Advanced Computer Security  
Assignment 2

 Cryptography Lab (INFO2230 - W2016)

Brian Hinds

6873343

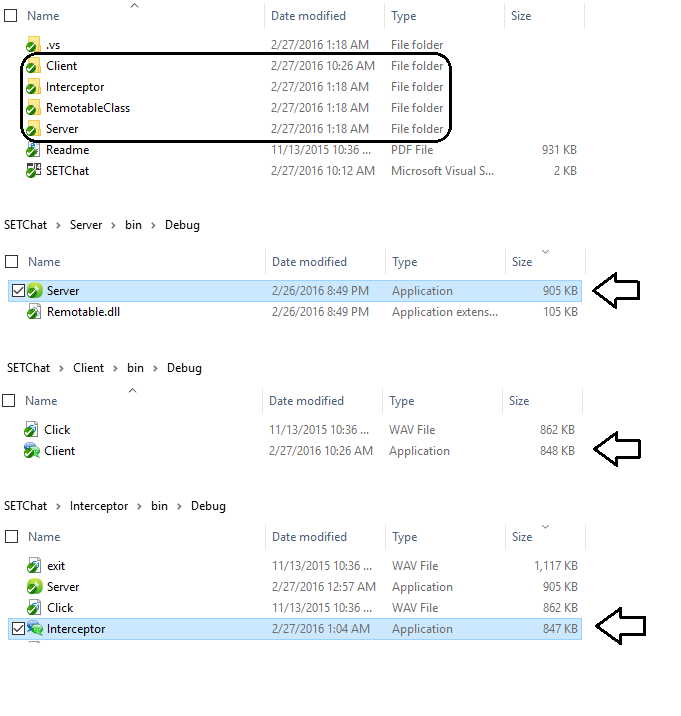
Date 2016-02-27

Overview

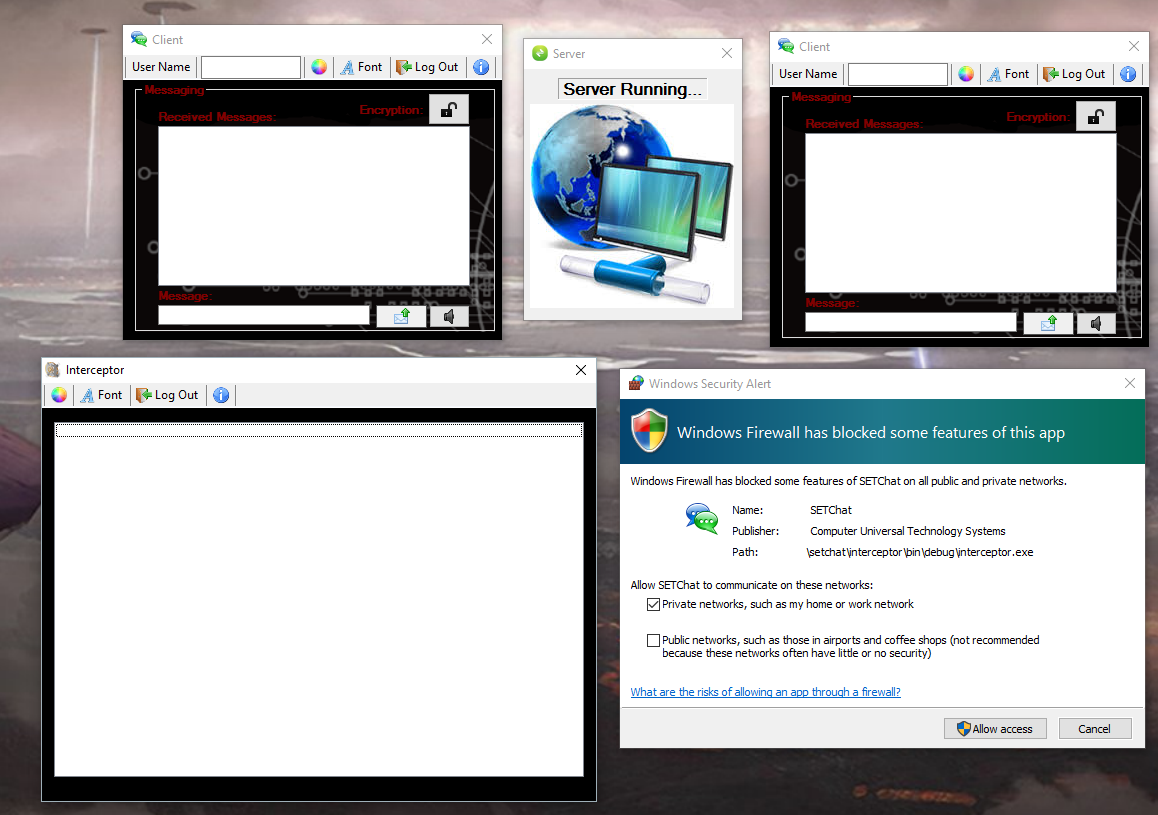
This assignment provides a chance to implement a known and trusted security algorithm into a network security scenario. The task is to create a small, instant messaging solution whereby 2 instances communicate with each other over the network, with and without encryption activated. Network packet analysis tools are then used to capture packets and reveal their contents.

