Department of Computer Science & Engineering
N.I.T.K.-Surathkal
II Sem M.Tech (CSE-IS)
ENDSEM EXAM- APRIL 2024
CS 850 DATABASE SECURITY

Time: 3 Hrs **Max Marks: 100**

Note : Answer ALL

Q1 a). In a medical information system that controls access to patient records and prescriptions, doctors may read and write patient records and prescriptions, nurses may read and write prescriptions only but should learn nothing about the contents of patient records. [10]

i. How can you capture this policy in a lattice model that prevents information flow from patient records to prescriptions?

ii. In your opinion, which security model is most appropriate for this policy? (Why?) Sketch a security model capturing the requirement.

iii. A doctor should not be allowed to make a prescription for herself. How can you augment your model above to prevent this kind of prescription abuse?

b) Consider the printserver scenario defined in the Authentication lab. The print server supports the following operations: [15]

print(String filename, String printer); // prints file *filename* on the specified *printer*
queue(); // lists the print queue on the user's display in lines of the form <*job number*> <*file name*>
topQueue(int job); // moves *job* to the top of the queue
start(); // starts the print server
stop(); // stops the print server
restart(); // stops the print server, clears the print queue and starts the print server again
status(); // prints status of printer on the user's display
readConfig(String parameter); // prints the value of the *parameter* on the user's display
setConfig(String parameter, String value); // sets the *parameter* to *value*

Not everybody working in the company has the same rights to access the print server. Alice is managing the print server, so she has the rights to perform *all*operations. Bob is the janitor who doubles as service technician, he has the rights to *start, stop* and *restart* the print server as well as inspect and modify the service parameters, i.e., invoke the *status, readConfig* and *setConfig* operations. Cecilia is a power user, who is allowed to *print* files and manage the print queue, i.e., use *queue* and *topQueue* as well as *restart* the print server when everything seems to be stuck. Finally, David, Erica, Fred and George are ordinary users who are only allowed to *print* files and display the print *queue*.

i. Prepare the access control list for the print server (i.e. the print server is considered as a single object with the different methods as the possible operations)

ii. Identify roles and define a role hierarchy and permissions for each role, so that the access control policy outlined above can be implemented?

iii. Now consider the situation where Bob leaves the company and George takes over the responsibilities as service technician. At the same time, two new employees are hired: Henry, who should be granted the privileges of an ordinary user, and Ida who is a power user and should be given the same privileges as Cecilia.

c) Assume that a database table named Students (SID, SNAME, DEPTID, LOANAMOUNT). Possible queries are COUNT, SUM and MEAN. The database does not reveal results when a small or large number of people are covered by the query. In our database it has been decided that 4-7 people must be covered by the query. We want to find a sequence of queries that tells us the size of Erika's loan. The obvious query SELECT SUM(Loan) FROM Students WHERE name = 'Erika' will not work because the result, 1, is not in the range 4-7. The query will be ignored. Find a general tracker and a sequence of queries that will give you the information. You are allowed to do 4 queries. [05]

Q2. Assume that you are the DBA for the ABC Toy Company and create a relation called Employees with fields *ename*, *dept*, and *salary*. For authorization reasons, you also define views EmployeeNames (with *ename* as the only attribute) and DeptInfo with fields *dept* and *avgsalary*. The latter lists the average salary for each department. [20]

a. Show the view definition statements for EmployeeNames and DeptInfo.
b. What privileges should be granted to a user who needs to know only average department salaries for the Toy and CS departments?
c. You want to authorize your secretary to fire people (you will probably tell him whom to fire, but you want to be able to delegate this task), to check on who is an employee, and to check on average department salaries. What privileges should you grant?
d. Continuing with the preceding scenario, you do not want your secretary to be able to look at the salaries of individuals. Does your answer to the previous question ensure this? Be specific: Can your secretary possibly find out salaries of *some* individuals (depending on the actual set of tuples), or can your secretary always find out the salary of any individual he wants to?
e. You want to give your secretary the authority to allow other people to read the EmployeeNames view. Show the appropriate command.
f. Your secretary defines two new views using the EmployeeNames view. The first is called AtoRNames and simply selects names that begin with a letter in the range A to R. The second is called HowManyNames and counts the number of names. You are so pleased with this achievement that you decide to give your secretary the right to insert tuples into the EmployeeNames view. Show the appropriate command and describe what privileges your secretary has after this command is executed.
g. Your secretary allows Todd to read the EmployeeNames relation and later quits. You then revoke the secretary's privileges. What happens to Todd's privileges?
h. Give an example of a view update on the preceding schema that cannot be implemented through updates to Employees.

i. You decide to go on an extended vacation, and to make sure that emergencies can be handled, you want to authorize your boss Joe to read and modify the Employees relation and the EmployeeNames relation (and Joe must be able to delegate authority, of course, since he is too far up the management hierarchy to actually do any work). Show the appropriate SQL statements. Can Joe read the DeptInfo view?

j. After returning from your (wonderful) vacation, you see a note from Joe, indicating that he authorized his secretary Mike to read the Employees relation. You want to revoke Mike's SELECT privilege on Employees, but you do not want to revoke the rights you gave to Joe, even temporarily. Can you do this in SQL?

Q3. Consider the following PHP script for a login page: [15]

```
$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 */ }
```

i. Because addslashes did not eliminate the problem of SQL injection, we decide to employ some form of input filtering. A recommends the use of JavaScript to validate the input before passing it over to the server. Is this enough to ensure that SQL injection will not happen? Why?

ii. As an extension to input filtering, we decide to strip the -- characters in the input so that attackers cannot inject a comment and thereby execute an injection. Can an attacker bypass this restriction? How?

iii. Stored Procedures have a reputation for being able to defend against SQl injection attacks. With this in mind, we decide to employ the following stored procedure:

```
CREATE PROCEDURE VerifyUser
        @username varchar(50),
        @password varchar(50)
AS
BEGIN
        SELECT * FROM UserTable
        WHERE UserName = @username
        AND Password = @password;
END
GO
```

The stored procedure is called from the PHP file using the following code:

```
$sql = "CALL VerifyUser ("+ $_GET[user] + "," + $_GET[pwd]+")";
```

Is the web application susceptible to an SQL injection? Why or why not?

Q4. a) You are given a firewall that can examine the contents of packets, including reconstructing connection streams. What types of buffer overflow attacks can it protect against, if any? What types of buffer overflow attacks can it not protect against, if any? Explain your answers briefly? [10]

b) Explain the difference between Signature-based vs. Anomaly-Based intrusion detection systems? Suggest at least two ways to improve the efficiency of Anomaly-Based IDS? Is there anything interesting about the false positives? [10]

Q5. a) Assume that multiple groups simultaneously query the same XML to specify access policies at various levels of granularity. Suggest ways to efficiently enforce those access policies? Compare the XACML and XACL models of XML security. [10]

b) Explain various Types of XML Injection Attacks with suitable examples? [5]

---Good Luck---