Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized in Cyber Security

Final Examination
Year 2, Semester 1(2019)
Regular Intake

IE2022 - Introduction to Cyber Security

Duration: 2 Hours

June 2019

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.
- Electronic devices capable of storing and retrieving text, including calculators and mobile phones are not allowed.

Question 1 (25 marks)

a) Differentiate between active attacks and passive attacks. Give one example for each attack.

(4 marks)

b) Briefly explain the following terms with respect to computer security;
   i) Vulnerability
   ii) Threat
   iii) Risk

(6 marks)

c) Consider an Automated Teller Machine (ATM) in which users provide a Personal Identification Number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case indicate the degree of importance (low, moderate or high) of the requirement.

(5 marks)

d) A deception is a threat to system or data integrity. The deception can be in the form of Masquerade, Falsification, or Repudiation. Describe these three attacks by providing an example per each.

(6 marks)

e) The first critical step in securing a system is to secure the base operating system upon which all other applications and services rely. As a security engineer of a company, recommend steps to be followed to secure an operating system.

(4 marks)

Question 2 (25 marks)

a) Compare symmetric and asymmetric cryptography.

(4 marks)

b) Two users Mulder and Scully use Diffie-Hellman key exchange with a common prime number $p = 13$ and generator $g = 6$ (which is a primitive root modulo 13). Let 3 and 10 be the private keys of Mulder and Scully respectively.

   i). Find the public keys of Mulder and Scully.

(4 marks)

   ii). What is the common shared secret key?

(2 marks)

c) Compare Electronic Code Book (ECB) mode and Cipher Block Channing (CBC) mode used in symmetric block cipher with respect to the following;

   i). Security provided for repeated plain text blocks
   ii). Speed of encryption (possibility of parallel encryption and decryption)
   iii). Effect to the encryption of other blocks if an error is generated when encrypting the first block.

(6 marks)

d) Janie wants to transmit a message over an insecure network to Jack in a way that only Jack can read it. When the message is received, Jack should be able to verify whether it actually came from Janie and make sure that the entire message is received without any change. In addition to this Jack should be able to take the message to a third party at a later time and prove to the third party that the data exchange did take place.

Propose a method to achieve the above data transmission using public key cryptography and cryptographic hash function. (Hint: A diagram can be used for the explanation)

(6 marks)

e) Describe the use of certificate authorities (CA) in public key infrastructure.

(3 marks)

Question 3 (25 marks)

a) Access control is a process of prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

i) What are the three elements of access control? Provide example for each.

(3 marks)

ii) Explain what access matrix is with the aid of a diagram.

(3 marks)

iii) An access matrix is usually sparse and is implemented by decomposition in one of two ways named access control list and a capability ticket. Differentiate between access control list and a capability ticket.

(3 marks)

b) Briefly explain the following concepts and features that should be supported by an access control system.

i) Least privilege
ii) Separation of duty
iii) Open and closed policies

(6 marks)

c) List the four means of authentication. Give two examples for each.

(6 marks)

d) Workstation hijacking is a situation where the attacker waits until a logged-in workstation is unattended in order to get unauthorised access to the system and use its data and functionalities. Recommend controls to prevent such from happening.

(4 marks)

Question 4 (25 marks)

a) Briefly describe three main malware propagation mechanisms. Give one malware example for each type of propagation.

(6 marks)

b) Assume you received an email which appears to have come from your bank, including your bank logo and the following contents:

"Dear customer, our records show that your internet banking access has been blocked due to too many login attempts with invalid information such as incorrect access number, password, or security number. We urge you to restore your account access immediately, and avoid permanent closure of your account, *by clicking on this link* to restore your account. Thank you from your customer service team."

i) What form of attack is attempted by this email?

(2 marks)

ii) How should you respond to such emails? Justify your answer.

(2 Marks)

c) Differentiate between signature based scanning and activity traps used in malware detection.

(3 marks)

d) Briefly explain the type of protection provided and the difficulty of enforcing the following in computer works such as computer programs.

i) Copyrights
ii) Patents
iii) Trade secrets

(6 marks)

e) Describe computer targeted crimes and computer assisted crimes using suitable example for each.

(6 marks)

-- End of the Question Paper --