CYEN 3331

Melvin D. Robinson

March 2, 2021

Project 1

The goals of this project are to use the skills that we have acquired to encrypt, transmit and decrypt a file on two different hosts. We will add network security in a subsequent project.

Procedure

1. Clone the git repository located here: https://github.com/tarequeh/DES
2. Build the executable. You may deviate slightly from the build instructions.
3. Run the executable to create an encryption key.
4. Download this key for safe keeping.
5. Modify the client program to send a text file to the server.
6. Place the encryption key on the server machine.
7. Encrypt the file by running the executable with the encryption key you generated.
8. Send the encrypted file back to the client on the same connection.
9. Decrypt the file and verify that it is the original message.

Preparation

Resurrect your client/server program from COSC 3342.

Be prepared to do a good amount of research for this project. It will stretch you a bit, but it is important to know what to expect.

Refresh yourself on socket programming. This implementation is at your discretion.

Choose an appropriate IP addresses for the client and server, that is place them on the same subnet. Make sure to use a different scheme from the other groups.

Hints(?)

You may find the sendfile() function useful.

For running the encryption function on the server you may want to investigate the system() function. Decryption on the client side need not occur within your client program.

Come up with some naming convention for your encryption keys that include perhaps the date and/or attempt number. This simple tip might save a lot of time and prevent you from encrypting and decrypting with the wrong key.

Be sure to take into account that, particularly when working with the keys, you are using binary files.

Deliverables

Zipped encryption key file, server C file and client C file.

Demonstration