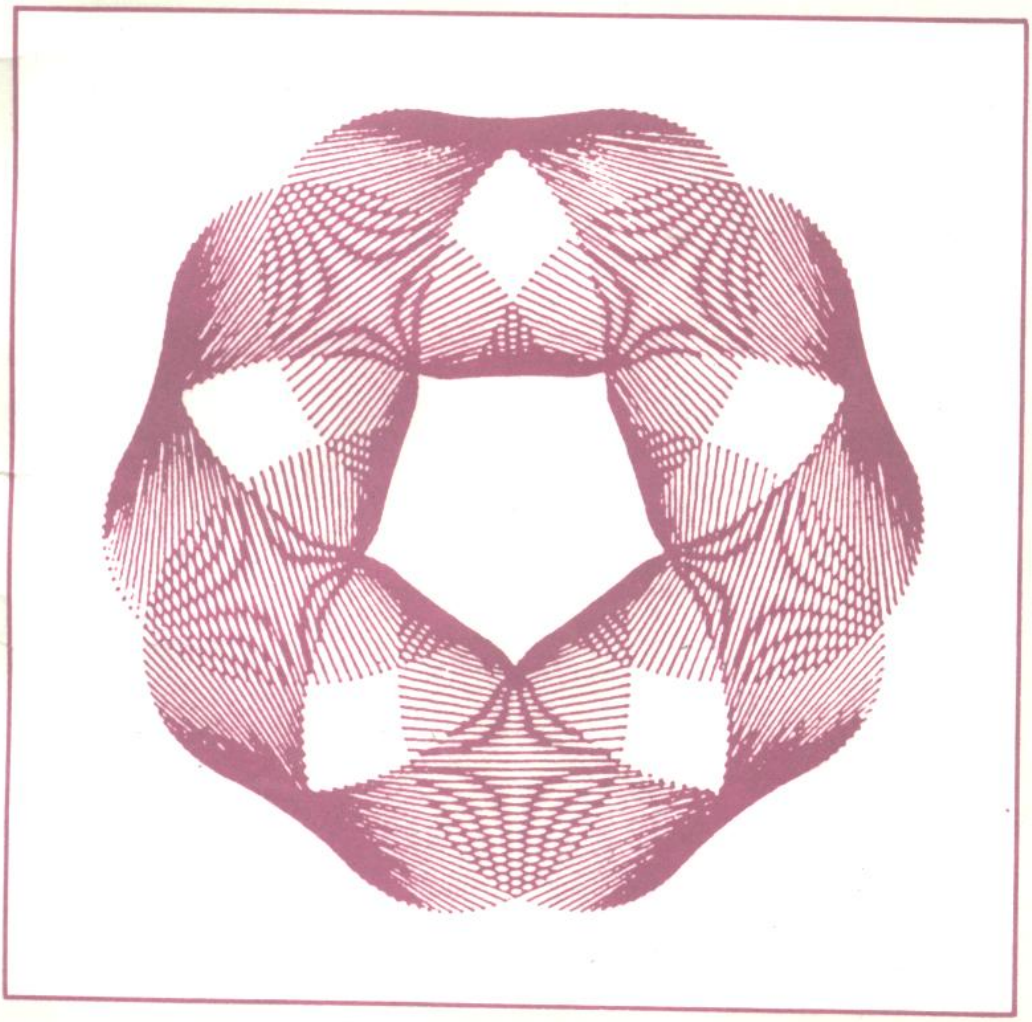
计算机的安全与保密

陈爱民　于康友　管海明　编著



電子工業出版社

计算机的安全与保密

Computer security and privacy

陈爱民　于康友　管海明　编著

電子工業出版社

内容提要

本书共分十三章，分别介绍计算机安全的基本要求、安全组织管理、实体安全、密码体制和加密技术、密钥管理、鉴别、访问控制、安全操作系统、安全模型、计算机网的安全体系结构与实现方法、数据库系统的安全保密、安全评估、计算机病毒。本书是作者在长期从事科研实践基础上编写的，内容广泛，深入浅出，可供广大计算机用户和管理人员、大专院校师生以及从事计算机安全保密研究和管理、技术人员参考。

计算机的安全与保密
陈爱民　于康友　管海明　编著
责任编辑　杜振民
*
电子工业出版社出版（北京市万寿路）
电子工业出版社发行　各地新华书店经售
北京顺义李史山胶印厂印刷
开本：787×1092 毫米 1/16　印张：24.25　字数：596 千字
1992 年 9 月第 1 版　1992 年 9 月第 1 次印刷
印数：1—10100 册　定价：14.00 元
ISBN7-5053-1701-6/TP・379

