Reflecting on Visualization for Cyber Security

Carrie Gates
CA Labs
carrie.gates@ca.com

Sophie Engle
University of San Francisco
sjengle@cs.usfca.edu

***Abstract*—In this short position paper, we explore three questions regarding cyber security visualization: (1) why cyber security visualization has not been more effective in the past, (2) how visualization can be utilized in cyber security, and (3) how to evaluate cyber security visualization.**

I. Introduction

It has been nearly a decade since the first Visualization for Cyber Security workshop was held in 2004 [1]. In this position paper, we reflect on cyber security visualization, and provide our thoughts on three questions:

- Why has visualization not been more successful in cyber security? In particular, we examine pitfalls and pet peeves that may have contributed to the limited use of visualization for cyber security.
- How can visualization be used for cyber security? We provide the results of our brainstorming, and discuss five different use cases.
- How do you evaluate visualization for cyber security? While evaluation of visualization is challenging for many domains, there are specific aspects of cyber security that make traditional forms of visualization evaluation difficult.

After we discuss these three questions, we provide some final thoughts on future directions for cyber security visualization research.

II. Pitfalls

We begin by discussing some common pitfalls and pet peeves that may be hindering wider spread adoption of cyber security visualization. Most of these pitfalls fall under a single category: visualizing for the wrong reasons. When the visualization has inappropriate or unclear goals, it is no surprise the visualization does not perform well. After we discuss these pitfalls, we begin to identify situations where visualization might be useful for cyber security.

A. Pretty Pictures

A common pitfall is visualization for the sake of visualization. While this type of visualization has artistic value, its usefulness for cyber security is limited. Aesthetics should always come second to the ability of cyber security visualization to convey information and support data analysis. This issue can often be avoided by specifying a question or goal first before attempting visualization.

It is also easy to get distracted by trying fancy data encodings and unusual techniques, and lose sight of what the visualization was originally created to convey. Rather than attempting to apply novel and untested techniques, cyber security visualization should start with the reasoned application of existing and well-tested visualization techniques. Often, many user studies have already been performed for standard techniques that can help guide their application to cyber security tasks. When these techniques fail to perform well, then it may be time to apply state-of-the-art techniques or try a novel approach.

B. Magic Bullet

Visualization is not a magic bullet, and will not help every problem. If a problem is too simple, visualization will not add any additional value. For example, simple DDoS attacks or port scanning are types of events that can be detected without visualization, and make poor use cases for evaluating visualization tools. Another tendency is to apply visualization to a complex problem without first fully understanding the problem. Without fully understanding the problem, environment, and workflow, visualization tools risk distracting analysts from their task.

III. Use Cases

In this section, we brainstorm how visualization might be useful for cyber security specialists. We identify five broad use cases for how visualization may be useful for cyber security: visualization for a specific cyber security goal, visualization for exploration, visualization as a stepping stone, visualization for evaluation, and visualization as evidence.

A. Visualization for a Specific Goal

Visualization often requires extensive resources to develop, evaluate, and iterate. To help ensure visualization will be successful, a specific goal or question should be identified for that visualization. However, not all visualization goals are appropriate in a cyber security context. As we discussed in the previous section on pitfalls, visualization may not add any value for questions with a simple answer. For example, consider anomaly detection. In situations where an event can be flagged as normal versus anomalous with high confidence, visualization is not necessary. (A simple text message would suffice.) However, most of the time, an event is flagged as anomalous but it is unclear whether it is also malicious. Visualization could support an analyst in being able to make that determination.

For the most part, visualization must support data analysis but the type of analysis may differ. The following use cases are essentially sub-cases, identifying different types of analysis where cyber security visualization may be appropriate.

B. Visualization for Exploration

Sometimes, we do not have a well-formed question to start with. In this case, the goal of visualization is less specific and focuses more on exploration of data and providing context. Often times, this process itself can help form more specific questions and goals for visualization. For example, visualization can help an analyst understand the flow of network traffic in a network [2], [3], [4]. Or, visualization can pull together multiple sources and datasets to provide greater context. For example, Goodall *et al.* use visualization to help analyze vulnerabilities in source code by pulling together the output of several source code analysis tools into a single visual display [5].

C. Visualization as a Stepping Stone

We have a tendency to view visualization as either the starting point or the ending point, but rarely the middle. In this case, we already have a question but no idea where to look for the answers. Visualization can be used as a stepping stone to help guide where to focus analysis performed by other tools. For example, suppose we want to perform a root cause analysis to determine why a particular service operating in a complex environment is performing poorly. We can use visualization to provide context, such as interconnected services and dependency relationships, so that we can determine where to target our analysis using other tools [6], [7]. The visualization itself does not provide the question or the answer, but is used instead as a stepping stone in between the two.

