FIT2093: Tutorial 3

Access Control & Security Models

Review Questions

1. Briefly define the difference between DAC and MAC.
2. List and define the three classes of subject in an access control system.
3. In the context of access control, what is the difference between a subject and an object? What is an access right?
4. What is the difference between an access control list and a capability list?
5. What are the three rules specified by BLP model?
6. In general terms, how can MLS be implemented in an RBAC system?
7. A directory is also an object to which access should be controlled. Why is it not appropriate to allow users to modify their own directories?
8. Why should the directory of one user not be generally accessible (for read-only access) to other users?

Problems

1. Unix treats file directories in the same fashion as files; that is the same type of data structure, called an inode, defines both. As with files, directories include a nine-bit protection string. If care is not taken, this can create access control problems. For example, consider a file with protection mode 644 (octal) contained in a directory with protection mode 730. How might the file be compromised in this case?
2. In the traditional UNIX file access model, which provides a default setting for newly created files and directories, which owner may later change. The default is typically full access for the owner with one of the following:
   - No access for group and other
   - Read/execute access for group and none for other
   - Read/execute access for both group and other.

Briefly discuss the advantages and disadvantages of each of these cases, including an example of a type of organisation where each would be appropriate.

3. The necessity of the " non read up " rule for a multilevel secure system is fairly obvious. What is the importance of the " no write down " rule?
4. The *-property requirement for append access (blind write) {SC(S) ≤ SC(O)} is looser than for the write access {SC(S) ≥ SC(O)}. Explain the reason for this. [SC(S) refers to the security clearance level of subject, S and SC(O) is the security classification level of the object, O in a BLP model].
5. In Discretionary Access Control (DAC) the Operating System generally uses an access control matrix. Refer to the table 1 shown below. The access rights assigned to each subject are read or write. In addition the owner of the file is included in the access control matrix.
    a. Create an access control list for each of the 4 files, File 1, File 2, File 3 and File 4.
    b. Create a capability list for each of the users, User A, User B and User C.

	File 1	File 2	File 3	File4
User A	Own, read, write		Own, read, write	
User B	Read	Own, read, write	Write	read
User C	Read, write	Read		Own, read, write

Table 1: Access Control Matrix

6. File access control relates largely to the secrecy dimension of security. What is the relationship between an access control matrix and the integrity of the objects to which access is being controlled?
7. Consider the following three kinds of access control mechanisms:

    1. per-subject capability list (that is, one list for each subject indicates all the objects to which that subject has access)
    2. per-object access control list (that is, one list for each object indicates all the subjects who have access to that object)
    3. access control matrix

    For each kind of access control mechanism, describe the:

a. ease of determining authorized access during execution
b. ease of adding access for a new subject
c. ease of deleting access by a subject
d. ease of creating a new object to which all subjects have access by default.

For each of the above cases, distinguish the complexity of the operation as **easy, moderately easy, moderately hard** or **very hard**.

8. Consider three users in a Unix system **Srini, Campbell** and **Maria** such that **Srini** and **Campbell** are in the same group **staff**, but **Maria** does not belong to this group. Consider the following files, with different access information.

```
- --- --- ---  1  srini  staff  4257 Sept 5 14:00 file01
- --- --- rw-  1  srini  staff  4257 Sept 5 14:00 file02
- --- rw- ---  1  srini  staff  4257 Sept 5 14:00 file03
- --- rw- rw-  1  srini  staff  4257 Sept 5 14:00 file04
- rw- --- ---  1  srini  staff  4257 Sept 5 14:00 file05
- rw- --- rw-  1  srini  staff  4257 Sept 5 14:00 file06
- rw- rw- ---  1  srini  staff  4257 Sept 5 14:00 file07
- rw- rw- rw-  1  srini  staff  4257 Sept 5 14:00 file08
```

Fill in the following table 2 based on the accessibility of each file by each one of the user (by putting yes or no in the box).

	Srini		**Campbell**		**Maria**	
	reads	**writes**	**reads**	**writes**	**reads**	**writes**
file01						
file02						
file03						
file04						
file05						
file06						
file07						
file08						

Table 2: Access Rights