00041

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	: 2020/21
Date	: 13th February 2022
Time	: 0930 - 1230 hrs
Duration	: **3 hours**

General Instructions

1. Read all instructions carefully before answering the questions.
2. This question paper consists of **Five (5)** questions in **Four (4)** pages.
3. Answer any **Four (4)** questions. All questions carry equal marks.
4. Answer for each question should commence from a new page.
5. Relevant charts/ codes are provided.
6. This is a Closed Book Test (CBT).
7. Answers should be in clear hand writing.
8. Do not use Red colour pen.

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

   a) Write a brief description on the security of an e-mail service (i.e.: gmail.com) in contrast of the Confidentiality, Integrity and Availability. Give 3 examples (one for each leg of CIA) of how these are implemented/could be achieved in the example you picked. **[8 Marks]**

   b) Explain how the ***availability*** is connected to Information Security assurance and use 2 example threats to justify your answer. **[8 Marks]**

   c) What is your opinion on the ***open design and following open standards*** when it comes to information security assurance? Discuss on the change it will bring to the overall security of an IT product. **[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 upon, and the list grows by the day.

   a) Discuss the importance of the concept of ***defense in depth*** and how you would implement it in a web application to secure the communication between the server and the client.

   [8 Marks]

   b) Compare and contrast the ***GET*** and ***POST*** methods of HTTP protocol with respect to information security.

   [9 Marks]

   c) Write a brief description on the following terms, usage and the contribution to the security of a web application.

      i. TLS

      ii. Load Balancer (another protocol can be added to maintain consistandy)

   [8 Marks]

   [Total 25 Marks]

3. The architecture of the network infrastructure is crucial for the security of the services offered. Original design should cater the security requirement of the organization rather than adhoc solutions.

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

      i. Network Firewalls

      ii. Web Application Firewalls

   [12 Marks]

   b) For a web application which 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. **[13 Marks]**

   [Total 25 Marks]

4. Encryption is the bedrock for modern information security techniques. It is important because it allows you to securely protect data that you do not 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) Write a brief description on the following topics considering the requirement, number of keys and general process performance/speed

      i. Symmetric Encryption

      ii. Asymmetric Encryption

   [8 Marks]

   b) Explain the concept of Digital Signing using an example diagram including relevant asymmetric cryptographic keys.

   [8 Marks]

   c) Considering Public Key Infrastructure (PKI) is being used for securing web applications (https), discuss the possibility of an attacker breaking the security provided by https. How can advisory break it and what measures should one take to secure against it?

   [9 Marks]

   [Total 25 Marks]

5. Even most current sophisticated infrastructures are susceptible to Distributed Denial of Service attacks (DDOS). Attackers are using complex methods of conducting these attacks daily which results in significant level of disruption to the IT services.

   a) Describe the below types of DDOS techniques and the methods we could use to reduce the impact.

      i. Network volumetric-Based DDOS

      ii. Protocol-Based DDOS

   [12 Marks]

   b) Describe how a SYN flood attack works using a diagram and select your recommended method of mitigation from "*Increase backlog queue size*", "*decrease timeout*" & "*avoid state until 3-way handshake*". Justify your answer comparing to the other two.

   [13 Marks]

   [Total 25 Marks]