Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2023/2024

COURSE NAME	:	SOFTWARE ENGINEERING SECURITY
COURSE CODE	:	BIE 33003
PROGRAMME CODE	:	BIP
EXAMINATION DATE	:	JULY 2024
DURATION	:	3 HOURS
INSTRUCTIONS	:	1. ANSWER ALL QUESTIONS 2. THIS FINAL EXAMINATION IS CONDUCTED VIA ☐ Open book ☒ Closed book 3. STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK

THIS QUESTION PAPER CONSISTS OF **FOUR (4)** PAGES

Q1 Answer **Q1 (a)** and **Q1(b)** based on **Figure Q1.1**

"A condition at an interface under which more input can be placed into a fender or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system."

Figure Q1.1

(a) Determine what is the software vulnerability type that described in **Figure Q1.1**.

(2 marks)

(b) Suggest **TWO (2)** countermeasures that can be implemented to overcome the software vulnerability answered in **Q1(a)**.

(4 marks)

(c) Which of the following statements are **TRUE** or **FALSE**.

(i) Many software security vulnerabilities are result from poor programming practices.

(1 mark)

(ii) Security flaws occur as consequence of sufficient checking and validation of data and error code in programs.

(1 mark)

(iii) Defensive programming assumes nothing check all potential errors.

(1 mark)

(iv) Software security is closely related to software quality and reliability.

(1 mark)

Q2 Answer **Q2 (a)** and **Q2 (b)** based on **Figure Q2.1**

"**Freedom bookstore** is a book shop that does sell different types of reading materials. The manager of the bookstore has used a database for their ordering system to enable customers' orders their books. The tables and their design requirements are as follows:

- The bookstore sells many different books. These books are group into Category ID, where each category may have at least one or many books. These books were identified by Book ID, whereas the other additional attributes are title, author, price, and publisher.

Customers submit order for books. The identifier for order is Order ID. Each order should have order date, books ordered by customer and total price for the order. One customer may submit any number of orders. However, customers may need not submit ANY orders. The identifier of customer is Customer ID. Other information includes customer name, address, postcode and phone number. ."

Figure Q2.1

(a) Develop a secure relational database schema to manage the information for Freedom Bookstore.

(10 marks)

(b) Design an access control policy using Role-Base Access Control (RBAC).

(10 marks)

Q3 Answer **Q3 (a)** to **Q3 (e)** based on **Figure Q3.1** in **Appendix A**

(a) Develop a use case diagram.

(10 marks)

(b) Outline **THREE (3)** critical assets.

(3 marks)

(c) Determine **THREE (3)** main security goals for the assets answer in **Q3(b).**

(10 marks)

(d) Based on security goals answered in **Q3 (C)**,

(i) Model the threat to the system using misuse case diagram.

(10 marks)

(ii) Asses the risks

(5 marks)

(iii) Specify the related security requirements.

(12 marks)

(iv) Suggest **ONE (1)** security mechanism to be applied for each of security requirements specified in **Q3(d) (iii).**

(10 marks)

(e) Develop the most suitable architecture design using separation of privileges design principle and protection architecture.

(10 marks)

- END OF QUESTIONS -

APPENDIX A

A patient Information system for mental health care.

A regional health authority wishes to procure an information system to help manage the care of patients suffering from mental health problems. A patient information system to support mental health care is a medical information system that maintains information about patients suffering from mental health problems and the treatments that they have received. Most mental health patients do not require dedicated hospital treatment but need to attend specialist clinics regularly where they can meet a doctor who has detailed knowledge of their problems. To make it easier for patients to attend, these clinics are not just run in hospitals. They may also be held in local medical practices or community centres. The mental health care patient management system is also an information system that is intended for use in clinics. It makes use of a centralised database of patient information but also has been designed to run on a PC, so that it may be accessed and used from sites that do not have secure network connectivity. When the local systems have secure network access, they use patient information in the system's database but they can download and use local copies of patient records when they are disconnected. The system is not a complete medical records system so does not maintain information about other medical conditions. However, it may interact and exchange data with other clinical information system.

The overall goals of the system are twofold: 1. To generate management information that allows health service managers to assess performance against local and government targets. 2. To provide medical staff with timely information to facilitate the treatment of patients. The health authority has several clinics that patients may attend in different hospitals and in local health centres. Patients need not always attend the same clinic and some clinics may support 'drop in' as well as pre-arranged appointments. The nature of mental health problems is such that patients are often disorganised so may miss appointments, deliberately or accidentally lose prescriptions and medication, forget instructions, and make unreasonable demands on medical staff. In a minority of cases, the patients may be a danger to themselves or to other people. They may regularly change address and may be homeless on a long-term or short-term basis. Where patients are dangerous, they may need to be 'sectioned' – confined to a secure hospital for treatment and observation. Users of the system include clinical staff (doctors, nurses, health visitors), receptionists who make appointments and medical records staff. Reports are generated for hospital management by medical records staff. Management has no direct access to the system. The system is affected by two pieces of legislation (in Malaysia, Acts of Parliament). These are the Data Protection Act that governs the confidentiality of personal information and the Mental Health Act which is known as Mental Health Act 2001 and has been amend as Mental Health (Amendment) Act 2023 that governs the compulsory detention of patients deemed to be a danger to themselves or others. The system is NOT a complete medical records system where all information about a patients' medical treatment is maintained. It is solely intended to support mental health care so if a patient is suffering from some other unrelated condition (such as high blood pressure) this would not be formally recorded in the system.

(Sommerville, 2011)

Figure Q3.1