对计算机带来伤害。计算机曾遭枪的射击和刀的刺杀。炸弹、纵火及碰撞曾毁灭过计算机房。普通的钥匙、钢笔和螺丝刀曾被用来使电路板和其他部件短路。机器曾被小偷拿走。人类对计算机的攻击数不胜数。

刚刚提到，人们对计算机进行无意或有意的攻击是为了危害可获性。偷窃和破坏是其主要的技术。大计算中心的管理人员很早前就意识到了他们计算机的弱点，并安装了物理安全系统来防护。但办公室微计算机数量的迅速增加使得人们常常把价值数千美元的设备搁置在计算机房外的无人看守的办公桌上（具有讽刺意味的是，价值只有数百美元的笔、文具和环形针的供给房却常常上着锁）。有时，硬部件的安全可通过采用诸如上锁或门卫这些简单的物理措施而得以大大增强。

二、对软件的攻击

没有用户所期望的软件（操作系统、服务程序和应用程序），计算设备就一钱不值。软件可被人居心不良地毁掉，也可无意地被更改、删除或放错地方。然而不管动机如何，其结果是一样的，当人们想运行的时候，软件的损失就显露出来了。这些攻击就是软件可获性的所有问题。

更微妙的是软件虽经更改而仍能运行。物理设备通常还可看到遭受创伤的痕迹，但在源或目标代码中损失一行关键的代码在程序中却可能不留下明显的痕迹。更有甚者，可以改变一个程序使他能够完成以前所做的所有工作，然后再干一些别的事。在这种情况下，要检测软件是否被改变是一件相当困难的事情，更不用说确定被改变的内容了。

1. 软件删除

软件极容易被删除。或许每一个编程者都偶然擦除过一个文件，或保存的是一个没拷贝好的程序，却把先前好的那一个毁掉了。由于软件对于商业计算中心有很高的价值，对软件的访问通常都是仔细控制的，通过称为配置管理（Configuration Management）的过程来实现，保证软件不被偶然地删除、销毁或代替。

2. 软件更改

在这类攻击中，工作程序受到更改，它他在执行中失败或干某些其他事情。软件极容易被更改：改变一两个比特就会使程序不能正常工作。这取决于改变什么比特，程序也许一开始运行就失败，或者在失败前还能运行一段时间。

只要做少量的工作，这种改变就可变得很微妙。这样一来，程序在大多数时间里工作得很好，但当特定条件出现时，就出故障。这类改变产生一种称之为“逻辑炸弹”（Logic Bomb）的程序。例如，一心怀不满的雇员可更改一个重要的程序，它他访问系统上的计时程序并令其突然在 7 月 1 日后停机。这个雇员也许在 5 月 1 日辞职并计划 7 月前在很远的地方找一个新工作。

另一种类型的改变可以扩展一个程序的功能，使得一个无害的程序具有隐蔽的副作用。例如，一个程序的表面结构是列出属于一个用户的文件，但却同时还改变所有这些文件的保护以允许另一个用户对这些文件的访问。

软件更改的类型包括：

（1）特洛伊木马（Trojan Horse），公开做一件事但暗地里还干另外事情的一段程序。