Towards a Model-Based Cyber Defense Situational Awareness Visualization Environment [*]

Gabriel Klein, Christoph Ruckert, Michael Kleiber, Marko Jahnke, Jens Toelle
Fraunhofer FKIE
Wachtberg
GERMANY

firstname.lastname@fkie.fraunhofer.de

1 *ABSTRACT*

A wide variety of security components such as firewalls, anti-virus scanners, or intrusion detection systems are extensively used in computer networks for providing information assurance. The incident messages generated in case these components detect certain events are typically processed by a human operator at a central security console. The types of visualizations presently used for the analysis do not support the establishment of situational awareness with regard to information security. If – as is common with commercial off-the-shelf incident analysis tools – the event messages generated by security components are displayed in the form of scrollable message lists, detailed reports or colored status icons for each network device, the user is inundated with a vast amount of data that needs to be processed before any meaningful action can be taken against detected threats.

Due to the fact that no correlation with any other external information is carried out, the important messages cannot be easily separated from those less important and the visualization of the situation cannot be adapted accordingly. Including a detailed model of the computer network to be protected and all its resources with their various interdependencies in the analysis process and basing the visualization on an intelligent interpretation of the current model instances can significantly improve the expressiveness of the operational picture with regard to cyber defense and aid in the creation of cyber situational awareness.

We have identified different use cases for cyber defense visualization. Based on these, different display modes and interface elements need to be offered to the user. The common base of these display modes is the underlying network model which changes over time depending, among others, on incoming event messages. Yet, the modalities of interaction and information requirements are inherently different for different types of users, e. g. a system administrator responding to an incident will need a more detailed view of the system than a CIO tasked with network planning. Thus, one of the main challenges is the fusion and transition between the different types of network visualizations. We are therefore investigating novel visualization techniques such as stereoscopic 3D displays, accentuation through preattentive features, and modified polar diagrams with a view to better capture the operator's attention and enabling a better separation between the important and less important elements on the display. Hence, human pattern matching capabilities can be optimally supported.

2 INTRODUCTION

A wide variety of security components is deployed in computer networks to provide information assurance. Among others, firewalls, intrusion detection/prevention systems and virus scanners are extensively used. So-called *Security Incident Event Message* (SIEM) and *Unified Threat Management* (UTM) systems are among the most wide-spread tools for centrally monitoring event messages from these security components. They allow for the collation and analysis of these messages, e. g. normalization or

[*] Published in: Proc. of the RTO Workshop "Visualising Networks: Coping with Chance and Uncertainty". Rome, NY, USA, Oct. 2010.

correlation of multiple messages. Results are then displayed at a security console workstation.

Visualization of IT security situations as it is currently performed has a number of drawbacks. The types of visualization presently used are not conducive to the establishment of a situational awareness. This concept, originally proposed by Endsley [1, 2] for aircraft pilots, involves the observation of objects in the vicinity, understanding their interdependencies and interactions, and the prediction of their behavior in the immediate future. It can be similarly used in a cyber defense context where the objects correspond to managed network devices, e. g. servers, routers, or switches.

If the event messages generated by security components are displayed in the form of scrollable message lists, detailed reports or colored status icons for each network device, the user is inundated with a vast amount of data that needs to be processed before any meaningful action can be taken against detected threats. Also, important information is often lost among the flood of non-important messages. Figure 1 shows some popular visualization methods (Cisco IPS, OSSIM – Open Source Security Information Management, phpLogCon).

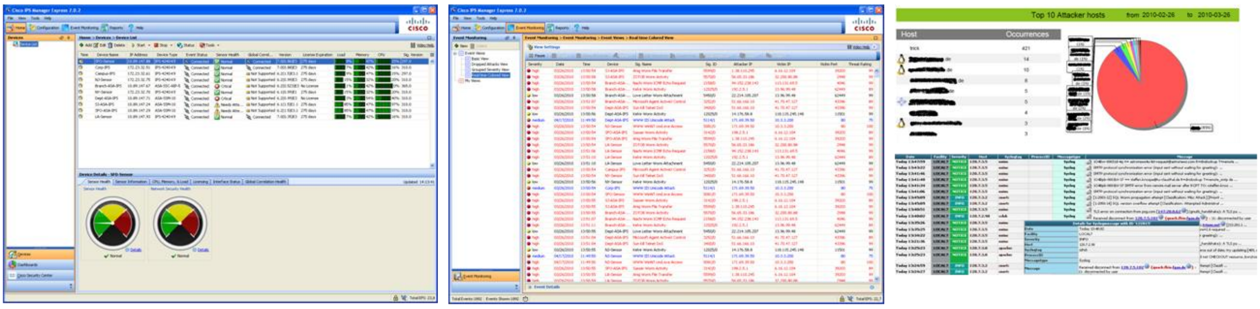


Figure 1: Popular visualization techniques.

