Networks and Systems Security II - Winter 2022

Sambuddho Chakravarty

March 31, 2022

Assignment 3: TLS 1.2 based echo client/server (total points: 50)

Due date: March 17, 2022.@ 23:59 Hrs. (hard deadline)

This assignment attempts to familiarise you with using TLS functions of the `OpenSSL` library. You need to create an Echo Client/Server program in C that relies on the OpenSSL library to encrypt the traffic. The Echo Client program prompts the user for input. The input could be newline terminated alphanumeric strings. The echo server receives the packets, decrypts them, converts the character to upper case and send it back, encrypted, using the same TLS connection that was initiated by the client (to send the string).

The server could use a self-signed X.509 certificate, for the sake of this assignment, *i.e.* the server creates a fake CA and fake root CA certificate. This fake CA signs the server's own certificate signing request (CSR).

The programs must use `OpenSSL` library's TLSv1.2 methods, *i.e.* you must ensure that TLSv1.2 is being used by the client and the server. Further, only ephemeral DH key exchange, or allied methods must be used for the connection.

Important assumptions:

1. The server uses self signed certificates, signed using a fake CA, whose root certificate must be present on the server as well as the client. The client would use this root CA certificate to validate the server.
2. Both programs could run on the same machine, whereby both use the local host prefixes and subprefixes (127.0.0.0/8) and ephemeral ports. Alternatively, the could be on separate VMs as well.

What you submit/Rubric:

1. Correctly compiled programs (both client and server) (via a Makefile) – 10 points.
2. Correct functioning of all the commands of the program, designed using `OpenSSL`'s TLS library functions – 20 points.
3. Correctly demonstrable TLS handshake (can be shown using `wireshark/tcpdump`), data encryption and transmission, with correct output at the client and server – 15 points.
4. Documentation describing the system design and the assumptions made – 5 points.