JARAMOGI OGINGA ODINGA UNIVERSITY

OF SCIENCE & TECHNOLOGY

UNIVERSITY EXAMINATIONS 2012/2013

1ST YEAR 1ST SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE (COMPUTER SECURITY AND AUDIT)

(KISUMU L.CENTRE)

COURSE CODE: IIT 3113

COURSE TITLE: PC SECURITY AND PRIVACY

DATE: 13/8/2013 **TIME: 2.00-4.00 PM**

DURATION: 2 HOURS

INSTRUCTIONS

1. **This paper consists of 5 Questions.**
2. **Answer Question 1 (Compulsory) and any other 2 questions.**
3. **Write your answers on the answer booklet provided.**

QUESTION ONE [30 MARKS]

(a) During a class lecture on PC security, students were asked their understanding on computer security and one responded "computer security is to prevent and detect unauthorized actions by users of a system".

(i) Do you agree with the student's response? Support your answer. [2 marks]

(ii) Explain any THREE key considerations that can be relied upon to facilitate achievement of computer security. [6 Marks]

(b) Using appropriate example, explain your understanding of the following terms as applies to PC security [8 Marks]

(i) Vulnerabilities

(ii) Threats

(iii) Attacks

(iv) Defenses

(c) While supporting your answer, classify the following as a violation of *confidentiality*, *integrity*, *availability*, *authenticity*, *survivability*, or some combination of these. [4 Marks]

(i) Angela hacks into university's payroll system

(ii) James crashes Anne's computer system

(iii) Emily cracks into Tom's Facebook account and use it to chat with Annette.

(iv) Bruce defaces the homepage of Mwalimu Sacco Ltd website.

(d) Name and explain any TWO proactive and reactive security measures that can be used to improve PC security. [4 Marks]

(e) Provide important steps to be considered when; [6 Marks]

(i) Detecting and removing malware that has invaded a PC

(ii) Installing and configuring personal firewall in a PC

QUESTION TWO [20 MARKS]

(a) "It is important to consider *goals of security* when safeguarding computing assets on a network". What are these goals of security and how are they achieved on a network? [6 Marks]

(b) Using a well labeled diagram, explain how the following can be used to secure computing assets. [8 Marks]

(i) Firewalls (ii) Intrusion Detection Systems

(c) Distinguish between *Cryptography* and *Stenography* as applies to computer security. [4 Marks]

(d) Biometrics is one of the authentication approaches employed to improve security. Identify any TWO shortfalls of this method. [2 Marks]

QUESTION THREE [20 MARKS]

(a) The following statements might be TRUE or FALSE as applies to computer security. For each case, support the choice of your answer. [8 Marks]

(i) *Physical access* allows an attacker to plug into an open Ethernet jack.

(ii) *Multiple factor authentication* makes it difficult for an attacker to have correct materials for authentication.

(iii) *Default shared keys* is one of the common exploits in wireless networks.

(iv) In *Denial of Service attack*, the attacker tries to exhaust of the host.

(b) Consider three computers that connect to the Internet through a proxy server with their IP Addresses as follows; Computer A is on 10.10.0.2, Computer B is on 172.16.3.8, Computer C is on 172.16.3.9 and Server S is on 172.16.3.1. In this case, explain whether; [6 Marks]

(i) Computer B can claim it is Computer C to the Server S.

(ii) Computer A can claim it is Computer C to the Server S.

(c) When asked by their Professor during one of Security lessons why computers are considerably insecure, two students provided answers as follows; [6 Marks]

(i) Most PCs use insecure operating systems

(ii) Most PCs runs buggy, vulnerable and even malicious code.

Comment on each answer provided by the students. Suggest corrective measures that can be used.

QUESTION FOUR [20 MARKS]

(a) While referring to computer security; [6 Marks]

(i) Briefly describe your understanding of *data security*.

(ii) Identify FOUR key threats to data security

(b) Giving appropriate examples, explain [10 Marks]

(i) Levels of Security Abuses

(ii) Types of Security Breaches

(c) Differentiate between *File Infector Virus* and *Multi-partite Virus*. [4 Marks]

QUESTION FIVE [20 MARKS]

(a) Explain *risk assessment* as applies in computer security management. Identify three basic activities in risk assessment. [5 Marks]

(b) Explain how *Risk Mitigation* and Uncertainty *Analysis* benefits risk management. [4 Marks]

(c) "Interrelationship of vulnerabilities, threats and assets are critical to analysis of risk". Use a diagram to support the above statement. [5 Marks]

(d) "Computers system can be exploited for both fraud and theft by both automating traditional methods of fraud and by using new methods". Discus. [6 Marks]

- END -