KABARAK UNIVERSITY

EXAMINATIONS

2008/2009 ACADEMIC YEAR

FOR THE DEGREE OF BACHELOR OF BUSINESS MANAGEMENT & INFORMATION TECHNOLOGY

COURSE CODE:	**BMIT 416**
COURSE TITLE:	**IT SECURITY, AUDIT AND ETHICS**
STREAM:	**Y4S1**
DAY:	**THURSDAY**
TIME:	**9.00 – 12.00 P.M.**
DATE:	**06/08/2009**

INSTRUCTIONS:

1. **SECTION A ANSWER *ALL* QUESTIONS IN THIS SECTION**
2. **SECTION B ANSWER *ANY THREE* QUESTIONS IN THIS SECTION**

PLEASE TURN OVER

SECTION A ANSWER *ALL* QUESTIONS IN THIS SECTION

QUESTION ONE (40 MARKS)

a) Systems provide computer security by controlling access using identification and authentication procedures.

  i. Distinguish between identification and authentication with respect to system access control [2marks]

  ii. Explain the theory behind the following authentication procedures [3 marks]

   I. Passwords
   II. Keys
   III. Physiological or behavioral traits

b) Discuss FOUR primary methods through which computer system security provide protection giving appropriate examples. [8 marks]

c) Explain the mechanisms that support confidentiality and integrity pillars of computer security. [5 marks]

d) Rebecca works for Getrude Motors Company (GMC) from which Rose ordered motor vehicle spare parts Rebecca wrote a business transaction email message to update Rose on the revised prices on parts but Joel an employee of GMC conspired with the accounts clerk to intrude into Rebecca's system and modify the notification message by adjusting the prices upwards so as to make Rose pay more for the Items and divert the extra amount to their personal accounts.

  i. Explain the type of attacks and the categories of threat depicted in this scenario [6 marks]

  ii. State the mechanisms or services that can counter these threats. [2 marks]

e)

  i. Define the term 'zombie' with respect to malicious software [2 marks]

  ii. Explain how zombies can be used by business competitors to gain business mileage [2 marks]

f)

  i. Giving appropriate examples distinguish between masquerading and delegation [4 marks]

  ii. Distinguish between the following types of intruders stating whether they are outsiders or insiders with respect to the organization they attack [6 marks]

   I. Masquerader

II. Misfeasor
III. Clandestine user

QUESTION TWO (20 MARKS)

a) For each of the following measures of intrusion detection state the type of intrusion detected [7 marks]

Measure	**Type of intrusion detected**
Password failure at login	
Failure to login from specified terminals	
Login frequency by day and time	
Time since last login	
Frequency of login at different locations	
Elapsed time per session	
Quantity of output to location	

b)

i. Describe the following type of viruses [5 marks]

I.) Parasitic virus
II.) Memory resident virus
III.) Boot sector virus
IV.) Stealth virus
V.) Polymorphic virus

ii. Explain how a computer affected by a boot sector virus behaves and outline the steps that you would take to treat such a computer [4 marks]

c)

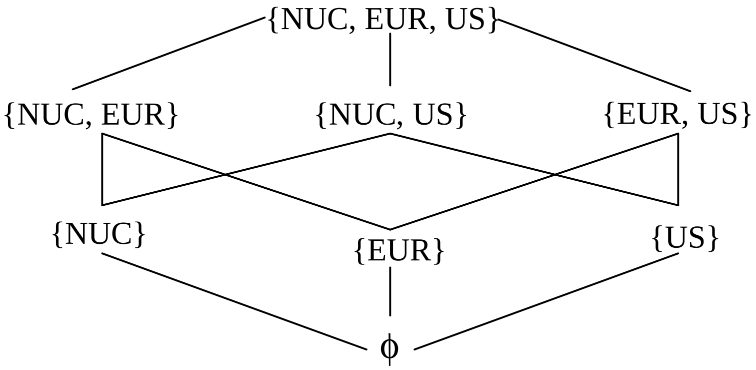
i. Define the term *'logic bomb'* with regard to malicious software [2 marks]

ii. Explain how a programmer can make legitimate use of a logic bomb to create a demonstration program for marketing software. [2 marks]

QUESTION THREE (20 MARKS)

a) Distinguish between integrity and confidentiality system access control models giving one example of a model in each category. [3 marks]

b) Objects can be placed in categories which arise from the **need to know** principle; objects placed in multiple categories have the kinds of information in all those categories. The set of categories to which a person may have access is the power set of the set of categories. For instance given the set of categories NUC, EUR, and US a person can have access to any of the following sets of categories Ǿ (none), {NUC}, {EUR}, {US}, {NUC, EUR}, {NUR, US}, {EUR, US}, {NUC, EUR,US}. These sets form a lattice under the operation subset of as depicted bellow



i. State the need to know principle [1 mark]

ii. George is cleared into security level (SECRET,{NUC,EUR}) , DocA is classified as (CONIDENTIAL,{NUC}) DocB is classified as (SECRET,{EUR,US}) and DocC is classified as (SECRET,{EUR}). state whether the following statements are valid or not valid giving appropriate reasons for your answer hence or otherwise state the documents that George can read [8 marks]

I.) George dom DocA

II.) George dom DocB

III.) Gearge –dom DocC

iii. Suppose Paul is cleared into security level (SECRET, {EUR, US, NUC}). Who of the two George or Paul have a higher security level? Explain [2 marks]

iv. State the highest level of documents that George and Paul can write [2 marks]

v. State the rule that prevents sensitive information for people with high security clearance from being copied to files accessible to persons with low security clearance. [2 marks]

vi. Supposing the person with the highest security level wants to send a message to the person with the lower security clearance explain how he will do this securely. [2 marks]

QUESTION FOUR (20 MARKS)

a) Using a relevant example explain what is meant by a well formed transaction [4 marks]

b) With respect to Clerk-Wilson integrity model explain the following terms using relevant examples [8 marks]

i. Constrained data items (CDIs)

ii. Unconstrained data items (UDIs)

iii. Integrity Verification Procedures (IVPs)

iv. Transformation Procedures (TPs)

c) Explain how you can create an integrity constraint in a table of students' performance for a constrained data item Marks to ensure that marks entered does not exceed 100. [3 marks]

d)

i. What is a trap door? [2 marks]

ii. Outline THREE legitimate uses of trap doors [3 marks]

QUESTION FIVE (20 MARKS)

a) Modern web browsers provide a number of features that help to protect your privacy and make your computer and your personally identifiable information more secure.

i. Explain the role of privacy and security features in a web browser [2 marks]

ii. Outline THREE categories of privacy features included in Internet Explorer [3 marks]

iii. Outline THREE categories of security features included in Internet Explorer [3 marks]

b)

i. You are a system administrator of a secondary school; one of the internet policy Statements states *'students should not view Web sites that contain violent or sexual content'*. State the feature of internet explorer that you might use to enforce this policy and explain how you can access it and use it to achieve the desired results [6 marks]

ii. Outline SIX activities that can be performed using the feature stated above to control access to the internet [6 marks]

QUESTION SIX (20 MARKS)

a)

i. Outline five ingredients of a symmetric encryption scheme [5 marks]

ii. Outline two requirements for secure use of a conventional encryption scheme. [2 marks]

b) Outline the THREE independent dimensions which characterized cryptographic systems [3 marks]

c)

i. Given the encryption key K= $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$ use the hill cipher to compute the cipher text for the plaintext *CRYPTANALYST* [10 marks]