Beyond an analysis with regard to message content, no further correlation is typically performed, especially with external data such as business process information. Therefore and because resource interdependencies are not analyzed and adequately portrayed, a coherent depiction of the overall security situation is impossible.

3 MODEL-BASED CYBER DEFENSE SITUATIONAL AWARENESS

An appropriate visualization of network structure and background information along with security-related data can immensely improve an operator's situational awareness. Previous work has focused solely on the visualization aspect and less on developing an underlying IT security situation model enabling an intuitive expert-level visual display with regard to cyber defense.

- The security events analyzed by SIEM/UTM systems is directly related to computer networks whose structure is intuitively displayed in the form of graphs [3]. To further increase the operator's intuition when viewing the network structure, IP network components can be geographically arranged using GeoIP databases. Overlay maps of the network deployment area support this effect.

- To reduce the amount of data to be processed by the operator, information about network structure and aspects of the overall network management situation is provided on an as-needed basis [4]. Other techniques for data reduction can be found in the database (data aggregation) and sensor fusion domains [5].

A model supporting situation awareness with regard to cyber defense needs to combine background knowledge about business processes and information flow in the specific context with information about protected networks and the resources it comprises along with their interdependencies. The current situation can then be derived from a known initial situation combined with information about situation changes that happened over time. Here, situation changes are induced by event messages from security components.

In the information assurance domain, three security metrics are often discussed: availability, integrity and confidentiality. Protection mechanisms are designed to safe-guard these properties of computing resources and data. Determining the effect certain actions or inactions have on these so-called resource status indicators is an important challenge, because it can potentially affect the selection of measures against attacks and thus the speedy mitigation of their effects.

GrADAR (Graph-based Automated DoS Attack Response, [8, 9, 10]) is a methodology for assessing the effects of attack countermeasures on the availability of resources in a networked scenario by evaluating their effects prior to their real-world application in a model that is updated during run-time. The availability of the key resources is measured using distributed sensor components in the network. Based on these values, GrADAR suggests the most appropriate alternative from a given set of network reconfiguration actions. Different metrics for quantifying the attack and response effects may be used, including the expected response success, application costs and durability. Due to its model-based character representing availability dependencies between resources, GrADAR is inherently suited as the back-end model for managing cyber defense situational awareness.

Figure 2 shows a canonical workflow for maintaining and using such a model-based situational awareness.

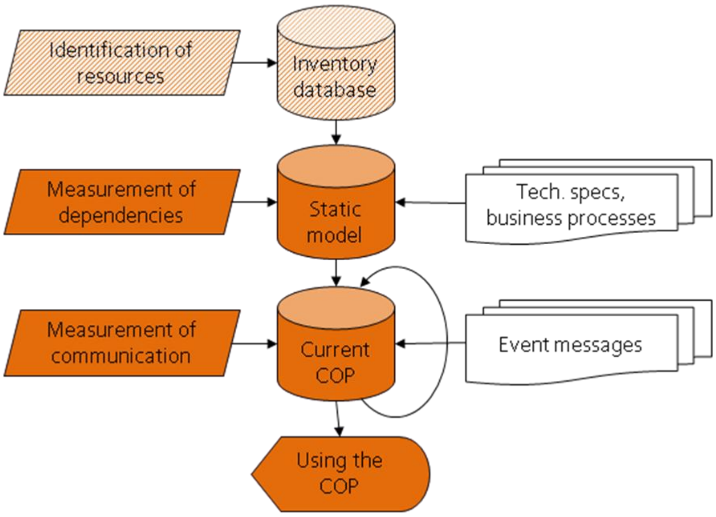

Identification of resources
Inventory database
Measurement of dependencies
Static model
Tech. specs, business processes
Measurement of communication
Current COP
Event messages
Using the COP

Figure 2: Overview of model-based situational awareness.