前 言

计算机已经渗透到了社会生活的各个方面。利用计算机对信息进行收集、加工、存储、分析以及交换等各种处理，越来越成为必不可少的手段。许多计算机处理的是涉及国家军政、经济、工商业情报以及一些私人数据等敏感信息，因此，它已成为敌对国家或组织及某些别有用心的人攻击的主要对象，所以计算机系统的安全问题越来越受到重视。危及计算机系统安全的因素很多，如硬件/软件工作不可靠，管理不善及用户有意无意的误操作，敌对者采用各种技术手段窃取、删改机密信息或破坏系统正常运行，以及计算机病毒等许多方面。如果不采取有效的安全防范措施，这些敏感信息以至整个系统的安全都将受到威胁，一旦受到攻击，将会对国家的政治、经济、军事、外交，以及一些使用部门和个人造成不可估量的损失。

目前国内还缺少全面、系统地介绍有关计算机系统的安全与保密问题的书籍，为了加快这方面的研究，普及这方面的知识，我们在多年来从事研究工作的基础上，参阅大量国内外的文献资料，编写了此书。旨在使管理部门、计算机应用、开发和使用人员都来重视安全保密问题，更多地了解计算机系统的安全与保密这门学科的基本原理以及它所涉及的范围，使读者在开发使用自己的系统时能够全面系统地考虑安全保密问题，使系统更加安全可靠。

全书共分十三章。

第一章介绍对计算机系统安全的主要威胁，计算机系统安全的主要意义和它的本质，描述了计算机系统安全与保密的三个主要方面，即，安全性、保密性和完整性。

第二章介绍人员安全素质，安全机构的设置和责任，以及为了保证计算机系统安全所必须制定的一些规章制度。

第三章介绍一些物理安全措施以及实施软件安全的主要技术手段。

第四章介绍传统的对称密钥密码体制和现代的非对称密钥密码体制(公开钥密码体制)的原理、设计原则以及目前的技术进展。

第五章讨论密钥的生成、保管、交换及注入等环节的要求和方法，介绍密钥的分层管理及密钥的秘密共享保管等基本的密钥管理模式的原理。

第六章讨论鉴别的意义，介绍了身份鉴别、报文鉴别、数字签名的原理及一般的实现方法。

第七章介绍访问控制模型，一般的访问控制技术的实现方法，如口令、访问控制表等等。介绍特洛伊木马的威胁以及针对一些特洛伊木马的强制性访问控制手段。同时还介绍了多级安全技术和隐蔽信道的概念。最后介绍信息流控制。

第八章介绍实现安全操作系统需要考虑的几个主要方面，对安全核方法作了详细的讨论，最后介绍了一个实例。

第九章介绍安全模型在设计安全的计算机系统中的作用以及开发安全模型需要遵守的一般规则。还介绍了形式描述技术，并给出一个范例。

第十章主要介绍计算机网络系统容易受到的威胁，网络系统的安全体系结构，网络加密技术和网络安全技术，还介绍了局域网的安全保密问题。

第十一章介绍数据库的一般概念，数据库的访问控制，数据库的完整性与一致性以及数据库的审计等，最后简单介绍了数据库的加密技术。

第十二章介绍可信计算机的一般概念，计算机安全等级的划分，每个等级需要的最低限度的要求，安全等级的评估等内容。

第十三章介绍计算机病毒的定义，对目前几种主要病毒的机理及传播方式作了说明，描述了计算机病毒与计算机操作系统的关系，最后介绍一般的病毒免疫及清除方法。

本书可供计算机管理部门、计算机应用、开发人员、大专院校师生以及专门从事计算机系统安全与保密的研究人员阅读，对于想了解这一学科内容、范围以及基本原理的人来说，也是一本适用的入门书籍。

本书第一、三、六、七、八、九、十三章由于康友编写，第二、十、十一、十二章由陈爱民编写，第四、五章由管海明编写。李德毅博士对本书进行了审阅修改。由于时间仓促，作者水平有限，不足之处在所难免，敬请各位读者批评指正。

作者

一九九二年二月于北京

目　录

第一章　计算机安全的基本要求

在当今科学技术飞速发展的时代，信息已成为推动社会向前发展的巨大资源。由于电子技术的不断发展，处理信息的技术手段也在不断地提高。许多业务变得越来越依赖电子信息处理了。但信息资源又有别于其它资源，它的脆弱性更加明显。一般的资源一旦被一人占有其他人就不能再占有，即它的利用只是一次性的。而信息资源不同，它可以同时被许多人占有而共同利用。

