Breesy Reyes
Sam Chen

Assignment 5 - Database and Cloud Security

1. Explain the concept of cascading authorizations.

The concept of cascading authorizations is granting and revoking rights cascading through users. A user grants the access rights to another user who can then pass the rights on through a number of other users. The users can also revoke the access rights of another user which then would revoke access from the other users they had granted access to.

2. What are the disadvantages to database encryption?

There are two disadvantages to database encryption which are key management and inflexibility. Key management is a complex task because authorized users must have access to the decryption key but databases are typically accessible to a wide range of users. It is inflexible because it is more difficult to perform record searches if part or all of the database is encrypted.

3. Consider a simplified university database that includes information on courses (name, number, day, time, room number, max enrollment) and on faculty teaching courses and students attending courses. Suggest a relational database for efficiently managing this information and explain why you chose that one.

Course name	Course number	Day	Time	Room Number	Max Enrollment

The course number is a primary key and will be a unique number for the course table.

Faculty Name	Course 1	Course 2	Course 3

Course number is the foreign key. Faculty can teach the same courses in several semesters

Student Name	Course 1	Course 2	Course 3

Course number will be a foreign key.

4. The following table shows a list of pets and their owners that is used by a veterinarian service.

P_Name	Type	Breed	DOB	Owner	O_Phone	O_Email
Kino	Dog	Std. Poodle	3/27/97	M. Downs	5551236	md@abc.com
Teddy	Cat	Chartreaux	4/2/98	M. Downs	1232343	md@abc.com
Filo	Dog	Std. Poodle	2/24/02	R. James	2343454	rj@abc.com
AJ	Dog	Collie Mix	11/12/95	Liz Frier	3456567	liz@abc.com
Cedro	Cat	Unknown	12/10/96	R. James	7865432	rj@abc.com
Woolley	Cat	Unknown	10/2/00	M. Trent	9870678	mt@abc.com
Buster	Dog	Collie	4/4/01	Ronny	4565433	ron@abc.com

(a) Describe four problems that are likely to occur when using this table.

Updating an owner's name or data can only be done in rows, The owner data must be consistent across rows, if you enter data in the table inconsistently there will be a problem, and there is no place to store your customer data unless they have a pet.

(b) Break the table into two tables in a way that fixes the four problems.

Pet	Pet ID	Pet Name	Type	Breed	DOB	Owner Phone

Owner	Owner Name	Owner Phone	Owner Email

5. Consider an SQL statement:

SELECT id,forename,surname FROM authors WHERE forename='john' AND surname='smith'

(a) What is this statement intended to do?

It retrieves the id, forename, and surname columns from the authors table. Then returns all the rows in the table that match the forename = john and surname = smith

(b) Assume that the forename and surname fields are being gathered from user-supplied input, and suppose the user responds with:

* **Forename: jo'hn**
* **Surname: smith**

What will be the effect?

It will return an error because the insertion of a single quote ' character will break out of the single quote delimited data. So when the database tries to run 'hn' it will fail.

(c) Now suppose the user responds with:

Forename: jo'; drop table authors--
Surname: smith

What will be the effect?

The authors table will be deleted.

6. The following shows a fragment of code that implements the login functionality for a database application. The code dynamically builds an SQL query and submits it to a database.

```
String login , password , pin , query
login = getParameter (" login ");
password = getParameter (" pass ");
pin = getParameter (" pin ");
```

```
Connection conn . createConnection (" MyDataBase ");
query = " SELECT accounts FROM users WHERE login ='" +
        login + "'AND pass ='" + password +
        "'AND pin =" + pin ;
ResultSet result = conn . executeQuery ( query );
if ( result != NULL )
        displayAccounts ( result );
else
        displayAuthFailed ();
```

(a) Suppose a user submits login, password, and pin as doe, secret, and 123. Show the SQL query that is generated.

SELECT accounts FROM users WHERE login='doe' AND pass='secret' AND pin=123

(b) Instead, the user submits for the login field the following: ' or 1 = 1 - - . What is the effect?

SELECT accounts FROM users WHERE login="or 1=1 -- AND pass=" AND pin=

The code that has the conditional (OR 1=1) transforms the WHERE clause into a tautology. Because of this, the query sets to true for each row in the table then returns all. Therefore, this would call displayAccounts() and show all the accounts returned by the database.

7. Consider the parts department of a plumbing contractor. The department maintains an inventory database that includes parts information (part number, description, color, size, number in stock, etc.) and information on vendors from whom parts are obtained (name, address, pending purchase orders, closed purchase orders, etc.). In an RBAC system, suppose that roles are defined for accounts payable clerk, an installation foreman, and a receiving clerk. For each role, indicate which items should be accessible for read-only and read-write access.

Payable clerk:

- Read-write access to both parts information and vendor information.

Installation foreman:

- Read-only access to parts information

Receiving clerk:

- Read-write access to parts information
- Read-only access to vendor information

8. Imagine that you are the database administrator for a military transportation system. You have a table named cargo in your database that contains information on the various cargo holds available on each outbound airplane. Each row in the table represents a single shipment and lists the contents of that shipment and the flight identification number. Only one shipment per hold is allowed. The flight identification number may be cross-referenced with other tables to determine the origin, destination, flight time, and similar data. The cargo table appears as follows:

Flight ID	Cargo Hold	Contents	Classification
1254	A	Boots	Unclassified
1254	B	Guns	Unclassified
1254	C	Atomic bomb	Top Secret
1254	D	Butter	Unclassified

Suppose that two roles are defined: Role 1 has full access rights to the cargo table. Role 2 has full access rights only to rows of the table in which the Classification field has the value Unclassified. Describe a scenario in which a user assigned to role 2 uses one or more queries to determine that there is a classified shipment on board the aircraft.

A scenario in which a user assigned to role 2 could determine if there is a classified shipment would be if they see that there is nothing for cargo hold C and tries to insert a record for it but fails. This tells the user that their is information there but they cannot view it therefore the information must be classified.

9. Users luke and leih do not have the SELECT access right to the Inventory table and the Item table. These tables were created by and are owned by user palpatine. Write the SQL commands that would enable palpatine to grant SELECT access to these tables to luke and leih.

```
AUTHORITY  palpatine
        GRANT     SELECT
        ON        Inventory
        TO        luke, leih;

AUTHORITY  palpatine
        GRANT     SELECT
        ON        Item
        TO        luke, leih;
```

10. Consider a database table that includes a salary attribute. Suppose the three queries sum, count, and max (in that order) are made on the salary attribute, all conditioned on the same predicate involving other attributes. That is, a specific subset of records is selected and the three queries are performed on that subset. Suppose that the first two queries are answered and the third query is denied. Is any information leaked?

Yes, the max query will be denied whenever its value is equal to the ratio of the sum and the count values. This is because the query restriction technique has a weakness which is denial of query. By doing calculations of the sum, count, and max, the first two queries will produce the same result. This query denial will leak info to the hacker. The hacker will then learn all the salary numbers of all the selected rows when denial occurs.