The initial step in the creation of the model is the identification of resources that are to be protected and the formation of an inventory database. Subsequently, dependency relationships between these resources with respect to the above mentioned status indicators (availability, in the GrADAR case) needs to be determined, for example by performing a sensitivity analysis. Combined with background information about these resources, the so-called static model is formed. This static model reflects the ideal state of the protected system. Run-time measurements of communication between resources and event messages from deployed security systems provide the basis for the information assurance common operational picture (COP). Over time, this model needs to be updated dynamically. These updates reflect structural changes such as, for example, the migration or replication of servers, and resource status changes such as impaired availability.

4 NEXT-GENERATION VISUALIZATION ENVIRONMENT

According to Endsley, situation awareness is a human state of mind which computers can only aid in achieving. As the eye is the primary human perceptive organ, cyber defense visualization is of vital importance. The model described in the previous section reflects all aspects of the current security situation. Thus, users' unique requirements with regard to information content form the basis of any visualization. In this section we discuss these requirements, their impact and incorporate lessons learnt from previous visualization projects. We finally provide concrete implementation ideas.

Use case-driven visualization design

A cyber defense situational awareness visualization environment should assist its user in making decisions with respect to the defended systems. However, there is a multitude of users which can potentially interact with the system. We have identified different use cases, each with different requirements with regard to information content and visualization type. For example, a system administrator tasked with responding to currently active threats requires a finer granularity of presented information than a member of middle management who is interested in the abstract network topology. Examples for tasks and the corresponding information and visualization requirements of these two users are presented in more detail in Table 1 and Table 2.

Table 1: Information and visualization requirements for user group system administrator.

User	Tasks	Information requirements	Visualization requirements
System administrator	• Network attack response • Reconfiguration of resources for attack mitigation • What-if analyses with respect to reconfiguration • Trend analyses for resource status indicators based on past event messages	• Resource status indicator values • Concrete resource status indicator dependency relationships • Location of resources with regard to network zone separation • Rapid alerting in case of attacks	• Georeferenced map with respect to system location (e. g. building layout) • Cyber-referenced map, e. g. graph-based map of network • Resource dependency visualization • Arbitrary detail granularity • Easy editing of resource map and inter-dependencies

Table 2: Information and visualization requirements for user group management member.

User	Tasks	Information requirements	Visualization requirements
Management	• Generation of reports for marketing purposes • Equipment procurement planning	• Representation of the network topology with the corresponding status indicators • Comparison which user groups needs which service • High-level resource dependencies	• Georeferenced map with respect to different logical business structures • Limited granularity

The premise of this use case-driven development approach is to display as little information as possible but as much as necessary for the currently performed task. Thus, the user interacting with the system is presented only with important data and not distracted by less important aspects.

We are aware that the identified use cases and the corresponding requirements are of a preliminary nature and future research is necessary to determine the exact usage scenarios along with the required visualization elements. These are most likely highly dependent on the systems to be protected. A further challenge is the creation of an integrated display environment that supports seamless transition between the different display options.

Novel visualization techniques

Next-generation visualization types should focus the user's attention and optimally support the human pattern matching capability which is extremely well suited for detecting anomalies. We are examining innovative visualization techniques enabling such intuitive interaction with the system. In this section we discuss a few examples.

Multi-dimensional polar diagrams are an established medium for indicating anomalies. Originally developed for use in nuclear power plants [6], their usefulness was also shown for air combat situations [7]. Figure 3 depicts how the use of shapes in these polar diagrams indicates either a normal situation (symmetry) or abnormalities (asymmetry) for selected attributes relevant to aircraft control.

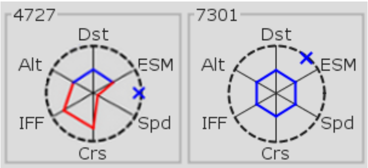


Figure 3: Polar diagrams aid in recognizing deviations from normal behavior (right: normal state, left: deviation).

