Visualizing Network Traffic for Intrusion Detection

John R. Goodall
Dept. of Information Systems, UMBC
1000 Hilltop Circle, Baltimore, MD 21250 USA
jgood@umbc.edu

ABSTRACT
Intrusion detection, the process of using network data to identify potential attacks, has become an essential component of information security. Human analysts doing intrusion detection work utilize vast amounts of data from disparate sources to make decisions about potential attacks. Yet, there is limited understanding of this critical human component. This research seeks to understand the work practices of these human analysts to inform the design of a task-appropriate information visualization tool to support network intrusion detection analysis tasks. System design will follow a user-centered, spiral methodology. System evaluation will include both a field-based qualitative evaluation, uncommon in information visualization, and a lab-based benchmarking evaluation.

Author Keywords
Information visualization, HCI, intrusion detection, network security.

ACM Classification Keywords
H.5.2. User Interfaces. User-Centered Design.

INTRODUCTION
Despite an increase in the frequency and severity of network-based computer attacks and concerted efforts on preventative security measures, vulnerabilities remain. To combat this threat, intrusion detection (ID) analysts continually monitor their networks for signs of suspicious activity. Intrusion detection systems (IDSs) help analysts recognize threats by producing alerts describing the details of potential intrusions. The number of alerts generated by these systems can be overwhelming: thousands of alerts per day, up to 99% of which are false positives [4]. Analysts combine their knowledge and experience with an understanding of the surrounding context to determine the accuracy and severity of an alert amid changing configurations in their operating environment and newly discovered vulnerabilities or intrusion methods. This complex work must be accomplished quickly and effectively. Unfortunately, as networks increase in size and complexity, it becomes increasingly difficult for security analysts to stay ahead of attackers.

Copyright is held by the author/owner(s).
DIS 2006, June 26–28, 2006, University Park, Pennsylvania, USA.
ACM 1-59593-341-7/06/0006.

Current support for ID often focuses on increasing automation. While automation allows for increased scalability, humans provide the ability to handle exceptional events. ID support tools should integrate the intricate sense-making capabilities of humans with the ability of technology to process vast quantities of data. This effort would benefit from information visualization: graphical representations of abstract data to amplify cognition by taking advantage of human perceptual capabilities [1]. Because of the vast amounts of data analysts work with, information visualization shows great potential for supporting ID work by assisting the recognition of patterns and anomalies.

This research is motivated by the criticality of network security in today's world, particularly the overarching importance of the human defender's role in protecting the network infrastructure and detecting malicious activity. However, there has been little research into understanding how ID is accomplished. This research seeks to answer the following research questions:

1. What are the core tasks in ID analysis?
2. How can information visualization support learning "normal" behavior and present essential details in the context of the larger picture?
3. How effective is the developed tool in comparison to current tools and in the context of actual use?

I am currently collecting data to answer the first of these questions, and have begun development of a prototype visualization to begin exploring an answer to the second. The proposed research will focus on expanding the prototype's functionality and evaluating its utility.

COMPLETED WORK
In exploratory research, we developed a preliminary model of ID work that includes three core tasks: monitoring, analysis, and response [2]. Monitoring typically involves the surveillance of an IDS. Analysis determines the accuracy and severity of a security event uncovered during the monitoring task. This is the most complex task, requiring a great deal of knowledge and experience to accomplish successfully. Response refers to an analyst's reaction to a security event. Both the monitoring and analysis tasks can be aided through information visualization tools. However, current visualization for computer security research is targeted almost exclusively towards facilitating monitoring [e.g., 5, 6]. Because of the complexity and lack of support for analysis, this research to date has focused on developing a

