Network Situational Awareness: A Representative Study

Thomas Eskridge, David Lecoutre, Matt Johnson, Jeffrey M. Bradshaw

Florida Institute for Human and Machine Cognition (IHMC)
40 S. Alcaniz St., Pensacola, FL 32502
{teskridge,dlecoutre,mjohnson,jbradshaw}@ihmc.us

Abstract: Recent developments in visualization techniques for network monitoring and analysis have advanced dramatically over the simple topological graphs and color-coded textual representations found in early systems. These developments are employed in network visualization systems that attempt to present a complete and coherent view of the traffic on a network and the possible security events that may occur. In this paper we describe several representative integrated network visualization systems and discuss the network status and security questions they answer. We then describe an organizational approach to categorizing visualization systems and provide examples of each. We discuss the strengths and weaknesses of each approach and conclude with a proposal for two directions for next-generation systems.

1 Introduction

Threats against computer networks have never been greater, nor have they had a greater impact on the use of computer and network resources [Ce09]. The sophistication of network attacks has also been steadily increasing. First generation attacks propagated uniquely-named executables that could be easily stopped once discovered. Newer attacks use random names and execution patterns to throw off signature-based Intrusion Detection Systems (IDS). Similarly, Denial of Service (DoS) attacks have increased in sophistication from single computer attacks to distributed mobile attacks.

Foreseeing the prospect of even more clever variants on such attacks in the future, computer network defense (CND) analysts require tools that permit the rogue processes to be discovered, identified and remediated. The continual rapid evolution of attack strategies means that IDSs will never be able to provide complete protection against every form of attack, with the consequence that false alarms and multiple incident reports will never completely go away and, in fact, are likely to increase. Even today, the amount of data generated by IDSs is often overwhelming [Co06]. The goal of visualization for CND is to provide an interactive interface which will allows the analyst to acquire and maintain a high level of situational awareness to react more quickly and efficiently to attacks.

Experienced CND analysts, and people in general, are adept at discovering patterns and at noticing deviations from the norm. Because of the deep understanding of their own network and network interfaces, analysts can infer that there is “something wrong” with

the network by observing key changes in measures of network properties. One such property is the rate of bandwidth usage for a given time of day. For instance, while a high bandwidth usage may be typical first thing in the morning when employees are arriving at work, it might be suspicious at times when only a few users are at work. By using experience as a guide, the analyst can rapidly diagnose anomalies and be better able to analyze and interpret the results of IDS and other network monitoring tools to identify and neutralize threats.

This paper presents a discussion of three main approaches to network situational awareness and gives examples of implemented systems for each approach. The strengths and weaknesses of each approach are identified.

2 Human-Centered Design

Computer network defense analysts continually strive to maintain a high level of situational awareness. Graphic visualization of network status and intrusion events is one way that CND analysts can stay ahead of threats. Visualization allows analysts to detect new intrusions, identify anomalous events, and to begin to predict where new threats may occur. By identifying the SA goals held by analysts and the tasks they perform to acquire and maintain SA, a better understanding of the necessities and requirements for CND visualization can be found.

Embracing a human-centered design agenda [Fla97; Hof00], Chen takes an information-theoretic view of visual analytical problems such as NSA and CND and divides the process into information foraging and sense-making [Che08]. Information foraging is a predictive model of search behavior that assumes that the environment is composed of connected islands of information, and that people strive to maximize the amount of relevant information found by modifying their search strategies that traverse and assimilate these islands. Sense-making involves developing numerical models or graphical displays that express properties and relationships in the data. For CND analysts, information foraging and sense-making form a continuous cycle of investigating suspicious connections and interpreting their relationships to the internal network.

D'Amico, *et al*. use cognitive task analysis to identify the mental processes and tasks performed by analysts when identifying and remediating network intrusions [DAm06]. To complete their analysis, they studied more than forty network security analysts to determine what they do, what information they need, and how they go about mediating network threats. They identified several aspects of the mediation process the analysts work through. These aspects include information foraging tasks, such as identifying and quantifying the threat, and correlating indicators and other network data to form patterns and trends. They also identified sense-making tasks such as attacker profiling, and response formulation and execution.

