NetVis: A network traffic visualization tool

SUBMISSION ID
AFFILIATION ID

May 19, 2013

Abstract

Computer network traffic visualizations attempts to deliver improved understanding of traffic on a network to an observer. Many existing tools opt for graph or plot-based visualizations to detect patterns or outliers in the data, but still largely provide a segmented view of any data feed. In this paper, we present a novel network traffic visualization framework that makes use of a variety of complementary visualizations to obtain better situational awareness. Our proposed solution is to look at different..

1 Introduction

2 Related Work

JH

3 NetVis Architecture

Describe the architecture, how traffic is read and processed, the format of the CSV, why was it designed the way it is? Add diagram How real-time is it? What filtering do you support + protocols? How modular is the code base, can one simply script in another vis?

4 NetVis Visualizations

4.1 GUI

4.2 Attribute Distribution

4.3 Dataflow

Port scan attack example?

4.4 Spinning Cube

The spinning cube is an implementation of an existing visualization tool known as the spinning cube of potential doom [**?**].

4.5 Traffic Volume

4.6 Heat Map

4.7 Activity Groups

5 Discussion

Why were the five vis picked? how do they complement each other?

5.1 User Workflow

Describe a typical workflow of an analyst, include a workflow diagram (e.g. UML or CONOPS (concept of operations, see))

Describe how the visualisations complement each other

Describe how many alerts it can process at any time and accumulative.

5.2 Advantages

Complementarity Dynamic Filtering Real Time Can be used as a learning tool

5.3 Limitations

Doesn't use all data

5.4 Future Work

More advanced data processing Machine Learning Save current configuration and have access to sensible filter packages

6 Conclusion

In this paper we have presented..