Visualization Design for Immediate High-Level Situational Assessment

Robert F. Erbacher
Computational and Information Sciences Directorate,
U.S. Army Research Laboratory, Adelphi, MD, USA
Robert.F.Erbacher.civ@mail.mil

Abstract

We present the design of a visualization technique based on the results of a human in the loop process, which relied heavily on actual network managers and network analysts, i.e., the domain experts. This visualization design was directly targeted at supporting one set of tasks identified by the interviewed domain experts. Specifically, this was the need for the ability to provide rapid and immediate assessment of the state of the network and associated hosts. This visualization technique, the Cyber Command Gauge Cluster (CCGC), allows analysts to review the state of the network and immediately locate potentially problematic anomalies, drill down into those anomalies, and prioritize said anomalies for detailed analysis and remediation. By providing a summary representation combined with independent representations of critical parameters, the visualization technique is unique in its ability to aid decision makers in making rapid assessments and prioritization of identified anomalies in the network. A prototype environment was implemented based on the initial mockups and extensive feedback was provided by the target domain experts on the resultant visualization technique design. While the prototype focuses on typical network analysis scenarios, the visualization technique itself is devised to provide generalized support to decision makers and situational awareness in any domain. Similarly, the generalized parameter mapping allows the visualization technique to be applicable to any level of decision making, from the front-line network analyst to the CIO.

Keywords: Situational Awareness, Decision Makers, Visualization, Human in the Loop, Cyber Security

1. INTRODUCTION

The network managers' goal, as a main line decision maker, is to prioritize network events and anomalies based on their likelihood of maliciousness and their potential ramifications. To handle the ever-increasing numbers of attacks, network analysts and managers have processes and analysis stratagems for dealing with typical cyber anomalies. Their first level of analysis is at a highly abstract, situational awareness level, derived from our recent cognitive task analysis with network managers and network analysts [7][8]. In essence, the network analysts and network managers identified the need for visualization techniques that allow a manager to immediately identify the state of the network. Only when an anomaly is identified at this high-level do analysts drill down into more detailed techniques for actual analysis.

We have created a set of next-generation, situational-awareness capabilities that while applied here to cyber security and associated anomalies, in the long term, will be broadly applicable to other domains. Situational awareness is the creation of abstract higher-level representations of the underlying raw data. It focuses on immediate comprehension rather than detailed analysis. Situational awareness is '… knowing what is going on so you can figure out what to do' [1].

The goal of situational-awareness visualization for cyber analysis is to provide perceptually based displays that allow decision makers to rapidly understand the readiness of all available cyber resources. Readiness in this context is the ability of cyber resources to perform day-to-day tasks and deploy cyber operations and effects should they be designated to such activities. For instance, even a desktop that is overloaded may not be able to deploy Microsoft Office applications. Existing situational-awareness environments such as VisAlert [10], are designed with more detailed analysis in mind and do not provide for the immediate assessment needs of decision makers. In fact, VisAlert can be seen as providing the follow-on analysis capability for the immediate assessment capability we are proposing here.

For situational awareness, we used Endsley's model [5]. This model intrinsically consists of three levels: perception, comprehension and projection. Perception is providing a representation of the current state of a situation. Comprehension relates to a higher-level understanding of all available data. Comprehension requires a far greater level of correlation and data integration than is incorporated into the perception level. Finally, the projection level looks at projecting the event into the future to determine its impact and progression. The goal with situational awareness is to rapidly answer:

- What is happening?
- Why is it happening?
- What will happen next?
- What can I do about it?

The goal of this research is to improve the decision making process such that better actions are taken. D'Amico et al. [3] identify the need to develop different visualization techniques designed for the desired level of situational awareness. Jajodia et al. [14] lay out the research issues and challenges specifically in applying situational awareness to cyber security. These two works exemplify much of our research process resulting in a technique that will allow analysts to make better decisions and better prioritizations than is currently being done.

With the goal of improving the decision making process in mind, we document a high-level situational awareness visualization technique designed for decision makers, detail how the design and implementation came about, provide a case study on the applicability of the technique, and summarize the feedback from actual network analysts and managers from Pacific Northwest National Laboratory (PNNL).

2. PREVIOUS WORK

There are currently too many visualization techniques designed for cyber security to enumerate here. The VizSec [25] workshop alone has been geared towards publishing a dozen such techniques a year. These techniques cover the gamut of approaches, techniques, and goals. The typical goals of visualization for cyber

security will focus on data analysis, event identification, event analysis, and situational awareness. These techniques can be designed for either the network analyst at a low level or for the decision maker, a higher level view. Our goal in this work is to present a high-level situational awareness technique designed for the decision makers; though the configurability of the system allows it to be used in a wide array of tasks and users.

Focusing on visualization for situational awareness of cyber security has received the least amount of attention in this domain. The best-known tool for this purpose is VisAlert [10], which is designed to provide correlation of events within a topology and provide high-level analysis of events. Its ability to correlate events ensures it is effectively suited for identification of the sophisticated persistent threat. Its configurability and high-level view allows it to be of use to both the network analyst and the decision maker.