现在，大量的数据信息被集中和存储在大型的计算机数据库中，并在与综合通信网相连的计算机及终端设备之间传送。如果没有适当的安全措施，这些信息在传输过程中就易被截收，或在存储时被取出和复制，造成信息的泄露，产生保密隐患。另外，信息在存储和传输期间还会受到非法删除、更改或增添，从而导致对计算机资源及计算机服务的非法干预与使用，对个人数据、商业记录以及政府或军事信息的篡改与窃取。

计算机本身固有的脆弱性也在不断地被利用。计算机硬件设备易受自然灾害与人为灾害的破坏，工作期间各种硬件设备会向外辐射电磁波，从而产生信息泄露；另外，如果受到外界电磁场的干扰，也很容易破坏系统的正常运行，导致大量信息出错甚至丢失。计算机系统软件易受到各种各样的攻击，如有价值的软件可以很容易被非法复制；利用计算机操作系统的弱点可以对系统资源进行非法的使用；对系统软件的修改可以导致敏感信息的泄露，也可能对个人带来非法的经济收入等等。

在国家的金融、商业、文化教育、科研、工农业生产、交通运输、公安及军政等诸多部门中，已使用了大量的计算机系统，可以说计算机目前几乎已渗透到了社会的各个方面。对于计算机系统中的机密信息、个人数据以及工商业情报等必须采取有效的安全防范措施，否则这些信息一旦被非法窃取或删改，将产生难以估量的损失。

1.1　计算机系统安全的本质

在现实社会里，每天都会遇到各种各样的威胁，这些威胁来自各个方面，有我们自身的弱点以及各种失误产生的，有各种设施、设备的失常造成的，也有各种自然灾害引起的。这些威胁的一个共同特点是“被动的”，或者说是偶然的。对于这种威胁，一般可以采取一定的预防措施，以尽量避免这些意外事件的发生或者减少事故发生后的损失。最危险的一类威胁是“主动性”的威胁。所谓主动性的威胁是指由人故意做出的。这些人可能出于各种各样的目的，他们的目标就是要使对手蒙受损失或使自己获得某种非法利益。

一个计算机系统涉及到很多的因素，有人、各种设施与设备、计算机系统软件与应用软件、计算机系统内存储的数据、各种供给品等等。计算机系统安全的本质就是要保证这些因素能够发挥它们的正常作用，避免各种偶然的和人为的破坏与攻击，保证系统安全可靠地工作。它包括以下几方面的内容：

①要保护系统内的各种资源免遭自然与人为的破坏。

②要明确计算机系统的脆弱性与它的弱点。

③要估计到对计算机系统的各种威胁，以及它存在的特殊问题。

④要开发与实施卓有成效的安全策略，尽可能减小系统所面临的各种风险。

⑤要准备适当的应急计划，使系统遭到破坏或攻击时能够尽快恢复正常工作。

⑥要定期检查各种安全管理措施的实施情况与有效性。

不同的计算机系统有不同的安全要求，这要根据它的作用以及在受到破坏与攻击时所造成的损失来决定，这方面并没有一个统一的标准。从理论上讲，一个计算机系统越安全越好。但从实际上看，为安全而采取的措施越多，成本就越高。所以，要根据实际情况采取相应的措施，使系统的性能价格比达到一个合理的水平。

1.2 计算机系统的脆弱性和面临的主要威胁

计算机安全的主要目的是保护存储在系统中的电子信息，这些信息有三个特性：

①完整性。完整性是指信息必须按它的原型保存，不能被非法修改，无论这种修改是偶然无意的还是恶意的。完整性是对信息的精确性与可靠性的度量。

②可用性。无论何时，只要需要，信息必须是可用的。

③保密性。信息必须按拥有者的要求保持一定的秘密性。只有得到拥有者的许可，其他人才能够获得该信息，必须防止信息的非授权泄露。

正是信息的这些特性构成了计算机系统安全策略的基础。计算机对电子信息提供的保护，至少应与其它方法对非电子信息提供的保护达到一样的程度。然而，由于电子信息比其它形式的信息面临着更大的威胁，所以计算机安全更严格。无论对电子信息采用什么样的安全措施，都必须考虑到计算机系统的脆弱性与计算机系统面临的各种威胁。

1.2.1 计算机系统的脆弱性

计算机本身存在着一些固有的弱点与脆弱性，非授权用户利用这些弱点可以对计算机系统进行非法访问，这种非法访问会使系统内存储信息的完整性受到威胁，也可能使信息遭到破坏而不能继续使用，更为严重的是可以窃取有价值的信息而不留任何痕迹。另外，计算机系统还易受各种自然灾害以及各种误操作的破坏。计算机系统的脆弱性主要表现在以下几方面：

