Hall Monitor:
An interactive visualization to monitor “who goes where” on the network

Cody Fulcher and Diane Staheli

MIT Lincoln Laboratory

Keywords: Visualization, Cyber security, interaction, netflow.

1 Introduction

Visual and interaction metaphors for cyber security either draw from a pool of general visualization techniques or borrow from other domains to adapt them to cyber-specific data and use cases. We ask the question: do these existing metaphors best serve the needs of the cyber domain, or do we need to design visualizations using fundamentally different visualization techniques? We present a design study to explore new visualization and interaction metaphors based on needs specific to cyber security analysts, and describe “Hall Monitor”, a novel interactive visualization.

The Hall Monitor interactive visualization builds upon and re-imagines existing visualization techniques, and was inspired by the needs of cyber security analysts, which have been well-documented in research. The key challenge specifically addressed in this design study is: understanding the cadence of the network [2]. The initial concept was to create a tool to answer the questions:

- Who is talking to our network?
- Who on our network is responding?
- What is the regular cadence of these communications?
- How do these communication patterns change over time?

To answer these questions, we present the Hall Monitor metaphor. In elementary schools, the hall monitor is a person who patrols the halls during class time and checks to make sure any people in the halls are going to the right places. Similarly, Hall Monitor is a tool to allow analysts to ensure the traffic on their networks is coming from and going to the appropriate entities.

In the following sections, we discuss the inspiration for the Hall Monitor, describe the visualization and interactions, and discuss future work.

2 Design Inspiration

The primary inspiration for the visual metaphor came from a static visualization created by Team Cymru, a non-profit US based internet security organization, called the Map of Internet Malicious Activity [1]. This visualization compresses an entire logical grouping of IP addresses into a single box, in both cases this resulted in a single box representing an entire /8 subnet.

The Internet Malicious Activity Map compresses IP addresses into a high-level overview of how the malicious activity is distributed over the Internet, providing a quick overview of where the network traffic is coming from. However, this static visualization technique limits the ability to refine analytic insights or data exploration. Each pixel in the map represents 4096 IP addresses, meaning that the most fine-grained detail available is still far too broad to be useful. Furthermore, the Team Cymru Map only visualizes traffic in one direction; this effectively cuts out half of the conversation. The Hall Monitor seeks to build upon the strengths of this visualization technique, incorporate network traffic from both directions, and extend the interactive capability.

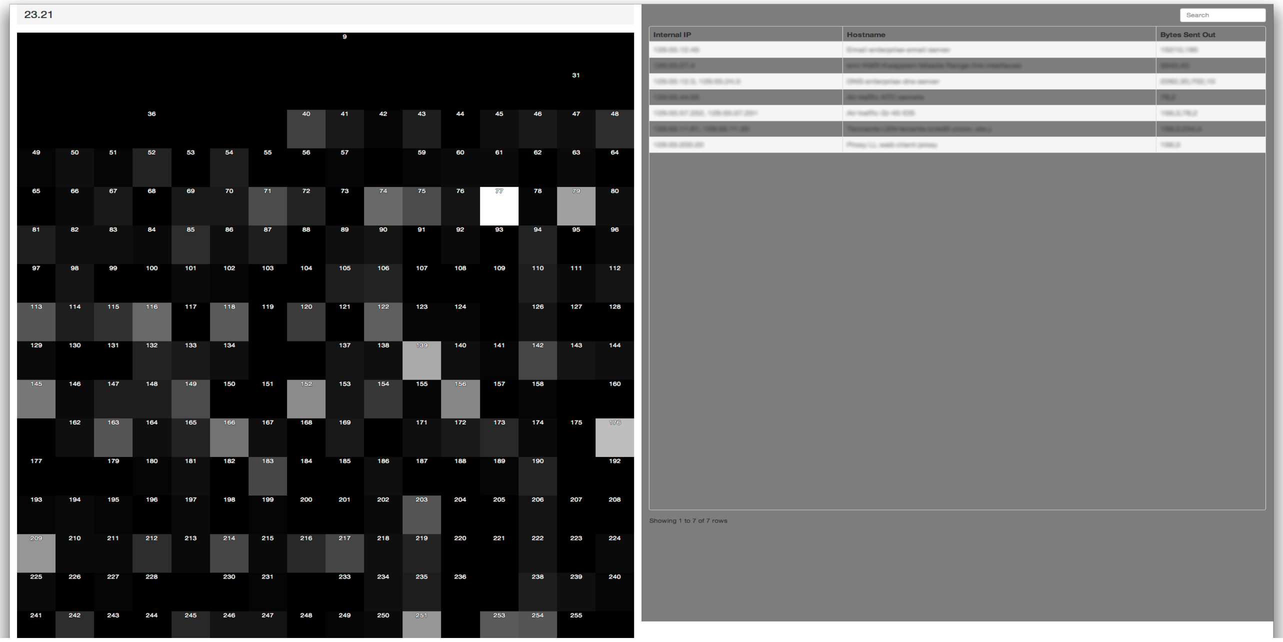
3 Hall Monitor Visualization

The visualization is divided into two linked views (see Figure 1), each occupying half the screen. The left side contains a grid-based visualization of the external IP addresses found in incoming network traffic, and the right side contains a tabular view representing the internal addresses that responded. Traffic sent to non-existent internal hosts is excluded from the visualization.

