THE CO-OPERATIVE UNIVERSITY OF KENYA

END OF SEMESTER EXAMINATION DECEMBER -2022

EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY, COMPUTER SCIENCE
(YR IV SEM I)

UNIT CODE: BCIT 4139

UNIT TITLE: COMPUTER SYSTEMS SECURTY

DATE: FRIDAY, 16TH DECEMBER, 2022

TIME: 11:30 AM – 1:30 PM

INSTRUCTIONS:

- **Answer question ONE (compulsory) and any other TWO questions**

QUESTION ONE **[30 MARKS]**

(a) Using appropriate example in each case, explain the security contributions of the following terms and concepts to computer systems security. [8 Marks]

i. KERBEROS

ii. MIME

(b) Using suitable example, describe how public key cryptography can be used for identification. [6 Marks]

(c) It is common knowledge that people pick bad passwords and often use the same bad password across many sites. Someone proposes using the blockchain to solve this problem, that is, for every site *S*, user email address *M*, and password *P*, put **{*S*,*H*(*M*,*P*)}** on the blockchain, where *H* is a strong cryptographic hash function such as SHA-3.

i. Is this a good idea? Briefly explain. [4 Marks]

ii. Explain whether it would be better if sites put {*H*(*S*,*M*,*P*)} on the blockchain instead. [4 Marks]

(d) SWIFT is a worldwide network used by banks to send each other financial transaction information. Consumers and businesses do not connect directly to SWIFT; only financial institutions can. It has been abused—in 2016, hackers allegedly working on behalf of North Korea tried to use it to steal US$1 billion via a Bangladeshi bank. *Ars Technica* wrote:

SWIFT's security stems from two major sources. Notionally, it's a private network, and most banks set up their accounts such that only certain transactions between particular parties are permitted. The network privacy means that it should be hard for someone outside a bank to attack the network, but if a hacker breaks into a bank—as was the case here—then that protection evaporates. The Bangladesh central bank has all the necessary

SWIFT software and authorized access to the SWIFT network. Any hacker running code within the Bangladesh bank also has access to the software and network.

Consider yourself having been hired to do a penetration test of some bank's SWIFT gateway. Of course, you do not want to damage the SWIFT gateway in any way, and especially not do anything that would leave it open to other attackers. Outline the requisite steps you would take to ensure that there was no damage. [8 Marks]

QUESTION TWO **[20 MARKS]**

(a) "An ideal password authentication scheme has to withstand a number of attacks". Describe any of the five attacks that fits this statement. [10 Marks]

(b) Describe the goals an ideal password authentication scheme should achieve. [10 Marks]

QUESTION THREE **[20 MARKS]**

(a) Explain how access control lists are used to represent access control matrices. [4 Marks]

(b) Describe the environments in which the mentioned access control lists in 3(a) above are widely used and their advantages and disadvantages. [8 Marks]

(c) Suppose the following groups are defined to shorten a system's access control lists:

Group1: Alice, Bob, Cynthia, David, Eve

Group2: Alice, Bob, Cynthia

Group3: Bob, Cynthia

Suppose the access control list for File 1 is:

File 1: Group 1, R; Group 2, RW

If Alice wants to write to File 1 giving your reasoning state whether Alice will be allowed to do so if:

i. The first relevant entry policy is applied [3 Marks]

ii. The any permission in list policy is applied [3 Marks]

Suppose the access control list for File 2 is:

File 2: Group 3, RWE

iii. Show how the need for a Group 3 for File 2 can be removed using access none. [3 Marks]

QUESTION FOUR **[20 MARKS]**

(a) Using a suitable practical example, describe the principle of least privilege. [6 Marks]

(b) Explain how capability lists are used to represent access control matrices. [4 Marks]

(c) Discuss the main problem associated with the use of capability lists and its consequences. [6 Marks]

(d) Explain how capability lists are now commonly implemented in the form of attribute certificates to get around the main problem associated with the use of capability lists for access control. [4 Marks]

QUESTION FIVE **[20 MARKS]**

(a) With a suitable example in each case, explain the significance of the following concepts to computer systems security.

i. one-way function [4 Marks]

ii. one-way hash function [4 Marks]

iii. trapdoor one-way function [4 Marks]

(b) Explain why a stream cipher fails to protect message integrity. [3 Marks]

(c) Describe how a one-way hash function may be used for message authentication. [5 Marks]