00063

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

Study Programme	: Bachelor of Technology Honours in Engineering Bachelor of Software Engineering Honours
Name of the Examination	: Final Examination
Course Code and Title	**: EEI5270/EEX5270 - Information Security**
Academic Year	: 2021/22
Date	: 2nd February 2023
Time	: 09:30-12:30hrs

General Instructions

1. Read all instructions carefully before answering the questions.
2. This question paper consists of **Five (5)** questions on **Four (4)** pages.
3. **Answer any four (4) questions out of the five (5) questions.**
4. All questions carry equals marks.
5. Answer for each question should commence from a new page.
6. This is a Closed Book Test **(CBT).**
7. Answers should be in clear handwriting.
8. Do not use red colour pen.

Answer any four (4) questions out of the five (5) questions

1. Confidentiality, Integrity, and availability (CIA) are the three fundamental information security principles that we have built our security infrastructure around. In designing any kind of security solution, we should be focusing our effort on ensuring these properties.

   a) Discuss the risk of not ensuring CIA properties in a Food Delivery (Applications similar to UberFoods, PickmeFoods) application and its infrastructure. Also include the mitigation techniques you can take to make it more secure and reliable for each property in CIA.

   [8 Marks]

   b) Explain the approach you are going to take if you are given the responsibility of building the information security initiative within an organization. Include the steps you would take to complete the task by justifying each step.

   [8 Marks]

   c) Compare and contrast Opensource Software & Closed source software with respect to **security of each methodology**.

   [9 Marks]

   [Total 25 Marks]

2. Web Applications are one of the most targeted areas in the information security field. There are various types of attacks that you need to safeguard your application against, and the list grows by the day.

   a) Discuss the **differences between GET and POST** methods related to both intended design and the security.

   [8 Marks]

   b) Explain the **shortfall of HTTP** protocol in securing a web application that HTTP **cookies are being used to solve**.

   [9 Marks]

   c) "*In a distributed denial-of-service (DDoS) attack, it's extremely hard to identify the legitimate users from malicious users* ". Discuss the above phrase and **defend** your answer.

   [8 Marks]

   [Total 25 Marks]

3. Encryption is the bedrock of modern information security techniques. It is important because it allows you to securely protect data that you don't want anyone else to have access to. Businesses use it to protect corporate secrets, governments use it to secure classified information, and many individuals use it to protect personal information to guard against things like identity theft.

   a) Briefly describe **the requirement of Digital Signatures** and the **use of them** in current day-to-day life. Describe minimum of 2 uses.

   [8 Marks]

   b) Explain the steps in **getting a Digital certificate** for a web application. Your answer should contain information on Private Keys, Public-Keys, and Certificate Authority (CA) at minimum.

   [8 Marks]

   c) Discuss **how an attacker would break** the protection which is provided by the Digital Certificate for a Web application without the private key being leaked. In the scenario, the attacker can see the content of which is being transferred. Discuss only with related to the Digital Certificate and PKI. Information on network penetration is not required.

   [9 Marks]

   [Total 25 Marks]

4. It is a common saying that "Humans are the weakest link in cybersecurity." This negative characterization of human nature is deeply rooted in the cybersecurity industry. The human factor problem is complex because, by its nature, it involves a serious sociological, psychological, and philosophical discussion

   a) Briefly describe the **reasons behind** the human factor being the weakest link in the chain of Cyber Security and propose the **mitigation techniques** for it. Your answer should contain techniques beyond "Awareness and Training".

   [8 Marks]

   b) Discuss the **importance on code review** for a secure software development lifecycle with minimum **3 distinct examples**.

   [8 Marks]

   c) With the recent hike in Ransomware attacks, what kind of **preparational safeguards** which we can take which is beyond the malware/virus identification tools against a ransomware attack. You should discuss the **safeguards which are changing the way human interact with IT operations** rather than tool-based controls.

   [9 Marks]

   [Total 25 Marks]

5. The design/architecture of the infrastructure is crucial for the security of the services offered. Original design should cater to the security requirement from the beginning of the organization rather than ad-hoc solutions.

   a) Briefly **describe** the Bell–LaPadula model and the **importance of following them** for our solutions.

   [8 Marks]

   b) Write a brief description on the following security products, focusing on **what do they do to secure the infrastructure**.

      i. Honeypot

      ii. Intrusion Detection Systems (IDS)

   [8 Marks]

   c) For a web application that is hosted on your organization's infrastructure, discuss the requirement of having both *Network Firewall* and a *Web Application Firewall*. Do you recommend having both or one? Justify your answer.

   [9 Marks]

[Total 25 Marks]

End of the Paper