CSCE 664 Wireless and Mobile Systems

Homework 1
(290 points; Submit through canvas.tamu.edu)
Name: RADU STOLERU

You MUST use this latex template for writing your answers to questions that require written answers. You are free to use any Latex editor you wish. A free, friendly version is at overleaf.com. Upload the two latex files provided and you will be ready in a few minutes to edit them and produce a pdf.

1 Operating Systems Review

1.1 Static PIN Code Cracking Library and Test Client [60 points]

In this part of the assignment you will develop a library that implements the concept of REMOTE PROCEDURE CALL. The library is a static library that a client application will use to communicate with a server to crack a 4 digit PIN code. The idea is that the client should not need to worry about any networking: socket creation, communication, etc. The client, simply, invokes a function that returns a value, similar with how a function, executed locally, will return a value. The difference in this part of the assignment is that the function will execute in a server (in another address space, on a different computer). **In this part of the assignment, we are only concerned with up to 4 digit PIN codes, since we will use brute force to recover the PIN.**

To experiment with SHA-1 which is a one way has function frequently used, from a command line you can run the following:

```
$echo -n "hello" | openssl sha1
```

, which will output the sha1 hash of the provided string ("hello" in this case).

1.1.1 Sample Code Provided

Start with the sample code covered in class and attached to this assignment: client.c and server.c that implement a TCP-based client server. Compile the code, run the code, make sure the client and server communicate.

Study the provided sha1test.c which shows how SHA-1 computes the hash for a given string. In order to compile and execute this code you need to have OpenSSL installed in your machine. **You need to find out WHERE OpenSSL is installed on your computer, since you will need the header files and libraries that OpenSSL provides**. In order to compile the sha1test.c code you will need to execute the following:

```
$gcc -I<path to OpenSSL headers> -L<path to OpenSSL libraries> -o sha1test
sha1test.c -lcrypto -lssl
```

1.1.2 What To Do

You need to modify the provided server.c to implement a brute force algorithm that computes the hash value for all integers in the range 0 to 9999. If any of these computed hash values matches the provided hash from the client, the server returns the up to 4 digit pin that hashes to the provided hash from the client. To compile the server code, you will likely need something along the following:

```
$gcc -I<path to OpenSSL headers> -L<path to OpenSSL libraries> -o sha1test
sha1test.c -lcrypto -lssl
```

You need to implement in pincrack.c the communication with the server as. static library. To compile your static library:

```
$gcc -c -o libpincrack.a pincrack.c
```

The IP address and port number can be hardcoded in your library. You should not make the client aware about these, since the whole purpose is to make the client believe the execution is local.

Once the libpincrack.a is obtained, you can compile the test client as follows:

```
$gcc -o pincracktest -L. pincracktest.c -lpincrack
```

One execution of the test client could be:

```
$./pincracktest 356a192b7913b04c54574d18c28d46e6395428ab
PIN found: 1
```

or

```
$./pincracktest aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d
PIN could not be found
```

1.1.3 What to Submit

(a) (40 points) pincrack.c, pincrack.h, libpincrack.a

(b) (20 points) server.c and instructions to compile it

1.2 Dynamic PIN Code Cracking Library and System Calls Inspection [55 points]

In this part of the assignment you will build a dynamic library for PIN cracking and will investigate the system calls made during execution.

1.2.1 What To Do

Using the code developed in Problem 1 of this assignment, build a dynamic library libpincrack.so

Trace the system calls made by your pincracktest client and store the results in a file pincracktest.output. To store the output from strace in a file, you can execute:

```
$strace ./pincracktest <your SHA hash> &> pincracktest.output
```

Please answer the following questions

(a) (5 points) What dynamic libraries is your client loading and where in the file system it finds each library. Write the full path for the dynamic library.
Answer: Write your answer here

(b) (5 points) What is the first system call your client program is making and what arguments are given to that system call?
Answer: Write your answer here

