AFRICA UNIVERSITY
A United Methodist-Related Institution

"Investing in Africa's future"

COLLEGE OF BUSINESS, PEACE, LEADERSHIP AND GOVERNANCE

NCIS 207: FUNDAMENTALS OF INFORMATION SYSTEMS SECURITY

END OF FIRST SEMESTER EXAMINATIONS

JULY 2022

LECTURER: DR. C. MANJEESE

TIME: 3 HOURS

INSTRUCTIONS

Answer **TWO** Compulsory questions from Section A.

Answer any **THREE** questions from section B

Each question carries 20 marks.

The marks allocated to **each** question are shown at the end of the section.

Marks will be awarded for giving logical examples.

SECTION A

QUESTION 1

a) Define access control lists and capabilities, and discuss their relative strengths and weaknesses. [5]
b) Describe how the access control list mechanisms work in Unix. [5]
c) You have been asked to build a funds transfer system in which a payment is authorised only once it has been approved by both a manager and an accountant at a bank branch. How would you implement this system using Unix security mechanisms as the foundation? [10]

QUESTION 2

a) A moral and ethical issue raised by the information age is the collection and use of information about individuals, i.e. privacy concerns? Explain why privacy is an issue of concern to those using any kind of information systems and how organizations can guarantee privacy. [10]

b) Outline briefly the purpose of an organisation's security policy and what steps should be considered in its development. [10]

SECTION B

QUESTION 3

Consider the following two separation-of-duty policies:

A transaction needs approval from two people, one in group A and one in group B.
A transaction needs approval from two distinct users of the system.

a) Which of these is harder to implement using the standard Unix access control mechanisms, and why? [10]

b) Sketch an implementation of the easier policy using Unix mechanisms. [5]

c) Describe at least two alternative mechanisms that might be used to implement the other policy. [5]

QUESTION 4

Which mode (or modes) of operation of the Advanced Encryption Standard (AES) block cipher would you use to protect the following? Give a brief justification for your answers.
a) Inter-bank funds transfers. [4]
b) Email messages. [4]
c) A high-frequency radio modem link. [4]
d) Passwords stored on a local disk. [4]
e) The pulse train from a gearbox sensor to the tachograph in a truck. [4]

QUESTION 5

(a) Name three types of software vulnerability; give an example of each and a brief description of how each could be exploited. [9]
(b) Alice wants to attack Bob's computer via the Internet, by sending IP packets to it, directly from her own computer. She does not want Bob to find out the IP address of her computer.
i. Is this easier to achieve for Alice with TCP- or UDP-based application protocols? Explain why. [3]

ii. For the more difficult protocol, explain one technique that Alice could try to overcome this obstacle and one countermeasure that Bob could implement in his computer. [3]
iii. Name three functions that Alice's Internet service provider could implement to make it more difficult for Alice to achieve her goal? [2]

QUESTION 6

a) Give an example each for authentication by something you know, something you have, something you are, something you do. [4]

b) Describe two different techniques that prevent viruses from being detected by an anti-virus software (even an up-to-date one). [4]

c) An administrator installs an IDS that generates an alarm each time it detects an intrusion.

i) Mention a typical attack that can be detected by an IDS. [4]

ii) Mention a threat to which we expose ourselves by using such a system. [4]

iii) Name two ways of determining whether an action is classified as an intrusion. [4]

==========END OF PAPER==========