BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE

MAR 2023

BACHELOR OF SCIENCE HONORS DEGREE IN COMPUTER SCIENCE/INFORMATION TECHNOLOGY

2 HOURS 30 MINUTES

CS412: COMPUTER SECURITY

DURATION: 2HOURS 30 MINUTES TOTAL MARKS: 100

INSTRUCTIONS TO CANDIDATES

The paper contains **five** questions. Answer **ALL** questions.

Question 1

a) Explain the difference between fabrication and modification attacks. **[2]**

b) Bindura University of Science Education (BUSE) is implementing an electronic voting (e-voting) system to elect their chancellor. Only the faculty of Science are allowed to vote online at a voting website that the university IT department is implementing.

What is the security attributes that need to be considered for the e-voting system? Be specific. For instance, do not just say `confidentiality', but enumerate which (all) kinds of information need to be kept confidential. Note that the security attributes could go beyond the classical three used in CIA-triad. **[6]**

c) Provide one example each for preventive, detective and corrective security controls, for each of the following categories :

i. People

ii. technology

iii. operations **[9]**

d) The principle of `need to know' in information security advocates that each user should have access to only as much information as needed to carry out the tasks they are assigned, and no more (least privilege access). What are potential shortcomings of such an approach to security? **[3]**

Question 2

a) Knowledge of worm life cycle helps us to make good defense mechanism against internet worms.

i. Give the phases in the life cycle of a computer worm. **[4]**

ii. Explain any **three** effects of worms on computer security. **[6]**

b) Answer the following questions on Denial of Service.

i. What is denial of service (DOS) attack? **[2]**

ii. Describe the following examples of DOS. In your description suggest a possible solution to each DOS attack **[6]**

Smurf, Ping flood, Fraggle

c) Describe briefly the role of signature detection. **[2]**

Question 3

a) You are responsible for the security of cloud storage and computing service. Naturally, you need to protect your customers' data by fully encrypting their reserved blocks on your server. You distinguish:

IT team: This team has access to the server and all system files for maintenance.

Executive team: This team has access to customers' addresses and billing data.

The customers: Each customer has access to his reserved block on the file system.

i. When a customer enters/edits their billing data, it has to be protected from unauthorized access. Choose one of the following encryption schemata (explain your choice): Triple DES,RSA,AES **[1]**

ii. Given your choice above, write for each group which key should be available to them (write the key type or "none"): **[3]**

b) The IT team has access to the system files, including sensitive files such as /etc/passwd. Describe how you prevent them from using an executive team member's credentials. **[2]**

c) Sales expert Alice (executive team) does not have PGP/RSA installed on her private e-mail client, however she does have a public/private key pair which

she uses when communicating over her corporate mail client. She wants to send a sensitive message to sales expert Bob as she often does, however she currently cannot use the corporate client. She considers two options:

(1) She sends this one e-mail unencrypted.

(2) She uses an online encryption/decryption service she found at www.isilver.com, where she can submit the message and Bob's public key and receives a cipher text which she sends to Bob. Bob can likewise decrypt the cipher text by uploading it together with his private key to the same site.

Which option poses the greater security risk? Please explain! **[2]**

d) Which algorithm among AES, DES and RSA would you use to secure the customers' data inside their blocks? Explain your answer. **[2]**

e) Address the following questions concerning cookies.

i. How do the HTTP cookies work in general? **[3]**

ii. Can the HTTP cookies be used to exchange for personal information? **[2]**

f) A virtual private network (VPN) is a network that uses public means of transmission (Internet) as its WAN link and a well-designed VPN uses several methods for keeping your connection and data secure. Give any **five** ways that can be employed to keep a connection secure. **[5]**

Question 4

a) Answer the following on network attacks.

i. Explain TCP Syn Flooding attack briefly. **[2]**

ii. Suggest a solution for ARP Cache poisoning attack. **[2]**

iii. Give names of two attacks at the network layer. **[2]**

b) Answer the following questions on Wi-Fi Security

i. Describe how a man-in-the-middle attack may be performed on a Wi-Fi network and the consequences of such an attack. **[6]**

c) An access attack is an attempt to access another user account or network device through improper means. As a network administrator you are responsible for ensuring that only authorized users access the network. Unauthorized attacks are attempted via four means, all of which try to bypass some facet of the authentication process. Give the **four** attacks. **[4]**

Question 5

a) Describe ,with examples and proposed penalties, the following offences as stated in Zimbabwe's Computer Crime and Cybercrime Bill

.

i. Illegal Access **[2]**

ii. Illegal interception **[2]**

iii. Illegal Devices **[2]**

iv. Computer-related Fraud **[2]**

v. Violation of Intellectual Property rights **[2]**

b) Cloud computing has taken centre-stage in today's computing environment and it comes with its challenges and benefits. Give any **five** obstacles and opportunities for adoption and growth of cloud computing. **[5]**

c) Virtual Machines come with several benefits as well as security concerns. Describe the following security issues.

i. VM Sprawl

ii. Mobility

iii. Hypervisor Intrusion

iv. Hypervisor Modification

v. Communication **[5]**

END OF PAPER