A second environment is NVisionIP [15], which provides numerous techniques for the identification of network characteristics. It is focused on providing situational awareness for the analyst and not for the decision maker. VisFlowConnect [24] provides a specialized link relationship visualization technique to provide a more narrow-scoped situational awareness capability to analysts. Panameto [22] while providing separate passive monitoring capabilities uses a simple network connectivity graph to display network topology and topology changes. Best et al. [4] provide real-time visualization for situational awareness geared towards monitoring network traffic by support staff.

What becomes clear quite readily from the existing previous work is that the majority of the work focuses on situational awareness for the network analyst and not for the decision maker. Overall, very little of the visualization effort itself has been focused on situational awareness; rather, the majority of the research has focused on identification and analysis techniques. While VisAlert does consider situational awareness for the decision maker it still focuses on an analysis (correlation) perspective and not the high-level rapid assessment we focus on for decision making.

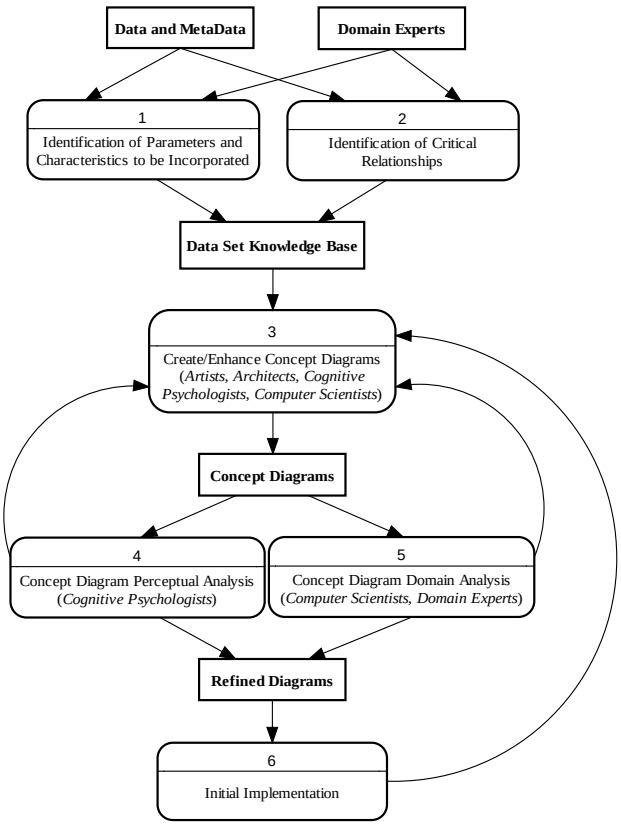

Figure 1. The iterative process followed in the design of the visualization techniques.

3. VISUALIZATION DESIGN FOR DECISION MAKERS

The visualization design process involved several steps. This process was focused on keeping the user in the loop and integrated extensive input from network analysts and managers; the complete details of this user process is documented in our cognitive task analysis [7][8]. First, was an initial brainstorming meeting with analysts, network managers, security researchers, and visualization researchers at PNNL. This resulted in an initial series of questions such as the time frame we needed to consider for this level of analysis. Such questions were primarily answered from existing Cognitive Task Analysis (CTAs), especially Anita D'Amico's from Secure Decisions [2] and Stefano Foresti's from the University of Utah [11]. Second, was an initial set of individual interviews with network analysts and managers. Third, was the examination of previous work. These knowledge-gathering steps provided the initial background needed to conduct a more detailed interview/brainstorming meeting with analysts and network managers. The resulting discussion session led to the development of a new task flow diagram [7][8] for our target network analysts and managers.

Based on the task flow diagram we created several visualization mockups. In order to meet the full needs of this task flow diagram, the mockups targeted the needs of both the assessment and response phases of the developed task flow model. While we have identified how characteristics for other phases could be incorporated, we did not actively pursue aspects from those phases as they were deemed to be out of scope of the current project. Of note is that after the design of these mockups we performed a set of evaluations with analysts and visualization experts to acquire their feedback and aid in refinement of the visualizations. These interviews also aided in identification of which visualizations would be targeted for implementation. Here we focus on the design of a visualization technique specifically geared towards decision-making; many of the other mockups focused on the analysis task.

The design of the mockups, conceptual designs, essentially followed the process exemplified by Figure 1. The cognitive task analysis exemplified the incorporation of the domain experts and their impact on phases 1, 2, and 5 of the process. Phases 1 and 2 revolved around acquiring the understanding necessary to design effective visualization techniques. Phase 3 was the main effort in designing initial concept diagrams for the visualization techniques. Phase 4 employed a review of the cognitive aspects of the visualization techniques and phase 5 employed a domain expert review of the visualization techniques. Clearly, the process was iterative based on feedback. Finally, prototype implementation is exemplified by phase 6.