The adoption of visualization tools has been hampered by the immense amount of data to be processes, the short response times required, and the difficulty of making

visualization part of the standard operating procedures. D'Amico, *et al*. found that many visualization tools were not useful to professional analysts because they did not fit the workflow, could not handle the data volume, did not interface well with other systems, or were too difficult to learn to use [DAm06].

3 Approaches to Network Visualization

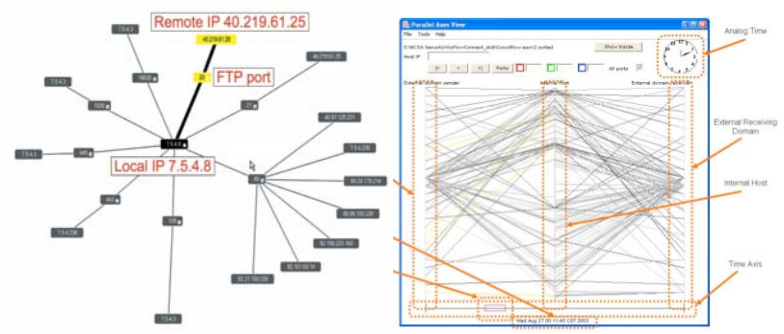
The issues facing CND analysts are significant. There are large amounts of data whose meaning can only be determined in the context of the specifics of the monitored network. There are a large number of known patterns of intrusions, but there are also a larger number of unknown or yet to be discovered patterns of intrusions that must be made detectable. Finally, the intrusions themselves vary in criticality with respect to the context in which the intrusion appears. The visualization systems discussed in this paper each attempt to use visual presentation as a means of mitigating these issues.

While the visual display and user interaction techniques are different for each class of visualization systems discussed, it is useful to understand how the methodological approach of the class determines the context in which the system will be effective. While no one approach has been shown to be superior to all others, lessons can be learned from each methodological approach, allowing promising new areas of investigation to be identified.

The Direct Approach. One methodology is to show what is happening as it is happening in a direct one-to-one relationship between the physical networking components and computers to the visualized elements. This approach yields systems that are intuitive to use and understand and operate in real-time or near-real-time. They generally take low-level data directly from packet or IDS logs and display it without abstracting either visualized elements or input data.

VIAssist [DAi06] and *VisFlowConnect* [Yi04] are examples of the direct approach to network visualization. The graph-based approach of *VIAssist* (Fig 1a) is a direct one-to-one mapping from the physical network to the graphical network, and shows traffic with connecting line color/thickness/style that clear and easily understandable. *VisFlowConnect* uses a parallel coordinates construction to represent the netflow data. Fig. 1b shows external senders on the left, internal hosts in the center, and external receivers on the right. This technique facilitates easy recognition of intrusions such as port scans and distributed denial of service attacks.

While the lack of abstraction makes direct approach interfaces easy to read (at least in low-volume, small network situations), it also places a large burden on the operator to notice the patterns indicative of intrusions. To this end, large or multiple screens can be used very effectively for this class of systems. However, even with large or multiple screens, as the volume of traffic increases the visual clutter also increases. Clutter from overlapping connection lines can increase to the point where important information needed by the analyst to recognize the patterns indicative of intrusions may be obscured.



(a) (b)

Figure 1. *VIAssist* (a) and *VisFlowConnect* (b)

As an alternative to the graph or coordinate plot views, textual charts can also be used for real-time monitoring of network attacks and to cleanly and efficiently display connection data. *SnortView* [KO04] uses a spreadsheet-like display to display the source and destination of the detected transmission, along with its time and alert type.

With the direct approach, the data is not visualized in context. The same message passed between different source and destination pairs will be visualized in the same way. It will be up to the analyst to either: 1) recognize contextually important factors outside of the visualization, or 2) setup filters to focus on only the contextually important factors while ignoring others. The lack of contextual focus as part of the visualized display is one of the most significant weaknesses of the direct approach.