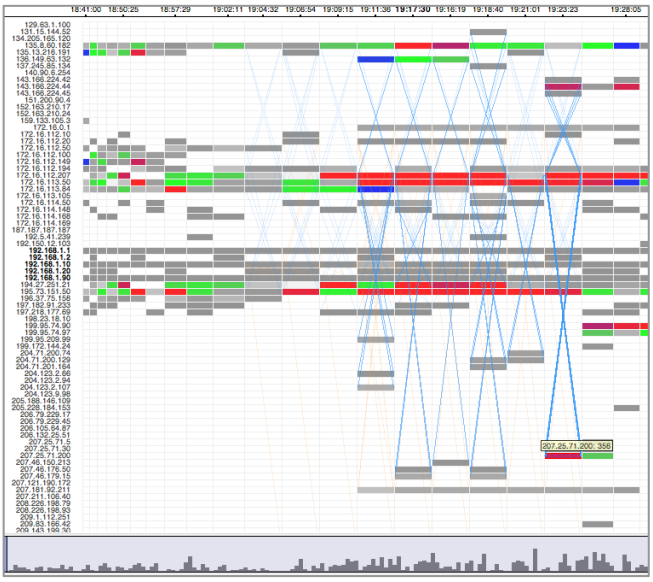

Figure 1. Initial visualization prototype.

richer understanding of how the analysis task is accomplished. This understanding will be used to inform the design of an information visualization tool to support ID analysis.

METHODOLOGY / DESIGN

System design will leverage the field study results to inform the design of a task-appropriate visualization tool to integrate human analysts more fully into the ID analysis processes. Development will follow a user-centered, spiral methodology. The first spiral has been completed, using results from the field study to generate an initial design [3]. A screenshot of the initial prototype is shown in Figure 1.

The next iteration of the design cycle will seek to confirm the results of the field study with a wider population and to fully develop and evaluate the tool. In this research, a brief survey will be used to confirm the results of the interviews and observations with a broader, geographically distributed population and establish the tasks to be used in the later system evaluation.

User testing is a necessary component of design in order to determine the utility and limitations of the developed tool. The proposed research will include a benchmark evaluation and a field evaluation in the analysts' own environments with their own data.

The lab-based, benchmark evaluation will compare the prototype and the current state of the art tool used for network traffic analysis, Ethereal. Tasks derived from the field study will be representative of typical ID analysis tasks. These will include both structured and unstructured tasks. The former will be directed (one possible correct answer) tasks to measure efficiency and error rate and the latter will ask subjects to draw open-ended conclusions from the data.

Field evaluations have the advantage of demonstrating feasibility and usefulness of a system within its actual context of use. A field evaluation allows for an understanding of how (or if) a visualization tool can be integrated into the current work practices of the target user population. The evaluation tasks will be determined by the subjects according to their individual needs and practices. As such, the focus of the evaluation will be on unstructured data exploration rather than structured tasks. This will be the first evaluation of its type for a security visualization tool.

CONTRIBUTIONS

This dissertation research will provide a foundational understanding of ID work practices that will be of use to future researchers and developers in designing task-appropriate support tools. The developed system will be of practical use to ID analysts looking for innovative methods to manage and analyze vast amounts of network data. The evaluations methods will help move information visualization beyond standard usability metrics towards more effective measures of utility.

ACKNOWLEDGMENTS

Thanks to my dissertation advisor Wayne G. Lutters.

REFERENCES

1. Card, S.K., Mackinlay, J.D. and Shneiderman, B. *Information visualization: Using vision to think*. Morgan Kaufman Publishers, San Francisco, CA, 1999.
2. Goodall, J.R., Lutters, W.G. and Komlodi, A., The work of intrusion detection: Rethinking the role of security analysts. *Proc. of AMCIS*, (2004), 1421-1427.
3. Goodall, J.R., Ozok, A.A., Lutters, W.G., Rheingans, P. and Komlodi, A., A user-centered approach to visualizing network traffic for intrusion detection. *Ext. Abstracts ACM CHI*, (2005), 1403-1406.
4. Julisch, K. and Dacier, M., Mining intrusion detection alarms for actionable knowledge. *Proc. of ACM SIGKDD*, (2002), 366-375.
5. Stolze, M., Pawlitzek, R. and Wespi, A., Visual problem-solving support for new event triage in centralized network security monitoring: Challenges, tools and benefits. *GI-SIDAR Conf. IMF* (2003).
6. Yurcik, W., Barlow, J., Lakkaraju, K. and Haberman, M., Two visual computer network security monitoring tools incorporating operator interface requirements. *ACM CHI HCISEC Workshop*, (2003).