5-2009

Utilizing Visualization Mechanisms to Improve User Performance during Cyber Defense Competitions

Andy Luse
Iowa State University, andyluse@iastate.edu

Janea Triplet
Iowa State University, rdtrip@iastate.edu

Utilizing Visualization Mechanisms to Improve User Performance during Cyber Defense Competitions

Andy Luse
Iowa State University
andyluse@iastate.edu

Janea L. Triplett
Iowa State University
rdtrip@iastate.edu

ABSTRACT

This paper describes the development of a visualization system used by students participating in a collegiate cyber defense competition and a first-pass exploratory analysis of the system. Feedback was gathered from first-time users of the system through open-ended field interviews. This initial contextual analysis examined user attitudes about appropriating a new technology in their overall competition strategy. While challenges in the data display and user interface were reported, the interviewees reported that the team and network views offered by the new visualization system enabled them to improve their performance during the competition activities.

INTRODUCTION

Computer and network security has gained national recognition in recent years due to its importance to both the corporate and governmental communities. The 2008 CSI (Computer Security Institute) Computer Crime and Security Survey, arguably one of the most cited surveys in the area, reports that "broad changes in the habits of the criminal world—are making significant, hard-hitting attacks easier and more lucrative for their perpetrators" (Richardson, 2008). Specifically, the survey reported that 43 percent of respondents experienced security incidents with another 13 percent who were unsure. Also reported was that average financial loss due to each security incident was $289,000. These types of statistics confirm that organizations are in need of individuals trained in the area of computer and network security. Many different educational programs are now offering studies in computer and network security, or Information Assurance (IA) education. The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in IA Education for those schools that have such programs and meet certain criteria. Originally, in 1999, seven schools met this criteria and this number has grown to 94 with the increased demand for students educated in this area. Even with all these new programs and educational opportunities, educators are always searching for innovative ways of teaching computer and network security concepts.

Cyber defense competitions (CDCs) are simulation activities which allow student teams to learn computer and network security concepts by requiring them to defend a "corporate" network from attack. These competitions have been shown to be effective for learning network security concepts (Conklin, 2006). Many different types of these competitions have been utilized in varying degrees all over the United States. Now that these competitions are becoming more commonplace, educators are looking for ways to improve the educational quality of these exercises. Security visualization for network security has become a very large area for research within the past decade. Research has found that visualization allows users to take advantage of the parallel processing nature of the human visual system to more effectively discover possible network attacks (Luse et al., 2008). While these systems are being researched for computer and network security, very little research has looked at how these systems can be utilized for cyber defense competitions in educational settings. This research describes the development of CDCVis (Cyber Defense Competition Visualization), a system for use during such an exercise. The structure of the developed system is discussed as well as a first-pass exploratory view of user response to the system.

The manuscript is organized as follows. The Background section describes the expansion of security visualization and cyber defense competitions. The CDCVis section provides a brief overview of the developed visualization system utilized for one such competition. Data Collection and Results gives information surrounding the deployment of the user study to help evaluate the system. The Discussion section offers some proposed explanations about the results found in the study. Finally, the Conclusion and Limitations and Future Work sections provide final comments, future avenues of research, and shortcomings of the current study.

BACKGROUND

Security Visualization

Various streams of research on network security visualization have become popular over the past decade. This research has dealt both with products designed for network security visualization as well as development methodologies for such systems. Products such as NVisionIP (Lakkaraju et al., 2003), TNV (Goodall et al., 2005), and VizFlowConnect (Yin et al., 2004) provide differing views of network traffic and events for security analysis. Also, various government organizations such as the department of defense have utilized information dashboards for security administration (Few, 2006). Research has also looked at various methodologies for effectively developing network security visualization products. Three primary methodologies have been researched. First, the user-based framework looked at security visualization systems from the user's perspective (Goodall, 2005, Goodall et al., 2004, Goodall et al., 2005, Komlodi et al., 2004, Komlodi et al., 2005) by utilizing interviews with experts in the area to develop a framework based on the three phases of user interaction with the system: monitoring, analysis, and response. Second, the alert-oriented framework, or w^3 premise, was designed around the alerts which occurred during possible system threats (Foresti et al., 2006, Livnat et al., 2005). The framework looked at **w**hen the alert occurred, **w**here on the network it took place, and **w**hat type of alert was triggered. The final network security visualization development framework looked at the components which made up the system (Luse et al., 2008). Visualization components were taken from Shneiderman's information visualization theory (Shneiderman and Plaisant, 2005) and Few's research on the real-time imperative (Few, 2006).

