Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized in Software Engineering

Final Examination
Year 4, Semester 2 (2019)

SE4030 – Secure Software Development

Duration: 2 Hours

October 2019

Instructions to Candidates:

- This paper has 4 questions. Each question carries 25 marks.
- Answer all questions in the booklet given.
- The total marks for the paper is 100 (contributes to 50% of the final mark).
- This paper contains 5 pages, including the cover page.
- Electronic devices capable of storing and retrieving text, including calculators and mobile phones are not allowed.
- There is an additional reading time of 10 minutes.

Question 1 (25 marks)

a) Name two advantages of considering Software security in each stage of the Software Development lifecycle.

(2 marks)

b) Name one activity each, which can be incorporated to ensure Software Security, at the Requirement analysis phase, Design phase, Implementation phase and Testing phase according to the S-SDLC (Secure Software Development Lifecycle).

(4 marks)

c) Briefly explain the Kerckhoff's Principle and how it is applicable in modern cryptographic algorithms.

(3 marks)

d) For each of the following scenarios, suggest the most appropriate cryptographic technique to be applied, out of Symmetric encryption, Asymmetric encryption, Hashing and Encoding. Briefly justify (using 1 sentence each) why you selected each technique for each scenario.

i. Need to securely exchange a symmetric key between two parties

ii. Need to share information between a few trusted servers. Speed of encryption/decryption is of paramount importance.

iii. Need to covert a URL so that any special characters are removed. No need to ensure the confidentiality of the data.

iv. Need to create a unique string that cannot be reversed and that can be used to uniquely identify a text or binary file.

(8 Marks)

e) Briefly explain (using 2-3 sentences) what is meant by Salted Hashing and how it can be used to prevent hash lookups.

(3 marks)

f) Briefly explain what is meant by Pretty Good Privacy (PGP) (using 2-3 sentences) and justify (2-3 sentences) its application in most cryptography based communication protocols.

(5 Marks)

Question 2 (25 marks)

a) Briefly explain (using 2-3 sentences) how Digital Certificates can reduce phishing attacks.

(3 marks)

b) Briefly explain (using 2-3 sentences) how the Transport Layer Security (TLS) ensures the confidentiality of the messages in a Distributed System.

(3 Marks)

c) Briefly explain (using one sentence each) the meaning of the following terms.

i) Cipher suite
ii) Self-signed certificate
iii) Certificate Authority
iv) Root authority

(4 marks)

d) Briefly explain (using 2-3 sentences) the purpose of the TLS handshake and name any two steps of that process.

(5 marks)

e) What's the main advantage of using a Cookie in a web application? Name three ways that a cookie can be secured both at the client side and along the network.

(4 marks)

f) Justify (using 3-4 sentences) how the synchronizer token pattern prevents Cross Site Request Forgery (CSRF) attacks. You may use a diagram to explain this.

(6 marks)

Question 3 (25 marks)

a) Differentiate (using 2-3 sentences) the operation between Reflective Cross site scripting and Stored/Persistent cross site scripting.

(4 marks)

b) i) Briefly explain (using 2-3 sentences) how output sanitization can prevent XSS (Cross site scripting) attacks.

ii) Give two reasons why it is advisable to use an encoder library to do the output sanitization.

(6 marks)

c) Briefly explain (using 2-3 sentences) how Union based SQL injection can be used to steal sensitive information from a system. You may apply a sample SQL query in your answer. Briefly explain (using 1-2 sentences) the standard method to prevent SQL injection attacks.

(6 marks)

d) Name two ways how Security misconfiguration can compromise the security of a system.

(4 marks)

e) Briefly explain (using 2-3 sentences) how the National Vulnerability Database (NVD) and the Common Vulnerability Scoring System (CVSS) score is used to check for vulnerabilities of the dependency libraries. Justify the integration of dependency checking into the continuous integration and continuous delivery process.

(5 marks)

Question 4 (25 marks)

a) Differential (using 1-2 sentences) between Directive controls and Detective controls. Give an example for each type of control.

(4 marks)

b) Explain the Authorization code grant type in OAuth. You may use a diagram to explain it. You may explain the HTTP requests that are used to get an access token.

(10 marks)

c) Briefly explain (1-2 sentences each) the purpose of each of the following aspects of OAuth.

i) Token introspection
ii) Refresh token
iii) Token revocation

(6 marks)

d) Briefly explain (using 2-3 sentences) how the Resource server can verify whether the contents of a JSON web token (JWT) has been modified by an unauthorized party.

(3 marks)

e) Briefly explain (using 2-3 sentences) why OpenID Connect specification has a pre-defined set of scopes.

(2 marks)

-- **End of the Question Paper** --