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

James Wernicke, Joshua Neil, and Curtis Hash
Los Alamos National Laboratory

VizSec 2013

Purpose

PathScanUI was developed to address the need for:

- A tool specialized for cyber security analysts
- Interacting with visualizations
- Highlighting interesting traffic
- Attaching to other tools and data sources
- Searching, filtering, combining, visualizing and exploring network data
- Supporting any type of network data

Goals

Interactivity

Color, hide, hover and click graph elements to highlight and get more details.

Multi-Dimensional Viewing

Switch seamlessly between time, anomaly, host, and path-centric views of network flows.

Data Aggregation

Combine data sets into a single graph.

Scalability

Visualize complex graphs on-demand even on commodity hardware.

Platform Independence

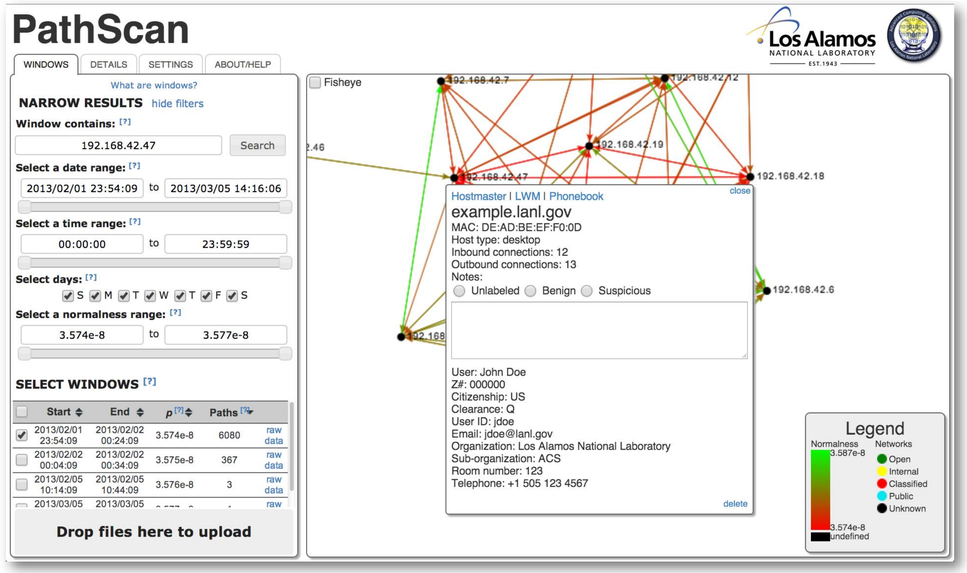
Useable on any device with a modern HTML5-capable browser.

Collaboration

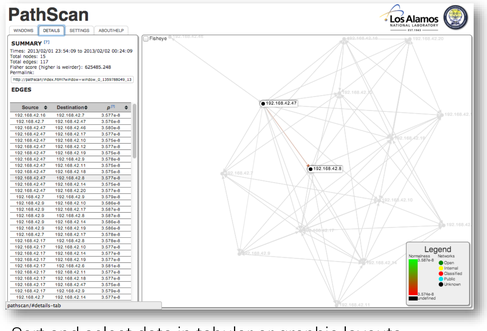
Share interesting findings via hyperlinks.

Data Import/Export

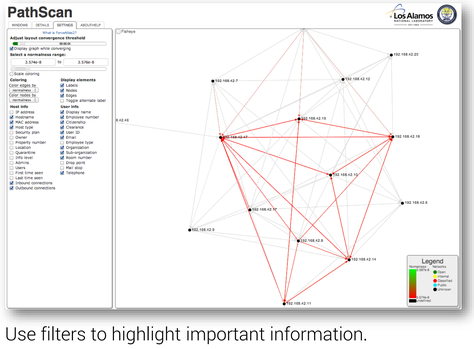
Visualize any type of network data, pull data from other data sources, and export data to other tools.



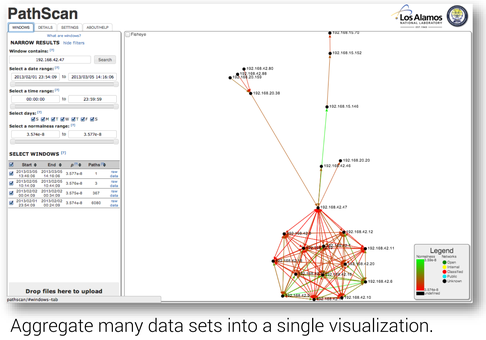
Graphs are highly interactive and allow most exploration with simple point-and-click actions. Hover over an element to highlight neighbors. Click an element to view more details about it, hide it, or pass it to external tools.



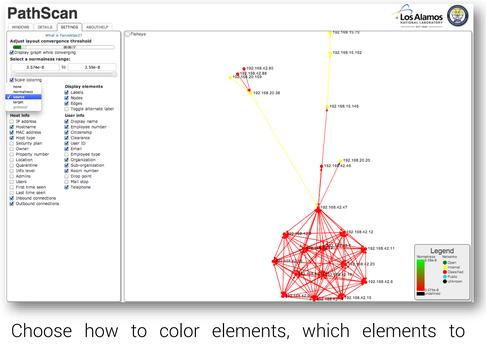
Sort and select data in tabular or graphic layouts.



Use filters to highlight important information.



Aggregate many data sets into a single visualization.



Choose how to color elements, which elements to display, and which details to display about them.

Evaluation

Based on the responses from LANL cyber security analysts, PathScanUI can improve analysis, discovery, and response, but the UI needs some work.

Productivity

	Disagree — Agree
Increases threats discovered	★★★★☆
Increases responses to threats	★★★★☆
Increases number of anomalies analyzed	★★★★☆
Decreases analysis time	★★★★☆

User Experience

User interface intuitiveness	★★★☆☆
User interface responsiveness	★★★★½
Visualization interactivity	★★★★½
Visualization readability	★★★★½

Future Work

Data Support

Tables, search filters, and other visualization controls dynamically change based on the type of network data.

Collaboration

Share complete “cases” with their own instances of windows including related notes, findings, and configurations.

Integration

Interfaces to allow sending and receiving data to and from more external tools.