December 2006

Evaluating Visualization of Security Alerts in Complex Network Environments for Maintenance of Situational Awareness

Richard Swart
Utah State University

Evaluating Visualization of Security Alerts in Complex Network Environments for Maintenance of Situational Awareness

Richard S. Swart
Utah State University
richard.swart@usu.edu

ABSTRACT

Network security manager are faced with a rapidly changing and complex threat environment due to the proliferation of sophisticated hacking tools. Field studies of network security managers show that they rely on ad hoc collections of log analyzers and custom tools to make sense of multiple sources of data from distributed sensors. The volume of log data exceeds the ability of network security managers to analyze and interpret it. Network security managers must maintain a high level of situational awareness in order to respond to attacks. A variety of tools have been developed to visualize alerts from network intrusion detection and other security tools. No empirical research has demonstrated their usefulness. Limitations in the existing literature are described and an initial framework for empirically evaluating the effectiveness of visualization environments for network security is presented using the VisAlert tool.

Keywords

Visualization, security management, network intrusion detection, usability, situational awareness.

INTRODUCTION

Businesses face unprecedented levels of sophisticated attacks on their computer networks. The maintenance of confidentiality, integrity and availability of data are key factors in organizational success. Network security managers must be able to quickly and accurately gauge the state of their systems in order to protect an organization's computing infrastructure. Industry executives are witnessing a convergence of two trends that account for increased network attacks: (1) a decrease in the technical expertise required to launch attacks on computer systems, and (2) an increasing sophistication of attacks. The most damaging attacks use blended strategies coming from distributed computers (Lee, 2000). These blended attacks cannot be detected using a single alert tool or algorithmic techniques (Komoldi, 2004).

The correct classification of alert data (as attack or not an attack) is crucial for effective network security. Traditional tools in intrusion detection systems (IDS) rely on algorithmic techniques to detect known attack signatures, or use artificial intelligence methods to classify packets of network traffic. The use of IDS systems is hampered by the fact that up to 99% of their alerts are false positives (Julisch, 2002). A previously conducted cognitive task analysis demonstrated that network security managers must monitor, analyze, and make decision based on the correlation of complex interrelated data. Field studies of network security managers show that they rely on manual analysis of log files (Barrett, 2004). However, it is well known that comprehending text based information requires intensive cognitive processing and therefore increases the stress level of network security managers (Lim, 2002). Humans are also error prone when faced with increased cognitive workload. These text files can be enormous and complex, which makes manual review of even a significant portion of the log files infeasible, and can result in both additional false alarms and undetected attacks (Komoldi, 2004). Further, system complexity places a substantial cognitive load on network security managers as they attempt to understand data about the system using information from dynamic, distributed, and complex sources. It is difficult to relate this date to the topology and configuration of networks. Modern networks systems are so complex that security managers can have at best an incomplete mental model of the network.

Visualization and Security Decision Making

Security events can escalate to crisis proportions in a matter of minutes. Viruses and worms are showing increasing sophistication. Security managers struggle to comprehend and make decisions based on an ever increasing amount of data. Though intrusion detection tools have been developed to aid the security manager, these tools are not designed to aid in

decision making with highly complex correlated data, nor are they designed for making rapid judgments about highly correlated events such as blended attacks. Decision making in network security environments carries a high degree of risk and requires exceptional awareness of the network status and configuration. Tools are needed to help reduce the demands on network security managers. One proposed solution is to develop visualization tools that aggregate data from multiple sensors into one display environment.

Optimal decision making depends on reducing the complexity of information to a level that does not exceed human information processing capacity (Birney & Halford, 2002). One strategy to reduce the cognitive demands on decision makers is to reduce the relational complexity of the problem. The amount of information that has to be processed can be reduced by conceptual chunking of data into a larger entity, or by segmenting the task into smaller tasks that are performed serially (Halford et al., 1998). However, both conceptual chunking and segregation are constrained in interactions because of the need to process the variables jointly.

