



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

DATE: 14th April 2026

Time: 2 Hours

Instructions

1. This examination consists of **EIGHT** questions and is worth a maximum of **50 points**.
2. Answer **all questions**.
3. For each question, provide your answers in the style and with the level of detail specified in **the instructions**.

Questions

1. Describe IT security concepts of Confidentiality, Integrity, Availability, and Non-repudiation. **(6 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 the concept of a "proxy user" in the case of Authentication at the application level and Authorization at the database level. Describe the individual steps of interaction between an end-user, an application layer (front end), and a database layer (back end) during the authentication process. How can the proxy user concept be implemented in Oracle database? **(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 in Virtual Private Databases (two approaches)? **(6 points)**
5. What is the purpose of Data Masking and Data Redaction and how they affect query results? Are there any differences between these two? Provide examples. **(6 points)**
6. What is Polyinstantiation and Cover Stories? Why and how the polyinstantiation can be used to secure private information? **(5 points)**
7. Define database auditing and explain the 'Why, When, and How' of its implementation within an enterprise environment. Critically compare the Database Auditing process against Quality Assurance (QA) and Performance Monitoring. In your comparison, highlight the distinct objectives and the types of data collected for each process. **(6 points)**

8. 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 is any resulting row 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)**