(c) (5 points) Which system call is used for finding out the IP address of the server? Where does the client get the IP address of the server?
Answer: Write your answer here

(d) (15 points) What system calls are made by the client to communicate with the server?
Answer: Write your answer here

(e) (15 points) Which system call takes the longest time? For this, find out the flag needed for strace to write output with microsecond precision.
Answer: Write your answer here

1.2.2 What To Submit

(a) (10 points) libpincrack.so binary for Ubuntu Linux. Specify version of Ubuntu you have used for compiling it

(b) (45 points) Answers to the questions above

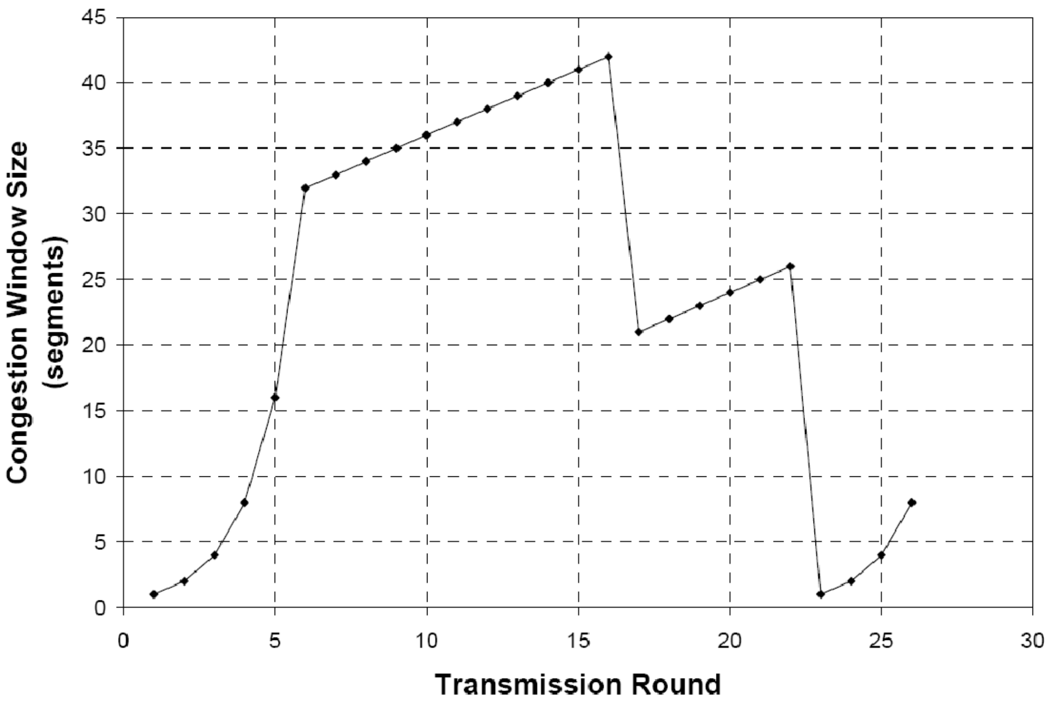
2 Networking Review

2.1 TCP Fundamentals [20 points total, equal weight all questions]

Consider the plot shown below for the TCP window size as a function of time. Assuming the TCP protocol discussed in class is experiencing the behavior shown above, answer the following questions.

(a) Identify the intervals of time when TCP slow start is operating.
Answer: Write your answer here

(b) Identify the intervals of time when TCP congestion avoidance is operating.
Answer: Write your answer here



(c) After the 16th transmission round, is segment loss detected by a triple duplicate ACK or by a timeout?
Answer: Write your answer here

(d) What is the initial value of ssthreshold at the first transmission round?
Answer: Write your answer here

(e) What is the value of ssthreshold at the 18th transmission round?
Answer: Write your answer here

(f) What is the value of ssthreshold at the 24th transmission round?
Answer: Write your answer here

