**第五章习题答案**

**1.名词解释：访问控制，自主访问控制，强制访问控制，基于角色的访问控制，基于任务的访问控制和基于属性的访问控制。**

**参考答案：**

访问控制是对主体访问客体的能力或权力的限制，它包括四个要素：主体，客体，引用监控器和访问控制策略。

自主访问控制：资源（客体）的所有者（主体）即为该客体的属主，每个客体有且仅有一个属主。属主能够根据自己的意愿将该资源的访问权限子集直接或间接地分发给其他主体，或从其他主体收回，不受任何安全策略的限制，即在自主访问控制之下。一个主体的访问权限具有传递性，同时，资源的拥有者能够自由选择与其共享资源的主体。

强制访问控制：普通用户不再具有资源的管理权限。系统（如系统管理员）为每个主体（或进程、用户）和客体（资源）赋予一定的安全属性，任何主体不能改变自身、任何主体或任何客体的安全属性，即只有系统管理员才能确定用户或用户组的访问权限。

基于角色的访问控制：系统操作的各种权限不是直接授予具体的用户，而是在用户集合与权限集合之间建立一个角色集合。每一种角色对应一组相应的权限。一旦用户被分配了适当的角色后，该用户就拥有此角色的所有操作权限，但用户不直接与权限关联。

基于任务的访问控制（TBAC）采用“面向任务”的观点，从任务（活动）的角度建立安全模型和实现安全机制，在任务处理的过程中提供动态实时的安全管理。在 TBAC 中，对象的访问权限控制不是静止不变的，而是随着执行任务的上下文环境发生变化，因此，它是一种主动访问控制模型。

基于属性的访问控制（ABAC）是通过对实体属性添加约束策略的方式实现主、客体之间的授权访问。ABAC 模型以属性为最小的授权单位，替代基于角色的访问控制模型中以身份标识为依据的授权方式，以满足开放网络环境下资源访问控制的要求。

**2.访问控制遵循的基本原则是什么？举例说明。**

**要点：（1）遵循最小特权、最小泄漏、多级安全原则。（2）举例的要求：最小特权应强调权限的最小划分，以保证对主体权力最大限度的限制，同时又不影响主体的功能实现；最小信息泄漏需要说明只有必要的信息被主体知道，是在主体确定做某件事之前把信息分配给主体；多级安全原则强调安全等级的划分，并基于安全等级限制信息的流动。**

**参考答案：**

访问控制策略的制定必须体现主体、客体和访问规则集等三者之间的关系，遵循的原则如下：最小特权原则。在主体执行操作时，按照主体所需权力的最小化原则分配给主体权力。其优点是最大限度地限制了主体行为，可避免来自突发事件、操作错误和未授权主体等意外情况的危险，即为了达到一定目的，主体必须执行一定操作，但只能做被允许的操作。最小泄漏原则。主体执行任务时，按其所需知道的最小信息分配主体权限，防止信息泄密。多级安全原则。根据主体和客体之间流动的数据安全级别，将主、客体划分成 5个安全等级：绝密（TS），秘密（S），机密（C），限制（RS）和无级别（U）。信息不允许从高安全级别向低安全级别流动，具有安全级别的信息资源，只有高于安全级别的主体才可访问，这样可以避免敏感信息扩散。

最小特权原则体现于惠普的Praesidium/Virtual Vault。它通过以最小特权机制将根功能分成42种独立的特权，仅赋予每一应用程序正常运行所需的最小特权。因而，即便一名黑客将Trojan Horse(特洛伊木马)程序安装在金融机构的Web服务器上，入侵者也无法改变网络配置或安装文件系统。最小特权是在惠普可信赖操作系统Virtual Vault的基本特性。

最小信息泄漏原则体现在面向对象的安全体系设计过程中。第二章提到的CORBA安全服务规范，各层次只将其他层次或模块需要的最小的信息对外开放，这些信息恰好能保证系统的正常运作。

Linux等多用户的操作系统访问控制中应用到了多级安全策略。以root用户作为最高的安全级别，按照不同的安全级别可配置不同的用户组，以此来管理不同访问权限的文件和应用程序。

