PathScanUI: A Web Application for Viewing and Analyzing Anomalous Network Activity (Or Any Graph Data Really)

[Extended Abstract]

ABSTRACT
PathScanUI is a browser-based application that was developed to view and analyze network graph data generated by PathScan, a system for detecting multi-hop anomalies created by adversary traversal of networks. Although it is primarily used for analyzing IP traffic, PathScanUI can be used to view virtually any type of graph data and can be integrated with other tools and data sources. It is a powerful and robust tool for searching, filtering, combining, visualizing and exploring graphs to aid analysts in discovery of interesting information in their data.

Categories and Subject Descriptors
Human-centered computing [Visualization]: Visualization systems and tools—Visualization toolkits.

Keywords
PathScan, anomaly, detection, graph, visualization, analysis, interface

1. INTRODUCTION
Quickly detecting, analyzing, and responding to network intrusions is a critical task in the current cyber threat landscape. Ever-increasing network flows mean more data must be analyzed. Better detection algorithms are needed to reduce the amount of data processed by a human analyst, and better visualization tools are needed to help analysts quickly process that data. In this work, we present PathScanUI, a web application developed as a user interface to anomalous multi-hop network traffic generated by the PathScan system. It has since been developed to visualize and analyze virtually any graph data using only a modern web browser.

2. FEATURES
PathScanUI was created to address several requirements we could not find in any other single graph analysis tool:

Figure 1: PathScanUI helps analysts quickly identify network anomalies and highlight relevant data.

1. Interface quality Data is presented in multiple, interactive, and intuitive views to help analysts extract useful information from graph data.

2. Dynamic graph support Graphs can be manipulated, aggregated, and visualized on demand. A force-directed layout algorithm optimizes graph viewability.

3. Flexibility Use it standalone or connect to other applications and data sources. It is supported on any platform with a modern web browser. Future development includes support for more data formats and popular data analysis tools (e.g., Splunk).

4. Scalability Dynamically render graphs containing several thousand nodes and edges on commodity desktop and laptop hardware.

5. Collaboration Graphs can be shared with other analysts. Other collaborative features are a focus of future work.