**网络安全技术第四次作业**

陆圣珩

2017221302009

1. **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）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| R/W | R | R | R | TS |
| W | R/W | T | T | C |
| W | W | R/W | T | S |
| W | W | W | R/W | U |
| TS | C | S | U |  |

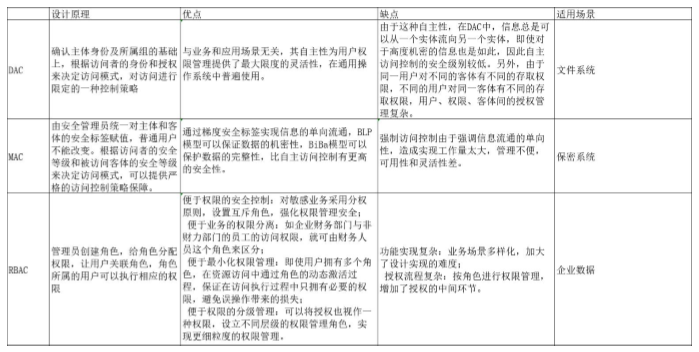
(T:绝密；C:机密；S:秘密；U:无密)

1. **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:** 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。

**MAC:** 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。根据访问者的安全等级和被访问客体的安全等级来决定访问模式，可以提供严格的访问控制策略保障。

**RBAC:** 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



1. **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是自助访问控制策略和强制访问控制策略的结合体。

在划分不同的角色时，需要一个集中的权威管理员来确定需要哪些角色，每个角色的权限有哪些，以及每一个新的主体属于某个或某几个角色，此时RBAC 属于强制访问控制。在分配完角色和每个主体所属的角色时，主体进入系统，开始在自己的权限范围内工作，每次访问时根据访问控制列表检查用户标志实现对访问的控制，此时RBAC 属于自主访问控制策略。

**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）是安全机制？**

用 9 位二进制来表示访问权限:

前 3 位：所属用户权限（u）。是否可读，是否可写，是否可执行。每一位可以用二进制 0/1 表示，3 为合起来就是十进制数字。比如 rwx，二进制表示就是 111，十进制表示就是 7

中 3 位：所属组权限（g）。是否可读，是否可写，是否可执行。每一位可以用二进制 0/1 表示，3 为合起来就是十进制数字。比如 r-x，二进制表示就是 101，十进制表示就是 5

后 3 位：其他用户权限（o）。是否可读，是否可写，是否可执行。每一位可以用二进制 0/1 表示，3 为合起来就是十进制数字。比如 r-x，二进制表示就是 101，十进制表示就是 5

**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”的真正含义指的是服务器控制网络上的计算机能否加入的计算机组合。其实可以把域和工作组联系起来理解，在工作组上你一切的设置在本机上进行包括各种策略，用户登录也是登录在本机的，密码是放在本机的数据库来验证的。而如果你的计算机加入域的话，各种策略是域控制器统一设定，用户名和密码也是放到域控制器去验证，也就是说你的账号密 码可以在同一域的任何一台计算机登录。

域组的范围包括域本地组、全局组和通用组。在管理域资源时，一般把权限赋予本地域组；实际应用中一般会把隶属于同一部门的用户组织成全局组，再将全局组加入本地域组中，让这些用户一次获得相同的权限。