第四讲 访问控制技术

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。（形式参考 BLP 模型信息流示意图）**

Object

R/W	R	R	R	TS
W	R/W	R	R	C
W	W	R/W	R	S
W	W	W	R/W	U

Subjects TS C S U

绝密 TS 机密 C 秘密 S 无秘级 U

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。**

	DAC	MAC	RBAC
设计原理	根据访问者的身份和授权来决定访问模式	安全管理员统一对主体和客体的安全标签赋值	管理员创建角色，给角色分配权限，让用户关联角色
优点	与业务和应用场景无关，为用户权限管理的灵活性	通过梯度安全标签实现信息的单向流通	权限的安全控制、业务的权限分离、最小化权限管理、权限的分级管理
缺点	存在权限传递风险	实现工作量太大，管	功能实现复杂、授

		理不便，可用性和灵活性差	权流程复杂
适用场景	通用操作系统	WEB 服务器的访问过程	资源由系统共有且具有多种分层的角色的责任分立的系统。

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？

不正确。RBAC 由管理员来创建角色，而用户来关联角色，权限是以角色为载体分配的，如果某一角色下的个别用户需要进行特别的权限定制，如同加入一些其他角色的小部分权限或去除当前角色的一些权限时，RBAC 就无能为力了，因为 RBAC 对权限的分配是角色为单位的。

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）

给 R，W，X 分配不同的权重，R 为 4，W 为 2，X 为 1，对每个用户会有一个文件权限文档与之对应，权限文档以中每个文档的权限以二进制表示。

例如用户 A 对文档 A 有读写但没有执行权，则对应的权限为 110，对文档 B 有读写执行权，则对应权限为 111，对文档 C 有写权限但没有执行、读权限，则权限表示为 010。每当用户点击文件时，文件会先访问权限文档以判断当前用户有无权限，若有则执行否则禁止访问。

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。**

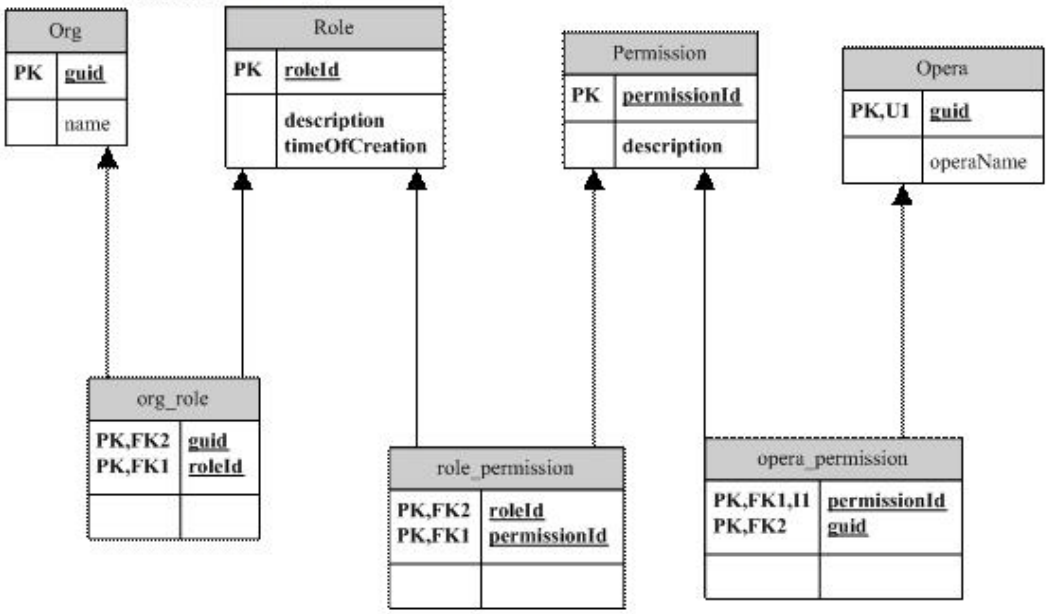
域(Domain)是 Windows 网络中独立运行的单位，域之间相互访问则需要建立信任关系。信任关系是连接在域与域之间的桥梁。当一个域与其他域建立了信任关系后，2 个域之间不但可以按需要相互进行管理，还可以跨网分配文件和打印机等设备资源，使不同的域之间实现网络资源的共享与管理，以及相互通信和数据传输。

在“域”模式下，至少有一台服务器负责每一台联入网络的电脑和用户的验证工作，相当于一个单位的门卫一样，称为“域控制器（Domain Controller，简写为 DC）”。

