自主访问控制：

客体的属主对自己的客体进行管理，由属主自己决定是否将自己的客体访问权限或部分访问权授予其他主体。

用户可以在自己的意愿下，有选择地与其他用户共享他的文件。

强制访问控制：

有操作系统约束的访问控制。

主体是一个进程或线程。对象可能是文件、目录、TCP/UDP端口、共享内存段、IO设备等。

主体和对象个字具有一组安全属性。每当主体尝试访问对象时，会由操作系统内核强制实施授权规则——检查安全属性并决定是否可进行访问。

客体重用：

计算机信息系统可信计算基的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤销客体所含信息的所有授权。

实例：IT部对所有的新员工、调岗员工分配计算机之前，将计算机中原存有的所有信息另做备份后进行彻底删除

审计：

信息安全审计主要是指对系统中与安全有关的活动的相关信息进行识别、记录、存储和分析。信息安全审计的记录用于检查网络上发生了哪些与安全有关的活动，谁（哪个用户）对这个活动负责。

安全操作系统主要特征：

1 、最小特权原则，即每个特权用户只拥有能进行他工作的权力； 2、自主访问控制；强制访问控制，包括保密性访问控制和完整性访问控制； 3 、安全审计； 4 、安全域隔离。只要有了这些最底层的安全功能，各种混为“ 应用软件 ” 的病毒、木马程序、网络入侵和人为非法操作才能被真正抵制，因为它们违背了操作系统的安全规则，也就失去了运行的基础。

安全内核

安全内核是指计算机系统中，能根据安全访问控制策略访问资源，确保系统用户之问的安全互操作，并位于操作系统和程序设计环境之间的核心计算机制。

         毕巴模型用完整性级别来对完整性进行量化描述。设i­1和i2是任意两个完整性级别，如果完整性级别为i2的实体比完整性级别为i1的实体具有更高的完整性，则称完整性级别i2绝对支配完整性级别i1，记为：i1< i2

毕巴模型定义了信息传递路径的概念。

“写”和“执行”操作（规则1）

①   当且仅当i(O) ≤ i(S)，主体S可以写客体O。

②   当且仅当i(S2) ≤ i(S1)，主体S1可以执行S2。

“读操作”

对于“读”操作，通过定义不同的规则，毕巴模型呈现为三种略有不同的形式。

1. 毕巴低水标模型（Low-Water-Mark）  
   设S是任意主体，O是任意客体，imin = min(i(S), i(O))，那么，不管完整性级别如何，S都可以读O，但是“读”操作执行后，S的完整性级别被调整为imin。
2. 毕巴环模型（Ring）  
   不管完整性级别如何，任何主体都可以读任何客体。
3. 毕巴严格完整性模型（Strict Integrity）  
   在满足规则1的基础上，当且仅当i(S) ≤ i(O)，主体S可以读客体O。在严格完整性模型中，当且仅当主体和客体拥有相同的完整性级别时，主体可以同时对客体进行“读”和“写”操作。

假定系统中有H和L两个进程，H的安全级高于L的安全级。H中隐藏有特洛依木马试图泄露信息给窥探者L，但是按照强制访问控制的策略，L无法访问到H的信息，因此H不敢直接传送信息给L，并且也担心审计的监督，于是H和L寻求利用系统的安全漏洞，采用表面上合法的手段泄露信息。

L开辟一个属于自己的文件目录，H合法地具有了读这个目录的权力，假定磁盘上从51磁道到第59磁道属于这个目录，H和L按以下约定进行操作：

1．  L请求读磁道55（此请求完成后，释放CPU）；

2．  H请求读磁道53（送“0”）或读磁道57（送“1”）（请求完成后，立即释放CPU）；

3．  L同时请求读磁道51和磁道59，并观察这两个请求完成的先后次序，以确定H发出的信息，若访问磁道51先完成，则L确认收到“0”，反之，L确认收到“1”。

重复以上操作，就可以在H和L之间传送连续的比特流。（当然还要采取一定的同步措施）