

## 第四章 课后作业

1、对于本章讨论的 DAC 模型，保护状态的另一种表示方法是有向图。保护状态中的每个主体和每个客体都用结点表示（单个结点表示既是主体又是客体的实体）。从主体指向客体的有向线段表示访问权，线上的标记定义访问权。

a.画出对应于下图中访问矩阵的有向图。

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read Write	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix

b.画出对应于下图中访问矩阵的有向图。

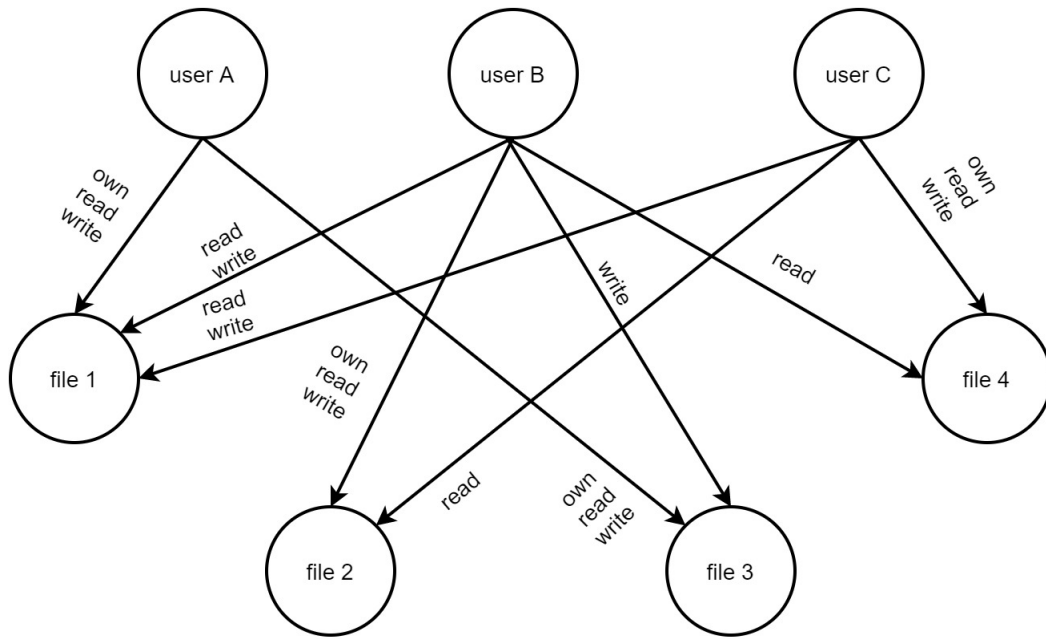
		OBJECTS								
		subjects			files		processes		disk drives	
		S <sub>1</sub>	S <sub>2</sub>	S <sub>3</sub>	F <sub>1</sub>	F <sub>1</sub>	P <sub>1</sub>	P <sub>2</sub>	D <sub>1</sub>	D <sub>2</sub>
SUBJECTS	S <sub>1</sub>	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S <sub>2</sub>		control		write *	execute			owner	seek *
	S <sub>3</sub>			control		write	stop			

\* - copy flag set

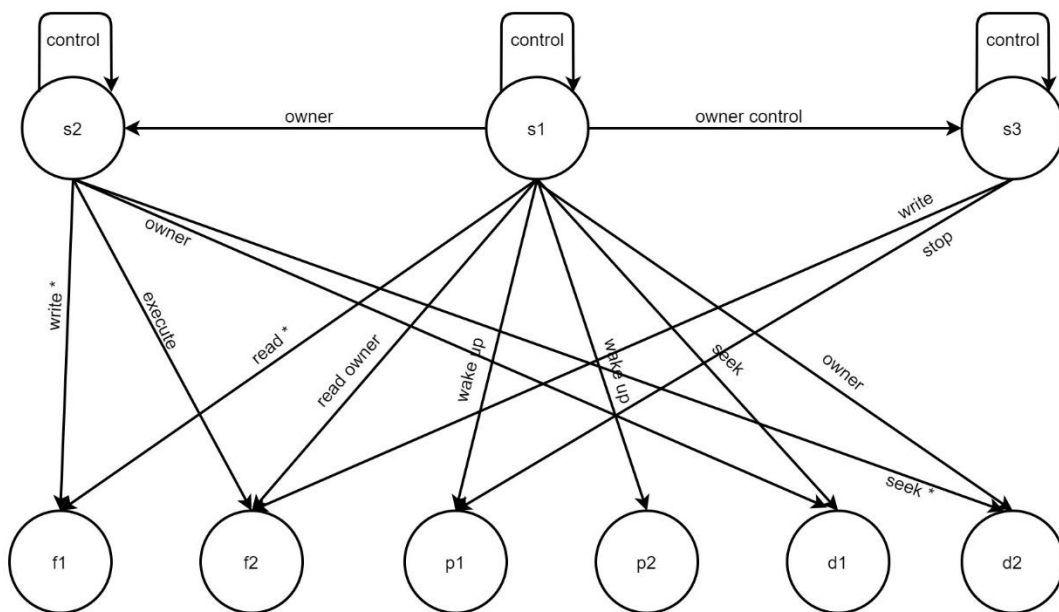
c.有向图表示与访问矩阵表示是否是一一对应的？解释之。

答：

a.



b.



c.

有向图表示与访问矩阵表示是一一对应的，因为将主体和客体表示为结点，对于主体结点对自身有控制权限的可连成自身的环，对于主体结点对主体结点或客体结点有控制权限的可以连接构成单向边，在边上注释权限信息，等同于访问矩阵中主体对客体的访问权限表示，所以有向图表示与访问矩阵表示是一一对应的。

2、UNIX 将文件目录与文件同等对待，就是说，都用相同类型的数据结构——结点来定义。与文件一样，目录包括 9 位的保护串。如果不注意，就会产生访问控制问题。例如，考虑一个保护模式为 644 的文件，它包含在保护模式为 730 的目录中。这种情况下该文件可能受到怎样的安全威胁？

答：

文件：644 转化为二进制为 110100100

目录：730 转化为二进制为 111011000

对于属主来说，文件目录可读可写可执行，文件可读可写不可执行，因为是属主，所以不会造成安全威胁。

对于同组用户来说，文件可读不可写不可执行，目录不可读可写可执行，安全威胁是会导致文件目录被篡改，导致正常用户找寻不到文件所在的位置。

对于其他用户来说，文件可读不可写不可执行，目录不可读不可写不可执行。当攻击者获得其他用户权限之后，如果知道对应文件所在目录位置，或者通过穷举搜索，可以轻松绕过目录读取文件信息，信息会被盗取。

3、请为下边的各种角色分配对应各个数据表的操作权限（查询、新增、删除、修改）。

	教师信息表	学生信息表	课程信息表	学生成绩表
教师	查询	查询	查询	查询、新增、删除、修改
学生	无	查询	查询	查询
管理员	查询、新增、删除、修改	查询、新增、删除、修改	查询、新增、删除、修改	查询、新增、删除、修改
访客	无	无	查询	无