**3.访问控制的描述方法有哪些？它们之间有什么关系？**

**要点：（1）访问控制矩阵、访问控制列表、访问能力表、授权关系表；（2）都是对访问控制二元组的描述/描述对象相同；（3）访问控制列表从客体出发，访问能力表从主体出发，都是对访问控制矩阵的简化描述。（4）对授权关系表按主体或客体排序可得到访问能力表或访问控制表。  
参考答案：**

访问控制矩阵、访问控制列表、访问能力表、授权关系表。

关系：

访问控制可以用一个二元组（控制对象，访问类型）来描述，其中控制对象是指信息

系统中一切需要进行访问控制的资源，访问类型是指对于相应的受控资源的访问操作，如读、写、创建、修改和删除等。访问控制的描述方法都是对二元组的描述。

访问控制矩阵描述了任意主体和任意客体的访问权限。而访问控制列表，从客体出发，能够表达访问控制矩阵某一列的关系，以表示某一资源对任意一个用户的访问权限。访问能力表从主体出发，表示某一主体对不同客体的访问权限。如果将授权关系表按客体进行排序，授权关系表将得到与访问控制表相当的二维表；如果这张表按主体进行排序，授权关系表将得到与访问能力表相当的二维表。

**4.访问控制实现的类别有哪些？如何应用，举例说明。**

**要点：（1）接入访问控制，举例体现对于用户的验证。（2）资源访问控制，包括文件系统访问控制、文件属性访问控制、信息内容访问控制。（3）网络端口和节点的访问控制**

**参考答案：**

接入访问控制。ISP 服务商实现的就是接入服务。用户的接入访问控制是对合法用户

的验证，通常使用用户名和口令的认证方式。一般可分为三个步骤：用户名的识别与验

证，用户口令的识别与验证，用户账号的缺省限制检查

资源访问控制。最新的Linux内核中已经提供文件系统ACL的支持，能够基于文件和目录针对不同的用户和用户组设置访问控制列表。而传统的基于用户角色的文件访问控制列表，类似于管理员可读写等指令，仍然存在于多用户操作系统中。

网络端口和节点的访问控制。网络中服务器的端口常用自动回复器、静默调制解调器等安全设施进行保护，并以加密的形式来识别节点的身份。自动回复器主要用于防范假冒合法用户，静默调制解调器用于防范黑客利用自动拨号程序进行网络攻击。还应经常对服务器端和用户端进行安全检查，如通过标识检测用户真实身份，然后，用户端和服务器再进行相互验证。

**5.BLP 模型和 Biba 模型的安全策略和安全访问规则？分析它们的适用范围和可能存在的问题。**

**要点：（1）BLP模型采用多级安全的策略，访问规则包括强制安全访问规则和自主安全访问规则。（2）Biba模型采用多级安全原则和最小泄漏原则。采用了五种非自主安全访问规则和基于ACL、客体层次结构、环的自主安全访问原则。（3）BLP模型中信息单向不可逆，客体具备高度机密，但是会带来隐藏通道问题。不能阻止未授权主体修改客体。（4）Biba是完整性模型，能够于BLP模型结合。但是完整性级别标签确定困难、目的性不明确、与BLP结合困难。**

**参考答案：**

**BLP 模型**的目的是保护数据的机密性，它将客体的安全级别分为绝密、机密、秘密和公开等四类。该模型详细说明计算机系统的多级操作规则，对应军事类型的安全级别分类，其基本安全策略是“下读上写”，即主体对客体向下读、向上写，保证敏感信息不泄漏

1）安全访问规则。BLP 模型的安全访问规则包括两类：强制安全访问规则和自主安全访问规则。强制安全访问规则包括简单安全规则和\*策略，系统对所有的主体和客体都分配一个访问类属性，它包括主体和客体的密级和范围，系统通过比较主体与客体访问类属性来控制主体对客体的访问。自主安全访问规则使用一个访问矩阵来表示，主体只能按照矩阵中授予的访问权限对客体进行相应的访问。安全访问规则可以用三元组（s，o，m）表示主体 s 能够以权限 m 访问客体 o；m＝M（s，o）表示主体 s 能够以权限 m 访问客体 o，其中 M 为访问矩阵；f 是主体或客体的安全级别函数，其定义为 f:s∪o→L，其中 L 为安全级别的集合。

