00043

Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized in Software Engineering

Final Examination
Year 4, Semester 2 (2022)

SE4030 – Secure Software Development

Duration: 2 Hours

November 2022

Instructions to Candidates:

- You will get 10 Minutes reading time
- This paper has 4 questions.
- Answer all questions in the booklet given.
- The total marks for the paper is 100.
- This paper contains 6 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. Below are the details of an attack that was successful on the database of a small company. Apply your knowledge of threat modeling to analyze the scenario and model the 3 main attack vector components for the attack described:

> "A disgruntled employee unhappy with his pay uses the shared password used by the finance department to change his pay in the database"

(6 Marks)

b. The following sections describe five scenarios where information security requirements have been violated. Apply your knowledge on information security to identify which information security requirement is violated in each situation:

i. Your PC is damaged due to lighting and not usable
ii. A competitor intercepts a private business mail between two companies
iii. A buyer places an order via email but later denies placing that order
iv. An attacker accesses your online banking system and transfers money to his account
v. A worker logs into the system pretending to be their boss to gain additional privileges

(5 Marks)

c. For each of the following scenarios, evaluate the requirements and suggest the most appropriate cryptographic primitive to be used, out of Symmetric encryption, Asymmetric encryption, Hashing and PRNG. Justify your selection briefly

i. Need to securely exchange information between two parties who have not communicated before.
ii. Need to share information between a few trusted servers. Speed of encryption/decryption is of paramount importance.
iii. Need to securely store a password so it can be later used for authentication but is not at danger of being compromised
iv. To generate the keys used by an asymmetric key algorithm

(8 Marks)

d. Evaluate the access control requirements for the below situations and select and justify the best access control method to be used:

i. Access control method to be used for files stored on a laptop shared by a family member
ii. Access control method to be used in a small company which works in retail and has the same people assuming different roles.
iii. Access control method to be used by a company which works for the government and stores highly confidential documents.

(6 Marks)

Question 2 (25 Marks)

a. Differentiate between Application Security and Software Security on at least 3 different points.

(6 Marks)

b. The company you are working for is mainly involved in developing software for external parties. Lately due to the increase in Cyber threats the management has decide to focus more on improving the security of the web applications they develop. They are currently in the process of developing a web app that will be used by the workers of your client company from home to access sensitive information from the company servers.

i. Apply your knowledge of SSDLC practices and identify and briefly explain **2 practices** that can be used during **requirements analysis and design phases** of this project

ii. Apply your knowledge of SSDLC practices and identify and briefly explain **2 tools/frameworks/protocols** that be used during the **implementation phase** of this project

(8 Marks)

c. Analyze and describe the HTTP requests and responses used by OAuth during Authorization code grant type to explain how they allow authorization with reduced risk of interception

(7 Marks)

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

i. Token introspection

ii. Refresh token

(4 Marks)

Question 3 (25 Marks)

a. Explain the function of each of the below components in PKI

i. RA

ii. CA

iii. Digital Certificate

(6 Marks)

b. Briefly explain the process behind digitally signing an electronic communication to ensure to ensure its secrecy. You will need to explain how the authenticity, integrity, and non-repudiation is guaranteed by digital signatures

(6 Marks)

c. The basic TLS handshake does not provide “Forward Secrecy

i. What is meant by forward secrecy?
ii. Explain why this is true based on the basic handshake used by TLS
iii. How is this weakness removed when using the Diffie-Hellman handshake?

(7 Marks)

d. You are in the process of building a website which has the below nonfunctional requirements. Once the website is operational is the following issues is identified via logging and auditing

i. The time it takes for the website to initially load was high which led to users not using the website
ii. It was also noticed that the server CPU was struggling with the load placed on it due to the number of TCP connections and due to users resuming existing sessions that died due to time out while the memory (RAM) utilization was low

Identify and justify 1 optimization each you would carry out to alleviate these issues

(6 Marks)

Question 4 (25 Marks)

a. Consider the below code scripts to answer the question i) and ii).

SCRIPT 01

```
var count;

count = Request.form ("count");

var SQL = "select * from Orders where count = '" + count + "' ";
```

SCRIPT 02

```
var count;

var SQL = "select * from Orders where count = '" + count + "'";
```

i. Identify the script/scripts with possible SQL injection attacks.

(02 Marks)

ii. Justify the reason for your selection.

(03 Marks)

b. Differentiate Little **Endian** with **Big Endian** using a suitable example

(4 Marks)

c. Buffer overflows can affect all types of software and can cause the program to behave unpredictably and generate incorrect results or crashes. Use below C program to answer the question i) and ii).

```
     int main(void)
     {
         char password[15];
         int valid = 0;

         printf("\n Enter the password : \n");
         gets(password);

         if(strcmp(password, "password"))
         {
             printf ("Incorrect Password \n");
         }
         else
         {
             printf ("Correct Password \n");
        valid = 1;
    }

    if(valid)
    {
        printf ("Valid user \n");
    }

    return 0;
}
```

i. Interpret how a buffer overflow attack can be done for this program.

Hint: You need to write the steps one after the other. Theoretical explanation is enough. Commands are not expected.

(8 Marks)

ii. How to avoid the above buffer overflow attack?

(4 Marks)

d. Analyze and describe the danger posed by 4 current mobile applications issues/risks.

(4 Marks)