Assignment 2

Assume you are working as an IT administrator for an organization and describe a case scenario where you can apply access control privileges to the organization employees over the organization resources. Then apply three access control method which you have learnt in your course to define the access privileges

For example:

Step 1: Describe the access privilege (2 Points)

PSAU college of computer engineering and sciences has three computer labs namely, AI lab, security Lab, microprocessor lab. If access privilege is as follows

1. **"Each of these labs can be accessed only by the corresponding course teacher and the students registered for this course".**
2. **Course teacher can install any new software, create, compile and execute new application in the lab**
3. **Students can only create, compile and execute new application in the lab**

Step 2: Define the access policy / structure using the methods (3 Points)

a. Discretionary access control

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

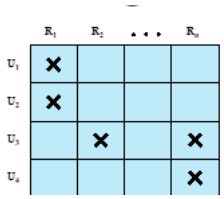
(a) Access matrix

Discretionary Access Control (DAC)

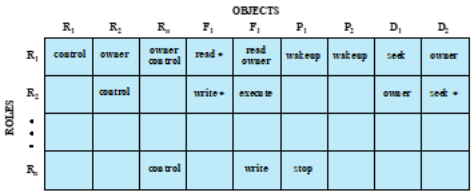
DAC is an access control model in which the owner of a resource determines who has access to it and what permissions they are granted. In this case, the course teacher would be the owner of the lab resources, and they would be responsible for granting access to students.

Subjects	Objects	Permissions
Course teacher	Al lab	Read, write, execute, install
Course teacher	Security lab	Read, write, execute, install
Course teacher	Microprocessor lab	Read, write, execute, install
Student	Al lab	Read, write, execute
Student	Security lab	Read, write, execute
Student	Microprocessor lab	Read, write, execute

b. Role based access control



User – role Matrix



Role based access control matrix

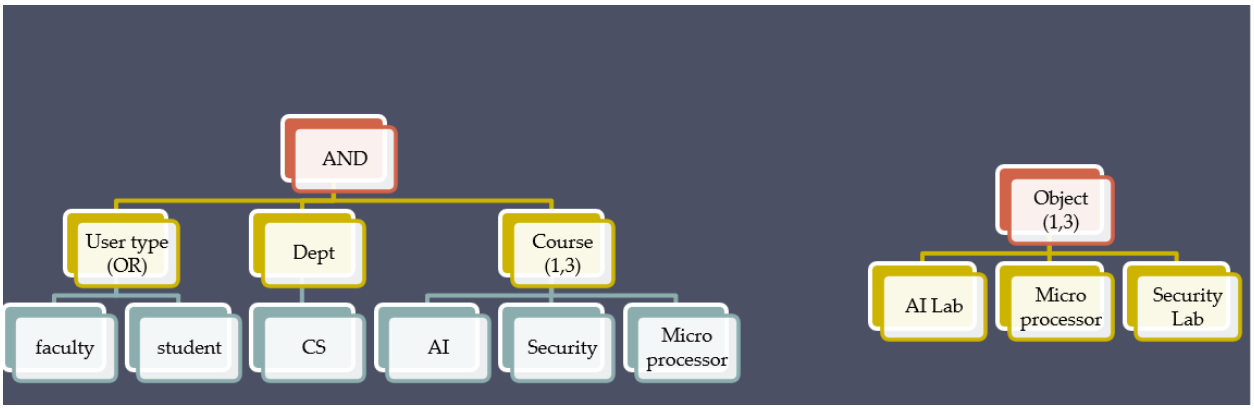
Role-Based Access Control (RBAC)

RBAC is an access control model in which users are assigned roles, and roles are granted permissions to resources. In this case, there would be two roles: course teacher and student. The course teacher role would have all permissions to the lab resources, while the student role would only have read, write, and execute permissions.

User	Role
Course teacher	Course teacher
Student	Student

Roles	Objects	Permissions
Course teacher	Al lab	All
Course teacher	Security lab	All
Course teacher	Microprocessor lab	All
Student	Al lab	Read, write, execute
Student	Security lab	Read, write, execute
Student	Microprocessor lab	Read, write, execute

c. Attribute based access control



Access rights → Installation, Creation, Compilation and Execution
If user type = faculty and dept = CS and course = AI then
Install, create, compile and execute Object (AI)

```
If user type = faculty and dept = CS and course = AI then
    Allow access to AI lab
    Allow installation, creation, compilation, and execution of
objects in the AI lab
If user type = student and dept = CS and course = AI then
    Allow access to AI lab
    Allow creation, compilation, and execution of objects in the
AI lab
```

This policy allows faculty members in the CS department who are teaching the AI course to install, create, compile, and execute objects in the AI lab. It also allows students in the CS department who are registered for the AI course to create, compile, and execute objects in the AI lab.

Lab	User type	Department	Course	Access rights
AI lab	Faculty	CS	AI	Install, create, compile, and execute
AI lab	Student	CS	AI	Create, compile, and execute
Security lab	Faculty	CS	Security	Install, create, compile, and execute
Security lab	Student	CS	Security	Create, compile, and execute
Microprocessor lab	Faculty	CS	Microprocessor	Install, create, compile, and execute
Microprocessor lab	Student	CS	Microprocessor	Create, compile, and execute