#louis tsui, 998995057, [louis.tsui@mail.utoronto.ca](mailto:louis.tsui@mail.utoronto.ca)

#han wang, 998001638, [hanwang.wang@mail.utoronto.ca](mailto:hanwang.wang@mail.utoronto.ca)

Much of the code was based off of Eric Rescorla’s tutorials as provided on Blackboard.

client

To build upon the sockets already in place, we used SSL, BIO, and CTX objects. The CTX object allowed the client to communicate with SSLv3 and TLSv1 only via SSLv23\_method and SSL\_OP\_NO\_SSLv2 parameter. SSL\_CTX\_set\_cipher\_list set SHA1 as the class of cipher suites to be used. SSL\_get\_verify\_result, the CA\_LIST “ece568ca.pem”, and SSL\_get\_peer\_certificate was used to verify the certificate. Failing a SSL\_connect causes the client to output errors from the BIO. X509\_NAME\_get\_text\_by\_NID, X509\_get\_subject\_name, NID\_commonName, and NID\_pkcs9\_emailAddress was used to extract and check the common name and email from the certificate. SSL\_write sent the secret and SSL\_read got the server response and checked for errors, whether to continue reading, and when the server finished (closed the connection). Upon connection close, the client responds with its own SSL\_shutdown. For cleanup, SSL\_free and SSL\_CTX\_free were used. The buf had to be null terminated at the number of bytes read, otherwise unexpected garbage characters could show up.

server

It is very similar to the client. Notable differences are that there is child spawned for every client connection to try SSL\_accept and output errors from the BIO if it failed. The SSL\_read is done first to react to the client’s SSL\_write and needs to be iterated until the secret has been completely read. The buf that stores the client’s message needs to be null-terminated at len due to possible unexpected garbage characters. Then the server does an SSL\_write to give the answer to the client. The server-side shutdown is a bit different. The first SSL\_shutdown will send a close\_notify to the client, but not look for the client’s. Next, shutdown is called to send a TCP FIN required for certain clients and then server calls SSL\_shutdown a second time.