THE OPEN UNIVERSITY OF SRI LANKA
B.SC. (IT) DEGREE PROGRAMME – 2024/2025
FINAL EXAMINATION
COU3305 – COMPUTER SECURITY CONCEPTS
DURATION: TWO HOURS ONLY (02 HOURS)

Date: 10.11.2025 Time: 01.30 p.m. – 03.30 p.m.

Answer any FOUR Questions ONLY.

Q1.

a) Define the term ***"Intruder"*** in the context of computer and network security. [03 Marks]

b) List three (03) primary TEMPEST countermeasures that are used to protect information systems from electromagnetic eavesdropping. [03 Marks]

c) Briefly describe the three (03) main types of hackers commonly recognized in the field of cybersecurity. [4.5 Marks]

d) Illustrate and explain the relationship among the key components of a Security Policy using a well-labeled diagram. [6.5 Marks]

e) Compare and contrast the three (03) main types of intruders based on their technical skills, motivations, and the level of threat they pose to an organization. [08 Marks]

Q2.

a) Define the term ***"Host Security"***. [2.5 Marks]

b) Briefly explain each principle of the CIA Triad. [4.5 Marks]

c) While the CIA Triad represents the core objectives of information security, there are also ***supportive security principles*** that enhance overall system protection. Briefly describe these supportive security principles. [06 Marks]

d) Briefly explain the eight (08) security design principles proposed by Saltzer and Schroeder (1975), describe how each principle contributes to the effective design and maintenance of secure information systems. [12 Marks]

Q3.

a) Define the term ***"Social Engineering"***. [03 Marks]

b) Identify and describe the four (04) main types of computer viruses, providing a brief explanation of each. [06 Marks]

c) Briefly explain the following modern cybersecurity concepts:

i. Cyberwarfare
ii. Insider Threats
iii. Hacktivism [06 Marks]

d) Compare and contrast the following four (04) different types of malwares: Viruses, Worms, Trojans, and Ransomware, with reference to their methods of propagation, primary objectives, and challenges in detection. [10 Marks]

Q4.

a) The term *"AAA"* in computer security stands for *Authentication, Authorization, and Accounting.* While authentication verifies a user's identity, briefly describe the meanings of the **other two (02) components** represented by the letter ***'A'*** in the AAA framework. [03 Marks]

b) Explain why authentication is important in a computer system. [4.5 Marks]

c) Compare ***Role-Based Access Control (RBAC)*** and ***Rule-Based Access Control*** mechanisms, highlighting their *working principles, advantages, and limitations.* [7.5 Marks]

d) Explain the limitations of Digest Authentication and discuss how these limitations are addressed by the Kerberos authentication protocol. [10 Marks]

Q5.

a) State three (03) common motives behind cyberattacks. [03 Marks]

b) Explain two (02) methods that can be used to defend against Denial-of-Service (DoS) attacks. [03 Marks]

c) Describe the difference between DoS and Distributed Denial-of-Service (DDoS) attacks. [04 Marks]

d) Explain the five-stage process of a cyberattack and discuss how understanding these stages can assist in designing effective defense mechanisms. [07 Marks]

e) Discuss the uses of Voice over IP (VoIP) technology and analyze the common security vulnerabilities associated with its implementation and operation. [08 Marks]

Q6.

a) Differentiate between ***"Castle and Moat Security"*** and ***"Zero Trust Security"*** models, highlighting their key principles and differences in access control approaches. [06 Marks]

b) Define the term ***"Risk Management"*** and explain why it is important for every organization. [05 Marks]

c) Explain the concept of ***Dumpster Diving*** and discuss how attackers use this technique to perform Social Engineering attacks, providing relevant examples to support your explanation.
Additionally, describe suitable ***mitigation strategies*** that organizations can implement to prevent such attacks. [14 Marks]