HOPE COMPUTER COMPANY LTD.

计算机安全与保密技术

段素娟 等编
王文钦

北京希望电脑公司

计算机安全与保密技术

王文钦
段素娟
等 编

北京希望电脑公司
一九九〇年十二月

前　言

随着计算技术的飞速发展及计算机的日益普及，计算机已进入社会生活中的各个角落，在金融现代化，企业管理科学化等方面发挥着巨大的作用。计算机在给各行各业带来巨大经济效益的同时，它的背后却潜伏着严重的不安全性、危险性及脆弱性。特别是进入八十年代以来，由于下面两个原因，使得安全问题变得更加突出：

· 个人计算机的使用。个人计算机已进入普通家庭。用户并未特别意识到在计算机使用过程中应考虑的安全因素；即使有这种考虑，他们也并未知道采取什么样的措施控制这些不安全因素。

· 远程网络计算系统的使用。远程存取访问在提供给用户资源共享的同时，却给用户一个存取远程计算机保密资源的机会。

在国外，许多青年人特别迷恋于攻击某些安全系统。如，1987年，一群西德青年通过远程终端进入了北大西洋公约组织(NATO)计算机网络中连入美国的计算机。在我国，也出现了多起银行犯罪，特别是近年来，大量微机病毒的出现，给我们的计算机系统带来了严重的危险。

本书正是围绕着计算机系统的安全问题，从描述计算机系统面临的安全问题入手，讨论怎样控制和检查计算机系统中所存在的缺陷以及在建立一个计算机系统时应考虑的安全因素。全书包括了六个领域的内容：

· 普通程序的安全性
· 操作系统的安全性
· 数据库管理系统的安全性
· 个人计算机的安全性

· 远程存取访问的安全性

· 多计算机网络的安全性

每个领域的讨论都从问题的定义入手，详尽描述该领域中所存在的安全方面的问题，然后讨论该领域中目前对这些问题所采取的控制方法及策略。文章的最后还讨论了计算系统安全方面的危险分析及安全规划，并探讨了计算机安全中法律和道德的关系。

本书可供使用计算机单位的领导，保卫人员，计算机技术人员，科研人员和计算机爱好者，以及大专院校的教师、学生参考。

目　录

第一章　计算机系统中存在着安全问题吗

当今社会，你会经常听到有关抢劫银行的事情。在西方，银行不仅储备金银而且还存放大量的现金。现金的使用远比支票广泛。先进的通讯及运输设施使得犯罪更趋现代化。门卫的设置不足以保证银行的安全性。尽管抢劫要求一系列常识而且需要花费几天时间分析情况，但是，它不需太多的高级训练便可获取钱财。因此，抢劫银行的案件屡有发生。

但是，今天也有许多办法能阻止犯罪的发生。例如，精密的警报系统用于银行防盗，犯罪侦破技术日趋成熟，使得人们可以借助于指纹、声音、人体的轮廓或其它难以伪造的特性来识别特定的人。由于银行的许多业务可以通过支票直接进行，因而许多分行的现金储量甚至比某些较大的零售商店还要少。而用于存放现金或货币的地方则采取多级的安全措施予以保护。这些措施包括：多层物理系统，复杂的锁，只有两人在场才允许启动的系统等。先进的通讯及交通设备，使得警察可在几分钟内赶到犯罪地点，并在几秒内通知其他警察追捕嫌疑犯。因此，在技术高度发达的今天犯罪分子往往采取更为巧妙和隐蔽的手段。

本书讨论的是计算系统的安全性。首先必须弄清计算系统和银行安全性的关系。

·设备尺寸及便携性。计算系统中的设备是如此的精小以致于上千元的计算机设备可以装在一个简易盒里，而且上万元价值的设备也可以简单地带在身上。

·避免实物接触的能力。电子资金传送构成了大多数银行资金传送的基础。例如，私人公司直接通过计算机传送设备代替支票支付雇员工资。公共事业机构，金融公司以及租赁公司自动处理其委托人银行帐号下的资金。顾客甚至可以在家里通过连入计算机的电话线把钱存入银行，将资金转入不同的帐号下并安排提款。

