A Framework for Context-Aware Visualization in Cyber Defense

Adam Fouse* Aptima, Inc.
Ryan Mullins Aptima, Inc.
Caroline Ziemkiewicz Aptima, Inc.

ABSTRACT

We present a conceptual framework for selecting and evaluating visualizations that support network vulnerability identification and classification. We examined the relationships between network vulnerabilities and the tasks of network defenders to identify visualizations that facilitate reasoning and critical thinking processes across abstraction levels – i.e., from tabular representation to figurative graphical representation to geometric graphical representation. Contextual factors provide additional characterizations that guide the selection and evaluation process. This framework is intended to: (1) aid designers, developers, and researchers when creating and testing visualizations included in cyber security tools and (2) aid trainers and network defenders trying to understand how or why certain visualizations are more suited for specific purposes.

Keywords: Visualization, defensive cyber operations, context-aware interfaces.

Index Terms: • Human-centered computing~Visual analytics • Human-centered computing~HCI theory, concepts and models • Human-centered computing~Visualization theory, concepts and paradigms.

1 INTRODUCTION

Cyber operators face a deluge of data about complex networks and need to efficiently identify, analyze, and mitigate anomalies. They are overloaded with information, and are often faced with situations that require immediate action to mitigate network effects. While computational techniques such as filters and fusion algorithms can help, the dynamic nature of cyber operations means that data still requires human interpretation to determine the best course of action. Existing efforts for visualization of cyber data have not been broadly successful, resulting in low adoption rates [4]. In many of these cases, visualization systems focus on visual appeal but have questionable utility or a poor fit within a cyber operator's overall workflow. Visualization designers often do not consider human cognitive constraints, or have a poor understanding of the tasks with which cyber operators are faced.

Context-aware decision support systems help maintain a sense of the relation between a user's current view and other parts of the information landscape by monitoring the user's interactions with the system and building a dynamic model of their context in real-time [7]. Loss of context awareness typically occurs when dealing with subsets of data, the narrow focus of which occludes the contextual links between relevant information from one data source to that of another. Decision support systems for cyber operations should provide an integrated, context-sensitive picture that helps users move from exploring low-level network data to determining potential courses of action to decision-making. This requires that visual interfaces provide the ability to adapt to the needs of the user based on a model of their task and context.

LEAVE 0.5 INCH SPACE AT BOTTOM OF LEFT COLUMN ON FIRST PAGE FOR COPYRIGHT BLOCK

In order to use network and user context to make effective decisions about cyber visualization presentation, it is necessary to model the relationship between context and user needs. Knowing the user's task and state of analysis is one thing; connecting that state to the most suitable visualization is another. It is impractical to map every possible cyber defense analysis task to a set of visualization requirements. However, if tasks can be classified into broad yet meaningful types, heuristics can be developed to narrow the design space and map context to presentation.

The best way to classify tasks in a domain is to look to the way work is understood by experts within that domain. In information security, the triad of confidentiality, integrity, and availability is a common model for classifying principles of defense, as well as associated threats [8]. By leveraging this domain knowledge as well as the principles of visualization theory, we can develop an initial framework (Figure 1) for connecting task and context to recommendations and adaptations.

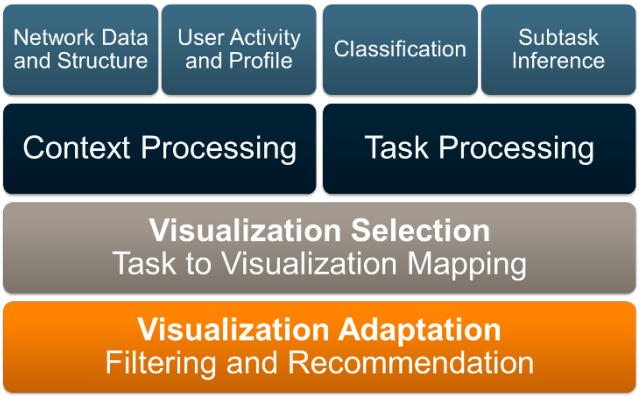

Figure 1. An outline of the proposed context-based visualization framework.

2 NETWORK VULNERABILITIES AND THE CIA TRIAD

Standards, academic literature, and the media commonly define information security as the practice of protecting and preserving three principles of information: (1) confidentiality – the assurance that information is not made available or disclosed to unauthorized parties; (2) integrity – the assurance that information delivered to a party is both complete and accurate; and (3) availability – the assurance that information is accessible when requested by an authorized party [8]. Collectively, these principles are called the CIA triad. Network security looks specifically at preserving these principles for information transmitted over a network.

Our work is built on the premise that the CIA triad can be used to classify and contextualize network vulnerabilities (also termed "threats") in terms of their impacts on information and users. For example, a denial of service (DOS) poses a threat to the availability of information, and is carried out by disabling critical nodes along network pathways between clients and servers. Similarly, IP address spoofing or man-in-the-middle attacks compromise the confidentiality or integrity of information by providing sufficient

credentials to make the affected party, or parties, believe that they are a trusted, authentic source.

