100

(University of Choice)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

MAIN CAMPUS

UNIVERSITY EXAMINATIONS

2021/2022 ACADEMIC YEAR

THIRD YEAR SECOND SEMESTER EXAMINATIONS

FOR THE DEGREE

OF

BACHELOR OF SCIENCE OF COMPUTER SCIENCE

COURSE CODE: BCS 321

COURSE TITLE: COMPUTER SYSTEMS AND SECURITY

DATE: Wednesday 20/04/2022 **TIME:** 12:00-2:00p.m

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) . Declassification (lowering the security level of an object) effectively violates the *-property of Bell-LaPadula because the information in that object flows from high to low.
   i. Would raising the level violate either of the BLP properties? Why or why not? **[8 Marks]**
   ii. Would raising the integrity level of an object violate any principles of Biba's Strict Integrity model? Explain your answer. **[8 Marks]**

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

c) 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]**

QUESTION TWO [20 Marks]

Consider an ecommerce website that includes the notion of a "shopping cart." Customers visiting the site put items of interest in their shopping cart. After finishing their browsing and shopping, they click on Checkout to pay for the items. At that point, the customerlogs into the site to enable the site to retrieve their payment information.

i. Suppose that the site implements the shopping cart by storing the associated items and prices in files on the server, with one file for each customer. The site identifies customers by their IP addresses. This design is vulnerable to a DoS attack. Argue your understanding **[8 Marks]**

ii. Suppose that instead the site keeps a list of shopping cart items on the client side. Every time a user clicks on add-to-cart, the server sends all of the associated details (item name, price, quantity) in its reply, incorporating them into a hidden HTML form field. Through some Javascript magic, now when the user finally clicks on Checkout, all of the previously bought items embedded in the hidden form field are sent to the server. The server then joins them together into a list and presents the user with the corresponding total amount for payment. Is this design vulnerable to the DoS attack you sketched above? Explain why or why not. **[12 Marks]**

QUESTION THREE **[20 Marks]**

i. In access control systems, what is a *capability*? **[6 Marks]**
ii. Explain an advantage of access control lists over capability lists. **[7 Marks]**
iii. Explain an advantage of capability lists over access control lists. **[7 Marks]**

QUESTION FOUR **[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. Is D able to use the capability? **[4 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 police and the public defender share a computer. What security problems does this present? Do you feel it is a reasonable cost-saving measure to have all public agencies share the same (set of) computers? **[6 Marks]**

QUESTION FIVE **[20 Marks]**

You return to Javalicious, the handy coffee shop nearby with free WiFi. You again settle in for an afternoon of web-surfing and tweeting. You know that the network sends all packets unencrypted, and you are not surprised to again see Prof. Evil seated at the table next to yours, using a laptop connected to the same WiFi network.

For your web connections, consider the basic security properties of confidentiality, integrity, and availability. For each of these, analyze three scenarios:

DNSSEC-only means that for a given web site, your laptop looks up all of the domain names for your web session using DNSSEC (including NSEC3); your actual web traffic, however, uses HTTP.

HTTPS-only means that for a given web site, your laptop looks up all of the domain names for your web session using ordinary DNS; your actual web traffic, however, uses HTTPS.

DNSSEC+HTTPS means that both your domain name lookups use DNSSEC and your actual web traffic uses HTTPS.

In the following, circle YES if using only his laptop (no additional equipment) Prof. Evil can undermine the given property for your web connections, or NO if not. At the end of each section, supply a brief explanation for your answers.

i. Confidentiality of your web connection content: **[5 Marks]**
ii. Confidentiality of keeping private what sites you communicate with: **[5 Marks]**
iii. Integrity of your web connections: **[5 Marks]**
iv. Availability of your web connections: **[5 Marks]**