The Abstracted Visualization Approach. The second methodology relaxes the real-time and direct representation constraints to allow some abstraction to be made over time and over network structure. Relaxing the real-time constraint allows the visualization to assist the analyst by highlighting traffic that is irregular or atypical for a particular destination-port combination. Relaxing the one-to-one direct correlation between network structure and visualization allows the display to take advantage of the human perception abilities of pattern completion, "popout" focusing on differences in patterns, and gestalt viewing of the display as a whole entity [Ju81].

Itoh, *et al*. [It06] present a technique that uses the address space hierarchy to organize the display of information on a two dimensional surface that is displayed in perspective. The goal is to place thousands of nodes, equal in size, in one distinct display. This interface allows the analyst to correlate incidents between a large number of computers. Because the surface is shown in perspective, the number of alerts generated at each address can be shown in a height dimension. This presents the analyst with a clear picture of which addresses are actively under attack (Fig. 2).

The abstracted visualization approach does trade-off the immediate feedback present in the direct approach, but suffers much less from problems of obscuring relevant data. This problem does not completely disappear, but the obscuration comes from two different sources. One source is the connecting lines that many visualization systems use to connect fixed source and destination pairs. With high volumes, these lines can still overwhelm a display, even when using very large displays or multiple monitors.

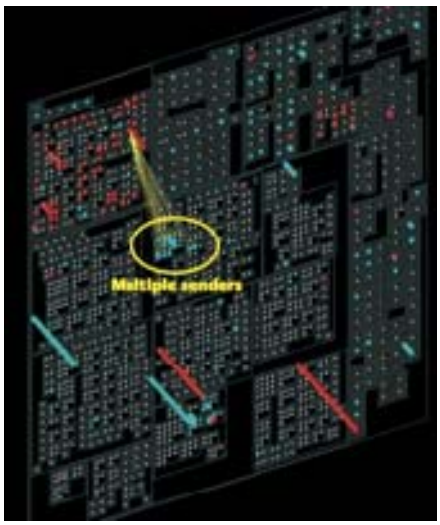


Figure 2. Itoh, *et al.* 2006, visualization display. The color of the extruded bars correspond to the number of sent and received incidents.

A key benefit of the abstracted visualization approach is that data can be displayed using context. Context is derived from the time-abstracted histories of port-destinations and typically is based on the likelihood of communication on the port-destination or deviations from historical or time-windowed averages based on normal operation. Because of time abstraction, the visualization can show that a message going from one source-destination falls within the bounds of typical behavior, while the same message going to a different destination from the same source would be anomalous. This difference can be directly shown in the visualization and can make the pattern recognition task of the analyst much less demanding and error-prone.

The Abstracted Semantics Approach. The third approach to network visualization is to extend the abstracted visualization approach to include abstracting the semantics of the data as well. By abstracting the data from the low-level packet, netflow, and IDS logs to higher level semantics allows the analyst to both create sets of knowledge that represent specific conditions on an individual network, rather than general conditions that may exist anywhere. In doing so, the visualization can now not only highlight indicators of intrusion patterns, but directly identify the type of intrusion itself. So instead of requiring the analyst to notice that a configuration of connecting lines (some of which may be obscured) indicates a distributed port scan, the abstracted data semantics allows the source of the attack to be directly indicated. This ability to reduce perception and reasoning requirements on the analyst is a major benefit of the abstracted semantics approach.

Visitors (Visualization and Exploration of Multiple Time-Oriented Records) is an abstracted semantics intrusion detection visualization and monitoring program that uses Knowledge-based temporal abstraction to represent incident data in different ways for different time scales [Sh06]. The abstraction allows the analyst to aggregate large amounts of data from single or multiple computers into abstractions that can be queried, summarized, or graphically displayed.

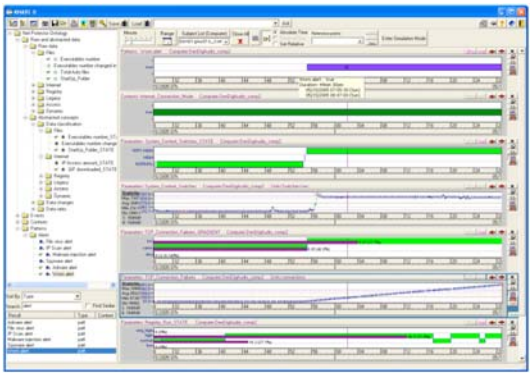


Figure 3. Visitors system inteface.

