Question 1

Provide suitable short-answers to the following questions.

a) Why do we need database encryption after the implementation of role-based access control? Give a real-world example.

Sol:-

In top security environments we do not want to disclose all database contents (rows) to users granted permission on a certain table. This means users can only see database table rows if s/he has a key assigned that can decrypt that row. So in a military database, two users having select privilege on a table can see only rows that they can decrypt using their own key. This confidentiality can not be achieved only with access control.

b) A user answers a phone call from an individual claiming to be from IT services and requests the user to confirm their username and password for auditing purposes. Explain the form of malware propagation associated with this phone call.

Sol:-

Social engineering attempts to gain the confidence of an employee and convince that person to divulge confidential and sensitive information, such as usernames and passwords.

c) Explain the concept of Cloud Security as a Service (SECaaS). Provide examples of security services typically offered under SECaaS.

Sol:-

SECaaS is a cloud-based delivery model for security services and tools. It allows organizations to outsource their security needs to cloud service providers, enabling them to benefit from specialized security expertise, scalability, and cost-effectiveness.

Examples of Security Services Offered Under SECaaS: Identity and access management, Data loss prevention, Web security, E-mail security, Security assessments , Intrusion management, Security information and event management, Encryption, Business continuity and disaster recovery, Network security

d) List three components (code segment) and four phases of malicious software.

Sol:-

The student needs to define: **Infection mechanism**, **Trigger** and **Payload**.

Infection mechanism: The means by which a virus spreads or propagates, enabling it to replicate. The mechanism is also referred to as the **infection vector**.

• **Trigger:** The event or condition that determines when the payload is activated or delivered, sometimes known as a **logic bomb**.

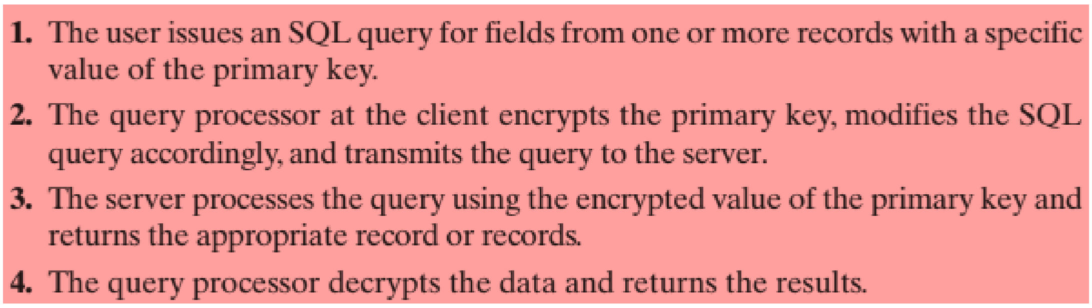
• **Payload:** What the virus does, besides spreading. The payload may involve damage or may involve benign but noticeable activity.

Phases:-

Dormant phase, Propagation phase, Triggering phase, Execution phase

e) Why is RBAC considered fit for database access control?

Sol:-



1. The user issues an SQL query for fields from one or more records with a specific value of the primary key.
2. The query processor at the client encrypts the primary key, modifies the SQL query accordingly, and transmits the query to the server.
3. The server processes the query using the encrypted value of the primary key and returns the appropriate record or records.
4. The query processor decrypts the data and returns the results.

Question 2

a) What would be a successful SQL injection attack given the following SQL statement? Give steps utilized by an attacker for a successful attack. **[1.5]**

SELECT * FROM employee WHERE eid='$eid' AND password='$password';

Sol:-

The potential vulnerability lies in the direct use of user-provided variables $eid and $password without proper validation and sanitization. An attacker can exploit this vulnerability to gain unauthorized access. The attacker recognizes that the SQL statement is constructed using user-provided variables $eid and $password, which are not properly sanitized or validated.

By setting the $eid to ' OR 1=1/* and the $password to */# we can make the SQL query look like this

SELECT * FROM employee WHERE eid='' OR 1=1/*' AND password='*/#'

Filtering out the comments gives us: SELECT * FROM employee WHERE eid='' OR 1=1

The injected code effectively bypasses the authentication check, and the condition 1=1 is always true. As a result, the attacker can potentially log in successfully without providing valid credentials.

b) A series of grant operations for a particular access right is shown in the figure below. Assume that B revokes the access right at t = 70, from C. Display the resulting diagram of access right dependencies using the established conventions. **[1.5]**

