Dynamic Visualization of Network Traffic for Situation Awareness in Computer Security

Kaitlyn DeValk and Niklas Elmqvist
{ksdevalk, elm}@umd.edu, University of Maryland

Riverside

WEB01

198.57.218.14

WS02

WS03

FILE01

WEB01

Created At	2022-08-29T21:44:37.057452Z
Updated At	2022-08-29T21:44:37.057452Z
Hostname	WEB01
Operating System	linux
Architecture	amd64

Known IP Addresses

1. 127.0.0.1
2. 10.10.10.108

Motivation

Visualizations are increasingly being used to help with network security, but the needs of users are often not considered, leading to many of these tools never being used operationally. To understand this problem domain, we conducted 24 interviews and developed Riverside, a user-centered network security visualization tool.

Interviews

Interviews were conducted with 24 network and security professionals centered around their current tooling, professional practices, and experiences with network visualizations. Some participants created sketches of visualization layouts, providing concrete examples for my tool design. We performed qualitative coding and thematic analysis to distill themes and specific visualization features that participants desired in a network visualization tool.

Riverside Visualization

Riverside uses animated node-link diagrams to display network traffic over time. Users can customize aspects of the layout as seen on the poster and navigate the timeline (blue cursor) or observe their network in real-time (red cursor). Nodes can be dragged to change the layout, and Riverside uses an infinite canvas that can be dragged or zoomed to change the user's view.

Future Work

We plan to evaluate Riverside with a user study and incorporate feedback from those trials, as well as continue to add features mentioned from the interviews.

Change Shape

Change Label

Lateral Movement #1

Theme Colors

Standard Colors

Web Colors History

#f2dcdb #f2dcdb

Cancel

FTP: 10.10.10.101:21 ⟷ 10.10.10.104:46954

Start Time Mon Aug 29 2022 17:47:20 GMT-0400 (Eastern Daylight Time)

End Time Mon Aug 29 2022 17:47:33 GMT-0400 (Eastern Daylight Time)

Throughput 14

08/29/2022, 05:45:30 PM

50 0 10 20 30 40 50 0 10

29 August 17:45 29 August 17:46