Designing STAR: A Cyber Dashboard Prototype

Sean McKenna
University of Utah & MIT Lincoln Laboratory
Salt Lake City, UT | sean@cs.utah.edu

Keywords

Visualization, cybersecurity, storytelling, interaction, treemap

1. INTRODUCTION

A central challenge for a strong cyber defense is the appropriate communication of cyber information. There are many key stakeholders that make decisions and convey information up to different levels of authority, and this information may not always be in sync. Additionally, cyber analysts know and often utilize technical jargon to pass along information, and these analysts can spend significant time and effort to building their own visualizations manually, such as network summaries, patterns, and recent attacks. To aid communication, we have developed a working prototype of a cyber dashboard which visualizes a simplified view of a network, particularly the key external players which are extracted from both IDS alerts and reports from a traffic analyst. This prototype is one step towards enabling analysts to simplify and encode information into a visualization that can help tell the story of a cyber attack or a network's current defense status.

2. DESIGN PROCESS

To build the novel cyber dashboard presented in Figure 1, we conducted a user-centered design process. A prevalent challenge in the field of cybersecurity is access to end users [3, 4]. We involved various stakeholders through interviews and informal evaluations, and we strived to keep our design grounded to users through personas. Our design process was largely based off of a design activity framework [2], which characterizes design into different activities: understand, ideate, make and deploy, with evaluation throughout.

We started off the design process by conducting a literature review, an existing tool analysis, and a series of interviews with over a dozen different stakeholders. Through this *understand* activity, we were able to generate specific user needs, tool requirements, and a broad range of different design opportunities for the dashboard. After identifying key design opportunities, we proceeded to *ideate*, where different design ideas were tested and evaluated against these criteria in order to pinpoint the most impactful visualization idea. Lastly, we concluded the project in the *make* activity where we crafted several design mockups and implemented them as a fully interactive prototype with real data. This project is still ongoing, so it has not been deployed yet.

Poster Presentation
VizSec '14, November 10 2014, Paris, France
.

3. DESIGN ARTIFACTS

We created several design artifacts which influenced the design of our prototype, specifically personas and scenarios. The use of personas for cybersecurity visualization design was originally showcased by Stoll *et al.* [4]. We established four kinds of personas for the communication of cyber information: cyber analyst, network operations center (NOC) manager, director of IT, and a CEO. For each persona shown in Figure 2, we identified their high-level goal, general knowledge, focus for cyber SA, and key questions for cyber SA. These key questions were influenced largely by the work of Paul and Whitley [3].

Scenarios enabled us to design a cyber dashboard prototype for the purpose of crafting stories. For communication of analysts and NOC managers, we focused the dashboard to tell the stories of these scenarios through different visualizations. We identified three types of scenarios: daily status of operations, report of an attack, and trend analysis from detection of correlated events. In these scenarios, variations can still occur: computer maintenance or security patches; machines with critical vulnerabilities; attackers that downloaded network information; or correlation to similar attacks. We could not address all these scenarios with our dashboard, so we narrowed our focus to specific kinds of data: IDS alerts and reports from an analyst.

4. STAR: A CYBER DASHBOARD

The visualization prototype we designed is the **storytelling treemap for alerts and reports** (**STAR**) dashboard, as shown in Figure 1. *STAR* contains several linked views, and the main view is a squarified treemap [1] of external countries and cities or states which are geolocated IP addresses from IDS alerts and reports. This treemap has been simplified and aesthetically altered with white-space, and we represent each city or state with a hexagon icon to symbolize this abstraction.

The STAR dashboard is a web-based tool built with many component linked views, with dynamic bar charts on the priority level and categorization of alerts, and the main treemap view has a dynamic color scheme based on the selected bar. Additionally, we have several static views at the top, such as the date and time last updated, daily summary, a legend, and a temporal heatmap of alerts per hour. The most-recent report summary is shown in the bottom-right, and a panel also contains a list of all reports, linked to highlight the cities of interest in the main view.

5. CONCLUSIONS AND FUTURE WORK

We have introduced a prototype of the STAR dashboard, designed to convey a summary of cyber information at a glance and through interaction. For future work, we are cur-

