

CONFIDENTIAL



UTHM

Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

**FINAL EXAMINATION
SEMESTER I
SESSION 2018/2019**

COURSE NAME : SPECIAL TOPICS IN
INFORMATION SECURITY

COURSE CODE : BIS 33403

PROGRAMME CODE : BIS

EXAMINATION DATE : DECEMBER 2018 / JANUARY 2019

DURATION : 3 HOURS

INSTRUCTION : ANSWER ALL QUESTIONS

THIS QUESTION PAPER CONSISTS OF FIVE (5) PAGES

CONFIDENTIAL

TERBUKA

SECTION A

State whether these statements are TRUE or FALSE.

- Q1** Cloud computing gives you the ability to expand and reduce resources according to your specific service requirement.
- Q2** Infrastructure as a Service (IaaS) provides service to customers in the form of software, specifically application software, running on and accessible in the cloud.
- Q3** There is an increasingly prominent trend in many organizations to move a substantial portion or even all IT operations to enterprise cloud computing.
- Q4** In a public cloud model, the provider is responsible both for the cloud infrastructure and for the control of data and operations within the cloud.
- Q5** The major advantage of the public cloud is cost.
- Q6** Security assessments are third-party audits of cloud services.
- Q7** An Intrusion Prevention System (IPS) is a set of automated tools designed to detect unauthorized access to a host system.
- Q8** The security module for *OpenStack* is Keystone.
- Q9** The *smart* features in a smart device is provided by a deeply embedded actuator.
- Q10** A key element in providing security in an Internet of Things (IoT) deployment is the gateway.

(10 marks)

SECTION B

Answer ALL questions.

Q11 (a) Provide **TWO (2)** differences between Mass Phishing and Spear Phishing attacks.

(5 marks)

(b) Suggest **THREE (3)** actions for a victim of Voice Phishing.

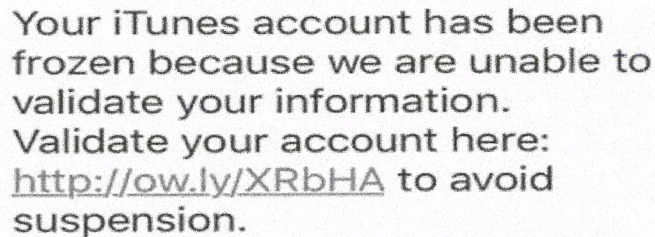
(6 marks)

(c) Based on the following scenario:

(12 marks)

Haris recently received several SMS messages claiming that her iTunes account has been frozen due to some security reasons. Haris responds to the SMS and it redirects him to a login page, where he enters his username and password. The following day, Haris realized the SMS is a phishing attack when his friends also received the same message.

Identify **SIX (6)** characteristics of SMS Phishing according to **Figure Q11(c)**.



Your iTunes account has been frozen because we are unable to validate your information. Validate your account here: <http://ow.ly/XRbHA> to avoid suspension.

Figure Q11(c)

Q12 (a) Justify **FIVE (5)** security risks of Social Networking

(10 marks)

(b) Justify **FOUR (4)** security risk solutions based on your answer in Q12(a).

(8 marks)

- (c) Based on the following scenario:

(10 marks)

In May 2017, Russian hackers gained access to the computer of a Pentagon official, who opened a Twitter link about a 'family friendly summer vacation'. There were also 10,000 attempts on Twitter accounts for people in the Department of Defence. No matter how secure you are, it just takes one person to open up your network to attack. Even a smaller social network like LinkedIn can be targeted. Although it has about a quarter of the users that Facebook has, it is mainly a business-to-business social networking site. In August 2017, a bogus profile from someone calling themselves Mia Ash went around LinkedIn, offering more personal chats on Facebook. If a friend request was accepted, an email was sent including a fake Word or Excel document that launches a remote access Trojan if macros are enabled.

Suggest **FIVE (5)** security practices that will help your organization from social networking attacks according the scenario above.

- Q13** (a) Suggest **TWO (2)** examples of Internet of Things (IoT) application. (4 marks)
- (b) Describe **THREE (3)** Home Internet of Things (IoT) security attacks. (6 marks)
- (c) Sketch an IoT network design for Smart Home which consist of sensor, wireless, server and Internet. (10 marks)
- Q14** (a) Describe **TWO (2)** differences between Augmented Reality (AR) and Virtual Reality (VR). (4 marks)
- (b) Explain **TWO (2)** security and privacy attacks for Augmented Reality (AR). (5 marks)

(c) Based on the following scenario:

(10 marks)

Today's educational environment is increasingly offering immersive experiences such as mobile Augmented Reality (AR). This technology help children, teens, and adults truly enjoy the process of learning. However, there are some limitation of AR that make the school still used the traditional learning method.

Justify **FIVE (5)** advantages and **FIVE (5)** disadvantages for mobile Augmented Reality (AR) in the classroom.

- END OF QUESTION -

TERBUKA
CONFIDENTIAL