Grid View: The left section visualizes the traffic coming into the network as a grid of boxes, with each box aggregating one subnet; on page load each box represents one /8. (For example, the box marked 23 in the corner represents an aggregation of all traffic from 23.0.0.0/8.) Each box can be clicked to zoom into a given subnet. (For example, clicking box marked 23 will change the top-level aggregation to represent all traffic from 23.0.0.0/8 as depicted in Figure 1; at this level, the box marked 21 will now represent an aggregation of traffic from 23.21.0.0/16.) This aggregation condenses up to 16 million IP addresses into a single box, while still allowing analysts to drill down to the level of a single IP address with 3 clicks.

The visualization can aggregate either the number of unique connections from that IP range, or the number of bytes of packet payloads sent. This data is encoded in the color of the box as a range from white to black; an entirely black box (devoid of even it’s number) means no traffic at all was received from that subnet, and a bright white box means that traffic was high, relative to the other subnets shown.

Tabular View: The right side of the screen contains a tabular view listing the IP addresses on the network that communicated with the subnets represented on the left side of the screen, the number of payload bytes sent or unique connections, plus any additional enrichment that can be provided (in this case, host name for the internal IP address is displayed). The tabular view allows analysts to quickly triage network activity based on the size and distribution of responses.



Internal IP	Hostname	Bytes Sent Out
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Showing 1 to 7 of 7 rows

Figure 1: Hall Monitor. In this example the subnet 23.21.0.0/24 is selected

4 Discussion

The Hall Monitor visualization improves upon the Team Cymru map in several key ways.

High-Level Aggregation: Hall Monitor uses each box to represent an aggregation of all the traffic from a single subnet, as opposed to dots within a box representing much smaller groupings. This design choice was made to better highlight "one-to-many" traffic (traffic coming from one external IP to many internal hosts).

Interactivity: Hall Monitor allows analysts to interact with the data and narrow down the results, going from an aggregation of an entire /8 to showing single hosts in 3 clicks. While the Team Cymru map effectively shows traffic across the entire Internet, seeing where the traffic is coming from within a single /8 is challenging. By allowing users to zoom into a /8 and see the subnets within it, we allow users to obtain details on demand.

Visual Representation: The Hall Monitor grid visualization appears to have elements in common with a traditional treemap. The distinction between the Hall Monitor's grid and a tree map is that size and location of the boxes in the grid are always constant; in a treemap one or both of these factors would be variable based on chosen data parameters. Visual consistency is important because it allows the grid to function as a map; the box for a given subnet will always be in the same location. This consistency helps analysts detect changes in the cadence of the network [2] by showing the visual changes in predictable ways. If a box for a given subnet is normally grey and suddenly becomes bright white, an analyst can quickly identify this change and recognize that it does not fit within the expected behavior of their network.

5 Future Work

The prototype of this tool highlights several potential avenues for further investigation.

User Evaluation: The current prototype was created in a laboratory environment, and evaluated solely based on developer critique. The visualization and interactions would benefit from more formal user testing for validation.

Grid Metaphor: The grid-based interaction can easily be adapted into any tool and used as a filtering mechanism. Currently, the filters are based on subnet and the groupings are all logical, but future adaptions could be grouped in a different manner. The benefit of this metaphor is that it serves dual purposes; in addition to serving as a navigation device, the grid also conveys information to analysts.

Adaptable Data Sources: Future iterations could incorporate additional data sources into the tabular view. The data displayed in the tabular view could dynamically change based on the selected zoom level. As an example of this adaptable level of detail: in the /8 level the tabular view might only display high-level traffic metadata, but in the /24 view, more fine-grained host information such as IDS alerts could be shown.

Tangible Interactions: The grid system could allow an analyst to filter through IP addresses, using a grid-based input device as an alternative to a keyboard. Adapting the grid to a tangible interface or touch screen display would take advantage of human muscle memory and potentially allow analysts to filter their data faster and easier.

6 Conclusion

We have presented Hall Monitor, a novel concept for interactive cyber security visualization. We discuss ways in which these new visual and interaction metaphors improve upon currently established practices, and discuss future research directions for this work.

7 Acknowledgements

This work is sponsored by the Assistant Secretary of Defense for Research and Engineering under Air Force Contract #FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.

8 References

[1] Team Cymru Research NFP. (Retrieved September 2015) *Internet Malicious Activity Maps* [Online]. Available: http://www.team-cymru.org/malicious-activity-maps.html.

[2] Best, Daniel M., Alex Endert, and Daniel Kidwell. "7 key challenges for visualization in cyber network defense." In *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*, pp. 33-40. ACM, 2014.