Step 01

This step requires the following applications to be open in the following order. The illustration below shows the correct order; Server -> Client -> Interceptor. The client should be launch twice or more for communication.

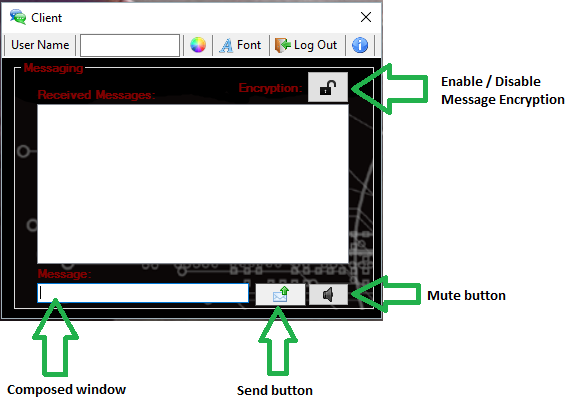


Step 02

During the launch of the application, you will encounter Windows Security Alert; you must allow access in order to run the applications.

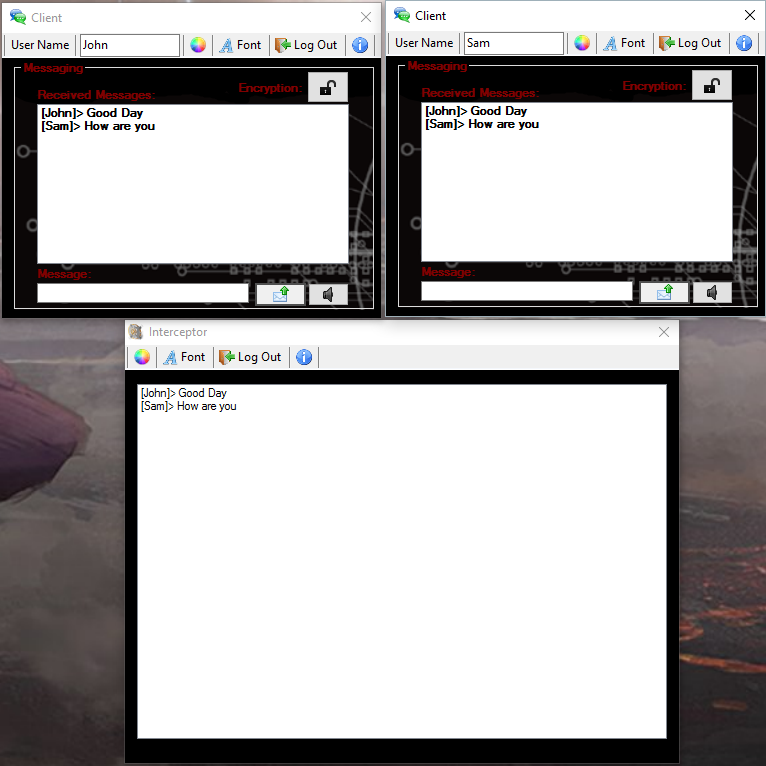
Step 03

The client application has several features and functions; the main ones are highlighted below. The client starts with encryption disable as default. The mute button mutes the messenger sound, send button sends the composed messages; note, the return key can also be used to send messages.