Cyber Defense Competitions

Cyber Defense Competitions (CDCs) are contests where students can apply network security concepts in a live exercise. These competitions utilize active learning which enables students to apply and practice computer and network security concepts (Riding and Rayner, 1998). These competitions have been shown to be effective both in education of network security concepts as well as raising awareness for security methods in a rapidly changing field (Jacobson and Evans, 2006).

Many different types of CDCs have been utilized to educate students in network security concepts. These have ranged from small intra-university competitions (Chamalese and Pridgen, 2004, Jacobson and Evans, 2006) and competitions with a few universities (Dodge and Ragsdale, 2004, Schepens et al., 2002, Schepens and James, 2003) all the way to large competitions involving remotely connected university teams (Vigna, 2003b, Vigna, 2003a). The competitions typically involve one of two competition types. One type requires students to be both defenders of their own network as well as attackers of other student networks which allows students to get inside an attacker's head (Cowan et al., 2003, Hoffman et al., 2005). The other type allows students to only act as network administrators defending their own networks against an outside team which is charged with attacking the student networks (Jacobson and Evans, 2006).

The competition utilized for this research involved student teams which were only allowed to defend their networks. The competition was composed of four primary team types. The Blue Teams consisted of the student teams which were charged with setting up and defending their small corporate network (more details given in data collection section). The Green Team was comprised of individuals who acted as users of the services provided by each Blue Team. The Red Team acted as the hackers of the Blue Team networks and could use most any means necessary to remotely attack the systems. Finally, the White Team acted as administrators of the competition by providing assistance to all teams and interaction between the Red Team and any Blue Teams if the need arose. The White Team was also in charge of scoring and allowed each Blue Team to submit reports if they were able to correct a problem found by either the Green or Red teams to gain back points.

CDCVIS

CDCs, as described above, are very hectic and stress-filled environments. The competitions themselves last from eight to 16 hours and can consume either an entire day or span overnight. Each team does its best in the allotted time and scenario to protect their network from attack while supplying the necessary services to the users of their network. In order to make effective decisions regarding their network, team members need as much information as possible about both the competition itself and the state of both their respective team network as well as the overall competition network as a whole. Effective dissemination of information to the teams is tantamount to their success and the overall learning outcomes of the competition.

While many different CDCs have been organized and held in recent years, very little research has been performed regarding the visualization systems for CDCs. The only research found was for a visualization system utilized during Defcon's Capture the Flag competition (Cowan et al., 2003). This visualization system was designed after a Nasdaq-like display system. The system was very simple in that it only showed updates to team performance and did not disclose overall team scores. Very little information was given about this system, but the purpose was only for updates of performance and to act as a

mechanism to keep the audience entertained.

The purpose of a CDC is to help educate students in computer network security. A visualization system for CDCs can be utilized for a number of functions to help further this educational objective. CDCVis, or Cyber Defense Competition Visualization, was designed to provide features above and beyond just updating team performance. CDCVis was designed around two different informational views: a team-based view and an overall network view. The two informational views were deemed necessary to allow students to both visualize their own progress as well as view activities which would enable them to envision potential threats on the competition network at large. The system was also designed around a modular, plug-and-play interface. This allowed for visualization modules to be aggregated and arranged in different configurations on the display depending on the needs of the competition. This also allowed for many of the modules to be utilized both at the team and overall network levels of visualization.

