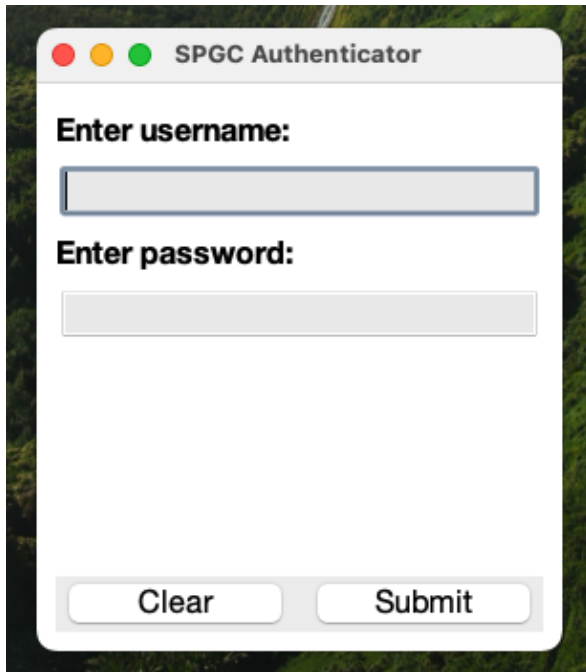Private Group Chat
Preliminary Project Report
COMP 4911 – Computer Networks
Anthony Arseneau

The secure private group chat project is about halfway accomplished. For the networks side of the project, there are three classes named ChatServer.java, ChatClient.java, and ChatClientHandler.java. The ChatClientHandler and ChatServer classes are on the server side of the network. ChatServer is responsible for accepting new connections from clients and ChatClientHandler is responsible for holding a list of connected clients and sharing their sent messages. ChatClient is the program that will be running on the client side of the network. The group chat works in the terminal, but eventually, there will be an intuitive interface.

So far, there is no authentication before getting access to the group chat, the server does not yet hold a list of hashed username and password pairs, and there is no encryption key sharing between the server and clients. Looking at some examples online from previously given resources, encryption with RSA, AES, and SHA-256 seems straightforward. Only simple setups and method calls are needed to use them on strings, which is ideal.

The AuthenticatorView.java class is the GUI (see Figure 1 & Figure 2) for the group chat authentication. In the future, the ChatClient class will retrieve the username and password strings from the GUI, encrypt them, and send them to the server for authentication. If the user is authorized, the AuthenticatorView will disappear, and a new GUI will appear with the group chat.

Figure 1 Secure Private Group Chat Authenticator GUI with empty fields.
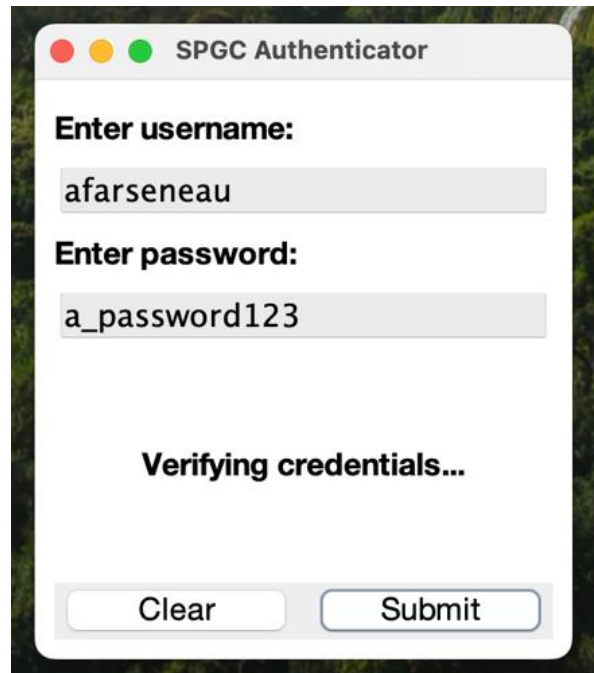
Figure 2 Secure Private Group Chat Authenticator GUI with filled fields. Pressing "Submit" will store the values in variables to eventually be sent to the server. A message appears indicating that things are happening in case of a delay.