规则 1：简单安全规则（Simple Security Property）如果主体 s 对客体 o 有读（Read）权限，则前者的安全级别不低于后者的安全识别。这一规则的形式化表示为

Read ∈ M（s，o） ⇒ （f s） ≥ （f o）

这被称为“下读”原则。

规则 2：\*策略（Star Property）

如果一个主体 s 对客体 o 有追加记录（Append）权限，则后者的安全级别一定不低于前者；如果主体 s 对客体 o 有读写（Read-Write）权限，则它们的安全级别一定相等；如果主体 s 对客体 o 有读（Read）权限，则后者的安全级别一定不高于前者。这一规则的形式化表示为

*Append ∈* M（s，o） ⇒ （f s） *≤ （*f o*）*

*Read and Write ∈* M（s，o） ⇒ （f s） ＝ （f o）

*Read ∈* M（s，o） ⇒ （f s） *≥* （f o）

这被称为“上写”原则。

规则 3：自主安全访问规则

当前正在执行的访问权限必须存在于访问矩阵 M 中。这个规则保证主体 s 对客体 o

的权限是通过自主授权来进行的。这一规则的形式化表示为

*（s，o，m） ∈ b ⇒ m ∈ M（s，o）*

其中，b 表示在某个特定状态下，哪些主体以何种访问属性访问哪些客体的一个集合上述规则保证了客体的高度机密性，保证了系统中信息的流向是单向不可逆的，即信息总是从低密级的主体向高密级的主体流动，避免敏感信息的泄露。同时，利用 BLP模型可以分析同一台计算机上并行运行不同密级的数据处理程序的安全性问题，可以检验高密级处理程序是否把敏感数据泄漏给了低密级处理程序，或低密级处理程序是否访问了高密级数据。

**Biba 模型**规定，信息只能从高完整性等级向低完整性等级流动，为此，它将完整性等级从高到低分为三级：关键级（Critical，C），非常重要（Very Important，VI）和重要（Important，I），它们的关系为 C＞VI＞I。在 Biba 模 型 中 ，主 要 访 问 方 式 有 四 种 ：修 改（modify），调 用（invoke），观察（observe）和执行（execute）。与 BLP 类似，Biba 模型的访问规则也分为两类：非自主安全访问规则和自主安全访问规则。

非自主安全访问规则。非自主安全访问规则是基于主体和客体各自的完整性级别，确定主体对客体的访问方式。Biba 模型中有五种非自主安全访问规则：严格完整性规则、针对主体的下限标记规则、针对客体的下限标记规则、下限标记完整性审计规则、环规则。

自主安全访问规则。Biba 模型中的自主安全访问规则用到了如下访问策略：1）访问控制列表（Access Control List）对每个客体分配一个访问控制列表，指明能够访问该客体的主体，以及主体访问该客体的方式。但客体的访问控制列表可以被对该客体拥有 modify 访问权限的主体修改。

2）客体层次结构（Object Hierarchy）模型将客体组织成树状结构，一个客体的中间节点是从此客体节点到根的路径上的所有节点。如果一个主体要访问一个客体 ，则必须对此客体的所有中间节点拥有observe 权限。

3）环（Ring）对每个主体分配一个权限属性，称为“环”。环用数字表示，数字越低，权限越高。

自主安全访问规则基于以下要求：

一个主体仅在环允许的范围内对客体拥有 modify 访问方式。

一个主体仅在环允许的范围内拥有对另一个具有更高权限的主体的 invoke 访问方式。

一个主体仅在环允许的范围内对客体拥有 observe 访问方式。

Biba 模型是一个完整性模型，但却是一个与 BLP 模型完全相反的模型，一旦将保密性和完整性同时考虑时，必须注意不要混淆保密性访问和完整性访问，它们两个是相互独立的，之间没有任何关系。Biba 模型的优势在于其简单性以及与 BLP 模型相结合的可能性，但也存在以下方面的缺陷：完整性级别的标签确定困难。由于 Biba 模型的机密性策略与政府分级机制完美结合，所以很容易确定机密性标签的分级和范围，但对于完整性的分级和分类一直没有相应的标准支持。Biba 模型的目的性不明确。Biba 模型保护数据免受非授权用户的恶意修改，同时认为内部完整性威胁应该通过程序验证来解决，但在该模型中没有包含这个要求，因此，Biba 模型在保护数据一致性方面不充分。Biba 模型与 BLP 模型结合困难。虽然这种实现机密性和完整性的方法在原理上是简单的，但是由于许多应用内在的复杂性，使得人们不得不通过设置更多的范围来满足这些复杂应用在机密性和完整性方面的要求，这些不同性质的范围在同时满足机密性和完整性目标方面是很难配合使用的，很容易出现进程不能访问任何数据的局面。同时，Fred Cohen 已经证明即使使用了 BLP 模型和 Biba 模型，也无法抵御病毒的攻击

