Strathmore
UNIVERSITY

FACULTY OF INFORMATION TECHNIOLOGY
MASTER OF SCIENCE IN INFORMATION SYSTEMS SECURITY
END OF SEMESTER EXAMINATION

MST 8302 Enterprise Security

DATE: 02nd OCTOBER 2019 Time: 2 Hours

Instructions

1. This examination consists of **SEVEN** questions. You can get up to **40 points**.
2. Answer **all** the questions.

Questions

1. Describe IT security concepts of Authorization, Accounting, and Authentication. In which order do these concepts have to be implemented and why? Provide an example. **(6 points)**

2. Briefly describe the four basic access control models: Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role Based Access Control (RBAC), and Rule Based Access Control (RBAC or RB-RBAC). **(8 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 theses 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. Why do we need Fine-grained Access Control in database security (why SQL Data Control Language statements are not good enough) and how it can be implemented by Virtual Private Database approach? **(4 points)**

5. What is Polyinstantiation and Cover Stories? Why and how can the polyinstantiation be used to secure sensitive informations? **(5 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 login/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 management system 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). **(5 points)**

The source code:

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

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