MACHAKOS UNIVERSITY COLLEGE

University Examinations 2016/2017

SUPPLEMENTARY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE

SCO 406 : computer systems security

DATE: DECEMBER 2018 **TIME: 2 HOURS**

INSTRUCTIONS: ANSWER QUESTION ONE AND ANY OTHER TWO QUESTIONS

QUESTION ONE (30 MARKS)

a. Describe business model for information system security (8 Marks)

b. What is a dictionary attack? Briefly describe the two types of dictionary attacks. **(6 Marks)**

c. Explain the following design principles mean **(6 Marks)**

   i. Fail-safe defaults

   ii. Economy of mechanisms

   iii. Psychological acceptability

d. Expalin three main types of firewalls. (6 Marks)

e. Distinguish between Computer security and Information security (4 marks)

QUESTION TWO (20 MARKS)

a. Describe the following information security risks in the contest of machakos university (16 Marks)

   i. Assets security risk

   ii. people security risks

   iii. operational risk

iv. communications security risk

b. Differentiate between the two IPSec protocols **(4 Marks)**

QUESTION THREE (20 MARKS)

a. What are the two types of intrusion detection systems? Differentiate between them by writing their characteristics. **(6 Marks)**

b. Discuss two key elements that a security plan should address and state what they mean **(8 Marks)**

c. RSA can be used to support secrecy, authenticity and integrity. Illustrate how it can be used in the following scenarios;

i. Mary wishes to send a secret message M to John (3 marks)

ii. Mary wishes to send a message M to John such that John is assured that the message could only have originated from Mary (3 marks)

QUESTION FOUR (20 MARKS)

a. A computer virus is a self propagating computer program designed to alter or destroy a computer system resource. Describe four techniques that can be used to manage viruses in a computer. (8 marks)

b. You return to Javalicious, the handy coffee shop nearby with free WiFi. You again settle in for an afternoon of web-surfing and tweeting. You know that the network sends all packets unencrypted, and you are not surprised to again see Prof. Evil seated at the table next to yours, using a laptop connected to the same WiFi network. For your web connections, consider the basic security properties of confidentiality, integrity, and availability. For each of these, analyze three scenarios:

- DNSSEC-only means that for a given web site, your laptop looks up all of the domain names for your web session using DNSSEC (including NSEC3); your actual web traffic, however, uses HTTP.

• HTTPS-only means that for a given web site, your laptop looks up all of the domain names for your web session using ordinary DNS; your actual web traffic, however, uses HTTPS.

• DNSSEC+HTTPS means that both your domain name lookups use DNSSEC and your actual web traffic uses HTTPS. In the following, circle YES if using only his laptop (no additional equipment) Prof. Evil can undermine the given property for your web connections, or NO if not. At the end of each section, supply a brief explanation for your answers. **(12 Marks)**

i. Confidentiality of your web connection content

ii. Confidentiality of keeping private what sites you communicate with

iii. Availability of your web connections

QUESTION FIVE (20 MARKS)

a. Explain at least four kind of information contained in a certificate. (8 Marks)

b. KCB has successfully implemented IS security on their distributed systems especially in system access control.

i. Discuss three techniques that they might have used to secure their network. (6 marks)

ii. Explain three main objectives of IS security that they wanted to achieve. (6 marks)