JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN IT SECURITY AND AUDIT

1st YEAR 1st SEMESTER 2018/2019 ACADEMIC YEAR

KISUMU CAMPUS

COURSE CODE : IIT 6111

COURSE TITLE : ADVANCED ISSUES IN INFORMATION SECURITY

EXAM VENUE : **STREAM :**

DATE : December, 2018 **EXAM SESSION :**

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer ANY other three questions of your choice**
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) Big data changes the nature of information security. The collection and storage of abundant or large data including IP address of customers, the budget of companies, and key information of governments result in information security lapses. You are required to describe;
   i. Current challenges of information security in the age of big data **(4 Marks)**
   ii. Possible solutions to protect information security in the age of big data **(4 Marks)**

b) Cloud computing is an Internet-based computing solution which provides the resources in an effective manner. A very serious issue in cloud computing is security which is a major obstacle for the adoption of cloud. You are required to describe the following;
   i. Three types of cloud deployment models. **(3 Marks)**
   ii. Three types of cloud delivery models. **(3 Marks)**
   iii. Emerging security issues and challenges in cloud computing adoption. **(6 Marks)**

QUESTION TWO 20 MARKS

a) 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 FOUR Network security threats **(2 Marks)**

b) 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. **(6 Marks)**

c) Risk analysis is a well-known planning tool, used often by System auditors, accountants, and managers. Describe three good reasons to perform a risk analysis in preparation for creating a security plan. **(6 Marks)**

d) Risk is inevitable in life. You are required to discuss SIX strategies that can be used in dealing with the risks. **(6 Marks)**

QUESTION THREE 20 MARKS.

a) Information Security Management System (ISMS) can be defined as a collection of policies concerned with Information Technology (IT) related risks or Information Security Management (ISM). It is a documented system that provides security for information and data in an organization. Every organization is faced with the task of providing a

comprehensive plan for information security. Describe SIX major steps involved in building an ISMS. **(12 Marks)**

b) For the effective management of information security in an organization, Information Security Management Systems (ISMSs) have to be developed and evaluated. In development of advanced Information Security Management Evaluation System (ISMES), There FOUR key stages in management process of the ISMES before establishing a classification standard which can be evaluated by the organization itself and the evaluation committee. Explain those four stages involved in management process of ISMES **(8 Marks)**

QUESTION FOUR 20 MARKS

Access control is the process of mediating every request to resources and data maintained by a system and determining whether the request should be granted or denied. The development of an access control system requires the definition of the regulations according to which access is to be controlled and their implementation as functions executable by a computer system.

Tasks:

a) Explain at least TWO concepts used in development of an access control system which is usually carried out with a multi-phase approach. **(2 Marks)**

b) Describe at least TWO main classes under which access control policies can be grouped. **(2 Marks)**

c) Explain what the following commands will effect in the access control system:-

i. **command** CREATE(creator,file)
create object file
enter Own *into A*[creator,file] **end.** **(1 Mark)**

ii. **command** CONFER*a*(owner,friend,file)
if Own in *A*[owner,file]
then *enter a into A*[friend,file] **end.** **(1 Mark)**

iii. **command** REVOKE*a*(owner,ex-friend,file)
if Own in *A*[owner,file]
then *delete a from A*[ex-friend,file] **end.** **(1 Mark)**

iv. **command** TRANSFER*a*(subj,friend,file)
if *a** in *A*[subj,file]
then *enter a into A*[friend,file] **end.** **(1 Mark)**

d) In your own opinion, discuss the strength and weaknesses of discretionary policies and mandatory policies in access control. **(2 Mark)**

e) In the first formulation of their model, Bell and LaPadula provide a *Basic Security Theorem (BST)*. State the TWO conditions underlying this theorem. **(2 Marks)**

f) In your own wisdom, Critique this *Basic Security Theorem (BST)* by Bell and LaPadula. **(4 Marks)**

g) Compare and contrast Bell LaPadula Model and The Biba model as far as mandatory policies are concerned in access control. **(4 Marks)**

QUESTION FIVE 20 MARKS

a) Wireless communications use radio frequency carriers which carry the information. These may be direct communications between two wireless devices or these communications may be routed through a wireless network, such as through intermediate communication devices. This technology has come up with several security challenges such as text communication through wireless is prone to sniffing, eavesdropping, man-in-the-middle attacks, and the like. One of the solutions provided for some of the information security issues on wireless is encryption. You are required to describe the TWO Wi-Fi encryption standards that can be used to protect Wireless communications. **(4 Marks)**

b) As an IT Security and Audit expert, you are required to explain how the following mechanisms can be used to attack wireless networks;

i. MAC spoofing, **(1 Mark)**

ii. Unauthorized association **(1 Mark)**

iii. Adhoc association **(1 Mark)**

iv. Use of rogue access points. **(1 Mark)**

v. War-Walking and War-Driving **(1 Mark)**

vi. Powerful jamming signals **(1 Mark)**

c) Wi-Fi authentication can happen using a centralized authentication server, open system authentication, or shared key authentication by the access point. Further, to strengthen the authentication process MAC filtering may be enabled. As an expert in this field, give a technical advice to your Chief Executive Officer on the Wi- Fi authentication mechanism the corporate organization should use and why? **(2 Marks)**

d) Highlight some of the best practices to avoid / reduce the propensity for wireless attacks. **(2 Marks)**

e) Bluetooth is the wireless communication technology that is used for short range communication (usually about 25 feet). This technology is used for transferring the files between one mobile device to the other (e.g., from mobile phone to the laptop or laptop to the mobile phone, etc.). As the range of communication is short the possibility of hacking it is

less but cannot be denied. Highlight some of the best practices to ensure security of the Bluetooth communication. **(3 Marks)**

f) Mobile phones, smartphones, and tablets are being widely used now-a-days. Various operating systems are used in these mobile devices. Mobile devices are being used for transacting on the web, sending e-mails, instant messaging apps / tools, gaming, and various official / personal purposes. Mobile apps are being used heavily by the users of these devices as most of them are free or are available at very low cost. Mobile devices have made the lives of users easy and more active; however, at the same time they have created a number of security issues and all of us need to be concerned about them because many of us may be using the same mobile phone for both personal and work use. Give advice on some of the best practices for information security of mobile devices. **(3 Marks)**