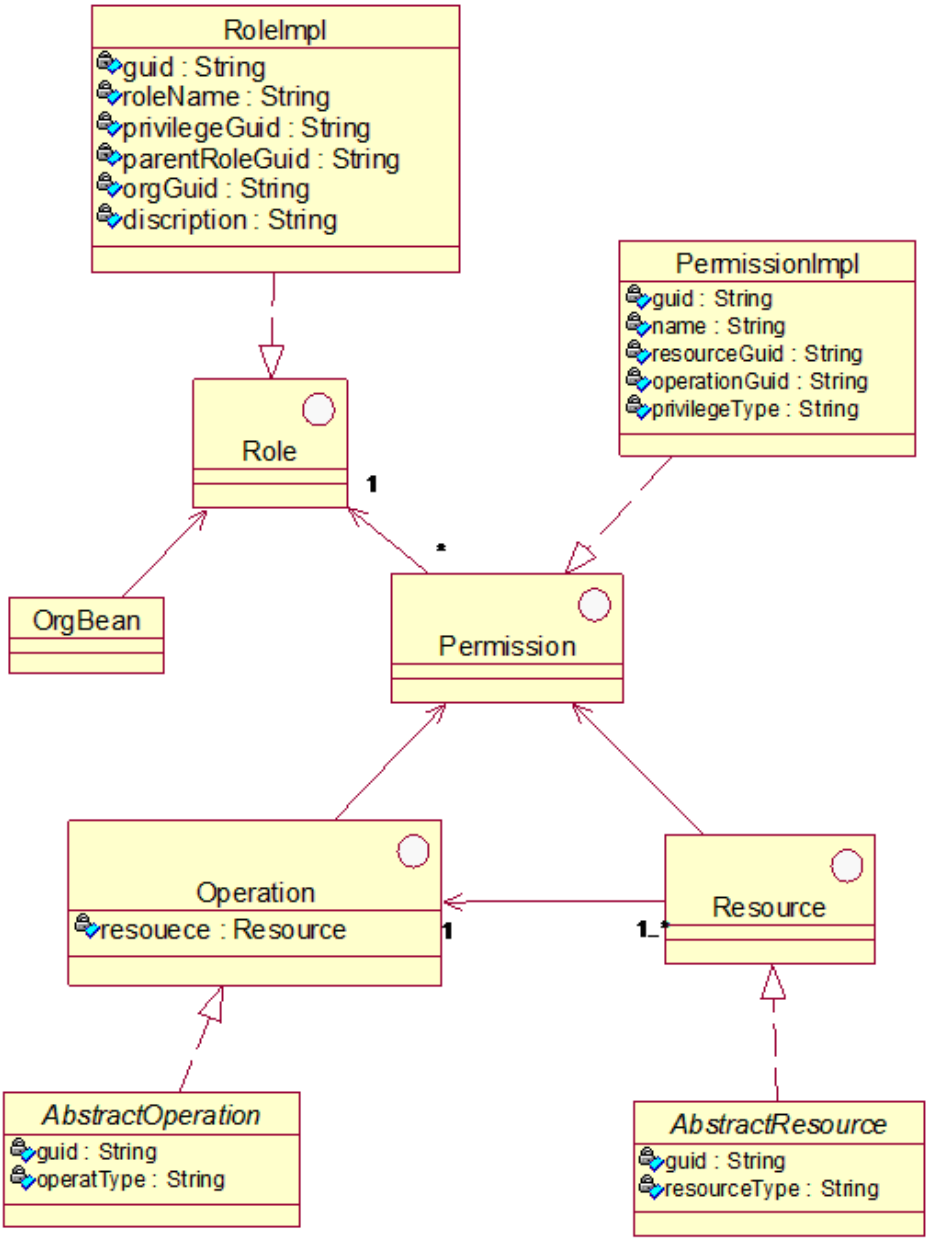
要把一台电脑加入域，仅仅使它和服务器在网上邻居中能够相互“看”到是远远不够的，必须要由网络管理员进行相应的设置，把这台电脑加入到域中。这样才能实现文件的共享，集中统一，便于管理。

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。

数据库 ER 图：


Org
PK guid
name
Role
PK roleId
description
timeOfCreation
Permission
PK permissionId
description
Opera
PK,U1 guid
operaName
org_role
PK,FK2 guid
PK,FK1 roleId
role_permission
PK,FK2 roleId
PK,FK1 permissionId
opera_permission
PK,FK1,I1 permissionId
PK,FK2 guid

关系图



整个权限可以抽象为五个对象组成。

OrgBean：用于描述 org 模型。

Role ： 用于描述角色。

Permission ： 用于描述权限。

Resource ： 用于描述资源。

Operation ： 用于描述操作。

思想：

权限系统的核心由以下三部分构成：1. 创造权限，2. 分配权限，3. 使用权限，然后，系统各部分的主要参与者对照如下：1. 创造权限 - Creator 创造，2. 分配权限 - Administrator 分配，3. 使用权限 - User ：