The focus of the techniques on decision makers combined with the goal of representing an array of nodes and parameters through clusters of such gauges resulted in the name decision maker command gauge cluster (DMCGC). More specifically, for cyber security scenarios we term the display the cyber command gauge cluster (CCGC). The unique name actually has an important

etymology. Information visualizations have several mechanisms for representing parameters of a node in a dataset:

- Pixel [17] – A single pixel can be used to represent multiple parameters by mapping the different parameters to the hue, lightness, and saturation values of the pixel.
- Icon [9] – An icon is designed to represent multiple values and displayed en-masse, forming a texture. An icon can be thought of as a generalization of a pixel. By making use of a box of pixels, many parameters can be represented simultaneously. An icon is not meant to be interpreted individually.
- Glyph [9] – A glyph is similar to an icon with the main difference that they are meant to be interpreted individually. This does not necessitate that they be more complex than icons.
- Gauge [33] – A gauge can be thought of as a very complex glyph. This is exemplified by the incorporation of many components that need to be interpreted individually. A gauge can be considered a visualization display in its own right. Typically, a single gauge will be the entirety of one visualization display.
- Gauge Cluster – We arrived at the "gauge cluster" term to represent the duality of the fact that our gauges are actually a cluster of elements (a cluster of gauges) and the fact that the visualization incorporates a number of gauge clusters.

3.1 Concept 1

This design, Figure 2, is geared towards providing a clear summary of the network status. In particular, in our actual implementation we focused this design on the representation of impact and vulnerability assessment; a similar goal as identified by Nusinov et al. [16]. Similarly, activity of interest scores [20] can be used. Wang et al. [23] examine the extraction of other factors for network security situational awareness. In this design, the large dial provides the overall status of the system, network, or mission; while the prototype focused on systems, the design can easily be generalized. The smaller dials provide more detail identifying how individual components of the system are being impacted. In terms of systems, we generally look at the impact on the system's disks, memory, network, and CPU usage. For a mission, these dials could represent the analyst, the analyst's systems, the analyst's network connectivity to the outside world, redundancy, etc. Again, in the long term the design can be completely generalized for any summary display needs.

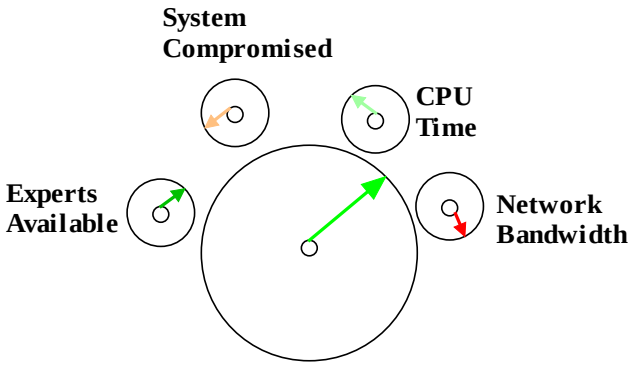

Figure 2. Concept diagram 1. The first high-level visualization design for decision makers. History information wasn't shown. Angles followed the standard trigonometric layout.

The design itself uses dial-like metaphors that are well known and easily interpreted by analysts and the general user. The dial itself is reinforced with color to make interpretation of value far more rapid. In this initial design, the dials were designed to go counterclockwise.

Looking back at the situational awareness model, it is this type of design concept that will provide the desired immediate comprehension of the state of the network. Clearly, the design allows for less analysis but that can be resolved with additional visualization designs.

3.2 Concept 2

This design, Figure 3, is a refinement of concept 1 based on feedback from analysts and visualization experts. First, the dials were redesigned to go in a clockwise fashion. Second, history information was added by providing rings within each of the dials. The outer ring provides the most current value. The filling of the rings also reinforces where the zero axis is, an issue identified with concept 1.

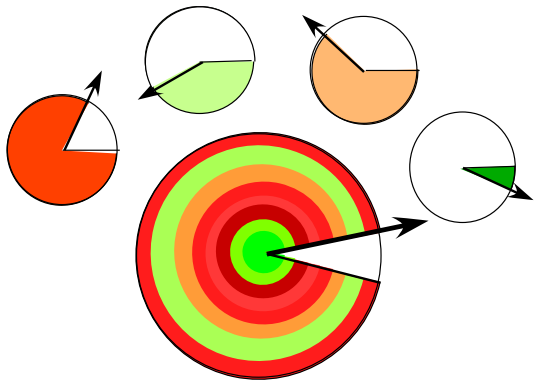

Figure 3. Concept diagram 2. A follow-on high-level visualization design concept for decision makers. History information was included and angles were computed in a clockwise fashion. Filling the angles provides visual reinforcement of the values.