3 Threat Types and Visualization Requirements

The advantage of classifying threats using the CIA triad is that it provides a framework for identifying data and visualization needs in a way that can be generalized across similar tasks. If a user's task is to identify the source of a potential data exfiltration, they most likely need to see and analyze similar types of information to users exploring other Confidentiality threats (e.g., spoofing, phishing). These needs fall under two categories: data types required to find a threat, and visualization tasks that must be supported in order to analyze that threat (Table 1).

Identifying the data requirements for a threat type can be done through knowledge elicitation with domain experts. Cognitive task analysis and other requirements gathering methods typically identify the tools and types of data or information needed to make decisions necessary to a given high-level task (e.g., "identify threats to information integrity"). The results of recent task analyses in the cyber security analysis domain can be used to identify an initial set of data requirements for identifying and exploring each type of threat [6]. Further knowledge elicitation with domain experts can clarify the connections between threat types and data types and check assumptions for accuracy.

Table 1. A summary of initial data and visualization task requirements for an operator looking for threats against each of the CIA triad principles.

Threat Type	Data Needs	Visualization Tasks
Confidentiality	User behavior, event and access logs	Characterize long-term temporal patterns, find anomalies
Integrity	Message contents, error logs	Compare data, view uncertainty data
Availability	Traffic patterns, network response times	Characterize temporal patterns, view relationships

A survey of existing task analysis literature can also provide an initial breakdown of tasks and subtasks related to analysis of each of the CIA triad threat types. This breakdown would serve two purposes. First, it would provide guidance to associate a user's current tasking with a threat type, even if it is described at a lower level than the CIA triad. Second, low-level analytical subtasks can be associated with generic visualization tasks [1]. For example, the analytical subtask "find IP addresses that may be compromised" is equivalent to the generic visualization task "find anomalies." In this way, each of the threat types could be associated with a set of data types as well as a set of generic, low-level visualization tasks.

4 Applying the Framework

A substantial body of work in the visualization research field has sought to build recommendations for best practices in visualizing data given the type of data (e.g., numerical, categorical, temporal, multidimensional) and/or the necessary visual analysis tasks (e.g., finding correlations, identifying clusters, characterizing trends). The findings of this research have provided general guidelines for the best visual mappings to improve readability for various low-level data types [3]. The "Show Me" feature integrated in Tableau visual analytics software uses this body of knowledge to automatically recommend visualization types once a user has selected a set of data dimensions to explore [5]. Other taxonomies and models have combined data types and task or interaction types to provide a more context-dependent set of classifications for visualizations [2] [9].

Therefore, once a general threat type has been associated with data type requirements and visualization tasks, it becomes possible to associate it with a recommended visualization or visualizations. By leveraging the existing body of work in visualization theory, we can develop a set of heuristics to select visualizations based on the readability of the necessary data and the low-level tasks that are supported. For example, if a user needs to find anomalies in temporal data because they are searching for Confidentiality threats, a line chart or heat map can be recommended. Further context information can help to choose between similar visualizations; for example, if there are a large number of data rows that must be compared, a heat map is preferable to a line chart. Once developed, these heuristics can be captured as written guidelines for visualization designers as well as integrated into visual analytics systems as recommendations.

5 Conclusions and Ongoing Work

We have outlined an initial framework for selecting and adapting visualizations for cyber security based on user and network context. In ongoing work, we have created an initial prototype tool using these ideas, and continue to refine and add detail to this framework in order to produce a concrete set of threat type and requirement relationships, and visualization selection heuristics. We will make use of existing cyber security task analyses and visualization taxonomies where possible, and further refine and validate this information through expert feedback and evaluation.

References

[1] Amar, R., Eagan, J., & Stasko, J. (2005). Low-level components of analytic activity in information visualization. In Information Visualization, 2005. INFOVIS 2005. IEEE Symposium on (pp. 111-117). IEEE.

[2] Card, S. K., & Mackinlay, J. (1997). The structure of the information visualization design space. In *Information Visualization, 1997. Proceedings., IEEE Symposium on* (pp. 92-99). IEEE.

[3] Cleveland, W. S., & McGill, R. (1984). Graphical perception: Theory, experimentation, and application to the development of graphical methods. *Journal of the American statistical association*, *79*(387), 531-554.

[4] Gates, Carrie, and Sophie Engle. "Reflecting on visualization for cyber security." *2013 IEEE International Conference on Intelligence and Security Informatics*. 2013.

[5] Mackinlay, J. D., Hanrahan, P., & Stolte, C. (2007). Show me: Automatic presentation for visual analysis. *Visualization and Computer Graphics, IEEE Transactions on*, *13*(6), 1137-1144.

[6] McKenna, S., Staheli, D., & Meyer, M. (2015). Unlocking user-centered design methods for building cyber security visualizations. In *Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on* (pp. 1-8). IEEE.

[7] Pfautz, S.L, Ganberg, G., Fouse, A., and Schurr, N. (2015). A General Context-Aware Framework for Improved Human-System Interactions. *AI Magazine,* 36(2), 42-49.

[8] Perrin, C. (2008). The CIA Triad. *TechRepublic IT Security Blog*. TechRepublic, June 30th 2008. http://www.techrepublic.com/blog/it-security/the-cia-triad/

[9] Shneiderman, B. (1996). The eyes have it: A task by data type taxonomy for information visualizations. In *Visual Languages, 1996. Proceedings., IEEE Symposium on* (pp. 336-343). IEEE.