·资源的价值。存在于计算机中的信息具有很高的价值。某些计算机中存放个人税收、投资、病历或教育等机密信息。而另一些计算机则存放新产品、销售情况、市场策略或军事目标、部队调派、武器状况等绝密信息。

就安全性而论，计算系统的安全状况非常类似于当今西方银行。在某些设施中，计算机及其上面的数据被当作极有价值的资源和易受攻击的目标，因此，都已对它们采取了适当的保护措施。而其它设备则相当缺乏安全保护措施。但是，和“西方”的银行家不同，某些计算机专家及管理者甚至没有意识到他们所使用或控制着的资源的价值。甚至在犯罪发生后，某些公司害怕损害它们在公众中的形象，对犯罪不作调查或起诉。例如，在你将钱存入一个由于通过计算机提款而丢失五百万元的银行时你是否放心？事实上，那家银行也已经意识到它在安全方面的缺陷。它为了不再被欺骗也确实可能在安全方面采取了一系列措施。

对犯罪的调查及起诉受到了有关电磁信号不是物质的法令的限制。最近，一伙青少年的恶作剧侵入了计算机系统，而新闻媒介在对它的报道中，竟看作是无关紧要的。

显然，计算系统中的安全性是一个非常重要的问题。它是一个值得计算机专家，管理人员甚至许多计算机用户研究的领域。本书则是为这些不同层次的人们所书写的。通过学习本书，你会了解计算系统中所面临的安全问题以及解决这些问题的方法。

本书的目的是为了考察计算系统中所受到的安全威胁，考虑可行的对策并且发现需作

更多工作的领域。本章，我们从考察什么样的计算系统易于受到什么样的侵入入手，然后讨论这些侵入是怎样进行的，即多种不同的进攻方法。在这之后我们将研究对计算系统安全产生影响的不同种类的人。最后，我们将介绍控制计算系统免受攻击的方法。

1.1 计算机侵入的特性

计算机中的犯罪目标可能是计算系统任何部分。一个计算系统由硬件、软件、存储介质、数据以及相应的人员组成。由于银行抢劫的目标显然是现金，因而储户的名字及地址表对银行来说将是非常有价值的。这种表可能记录在纸上、磁介质上或存于计算机中，也可能通过传播媒质如电话线传送到另一地方。目标的多样性增加了保证计算机安全的困难性。

在任何安全系统中，最弱的地方总是受攻击最严重的地方。一个打算从你房间中偷窃的小偷，若从窗口进入更容易的话，他是决不会去捣坏你那条两英寸厚的金属门而进入房间的。一个设备精良的物理安全系统是决不会对通过电话线及调制调解器的非防备进入在意的。"最弱点"遵循如下原则。

最易侵入原则。侵入者一定希望使用任何可用的侵入手段。它不必是最明显的手段，也不必是进入最严密设施时所采取的手段。

由于在加强某一方面的同时可能会使得另一方面易于受侵入，因而，此原理告诫计算机安全专家必须考虑所有可能的侵入手段。下面，我们研究这些侵入手段。

1.2 攻击的种类

在安全系统中，泄露是计算系统中信息丢失或遭破坏的一种可能的形式。泄露的例子有数据非授权访问、修改或非法进入计算系统。脆弱性是指安全系统中被利用从而导致信息丢失或破坏的弱点。攻击是指利用系统的脆弱性实施对系统的攻击。对计算系统的威胁是指可能导致信息丢失或破坏的环境；威胁的例子有人为攻击，自然灾害，人的疏忽大意，以及内部硬件或软件故障。最后，控制是指保护量度——一个减少脆弱性的措施、设备，过程或技术。

计算机系统中的主要资源包括硬件、软件以及数据。对计算机系统的安全威胁有四种：中断（干扰）、截取、修改及伪造。四种威胁都利用了计算机系统中的脆弱性。图 1.1 中说明了这四种威胁。