**6.如何理解“角色互斥”和“角色继承”？**

**要点：（1）静态角色互斥是用户的不同角色之间不冲突；动态角色互斥是在会话选择时，角色与主体任意一个角色都不冲突。（2）角色继承表明了角色的组织关系，体现了访问权限的继承。**

**参考答案：**

静态角色互斥：只有当一个角色与用户所属的其他角色彼此不冲突时，这个角色才能授权给该用户。它发生在角色分配阶段。动态角色互斥：只有当一个角色与一个主体的任何一个当前活跃角色都不互斥时，这个角色才能成为该主体的另一个活跃角色。它发生在会话选择阶段。

角色继承。在 RBAC 中，定义了这样一些角色，它们有自己的属性，但可能还继承了其他角色的权限。角色继承是将角色组织起来，自然反映系统内部角色之间的权利、责任关系。角色继承可以用“父子”关系来表示，可见教材图5.6。角色2是角色1的“父亲”，它包含角色 1 的权限，处于最左侧的角色拥有最大的访问权限，越靠右侧的角色拥有的权限越小。

**7.RBAC0，RBAC1，RBAC2 和 RBAC3 之间的关系？**

**要点：（1）RBAC0是最低要求的基本模型；（2）RBAC1基于RBAC0，增加角色层次；（3）RBAC2基于RBAC0，增加约束；（3）RBAC3组合了RBAC1和RBAC2,提供角色分级和继承。**

**参考答案：**

在这个模型族中，从简单到复杂一共有四个模型：RBAC0、RBAC1、RBAC2和RBAC3。RBAC0 模型是基本模型，它包含了支持 RBAC 的最低要求。RBAC1增加了角色层次的概念，又称为角色分级模型；RBAC2增加了约束，又称为限制模型；而RBAC3把RBAC1和RBAC2 组合在一起，提供角色分级和继承的能力，又称为统一模型。

RBAC1 模型是在 RBAC0 模型基础上增加了角色等级，其目的是权衡角色之间的层次关系。RBAC2 模型是在 RBAC0 模型的基础上增加了约束的概念，对用户角色和角色权限的分配进行限制。RBAC3 模型不仅集合了 RBAC1 模型中有关角色等级的概念，而且包含了 RBAC2 模型中的约束规则。

**8.如何理解强制访问控制中的保密性规则和完整性规则？**

**要点：（1）这两个规则体现在主体对客体的访问；（2）保密性规则包括下读和上写时候的密级确认，完整性规则需要在上读和下写时进行主客体之间的完整性级别比较，以限制主体对客体的修改。**

**参考答案：**

主体能否对客体执行特定的操作，取决于主体被分配的许可级别和客体被分配的安

全级别。主体对客体的访问，需要遵循保密性规则或完整性规则。（1）保密性规则：仅当主体的密级高于或者等于客体的密级时，该主体才能读取相应的客体（下读）。仅当主体的密级低于或者等于客体密级时，该主体才能写相应的客体（上写）。（2）完整性规则：仅当主体的完整性级别低于或者等于客体的完整性级别时，该主体才能读取相应的客体（上读）。仅当主体的完整性级别高于或者等于客体的完整性级别时，该主体才能写入相应的客体（下写）。

例如，在一个组织中，“不上读，不下写”意味着为了保证信息的机密性，不允许低密级的用户读取高密级的信息，不允许高敏感度的信息写入低敏感度的区域，禁止信息从高安全级别向低安全级别流动。强制访问控制通过这种梯度的安全标签实现信息的单向流动，如果主体既能读客体，又能写客体，则两者的安全级别必须相等。