Security Engineering - Winter 2017

Sambuddho Chakravarty

April 16, 2017

Lab Assignment 4 (Total points: 50)

Due date: April 17. Time: 23:59 Hrs.

Using OpenSSL Toolkit to Create and Validate Public Key Certificates

The objective of this assignment is to familiarize you with using OpenSSL toolkit to generate public and private keys and certificates.

Part 1

Create your own CA. The CA should have its own root certificate, and public private keys. Similar create client and server keys and certificates which need to be signed using the CA certificates.

Part 2

Using Openssl `s_server` launch a server which listens on a chosen port (Say 12345) and presents the CA signed server certificates to any connection. Use the Openssl `s_client` program to connect to the server and validate the certificate. The `s_client` program would also need to know the CA's certificate.

Part 3

Run the server in client verification mode so that both client and server could authenticate one another. The client should present the client certificate whenever connecting to the server. This helps achieve mutual authentication.

Part 4

Run the `s_server` program with `{www` option so as to emulate a simple HTTPS server. Your browser needs to be configured to connect to the HTTPS server and present the client certificate. When mutual authentication succeeds, the browser screen should display the client certificate validation information.

What to submit in the report:

- Commands used to create the client and server certificates.
- Commands used to run the OpenSSL server (`s_server`).
- Commands used to run the client (`s_client`) to authenticate the server.
- Commands used to run the server (`s_server`) to authenticate the client.
- Commands used to run the server as a webserver.
- Screen-shot showing client connecting to the server and the web page being rendered on client screen.