

CONFIDENTIAL



UTHM

Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

**FINAL EXAMINATION
SEMESTER II
SESSION 2017/2018**

**COURSE NAME : SOFTWARE ENGINEERING
SECURITY**

COURSE CODE : BIE 33003

PROGRAMME CODE : BIP

EXAMINATION DATE : JUNE / JULY 2018


DURATION : 3 HOURS

INSTRUCTION : ANSWER ALL QUESTIONS

TERBUKA

THIS QUESTION PAPER CONSISTS OF FIVE (5) PAGES

CONFIDENTIAL

- Q1** The following statements are the requirements of an Intrusion Detection System (IDS).
- i. Run continually with minimal human supervision.
 - ii. Be fault tolerant that it must be able to recover from system crashes.
 - iii. Impose a minimal overhead on the system where it is running.
 - iv. Be able to scale to monitor a large number of hosts.
- A. i, ii, iii, iv
 - B. i, ii, iii,
 - C. ii, iii, iv
 - D. All of the above.
- (2 marks)
- Q2** As a security manager, what are the elements that should be considered in developing a data classification policy?
- A. Sensitivity levels, marking procedures, access procedures and handling procedures.
 - B. Labeling procedures, access procedures and handling procedures.
 - C. Sensitivity levels, access procedures and handling procedures.
 - D. Sensitivity levels and handling procedures.
- (2 marks)
- Q3** What measures should be taken by an organization to surplus its old desktop computers considering the data remains?
- A. Erase the hard drives.
 - B. Format the hard drives.
 - C. Activate its TEMPEST shielding.
 - D. Clear the computers' RAM.
- (2 marks)
- Q4** What is the best defense against social engineering?
- A. Spyware filters.
 - B. Firewalls.
 - C. Data leakage protection (DLP).
 - D. Security awareness training.
-  (2 marks)

Q5 The best time to introduce security into an application is:

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

(2 marks)

Q6 (a) Discuss **THREE (3)** challenges of Database Security.

(6 marks)

(b) Explain **THREE (3)** requirements for the security of a database system.

(6 marks)

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

Consider the parts department of a plumbing contractor. The department maintains an inventory database that includes parts information (part no., description, color, size, quantity in stock, etc.) and information on vendors from whom parts are obtained (name, address, pending purchase orders, closed purchase orders, etc.). In an RBAC system suppose, that roles are defined for accounts payable clerk, an installation foreman, and receiving clerk. For each role, indicate which items should be accessible for read-only and read-write access.

Figure Q6

(8 marks)

Q7 (a) Determine **FOUR (4)** critical security flaws that related to insecure software code.



(4 marks)

(b) Modularity, low coupling and high cohesion are techniques that have been known as good design concepts in programming and software development. Discuss how the implementation of these concepts help software engineering security.

(8 marks)

- (c) Suggest at least **THREE (3)** techniques that required for testing a secure application software. Determine when and how they need to be implemented in software development process.

(8 marks)

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

PHILIPPINE BANKS ON ALERT AFTER CYBER ATTACK AT MALAYSIA CENTRAL BANK

MANILA: The Philippine central bank has sounded an alert to local financial institutions following a cyber attack at the Malaysian central bank, in which hackers sought to steal money using fraudulent wire transfers, its governor said on Saturday.

Bank Negara Malaysia (BNM) has said no funds were lost in the incident, which it identified on Tuesday, and involved falsified wire-transfer requests over the SWIFT bank messaging network, the latest in a series of electronic heists at financial institutions around the world.

"We issued a general alert reminder as soon as we got BNM advisory to be extra careful over the long holiday. Although banks already do that as SOP (standard operating procedure)," Bangko Sentral ng Pilipinas Governor Nestor Espenilla said in a phone message.

"Information sharing is part of enhanced defensive protocols against cyber-crime," Espenilla said.

The alert was issued on Wednesday, and there had been no specific threat, officials said.

Bank Negara did not say who was behind the hack or how they accessed its SWIFT servers. The central bank, which supervises 45 commercial banks in Malaysia, said on Thursday there was no disruption to other payment and settlement systems the central bank operates because of the cyber attack.

In February 2016, the Philippine financial system was thrown into the global spotlight after \$81 million that was stolen from Bangladesh central bank was channelled into several accounts at Manila-based Rizal Commercial Banking Corp (RCBC), before disappearing into the local casino industry.

The Bangladesh heist led financial institutions around the globe to bolster security. There is no word on who was responsible and Dhaka has been able to retrieve only about \$15 million.

The Philippine central bank fined RCBC a record one billion pesos (\$20 million) in 2016 for its failure to prevent the movement of the stolen money through it. RCBC has blamed rogue employees for the incident. - REUTERS

(Adopt from : <https://www.nst.com.my/world/2018/04/351510/philippine-banksalert-after-cyber-attack-malaysia-central-bank>, 1 April 2018)

TERBUKA

Figure Q8

- (a) Identify **TWO (2)** vulnerabilities that may cause the attack. (4 marks)
- (b) Suggest **TWO (2)** approaches that can be done as the countermeasure for each vulnerability identified in **Q8(a)**. (6 marks)
- (c) Determine **FOUR (4)** critical assets in the SWIFT bank system. (6 marks)
- (d) For each asset listed in **Q8(c)**,
- (i) determine a related security goal. (12 marks)
 - (ii) determine the related threats. Support your answer with a misuse case diagram or any related diagram. (8 marks)
 - (iii) analyze the related risks. (6 marks)
 - (iv) produce the related security requirements. (8 marks)

TERBUKA

- END OF QUESTION -