The goal of the *Visitors* system is to assist the analyst by reducing the amount of data necessary to screen, and to derive context-specific conclusions based on a security and intrusion detection knowledge-base. The system uses simple thresholding to discretize relevant continuous attributes, translating from low-level data such as packet counts to a qualitative description of those counts such as “low”, “medium”, and “high”. These new descriptions can now be used by a higher-level abstraction as attributes in conjunction with any lower-level data. The *Visitors* interface shows several different network measures with varying levels of semantic abstraction. The timeline graph at the top of Fig. 3 shows the onset of a worm, while the graphs below show various lower-level components of the “worm” knowledge-based abstraction.

This approach takes the idea of representing data in context to a higher level. Like abstracted visualization, the data is represented in a context that not only includes time abstraction, but also includes data abstraction. As in the previous case, the anomalous message send to one source-destination pair and the typical message sent to another source-destination pair can be displayed differently, but also displayed in a way that carries out the implications of the contextual differences. If the message is anomalous because it is sending oversized packets to a port associated with an SQL database, it may be correct to abstract that message and represent it as an SQL injection attack.

The difficulty in abstracting semantics for data visualization is the difficulty in developing the higher-level knowledge, and in determining when that knowledge applies to a particular situation.

4 Conclusions

The systems surveyed in this paper were chosen because they illustrate visualization principles and task-specific capabilities that have proven to be useful in visualization for CND and situational awareness. As part of a larger study on human-computer interaction

and network situational awareness, this lays the groundwork necessary to begin to understand the current state-of-the-art in network visualization and the directions future implementations may go.

Attempting to project beyond the trend established by the direct, abstracted visualization, and abstracted semantics approaches yields several interesting possible next steps. One approach is to improve the communicative qualities of the display itself. There are new developments in using large displays that show a significant advantage over smaller, conventional displays when the task is to discover hidden relations amongst data [Cz03; Cz06]. Similarly, the style in which the data is presented can have a significant impact on operator performance [Ju81; Be91; Th96; ST03].

Another approach is to leverage abstracted semantics to include reasoning and delegation support for network visualization and management. Having identifiable intrusions enables standard procedures to be carried out in response. Enabling delegation of these standard procedures will enable the analyst to handle more intrusions more efficiently. These procedures could include the delegation of the specification and construction of visualizations to isolate intruder actions, or spawn process to collect data related to the identity of the network threats. They could also perform interdictory actions to prevent the intrusion from propagating further or wasting more network resources.

Key questions to be answered by the delegation approach include: 1) how will the user interact with the user interface and interaction elements to allow for the direction and monitoring of delegated tasks? 2) How will the contextual conditions that trigger the execution of an automatically-delegated task be specified and operated? and 3) Can the conditions under which delegated tasks succeed or fail be used to learn new contextual conditions for task application? Both directions for extending the current classes of visualization systems show significant potential for increasing the efficiency and effectiveness of network analysts. As there seems to be no slowdown in the releases of new viruses, or in the rate of directed attacks against most organization's networks, progress in any or all of the approaches will be welcomed.

Ultimately, a successful future approach will need to go beyond the problem of visualization itself. To be able to accommodate the preferences of individual analysts and the idiosyncracies of differing contexts and situations, such displays must be highly configurable through policy [Bra04a] and, where appropriate, should learn and adapt as occasion requires [Jo05]. Moreover, future approaches will also benefit from advances in agent technologies that can proactively assist analysts and remove some of the more tedious aspects of their tasks [Bra04b].