(1)存储数据的密度极高

在一块磁盘或一卷磁带中，可以存储大量数据信息，而一块磁盘很容易放在口袋中带出办公室，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)数据泄露

计算机系统工作时能够辐射出电磁波，任何人都可以借助并不复杂的设备在一定的范围内收到它，从而造成信息泄露。这种电磁辐射在任何电子设备中都是存在的。

(3)数据的可访问性

电子信息可以很容易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接到计算中心的系统上，在一定条件下，他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。

(4)磁性介质的剩磁效应

保存在磁性存储介质中的数据可能会将存储介质永久性地磁化，所以存储介质中的信

息有时是擦除不净或不能完全擦除掉的。当将一块存储过机密信息的磁盘消密时，首先要做的就是将其中的数据擦掉。如果这种擦除不彻底的话，其中就会留下可读信息的痕迹。一旦被利用，就会产生泄密。另外，在大多数计算机操作系统中，删除文件仅仅是将该文件的文件名删除，并将相应的存储空间释放，而文件的真正内容还原封不动地保留在存储介质上，利用这一点可以偷取机密信息。

(5)信息的聚生性

当信息以分离的小块形式出现时，它的价值往往不大。当将大量相关信息聚集在一起时，方显出它的重要性。计算机的特点之一就是能将大量信息收集在一起，所以这种聚生性与计算机系统的安全性是密切相关的。特别是计算机能够对收集到的信息进行自动、高效的处理，这就会产生很有价值的结果。

(6)计算机的神秘性

除了专业的计算机工作人员以外，大部分人很少能够理解甚至是最简单的计算机的工作情况，这就给计算机蒙上了一层神秘的面纱。所以对于没有多少专业知识的管理与安全人员来说，可能看不出或觉察不到围绕着计算机的渎职与犯罪行为。

(7)保守秘密的困难性

一旦获得了对计算机系统的访问权，一般说来计算机系统内的所有数据都是可用的。虽然可以利用许多方法在软件内设置一些关卡，但对于一个谙熟系统的人来说，多下些功夫就可能突破这些关卡，所以要保守秘密很困难。

(8)通信与网络的弱点

随着技术的不断发展，越来越多的计算机连接在一起而形成计算机网络。现代的计算机本身就经常是由几个规模较小、分布式的处理器连接在一起的。连接系统的通信线路面对各种威胁就显得非常脆弱。典型的威胁有：对线路的物理破坏，不管是蓄意的还是偶然无意的；线路可能被搭线窃听；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等。所有这些威胁都是通过网络的通信线路产生的。

计算机系统本身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，就可能蒙受很大的损失。

1.2.2 对计算机系统安全的主要威胁

计算机系统的脆弱性直接构成了对系统的威胁，这些威胁可以分成三类：

(1)偶然无意的

有许多威胁是由于偶然的原因产生的。

①设备的机能失常

任何一种设备都不是十全十美、万无一失的，或多或少都存在着这样或那样的缺陷。有时会出现一些比较简单的故障，而有些则是灾难性的。有些简单故障，特别是周期性故障往往比那些大的故障更难于查找与修复。有些故障是当它们已经破坏了系统数据或其它设备时才被发现，而这时往往为时已晚，后果也是非常严重的。

②不可避免的人为错误

人比机器更容易犯错误，由于各种不经意或不小心的操作，可能会对系统产生特别严重的后果。心理学的研究表明，在最担心出错的地方，就肯定会有人出错。由于不小心、经验不

足以及对操作的错误理解都可能产生不良的后果。所以在设备的安装与操作过程中要尽量减少人的干预，最大限度地避免发生人为错误。有些人为错误是很难查找与清除的，特别是在软件开发过程中。即使是非常有经验的程序员也免不了由于疏忽而在软件中留下某种漏洞或逻辑错误，这对于系统软件来说非常危险，它可能危及整个系统的安全。

③软件的机能失常

对于一个软件，特别是较大的系统或应用软件来讲，要想进行全面彻底的测试是不可能的。随着应用要求不断提高，软件功能也越来越强，一个程序可能包含数百万条计算机指令，以及数不清的常数与变量。虽然在设计与开发过程中可以进行某些测试，但总是会多多少少留下某些"缺陷"，这些缺陷可能长时间也发现不了，只有当被利用或某种条件得到满足时，才会显现出来，而这时往往已经产生了意想不到的后果。