1. 在中断(干扰)过程中，系统资源变得易损失，不可得或不可用。例如，蓄意破坏硬设备、删除程序或数据文件或使操作系统文件管理程序失效使之不能找到特定的磁盘文件。

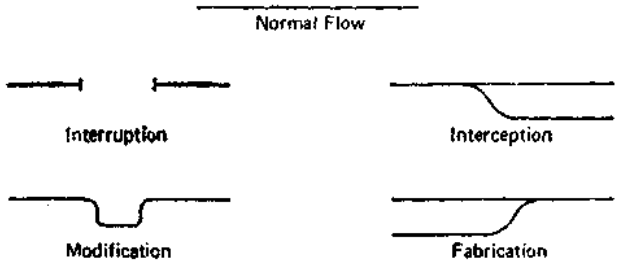

图1.1 系统安全失效的四种类型

2. 截取意味着某些非授权团体获得对资源的存取。团体可以是一个人，一个程序或一个计算系统。例如，在网络中为得到数据对程序或数据实施的非法拷贝、电话线上的窃取等。尽管丢失可以很快发现，但熟练的窃取者不会留下任何可以快速检测的痕迹。

3. 如果非授权团体不但存取资源而且对它进行篡改，则这种失效变为修改。例如，某人可能修改数据库中的数值，修改程序使之完成额外的计算或修改正在传送中的数据。甚至可能对硬件进行修改。某些修改可以通过简单的方法检测，但有些更为巧妙的改变几乎不可能被检测出来。

