Lab 10: TCP Basics
OSL, Thu April 9, 2015

Objective:

1. Learn how to intrepret a TCP trace and in the process understand its operation.

General instructions:

1. This lab is to be done in **groups of two students.**
2. As you proceed with the lab instructions below, note down observations or relevant output from whatever you do in a file named “rollno1-rollno2-lab10.txt”.
3. If you wish to upload a file on moodle for tracing purposes, use the playarea. But for lab submission, use the lab submission link.

Reference:

1. TCP slides on bodhitree1.cse.iitb.ac.in

Lab Instructions:

Mr. Tea See Pea spent considerable amount of time going through TCP theory and now wants to see it in action. To his horror he is now told that theory can differ considerably from practice. Help him come to grips with this reality by helping him 1) conduct the experiment, 2) interpret the trace and 3) answering the questions he has.

Guidance:

1. You basically need to upload a file to monitor TCP sender side behavior. “scp”, “google-drive uploads” etc come with lot of security related stuff which can distract. While you can give them a shot (in fact you should to see the difference), it will be cleaner if you upload a file to moodle and trace the flow.
2. For a cleaner trace, don't start tcpdump until you get to the point where you just have to click the upload button on moodle.
3. Examine the trace. In wireshark, you can play around with “Statistics”. Under Statistics: summary, conversations, HTTP and TCP stream are a few options to check out.
4. Before answering the questions, you should do a bit of further clean up. For this, in wireshark, select what you think is a packet belonging to your file upload (upload a reasonably large file like 1MB and you will know what packets belong to this upload). Right click and select “follow TCP stream”. This isolates all packets belonging to this TCP connection. Focus on this connection hence forth.
5. As mentioned some of the behavior you will see is very different from what was covered in class. Feel free to browse around to understand the reasons for such a behavior.
6. For question-9 below, it easier to just save the summary (that shows on the wireshark screen) to a file and run a script over it to get the relevant values. For this, select “File-> Export-packet-dissections -> as plain text file”.

Questions:

1. Why is TCP religious (hint: biblical significance related to Adam/Eve)? And why is TCP more welcome than UDP? (these are for fun ;-)
2. Identify the famous 3-way handshake. What is the 4 tuple associated with this TCP

connection? And what was the initial sequence number chosen in either direction?

3. What HTTP request message has been carried in this TCP connection? How did you find it?
4. What is the initial window size? How did you determine this?
5. What is peculiar about the way acks are generated? And why do you think they are generated this way?
6. What is the maximum and minimum size of TCP segments encountered in this connection?
7. What is the received window size of this TCP connection (from the perspective of sender of file)? How did you figure it out? There is something peculiar here as well. What is it and why does it happen so?
8. Who initiated closing of the connection? How did you determine this?
9. Calculate the TCP throughput achieved by this connection.
10. Plot outstanding data (data in the pipe) over time.
    1. Can you seperate out the slow start and congestion avoidance phase? Why or why not?
    2. What is in action in this trace: congestion or flow control? Explain.

Homework: The below will not be graded. This is just for kicks.

Now that you know how to examine TCP traces, you could try capturing traces when using google drive or scp and compare/contrast the differences.

Submission instructions

Submit the file “rollno1-rollno2-lab10.txt” via moodle for grading.