④电源故障

由于各种意外的原因，计算机设备的供电电源可能会突然中断或者产生较大的波动，这可能会突然中断计算机系统的工作。如果这时正在进行某些数据操作，这些数据就可能会出错或丢失。突然断电对系统硬件设备也会产生不良后果。

(2)自然灾害对计算机系统的威胁

计算机是一种易碎品，不能受重压或强烈的震动，更不能受强力冲击。所以各种自然灾害，如地震、风暴、泥石流、建筑物破坏等，对计算机系统构成了严重的威胁。另外，计算机设备对环境的要求也很高，如温度、湿度、各种污染物的浓度等等。所以要特别注意像火灾、水灾、空气污染等对计算机系统构成的威胁。

(3)对计算机系统的人为攻击

只要计算机系统存在着各种弱点，那么就总是有人或某个组织甚至是一个国家想方设法去利用它达到某种目的。从计算机设计的初衷看，它是无法避免这些利用的。从事工业、商业或军事情报收集工作的间谍对相应领域的计算机系统是最感兴趣的，这些威胁都具有明显的主动性，所以它们是对计算机系统安全构成的最主要的威胁。下面简要地介绍几种主要的人为攻击。

①情报机构

在军事领域中，对计算机系统的主动攻击主要来自敌方情报机关的间谍，为了达到军事目的，他们会想方设法去获取对方的各种军事情报。现在，这些情报往往都是利用计算机进行收集、加工、存储以及传输的，所以这种间谍活动对这类计算机系统是一个潜在的威胁。同样，在工商业界也存在着这种问题。

②雇员

如果有内部人员，如雇员的帮助，那就很容易获得对计算机系统的非法访问权，就会构成特别严重的威胁，正所谓"家贼难防"。

③用户

用户的不法行为或渎职行为可能会产生破坏性的后果，用户可能由于各种原因而进行一些非授权的操作，这些操作对系统及其数据会产生直接的影响。在计算机上玩各种游戏或一些消遣性的程序不仅会占用系统宝贵的时间和资源，而且对系统安全也构成了威胁。例如，现在有许多计算机病毒就是利用游戏程序广泛传播的。

④计算机犯罪

计算机犯罪已经越来越多地出现在金融系统中。罪犯们往往是具有一定专业知识的雇员，或者是对计算机系统非常熟悉的人。关于这类犯罪情况，目前还没有准确的记录。由于各种各样的原因和顾虑，受害者们一般不愿透露所受的损失。但可以肯定地说，计算机犯罪所造成的后果是很严重的。

1.3 计算机系统安全保密的三个主要方面

针对计算机系统安全的威胁，计算机系统安全保密主要涉及三个方面的内容，即，安全性、完整性与保密性。

1.3.1 安全性(security)

安全性大致包括以下几个方面的内容：

(1)内部与外部安全(internal and external security)

内部安全是在系统的软、硬件及周围设施中实现的。内部安全控制措施虽然是有效的，但它们必需与适当的外部安全控制措施相结合。

外部安全可以分成三类：

①物理安全(physical security)；

②人事安全(personnel security)；

③过程安全(procedural security)。

物理安全是解决计算机设备中心安全问题的不可缺少的一部份，包括对计算机中心设备与设施加建筑防护措施(如建立防护围墙)，加警卫人员，终端上锁，安装防电磁泄射的屏蔽设施等。但是，单单使用物理安全控制措施还不能解决分布系统的安全问题。随着计算机网络节点的不断扩充，物理安全的作用在不断地减少。我们不可能保证任何系统都有完备的物理保护措施。

人事安全是对某人参与计算机系统工作和接触敏感信息是否值得信任的一种审查手段。

过程安全包括：准许某人对机器的访问、处理物理输入输出(诸如打印输出，磁带、磁盘拷贝等)、装入系统软件、连接用户终端以及许多其它日常系统管理工作。

内部和外部安全措施相辅相承，交替使用。例如，当今最基本的多用户系统都有口令保护。口令保护是一种内部安全措施，它可以加强外部安全措施。在设计一个安全系统时，应力争最大限度地减少对外部安全措施的依赖，因为外部安全实现起来往往是非常昂贵的。

(2)系统边界与安全防线(the system boundary and the security perimeter)

一个系统是一个模糊的实体，它包括开发者进行某些控制的计算机和通信环境的总和，系统内的所有软、硬实体都由系统来保护，而在系统外的软、硬实体则未加保护。要想建立一个安全的系统，十分重要的一个问题是要对系统的边界有一个清晰的理解，并要保证系统在受到威胁时能够保护自己。如果对这些威胁没有一个清晰的理解，那就不可能构造出一个令人满意的安全环境。系统边界与安全防线，如图 1.1 所示。