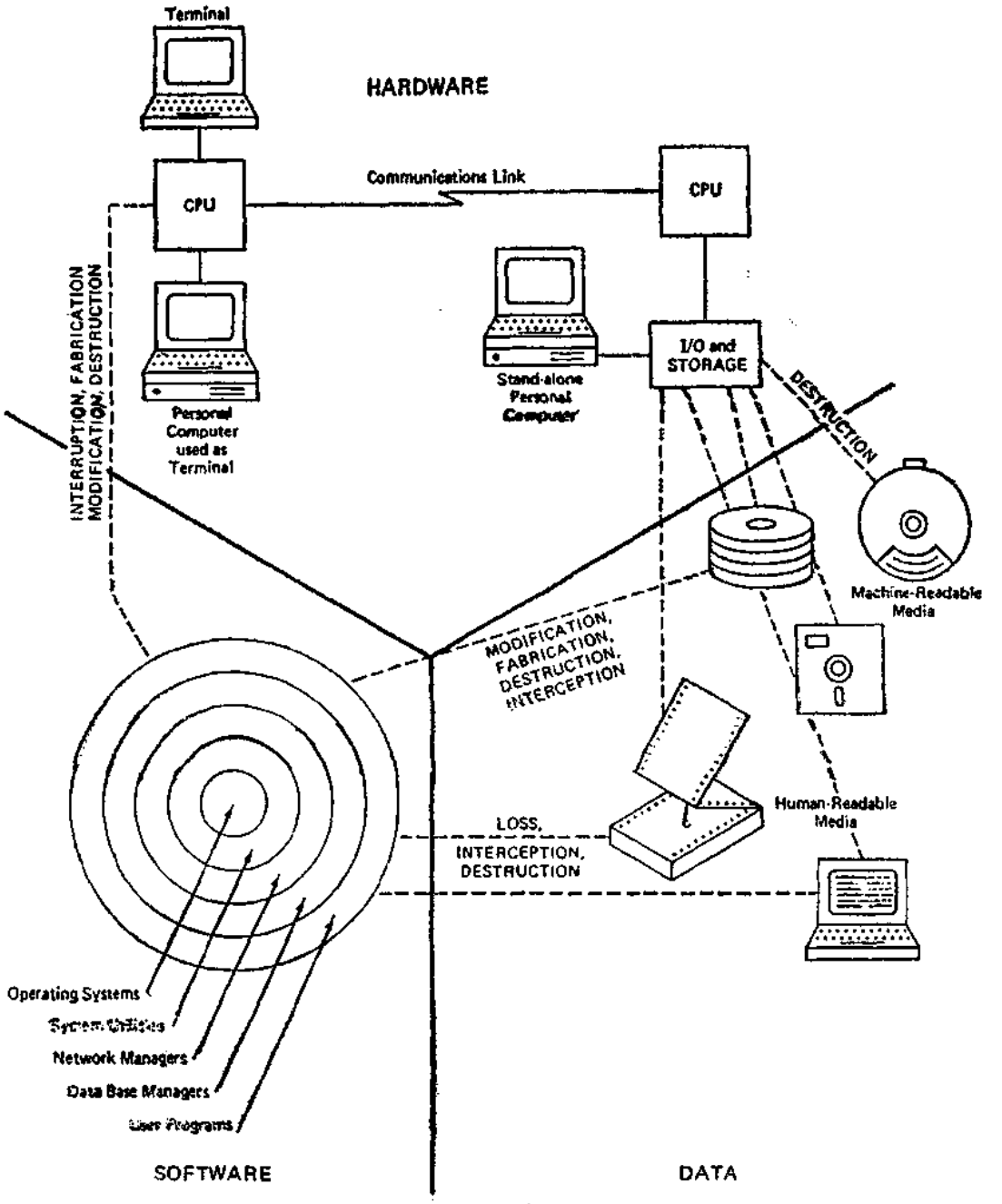

图1.2 计算系统中侵扰的类型

4. 最后，非授权团体伪造计算系统中的实体。例如，入侵者可能想将伪造的事务加入到网络系统中或向当前数据库加入记录，尽管有时可将这些加入作为伪造品检测出来，但是若实施巧妙，则它们完全可以假乱真。

这四类侵扰计算机的活动——中断(干扰)、截取、修改、伪造，它们描述所有可能泄露的种类。这些种类的侵扰的例子如图1.2中所示。有关问题则在下面描述。

1.3 安全的脆弱点

计算机安全具有如下三个特性：保密性，完整性及可用性。

·保密性意味着计算系统的资源仅能由授权团体存取。存取的类型为“读类型”的存取：读、视图、打印或仅只知道该实体的存在。

·完整性意味着资源只能由授权实体修改。这里的修改包括：写、改变、改变状态、删除及创建。

·可用性意味着资源仅能由授权团体使用。不应该将授权团体能合法存取的对象保护起来不让他或她使用。例如，一个安全系统可通过禁止任何人读某一特定实体而实现绝对保密，但是，此系统不满足适当的存取可用性的要求。

图1.3描述了将这三种特性应用于硬件、软件及数据资源时在安全方面应考虑的问题。

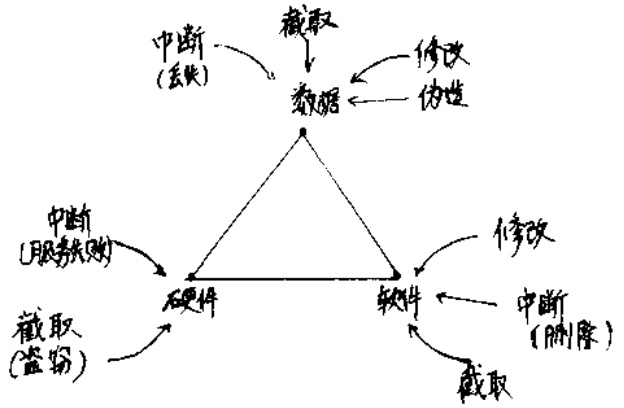

图1.3 计算系统的弱点

下面的几节将介绍计算系统中每一种特定资源的脆弱性。

1.3.1 对硬件的攻击

由于物理设备是可见的，因而总有很简单的攻击点，但是，总是为它安排了相应的保卫人员。计算机有可能被水、火及气体侵蚀而且也有可能由于爆炸或强光而遭破坏。人们也可能将软饮料、食物碎粒、番茄酱、啤酒及其它食物洒在计算机设备上。老鼠也可能咀嚼电缆。灰尘中的颗粒，特别是吸烟所产生的烟灰对精密的可移动部件非常有害。计算机也可能被抛置、敲打、冲撞、震动及冲压等。所有这些滥用都出自“无意的机器杀手”之手，即那些并未打算对硬件造成严重破坏的偶然行为。

