00045

Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized in Cyber Security

Final Examination
Year 2, Semester 1(2022)

IE2022 - Introduction to Cyber Security

Duration: 2 Hours

June, 2022

Instructions to Candidates:

- This paper is preceded by 10 minutes reading period. The supervisor will indicate when answering may commence.
- This paper has 4 questions.
- Answer all questions in the booklet given.
- The total marks for the paper is 100.
- This paper contains 4 pages, including the cover page.
- Calculators are allowed.

Question 1 (25 marks)

a. Differentiate between vulnerability, threat, and attack with respect to information security.

(6 Marks)

b. An organization is frequently facing difficulties with attacks originated from outside due to its internet connections. After performing a quantitative risk assessment, it was identified that the Annualized Loss Expectancy (ALE) of the organization due to outside attacks is 200,000 dollars. IT department is proposing a firewall solution to mitigate this problem costing 30,000 dollars per year to reduce the possibility of outside attacks by half for a year.

Perform a cost/benefit analysis and determine whether the proposed control is benefited for the organization.

(5 Marks)

c. You are hired as an IT security engineer to manage IT infrastructure security of a large organization. Recommend two physical controls, technical controls, and administrative controls each to protect valuable assets available in a server room.

(6 Marks)

d. Recently the management of your organization has decided to update the IT policy of the organization to facilitate BYOD (Bring Your Own Device) to allow employees to access enterprise data and systems using personal mobile devices such as smartphones, tablets, and laptops.

Evaluate the security threats associated BYOD for an organization.

(4 Marks)

e. Assume SLIET is a reputed university in Sri Lanka. They use a student information management system to detail with data (personal/ financial/ registration/ results) related to all students. Assess the impact of data loss of student information management system for SLIET.

(4 Marks)

Question 2 (25 marks)

a. Differentiate substitution ciphers and transposition ciphers using an example for each.

(4 Marks)

b. Briefly describe uses of the following with respect to Public Key Infrastructure (PKI)

i). Certifications Authority (CA)
ii). Public key certificate

(4 Marks)

c. Analize the advantages of using Cipher Block Chaining (CBC) mode over Electronic Code Book (ECB) mode in symmetric block cipher.

(5 Marks)

d. Two users Fred and George use Diffie-Hellman key exchange with a common prime number p = 11 and generator g = 7 (which is a primitive root modulo 11). Let 6 and 9 be the private keys of Fred and George respectively.

i). Find the public keys of Fred and George.

(4 Marks)

ii). Calculate the common shared secret key.

(2 Marks)

e. You are required to develop a secure communication protocol to satisfy the following security requirements using asymmetric cryptography and a cryptographic hash function.

- Sender wants to send large messages over an unsecure communication channel.
- Upon receiving the messages, receiver should be able to validate that the messages are originated from authorized sender.
- Upon receiving the messages, receiver should be able to verify whether messages are received without any intentional or unintentional modification.
- Sender should not be able to deny being the sender of the messages later on.

Propose a mechanism to be used to satisfy the above requirements. You are expected to clearly describe how the proposed mechanism works.

(6 Marks)

Question 3 (25 marks)

a. Differentiate between Access Control List (ACL) and Capability Ticket (CT) used in access control system implementations.

(4 Marks)

b. Using an example, clearly explain the use of a role-based access control policy.

(4 Marks)

c. You are supposed to implement an access control system for a banking system to control access to it resources. Propose four concepts/features that should be supported in an effective access control system develop for the banking system.

(4 Marks)

d. A Higher Education Institution has different systems/applications such as learning management system, IT help desk, lab machine login, internet login, etc which requires separate login each time using separate accounts. Authentication, authorization and accounting is handled separately in each system.

i) There is a proposal to provide a Single Sign-On (SSO) system. Evaluate the proposed solution by analysing the security and administrative perspectives.

(4 Marks)

ii) If a SSO system is implemented, justify the importance of using strong multifactor authentication mechanism for it.

(3 Marks)

e. Remote user authentication is a mechanism in which the remote server/system verifies the legitimacy of a user over an insecure communication channel. Password based authentication schemes have been widely deployed to verify the legitimacy of remote users as password authentication is one of the simplest and the most convenient authentication mechanism over insecure networks.

i). State additional security threats raises due to remote authentication.

(2 Marks)

ii). Propose a challenge-response to counter such threats in password based remote authentication. (Hint: A diagram can be used for the explanation).

(4 Marks)

Question 4 (25 marks)

a. Briefly describe following malware types.
i). Trapdoor
ii). Adware
iii). Trojan Horse
iv). Rootkit

(8 Marks)

b. Assess the impact of crimeware toolkits to the development of new malwares.

(5 Marks)

c. Recommend the most suitable legal devices that can be used to protect following computer objects and justify your answer.

i). Latest computer Graphics Processing Unit (GPU)
ii). Complied version of a commercial software package
iii). User manual of a computer product
iv). Source code of a closed source software

(8 Marks)

d. "*Even when there is clear evidence of a computer crime, the victim (e.g.; banks, insurance companies, investment firms, the government, and healthcare groups) may not want to prosecute sometimes.*"

Do you agree with this statement? Justify your answer by explaining why the statement is correct or incorrect.

(4 Marks)

-- End of the Question Paper --