In the cyber defense context, modified polar diagrams can be used to display the values of important status indicators for selected network or computing resources. Figure 4 shows polar diagrams indicating the availability, integrity and confidentiality of a resource. Here, an equilateral triangle indicates the optimal situation in which none of the status indicators is compromised (left). The degree of compromise of certain indicators is highlighted by a variable amount of stretch in the triangle (center, right). The additional use of color reinforces this.

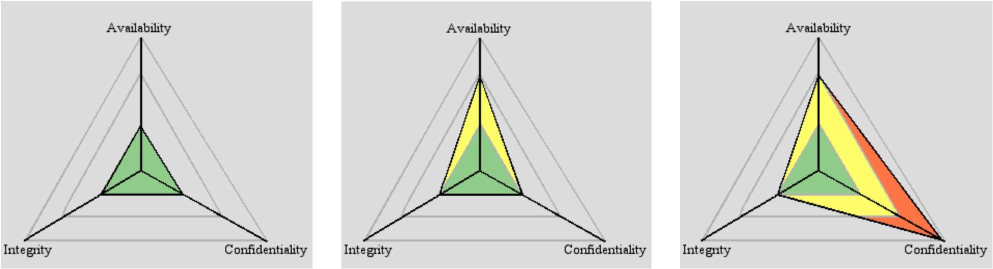


Figure 4: Modified polar diagrams for the three status indicators availability, integrity and confidentiality (left: normal state, middle: slight deviation, right: large deviation)

A set of visual properties that can be very rapidly and accurately perceived by the low-level visual system are called preattentive features [11]. The *accentuation of these preattentive features* can be intuitively used to indicate to an operator that a specific visual element is important and warrants further attention. Simple examples of preattentive properties are color and form of objects (as shown in Figure 5).

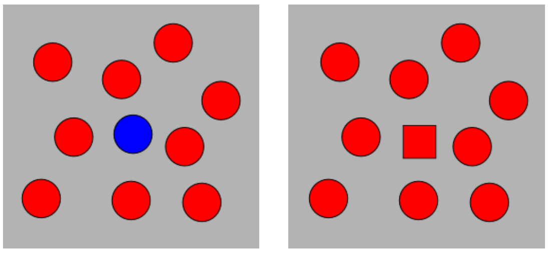


Figure 5: Accentuation of preattentive features (left: color, right: shape).

Another method of focusing the operator's attention on a specific display region is the use of *stereoscopic effects* [12]. Figure 6 shows an example of this. By adding varying degrees of drop shadows to displayed objects, the user-perceived depth or distance of these objects can be intelligently controlled. The user's intuition is then responsible for categorizing near and far objects into important and not so important.

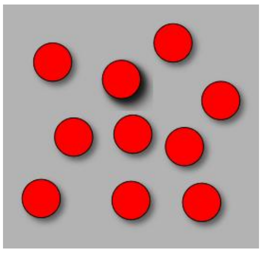


Figure 6: Stereoscopic three-dimensional focusing on a single element.

A similar effect can be achieved by red/green color shifting (as in some analog 3D movies) or light polarization. However, these two methods require additional accessories either for the viewer or the display equipment, and as such, are not as intuitive to use.

In computer network defense, these focusing mechanisms can be used to indicate to an operator, which resources are currently in need of attention. A different approach to achieving the same result is the distraction from less important objects. Here, *blurring of objects* is an ideal method of indicating to the human eye that an object is less important than another. In map- or graph-based displays, network resources can be blurred or "grayed out" to indicate either that they are not relevant to the currently selected view or that none of the predefined status indicators for that resource deviate from the norm. Alternatively, in the context of resource interdependency analyses, blurred objects can be those that do not possess any relationships to the currently selected resource.

To roughly indicate the status of a resource, it has been shown that traffic light analogies are very reliable. Here, a red light indicates a critical condition, amber denotes required attention and green implies that the resource is unimpaired (see Figure 7).

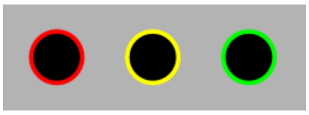


Figure 7: Traffic light color analogy to indicate approximate resource status.

Lessons learnt in previous projects

In a previous project, a situation report needed to be displayed on screen. This was realized using a 30-inch screen partitioned according the schematic shown in Figure 8. Here, the actual situation, i. e. own forces, are displayed in the center (area A). Area D contains brief global status data such as date and time. The content of the other areas is user dependent and can range from the display of custom information to an editing area. In this case, the size of the different areas reflects the relative importance of the display element.