(g) During what transmission round is the 70th segment sent?
Answer: Write your answer here

(h) Assuming a packet loss is detected after the 26th round by the receipt of a triple duplicate ACK, what will be the values of the congestion-window size and of ssthreshold?
Answer: Write your answer here

2.2 TCP with Burty Traffic [10 points]

In our discussion of TCP congestion control we implicitly assumed that the TCP sender always had data to send. Consider now the case that the TCP sender sends a large amount of data and then goes idle (since it has no more data to send) at t1 . TCP remains idle for a relatively long period of time and then wants to send more data at t2. What are the advantages and disadvantages of having TCP use the cwnd and ssthresh values from t1 when starting to send data at t2 ? What alternative would you recommend? Why?

Answer:

Answer: Write your answer here

2.3 TCP Implementation on Your Linux System [30 points]

In this part of the assignment you will investigate tunable TCP parameters of your Linux system.

(a) (5 points) Log on your Linux machine. What command will you run to find the available TCP congestion control protocols in your system? Which congestion control protocols are available on you system? Which command will you run to find the default TCP congestion control protocol on your OS? What is it?
Answer: Write your answer here

(b) (5 points) Inspect all tcp configurable parameters. Are you able to find one that allows TCP's window to be configured in a particular way, after a connection is idle? What is that kernel parameter? How is it set in your system?
Answer: Write your answer here

(c) (20 points) Inspect the tcp configurable net.ipv4.tcp_sack in your system. What value is it set to? How does the SACK in TCP work? You will need to do additional reading (besides lecture notes) to answer this question.
Answer: Write your answer here

3 Wireshark

3.1 Wireshark Lab (70 points)

Study the provided "Wireshark Lab: Getting Started v8.0" and "Wireshark Lab: TCP v8.0". Please answer the questions asked in the TCP lab.

1. (5 points) Answer:
   Answer: Write your answer here

2. (5 points) Answer:
   Answer: Write your answer here

3. (5 points) Answer:
   Answer: Write your answer here

4. (5 points) Answer:
   Answer: Write your answer here

5. (5 points) Answer:
   Answer: Write your answer here

6. (5 points) Answer:
   Answer: Write your answer here

7. (5 points) Answer:
   Answer: Write your answer here

8. (5 points) Answer:
   Answer: Write your answer here

9. (5 points) Answer:
   Answer: Write your answer here

10. (5 points) Answer:
    Answer: Write your answer here

11. (5 points) Answer:
    Answer: Write your answer here

12. (5 points) Answer:
    Answer: Write your answer here

13. (10 points) Answer:
    Answer: Write your answer here

14. (10 points) Answer:
    Answer: Write your answer here

3.2 Wireshark in Action (25 points)

In this part of the assignment you will use the acquired knowledge about Wireshark to understand networking you worked on at the beginning of the assignment.

For this, run Wireshark on an interface on which the client.c and server.c (code provided) communicate. One suggestion is to use the local loopback interface (lo0 or similar) and identify the sender and receiver packers based on the port number user. You know that the server listens to port 3005.

Please answer the following questions.

1. (5 points) What are the TSval and TSecr values in the TCP header? Are they the same? Why? When would they be different?
   Answer: Write your answer here

2. (5 points) The client sends a TCP packet that has two options: PSH and ACK. What is the PSH option for?
   Answer: Write your answer here

3. (5 points) When the server sends the ACK to the client for the receipt of the packet, what is the ACK value? Why is that value?
   Answer: Write your answer here

4. (10 points) What are the last two packets exchanged when the client terminates? The same question for when you shutdown the server through CTRL-C. Explain the Seq and ACK values in these last 4 packets. Answer:
   Answer: Write your answer here

4 Submission Instructions

Please submit the PDF as obtained from the provided latex template. Name your submission as ⟨your lastname⟩.hw1.pdf and submit it on canvas.tamu.edu. Also, please submit all source code as a single zip or tar file.