TECHNICAL UNIVERISTY OF MOMBASA

Faculty of Engineering & Technology

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

UNIVERSITY EXAMINATION FOR:
BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY
(BSIT 12J)

BIT 2317: FUNDAMENTALS OF COMPUTER SECURITY

END OF SEMESTER EXAMINATION
SERIES: DECEMBER 2013
TIME: 2 HOURS

Instructions to Candidates:
You should have the following for this examination
- *Answer Booklet*

This paper consists of **FIVE** questions. Attempt 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

Question One (Compulsory)

a) Explain the following terms:
(i) Computer security
(ii) Internet security
(iii) Vulnerability
(iv) Firewall
(v) Physical security **(10 marks)**

b) Explain any THREE reasons why computer and network security is important. **(6 marks)**

c) Explain the following methods of defense against attacks:
(i) Encryption

(ii) Biometrics
(iii) Security servers **(6 marks)**

d) Explain the following terms:
(i) Security policy
(ii) Demilitarized zone (DMZ) **(4 marks)**

e) Explain any TWO goals of security. **(4 marks)**

Question Two

a) The application of computer techniques in banking industry has produced the need to translate all banking operations into a form accepted by computers.
(i) Describe any FOUR properties of a digital signature **(8 marks)**
(ii) Describe any FOUR types of attacks that are likely to be experience by banks **(4 marks)**

b) Twenty-five thousand message arrive at an organization each year. Currently, there are no firewalls. On average, there are one or two 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 maintenance cost of $ 5,000. The estimated useful life is three years.

(i) Justify why the management should buy the firewall. **(2 marks)**
(ii) Discuss any three software access controls needed to protect data and software in the company. **(6 marks)**

Question Three

a) Cryptosystems are important in protecting data during transmission. The design analysis of today's cryptographical algorithms is highly mathematical. In the context of this statements, differentiate between the following terms.

(i) "Cryptography" and "steganography"
(ii) "Public-key encryption" and "Private-key encryption"
(iii) "Plaintext" and "Ciphertext" **(12 marks)**

b) Using Caesar's Cipher, with key value of 3, encode the message:
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG **(4 marks)**

c) Explain the following types of encryption keys:
(i) Rivest, Shamir and Addleman (RSA)
(ii) Data Encryption standard (DES) **(4 marks)**

Question Four

a) Explain the term "Virtual Private Networks" **(2 marks)**

b) A company relies on electronic transactions for its livelihood could suffer serious financial damage if its system are taken offline for even a short time. Indeed, cases have been reported where an e-commerce company's competitor launched a denial of service against the company's website, hoping that customers would abandon the targets non-responsive servers and take their businesses to the attackers website.
(i) Describe how denial of service attack works. **(2 marks)**
(ii) Explain any TWO roles of the Intrusion Detection System (IDS) to this company. **(2 marks)**
(iii) Discuss any FOUR purposes of a security policy **(4 marks)**

c) Security management must manage risks in terms of causes, effects and costs of security loss. The costs resulting from a security breach must be balanced with costs resulting from enhanced security measures. Since too much security wastes money while too little security wastes Information System capacity. Discuss the following stages in the systematic security management:

(i) Risk identification
(ii) Risk analysis
(iii) Risk handling
(iv) Disaster recovery **(10 marks)**

Question Five

As our computing infrastructures have grown non network-centric and much of lives revolve around networked computers, attackers have devised very clever means for undermining computer communications. Critically describe:

a) The following objectives of computer security:

(i) Confidentiality
(ii) Non-repudiation
(iii) Integrity
(iv) Availability
(v) Authentication **(10 marks)**

b) Any THREE types of computer crimes **(3 marks)**

c) Any THREE types of attack methods **(3 marks)**

d) Any FOUR types of attack motives to computer systems **(4 marks)**