3.3 Mockup Implementations

The implementation resulting from the original mockups is shown in Figures 4-6. Key components of the implementation include:

- The number of gauge clusters is configurable. Figure 4 shows nine while figures 5 and 6 show six. The gauge clusters are designed to form a square as closely as possible; N=number of gauge clusters.

$$Cols = \lceil \sqrt{N} \rceil$$
$$Rows = \lfloor \sqrt{N} \rfloor$$

- The number of sub-gauges is configurable, though we only show four in our examples. Positioning and size are determine by (S=number of sub-gauges, θ=angle, d=diameter of sub-gauge, r=radius of arc inscribed by sub-gauges):

$$\theta = \begin{cases} i \times 36° + 33.\overline{33}° & S \leq 10 \\ i \times \dfrac{360°}{S} + 33.\overline{33}° & S > 10 \end{cases}$$

$$d = \begin{cases} \dfrac{2\pi \times r}{10} - 5 & S \leq 10 \\ \dfrac{2\pi \times r}{S} \times .9 & S > 10 \end{cases}$$

- The percentage contribution of each sub-node is configurable (M=main gauge value, S=number of sub-gauges, s_i=sub-gauge value, w_i=sub-gauge weight).

$$M = \sum_{i=1}^{S} s_i \times w_i$$

- The parameter mappings are completely configurable. This includes what parameter gets mapped to the main node color, the main node angle, and the sub-gauge angle/color.

- The number of time periods represented by the rings in the main gauge, i.e., the number of rings, is configurable (R=radius of the main gauge, p=number of time periods, t=thickness of each ring).

$$t = \frac{2\pi \times R}{p}$$

- The duration of a time period is configurable. This impacts the duration of time represented by each ring in the main node as well as the duration of time that is encompassed by the represented data values. The time periods can be fixed or geometric (T=accumulated thickness, a=initial value, r=ratio):

$$T = t \times p, \qquad fixed$$

$$T = \sum_{i=0}^{p} (t_i = ar^i), \qquad geometric$$

- All angles follow the standard trigonometric organization. Note that the history rings are always fully mapped so as not to lose history information when current activity is of nominal concern.

$$y_0 = \sin(0)$$
$$x_0 = \cos(0)$$
$$y_i = \sin(\theta)$$
$$x_i = \cos(\theta)$$

In the complete environment selecting a node will bring up a detailed visualization representing the encompassed activity. This is currently related to visualizing and analyzing alerts. Ultimately, the context and focus visualization will be directly tied to the task being performed with the cyber command gauge cluster.

- The implementation supports basic network security and network health parameters, including:
  - Impact assessment score
  - Network impact
  - Memory impact
  - Disk impact
  - CPU impact
  - Vulnerability assessment score
  - Source IP
  - Destination IP
  - Source Port
  - Destination Port
  - Packet type
  - Alert classification
  - Alert priority
  - Date & time
  - Payload length

- Support for a broader array of parameters and application to other domains is designed in but not implemented generically.

Figures 4-6 exemplify the scenario in which the angle and color of each of the nodes is redundantly mapped to the same parameter, overall system impact, for the main node in this example. For the sub-nodes, we assume that both the angle and color are redundantly mapped due to the size of the node. Clearly, alternative-mapping strategies can be used to represent additional parameters.

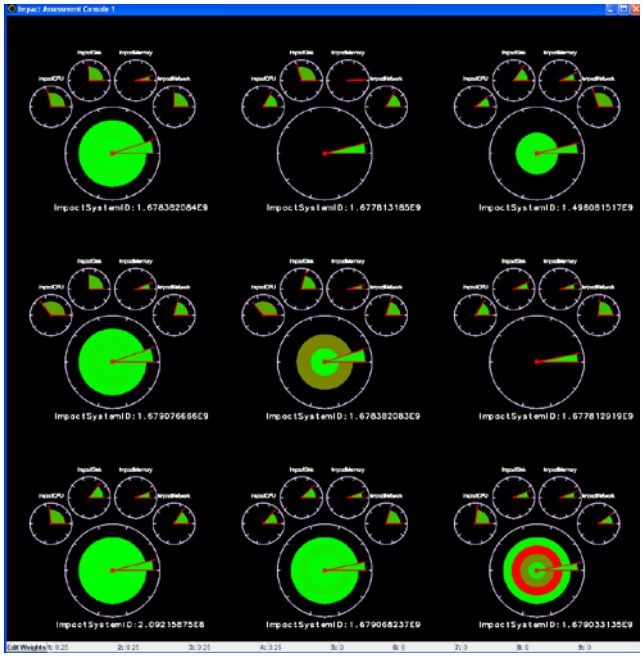

Figure 4. This is the prototype implementation of concept design 2. Originally termed the impact assessment console, we more recently named it the Cyber Command Gauge Cluster to be more representative of its full applicability. Any parameter may in essence be mapped to the gauges and the weighting of the sub-gauges as represented in the main gauge can be specified. Nine gauge clusters are shown with most activity nominal except for one short period in the bottom right gauge cluster.

