CS558 Assignment 3

Due: 11:59pm Nov. 6 (Sunday)

This assignment is done individually. You can use C/C++/Java/Python to work on this assignment.

You will implement a simple secure socket shell (SSH) using the **Secure Socket Layer (SSL)**. SSL is used to establish a secure connection between the server and the client.

Specifications

The SSH server has at least one argument <server_port>, which specifies the port at which the SSH server accepts connection requests. The port number used in this assignment should be a user-defined number (i.e., a number between 1024 and 65535). As multiple teams will be testing their servers, it is possible that multiple teams end up using the same port number. To prevent this, use a unique port number (e.g., the last 4 digits of your B number).

The SSH client has at least two arguments: <server_domain> and <server_port>.

<server_domain> specifies the server's domain name. The domain name is the name of the machine on which the server is running. After you log into remote.cs.binghamton.edu, it will show "remote01:~>", "remote02:~>" etc. If the server runs on remote01, then the domain name of the server is remote01.cs.binghamton.edu. If the server runs on remote02, then the domain name of the server is remote02.cs.binghamton.edu. If you use C/C++, your program needs to convert it to corresponding 32 bit IP address using the **gethostbyname().**
http://retran.com/beej/gethostbynameman.html

<server_port> specifies the port number of the server. You can add other arguments to the client and the server if needed.

For example, if you use C/C++, the SSH server can be invoked as:

./sshserv ***3479***

The SSH client can be invoked as :

./sshcli ***remote01.cs.binghamton.edu 3479***

Upon connecting to the server, the client prints ssh **>**, which allows the user to execute the following commands.

telnet > ls //list files and sub-directories under the current directory

telnet > pwd //print the working directory of the server

telnet > exit // ends the SSH session

If a user enters a command other than the above, then print "Invalid Command".

You need to generate a public key certificate in order to establish the ssl connection. E.g., in C, you can use the following command to generate certificate.

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365
```

If you use java, you can use keytool to generate the certificate.

To compile your C program, please use the following commands:

```
gcc -Wall -w -o sslcli sslcli.c -I/usr/local/ssl/include/ -L/usr/local/ssl/lib -lssl -lcrypto
gcc -Wall -w -o sslserv sslserv.c -I/usr/local/ssl/include/ -L/usr/local/ssl/lib -lssl -lcrypto
```

Important Note

You can use any code available on the web for SSL socket programming. However, you must write your own code for the rest part of the assignment (i.e., ls, pwd, exit). You should also generate the certificate by yourself. When you create a certificate, it will ask you for your name. Please use your name to generate the certificate (other information can be forged).

Grading guideline

- Readme: 4'
- Makefile (C/C++/Java): 8'
- SSL connection (C/C++): 38’
- SSL connection (python): 46
- ls: 25'
- pwd: 20’
- exit: 5'

Submission guideline

- Create a directory with a unique name (e.g. p3-[userid]), which contains the source code, the certificate, and a README file.
- **README** file (text file, please do not submit a .doc file) contains
  - ➢ Your name and email address.
  - ➢ Whether your code was tested on remote.cs.
  - ➢ How to compile and execute your program.
  - ➢ (Optional) Briefly describe your algorithm or anything special about your submission.

-Tar the contents of this directory using the following command.

```
tar –cvf p3-[userid].tar p3-[userid]
```

E.g. tar -cvf p3-pyang.tar p3-pyang/

- Upload the tared file you create above to brightspace.

Academic Honesty:

All students should follow Student Academic Honesty Code (**if you have not already read it, please read it carefully**). All forms of cheating will be treated with utmost seriousness. You may discuss the problems with other students, however, you must write your OWN codes and solutions. Discussing solutions to the problem is NOT acceptable. Copying an assignment from another student or allowing other students to copy your work may lead to an 0 in the assignment or an F in the course. Moss will be used to detect plagiarism in programming assignments. You need ensure that your code and documentation are protected and not accessible to other students. Use **chmod 700** command to change the permissions of your working directories before you start working on the assignments. If you have any questions about whether an act of collaboration may be treated as academic dishonesty, please consult the instructor before you collaborate.