

ESTR4120 (Spring 2018)

Assignment E1: A Secure Multi-Client File Transfer Application

Due on February 26, 2018, 23:59:59

In this assignment, you will extend the *MYFTP* application that you developed in Assignment 1 with a secure socket layer. The new secure MYFTP program should support all functionalities stated in Assignment 1's specification (e.g., multi-threaded send and receive functions). In addition, it also supports the following functions: (i) verification of server certificates (no client certificates are needed) and (ii) the encrypted communication.

Please start with the sample SSL program that we provided. Please generate your own CA and server certificates as described in class for this assignment.

During the demo, please use Wireshark to show that your programs actually transmit server certificates and encrypt the file data.

Submission Guidelines: Please follow the instructions of Assignment 1.