CS 850 DATABASE SECURITY
II SEM M.TECH (CSE-IS)
MIDSEM EXAM- 12 Feb 2024

Note: Answer ALL Questions **Max.Marks: 50 Marks**

Q1. By an example, show what problem/problems may arise in Bell LaPadula model if an object hierarchy function does not result in a tree, but results in a graph (such as a Directed Acyclic Graph or Graph with cycles). (8 Marks)

Q2. Discuss the revocation problem with respect to access control lists and capabilities. How might one efficiently implement a command to revoke access to an object by one particular user? (4 Marks)

Q3. The CSE department has decided to develop a new electronic grading system. Here are the key features the department wants the system to handle (do not assume any permissions or restrictions other than those explicitly mentioned): (15)

- Each course has some course instructors (CIs) and teaching assistants (TAs) assigned to it.
- TAs and CIs for a given course can both read and write that course's grades; in addition, a course's CI(s) can submit final grades.
- All faculty members can read the grades for every course.
- Graduate students and faculty are disjoint groups.
- No graduate student can be a TA for more than two courses.
- No graduate student can be a Course instructor for any course.
- Faculty members can be teaching assistants or Course instructors for any course, and there are no limits on how they are assigned to courses. (Yes, they may even serve as both the TA and the CI for the same course; I mention this only to make your task easier.)
- Because of the potential for confusion with final grades—especially if instructors have the same students in multiple courses—the electronic grading system must not permit anyone to perform in more than one Course-instructor role at any given time (e.g., login session).

As part of the system's initial test run, the department wants to configure the system to handle just three of the department's courses: CSE 123, CSE 456, and CSE 789. Thus, the department has identified the following roles and permissions for this system:

R = {Fac Grad, 123TA, 123CI , 456TA, 456CI , 789TA, 789CI }

P = {read 123, write123, submit 123, read 456, write456, submit 456, read 789, write789, submit 789}

For example, read 123, write123, and submit 123 are the permissions to (respectively) read, write, and submit the grades for CS 123.

Provide the following RBAC components to accurately meet and fulfill all of the department's desired features/criteria:

a) A role-hierarchy relation and a permission- assignment relation PA
b) A static separation-of-duty relation to capture necessary static constraints
c) A dynamic separation-of-duty relation to capture necessary dynamic constraints

4

Q3. Suppose you are the database administrator setting up security mechanisms for the Video Stores database (8 marks)

FILM (FNUM, TITLE, OPENED, LENGTH, BUDGET, DIRECTOR, SNUM, RATING, WRITER)
ACTOR (ANUM, FNAME, LNAME, BDATE, GENDER)
ROLES (FNUM, ANUM, PART, SALARY)
STUDIO (SNUM, NAME, ADDRESS, WEBSITE)
ITEM (INUM, FNUM, PRICE, RELEASE, FORMAT, BONUS, INVENTORY)
SHOPPER (SHNUM,FNAME, LNAME, SHIPADDR, CRCARD)
CART (SHNUM, INUM, QUANTITY)

Suppose that the database has the following users:

a) SPIELBERG works in the purchasing department.
b) SHYAMALN is in the shipping department.
c) MARSHALL is the manager of the customer service department.

Provide the SQL commands to grant appropriate access privileges and grant propagation privileges. Explain your choices based on how each user will be expected to use the database. If you make any assumptions about these types of users, be sure to explain them.

Q4. Consider the following PHP script for a login page: (15 Marks)

5

```
$username = $_GET[user];
$password = $_GET[pwd];
$sql = "SELECT *
        FROM usertable
        WHERE username = '$username'
        AND password = '$password' ";
$result = $db->query($sql);
if ($result->num_rows > 0) { /* Success */ }
else { /* Failure */ }
```

a) Explain why a URL where user is set to " ' or 1 = 1 -- " will result in a successful login.

b) Suppose we change lines 1 and 2 to

```
$username = addslashes($ GET[user])
$password = addslashes($ GET[pwd])
```

Recall that the addslashes function adds a slash before every quote. That is addslashes("a'b") will output the string "a\'b". Explain why this prevents the attack from part (a).

c) Does addslashes completely solve the problem? Consider the GBK Chinese unicode character set. Some characters in GBK are single bytes while others are double bytes. In particular, the following table shows a few GBK characters:

0x 5c = \
0x 27 = '
0x bf 27 = ¿'
0x bf 5c =

That is, the database interprets 0xbf27 as two characters, but interprets 0xbf5c as a single chinese character. Show that using addslashes as in part (b) leads to a SQL injection attack. What value of user will result in a successful login?

---Good Luck---

21