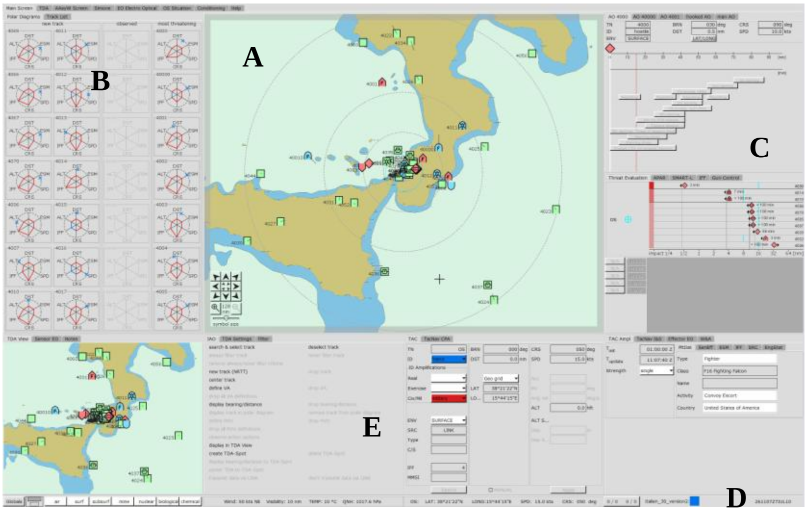


Figure 8: Partitioning of an on-screen situation report system [13].

Possible implementation of visualization environment

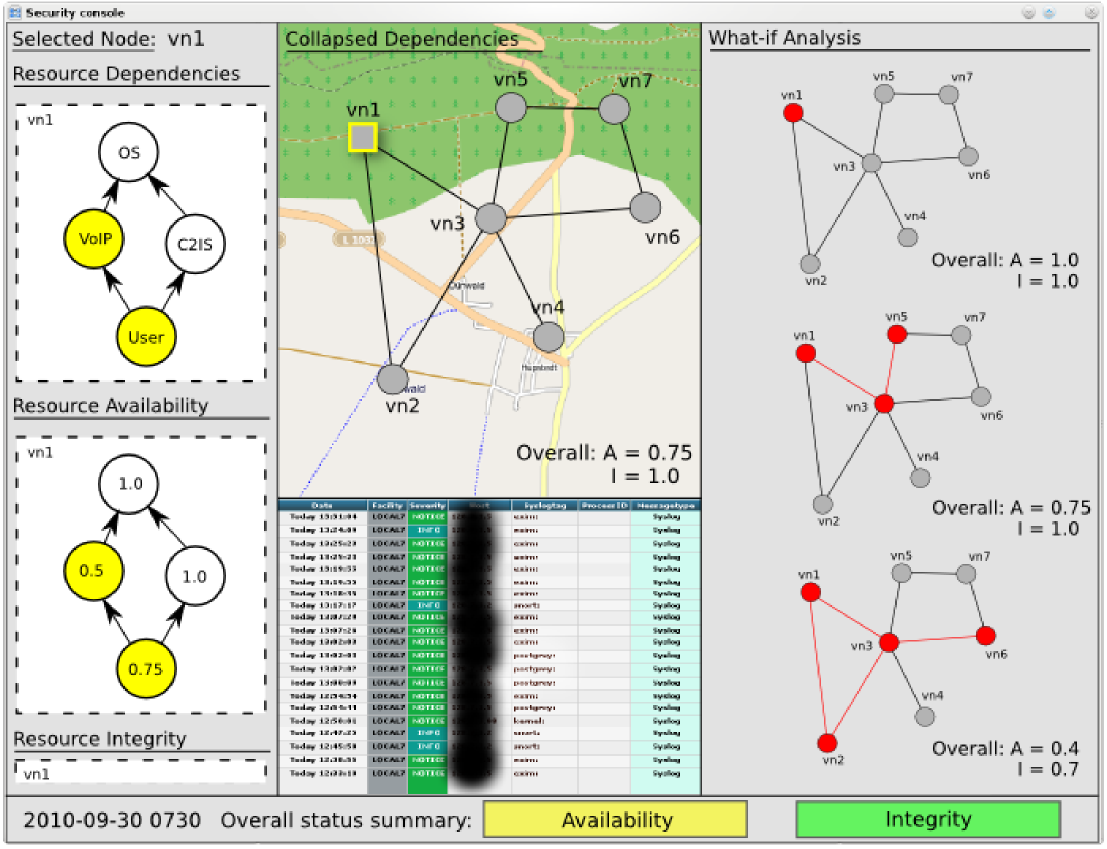
Since the research projected described in the previous section was conducted according to user-centric international standards [14], feedback was incorporated into the prototype directly, thus ensuring that all developed interaction components conform to user requirements. Therefore, a cyber defense visualization environment catering to comparable operators could similarly consist of different-sized areas as depicted in Figure 8. Table 3 shows an overview of the screen regions and the interface elements they could contain.

