20

(University of Choice)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

UNIVERSITY SUPPLEMENTARY EXAMINATIONS

2021/2022 ACADEMIC YEAR

THIRD YEAR FIRST SEMESTER EXAMINATIONS

FOR THE DEGREE

OF

BACHELOR OF SCIENCE INFORMATION & KNOWLEDGE MANAGEMENT

COURSE CODE: **BIT 315**

COURSE TITLE: **INFORMATION ASSUARANCE & SECURITY**

DATE: FRIDAY 29-07-2022 **TIME:** .8:00A.M-10:00A.M

INSTRUCTIONS TO CANDIDATES

Question ONE (1) in Section A is compulsory
Answer any other 2 questions from Section B

TIME: 2 Hours

►

MMUST observes ZERO tolerance to examination cheating

Question One

a) Explain the typical requirements of a secure distributed system. [3 marks]

b) Describe the meaning of a system in the context of security engineering. [6 marks]

c) Describe how public key cryptography may be used for identification. [4 marks]

d) Explain how a man-in-the-middle attack on a Wi-Fi network can be defeated.[4 marks]

e) In general, there are three types of identity authentication tasks. List these tasks.[4 marks]

f) Explain what the terms Honeypot, Honeynet and Padded Cell Systems mean when used in relation to information security and describe how each can be used to protect and secure an organisation's information assets (9 marks)

Question Two

a) Discuss the role of the logic of authentication. [5 marks]

b) An ideal password authentication scheme has to withstand a number of attacks. Explain five of these attacks. [10 marks]

c) Discuss the three main concerns with the use of passwords for authentication. [5 marks]

Question Three

a) Explain what is meant by a social engineering attack on a password. . [10 marks]

b) Describe how access control lists are use to represent access control matrices. Describe the environments in which they are widely used and their advantages and disadvantages. [6 marks]

c) Discuss the principle of least privilege. [5 marks]

Question Four

a) Describe how capability lists are used to represent access control matrices. Discuss the main problem associated with the use of capability lists and its consequences .[6 marks]

b) How might a hacker attempt to attack a cryptosystem and how can an organisation best defend itself against such an attack? (6 marks)

c) The permission bits associated with a program call Prog1 and a dataset called Data1 are as follows:

Prog1: 1 1 1 1 0 1 1 0 0

Data1: 1 1 1 1 0 0 0 0 0

State the permissions these bits give.

Explain the advantages and disadvantages of using permission bits for access control.[8 marks]

Question Five

a) Shannon proposed two measures of security: unicity distance and cover time. Describe how each of these concepts seeks to provide an indication of the security of a cipher system and outline the theoretical concept which has now superseded the notion of cover time. [10 marks]

b) You are finalizing your security test status report for a project that is ready for deployment into production. There is a high degree of risk for this project due to the nature of the system. As a result, you want to place particular emphasis on risk. Based on this, what is the best way to articulate risk on your report? (6 marks)

c) The concept of computational complexity has superseded the notion of covertime as a measure of the security of a cryptosystem. Discuss how computational complexity theory provides the theoretical basis for the design of modern scalable cryptosystems. [4 Marks]