更严重的攻击叫作“有意的机器杀手”或“机器杀手”，它是那些有意对计算机破坏的人所为，他们用枪射击机器或用刀破坏机器，使用炸弹 火灾破坏计算机房。普通的钥匙、钢笔及螺丝起子都可使电路板或其它部分短路。机器可能被小偷盗走。对计算机的人为破坏方

式几乎无法穷举。

我们已例举了一些人们有意或无意攻击计算设备旨在限制可用性的方法。偷窃和破坏是最基本的技术。主要计算中心的管理人员早就意识到他们机器的脆弱性并且安装了相应的物理安全系统来保护它们。但是，办公室里的价值几千元的微计算机则置于计算机房外的桌子上（很奇怪的是，机箱、仅值几百元的钢笔、文具以及纸夹则用锁锁起来）。有时，硬部件的安全性可通过采取简单的物理措施，如锁或门卫等而大大提高。

1.3.2 对软件的攻击

没有用户所要求的软件（操作系统，实用程序及应用程序），计算机设备可以说是毫无价值的。软件可被有意破坏或被无意地修改、删除或错放地方。尽管动机不同，但结果是一样的，即试图执行它时则会发生软件失效。这些攻击是软件可用性中的全部问题。

更为错综复杂的情况是所运行的软件已被改变。物理设备通常会留下某些损伤的痕迹，而源或目标代码中关键行的丢失不会在程序中留下明显的痕迹。而且，有可能改变程序的某些部分而程序照常和以前一样运行。此时，你很难检测软件已被改变，更不用说改变的内容了。

1. 软件的删除

毫无疑问，软件是很容易被删除的。有可能是程序员无意中删除一个文件或是保存了程序的一个错误拷贝从而破坏了以前的拷贝。由于软件对于商业性质的计算机中心来说是相当宝贵的资源，因此，通过一种叫分配管理的进程来严格控制对软件的存取，从而避免了软件的无意删除、破坏或替换。

2. 软件的修改

在这种攻击中，工作程序被修改，从而导致程序在运行过程中失败或使它完成了某些未能预料的任务。相对来说，软件是很容易修改的，改变程序中的一位或二位信息即可导致它失效。依据所改变的信息，程序可能在它开始执行时失败或在它执行几次后失败。

只需很少的工作，就可使这种改变变得错综复杂，此时，程序在大多数场合工作是正常的，但在特殊环境下则失败。这种改变的效果称作逻辑炸弹。例如，一个对单位不满意的雇员可以在程序的关键部分作些修改，从而使程序取系统日期并在七月一日之后突然停止工作。而该雇员则可能在五月一日辞职并在七月之前在几公里之外找到一个新工作。

另一种类型的改变可以扩大到程序的功能，从而使得正常的程序隐藏着付作用。例如，程序可能会伪造属于某一用户的文件表并修改所有这些文件的保护机制使得另一用户能存取这些文件。

软件修改的策略包括：

- 特洛伊木马（Trojan horse），程序在表面上做一件事的同时隐藏地做另一件事。
- 密钥（trapdoor），进入程序的一个秘密入口点。
- 泄露信息（leaks information）的程序使得非授权的人和程序能存取此信息。

当然，也有可能建立一个新程序并把它安装在计算系统中。对安装并运行在计算系统上的程序缺乏适当的控制则会发生这种软件安全攻击。

3. 软件盗窃

此种攻击包括非授权的软件拷贝。和音乐作品或著作的作者一样，软件制作者及发行者

有权对其产品的使用获取公平的补偿。尽管在此方面已采取了许多措施（参阅第10章），但是在阻止软件的非法拷贝方面并未收到令人满意的效果。

1.3.3 对数据的攻击：特别关心的领域

相对来说，除计算中心的专家外，很少有人对硬件的安全性加以考虑。而软件安全则是一个大问题，它涉及到所有建立或修改程序的程序员及系统分析员。计算机程序的书写最初是只有计算机专家才能掌握的工作，因此，即使“泄露”源程序清单对普通公众来说是不会有用的。

