THE MOMBASA POLYTECHNIC UNIVERSITY COLLEGE

(A Constituent College of JKUAT)

(A Centre of Excellence)

Faculty of Engineering & Technology

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

UNIVERSITY EXAMINATION FOR DEGREE IN BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

(BSC. IT M11 & BSC. IT 9S)

BIT 2317: FUNDAMENTALS OF COMPUTER SECURITY

SPECIAL/SUPPLEMENTARY EXAMINATION

SERIES: OCTOBER 2012

TIME: 2 HOURS

Instructions to Candidates:

You should have the following for this examination

- *Answer Booklet*

This paper consist of **FIVE** questions

Answer question **ONE** and any other **TWO** questions

Maximum marks for each part of a question are as shown

This paper consists of **THREE** printed pages

SECTION A (COMPULSORY)

Question One (30 marks)

a) Explain the following security goals
   i) Secrecy
   ii) Authentication
   iii) Integrity **(3 marks)**

b) Explain the difference between the following terms:
   i) "Steganography' and 'cryptography'
   ii) "Hardware Access Controls" and "Software Access Controls" **(12 marks)**

c) Explain the difference between the following terms:

i) "Computer Security" and "Network Security"
ii) "Risk" and "Penetration"
iii) "Plaintext" and "Ciphertext" **(12 marks)**

d) Explain the following terms:
i) Physical security
ii) Hash function
iii) Honeypot **(6 marks)**

SECTION B (Answer Any Two Questions)

Question Two (20 marks)

a) Define the following terms:
i) Trojan Horses
ii) Cookies
iii) Time bomb **(3 marks)**

b) Give your views on why protecting information systems is generally a difficult process. **(4 marks)**

c) A Company that relies on electronic transactions for its livelihood could suffer serious financial damage if its systems are taken off line for even a short time. Indeed, cases have been reported where an e-commerce company's competitor launched a denial of service (DOS) attack against company's websites hoping that customers would abandon the target's nonresponsive services and take their businesses to the attacker's website. Critically discuss the denial of service (DOS) attacks and defenses against these attacks. **(4 marks)**

d) Explain the following techniques as used in protecting programs and Data. **(6 marks)**
i) Copyrights
ii) Patents
iii) Trade Secrets

e) Twenty-five thousand messages arrive at an organization each year. Currently, there are no firewalls. On the average, there are 1.2 successful hacking each year. Each successful hacking will result in a loss to the company of about $130,000.

A major firewall is proposed at a cost of $66,000 and a maintenance cost of $ 5,000. The estimated useful life is 3 years. The chance that an intruder will break through the firewall is 0.0002. In such a case, the damage will be $100,00 (30%) or $200,000 (50%) or no damages at all. There is an annual maintenance cost of $ 20,000 for the firewall.
i) Should management buy the firewall? **(1 mark)**
ii) An improved firewall that is 99.9988% effective costs $84,000 with a life of 3 years and annual maintenance cost of $ 16,000 is available. Should this one be purchased instead of the first one? **(2 marks)**

Question Three (20 marks)

Security management must manage risks in terms of causes, effects and costs of a security loss. The costs resulting from a security breach must be balanced with the costs resulting from enhanced security measures. This means that systematic security management allows counter measures to be chosen in a planned and managed way. Since too much security wastes money while too little security wastes IS capability.

Explain your understanding to the following stages in the systematic management of security.
(20 marks)

Question Four (20 marks)

a) (i) In real life systems, describe a simple model of conventional (or secret key) encryption, identifying the problems inherent in the described approach. **(6 marks)**

(ii) Discuss how the public key encryption solves the problems of key distribution associated with the conventional encryption. **(4 marks)**

b) Briefly explain the Data Encryption Standard (DES) **(2 marks)**

c) The application of computer techniques in banking business has produced the need to translate all banking operations into a form accepted by computers. Discuss any FOUR properties that digital signatures should have to be able to sign documents using their local computers or terminals.
(8 marks)

Question Five (20 marks)

a) As our computing infrastructure has grown more network-centric and much of our lives revolve around networked computers attackers have devised very clever means for undermining computer communications. Therefore, various techniques exist for gaining access to computing resources using network-based attacks:
i) Sniffing
ii) IP address spoofing **(10 marks)**

b) Give a concise definition of the following concepts:
i) Threat
ii) Attack
iii) Vulnerability **(6 marks)**

c) State the reason why it is important to try to evade Intrusion Detection Systems (IDSs)?
(1 marks)

d) State the services that listen at TCP port 80 and UDP port 53 respectively?
(2 marks)

e) Briefly explain the term Demilitarized Zone. **(1 marks)**