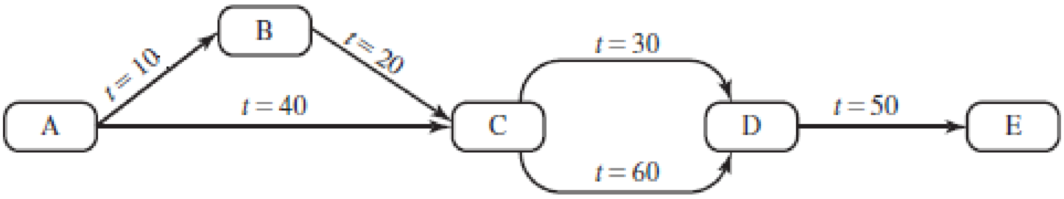
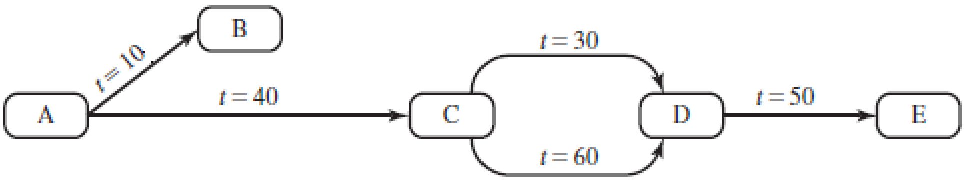


Figure 1

Sol:-



Since, C has redundant rights from A and B.

c) Illustrate how a plain text SQL query is interpreted by an encryption database (data and meta data are both encrypted). **[2]**

Sol:-

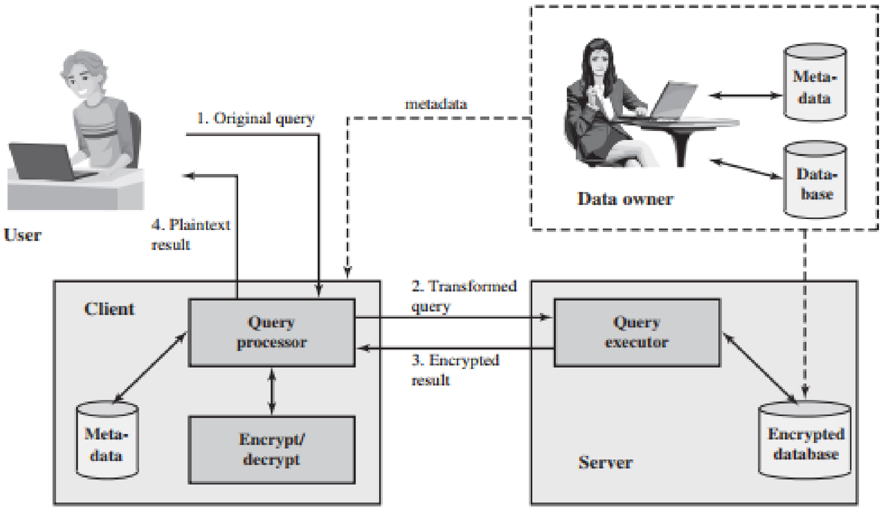


Figure 5.9 **A Database Encryption Scheme**

Question 3

a) Suppose FLEX has RBAC implemented already. When will ABAC become necessary instead of RBAC? Explain. **[1.5]**

Sol:-

In RBAC permission on objects are granted to roles and roles are assigned to users. ABAC provides attributes to users, objects and environment and a dynamic policy to grant access to objects. This means ABAC can be implemented at a finer level than simple permission on objects in RBAC. Attributes and admission policy could be defined arbitrarily providing utmost flexibility to changing internal and external (compliance) requirements. ABAC can start with a simple model and grows (evolve) into a more complex mechanism that can not be implemented in RBAC (similar to the movie example from the textbook).

b) Give one example each for the following cloud specific threat: Insecure interfaces and APIs, Shared technology issues, Data loss or leakage and Account or service hijacking**. [1.5]**

Sol:-

The student needs to provide any 1 real life example of each of the treat

c) Assume you have been hired by the CSE department to establish an Access Control specification for the computer labs and files in it. Describe the advantages and disadvantages of using Discretionary Access Control (DAC) or Role-Based Access Control (RBAC) to implement your policy. Give a sample specification of access permission for Role-Based Access Control (RBAC) **[2]**

Sol:-

DAC:

Can be very intuitive and easy to implement. However, depending on the number of students, resources, and the permitted accesses, the administration of the security policy can be overwhelming and error prone.

RBAC:

Simplifies administration, assigning users to roles and privileges to roles. Each user can use the privileges that are assigned to the roles that the user is assigned to. Generally, roles are more static and permanent than the user population, therefore, requiring less administration.

Sample specification:

1. **Roles:** student, faculty

2. **Users:** Mary , John

3. **Privileges:** (file1, +read) ; (file1, +write) ; (file1, -read) ; (file1, -write)

4. **User-Role assignment:** (Mary , student) ; (John , faculty)

5. **Role-privilege assignment:**
students: (file1, +read); (file1, -write)

Faculty: (file1, +read) ; (file1, +write)

----------(O)----------