DUBLIN INSTITUTE OF TECHNOLOGY

DT211C/4 BSc. (Honours) Degree in Computer Science (Infrastructure)

DT228/4 BSc. (Honours) Degree in Computer Science

DT282/4 BSc. (Honours) Degree in Computer Science (International)

SUMMER EXAMINATIONS 2017/2018

ENTERPRISE APPLICATION DEVELOPMENT [CMPU4023]

MR. BRIAN GILLESPIE
DR. DEIRDRE LILLIS
MR. ALAN FAHEY – DT211C
MR. PATRICK CLARKE – DT228/DT282

WEDNESDAY 16TH MAY 2.00 P.M. – 4.00 P.M.

TWO HOURS

QUESTION 1 IS **COMPULSORY.**
ANSWER QUESTION 1 **AND** ANY TWO OF THE OTHER THREE QUESTIONS.
QUESTION 1 IS WORTH 40 MARKS, ALL OTHER QUESTIONS ARE WORTH 30 MARKS
ILLUSTRATE YOUR ANSWERS WITH APPROPRIATE EXAMPLES AND DIAGRAMS

1 (a) In the context of enterprise application design, distinguish between a monolithic architectures and a service-oriented architectures (SOA). Mention one advantage and one disadvantage of the SOA approach to enterprise application construction.

(8 Marks)

(b) Explain how object-relational mapper (ORM) works using a simple example of your choice. What are the potential disadvantages of using an ORM over a direct SQL interface?

(8 Marks)

(c) Remote APIs can be implemented using a number of different paradigms. Briefly explain each of the following approaches and describe the main differences between them.

- Message Passing
- Remote Procedure Calls

(8 Marks)

(d) Explain the typical vulnerability that an attacker is able to exploit in an SQL-injection attack and how the attack works. Mention two ways that this vulnerability can be prevented.

(8 Marks)

(e) Describe the difference between user authentication and user authorisation in the context of enterprise API security. Explain how these concepts are related to enterprise identity management.

(8 Marks)

2 (a) Representational State Transfer (REST) has been described as a stateless client-server API design pattern. Describe the principles behind REST and how it works

(10 Marks)

(b) Consider a hypothetical service API for an ecommerce shopping cart having the following exposed resources:

Products	Items that can be bought including name, price, description, etc
OrderItems	Zero or more order items in the order, pending checkout and payment
Orders	Order items committed for purchase
Customers	Product purchasers, including delivery details

Provide the RESTful API interfaces that can perform the following actions. Illustrate each answer by providing an example REST query and response bodies, including the HTTP verbs, URIs, any query parameters and response status codes

- List all computer products for sale from €1 to €575 in price
- Add a product to the cart, specifying a quantity
- Create a new customer order
- Cancel a specific order
- List all orders for a given customer for the past 12 months

(20 Marks)

3 (a) Describe, in detail, the following API authentication schemes. In your answer, explain the use cases in which each is an appropriate approach.

- JSON Web Tokens
- Hash-based Message Authentication

(18 Marks)

(b) Consider the following security compromises on the authentication schemes in part (a). What is the minimum remedial action is required for each situation? State any assumptions you are making

- A user JWT has been obtained by an attacker
- The system JWT signing key has been leaked
- A user's secret key has been exposed

(12 Marks)

4 (a) One of the desirable characteristics of an API is that is should be learnable by its consumer - typically an application developer charged with implementing an API client in code. What, in your opinion, should good documentation describe about an API?

(10 Marks)

(b) Describe, in detail, the following approaches to API specification and documentation. Mention one advantage of each approach:

- Open API Specification (Swagger)
- GraphQL (Facebook)

(20 Marks)