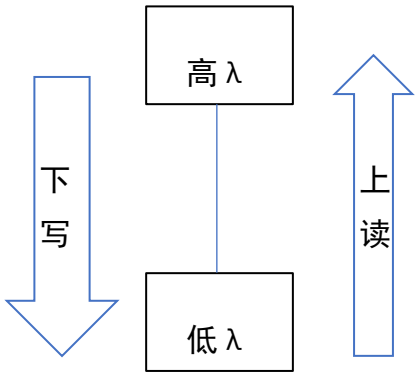
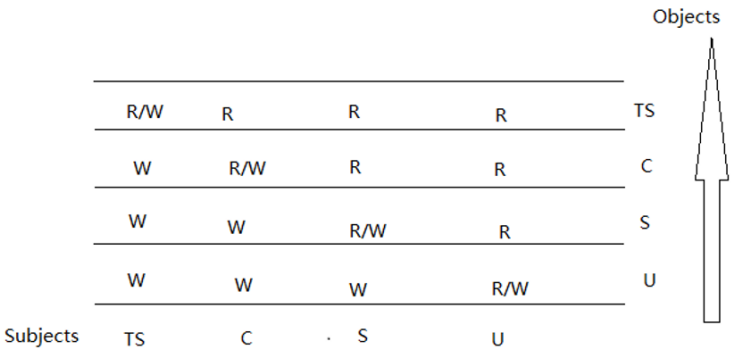
第四次作业

测试点 4-1

1. 依据 Biba 控制模型的定义，画出模型中信息流示意图。





2. 总结 DAC、MAC、RBAC 这三种常见访问控制模型的特点，用表格形式给出从模型设计原理、优点、缺点和适用场景的对比。

	模型设计原理	优点	缺点	适用场景
DAC	自主访问控制，确认主体身份及所属组的基础上，根据访问者的身份和授权来决定访问模式，对访问进行限定的一种控制策略。	与业务和应用场景无关，其自主性为用户权限管理提供了最大限度的灵活性。	安全级别较低，授权管理复杂，存在权限传递风险	在通用操作系统中普遍使用
MAC	强制访问控制，由安全管理员统一对主体和客体的安全标签赋值，普通用户不能改变	可以提供严格的访问控制策略保障，有更高的安全性	强制访问控制由于强调信息流通的单向性，造成实现工作量	对安全级别要求高的场景。

			太大，管理不便，可用性和灵活性差	
RBAC	基于角色，管理员创建角色，给角色分配权限，让用户关联角色，角色所属的用户可以执行相应的权限	便于权限的安全控制，业务的权限分离，业务的权限分离，业务的权限分离	功能实现复杂，授权流程复杂	对权限管理更加细腻的场景。

3. **RBAC 被认为是一种与访问策略分离的访问控制模型，即权限管理可以采用自主访问控制策略，也可以采用强制访问控制策略，这种观点是正确的吗？如何理解？**

我觉得不正确，RBAC 的权限管理是基于角色管理的，也就是在给某一主体分配权限的时候，实际上是给该主体分配了某一角色，权限本身是与角色绑定的，无法直接将某一权限分配给某一用户，而是只能给予或取消某一类用户的某一权限，这与 DAC 是不同的，而某一用户又可以通过被动更改角色，从而改变自己的权限集，但这种角色并不存在明显的上下级之分，主体不存在 MAC 明显的安全等级的标志。

测试点 4-2

1. **假设操作系统中客体的访问权限（R，W，X）可以划分为属主（客体的创建者）、属组（只考虑用户加入一个用户组）和其余三类，请给出一个用二进制表示用户对文件访问权限的方法，要求对任意一个给定文件，可以确定每类用户对它的访问权限。并写出一个实例加以说明。（提示：可参考 Linux 系统的权限管理实现方式）**

可用三位的二进制数表示 000—111 即 0-7，按位分别表示 R，W，X，1 代表有权限，0 代表无。例如 110 表示可以读写但是不能执行。

测试点 4-3

1. **Windows 的访问控制有本地模式和域模式两种类型，请查阅资料，理解域模式下访问控制的原理和过程，并进行简要描述。**

在域模式下，一个域中含有多个用户、多个终端以及至少一个域控制器，每个域可以采用不同的安全策略，域控制器负责控制用户的接入。终端连入网络时，域控制器要验证这个终端是否属于这个域、用户使用的登陆账号密码是否正确。如果有一项不正确，那么域控制器就会拒绝用户登录，用户就无法访问服务器上有权限保护的资源，只能以对等网用户的方式访问 windows 共享出的资源。多个域之间如果建立了信任关系，那么相互建立了信任关系的域之间可以按需进行互相管理，而且可以跨网分配文件和设备资源，实现不同域之间的网络资源共享和管理。

2. 设计一个通用的基本 RBAC 访问控制系统的静态数据模型，要求给出数据库设计的表结构和表的 E-R 关系图。