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.
    a. 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.
    b. 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.
    c. 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:

i. 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.

ii. 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:

Task 1:

The first task of the assignment was to secure a communication channel using SSL. This task was relatively simple to implement as the only required knowledge to complete it was to review the lecture and lab material that had been discussed. The only issue I faced when completing this task was trying to understand what was required to complete it as I found the instructions very confusing due to them spanning across several files but once I understood them, I easily completed the task. After the completion of the program, I then had to answer questions about the security of the program. This allowed me to start to analyse and critically think about the task and the implementation of it.

After completing this task, I started to grasp how this is used in the real world with things such as HTTPS. For example, using SSL certificates to encrypt the communication between a web server and a client is crucial for things such as online banking. Each time the client visits the bank's website they are given an SSL certificate which prevents attackers from accessing the sensitive information. If this information were to be intercepted and used maliciously then there would be life-altering effects on the victim's life.

Task 2:

The completion of the second task was also relatively simple as the main problem I was having was understanding how to properly implement RSA and then use it appropriately in the given program. To attempt to understand the implementation I looked at [1] and used the lecture and lab materials to help create my initial pseudo code. Once I completed my initial implementation of the RSA class I then moved to implementing the interface for the Client file and setting up how the messages were sent to the Server.

In the assignment specification, it asks for the password to be encrypted to both the server and the website however I initially misread this and implemented both the website and password to be encrypted and only have the request type visible which I have left unchanged. This means that if someone were to intercept the message being sent, they would only be able to read the request type but would not be able to understand the sensitive data that is being stored or retrieved without the private key.

Referring to the banking server example discussed earlier, the client and server often use RSA keys in their certificates to encrypt the data being sent from the client to the server. This ensures the privacy and security of the sensitive information, which could be life-altering if it were intercepted and misused.

Bibliography:

[1] GeeksforGeeks, “RSA algorithm in cryptography,” GeeksforGeeks, https://www.geeksforgeeks.org/rsa-algorithm-cryptography/ (accessed Sep. 30, 2024).