This redundant mapping results in a low expected impact being bright green but also having no angle. In essence, this reduces the visual impact of the node in this scenario; effectively removing it from the network analyst's or network manager's consideration. Past history clearly stands out identifying when high impact events have been occurring. The historical information allows impact history to be reviewed even when a period of live activity may have been missed. The history information also shows when high impact(s) have occurred over multiple time periods, indicative of sustained activity. Similarly, intermittent high impact events are also clearly identifiable.

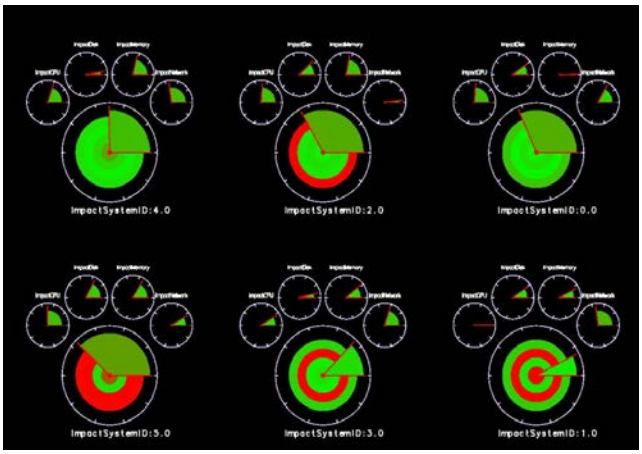

Figure 5. A second example showing six gauge clusters. This example in particular shows far more anomalous activity among all of the represented nodes. Such a display should raise concern among any decision maker. Of particular note is the long and repeated periods of concern in the bottom left gauge cluster.

When a node is representing multiple related components in aggregation, it is important to use the correct aggregation formula. For instance, using the average of the aggregated components is quite typical. However, in the security paradigm the most appropriate aggregation formula is simply to revert to the worst common denominator, i.e., the most significant attack. This is critical since a formula such as using an average of the aggregated components can very easily intentionally or accidentally obfuscate critical attacks.

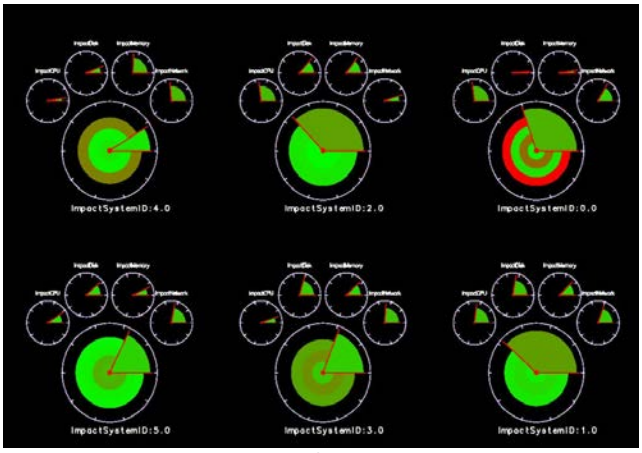

Figure 6. A third example of the Cyber Command Gauge Cluster, also representing six nodes. In general, the activity is innocuous. However, the upper right gauge cluster contains *repeating* periods of anomalous activity that should raise a concern.

4. EVALUATION AND FEEDBACK

Our main source of feedback was the analysts and network managers from Pacific Northwest National Laboratory. These individuals are domain experts within the network analysis arena. In general, the analysts liked the display. The display provides more details about the available metrics than current techniques do. The analyst's comments fell into six categories: interaction, legend information, color, display structure, configurability, and scalability. Obviously, the majority of the comments fell into the display structure category.

Interaction:

- Provide a mechanism for retrieving the weighted average, by either clicking or preferably through mouse over.
    - Have the mouse over display a pie chart in the center of the gauge representative of the contribution of each subcomponent.
- Provide interaction with the dials. Additionally, incorporate a menu setting to enable or disable intractability.
    - Incorporate a scale on the edge of each dial that can be adjusted. This will allow for the scaling of values, resetting the configuration, setting the color range, specifying parameter mappings, etc.
    - Allow selection of each component to lead to a drilled-down view.

Legend Information:

- Incorporate scales and labels particularly time scales
- Incorporate a legend for all components
    - The current display is too black boxed. The display should show the relative contribution of each subcomponent.
    - Specifically, show the weighting of each sub-gauge in the display.
- Provide the ability to see, and possibly change, the time scale

Color:

- Have the ability to choose different fill colors
    - Have someone doing research in the area pick the colors. This may not necessarily be configurable by the analyst since they may choose less desirable color combinations.
    - Color may not be a good indicator. For instance, the navy uses red lights a lot that affects the user's view of the visualization and may affect the interpretation of the visualization.
- There is too much color in the filled version; the color becomes over powering.
- Fade out the fill colors in the center of the gauge, i.e., for older data. As with time periods discussed earlier, this can be either fixed or geometric in nature.

