University of Ruhuna - Faculty of Technology

Bachelor of Information and Communication Technology Degree

Level 3 (Semester 2) Examination, August 2020

Course Unit: ICT3243- Network, Computer and Application Security Time Allowed: **2 hours**

Answer all **four (04)** questions

This question paper contains **02 pages.**

Question 01

a) Define Computer security.

b) Consider an Automated Teller Machine in which provides users a Personal Identification number (PIN) and a card for account access. Briefly explain confidentiality, integrity, and availability requirements associated with the system with some examples.

c) "The objective of Cyber attackers is not only the money". Do you agree with this statement? Justify your answer with suitable examples.

d) Suppose that while trying to access a video collection on some web site, you see a pop-up window stating which you require to install a software (codec) in order to view the videos. What threat might this pose to your computer system if you approve this installation request?

e) What are the mechanisms that malware can use to propagate? What are the best practices to prevent malware and enhanced security of your system?

Question 02

a) Compare and contrast Access controller matrix and Access controller lists.

b) What are the types of XSS attacks? What can XSS be used for? Explain briefly.

c) Briefly discuss the difference between Authentication and Authorization.

d) Suppose you have been appointed as a project manager and assigned the task of developing a banking application system for a leading bank in Japan.

i. Briefly explain about Biometric authentication, Biometric techniques and discuss how it helps to improve your system security.

ii. "Your system might open to CSRF attack". Explain what is CSRF attack? Why CSRF token is important for your system?

iii. How do you prevent SQL injection in your application?

Question 03

a) What is the principal difference between the Bell–LaPadula Model (BLP model) and the Biba Integrity model?

b) Sandboxing provides an extra layer of security that prevents malware or harmful applications from negatively affecting to your system. Discuss how sandboxing helps to make secure applications using sandboxing environment.

c) "The TCP/IP suite has many design weaknesses so far as security and privacy are concerned." Discuss this statement using two types of TCP/IP Security Issues.

d) Cybercrime has created a major threat to those who use the internet, with millions of users' information stolen within the past few years. Briefly explain major three types of cybercrimes which had been widely spread in the world.

Question 04

a) One of the most common types of DNS cyber-attacks is known as DNS Cache Poisoning. Briefly explain above statement.

b) Why you need to protect your Intellectual Property? Discuss briefly Patent, and Copyright.

c) Briefly discuss why "Ethical hacking" is one of most valuable assets of an organization.

d) Cryptography is an indispensable tool for protecting information in computer systems.

   i. Compare and contrast "Public key" and "Private key" in cryptography.

   ii. Secure Hash Algorithm (SHA) and Message Digest (MD5) are the standard cryptographic hash functions to provide data security. Briefly explain why SHA hash function has become popular than MD5 hash function.

e) Briefly explain "Principle of Least Privilege" with suitable example. What are the benefits of the Principle of Least Privilege?

-----------------------------End of the paper---------------------------------