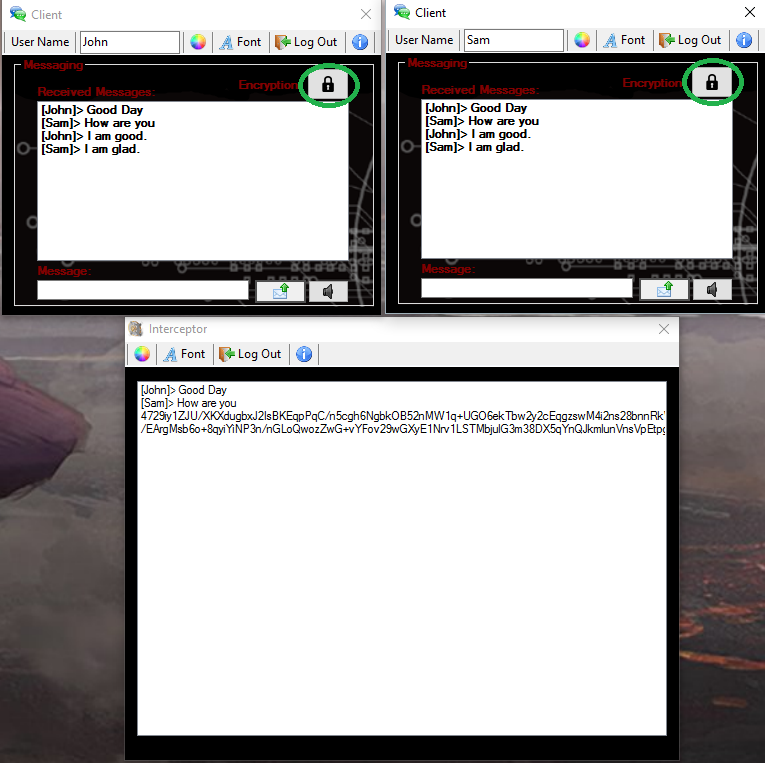
Step 04

Sending messages to other clients can be seen by the interceptor. The interceptor can view both conversation or any conversation that is transmitted.



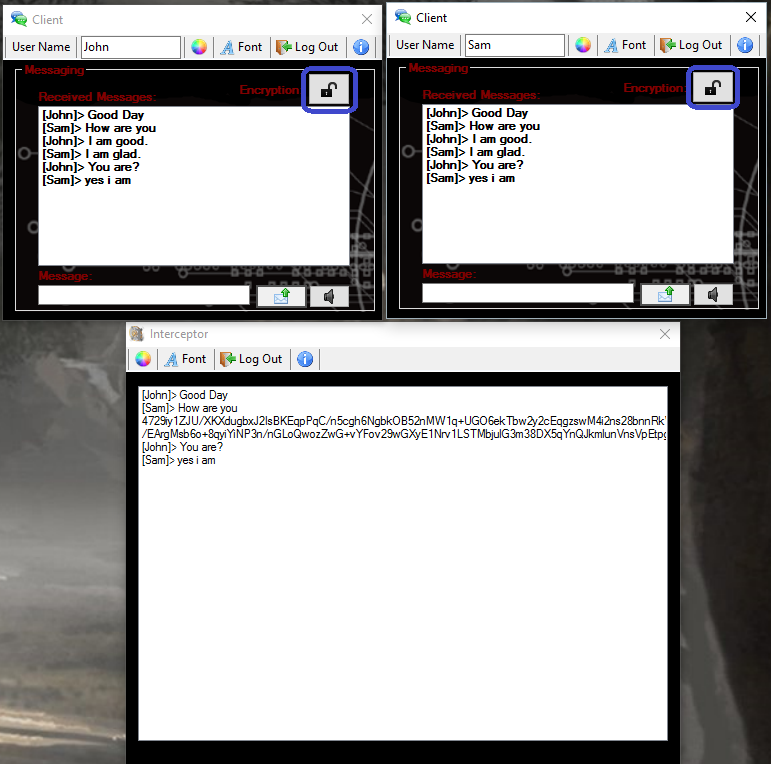
Step 05

Enabling the encryption on both clients allow encrypted messages to be transmitted between clients. The interceptor can only view the encrypted message, therefor can’t ease drop on the conversation.



Step 06

Once the client disables the encryption option, then the interceptor can ease drop and view regular messages that are being transmitted.



Step 07

In any scenario where only one client has data encryption enable, the receiver will get the message in its encryption format.