确定系统边界要根据系统与外界的接口而定。外部安全措施将加固这个接口。只要内部安全措施恰当，那么它将保护系统内的信息免遭威胁。然而，如果外部非法用户通过了外部安全控制并且进入了系统，或者系统遭到了意料不到的外部威胁，那么所有的外部措施都

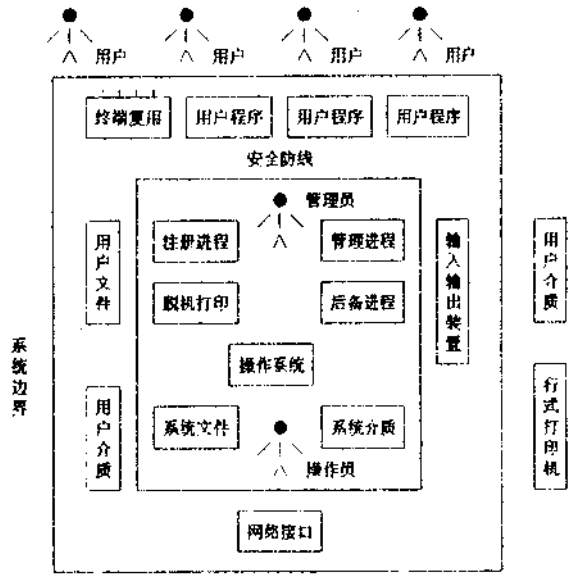


图 1.1 系统边界与安全防线

无济于事了。例如，一个非法用户进入了机房并能在控制台上输入命令，或者系统管理员向外界泄漏了口令，那么外部安全控制措施就完全失去了作用。然而，只要根据系统接口规则能够限制非法用户进入系统，那就可以挫败未经确认的终端或其它用户的侵入。

系统内的组件可分成两类，其中负责维护系统安全的，称为安全组件，其余的称为非安全组件。安全组件实现内部安全，分离这两种组件的界线可以形象地称其为安全防线。操作系统和计算机硬件通常都位于安全防线内。安全防线外一般是用户程序、数据、终端、调制解调器、打印机等由系统控制和保护的一类组件。在安全防线内，组件的性质必须予以精确的定义，因为任意一个组件的一个微小的机能失常都可能破坏系统安全性。反之，在系统安全防线外的组件是相当任意的，仅当它们通过系统边界时受到一些限制。在安全防线内的某组件如果有机能失常现象，将可能导致把系统安全防线扩充到系统边界的危险，使得原来在系统安全防线外的组件进入安全防线内。

正如通过系统边界的接口需要精确地加以定义一样，对通过安全防线的接口加以精确定义也是至关重要的。这个接口由安全组件加以限制。例如，操作系统中的系统调用表或者通信线路的电气参数就是进入安全防线的接口。只要系统边界由外界加以限制，安全防线将由安全组件加以维持。为了实现边界内的安全组件，必须仔细地定义一个完备的、连贯的以及受限制的安全防线接口规则。

(3)防止用户泄密(protecting the user from self—betrayal)

系统必须保证拥有或制作系统内某份信息的用户不会向不该知道这份信息的用户泄密。很明显，如果信息的拥有者想把这份信息泄漏出去，那么无论多么安全的计算机系统都不可能保护这份信息。但人们往往无视这个事实。可以设计一种系统来保证不允许用户对它们的信息进行其它方式的访问操作，不管是否有意。但这样的设计也很脆弱，因为一个打算泄密的用户完全可以不需要计算机来参与，有能力阅读一份文件也就等于他有能力把这份文件泄露给他人。所以，对系统的访问控制一定要有一个良好的工程用户接口，以最大限

度地防止用户意外泄密事件的发生。

(4)识别与确证(identification and authentication)

为了保证系统(用户)有充分的能力来判断是否允许某个用户访问某个文件,系统(或其它用户)必须有识别每个用户的手段。

唯一识别符(unique identifier,以下简称 ID)是一个用户名(诸如姓名、首字母缩写、银行帐号),没有人能够伪造或更改。所有的访问请求都可以由它来检验。识别符必须是唯一的,因为它是系统与用户打交道的唯一途径。因此,为确保一个用户不能假冒另一个用户,识别符必须是不可伪造的。