The team-based view was primarily concerned with team information as it pertained to the competition (see Figure 1). The upper strip of the view contained team logos along with respective team numbers which were provided for the teams in the competition. The currently active team in the visualization had a number which was larger and colored in red. Below this strip, in the left middle of the screen was the scoreboard for the competition. This gave scoring updates for each of the blue teams by each of the teams which were judging the competition as well as an aggregated total score. Next to this was the primary team panel. This panel displayed the relevant information for a single team. First, the name of the university and the members of the team were displayed as well as the team logo. Next to the logo, services were displayed along with their respective state. For example, in Figure 1, this team was expected to support user email connections (IMAP, POP3), a website, SSH, file transfer, and email transfer (SMTP). This allowed each team to see what services were currently up according to the White team and therefore which services were usable by the Green team. By showing this information, each team could work to reconfigure their network to allow these services to be reached. In the lower portion of the Team Panel were two real-time graphs. Each contained visual references to the traffic of a certain type and the current activity of that traffic type on the network. The traffic types included *web*, *file transfer*, *email*, *shell*, and other. The bargraph depicted the relative amount of each traffic type (delineated by a bar of a single color) at a specific moment while the NetSqual used a NURBS surface where the five traffic types were located at equal intervals along the width of the surface. The ripples indicated the amount of traffic of a specific type and displayed the traffic trends over time (running from front to back along the length of the graph). Finally, along the bottom was the most current announcement (described in greater detail below).

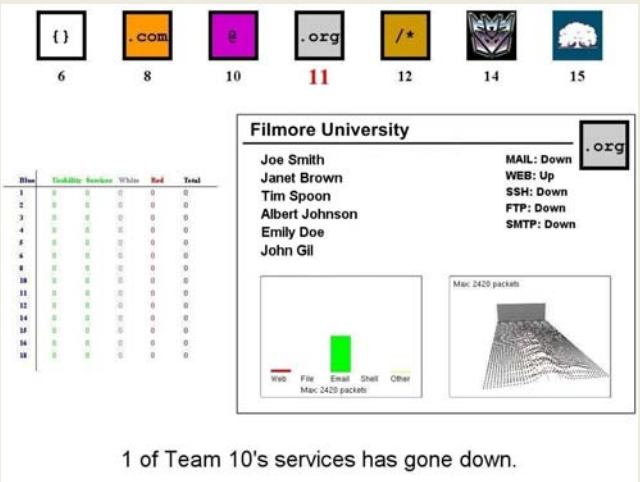

Figure 1. CDCVis Team-based View

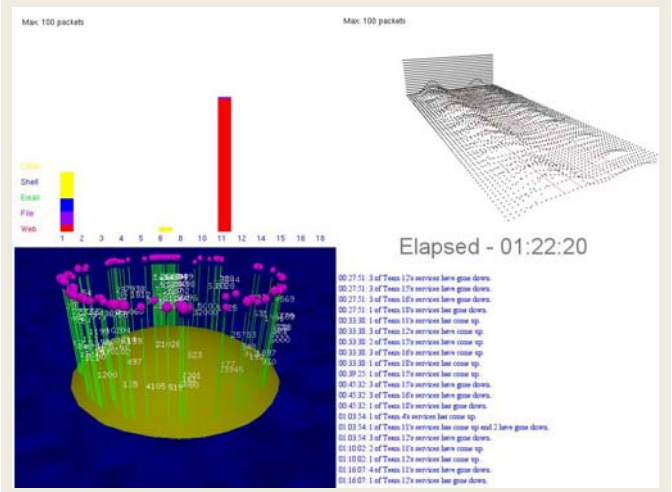

Figure 2. CDCVis Overall Network View

The overall network view provided visualizations pertaining to overall network events on the competition network (see Figure 2). First, in the upper left was a stacked bargraph. This bargraph was slightly modified from the team-based graph in that along the bottom, each Blue team number was listed. The bars for each team consisted of a stacked bargraph of colors pertaining to the five types of traffic either coming into or leaving the team's network at a particular moment. The NetSquall in the upper right again displayed the five traffic types over time, but instead aggregated these five types across all teams. In the lower left, the Island display presented traffic on specific ports as "trees" with the "fruit" on the tree representing the amount of traffic. The ports started at the outside with the lowest ports and increased in a circular pattern. This visualization module was adapted from work done by Oline and Reiners (Oline and Reiners, 2005) and helped to demonstrate the adaptability of the system by bringing in outside visualization modules to plug in. Finally, the lower right portion of the

panel contained a time clock with the amount of time which had elapsed in the competition as well as announcements posted by the system and the White Team for participant informational needs.

