UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2015/2016

COURSE NAME	:	SOFTWARE ENGINEERING SECURITY
COURSE CODE	:	BIE 33003
PROGRAMME CODE	:	BIP
EXAMINATION DATE	:	JUNE / JULY 2016
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **FIVE (5)** PAGES

SECTION A

Instruction: Choose the BEST answer for each of the following questions.

Q1 "Information systems should be configured to require strong passwords," is an example of a security _____________statement.

A. requirement
B. policy
C. objective
D. control

(2 marks)

Q2 The process of identifying a valid user and matching strong password of an information system is known as _____________.

A. authentication
B. strong authentication
C. Two-factor authentication
D. single sign-on

(2 marks)

Q3 When an information system authenticates a user based on "what the user is," this refers to the use of _____________.

A. authorization based upon the user's job title
B. role-based authentication
C. two-factor authentication
D. biometric authentication

(2 marks)

Q4 The following are categories of intruders **EXCEPT** _____________.

A. masquerader
B. misfeasor
C. hacker
D. clandestine user

(2 marks)

Q5 The best time to introduce security into software application is during ______________ phase.

A. Implementation
B. Design
C. Development
D. Testing

(2 marks)

SECTION B

Q6 (a) State **TWO (2)** purposes of database auditing.

(4 marks)

(b) Outline **THREE (3)** processes involve in auditing a database management of a software system.

(6 marks)

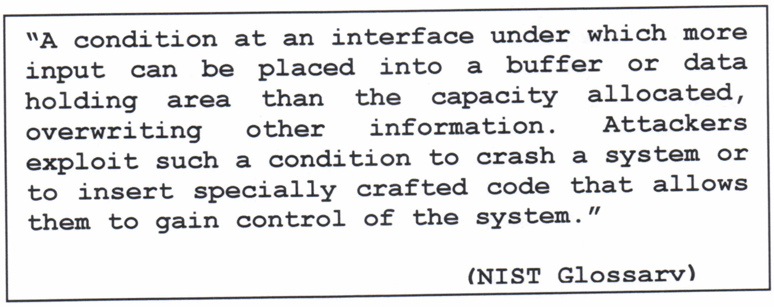
(c) Determine the information accessible level (read-only, read-write and etc) for each role in **Figure Q6(c).** Justify your answer.

> *Consider the Accounting Department of Syarikat ABC. The department maintains an accounting database that include accounts information (vendor, debit and credit details, dates of transactions, assets, number in stock, bills payable, amounts receivable, etc) and information on vendors from whom materials are obtained (name, address, pending purchase orders, closed purchase orders, etc). The roles in the Accounting Systems are defined as account clerk, an account manager, and a finance officer.*

Figure Q6 (c)

(10 marks)

Q7 Questions **Q7(a)-Q7(c)** are based on **Figure Q7**.



"A condition at an interface under which more input can be placed into a buffer 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."

(NIST Glossary)

Figure Q7

(a) Specify the type of software vulnerability defined in **Figure Q7**.

(2 marks)

(b) Suggest **THREE (3)** techniques to overcome the problem caused by the software vulnerability specified in **Q7(a)**.

(6 marks)

(c) Discuss **THREE (3)** other types of software vulnerabilities that occur in software development and their corresponding techniques to overcome the problems.

(12 marks)

(Q8) Questions **Q8(a)-Q8(d)** are based on **Figure Q8**

> This is a scenario of student registration system. The system will enable the student to register courses. A drop course option should be enabled. Student may view registered courses either by display or print. Lecturer can view student registration whereby he/she can view only his/her own taught course. Lecturer can have option to print the student registration list. Nevertheless, lecturer neither creates nor removes courses. This job is under the responsibility of the administrator who can create a new semester as well. A remove course option should be enabled.

Figure Q8

(a) Outline **FIVE (5)** critical assets for the registration system. Support your answer with a use case diagram.

(14 marks)

(b) For each asset listed in **Q8 (a),**

(i) determine a related security goal.

(12 marks)

(ii) determine the related threats. Support your answer with a misuse case diagram and any related diagram.

(8 marks)

(iii) analyze the related risks.

(8 marks)

(iv) produce the related security requirements.

(8 marks)

- END OF QUESTION -