

Greg Cernera

Software Development I

Project 2 Proposal

For my semester project, I plan to make a program that creates a secure file and message transfer between two hosts. The project will operate through a graphic user interface so that any user will be able to use it. The project will be created for the intention of establishing a secure connection between two users that wish to keep their exchanges private.

The project will allow for encrypted message sending and encrypted file sharing across hosts for the desire of staying anonymous. My program will be similar to an Internet Relay Chat server in that they both aim to maintain secrecy and anonymity. However, my program will, at the moment, only allow relay between two hosts. I will create a graphic user interface to make the sharing system simple and easy to use. Instead of relaying information through a command line format, I will create an instant messaging system that will be easy to use and navigate. The program will encrypt the message and send it over a secure tunnel to the opposite host, who will then either decrypt it manually or the program will decrypt it automatically.

In addition to sending encrypted messages, my program will allow for file sharing between the two hosts and allow the user to point and click the file they wish to send. I will either encrypt the contents of the file or the file itself, or I will offer the option of either and allow the user to pick. I plan to use the Diffie-Hellman Key Exchange or something similar to ensure a proper file share. For example, if person A wants to exchange a file to person B, person A will encrypt the file and put a key on the file. Person A will share the file to person B, and person B will put their own key on the file, leave person A's key on it, and send it back to person

A. Person A will then receive the file, take their key off, and send it back to person B, allowing person B to take their key off and be able to read the file.

Since I have an interest in encryption and cyber security, I believe that this project will be interesting to me since it will allow for anonymity and secrecy. If I think of any other modifications to this proposal, I will definitely try to implement those ideas into the program. But for right now, I believe that this is a good representation of the project I plan to create.