COSC 7370 Assignments

[1] Install WireShark on your machine and test it with some HTTP traffic before working on this assignment. Run a SSH client and connect to a Unix/Linux machine and issue a few Unix commands. It does not matter which machine you connect to. You can use a machine at UH or outside UH (preferred). You should collect all packets (both packet for the protocols and the contents) collected at your computer. Write a report to identify what the packet is for.

Due: October 10, 2016.

[2] In Chapter 6, the paper presented a distance function (δ) between two thumbprints. We did not look into the analysis because it is more complicated than necessary. I sort of defined my own δ function using “counts” thumbprint as an example. Please propose one for the “Frequency” thumbprint. No need to prove anything, but justify why the distance function works well. You may make up some examples to explain.

Due: October 17, 2016

[3] In Chapter 7, the paper used a quan(E,2α) to determine if the chain is too long. There is no justification of why that works other than some experiments. Can you come up with another way to do it?

Due: October 24, 2016

[4] Stepping-Stone Detection. You are given three incoming packet streams and three outgoing packet streams (see page 41 of Lecture 14 for example) of an intermediate node of a chain. Your job is to find all pairs "attack pairs" in this data set. You may use methods from any source (please cite all sources used) except using source code from someone else. You can design your own algorithm too. You have to provide the code and a report to support your conclusion. Simply saying the first IN stream and the first OUT stream forms an attack pair is NOT enough.

Each data stream contains 128 time stamps representing 128 packets collected at the node.

Due: Last day of class (November 30th)