DATA COLLECTION

Subjects for the usability portion of this research consisted of teams of individuals who participated in a CDC at a large Midwestern university. The teams consisted of college students pursuing a major involved with network and security administration. Teams came from eight different colleges/universities across the state. School size varied from community colleges to a Research I University. Teams were comprised of four to seven members. This group was solicited due to the live nature of the field study and the range of different participants. Participants were provided with a scenario one month before the competition which detailed a fictitious corporation they must setup and administer. Each team was allowed to use four machines with any legally obtained software they deemed fit, which was provided by the host university. The teams were given one month prior to the competition to remotely setup their networks and were also allowed to come in one day prior for any final setup. The competition lasted from Friday at 5:00 p.m. until Saturday at 11:00 a.m. in the spring semester.

The study of CDCVis was undertaken about seven hours into the competition around 12 midnight so the participants had become accustomed to the competition but were not yet drained from the all-night contest. One of the developers of CDCVis was on-hand and answered any questions about the system both before and after the study. Two interviewers questioned the students utilizing a PDA recorder and a pad of paper. Six teams were interviewed with seventeen individuals contributing to the discussion of the newly introduced visualization system. The purpose of the unstructured interview was to

1. explore the general attitudes of the group about the visualization system
2. assess how the visualization system was used during the competition
3. discover what problems existed which might suggest further development iterations

Attitudes were defined as the tendency to respond positively or negatively to a given person, situation, or object (Aiken, 2002). Usage was simply measured by how the system helped participants accomplish the task at hand. Problems were measured by the expressions and reports of frustration.

Nearly two hours of discussion was recorded which resulted in 145 statements from the participants about the system. The interview data was coded following recommendations given by usability researchers (Beyer and Holtzblatt, 1998, Kuniavsky, 2003). An affinity diagram approach (Beyer and Holtzblatt, 1998) was used to reveal common issues and themes.

RESULTS

Five of the six teams had prior experience participating in previous Collegiate Cyber Defense Competitions. However, none of the teams had used a visualization system to support their defense activities. Common themes emerged suggesting how the visualization system was being used and what problems were experienced.

Each of the six teams said that they used the visualization system to check on their scores. Three teams said that they used the system to check on their services. Another team stated that they used the visualization system to help them improve their response time, to discover their service vulnerabilities, and to focus on the task at hand.

- Now I look up there whenever to see your scores. [Team2]
- It helps seeing all the services. [Team 5]
- It definitely helps with the response time. What exactly we were vulnerable to. What we really needed to be looking at. And what's not important to be looking at. And it helps us cut down on what we don't need to worry about either. [Team 3]

Three teams expressed problems with interpreting the scoring. They were confused by the graph of negative and positive numbers. The problems were resolved by asking other teams for clarification. The confused teams were then assured that the negative numbers were good scores and the positive numbers were demerits.

- I went over and looked and then said, 'are high numbers good or bad?' [Team1]
- But once I figured out that the negatives were better, then it was pretty simple. [Team2]
- At the beginning we asked around a little bit because some of the things weren't clear. [Team 6]

Two teams expressed problems with the program's interface.

- Yeah, when you try to click on 'status' there's no way to go back that I've found. When you try to click the 'back' button you have to log back in. That's really annoying. [Team 4]
- It's just a pain in the ass when I'm sitting here going, 'refresh!' [Team 5]

Two teams requested a user guide to assist them with interpreting the visualization graphics.

- Some kind of user guide, I guess, would have been nice. [Team1]
- Are there any documents saying what each zone is about and how to use them? [Team 3]

Despite the problems experienced, the teams expressed more positive attitudes toward the visualization system than negative. Of the 79 statements that directly referred to the visualization system, 55 of those statements were positive and 24 were negative.