但是，打印的数据则可被普通公众所理解。由于社会的固有属性，因而对数据的攻击比对硬件或软件的攻击是一个范围更广且更为严重的问题。由于更多的人知道怎样使用及理解数据的含义，因而，数据项具有比硬件或软件更大的社会价值。

数据本身并不具有价值。因此，很难估价数据的价值。但是，数据具有价格，可以通过估价重组或重新开发所丢失数据的代价来计算。绝密数据泄露给竞争对手会大大增强其竞争力。最后，不完善的安全机制将使银行中的私人数据公诸于世从而导致金融犯罪。因此，尽管很难估价数据的价值，但它还是具有有限价值的。

相对来说，硬件和软件都具有较长的使用周期；并在其使用期内价值逐年下降。但是，数据的价值可能会很高，并且某些数据项仅只在特定短的时期内人们对它感兴趣。请看下面的例子。

政府分析员定期地产生有关国家经济方面的数据。其结果将在预定的日期及时间公诸于众。很显然，若某人提前获得有关信息，则他将根据此信息从股票市场获得丰厚的利润。假设分析员在公布数据24小时前生成好数据，并且他们希望在公布之前将结果送到其它分析员处进行验证，由于在24小时之后这些数据将不再保密，因此，有必要对这些数据采取必要的保护措施，以防泄露给旁观者。

对数据安全的研究产生了计算机安全的第二个原则。

时间性原则。计算机中的数据项仅在其无价值之前需要保护。

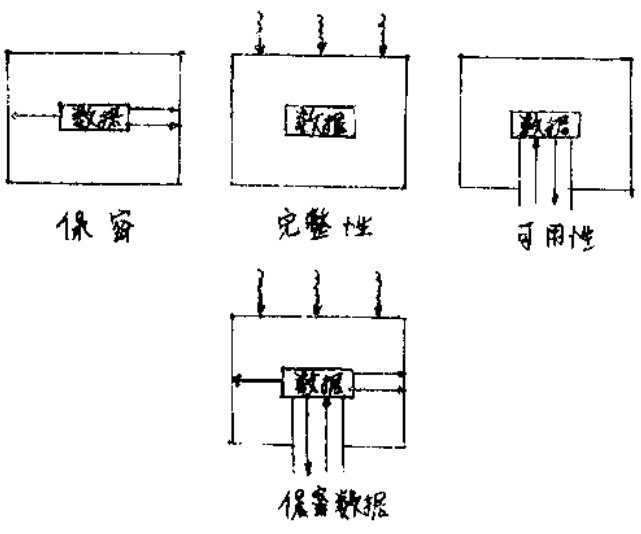

图1.4 数据的安全性

此原则说明了，采取安全措施保护的具有较短生命期的事物仅需在其较短生命期内采取安全措施。由于数据是计算机安全系统中具有最短生命期的元素，因此，此原则比较适合于数据保护。

图1.4给出了数据安全的三个因素：保密(防止非授权泄露)，完整性(防止非授权修改)以及可用性（防止非授权存取)

1. 数据保密

可以通过搭线窃听，在输出设备中产生故障，使用过滤器筛选，监测电磁波，收买关键雇员，从其它数据推出或简单请求等方法收集数据。由于数据以可读的形式出现，因此，数据的保密是计算机安全系统中主要关心的问题。

2. 数据完整性

偷窃、购买、查找或偷听数据无需任何计算机方面的知识，而修改或产生新的数据则不仅要了解数据传输或存储技术而且要知道所支持的数据格式。因此，修改当前数据或伪造新的数据而非截取当前数据需要更高层次的技巧。产生此类问题的主要根源是预先安置的程序、有错的文件、系统实用程序或有缺陷的通讯设施。