D. Visualization For Evaluation

Visualization may also be a useful tool in aiding evaluation of security mechanisms. For example, Zhang *et al.* illustrate how visualization can be used to evaluate whether a particular environment is well-suited for role-based access control [8]. Many publications also use visualization to analyze the configuration of firewalls (e.g., [9], [10]). These tools are not attempting to replace the security mechanisms in use, but to evaluate and improve their usage.

E. Visualization as Evidence

Prevention, detection, and response are all important aspects of protecting against cyber threats. Many of the use cases discussed thus far focus on aspects of detection or prevention of cyber threats. At some point, however, a security analyst may need to justify a response to a cyber threat to decision makers that may not be experts themselves in cyber security. In this case, visualization may be useful not as tool for analysis, but as a tool to illustrate the evidence of an attack or threat. The visualization goal here is very different than before, and more focused on story telling than supporting analysis.

Related to this use case is the problem of presenting forensic evidence to a jury. The forensic analysis has already been completed, but must be conveyed to individuals without cyber security expertise in a compelling and accessible way. Visualization may be able to assist in conveying this evidence [11].

IV. Evaluation

How can we evaluate cyber security visualization? Evaluating the effectiveness of visualization has long been challenging for any domain [12], but certain aspects of cyber security make evaluation even more difficult. In this section, we discuss many of the evaluation scenarios identified by Lam *et al.* [13] in a cyber security context. These scenarios are broken into two categories: evaluation focused on the data analysis process, versus evaluation focused only on the visualization itself. This study shows that the visualization community has largely focused on the visualization and not the related analysis process. We believe evaluation focused on the data analysis process is more vital for cyber security visualization, since research in this domain focuses less on pushing the boundaries in visualization itself and more on applying advances in visualization to the cyber security domain.

A. Visualization Evaluation

Several evaluation scenarios focus on the visualization itself, often in isolation. Lam *et al.* shows that 85% of papers at visualization conferences with an evaluation component focused on this category of evaluation [13]. We focus on two scenarios from this category, evaluating user performance and user experience, and discuss why these are not well-suited for evaluation of cyber security visualization.

Evaluating user performance often require controlled experiments with a large numbers of users and small number of variables. To perform these experiments, realistic tasks must be abstracted to simple ones that can be measured without requiring expert knowledge of the environment or analysis process. For example, Goodall *et al.* perform controlled experiements with 8 users to compare information visualization tool and a textual tool for network packet analysis [14].

However, these studies are often small in size. Large user studies are difficult to conduct for evaluation of cyber security visualization. Designing, using, and evaluating cyber security tasks often requires expert knowledge, limiting the number of potential users that can be recruited for evaluation. And, many of the tasks must support more complicated analysis than tasks which can be objectively evaluated in a large user study involving the general public. Aspects of the cyber security tasks may also be specific to the operating environment, further complicating user recruitment.

We may alternatively want to evaluate user experience. A simple approach is to release the visualization for anyone to download and use, track the adoption rate of the tool, and solicit feedback from users that downloaded and used the tool. However, unlike with user performance studies, meaningful user experience results require users that understand the context for which the tool is used. For some cyber security tasks, this will require expert users. Even for cases where expert users may not be necessary (e.g. phishing protection), low cyber security awareness of the general public reduces the pool of potential users.

B. Process Evaluation

The previous evaluation scenarios focused on the visualization itself, placing less emphasis on studying the environment

and processes for which the visualization will be used. We believe this type of evaluation is well-suited for studying visualization *techniques* which may be broadly applied, but less so for specific visualization *tools* which must be used within a specific context.

One of the most important questions to ask of a visualization tool is how well it meets the needs of its target audience. This is closely related to the pitfalls we discussed earlier—without understanding the needs of the users, it is difficult to specify a clear goal for our cyber security visualizations. There are two scenarios from the study by Lam *et al.* that focus on this question: (1) understanding environments and work practices, and (2) evaluating visual data analysis and reasoning [13].

The first scenario can either be done as a precursor to building a visualization tool and/or to evaluate how preexisting visualization tools are used in that environment. In either case, these types of studies can be conducted as observation in the field or in a lab or via interviews. This type of evaluation allows us to identify the current needs of the users, and later allows us to evaluate how well a visualization tool addresses those needs.

There have been some success stories of visualization tools taking this approach. For example, Sedlmair *et al.* studied visualization tools in a large organization and provided lessons learned, noting "First, retrospectively we learned that studying current practices of end-users was very important for the success of our visualization tools" [15].