Display Structure:

- Place the 0-degree angle at the bottom rather than follow the trigonometric model. This will result in a wide arc *falling* to the bottom.
- Allow the analyst to control, or specify the mapping, to the thickness and color of the gauge and sub-gauge borders, size, and intensity.
- The percentage representation is good
- Have the most recent data at the edges, creating a tunnel of the data. The history concept is good but might not be clear.
- The top four gauges are good but it might be better limiting them to 180 or 270 degrees rather than using the full 360 degrees.
- The scale for each of the gauges is difficult to determine; i.e., where is 0? This is resolved when the arcs are filled in.

- Make the most recent time frame thicker and the older time frames thinner, i.e., akin to an exponential scale (R=radius of the main gauge, p=number of time periods, t=thickness of each ring).
- Consider reinforcing the occurrence of bad conditions using thicker time frames.

Configurability:

- The gauge clusters should be highly configurable.
- Allow the weights used in calculating the averages to be configurable.
- Analyst must be able to specify what they want as thresholds. This includes things such as the cutoff for bright red alerts, the minimum values to display, etc.

Scalability:

- The analyst needs to be able to update and modify definitions. For example, a cluster of gauges needs to be able to represent a single system, a network of systems, a network of networks, etc. In essence, the user must be able to zoom in and out of a specific network scale.
- Consider the ability of the gauge clusters to display nodes en-masse, for a large number of hosts or networks?
- The gauge clusters do not appear to be compact or significantly scalable.

Summary

The focus of the analyst comments on how to improve the visualization shows that they primarily liked the general concept. There was consistency on many of the basic modifications desired.

5. CASE STUDY

Table 1 exemplifies several tasks a network analyst or network manager might perform and a potential configuration of the visualization for that task. The tasks listed and their explanations are:

- Network Status – provides immediate assessment of the health and usage levels of standard network components. Focused on the overall health of the entire network at a high level. The routers nodes focus on critical routers such as border routers.
- Network Status Zoom – provides an immediate assessment of the health and usage levels of standard network components. Focused on a subset of the entire network. This is essentially a zoom in from the top-level network status display; the same representation can be used for multiple levels of zoom-in. The routers nodes focus on routers between subnets, etc.
- Detailed Attack Analysis – the goal is to provide representations of critical parameters associated with the analysis of an event or otherwise identified attack. The representation should allow the analyst to more readily identify the nature of the attack.
- Host Review – this mode represents details of a host or group of hosts, essentially summarizing the health, performance, and utilization of the host(s).
- Attack Review – attack review can be used in conjunction with detailed attack analysis. Where detailed attack analysis is focuses on providing the analyst with the key components of a current attack, the focus of attack review is providing the analyst with a historical review of the appearance of that attack. This aids in providing historical knowledge of how frequently the attack is being seen. An attack that is being seen frequently, especially recently, or at distinct intervals should receive further attention.
- Network Activity Distribution – network activity distribution aids the analyst in identifying the types of packets being seen on the network such that deviations from the norm can be easily seen.
- Top Talkers – top talkers represents the hosts involved in the most network communication. This can be further subdivided into the top internal nodes, the top external nodes, the top inbound connections, and the top outbound connections.
- Server Status – server status is similar to host review but specifically focusing on servers.
- Service Status – identify the status of individual services network wide. For instance, verify redundancy and utilization of specific services. This essentially amounts to readiness. The network manager typically needs to determine if a service is capable of meeting the needs of the network community.
- Event Prioritization – provide a summary display of current events. Provide situational awareness details to aid rapid prioritization of the events and show the status of the events for remediation.

6. FUTURE WORK

The visualization implementation is still in a fairly prototype state. The goal is to add the robustness implicit in a deployable capability. This robustness requires extensive features beyond just the integrity of the code base, including:

- Selecting an older time-period should show the values of the sub-gauges at that period of time to aid analysis.
- Incorporate the ability to specify fill color values. In particular, the use of pastels may be less off putting to some users.
- Add command console capabilities to allow for the long-term management of events. This would include report tracking to ensure that remediation has occurred.
- Support for a wider array of parameter types is needed, including abstract types. This would include parameters affecting mission readiness such as: number of analysts available, number of systems compromised, number of DoS attacks, etc.
- Support for a large number of simultaneously monitored nodes with aggregation. As mentioned aggregation should be representative of the worst-case scenario.
- Complete quantitative user evaluation of the visualization technique needs to be performed.
- Incorporate support for mobile devices. The design of the Cyber Command Gauge Cluster is uniquely situated to allow support on mobile devices. This will allow decision makers to review the network status on the move.
- Substantial capabilities for the selection and probing of the display to aid the decision maker in understanding what they are seeing is critical.

