Yuvika Nibber

Assignment 8

1. DAC is the discretionary access control and MAC is the mandatory access control. DAC permits the requestors only. The entity must give rights to permit another entity. In MAC, the security label indicates if the system is sensitive or critical. The security decides who can get access to the resources.
2. The user has access to the computer and have their own ID. Each user has their own role within the organization. Permission is needed to access one or more objects. A mapping between a user and an activated subset of roles are assigned to the user.
3. SSD allows definition of a set to mutually exclusive roles. DSD limits the permission by adding constraints to the roles.
4. Mutually exclusive roles, cardinality, prerequisite roles are the three types of roles of hierarchy constraints.
5. Access matrix: it is the authentication policy of the user. It is in one dimension of the matrix. The other dimensions list the objects it has accessed.

Directed graph: it has notes which are connected by edges. This graph has a direction.

1. The owner and the group have access to the directory and the files in it. The owner has permission to write to the files and the group members can only view it but can not make changes it to. They do have access to removing and adding new files.
2. In the first case there is no access for the group, and we can restrict any user from the group. It is also not possible to give access to someone who is not in the group. Numeric access value is 0700.

In second case is read and execute case where people from a certain group can get access to the files and directory. Numeric access value 0700

In the third case both the groups have access to read and execute and this is beneficial because all the users have access to all the files and directories. Numeric access value 0777.

1. The user’s home directory must provide execute access in the path.

The web directory should have the read or execute access.

Access of read should be provided to any webpage in the directory.

In order to maintain permission, the user should set the permissions every time a new file or directory is created.

It they do not do that then the files are not accessible by the server.

User should not give too much access because that will leak information.

1. A. For a traditional DAC there can only be 1 possible relation.

B. For RBAC, the relationship will be determined by U\*P (user, permission) where U is the set of individuals and P is the set of permissions it requires.

1. A. role (x) > role (y) = role(x)\*position > role(y)\*position ^ role(x)\*function = role(y)\*function.

Role(x) is superior to role(y) and the position of role(x) is superior to role(y). The functions are identical.

B. Role(x) > role(y) = role(x)\*position > role(x)\*function = role(y)\*function

In this, role(x) is superior to role(y). The function and position of both are identical.