Table 3: Example visualization and interaction element placement in a cyber defense visualization environment.

Screen region	**Visualization elements**	**Interaction elements**
A	• Map of resources (cyber-, geo- or organizational referencing)	• Zoom slider for modification of abstraction level (e. g. ISO/OSI layer) • Multi-resource selection tool
B	• Internal resources for nodes selected in pane A along with their interdependencies • Dependency analysis: emphasize resources dependent on currently selected resource	• Selection tool for dependency analysis
C	• Parallel display of multiple possible reconfiguration/attack response options (what-if analysis) • Root-cause analysis	• Edit mode for quick modification of resource status indicators and resource dependencies (what-if analysis)
D	• System-global status data, e. g. date and time • Global alert status • Alert field displaying result of event message trend analysis (rapid alerting functionality)	• User group selection tool

E	• Status indicators for resources selected in pane A • Dashboard showing details of key resources • List of event messages • Display of event message that lead to last change in model state	• Highlight mode: emphasize messages' originators in pane A

To support user interaction with such a visualization environment, the human-machine interface can be realized either as a touch screen or with the help of input devices such as mice or graphics tablets. Figure 9 shows a mockup of the cyber defense situational awareness visualization environment.



Date	Facility	Severity	Host	Syslogtag	Process ID	Messagetype
Today 13:31:04	LOCAL7	NOTICE	[redacted]	exim:		Syslog
Today 13:24:09	LOCAL7	INFO	[redacted]	exim:		Syslog
Today 13:25:23	LOCAL7	NOTICE	[redacted]	exim:		Syslog
Today 13:25:23	LOCAL7	NOTICE	[redacted]	exim:		Syslog
Today 13:19:33	LOCAL7	NOTICE	[redacted]	exim:		Syslog
Today 13:19:33	LOCAL7	NOTICE	[redacted]	exim:		Syslog
Today 13:18:35	LOCAL7	NOTICE	[redacted]	exim:		Syslog
Today 13:17:17	LOCAL7	INFO	[redacted]	snort:		Syslog
Today 13:07:29	LOCAL7	NOTICE	[redacted]	exim:		Syslog
Today 13:07:29	LOCAL7	NOTICE	[redacted]	exim:		Syslog
Today 13:02:03	LOCAL7	NOTICE	[redacted]	exim:		Syslog
Today 13:02:03	LOCAL7	NOTICE	[redacted]	postgrey:		Syslog
Today 13:07:07	LOCAL7	NOTICE	[redacted]	postgrey:		Syslog
Today 13:00:03	LOCAL7	NOTICE	[redacted]	postgrey:		Syslog
Today 12:54:34	LOCAL7	NOTICE	[redacted]	exim:		Syslog
Today 12:54:11	LOCAL7	NOTICE	[redacted]	postgrey:		Syslog
Today 12:56:01	LOCAL7	NOTICE	[redacted]	kernel:		Syslog
Today 12:47:23	LOCAL7	INFO	[redacted]	snort:		Syslog
Today 12:45:58	LOCAL7	INFO	[redacted]	snort:		Syslog
Today 12:38:35	LOCAL7	NOTICE	[redacted]	exim:		Syslog
Today 12:23:10	LOCAL7	NOTICE	[redacted]	exim:		Syslog

2010-09-30 0730 Overall status summary: Availability Integrity

Figure 9: Mockup of cyber defense situational awareness visualization environment.