Table 1: Exemplifying the application of CCGCs to a variety of network monitoring and analysis tasks.								
Task/Goal	**Main Node Color**	**Main Node Angle**	**Sub-Node 1**	**Sub-Node 2**	**Sub-Node 3**	**Sub-Node 4**	**Sub-Node 5**	**Description**
Network Status	Network bandwidth usage	Percentage of expected capacity available	Router one network bandwidth usage	Router one CPU utilization	Router two network bandwidth usage	Router two CPU utilization	Overall impact assessment	This display would be used for rapid assessment of network health and broad identification of areas of congestion or problems.
Network Status Zoom	Network bandwidth usage	Percentage of expected capacity available	Router one network bandwidth usage	Router one CPU utilization	Router two network bandwidth usage	Router two CPU utilization	Overall impact assessment	Apply focus and context techniques and zoom into sub-areas of a network to narrow down problem locations and types.
Detailed Event Analysis	Event severity	Impact assessment	Event classification	Source IP	Destination port	Number of hosts with connected vulnerability		Provide key parameters on a reported event for initial evaluation and aid assessment as to remediation needs.
Host Review	CPU utilization	CPU throughput	Memory utilization	Disk utilization	Network utilization	Video utilization	Vulnerability assessment	Review host health and status. Aggregation with focus and context is critical.
Attack Review	Attack occurrence	Attack Frequency	Attack Priority	Attack Impact	Attack Vulnerability occurrence			Examine the history of an attack to ensure a world view and acquire insight into its characteristics.
Network Activity Distribution	% network utilization	% network utilization	% TCP	% UDP	% SNMP	%HTTP	% Encrypted	The distribution of the network traffic itself can identify anomalies. Aggregation with focus and context is critical.
Top Talkers	Internal host one volume	Internal host one volume	Internal host two volume	Internal host three volume	External host one volume	External host two volume	External host three volume	Identify the most active networks, sub-networks, and hosts.
Server Status	Server one uptime	Server one utilization	Server one network utilization	Server one memory utilization	Server one disk utilization	Server one time since last login	Server one number of running instances	Focus the host review on only servers. Review *server* health and status. Minimize or avoid aggregation due to the critically of the designated systems.
Service Status	Service utilization		Number of service instances	Service readiness	Service capacity	Service availability		Focus on the availability of services specifically. Consider accessibility and vulnerability of a *service* to disruption.
Event Prioritization	Event one predicted impact		Event one vulnerability occurrence	Event two predicted impact	Event three predicted impact	Event four predicted impact	Event five predicted impact	Assist the decision maker in identifying the order in which events should be remediated.

7. CONCLUSIONS

We created effective next generation situational awareness visualization techniques for the representation of cyber data of concern to decision makers. This includes traditional parameters representative of network health such as CPU utilization and network bandwidth utilization but also meta-data such as vulnerability and impact assessment scores. These visualizations were designed following a human in the loop process. We consulted with actual network analysts and network managers as well as other visualization experts during each phase of the design. The developed visualization techniques go a long way towards improving the cyber decision-making challenges being seen in today's network environments.

Analyst interviews identified the basic requirements, critical parameters, and characteristics needed for the next generation of cyber situational awareness visualizations for decision makers. These analyst interviews directly resulted in the generation of the visualization design that was the focus of this research. This visualization designed meets one of the principal needs identified by the analysts, namely, the summary representations of cyber status for immediate short-term analysis. An additional advantage of the summary representation is its direct solution to the scalability issues inherent in cyber situational awareness.

The immediate assessment situational awareness visualization technique we proposed here essentially matches the perception level in Endsley's model, namely providing for perception of events. The sub-gauges provide a limited capability for level 2 of Endsley's model, namely comprehension. Additionally, we provide examples of how level 3 in Endsley's model, namely projection, can be supported in the new visualization designs. This is primarily incorporated through the representation of vulnerability and impact assessment values [6].

While the presented mockups and prototype were designed for cyber situational awareness for decision makers, they are in fact designed to be completely generalizable. The main issue will be with the implementation and the need to support generalizable data in the long term.

8. ACKNOWLEDGEMENTS

This work was supported by AFRL [grant number #FA8750-07-C-0163] at Utah State University before being completed at the Army Research Laboratory. The project supported a number of students in significant roles and many more in minor roles. The students with major roles included: Anusha Davuluri, Srinidhi Kakani, Sarah Moody, Steena Montiero, Rian Shelley, Chris Harris, Anupama Biswas, RB Whitaker, Stephen Miller.

9. REFERENCES

1. Adam, E. C. (1993), "Fighter cockpits of the future," *Proceedings of 12th IEEE/AIAA Digital Avionics Systems Conference (DASC)*, pp. 318-323.

2. Anita D'Amico, Daniel Tesone, Kirsten Whitley, Brianne O'Brien, Emilie Roth, "Understanding the Cyber Defender: A Cognitive Task Analysis of Information Assurance Analysts," Report No. CSA-CTA-1-1. Secure Decisions. Funded by ARDA and DOD.

3. Anita D'Amico, Michael Kocka, "Information Assurance Visualizations for Specific Stages of Situational Awareness and Intended Uses: Lessons Learned," *IEEE Workshops on Visualization for Computer Security* (VizSec'05), p. 13, 2005.

4. Daniel M. Best, Shawn Bohn, Douglas Love, Adam Wynne, and William A. Pike. 2010. "Real-time visualization of network behaviors for situational awareness," In *Proceedings of the Seventh International Symposium on Visualization for Cyber Security* (VizSec '10).

