(University of Choice)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

MAIN CAMPUS

UNIVERSITY EXAMINATIONS

2022/2023 ACADEMIC YEAR

THIRD YEAR SECOND SEMESTER EXAMINATIONS

FOR THE DEGREE OF BACHELOR

OF

COMOUTER SCIENCE

COURSE CODE: BCS 321

COURSE TITLE: COMPUTER SYSTEM AND SECURITY

DATE: 13/04/2023 **TIME:** 8:00-10:00AM

INSTRUCTIONS TO CANDIDATES

Question ONE (1) is compulsory
Attempt any TWO (2) questions

TIME: 2 Hours

MMUST observes ZERO tolerance to examination cheating

This Paper Consists of 3 Printed Pages. Please Turn Over.

Question One [30 Marks]

a) In your view what is the role of the logic of authentication using MMUST as your case **[6 Marks]**

b) Suppose that the security systems on several of the computers on the university's network have been bypassed and personal information on staff and students was illicitly inspected and copied. You know who is responsible for this as it is one of your friends. They claim to have done this only in order to expose shortcomings in the university's computer security and have since destroyed their copy of this information. The university sends all staff and students an email asking for information concerning this incident. Describe the course of action you would consider and what suggestions would you take to come to your decision. **[8 Marks]**

c) Declassification effectively violates the *-property of the Bell-LaPadula Model. Would raising the classification of an object violate any properties of the model? Discuss why or why not,? **[8 Marks]**

d) Long before computers were invented, gathering of information about individuals, storing it, and retrieving were common. How did the invention of computers and the rapid development of information and communication technology transform these activities into serious risks to privacy? **[6 Marks]**

Question two [20 Marks]

a) A respected computer scientist has said that no computer can ever be made perfectly secure. Why might (s)he have said this? **[9 Marks]**

b) A noted computer security expert has said that without integrity, no system can provide confidentiality.
   i. Do you agree? Justify your answer.
   ii. Can a system provide integrity without confidentiality? Again, justify your answer.

c) Classify each of the following as an example of a mandatory, discretionary, or originator controlled policy, or a combination thereof. Justify your answers.
   i. A system in which no memorandum can be distributed without the author's consent. **[3 Marks]**
   ii. A military facility in which only generals can enter a particular room **[3 Marks]**
   iii. A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them. **[5 Marks]**

Question Three [20 Marks]

a) The text states that whether or not the integrity of a generic piece of software, or of generic data on which that generic software relies, has been compromised is undecidable. Prove that this is indeed the case. **[8 Marks]**

b) The system administrators on the development network believe that any password can be guessed in 180 days of continuous trial and error. They set the lifetime of each password at a maximum of 90 days. After 90 days a password must be changed. In you view why did they use 90 days rather than 180 days? **[4 Marks]**

c) In the Clark-Wilson model, must the TPs be executed serially, or can they be executed in parallel? If the former, why; if the latter, what constraints must be placed on their execution? **[8 Marks]**

Question Four [20 Marks]

a) Develop a construction to show that a system implementing the Chinese Wall model can support the Bell-LaPadula Model. **[8 Marks]**

e) Explain the level of privacy protection an employee in a big corporation can expect for each of the three types of communication conducted in the office setting: telephone, email, and traditional mail. Which is expected the highest level of privacy protection? And the lowest? **[4 Marks]**

b) Prove that applying a sequence of transformation procedures to a system in a valid state results in the system being in a (possibly different) valid state. **[8 Marks]**

Question Five [20 Marks]

a) A hospital patient record system provides login accounts for nurses. It is desired to implement the following policy:

(i) When a nurse registers a new patient, the nurse is granted access to the patient's records for a period of 90 days.

(ii) A nurse possessing the right to access a patient record can give that right to another user (this facilitates staff shift changes). This may be done offline.

To implement this policy, the system works as follows. When a nurse registers a new patient, a capability to access the patient record for the following 90 days is generated.

The nurse stores it on a USB stick, and may copy it onto other USB sticks to give to other users. When a user attempts to access patient records, she is prompted to upload the relevant capability. The capability has the following format:

patient-id, *issue-date*, hmac(K, (*patient-id*, *issue-date*)) where hmac(K,...) denotes a suitable keyed hash function with key K. The key K is a secret key known only to the patient record system. Any user in possession of this capability is able to access the records of the patient with *patient-id*, provided the date is within 90 days after *issue-date*.

i. Suppose nurse A registers a patient and receives such a capability. A passes it to B, B passes it to C, and C passes it to D. With explanation is D able to use the capability? **[5 Marks]**

ii. In order to stop long-lived capabilities being distributed widely, the hospital decides to adopt the policy that the nurse that initially registers the patient will have access to the records for 90 days, as before, but if she passes the capability to any other user, the validity should be 10 days from the issue date. Explain a new format for capabilities which would support this new policy. **[10 Marks]**

b) The president of a large software development company has become concerned about competitors learning proprietary information. He is determined to stop them. Part of his security mechanism is to require all employees to report any contact with employees of the company's competitors, even if it is purely social. Do you believe this will have the desired effect? Why or why not? **[5 Marks]**