"Investing in Africa's future"

COLLEGE OF BUSINESS, PEACE, LEADERSHIP AND GOVERNANCE

NCIS 207: FUNDAMENTALS OF INFORMATION SYSTEMS SECURITY

END OF FIRST SEMESTER EXAMINATIONS

APRIL 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) Briefly explain the following terms, and for each give one example of a technique that implements it:

    i.   secure commitment; [2]
    ii.   mandatory access control policy; [2]
    iii. perfect secrecy; [2]
    iv. message authentication code. [2]

b) While globalization and information technology are exciting, they are also carriers of threats to existing economies and businesses. List and discuss at least two of the difficulties brought about by this new environment in terms of security to ISs. [12]

QUESTION 2

(a) Explain the difference between mandatory and discretionary access control. [4]

(b) i. Explain the purpose and operation of cipher-block chaining (CBC). [4]

   ii. Explain how to decrypt a message in CBC. [4]

(c) To protect her interview partners, a journalist needs to ensure that what she records with her digital camera cannot be viewed by anyone before she returns to her home country. You were asked to design for her a camera that encrypts recordings immediately before they are stored on tape. The question arises, how to handle the encryption key. If it is stored in the camera, it could be extracted if the hardware were confiscated and analysed. A key memorised by the user might be obtained using coercion, so this is not a suitable solution either.

Suggest two alternative convenient ways of arranging the encryption inside the camera such that decryption of the tape is possible only on the journalist's home computer. [8]

SECTION B

QUESTION 3

For any four of the following, explain the features of each biometric security technique, giving a advantages as well as disadvantages of each and areas where such techniques are commonly applied.

i) Fingerprint; [5]
ii) Voice recognition; [5]
iii) Retina scan; [5]
iv) Iris recognition; [5]
v) Facial geometry. [5]

QUESTION 4

a) Discuss the following principles of information security;

      i. Confidentiality

      ii. Integrity

      iii. Availability   [12]

    b) When shopping at Chinyavada supermarket, after you've selected your purchases you take your cart full of goods to one of the registers. The check-out clerk scans your goods, totals what you owe, and upon receiving payment from you gives you an itemized receipt. However, you can't then simply exit the building with your goods. At the exit you're required to go by a staff member who inspects your receipt. If the receipt looks okay (appears to match the number and types of items in your cart), the staff member draws a line with a permanent marker down the receipt and hands it back to you. At this point, you can exit the building and take the goods to your car.

   i) Identify two security principles illustrated by Chinyavada's approach. For each, describe in a single sentence what aspect of Chinyavada's approach reflects the principle.   [6]

   ii) Identify an attack that chinyavada seeks to prevent by having the staff member draw the line down your receipt. Briefly describe how the attack works.   [2]

QUESTION 5

a. What are Biometric systems?   [3]

b. Describe any **five** problems that are associated with biometrics.   [10]

c. Describe the following DoS attacks. Briefly explain how you can protect against each type of attack.

   i)   SYN Flooding,   [4]

   ii)   Ping of death,   [4]

   iii)   UDP Flood attack,   [4]

   iv)   Smurf attack.   [4]

QUESTION 6

a. Explain **five** circumstances where safeguards may be preferred over counter measures.   [10]

b. Briefly explain the social engineering attack?   [4]

c. Describe any two techniques that are used by computer criminal to hijack a wireless association.   [6]

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