Once we have a better understanding of the environment and the needs of the users, evaluation can focus on the data analysis process itself. For example, evaluation can focus on how well the tool supports data exploration and knowledge discovery, or how well it allows analysts to generate hypotheses and make decisions. A large number of evaluations focused on this scenario are performed via case studies. Several factors make case studies well-suited for evaluation of cyber security visualization. A specific pool of actual users can be targeted, their needs identified, and the effectiveness of the tool can be evaluated within the actual context where it will be used.

Case studies avoid many of the issues with performing large user studies involving the general public, but limits the broad applicability of the evaluation results and the tool itself. However, we believe that many of the larger user study results would not be realistically applicable broadly. Instead, this approach gives others the information necessary to determine whether the tool would be well-suited for their specific environment.

Both the process and visualization evaluation scenarios ought to be pursued where possible, but evaluation focused on process and case studies will often be more feasible and applicable for evaluation of cyber security evaluation, and will contribute to its success.

V. Conclusion

In this position paper we present our thoughts on why an administrator or organization might want to adopt tools that use visualization for cybersecurity, along with our thoughts on why visualizations have not been adopted currently for cybersecurity analysis and how we might go about evaluating potential security-related visualizations.

References

[1] Visualization for cyber security (VizSec). [Online]. Available: http://vizsec.org/

[2] J. Glanfield, S. Brooks, T. Taylor, D. Paterson, C. Smith, C. Gates, and J. McHugh, "OverFlow: An overview visualization for network analysis," in *Proceedings of the 6th International Workshop on Visualization for Cyber Security*, ser. VizSec '09, 2009, pp. 11–19.

[3] T. Taylor, D. Paterson, J. Glanfield, C. Gates, S. Brooks, and J. McHugh, "FloVis: Flow visualization system," in *Proceedings of the Cybersecurity Applications and Technologies Conference for Homeland Security (CATCH)*, 2009, pp. 186–198.

[4] J. Glanfield, D. Paterson, C. Smith, T. Taylor, S. Brooks, C. Gates, and J. McHugh, "FloVis: Leveraging visualization to protect sensitive network infrastructure," in *NATO Information Systems Technology Panel Symposium on Information Assurance and Cyber Defense*, November 2010.

[5] J. R. Goodall, H. Radwan, and L. Halseth, "Visual analysis of code security," in *Proceedings of the 7th International Workshop on Visualization for Computer Security*, ser. VizSec '10, 2010, pp. 46–51.

[6] M. Velez-Rojas, S. Mankovskii, M. Roberts, S. Greenspan, and E. Kiris, "Managing information overload on large enterprise systems," in *2011 8th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT)*, Stonybrook, NY, November 2011, pp. 1–6.

[7] ——, "Layer select filter view," *CA Technology Exchange*, vol. 7, pp. 1–8, 2013.

[8] D. Zhang, K. Ramamohanarao, S. C. Versteeg, and R. Zhang, "RoleVAT: Visual assessment of practical need for role based access control," in *Computer Security Applications Conference (ACSAC)*, Honolulu, HI, December 2009, pp. 13–22.

[9] T. Tran, E. Al-Shaer, and R. Boutaba, "Policyvis: Firewall security policy visualization and inspection," in *Proceedings of the 21st Large Installation System Administration Conference (LISA '07)*, Dallas, TX, November 2007, pp. 1–16.

[10] F. Mansmann, T. Göbel, and W. Cheswick, "Visual analysis of complex firewall congurations," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security (VizSec)*, Seattle, WA, October 2012, pp. 1–8.

[11] T. Jankun-Kelly, J. Franck, D. Wilson, J. Carver, D. Dampier, and J. E. Swan II, "Show me how you see: Lessons from studying computer forensics experts for visualization," in *Visualization for Computer Security (VizSec)*, ser. Lecture Notes in Computer Science. Springer, 2008, vol. 5210, pp. 80–86.

[12] C. Plaisant, "The challenge of information visualization evaluation," in *Proceedings of the Working Conference on Advanced Visual Interfaces (AVI)*, 2004, pp. 109–116.

[13] H. Lam, E. Bertini, P. Isenberg, C. Plaisant, and S. Carpendale, "Empirical studies in information visualization: Seven scenarios," *IEEE Transactions on Visualization and Computer Graphics*, vol. 18, no. 9, pp. 1520–1536, 2012.

[14] J. R. Goodall, "Visualization is better! A comparative evaluation," in *Proceedings of the 6th International Workshop on Visualization for Computer Security*, ser. VizSec '09, 2009, pp. 57–68.

[15] M. Sedlmair, P. Isenberg, D. Baur, and A. Butz, "Evaluating information visualization in large companies: Challenges, experiences and recommendations," in *Proceedings of the 3rd Workshop on BEyond Time and Errors: Novel EvaLuation Methods for Information Visualization*, ser. BELIV '10, 2010, pp. 79–86.