To be effective, a visualization environment must not exceed the complexity of interactions that an individual is able to interpret. Recently, Halford et al. (2005) demonstrated that visual strategies for reasoning and decision making must entail the processing of no more than four variables in any one cognitive step. This four variable limit is consistent with previous research showing a visual and short-term memory capacity of four items, and is consistent with visual connectionist models (Cowan, 2001; Luck & Vogel, 1997).

Visualization and Information Processing Theories

Fayyad (1996) discusses the importance of user interactions and graphical representation of data as key components of the knowledge discovery process used to make patterns of events understandable by users of information systems. Research in human cognition and learning has shown that visualization can play an essential role in association, manipulation, correlation and use of information (Agutter, 2003). Visualization takes advantage of the parallel and pre-attentive nature of the visual-spatial cognitive modality (Wickens, 1983). Information visualization takes advantage of the pre-processing of visual information to support decision making. Thus, it is hypothesized that users of a visualization tool for security will have a reduced cognitive workload and hence show improved performance on attack classification and detection tasks.

It is crucially important to display complex and critical information effectively in order to minimize adverse events and increase the likelihood that the user can successfully manage the situation presented in a display. The utility of visualization systems has been established in many domains, but no research has been conducted to determine whether visualization systems are effective for users of security systems.

SITUATIONAL AWARENESS

Situational awareness (SA) is the ability to identify, process, and comprehend critical information about what is happening in a given situation (Livnat, 2005). SA is a basis for decision making in critical areas such as air traffic control, trade on exchange floors, power plant operations, and military operations. Unlike traditional tools for decision support and error detection in organizational data, network security visualization tool are designed to maintain situational awareness by the network security manager. The maintenance of high levels of situational awareness allows users of information systems of make projections into the future about the likelihood of events. In this research, higher levels of situational awareness are hypothesized to allow more timely detection of attacks and their correct classification.

RELATED WORK

Human processing limitations are the limiting factor in most existing visualization systems. Security software has not been developed in such a way as to avoid overtaxing the information processing capacity of humans. For example, the highly regarded ArcSight Enterprise Security Manager product presents mixed text and visual information requiring users to serially process text while associating the relationship of text to the visual displays. It presents extensive data that appear to exceed the information processing capability of users (Figure 1).

Figure 1. ArchSight ESM Screenshots Showing Integrated Text and Visual Displays

Oline and Reiners (2005) have developed a series of tools that utilize three dimensions. Their approach demonstrates several of the benefits and limitations in visualization for security and is presented in lieu of a comprehensive review of other research. The first of their tools utilizes the metaphor of an Island that maps the entire subnet space into a circle and then represents the activity on each active port by a modified tree (Figure 2). However, it should be noted that this display environment superimposes text containing information about the event on the tree, requiring users to process both text and graphics. The graphics are not immediately interpretable to an untrained user.

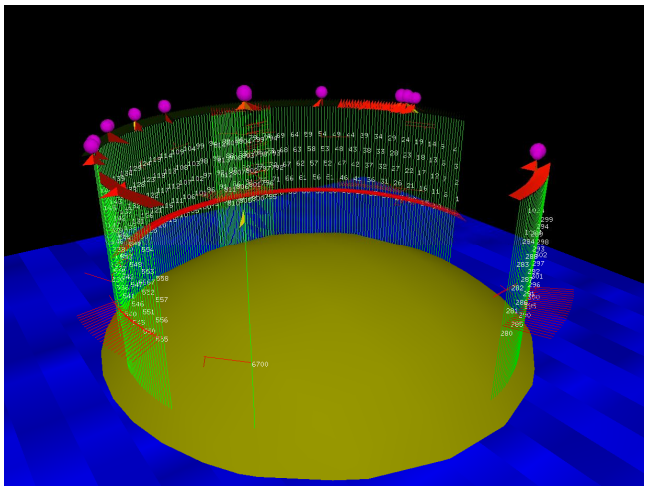

Figure 2. Island View Representing Port Activity as Modified Trees on IP Address Island

Accurate network security management requires understanding of attacks from multiple sources that often span subnet spaces. Visualization approaches for network intrusion detection often attempt to visualize activity from one subnet to another (Figure 3). The top left and right panels represent time and part of the IP address space for the alert, while the bottom center panel displays alerts over a twenty-four hour period. Alert types are color coded according to severity. This display shows a classic "fan" which is seen when one IP address scans a number of other IP addresses. On this display the "fan" is a triangle shaped collection of blue lines indicating alerts from the same address. This is a naïve form of scanning and is easily detectable by firewalls and other hardware and software solutions. Though Olin and Reiners (2005) have investigated a number of visualization approaches, their work is typical or existing research in that it does not provide an end user with the ability to understand current activity on particular nodes.

