**SENG2250: System and Network Security**

**Assignment 2**

**Due: 2024/10/11**

**C3362623**

**Task 1:**

1. (6 Marks) What other potential security issues are there with this program? Identify and discuss at least three.
   1. A potential security issue of this program is that there is no strong authentication mechanism to ensure the identity of the client. The private keys are stored on the client’s device, which means that is someone gets access to the client's computer, they could impersonate being the real client by using the stored keys. Since the key is the primary way of identification, an attacker that has access to the device can easily use the key to authenticate themself as the legitimate client and run the program.
   2. The program blindly trusts any certificate, including self-signed and fraudulent certificates. This makes man in the middle attacks possible to the client. This allows for it to be possible that a malicious entity can use its own fraudulent certificate to be used to decrypt the intercepted message between the client and the server.
   3. The program currently only verifies the server’s identity to the client however it doesn’t verify the client’s identity to the server. This allows for the server to be connected to unauthorized clients.
2. (4 Marks) If barry were to secretly be the leaker, would the program remain secure? Explain why or why not.

SSL protects data transmissions from being intercepted or altered by encryption the communication between the server and the client. This means that if the private keys and certificates are safe then the system is secure. However, if Barry is the leaker, then the private keys and certificates are no longer secure and opens the program up to the following vulnerabilities:

* + 1. Men-in-the-Middle-Attack: Due to Barry exposing the private keys or key store then an attacker could create a fake server or client using these leaked keys which makes the communication look real to both sides. This allows for the attacker to potentially intercept, decrypt, and modify the communication.
    2. Due to the certificates relying on trust and the certificates being leaked an attacker can impersonate a client or server and bypass the entire SSL security.

The keystore location and password are hardcoded into the program. This means that if Barry leaks this information that anyone with this information can easily compromise the SSL configuration. This is due to the attacker having access to the keystore and can extract the private keys and certificates and then use them for attacks.

In conclusion, no, the program would not remain secure if Barry were the leaker because the exposure of private keys, certificates, and keystore information would lead to vulnerabilities such as Man-in-the-Middle attacks and impersonation, which would compromise the SSL security.

**Reflection:**

To complete the first task, I focused on reviewing the materials covered in the lectures and labs. My primary focus was on understanding the creation of certificates and the process of importing the keys generated by the commands provided in the code files. Once I grasped this process, I was able to fulfil the task requirements with ease. This task simulates real-world scenarios where securing network communications is critical, particularly when sensitive data is being transmitted.