数据特别易遭到修改。很小的或很有技巧的修改是不可能通过通常的方法检测出来的。例如，罪犯可能会写一个程序将银行帐号下的每个用户的利息减去一分钱，然后将所收集到的钱存入到某一特定帐号下。每个顾客是不可能独立地计算他的利息的，而且顾客更不会由于怀疑一分钱的差错而将钱转出银行。这种攻击叫意大利香肠（salami）进攻术。此名称的由来是由于窃贼从许多帐号下偷窃很少很少的东西并将它们聚集在一块，从而形成一个有价值的整体，就跟聚集在意大利香肠中的肉屑一样。

更为复杂的处理则是试图对所使用的数据项重新加工。凭借银行之间的电传通讯，伪造者可能会截听到一条银行将一定数目的钱存入某一顾客帐号下的消息。伪造者可以试图模仿此消息，从而导致接收方银行认为它应该再次借贷给同一帐号。伪造者也可以将消息稍作修改，改变要贷款给的帐号或数目，然后发送已修改的消息。

1.3.4 其它易暴露的资源

计算系统易暴露的主要资源是硬件、软件及数据。但是，系统中的其它部分也可能成为暴露的目标。本节我们将讨论对其它资源的攻击。

1. 存储介质

尽管它们通常和硬件在一块，但它们是物理实体，因此，保存数据的存储介质仍是可能丢失的资源。有效的安全计划必须考虑数据有足够多的备份并对包含此备份的介质采取物理保护。

2. 网络

网络实际上是硬件、软件、数据这三种基本的计算系统资源的集合。网络中每个结点的计算系统面临着所有通常应考虑的安全问题。除此之外，网络还增加了一个通讯问题，即通过易暴露介质传输，以及从远程的、可能不可靠的计算系统中存取信息等问题。

网络大大地增加了安全系统的复杂性。缺乏物理邻接，非安全使用，共享介质以及识别远程用户都是计算机网络中更为复杂的安全问题。

3. 使用

另一种暴露则是计算机设备的使用。首先，侵入者可能只偷用计算机的时间来作计算。计

算机服务窃贼类似于电子设备的或其它设施的窃贼。但是，所偷窃到的服务的价值实际上大大高出偷窃电子设备的价值。这种不花钱的使用增加了计算系统中其它合法用户的实际开销。其次，对计算系统的有预谋的使用可能会破坏软件或数据。最后，非法使用可能会延缓一个合法用户的服务。例如，一个需完成费时任务的用户其任务的完成会大大依赖于计算系统的可用性。由于这三个原因，必须阻止对计算机系统的非法存取。

4. 关键人员

最后，人可能是安全中的关键弱点。若只有一个人知道怎样使用或维护某一特定程序的话，则在他病了、出事故或离职时会产生一系列问题。因此，对于可信赖的个人，如操作员或系统程序员，由于他们具有潜在地影响计算机用户的能力，因而必须认真选择。

1.3.5 总结

本节将计算系统中的三个基本脆弱性——保密性、完整性及可用性应用于计算系统的资源中。诸如数据丢失、数据泄露、服务盗窃、硬件失效、软件修改等问题都是满足这三个脆弱性的框架的。

本书的余下部分则是分析怎样操作并控制这些脆弱性。大多数控制工作在于利用这些脆弱性的人。下节讨论对计算机安全产生威胁的人。

1.4 卷入的人

计算机犯罪分子使用大量的硬件、软件及数据；他们对全世界的商业及行政管理具有潜在的威胁。

“计算机犯罪”就是任何通过使用计算机来进行的犯罪。

大多数专家意识到计算机安全是个主要问题。在计算机犯罪人员特性方面人们作了许多研究。这些研究用于发现可能的罪犯并阻止犯罪。下面是某些种类的计算机犯罪人员。

1. 业余爱好者

业余爱好者是当今主要的计算机犯罪者。大多数窃贼并非职业罪犯，而是观察到安全系统中允许他们存取现金及其它有价值东西这一缺陷的普通人。同一意义上讲，大多数计算机犯罪也是通常的计算机专家或用户，他们在发现能存取某些有用的东西时而进行犯罪。

