2015 European Intelligence and Security Informatics Conference

Interactive Visualization of Netflow Traffic

Thomas C. Eskridge, Marco Carvalho, Fitzroy Nembhard, Hari Thotempudi
Harris Institute for Assured Information
Florida Institute of Technology
Melbourne, FL 39201
teskridge,mcarvalho@fit.edu

Peter J Polack, Jr.
Georgia Institute of Technology
Atlanta, GA
petepolack@gmail.com

***Abstract*—We introduce a novel tool for visualizing netflow traffic on enterprise networks called 3D Parallel Coordinate Planes (3DPCP). This tool provides operators with the ability to manipulate the visual flow of network traffic information by arranging two-dimensional planes along a vertical time axis in 3D space.**

Keywords—Parallel Coordinate, 3D Visualization, Mission

I. Introduction to the 3DPCP Concept

A key problem in computer network defense is understanding the current state of the network, including what attacks are happening, what impacts the attack will have on current and future mission plans, if and how the attacks are changing, and what options are available to improve the situation [1]. The 3D Parallel Coordinate Planes (3DPCP) enables operators to construct a visual representation of the activity on their networks, to explore hypotheses about threat behavior, and to understand how current network activities affect currently active and planned missions. The basic structure of the 3DPCP is shown in Fig. 1.

Like traditional parallel coordinate plots [2], 3DPCP displays and organizes all data through several feature dimensions, in this case two-dimensional planes. Each plane represents a 2D relationship of the incoming data (e.g., packet size or source IP), and is also a node in a decision tree representing the underlying dependencies. Each particle is a netflow record. Fig. 1 shows the graphical implementation on the left side, and the decision tree representation that underlays the graphical representation and controls the movement of particles in the visualization.

3DPCP creates a visual structure that amplifies the differences between malicious and legitimate traffic, and by manipulating the criteria for the split the investigator can configure the display to answer a number of important questions about the data. Particularly useful configurations of planes and filters may be stored for reuse, sharing with colleagues, or used in briefings to present the results of an investigation.

We are beginning evaluations of 3DPCP and current development is focused on plane definition, representation of dependency structure between planes, user interaction and scaling to larger data sets.

Acknowledgment

This research project is sponsored by the U.S. Department of Defense. Any opinions, findings and conclusions or recommendations presented in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

References

[1] Kott, A., C. Wang and R. F. Erbacher, Eds. (2015). *Cyber Defense and Situational Awareness.* Springer.

[2] Inselberg, A. (2009). *Parallel Coordinates: Visual multidimensional geometry and its applications*, Springer.

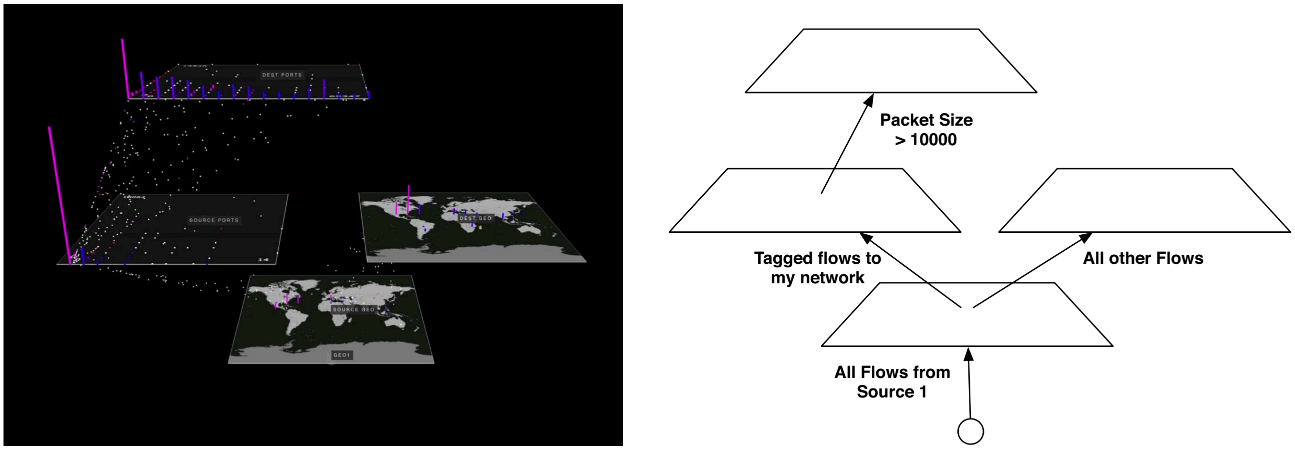

Fig. 1. The 3D Parallel Coordinate Planes. Shown on the left is the current implementation, and on the right is the filters implemented in the 3DPCP.

978-1-4799-8657-6/15 $31.00 © 2015 IEEE
DOI 10.1109/EISIC.2015.51