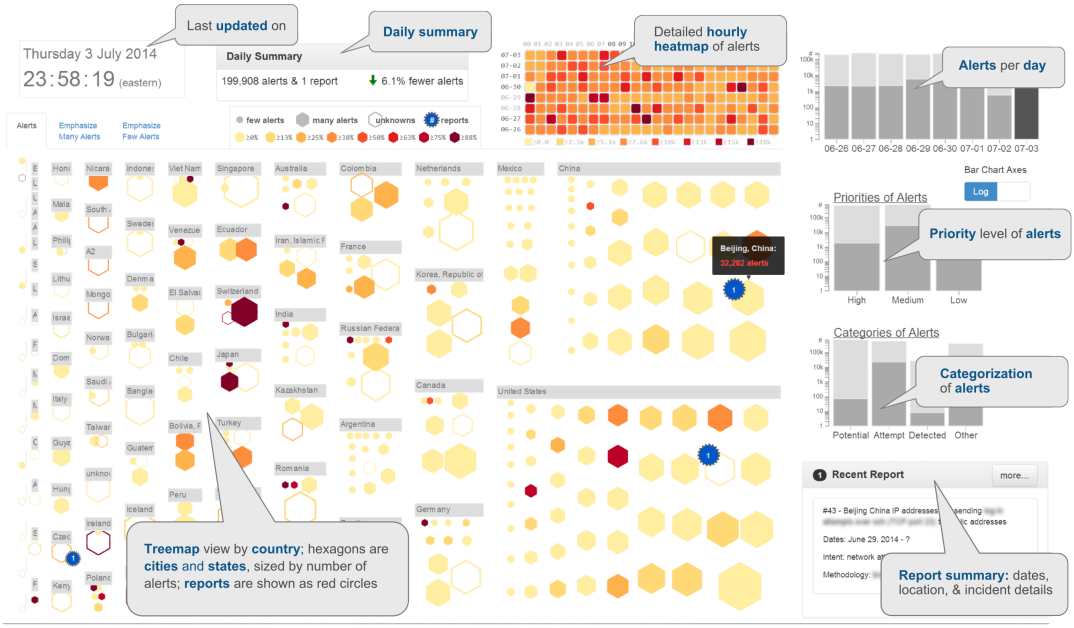

Figure 1: We present our cyber visualization, or the STAR dashboard, an interactive web prototype with linked views that enable the use of simple stories by conveying both IDS alert data on top of analyst-created reports, connected through the use of external entities, both countries and cities, in the main treemap view.

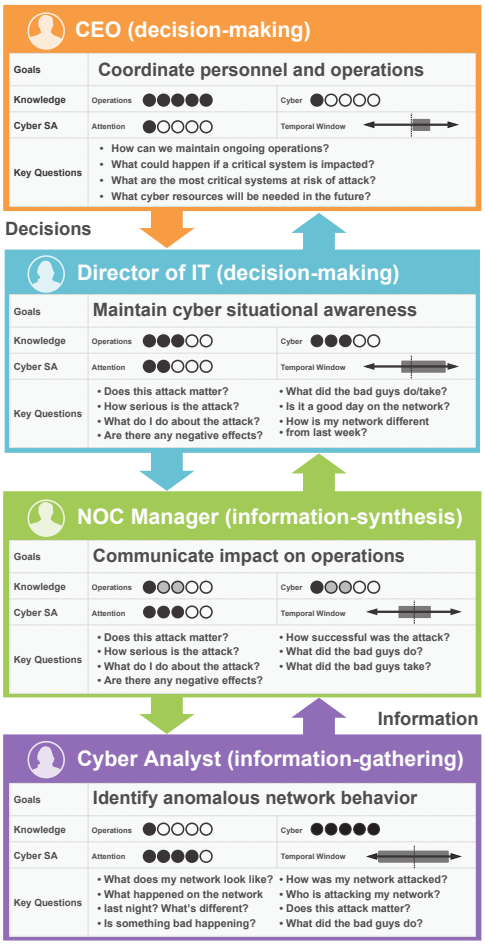

Figure 2: Four key personas identified through our design process: cyber analyst, network operations center manager, director of IT, and a CEO.

rently exploring a geospatial algorithm to create a spatially-influenced treemap [5], and we will also refactor the prototype to work with live, streaming data. As this is still a prototype, we have not yet deployed the tool, so it will need to be evaluated and tested with end users to evaluate its utility, particularly for storytelling.

6. ACKNOWLEDGMENTS

The author would like to thank Diane Staheli for guidance throughout the project, as well as our interviewees: Martine Kalke, Matt Leahy, Rick Larkin, Maureen Hunter, Raul Harnasch, Tamara Yu, David O'Gwynn, Scott Macdonald, Bill Young, Roop Ganguly, Chris Degni. This work is sponsored by the Assistant Secretary of Defense for Research & 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.

7. REFERENCES

[1] M. Bruls, K. Huizing, and J. J. Van Wijk. *Squarified treemaps*. Springer, 2000.

[2] S. McKenna, D. Mazur, J. Agutter, and M. Meyer. Design activity framework for visualization design. *Visualization and Computer Graphics, IEEE Transactions on*, 2014.

[3] C. L. Paul and K. Whitley. A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. In *Human Aspects of Information Security, Privacy, and Trust*, pages 145–154. Springer, 2013.

[4] J. Stoll, D. McColgin, M. Gregory, V. Crow, and W. K. Edwards. Adapting personas for use in security visualization design. In *VizSEC 2007*, pages 39–52. Springer, 2008.

[5] J. Wood and J. Dykes. Spatially ordered treemaps. *Visualization and Computer Graphics, IEEE Transactions on*, 14(6):1348–1355, 2008.