Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
MASTER OF SCIENCE IN INFORMATION SYSTEMS SECURITY
END OF SEMESTER EXAMINATION
MST8302 – ENTERPRISE SECURITY

DATE: 3rd October 2023 Time: 2 Hours

Instructions

1. This examination consists of **SEVEN** questions. You can get up to **40 points**.
2. Answer **all** the questions.
3. For each question, provide the answers according to the **instructions** (the instructions describe a style and level of detail of the answers).

Questions

1. Describe IT security concepts of Confidentiality, Integrity, Availability, and Non-repudiation. **(4 points)**

2. Describe which access control model (one of the four basic access control models) is implemented in the SQL standard and which SQL statements can be utilized to control the access to database objects and how. Provide an example of an SQL statement setting permissions to query (but not to modify) database table “employee” for user “bob”. **(6 points)**

3. Describe three different strategies on where Authentication and Authorization (AA) of a user should be performed (i.e., AA at application/database levels; both AA at one of those levels, as well as each of AA at different levels). What are advantages and disadvantages of these strategies? Also describe the concept of a "proxy user" in the case of Authentication at the application level and Authorization at the database level strategy. **(8 points)**

4. Describe which database triggers and views can be used (and how) to implement a Virtual Private Database to restrict access to specific columns and rows of table “employee” for particular database users (use “USER” variable or function to get the username of the current user). It is not necessary to write syntactically and semantically correct SQL statements (e.g., for Oracle views, triggers, or table alterations), however, you need to describe a list of views and/or triggers and possible modifications of the structure of the table (its database schema) and/or user permissions, and their purposes, properties, and usage in the approach. **(7 points)**

5. What is the purpose, advantages and disadvantages of data encryption at application, database, and operating system levels? **(4 points)**

6. What are Control Columns in relational database tables? Provide at least three examples of different control columns and explain how they can be utilized in database audit. **(4 points)**

7. An information system has the following source code in Java with JDBC API to authenticate a user by his/her password (i.e., to verify that a given username and a given password exist together as a row in 'user' table; method 'Statement.executeQuery' submits a given SQL query to a relational database and returns a set of resulting rows as the query response; method 'ResultSet.next' returns 'true' if there are any resulting rows in the query response, 'false' otherwise; the user is successfully authenticated if, and only if, the value of 'userHasBeenAuthenticated' output variable will be 'true' after the execution of the code).

   The source code:

   ```
   final ResultSet rs = stmt.executeQuery("SELECT 1 FROM user WHERE username = '" +
   username + "' AND password = '" + password + "';");
   final boolean userHasBeenAuthenticated = rs.next();
   ```

   What values of input text (string) variables 'username' and 'password' can be utilized to bypass the authentication by SQL Injection attack without knowledge of a correct username and password? **(7 points)**