Rajveer Dhillon

500777569

Section 2

Introduction:

The purpose of this lab was to encrypt the messages between the Server and Client to ensure no replay attacks and to use DES to encrypt between the messages of the Client and Server. The connection between the Server and the Client uses the session keys established with the opening of the session and is used to encrypt and decrypt ongoing messages through the connection.

Client Side:

```
run:
Client:
Connected to Server
Nonce A: 07-03-2020 00:13:05
Nonce B:07-03-2020 00:13:05
Enter Message to be Sent to Server:
Hello Server
Message Sent. Look at Server Output
BUILD SUCCESSFUL (total time: 13 seconds)
```

Figure 1: Client GUI and Message to Server.

When the Client file is running, the output of the Client shows the connection with the Server established and then shows the nonce's of the Client (A) and Server (B). These nonces indicate the time when the connection was made between the Client and Server over the secured connection. This prevents replay attacks as the timing of the message sent can be tracked. The message can then be sent to the Server with the Client with encrypting the public key of the Server with the message (public key of Server sent when establishing the connection). The received message can be viewed on the Server output.

Server Side:

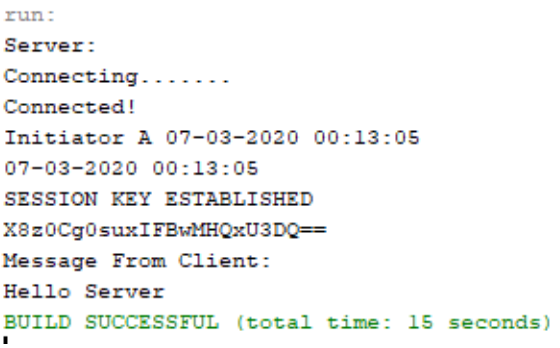

Figure 2: Server GUI and Message from Client.

The Server establishes the connection with the Client and the exchanges of keys are performed. The nonces of the Server and Client are displayed to alleviate the replay attack. The Session Keys are established as they can be used for the duration of the chat messages. The Session key is then displayed as well as the message encrypted and decrypted from the Client.