Outlier Detection in Temporal Network Data

Kyle Boyer and Erik J. Sturcke

Abstract—We propose using a chord diagram to visualize temporally varying network traffic so that a network security analyst can detect anomalies in the traffic. The visualization will visually represent network traffic via the chords of the diagram and the ability to encode attributes visually around the perimeter of the circle. This will provide both high level situational awareness of traffic with the ability to see details for specific traffic once an anomaly has been detected.

Index Terms—Information visualization, network security, intrusion detection, anomaly detection

INTRODUCTION

Organizations typically monitor internal network traffic for threats, many of which can automatically be detected and often even mitigated with the help of tools and network appliances like firewalls and intrusion prevention systems (IPS). Often these organizations will also have analysts dedicated to determining if further investigation and mitigation should take place for detected threats. Analyst may also look for threats not automatically detected, incorrectly detected or only detected in part. Because of the volume of traffic on the network, analysts can only consider a small fraction of the traffic in any detail. Automatically detected threats can often be assigned a severity to prioritize what analysts should look at first. For novel threats, however, there's a greater burden on analysts to find suspect traffic. Visually encoding network traffic might give analysts the ability to detect certain anomalous patterns and help guide further analysis.

1 RESEARCH QUESTION

Network traffic is both temporal and network (graph) data. It's important to note here that we are not considering network topology, but temporally varying graphs of hosts that are communicating with each other. Our primary area of investigation is how vis can enhance anomaly detection and evaluation of this kind of temporal graph data.

2 PRELIMINARY HYPOTHESIS

We propose that using a chord diagram and the ability for an analyst to choose visual encoding of attributes around the perimeter of the circle, certain anomalous traffic will be able to be visually detected.

3 IMPLEMENTATION DETAILS

We will be using VAST 2013 Mini-Challenge 3 data sets. The UI will be browser based, written in JavaScript and use D3.js to draw the vis. For the initial implementation, the data will be pre-processed to bring it to a size small enough to be used by the browser in whole and run on a laptop with 16GB of memory. The initial version will target the current version of Chrome, but should work in all modern browsers.

4 EVALUATION

The data is known to contain denial of service attempts (DoS), port scans, but most importantly exfiltration of several large files via FTP[1]. To keep this project within the scope of a half semester project, we will present our visualization to 1–2 people familiar with network security and see if they are able to detect the data exfiltration. This will be an informal evaluation with no metrics.

5 POTENTIAL CONTRIBUTION

We hope to demonstrate that visual anomaly detection is viable for temporal graph data sets and that in particular, the vis tool that we develop would aid network security analyst in detecting and evaluating anomalous behaviour on an internal network.

REFERENCES

[1] Whiting, M., et al. "VAST Challenge 2013: Situation Awareness and Prospective Analysis." *Visual Analytics Science and Technology, 2013 IEEE Conference on*. 2013.

• *Kyle Boyer and Erik J. Sturcke are with University of Maryland, Baltimore County, e-mail: {kyleboy1,sturcke1}@umbc.edu.*