Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized in Cyber Security

Final Examination
Year 2, Semester 1(2019)

IE2022 - Introduction to Cyber Security

Duration: 2 Hours

October, 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 inside attacks and outside attacks. Give one example for each attack.

(4 marks)

b) Briefly explain the following terms with respect to computer security;

i). Vulnerability

ii). Attack

iii). Countermeasure

(6 marks)

c) You are hired as a Systems engineer to manage IT infrastructure security of a large organization. Recommend two detective controls, preventive controls and recovery controls each.

(3 marks)

d) Unauthorized disclosure is a threat to system confidentiality. Unauthorized disclosure can be in the form of Exposure, Interception, Inference or Intrusion. Describe these four attacks by providing an example per each.

(8 marks)

e) Once the operating system is appropriately built, secured, and deployed, the process of maintaining security is continuous. This results from the constantly changing environment, the discovery of new vulnerabilities, and hence exposure to new threats. Recommend four steps needed for secure maintenance of deployed system.

(4 marks)

Question 2 (25 marks)

a) Differentiate cryptography and cryptanalysis.

(4 marks)

b) Two users William and Mark use Diffie-Hellman key exchange with a common prime number p = 23 and generator g = 5 (which is a primitive root modulo 23). Let 4 and 3 be the private keys of William and Scully respectively.

i). Find the public keys of William and Mark.

(4 marks)

ii). What is the common shared secret key?

(2 marks)

c) Compare block cipher and stream cipher with respect to the following;

i). Security provided

ii). Speed of encryption (on the fly encryptions and data at rest)

iii). Size of the encrypted data output

(6 marks)

d) Key management is often considered the most difficult part of designing a cryptosystem. Briefly describe five essential characteristics of key management.

(5 marks)

e) Describe the following with respect to Public Key Infrastructure (PKI);

i). PKI Certificates (Digital Certificate)
ii). Certificate Authority (CA)

(4 marks)

Question 3 (25 marks)

a) Explain the following with respect to access control. Provide example for each.
i). Subject
ii). Object
iii). Access rights

(6 marks)

b) Differentiate between Discretionary Access Control (DAC) and Mandatory Access Control (MAC).

(4 marks)

c) Briefly explain the following concepts and features that should be supported by an access control system.
i). Reliable input
ii). Support for fine and coarse specifications
iii). Administrative policies

(6 marks)

d) A widely used password security technique is the use of hashed passwords and a salt value. This scheme is found on operating systems and many other applications. Using a diagram explain how hashed passwords with salt is implemented.

(5 marks)

e) Recommend controls for following attacks related to password based authentication.
i). Offline dictionary attack
ii). Workstation hijacking

(4 marks)

Question 4 (25 marks)

a) One possible way of categorizing malware is based on the payloads/actions malware performs on the target. Briefly explain four possible malware payloads with examples for each.

(8 marks)

b) Assume that you received an email, which happens to have come from a member of your 2nd year project group with a subject indicating that a draft version of the proposal report. When you viewed the email, you saw that it asks you to review the attached final draft of the proposal report supplied as a PDF document before uploading it to courseweb. When you attempt to open the PDF, the viewer pops up a dialog labelled "Launch File" indicating that "the file and its viewer application are set to be launched by this PDF file." In the section of this dialog labelled "File," there are a number of blank lines, and finally the text "Click the 'Open' button to view this document." You also note that there is a vertical scroll-bar visible for this region.

i). What type of threat(s) might this pose to your computer system and how could you check your suspicions without threatening your system?

(2 marks)

ii). What type of attack(s) this type of message is associated with and how many people are likely to have received this particular e-mail?

(2 marks)

c) Differentiate between virus and worm.

(3 marks)

d) Briefly explain the type of protection provided to computer works such as computer programs by following legal objects.

i). Copyrights
ii). Patents
iii). Trade secrets

(6 marks)

e) Assess the challenges in prosecuting computer crimes.

(4 marks)

-- End of the Question Paper --