JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTERS OF SCIENCE IN IT AND SECURITY AUDIT

1ST YEAR 1ST SEMESTER 2016/2017 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE : IIT 5112

COURSE TITLE : ADVANCED INFORMATION SYSTEMS SECURITY

EXAM VENUE : **STREAM :**

DATE : Dec 2016 **EXAM SESSION :**

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION ONE 20 MARKS

a) Cite a reason why an organization might want two or more firewalls on a single network. **(3 Marks)**

b) Describe the term Information security management by explaining more on its three general objectives. **(3 Marks)**

c) Mehdi, Khajouei and Nasrabadi (2011) in their research aimed at identifying the priority of key success factors in implementing information security management system in Iranian Municipal Organization with the view of experts. They used a model adopted from Abuzineh (2006) which included seven key success factors. You are required to describe the conceptual model used in this research work. **(14 Marks)**

QUESTION TWO 20 MARKS

a) Availability attacks, sometimes called denial-of-service or DOS attacks, are much more significant in networks than in other contexts. There are many accidental and malicious threats to availability or continued service. In what ways is denial of service (lack of availability for authorized users) a vulnerability to users of single-user personal computers? **(5 Marks)**

b) The next day at SLS found everyone in technical support busy restoring computer systems to their former state and installing new virus and worm control software. Abigael found herself learning how to install desktop computer operating systems and applications as SLS made a heroic effort to recover from the attack of the previous day.

Tasks:

i. Do you think this event was caused by an insider or outsider? Why do you think this? **(5 Marks)**

ii. Other than installing virus and worm control software, what can SLS do to prepare for the next incident? **(5 Marks)**

iii. Do you think this attack was the result of a virus or a worm? Why do you think this? **(5 Marks)**

QUESTION THREE 20 MARKS

a) Alice and Bob participate in a public-key infrastructure that enables them to exchange legally binding digital signatures.

i. Name two reasons why, for some purposes, Alice might prefer to use a message authentication code, instead of a digital signature, to protect the integrity and authenticity of her messages to Bob. **(4 Marks)**

ii. Outline a protocol for protecting the integrity and authenticity of Alice's messages to Bob that combines the benefits of a public-key infrastructure with those of using a message authentication code. **(6 Marks)**

b) Describe security issues with respect to electronic payment and how far the new payment technologies are adopted by the users? **(6 Marks)**

c) With the aid of diagram; explain how digital signatures can ensure transaction integrity within an e commerce environment. **(4 Marks)**

QUESTION FOUR 20 MARKS

a) List three factors that should be considered when developing a security plan. **(3 Marks)**

b) Explain the risk management process **(8 Marks)**

c) In order to assess the level of risk, likelihood and the impact of incidental occurrences should be estimated. This estimation can be based on experience, standards, experiments, expert advice, etc. You are required to describe Risk analysis or assessment approach in terms of quantitative, semi quantitative and qualitative. **(9 Marks)**

QUESTION FIVE 20 MARKS

a) What is a Business Continuity Plan? **(1 Mark)**

b) Describe FOUR situations in which a business continuity plan would be helpful. **(8 Marks)**

c) The key to coping with Information System disasters is advance planning and preparation, identifying activities that will keep a business viable when the computing technology is disabled. Outline three

steps in business continuity planning.
(6 Marks)

d) Investigate your university's or employer's security plan to determine whether its security requirements meet all the conditions we studied during this course. Outline atleast FIVE Network security threats **(5 Marks)**