MURANG'A UNIVERSITY OF TECHNOLOGY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

UNIVERSITY ORDINARY EXAMINATION

2018/2019 ACADEMIC YEAR

FOURTH YEAR **FIRST** SEMESTER EXAMINATION

SIT 403 – SYSTEM SECURITY AND AUDIT

DURATION: 2 HOURS

DATE:

TIME:

Instructions to candidates:

1. Answer question One and Any Other Two questions
2. Mobile phones are not allowed in the examination room.
3. You are not allowed to write on this examination question paper.

SECTION A: ANSWER ALL QUESTIONS IN THIS SECTION

QUESTION ONE (30 MARKS)

a) Describe four kinds of security breaches associated with computer security (4marks)

b) Outline four types of biometrics that are used for authentications, discussing any two types of errors that occur when biometrics are used for authentication (4marks)

c) Explain how an audit log can be used as recovery tool (3marks)

d) Discuss 3 factors that need to be put into consideration when making across decisions in a DBMS (6marks)

e) Define the following terms as used in system security and Audit

i. Risk

ii. Security policy

iii. System Resource

iv. Usurpation

v. Deception (5marks)

f) Provide a brief description of how location based authentication can be used within the banking industry (5marks)

g) Explain why physical security is needed (3marks)

SECTION B – ANSWER ANY TWO QUESTIONS IN THIS SECTION

QUESTION TWO (20 MARKS)

a) Discuss the three goals of security (6marks)

b) Outline two vulnerabilities associated with each of the following;

i. Hardware (2marks)

ii. Software (2marks)

iii. Data (2marks)

c) (i) Discuss the two aspects of a virus (4marks)

(ii) Differentiate between virus types and virus variations (4marks)

QUESTION THREE (20 MARKS)

a) (i) with the aid of a well labeled diagrams, distinguish between a screening router, a proxy gateway and a guard (9marks)

(ii) Describe the defenses –in-depth strategy and explain why it is important (5marks)

b) Outline the four requirements that an e-commerce system must meet for it to be considered to be secure (4marks)

c) Distinguish between identification and authentication (2marks)

QUESTION FOUR (20 MARKS)

a) (i) Provide a brief description of how keystroke verification works (4marks)

(ii) Detail how a brute force attack can be perpetrated on a password (4marks)

b) Describe how intrusion detection and penetration testing can be implemented on a network (6marks)

c) Discuss the security threats associated with microwave transmission (6marks)