The Open University of Sri Lanka
Faculty of Engineering Technology
Department of Electrical & Computer Engineering

Study Programme	: Bachelor of Software Engineering Honours
Name of the Examination	: Final Examination
Course Code and Title	**: EEI5270 Information Security**
Academic Year	: 2024/2025
Date	: 19th August 2024
Time	: 0930 - 1230 hrs
Duration	: **Three(3) hours**

General Instructions

- Read all instructions carefully before answering the questions.
- This paper consists of **Four (4)** questions in Three (3) pages.
- Answer **ALL** Questions. All questions carry equal marks.
- Answers for each question should commence on a new page.
- Try to write answers in **point form**.
- This is a **Closed Book Test(CBT)**.
- Answers should be in clear handwriting.
- Do not use any colour pen other than **blue/black**.
- **General Examination Guidelines of the OUSL are applicable.**

QUESTION 1

1.1) Differentiate between **data** and **information**.

(4 marks)

1.2) Briefly describe the following terms about information security:

i) Threat

ii) Risk

(4 marks)

1.3) Briefly explain the process of risk assessment. Give three (3) examples of risk response strategies for organizations.

(4 marks)

1.4) Briefly explain the components of the **CIA Triad**.

(6 marks)

1.5) Categorise and explain the following risk-related conditions according to the **Risk Management Matrix** using a figure.

i) Likelihood of Occurrence

ii) Impact

(7 marks)

QUESTION 2

2.1) Define **Asymmetric Key** cryptography.

(4 marks)

2.2) Briefly explain the **Hash Functions** in Cryptography.

(4 marks)

2.3) What are the key priorities of the Cryptographic Hash Functions? (Name at least four (4))

(4 marks)

2.4) Explain three (3) management challenges associated with symmetric key cryptography.

(6 marks)

2.5) Solve the following ciphertext and give the plain text using the **columnar transposition cypher**. The **answer only carries one (1) mark**; the rest are for steps.

Alphabet: QZRBNYVTWOEAKMJXSLIDCFUHGP
Keyword: **COBRA**
Ciphertext: **NGARSCAAPOSECTDFIJGOSTUTIEOSHB**

(7 marks)

QUESTION 3

3.1) Differentiate between ***HTTP*** and ***HTTPS*** protocols.

(4 marks)

3.2) Briefly describe the following certificates in *SSL/TLS.*

i) Domain Validated (DV) Certificates
ii) Extended Validated (EV) Certificates

(4 marks)

3.3) Briefly explain the ***Network Access Control(NAC)***. Give three (3) benefits of NAC for organizations.

(4 marks)

3.4) Briefly explain the following HTTP methods.

i) POST
ii) PUT
iii) PATCH

(6 marks)

3.5) Briefly describe **four(4)** software security best practices.

(7 marks)

QUESTION 4

Read the following hypothetical case of an incident and write answers for the questions (4.1 - 4.4) using the case.

GreenBank, a mid-sized digital banking service provider in Southeast Asia, prided itself on its customer-centric online platform and robust mobile banking services. The organization managed over 500,000 customers and stored sensitive user credentials, transaction data, and personal identifiable information (PII) on its internal servers. In early April 2025, GreenBank suffered a serious information security incident involving unauthorized access to its internal systems. The breach came to light after a group of users reported suspicious withdrawals from their bank accounts despite not initiating any transactions. Following this, GreenBank's cybersecurity team launched an internal investigation, which revealed that attackers had exploited a vulnerability in the bank's legacy login portal. The attackers bypassed the basic authentication mechanism used by GreenBank's online portal. Authentication is the process of verifying the identity of a user or system. It ensures that the entity requesting access is indeed who they claim to be. This is often the first line of defense in any system, and if improperly configured, it can be exploited, as was the case here. GreenBank primarily used password authentication as the method for user verification. This means that a user was required to enter a predefined password associated with their username to gain access. Although the system enforced minimum password length and complexity rules, it did not implement any advanced protective measures such as rate-limiting or multi-factor authentication. The attackers exploited an exposed API endpoint that allowed for brute-

force attempts without triggering alerts. This oversight enabled them to guess multiple weak passwords over time, ultimately gaining access to thousands of customer accounts. Upon further forensic analysis, the cybersecurity team found that the passwords stored in the system had been compromised due to improper cryptographic storage. The bank's system stored hashed versions of user passwords in a file on its authentication server. However, GreenBank's development team had relied on an outdated hash function (MD5). Worse still, the hash file was accessed and downloaded by the attacker once they obtained admin privileges. Another critical weakness was the absence of password salting. This significantly accelerated the process for attackers to reverse the hash and retrieve original passwords. The internal audit report emphasized that the lack of Multi-Factor Authentication (MFA) significantly contributed to the scale of the breach. MFA is a security mechanism that requires users to present two or more verification factors to gain access to a resource. MFA typically involves three categories of verification factors. Had GreenBank enforced MFA, even if the attacker obtained valid usernames and passwords, they would still have been unable to access accounts without the second or third factor. The breach cost GreenBank both financially and reputationally. The bank had to compensate affected customers and invest heavily in upgrading its cybersecurity infrastructure. Following the security breach, GreenBank implemented several critical measures to strengthen its cybersecurity framework. First, the outdated MD5 hashing algorithm was replaced with a more secure alternative. To further enhance password protection, the bank introduced per-user password salting. Additionally, Multi-Factor Authentication (MFA) was enforced for all customer and administrative logins, adding an extra layer of security beyond simple password entry. Finally, mandatory security training was conducted for all IT staff to improve awareness and ensure best practices are followed consistently across the organization.

4.1) Define the term ***Authentication***.

(4 marks)

4.2) Briefly explain **password authentication**.

(4 marks)

4.3) Briefly explain what **password salting** is.

(4 marks)

4.4) Describe the **Hash function** for protecting the password file.

(6 marks)

4.5) Briefly explain the three (3) **MFA** methods with examples.

(7 marks)

------- ALL RIGHTS RESERVED -------