- Would it be possible to get this kind of thing running at our school? We would definitely be interested. [Team 1]
- The visualization helped us focus more on what exactly the problem was at the time. [Team 3]
- It's definitely not something I would want to get rid of. There are just tweaks and of course, that just comes with time. [Team 4]
- I think it would be real cool if we could use it at name of school. [Team 5]
- This is my second year coming to competitions and I feel like it's really neat to just see, 'oh shoot' we're going to get hit with this sort of traffic or whatever. [Team 6]

DISCUSSION

The investigative study of the usability of the newly introduced CDCVis program provided valuable information as to how the participants appropriated this technology into their overall team strategy. Training materials had not been disseminated before the competition pertaining specifically to the visualization system. The feedback received from the user interviews lead to the development of a 'how-to' CDCVis document for future competitions. Even though the field interviews and user observation revealed that the visualization system could be improved by further iterations, the user feedback was more positive (71 percent) than negative.

There were challenges noted with the display of information. The scoring schema reproduced in the graphs was not intuitive to the users. Teams were initially confused because the graph displayed positive team scores with negative numbers and team demerits with positive numbers. This issue was subsequently addressed and the scoring system revamped. There were also suggestions offered from the interviewees about the general usability of the program's interface. Users requested quicker "refresh" times and a more visible "back" button to allow them to return to the main views.

These new users learned to interpret the team and network views in the first hour of exposure to the information visualization program. The teams then used the visualization to check their scores and to discover higher-level threats and vulnerabilities. The team and network views were used to assist competition participants with decision making and performance. Several teams noted that their performance improved because their response times decreased. In addition to improving team performance, several interviewees also noted that the visualization system reduced the stress of the competition because the display allowed them to focus on the immediate problems and ignore the periphery, non-threatening activities.

The user interviews concluded with half of the teams inquiring if the visualization system would be used in future cyber defense competitions. The qualitative interviews and field observations indicated that the visualization system added value to the competition. New users were able to quickly interpret the team and network views and were able to appropriate that information in their overall strategy.

CONCLUSION

The purpose of this study was to look at the utilization of visualization systems for network security. Specifically, this research explored the types of visualization systems used during a cyber defense competition. The study has two main contributions. First, it details a visualization system which has been implemented for a current cyber defense competition. This information can be used by others who may be interested in developing such systems for use during similar competitions. Second, the research provides a first-pass look at the usefulness of the system. This provides initial insights into the educational impacts of the system and how the system can be better leveraged to accomplish these objectives.

While not direct, this study in this type of environment provides a corollary to actual corporate network security administrators utilizing visualization systems for computer and network security. As with many corporate situations, it is difficult to adequately conduct research in actual production environments. CDCs provide a valid testing ground for field experiments in the area of corporate network security. This study capitalizes on this environment to provide an initial look at the use of visualization systems in corporate environments for network security.

LIMITATIONS AND FUTURE WORK

The exploratory nature of the open-ended interviews and the small sample size are limitations of this study. In order to develop a richer understanding of the usability and value of the information visualization system to participants of cyber defense competitions, more field interviews need to be gathered. In addition to interviews, formal usability testing of the visualization system should also be conducted. Many participants noted that their performance in the competition improved by utilizing CDCVis, however, those individual reports should be corroborated by quantitative measures.

Various changes to the system have been instituted since this work has been completed. First, a 'how-to' document was written and has been provided to users at the start of subsequent competitions to allow for better understanding of the system. Similarly, the scoring metrics of the competition have been changed in response to user feedback so that higher scores are now better and demerits are applied negatively. A written explanation of the scoring has also been provided to participants in subsequent competitions. Also, the Island visualization has been removed due to user confusion. Another future direction would be to explore the use of CDCVis components in actual network security settings as opposed to just CDCs.