5. Endsley, M. R. (1995b), "Toward a theory of situation awareness in dynamic systems," *Human Factors*, 37(1), pp. 32-64.

6. Robert F. Erbacher, "Visual Situational Awareness for Vulnerability and Impact Assessment," AFRL Final Report, Final Report number in DTIC AFRL-RI-RS-TR-2008-269, C Distribution Restrictions, October 2008.

7. Robert F. Erbacher, Deborah A. Frincke, Sarah J. Moody, Glenn Fink, "A Multi-Phase Network Situational Awareness Cognitive Task Analysis," *Information Visualization Journal*, pp. 204-219, 2010.

8. Robert F. Erbacher, Deborah A. Frincke, Sarah J. Moody, Glenn Fink, "Cognitive Task Analysis of Network Analysts and Managers for Network Situational Awareness," *Proceedings of the SPIE 2010 Conference on Visualization and Data Analysis*, Santa Clara, CA, January 2010, pp. 75300H-1-75300H-12.

9. Robert F. Erbacher and Georges G. Grinstein, "Issues in the Development of 3D Icons," *Visualization in Scientific Computing*, Springer-Verlag, 1995, pp. 109-123.

10. Foresti, S., Agutter, J., Livnat, Y., Erbacher, R. and Moon, S. (2006) Visual correlation of network alerts. *Computer Graphics and Applications* 26(2): 48–59.

11. Stefano Foresti and Jim Agutter, "Cognitive Task Analysis Report," University of Utah, CROMDI.. Funded by ARDA and DOD.

12. Salim Hariri, Guangzhi Qu, Tushneem Dharmagaddam Modukuri Ramkishore, Cauligi Raghavendra "Impact Analysis of Faults and Attacks in Large-Scale Networks," *IEEE Security and Privacy*, September/October 2003, pp. 49-54.

13. Will Iverson: *Hibernate: A J2EE Developer's Guide*, Addison Wesley Professional, 2004.

14. Jajodia, S., Liu, P., Swarup, V., and Wang, C., *Cyber Situational Awareness: Issues and Research*, Springer, 2009.

15. Kiran Lakkaraju, William Yurcik, and Adam J. Lee. 2004. NVisionIP: netflow visualizations of

system state for security situational awareness. In *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security* (VizSEC/DMSEC '04).

16. Nusinov, M.; Yang, S.J.; Holsopple, J.; Sudit, M.; , "ViSAw: Visualizing threat and impact assessment for enhanced situation awareness," *Military Communications Conference, 2009. MILCOM 2009. IEEE* , vol., no., pp.1-7, 18-21 Oct. 2009.
17. Patro, A., "Pixel Oriented Visualization in XmdvTool," *Master Thesis*, Worcester Polytechnic Institute, Worcester, MA, August 2004.
18. Phister, P. W., Fayette, D. Krzysiak, E., "CyberCraft: Concept Linking NCW Principles with the Cyber Domain in an Urban Operational Environment," AF Research Lab, Presented at the DODCCRP Conference 2005.
19. Phister, P. W., Fayette, D. Krzysiak, E., "The CyberCraft Concept Linking NCW Principles with the Cyber Domain in an Urban Operational Environment," *MILITARY TECHNOLOGY,* Vol. 31, No. 9, 2007, pp. 123-131.
20. Salerno, J., "Measuring situation assessment performance through the activities of interest score," *Information Fusion, 2008 11th International Conference on* , vol., no., pp.1-8, June 30 2008-July 3 2008.
21. Mike Schiffman, Gerhard Eschelbeck, David Ahmad, Andrew Wright, Sasha Romanosky, "CVSS: A Common Vulnerability Scoring System", National Infrastructure Advisory Council (NIAC), 2004.
22. Streilein, W.; Kratkiewicz, K.; Sikorski, M.; Piwowarski, K.; Webster, S., "PANEMOTO: Network Visualization of Security Situational Awareness Through Passive Analysis," *Information Assurance and Security Workshop, 2007. IAW '07. IEEE SMC* , vol., no., pp.284-290, 20-22 June 2007.
23. Huiqiang Wang; Ying Liang; Haizhi Ye, "An Extraction Method of Situational Factors for Network Security Situational Awareness," *Internet Computing in Science and Engineering, 2008. ICICSE '08. International Conference on* , vol., no., pp.317-320, 28-29 Jan. 2008.
24. Xiaoxin Yin, William Yurcik, Michael Treaster, Yifan Li, and Kiran Lakkaraju. 2004. VisFlowConnect: netflow visualizations of link relationships for security situational awareness. In *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security* (VizSEC/DMSEC '04).
25. http://www.vizsec.org/vizsec-events-2/
26. http://www.first.org/cvss/
27. http://www.hibernate.org/
28. http://www.mysql.com/
29. Visualization: Gauge, http://code.google.com/apis/chart/interactive/docs/gallery/gauge.html