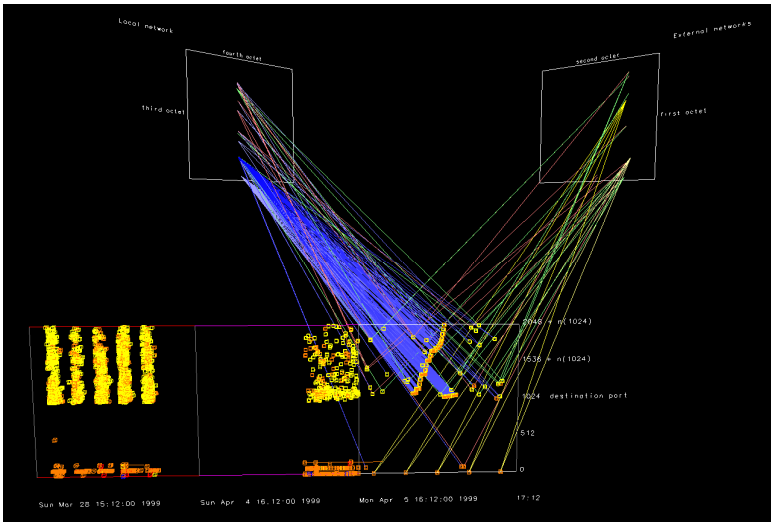

Figure 3. Alert Plots showing network intrusion alerts by time and IP address using color classification

VISUALIZATION AND SITUATIONAL AWARENESS

There has been no empirical research demonstrating that effective visual chunking of information in security software reduces the cognitive demands on users, or leads to faster and more accurate attack detection. No research has been conducted to identify which visualization techniques work better on different data sets (Erbacher, Walker, & Frincke, 2002).

Livnat et al. (2005) identified three key factors that lead to increased situational awareness in network security managers. These key factors are "what, where, and when." In network security terms this means that a security manager needs to know what attacks are occurring at any point in time and be able to discern in the timing of these attacks whether a pattern is forming. This is crucial since distributed and blended attacks come from multiple IP addresses and algorithmic techniques cannot always associate the attack activity. In order to determine what nodes are under attack, the network security manager needs to be able to visualize the attack data in reference to the network topology. This removes a time intensive task and should increase response times. Situational awareness is a prerequisite to effective monitoring, which along with analysis and response, are the three tasks of a network security manager (Goodall, Lutters, Rheingans, & Komoldi, 2006).

Based on the limitations of existing tools, a novel visualization tool for network security data has been developed. *VisAlert* tool attempts to address the signal-to-noise issue in intrusion detection and network security through the presentation of a visual display of alert data from multiple programs superimposed on an image of a network topology (Figure 4). The *VisAlert* tool was designed to provide complementary visual cues from diverse alert sensors that can improve the comprehensibility of information while requiring minimal information processing.

ONGOING RESEARCH

The *VisAlert* tool attempts to address the need to maintain situational awareness through presenting an image of the network topology for the user. When alerts are triggered for a node, it changes in size and a color coded ray segment is created from the center to the edge of the circle representing the node that points to the portion of the outer ring of the display representing that alert type. Thus a network security manager can immediately comprehend what attacks are occurring where, what type of attacks are occurring, and view the history of the attacks by observing the outer rings of the display that represent time segments. Alert beams can also be configured to show patterns of attacks on particular nodes.

This research will compare the performance of users of this system with the performance of users of non-integrated displays to evaluate the effectiveness of conceptual chunking of data in visual displays, to determine the accuracy and latency of detection for users of this system, and will measure the cognitive workload on users through the NASA-TLX instrument.