REFERENCES

1. Aiken, L. (2002) Attitudes and Related Psychosocial Constructs: Theories, Assessment, and Research, Sage Publications, Thousand Oaks, CA.
2. Beyer, H. and Holtzblatt, K. (1998) *Contextual Design: Defining Customer-Centered Systems,* Morgan Kaufmann Publishers, Inc, San Francisco, CA.
3. Chamalese, G. and Pridgen, A. (2004) In 8th Colloquium for Information Systems Security Education, pp. 9-12.
4. Conklin, A. (2006) In Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006. HICSS '06, Vol. 9 IEEE, pp. 220b-220b.
5. Cowan, C., Arnold, S., Beattie, S., Wright, C. and Viega, J. (2003) In *2003 DARPA Information Survivability Conference and Exposition*, Vol. 1, pp. 120-129.
6. Dodge, R. C. and Ragsdale, D. J. (2004) In Proceedings of the IEEE International Conference on Advanced Learning TechnologiesIEEE Computer Society pp. 768-770.
7. Few, S. (2006) Information Dashboard Design: The Effective Visual Communication of Data, O'Reilly Media, Inc., Sebastopol, CA.
8. Foresti, S., Agutter, J., Livnat, Y., Moon, S. and Erbacher, R. (2006) *IEEE Computer Graphics and Applications,* **26,** 48-59.
9. Goodall, J. R. (2005) In *Proceedings of the 2005 IEEE Workshop on INformation Assurance and Security*IEEE, United States Military Academy, West Point, NY, pp. 394-401.
10. Goodall, J. R., Lutters, W. G. and Komlodi, A. (2004) In *Proceedings of the Tenth Americas Conference on Information Systems*New York, NY, pp. 1421-1427.
11. Goodall, J. R., Lutters, W. G., Rheingans, P. and Komlodi, A. (2005) In *IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05)*Minneapolis, MN, pp. 47-54.
12. Hoffman, L. J., Rosenberg, T., Dodge, R. and Ragsdale, D. (2005) *IEEE Security & Privacy,* **3,** 27-33.
13. Jacobson, D. and Evans, N. (2006) In 2006 ASEE Annual Conference & Exposition: Excellence in Education.
14. Komlodi, A., Goodall, J. R. and Lutters, W. G. (2004) In *Conference on Human Factors in Computing Systems*ACM Press, Vienna, Austria, pp. 1743-1746.
15. Komlodi, A., Rheingans, P., Ayachit, U., Goodall, J. R. and Joshi, A. (2005) In *IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05)*Minneapolis, MN, pp. 21 - 28.
16. Kuniavsky, M. (2003) *Observing the User Experience: A Practitioner's Guide to User Research,* Morgan Kaufmann Publishers, Inc, San Francisco, CA.
17. Lakkaraju, K., Bearavolu, R. and Yurcik, W. (2003) In International Multiconference on Measurement, Modelling, and Evaluation of Computer-Communications Systems (Performance TOOLS).
18. Livnat, Y., Agutter, J., Moon, S., Erbacher, R. F. and Foresti, S. (2005) In *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security*IEEE, United States Military Academy, West Point, NY, pp. 30-37.
19. Luse, A., Scheibe, K. P. and Townsend, A. M. (2008) *Information Security Journal,* **17,** 95-107.
20. Oline, A. and Reiners, D. (2005) In IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05)Minneapolis, MN, pp. 113 - 120.
21. Richardson, R. (2008) *Computer Security Institute***,** 1-30.
22. Riding, R. and Rayner, S. (1998) *Cognitive styles and learning strategies,* David Fulton Publishers, London.
23. Schepens, W., Ragsdale, D. and Surdu, J. R. (2002) *The Journal of Information Security,* **1**.
24. Schepens, W. J. and James, J. R. (2003) In *IEEE International Conference on Systems, Man and Cybernetics*, Vol. 5

IEEE, pp. 4300-4305.
25. Shneiderman, B. and Plaisant, C. (2005) *Designing the User Interface,* Pearson Education, Inc.
26. Vigna, G. (2003a) Journal of Information Warfare, **3,** 8-24.
27. Vigna, G. (2003b) In 3rd Ann. World Conf. Information Security Education (WISE 3)Kluwer Academic Publishers, pp. 3-18.
28. Yin, X., Yurcik, W., Treaster, M., Li, Y. and Lakkaraju, K. (2004) In *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*ACM Press, Washington DC, pp. 26 - 34.