MACHAKOS UNIVERSITY

University Examinations 2018/2019

SUPLEMENTARY EXAMINATION FOR BSC (INFORMATION TECHNOOLOGY)

Sit 3: information SYTEMS SECURITY

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

Instructions: Answer Question ONE and any other TWO Questions

Question ONE (30 Marks)

a) Describe the objectives of a security (6 Marks)

b) Explain why DES encryption scheme is considered to be weak (8 Marks)

c) Explain three practical goals of an Intrusion Detection System (6 Marks)

d) Alice and Bob have each generated a public and private key pair. However, they do not know each others' keys yet. Now they are trying to exchange a message M over a network. **(6 Marks)**

   i. What is the procedure to exchange the message confidentially, if only passive attacks need to be considered

   ii. What can be done to mitigate the risk if active attacks are possible

e) List four threats that result from cyber crimes. (4 Marks)

Question TWO- 20 Marks

a) Machakos university would like to implement a new security feature. Briefly describe

the process they should follow (16 Marks)

b) Name four goals of auditing (4 Marks)

Question THREE- 20 Marks

a. Define forensic and briefly explain two tools that are useful for forensic analysis of Computer intrusions. **(8 Marks)**

b. Identify two natural disasters and explain disaster recovery panning for each how one may protect information system resources against them. (8 Marks)

c. Explain briefly the concepts of one-way function, one-way hash function and trapdoor one way function. (4 Marks)

Question Four- 20 Marks

a. Consider an ecommerce website that includes the notion of a "shopping cart." Customers visiting the site put items of interest in their shopping cart. After finishing their browsing and shopping, they click on Checkout to pay for the items. At that point, the customer logs into the site to enable the site to retrieve their payment information. (8 Marks)

i. Suppose that the site implements the shopping cart by storing the associated items and prices in files on the server, with one file for each customer. The site identifies customers by their IP addresses. This design is vulnerable to a DoS attack. Sketch it in a single sentence.

ii. Suppose that instead the site keeps a list of shopping cart items on the client side. Every time a user clicks on add-to-cart, the server sends all of the associated details (item name, price, quantity) in its reply, incorporating them into a hidden HTML form field. Through some Javascript magic, now when the user finally clicks on Checkout, all of the previously bought items embedded in the hidden form field are sent to the server. The server then joins them together into a list and presents the user with the

corresponding total amount for payment. Is this design vulnerable to the DoS attack you sketched above? Explain why or why not.

b. Describe in details the THREE types of information that can be used in authentication (6 Marks)

c. Clearly describe secure electronic transactions (SET). (6 Marks)

Question FIVE- 20 Marks

a) Using Diffie Hellman algorithm and supposing Alice and Bob agrees that N is 7 and α is 3. Alice decides to choose X_A as 2 and Bob chooses X_B as 3. What is Y_A and Y_B? Calculate the key. (10 Marks)

b) Describe THREE main attack techniques to operating system. (6 Marks)

c) Explain how public key cryptography may be used for identification. (4 marks)