在无人私自使用计算机设施时，业余者可能会启动计算机工作、写信、支持球队或记帐。这种情况一直持续到雇员继续记帐，股份有价证券管理、办公管理或使用雇主其它设施为止。另一方面，业余者可能会对消极的工作环境（如响应失败或过慢）不满意而通过在计算机安装时制造混乱进行报复。

业余计算机犯罪的问题是很少在其背景或获利方面能提供人们怀疑的东西。

2. 窃贼、攻击者、神童

系统窃贼通常是大学或高中学生，他们试图使用他们无权使用的计算机设施，进行业余对话，以此作为一种乐趣。它的后面则是电子屏蔽、安全及保密。

偷窃和攻击都是导致成百万美元损失的严重的进攻。由于巨大的损失而起诉罪犯。但他们对犯罪会继续有兴趣，特别是青少年更是如此。

3. 职业罪犯

职业计算机罪犯懂得犯罪目标。他们的犯罪范围不再是纵火、谋杀或对计算机进行偷窃。而更多的是他或她从参于计算机犯罪的计算机专家开始，找到攻击的可能性并实施攻

击。

某些公司不愿意起诉计算机罪犯；事实上，在发觉计算机犯罪之后，若罪犯悄悄退职，公司将会非常感激。于是，罪犯到另一家公司继续同一非法勾当。

1.5 防御方法

计算机安全的目标则是实施保密性、完整性及可用性的控制。有时，这些控制能够防止攻击，而其它威力较小的方法则只能在攻击发生时或之后检测缺陷。

1.5.1 控制

本节我们将介绍防止计算机系统脆弱性被利用的控制方法。

加密

提供给计算机安全最有效的工具是编码。通过转换数据使得外部观察者无法理解，从而使得截取者利用它进行修改或伪造的希望成为泡影。

加密使数据保密。而且，由于数据不能按通常方法读也不能被改变，因而，加密也可用于提高完整性。更进一步，加密的重点在于协议，它是为完成某些任务而协同一致的动作序列。某些协议保护资源的可用性。因此，加密是保证计算机安全的三个目标实现的所有方法的核心。

尽管加密在计算机安全中是一个重要的工具，但也不能过高估计其重要性。用户必须知道，加密不能解决计算机安全中的所有问题。而且，若加密使用不当，它可能会毫无用处，而且在实践中会降低整个系统的性能。因此，最重要的是了解使用加密的环境使之充分发挥作用。

软件控制

程序本身是计算机安全的第二道环节。程序的安全性必须足以排斥外来攻击。必须对程序进行开发及维护使得人们可以相信程序的可靠性。

程序控制包括下列几个方面：

1. 开发控制，指在什么标准下设计、编码及维护。
2. 操作系统控制，通过操作系统施加限制用来保护每个用户免受其他用户干扰。
3. 程序内部控制，施加安全约束，如在数据库管理程序中增加存取限制。

软件控制会采用诸如硬件设备、加密、或信息收集等方面的工具。软件控制通常直接影响用户，因此，通常它是安全系统给用户的第一印象。由于它影响用户和计算机系统打交道的方式，因此，软件控制的设计必须十分谨慎。易于使用及功能强大是软件控制设计中的主要目标。

硬件控制

多数硬设备在计算机安全中起着辅助作用。这些设备的范围从用于限制存取的加密硬设备到验明用户身份的防窃贼设备。

规章制度

如上面所述，某些对计算系统的控制通过加入硬件或软件设施来实现。而其它控制则是规章制度控制。事实上，某些最简单的控制，例如，频繁改变口令等则能达到有效控制的目的而不需任何花费。

法律及伦理控制是计算机安全的重要部分。法律很少变化，而计算机中的技术则是突然