把一个用户(更精确地说是一个用户运行的程序)与唯一识别符相结合的过程称为确证。确证过程总是需要用户输入一个口令,当然也可采用更先进的技术(诸如指纹鉴别器)。识别过程(将某个用户的 ID 与一个程序相结合)与确证过程(将实际用户与这个用户的 ID 相结合)很容易混淆。但是区分它们之间的差别是很重要的。系统必须最大限度地隔离确证信息(口令)与识别信息(唯一的 ID)。因为口令是秘密的,但用户的 ID 是非秘密的,仅当用户第一次对系统进行访问时需要提供口令,一旦唯一的 ID 被确证,系统就不再需要口令。换言之,在进行访问判决时要多次使用 ID。由于系统的安全完全依赖于口令的保密程度,所以使用口令的场合与次数愈少,暴露它的危险就愈小。

识别与确证是涉及系统、程序以及用户的一个总的过程。用户可能需要知道它正在与哪个系统或系统中的哪个程序打交道。它们必须通过一种系统与程序都不能伪造的途径来获得这些信息。因而,网络中的系统需要彼此确证,仿佛每一个都是另一个的用户。在许多情况下,一个程序冒充另一个程序或一个系统冒充另一个系统的能力是安全系统十分关切的严重问题。系统间与程序间的确证技术和用户与系统间的确证技术是完全不同的,这种情况下利用口令确证技术是非常脆弱的,因为系统或程序每次使用口令都会导致口令对接收者的泄露,因而存在着潜在的危险。

(5)可信系统(trusted systems)

虽然我们必须相信用户能够保证他们访问的数据的安全,但是对于他们运行的计算机程序来讲情况就完全不同了。大家都知道对计算机程序是不能完全相信的,无论对某个用户是多么地信任,也不能让他的程序完全自由地使用敏感信息,最好的程序员也承认,他们的程序有时也会出错。

软件可以粗略地分成三种类型

①可信的(trusted)

这类软件负责实施系统安全。因此,系统安全完全依赖于它的正确无误的操作。

②良性的(benign)

这类软件不负责实施系统安全;但是,它可以利用特权访问某些敏感信息。所以必须确信它不会有意地破坏系统安全规则。我们姑且认为良性软件中的缺陷是无意的。这些缺陷不应影响系统安全。

③恶性的(malicious)

这类软件来源不明。从安全角度来看,它是一类恶性的、试图暗中破坏系统的软件。例如,某些病毒程序就是恶性的。

这三类软件的质量在不同的系统中变化较大。我们日常使用的大部分软件都是良性的,

无论软件是由优秀的程序员编写的还是由不太熟练的程序员编写的，也不论它是系统程序还是应用程序。虽然这类软件不是恶性的，程序员也不想欺骗用户，但由于它们对实施系统安全并不负责，所以这类软件还是不可信的。因此，某个系统完全相信的软件，在另一个系统中就如恶性程序一样是不可靠的。在一个系统内，不可能完全地区别一个恶性程序与一个良性程序，也无法保证一个有缺陷的良性程序不会泄露或破坏数据，无意中它可能会产生恶性程序的效果。由于缺少一种客观地描述这种差别的方法，所以我们经常（但不总是）认为在一个目录下的良性与恶性程序都是不可信的，这种解释在处理特别敏感信息的环境下是很普遍的，它构成了建造系统安全核的基本准则。

在大多数情况下，操作系统是可信的，而用户程序与应用程序是不可信的。所以，设计系统时，要保证不可信的软件不能损害操作系统，甚至对恶性的软件也是如此。只有当系统的全部操作系统以及操作系统外的大部分软件都是可信的，整个系统才是安全的。

当我们谈到在一个安全的操作系统内的值得信任的软件时，首先认为它是由可信任的个人或组织按照一个限定的标准编写的。其次，要借助诸如规范模型等工程技术手段对它有一个正确的描述与验证。

对一个安全操作系统信任的标准远远高于现存的大部分操作系统的标准，它们实现起来往往非常昂贵。因此，应当通过尽量减少必须可信的软件的数量来设计一个安全系统，可信软件仅仅是安全防线内的安全组件部分，它的任何一个错误都可能对系统安全产生不利的影响。不信任软件不属于安全组件的任何部分，并且位于安全防线以外，它可能保持系统的运行但它不应破坏系统的安全。

在一个单机系统内，将可信软件划分成不同的信任等级一般来讲是没有意义的。把一些安全组件程序看得比另外一些安全组件程序更值得信任并不好，因为它们中的任何一个都可能破坏系统。类似的，也应尽量避免设立不同的不信任等级。在绝大部分常规系统中，安全防线并没有精确的定义，然而，区分良性与恶性程序还是很有意义的。在有些情况下，某些程序的不正常运行也不会破坏系统的安全，但是，如果它们是恶性的，那么它们就会毫无声息地留下损坏系统的隐患。

