6397 Homework 3

Network Intrusion Detection

This homework is based on “Correlating Temporal Thumbprints” (Ch. 13) and related work. You should implement a variation of the algorithm mentioned in the slides. The primary work is a function to compare similarity of two series of time stamps. You can make changes to the algorithm. In fact, you are asked to use only one threshold value instead of two.

You will be provided with a spreadsheet (“Correlation Data.xlsx”) containing actual data collected from prior experiments. There are two tabs in the spreadsheet. “Part 1” contains 10 incoming connections (only the timestamps) and “Part 2” contains 10 outgoing connections. You job is to detect which input and output pair forms a stepping-stone pair. You may have to do some experiment to determine the threshold value. The selection of threshold value can be determined similar to “A Grid-based clustering” paper in Ch. 12.

Write a report to discuss the experience.