Kirinyaga University

**UNIVERSITY EXAMINATION 2018/2019**

**YEAR IV SEMESTER I EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY**

**BIT 2317-Computer Systems Security Year Iv Semester I 2018**

DATE: Wednesday 5th December 2018 TIME: 2.00pm – 4.00pm

INSTRUCTIONS

*Answer question one (compulsory) and any other two questions*

**Question One (30mks)**

a) Encryption is arguably most important/versatile tool for network security. Describe any three kinds of encryption in networks (6 Marks)

b) In computer security there are five basic method of defence from an attack, with reference to these methods describe how you would protect the KyU finance management sever from an attack. (5 marks)

c) Describe what understand by the term Intrusion detection prevention programs (IDPS) (2 Marks)

d) In the context of computers, security generally means three things: confidentiality, integrity and availability (CIA). A computing system is said to be secure if it has all three properties. Making reference to CIA describe how you would secure the KyU examination management system. (6 Marks)

e) Developers often think of software quality in terms of faults and failures. (6 Marks)

(i) How do software vulnerabilities fit into this scheme of faults and failures?

(ii) Is every fault a vulnerability?

(iii) Is every vulnerability a fault?

f) Define what loose lipped systems are within computer systems and using an example illustrate how you would control this system vulnerability (5 marks)

**Question Two (20mks)**

Assurance is the process used to justify our confidence in the security features present in an operating system. Describe the three techniques used to demonstrate presence or lack of required security features in operating systems (6 marks)

Not all of security is addressed by technology. Justify this system (1 Mark)

Describe any three non-technical measures you would implement to complement the technical measures in securing the computer labs at KyU (6marks )

Define the term firewall and state its role as a network security tool (3Marks)

Describe the following firewall default behaviour (4 marks)

(i) Default permit

(ii) Default deny

**Question Three (20mks)**

a) Describe the term defence in depth (2 marks )

b) An operating system can support separation and sharing in several ways, offering protection at any of several levels. Describe each of the following Security Methods offered by the Operating Systems (8 marks)

(i) Do not protect

(ii) Isolate different processes

(iii)Share all or nothing

(iv)Share via access limitation

c) Describe any three network security control measures that you would implement at KyU if you were the network administrator (6 marks)

d) Explain the Principle of effectiveness as used in computer security (2Marks)

e) List any two reasons why you would recommend the use of intrusion preventions systems (IPS) with an network (2 marks )

**Question Four (20mks)**

a) List any four functions of a security policy (4 marks)

b) Risk Analysis is one the first steps in securing any computer systems, describe how you would carry out a Risk Analysis for KyU systems. (6 marks)

c) Distinguish between a program fault and program failure (4 marks)

d) Early computer security work used "penetrate and patch" method where analysts searched for and repaired faults. Outline any three reasons why this approach (patch efforts) Often made system less secure. (6marks)

**Question Five (20 marks)**

a) With the aid of examples justify the following statements (8 Marks)
   (i) Interruption – attack on availability
   (ii) Interception – attack on confidentiality
   (iii) Modification – attack on integrity
   (iv) Fabrication – attack on authenticity

b) Describe the two phase update as a security requirement for databases (4 marks)

c) Define the term social engineering with reference to computer security (2 marks)
   (i) Define Multilevel databases security (2marks )
   (ii) Describe any two ways of implementing Multilevel databases security is through the Separation Mechanisms (4marks )