Project #4 – Secure HTTP Client-Server (subject to revision)

A. Overview

This project extends the NetProbeClient (only in Linux) and NetProbeServer (only in Linux) in Project #2 with two new functions:

HTTP Protocol Processing

To implement basic HTTP protocol processing such that the NetProbe Client can generate HTTP GET request to a HTTP server; and the NetProbe Server can accept and process HTTP GET request to return the requested object (i.e., a file in the file system). Note NetProbeClient/NetProbeServer should also be compatible with standard web servers/browsers.

SSL/TLS Authentication and Secure Communications

To implement: (a) secure communications over SSL/TLS; and (b) authentication of peer using digital certificates. Both are to be implemented using the OpenSSL library. For authentication the client should support authentication using the operating system's trust store as well as self-signed certs in the local directory. The server is to make use of a self-signed cert for authenticating itself. If the self-signed cert is installed into the client then it will allow authentication of the server.

We provide two self-signed HTTPS servers for testing of your client:

https://ierg4180.mclab.org – authentication should fail but hostname verification should succeed.

https://ierg4180x.mclab.org – Both authentication and hostname verification should fail.

To test a positive case just connect to any public HTTPS server, e.g., https://www.google.com. Both authentication and hostname verification should succeed.

B. NetProbeClient Specification

The command line arguments are specified below.

Specification of Command-line Arguments:

NetProbeClient URL <*more parameters, see below*>

URL: The URL (HTTP or HTTPS) to retrieve. Note that if HTTPS is specified then server authentication and secure communications will apply. The URL must support specifying port numbers. We only need to get text files, such as html files, txt files. You do not need to handle binary files such as PDF files, video files, etc.

e.g., http://www.cuhk.edu.hk,

http://www.cuhk.edu.hk/english/admissions/study-in-hong-kong.html,

https://www.google.com

https://ierg4180.mclab.org:443

https://www.ietf.org/rfc/rfc2616.txt

More parameters:

"-file filename" save the received text files (excluded the response header infomation) to the file named 'filename'. (Default: output to stdout)

"-verifyhost name" set the hostname to be "name" such that we can do hostname verification for HTTPS (Default: name would be empty, so you must set it for HTTPS)

Display Output:

If a filename is not specified (without –file option), then the entire HTTP response including the received text file will be displayed to the console (stdout). Otherwise, if a filename is specified (with –file filename option), just display the HTTP response header information (without the received text file) to the console (stdout), and the received text file will be stored into the filename.

After the HTTP/HTTPS transaction is completed, then statistics of the transaction should be displayed, including: (a) response time in ms; (b) bytes transferred (total & file); (c) mean reception throughput (total & file). For example, if the client spends 1000ms to receive a http response with total size 1234 bytes including the header information of size 234 bytes and a text file of size 1000 bytes, then it should display like:

```
Response Time [1000ms] Total [1234B, 1234Bps] File [1000B, 1000Bps]
```

If HTTPS is specified then it should display results for server certificate authentication and hostname validation, e.g.,

```
Retrieved the server's certificate from: cic10.ie.cuhk.edu.hk:4080
Displaying the certificate subject data:
C=HK, ST=HK, O=CUHK, OU=IE-Server, CN=cic10.ie.cuhk.edu.hk/emailAddress=dl013@ie.cuhk.edu.hk
Successfully validated the server's certificate from: cic10.ie.cuhk.edu.hk:4080
Successfully validated the server's hostname matched to: cic10.ie.cuhk.edu.hk
```

Platform:

The client is to be implemented in Linux platform only.

C. NetProbeServer Specification

The command line arguments are specified below.

Specification of Command-line Arguments:

NetProbeServer <*optional parameters, see below*>

> "-stat yyy" set update of statistics display to be once yyy ms. (Default = 500 ms)
>
> "-lhost hostname" hostname to bind to. (Default late binding, i.e., IN_ADDR_ANY)
>
> "-lhttpport portnum" port number to bind to for http connection. (Default "4080")
>
> "-lhttpsport portnum" port number to bind to for https connection. (Default "4081")
>
> "-server model" concurrent server model where model={thread, threadpool} for both HTTP and HTTPS. (Default threadpool)
>
> "-poolsize numthread" If "-server threadpool" is specified, set the pool size to be numthread. (Default = 8)

The two concurrent server models are: (a) thread – a new thread is created for each incoming connection accepted, and destroyed after the connection ends; and (b) threadpool - a preconfigured fixed number of threads are pre-created and assigned to incoming connections. Upon connection completion the thread is returned to the pool rather than destroyed.

Display Output:

If elapsed time since the server began is 120s and currently it handles 10 active http connections and 15 active https connections, then display

```
Elapsed [120s] HTTP Clients [10] HTTPS Clients [15]
```

Platform:

The server is to be implemented in Linux platform only.