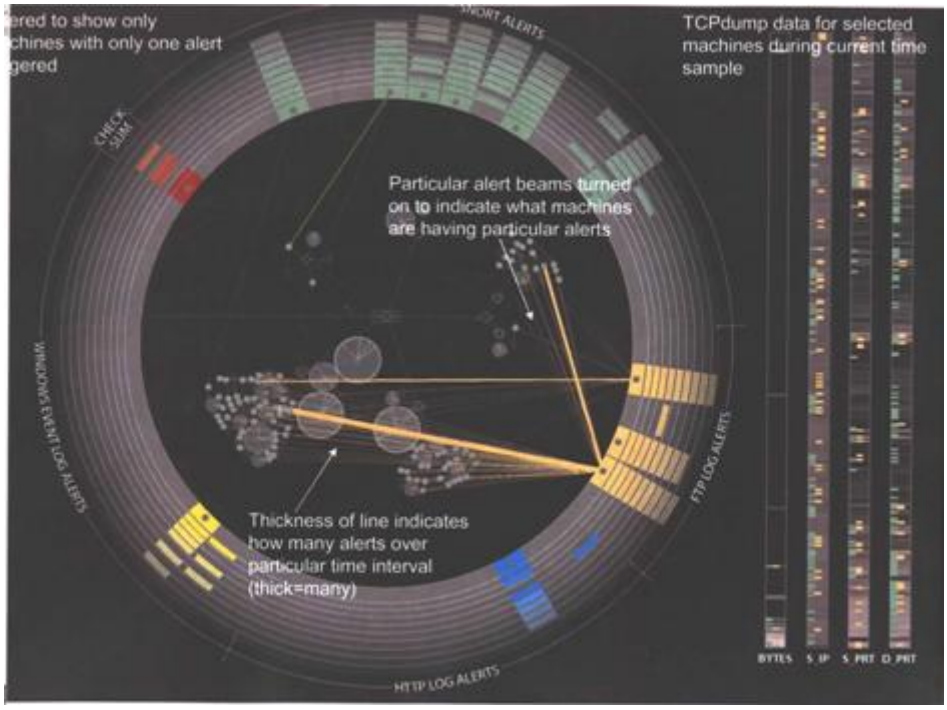

Figure 4. VisAlert Screen Shot Showing Alert Data Superimposed On Network Topology

Situational Awareness will be evaluated using the Situational Analysis Rating Technique (SART) self-report instrument (Taylor, 1990) and Situational Awareness Global Assessment Technique (SAGAT) (Endsley, 1995). SAGAT involves stopping the visualization at intervals unknown to the subjects and measuring their awareness of the environment through testing recognition of events and patterns on the screen. Lastly, perceived usefulness will be evaluated the Purdue Usability Testing Questionnaire (Lamb, 2003).

A FRAMEWORK FOR FUTURE RESEARCH

Early research in information systems evaluated display color, graphical formatting and environments to determine user ability to make effective decisions (Lucas, 1981; Desanctis, 1984; Remus, 1984; Benbasat & Dexter, 1986; Jarvenpaa, 1989). While this seminal work laid the foundation for much of the later research in the design of effective decision support systems, no extant work has formally evaluated the design of security monitoring systems displays. This environment poses exceptional challenges to users. They must understand the architecture and configuration of ever-expanding networks, and relate streams of data from multiple sensors to the network configuration. Decisions must be made in a matter of minutes, and the consequences of failing to detect an attack can have significant effects on the organization.

Future research needs to evaluate user's ability to utilize information presented in mixed graphical and text displays and determine their impact upon decision making given the limited cognitive resources of visual memory (Cowan, 2001; Luck & Vogel, 1997). The effectiveness of different display environments needs to be determined for monitoring, analyzing and responding to security events. Since network security managers are faced with a deluge of data in enterprises, the ability of the tools to correlate events and present alerts based only on predetermined rule sets is crucial. However, this problem is one of data mining. From a visualization research perspective, the key questions to be answered must include determining the most effective visual display for decision making under pressure and when presented with massive amounts of data (monitoring), and which visualization formats best support ad hoc querying about alert data (analysis).