(6)特洛伊木马(Trojan Horses)

大部分损坏系统的恶性程序都涉及到一个从远程终端编写与运行该程序的用户(侵入者)。系统肯定能够抵御这类直接的威胁。但是另一类恶性程序，我们称其为特洛伊木马，并不需要终端上的一个活动用户。一个特洛伊木马是一个程序或子例程，它们伪装成一个友好的用户程序，由一个值得系统信任的人来运行，看起来仿佛是一项合法的工作。一个特洛伊木马可以镶嵌在文字处理程序、编译程序或游戏程序中。一个有效的特洛伊木马对程序的输出没有明显的影响，它的破坏作用可能永远也检查不出来。在一个文本编辑程序中的一个简单的特洛伊木马的例子是：它可以小心谨慎地把用户要编辑的所有文件都拷贝一份并存在一个特定的地方，入侵者(编写特洛伊木马的人)事后可以访问这些拷贝。一旦一个毫不受怀疑的合法用户随意访问某些文件，那么系统就毫无办法防止特洛伊木马的任何动作，因为系统不能区分特洛伊木马与合法程序。文本编辑程序中的一个更高级的特洛伊木马是：它不必限制自己只对用户编辑的文件进行拷贝。用户在编辑过程中潜在访问的所有文件对特洛伊木马来说都是可以访问的。

特洛伊木马之所以能够工作，是因为由某个用户运行的任意一个程序，通常都继承了相

同的唯一标识符、特权和作为一个用户的访问权，因而，特洛伊木马能在丝毫不侵害系统安全规则的情况下工作，这是最难查找的威胁。

(7)访问控制(access control)

在计算机系统中，安全机制最基本的任务就是访问控制。它主要有三个任务：

①授权(authorization)

决定哪个主体有资格访问哪个客体

②确定访问权限(determining the access rights)

决定是否有权读、写、运行、删除以及附着(append)

③实施访问权限(enforcing the access rights)

在一个计算机系统中，访问控制仅指本系统内主体对客体的访问控制，不涉及访问本系统外的其它系统。访问本系统外的其它系统的访问控制技术属于用户识别与确证的范畴。所以，在一个计算机网络中，访问控制不仅要涉及本系统内主体对客体的访问控制，而且还要涉及对外部系统以及远程系统的访问控制。

系统可以实现多种类型的访问模式，安全系统通常集中区分读与写之间的差别。但是定义一些诸如删除文件、将文件写入全"0"、向文件写入随机数以及在文件末尾附着一些信息等的访问模式也是有意义的。

对客体的访问权由主体授予与撤销。通常，一个具有能力修改对客体访问权的主体被认为是这个客体的拥有者，但对一个客体可能有多个拥有者，并非所有系统都能确切地识别一个客体的所有拥有者。所以，通常是主体而不是客体的拥有者，有授予访问这个客体的权力的能力。

与每个客体相关联的是一个用以决定确证和访问权限的安全属性的集合。一个客体的安全属性可能只需两个比特(一比特确定读，一比特确定写)就可以指明所有主体对这个客体的访问模式。另一方面，某一客体的安全属性可能是比较复杂的，它可能有一个很长的访问控制表，该表标明不同的主体以及它们对该客体的访问权限。

有些系统不仅对客体分配安全属性，而且，对主体也分配安全属性。主体的安全属性可以包括识别符、使用它们的安全层、以及确证数据基。

有些系统不使用主体与客体的安全属性作为访问控制的依据，而是利用权力表。一种权力就是对客体的一把钥匙，如果一个主体具有这个权力，它就能够访问这个客体。主体可能会有一个很长的权力表。

在实现访问控制时，需要区分授权(在高层实现)与实施权限(在访问时实现)之间的差别。因为在未发生非法访问事件时，系统安全并未遭到威胁。例如，将一份秘密信息放入一个公开文件中，在没有未确证的用户读它时，对这份信息并不会产生任何损害，但是由于它存在公共文件中，所以，对它的安全问题留下了隐患。这种差别可能是很微小的，但是有些系统设计要求在授权时使用某些控制，而在使用访问权时使用另一些不同的控制。

(8)审计跟踪(auditing trail)

在一个计算机系统中，审计跟踪对使用何种系统资源、使用时间、如何使用以及由哪个用户使用等问题提供一个完备的记录，以备非法事件发生后能够有效地追查，它是对系统安全实施有效监控的一种重要手段，它是在终端进入系统进行各种操作时自动进行的。审计跟踪记录一般包括以下内容：