Bibliography

[Be91] Bergen, J. R.: Theories of visual texture perception. Spatial Vision Vol 10: Vision and Vision Dysfunction. D. Regan. Boca Raton, FL, CRC Press, 1991

[Bra04a] Bradshaw, J. M.; Beautement, P.; et al.: Making agents acceptable to people. In Intelligent Technologies for Information Analysis: Advances in Agents, Data Mining, and Statistical Learning, edited by N. Zhong and J. Liu, 361-400. Berlin: Springer Verlag, 2004.

[Bra04b] Bradshaw, J. M.; Feltovich, P.; et al.: Dimensions of adjustable autonomy and mixed-initiative interaction. In Agents and Computational Autonomy: Potential, Risks, and Solutions. Lecture Notes in Computer Science, Vol. 2969, edited by Matthias Nickles, Michael Rovatsos and Gerhard Weiss, 17-39. Berlin, Germany: Springer-Verlag, 2004.

[Ce09] CERT-CC: CERT Full Statistics. Retrieved Jan 26, 2009, from http://www.cert.org/stats/full-stats.html#hist-year.

[Che08] Chen, C.: An Information-Theoretic View of Visual Analytics. IEEE Computer Graphics and Applications 28(1), 2008: p. 18-23.

[Co06] Conti, G.; Abdullah, k.; et al.: Countering security information overload through alert and packet visualization. Computer Graphics and Applications, IEEE 26(2), 2006,60-70.

[Cz06] Czerwinski, M.; Robertson, G.; et al: Large display research overview CHI '06 extended abstracts on Human factors in computing systems. Montreal, Quebec, Canada ACM, 2006**:** p. 69-74.

[Cz03] Czerwinski, M.; Smith, G.; et al.: Toward Characterizing the Productivity Benefits of Very Large Displays. Proceedings of IFIP INTERACT03: Human-Computer Interaction, 2003**:** p. 9-16.

[DAm06] D'Amico, A. D.; Goodall, J.R.; et al.: Visual Discovery in Computer Network Defense. Computer Graphics and Applications, IEEE 26(2), 2006: p. 20-27.

[Fla97] Flanagan, J. L.; Huang, T. S.; et al.: Final Report of the National Science Foundation Workshop on Human-Centered Systems: Information, Interactively, and Intelligence (HCS). Beckman Institute for Advanced Science and Technology, University of Illinois at Urbana-Champaign, 1997.

[Hoff00] Hoffman, R. R.; Ford, K. M.; et al.: The Handbook of Human-Centered Computing. Report, Institute for Human and Machine Cognition, University of West Florida, Pensacola FL, 2000.

[It06] Itoh, T.; Takakura, H.; et al.: Hierarchical visualization of network intrusion detection data. Computer Graphics and Applications, IEEE 26(2), 2006: p. 40-7.

[Jo05] Johnson, M.J.; Kulkarni, S.P.; et al.: AMI: An Adaptive Multi-Agent Framework for Augmented Cognition. In the Proceedings of the 1st International Conference on Augmented Cognition. Mahwah, NJ: Lawrence Erlbaum Associates, 2005.

[Ju81] Julesz, B.: Figure and ground perception in briefly presented isodipole textures. Perceptual Organization. M. Kubovy and J. Pomerantz. Hillsdale, NJ, Erlbaum, 1981**:** 27-54.

[KO04] Koike, H.; Ohno, K.: SnortView: visualization system of snort logs. Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. Washington DC, USA, ACM, 2004.

[Sh06] Shabtai, A.; et al.: An intelligent, interactive tool for exploration and visualization of time-oriented security data. Proceedings of the 3rd international workshop on Visualization for computer security. Alexandria, Virginia, USA, ACM, 2006.

[ST03] Still, D. L.; L. A. Temme: OZ: A human-centered computing cockpit display. Interservice/Industry Training, Simulation & Education Conference (I/ITSEC). Orlando, FL, 2003.

[Th96] Thibos, L. N.; D. L. Still; et al.: Characterization of spatial aliasing and contrast sensitivity in peripheral vision. Vision Research 36, 1996: p.249-258.

[Yi04] Yin, X.; Yurcik, W.; et al.: VisFlowConnect: netflow visualizations of link relationships for security situational awareness. Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. Washington DC, USA, ACM, 2004.