5 CONCLUSION AND NEXT STEPS

A wide variety of security systems such as firewalls or IDSs is deployed today. Even though, the event messages generated by these components are often aggregated at a central location and presented to the operator, little or no correlation takes place with external information such as business processes in the deployment location. Also, popular cyber defense visualization tools do not aid the establishment of cyber security situation awareness. As a result, it is made difficult for security personnel to take optimal action against detected threats or other critical situations. To remedy this, we have proposed the concept of model-based cyber defense situational awareness in which a model represents the current security situation of all protected resources. This model is updated over time according to event messages received from security components on the one hand and appropriate available background information on the other hand. Based on this model, intuitive visualization techniques can be employed to assist security operators with their tasks, be they mitigation of attack effects, initiation of countermeasures or simply network information assurance provisioning.

Thus far, our work has been of a conceptual nature. Three aspects are central to proposed future work:

1. Improvement of the cyber defense situational awareness model with respect to the incorporation of integrity and other information assurance metrics.

2. Prototypical demonstrable implementation of network security visualization techniques.

3. Inclusion of operator feedback into the further development process.

REFERENCES

[1] M. Endsley. Theoretical Underpinnings of Situation Awareness: A Critical Review. In: M. R. Endsley & D. J. Garland (Eds.), Situation Awareness Analysis and Measurement. Mahwah, NJ, USA, 2000.

[2] M. Endsley. Situation Awareness: Progress and Directions. In: S. Banbury & S. Tremblay (Eds.), A Cognitive Approach to Situation awareness: Theory, Measurement and Application, pp. 317–341. Aldershot, UK, 2004.

[3] G. Conti. Security Data Visualization. No Starch Press, San Francisco, CA, USA, 2007.

[4] J. Glanfield, S. Brooks, T. Taylor, D. Paterson, C. Smith, C. Gates, J. McHugh. Overflow: An Overview Visualization for Network Analysis. In: Proc. of the 6. International Workshop on Visualization for Cyber Security, 2009.

[5] J. Bjorke. Reduction of complexity: an aspect of network visualization. In: Visualising Network Information. NATO RTO-MP-IST-063, 2006.

[6] D. Woods, J. Wise, L. Hanes. An Evaluation of Nuclear Power Plant Safety Parameter Display Systems. In: Proc. of the 25th Annual Meeting of the Human Factors Society, Santa Monica, CA, USA, 1981.

[7] M. Grandt, H. Distelmaier, C. Pfendler. A Knowledge-based Human-Machine Interface for Future Naval Combat Direction Systems. In: Proc. of the NATO-RTO IST 043/RWS-006 Workshop Visualisation and the Common Operational Picture (COP), Toronto, Canada, 2004.

[8] M. Jahnke, J. Tölle, C. Thul, P. Martini. Validating GrADAR – An Approach for Graph-based Automated DoS Attack Response. In: Proc. of the 34. IEEE Conference on Local Computer Networks (LCN 2009), Zürich, 2009.

[9] G. Klein, M. Jahnke, J. Tölle, P. Martini. Enhancing Graph-based Automated DoS Attack Response. In: C. Czossek, K. Geers (Eds.), The Virtual Battlefield: Perspectives on Cyber Warfare, Cooperative Cyber Defence Centre of Excellence (CCD-CoE), Tallinn, Estonia, 2009.

[10] G. Klein, A. Ojamaa, P. Grigorenko, M. Jahnke, E. Tyugu. Enhancing Response Selection in Impact Estimation Approaches. To be published in: Proc. of the Military Communications and Information Systems Conference MCC 2010, Wroclaw, Poland, September 2010.

[11] A. Treisman. Preattentive processing in vision. Computer Vision, Graphics and Image Processing 31 (1985), 156–177.

[12] K. Nakayama, G. H. Silverman. Serial and parallel processing of visual feature conjunctions. 1986.

[13] A. Kaster, J. Maas. Supporting Human Decision Making and Control in Naval Combat Direction Systems. In: Proc. of 27th European Annual Conference on Human Decision-Making and Manual Control (EAM'08), Delft, Netherlands, 2008.

[14] DIN EN ISO 13407. Human-centred design processes for interactive systems. Beuth, Berlin 1999.