CONCLUSION

Information security in part depends on the ability of security managers to monitor their networks in real time to detect and react to attacks and intrusions. Research in visualization for computer security is emerging, but the computer science visualization community is not incorporating the rich literature from information systems in the development of visualizations. Based on case studies and other research, it is known that security managers perform three distinctly different tasks: monitoring, analyzing and responding to security events. The current research investigates a novel display environment that takes advantage of the human brain's ability to react to change in color and size and detect motion to create an environment to support the maintenance of situational awareness among security monitors. Existing security tools mix text and graphics in complex display environments that appear to exceed the visual information processing capabilities of network security managers, though this conclusion needs empirical validation.

REFERENCES

1. Agutter, J., Drews, F., Syroid, N., Westenskow, D., Albert, R., Strayer, D., Bermudez., J., & Wiegner, M. (2003). Evaluation of graphic cardiovascular display in high fidelity simulator. *Anesthesia Analgesia, 97*(5), 1403-1413.
2. Barrett, R., Kandogan, E., Maglio, P., Haber, E., Takayama, L., & Prabaker, M. (2004). Field studies of computer system administrators: Analysis of system management tools and practices. Paper presented at the CSCW '04, Chicago, Illinois, USA.
3. Benbasat, I., & Dexter, A.S. (1986). An empirical investigation of the impact of graphical and tabular data presentations on decision making. *MIS Quarterly, 2*(1), 59-83.
4. Desanctis, G. (1984). Computer graphics as decision aids - directions for research. *Decision Sciences, 15*(4), 463-487.
5. Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*(1), 32-64.
6. Erbacher, R. F., Walker, K. L., & Frincke, D.A. (2002). Intrusion and misuse detection in large-scale systems. *IEEE Computer Graphics and Applications, Jan/Feb 2002*, 38-47
7. Erbacher, R. F. (2003). Intrusion behavior detection through visualization. Paper presented at the IEEE International Conference on Systems, Man and Cybernetics.
8. Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). The KDD process for extracting useful knowledge from volumes of data. *Communications of the ACM, 39*(11), 27-34.
9. Jarvenpaa, S. L. (1989). The effect of task demands and graphical format on information processing strategies. *Management Science, 35*(3), 285-303
10. Julisch, K., & Dacier, M. (2002). Mining intrusion detection alarms for actionable knowledge. Paper presented at the ACM Conference on Knowledge Discovery and Data Mining.
11. Komoldi, A., Goodall, J.R., & Lutters, W.G. (2004, April 24-29). *An information visualization framework for intrusion detection.* Paper presented at the CHI 2004, Vienna, Austria.
12. Lee, W., Stoflo, S.J. & Mok, K.W. (2000). Adaptive intrusion detection: a data mining approach. *Artificial Intelligence Review, 14*(6), 533-567.
13. Lim, K. H., & Benbasat, I. (2002). The Influence of multimedia on improving the comprehension of organizational information. *Journal of Management Information Systems, 19*(1), 99-127.
14. Livnat, Y., Agutter, J., Moon, R., Erbacher, R.F., & Foresti, S. (2005). A visualization paradigm for network intrusion detection. Paper presented at the IEE Systems, Man and Cybernetics Information Assurance Workshop.
15. Lucas, H. C. (1981). An experimental investigation of the use of computer based graphics in decision making *Management Science, 27*(7), 757-768.
16. Remus, W. (1984). An empirical investigation of the impact of graphical and tabular data presentations on decision making. *Management Science, 30*(5)**,** 533-542.
17. Olin, A., & Reiners, D. (2005). Exploring three-dimensional visualization for intrusion detection. Proceedings of the IEEE Workshop on Visualization for Computer Security, October 26, 2005, Minneapolis, MN, 113-120.
18. Taylor, R. M. (1990). Situational awareness rating technique (SART): the development of a tool for aircrew systems design. Neuilly Sur Seine, France: NATO-AGARD.
19. Wickens, C., Sandry, D., & Vidulich, M. (1983). Compatibility and resource competition between modalities of input, central processing and output. *Human Factors, 25*(2), 227-248.