

This work was written as part of one of the author's official duties as an Employee of the United States Government and is therefore a work of the United States Government. In accordance with 17 U.S.C. 105, no copyright protection is available for such works under U.S. Law.

Public Domain Mark 1.0

<https://creativecommons.org/publicdomain/mark/1.0/>

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

Please provide feedback

Please support the ScholarWorks@UMBC repository by emailing scholarworks-group@umbc.edu and telling us what having access to this work means to you and why it's important to you. Thank you.

Enhancing Cyber Defense Situational Awareness Using 3D Visualizations

Kaur Kullman^{1,2}, Jennifer Cowley¹ and Noam Ben-Asher¹

¹Computational and Information Sciences, US Army Research Laboratory, Adelphi, USA

²Tallinn University of Technology, Tallinn, Estonia

kaur@ieee.org

jennifer.a.cowley.civ@mail.mil

noam@noamba.com

Abstract: The human visual system is generally more adept at inferring meaning from graphical objects and natural scene elements than reading alphanumeric characters. Graphical objects like charts and graphs in cybersecurity dashboards often lack the requisite numbers of features to depict behaviors of complex network data. For example, bar charts afford few features to encode a panoply of parameters in network data. Furthermore, dashboard visualizations seldom support the transition of human work from situation awareness building to requisite responses during intrusion detection events. This research effort aims to identify how graphical objects (also referred as data-shapes) depicted in Virtual Reality tools, developed in accordance with an analyst's mental model of an intrusion detection event, can enhance analyst's situation awareness. We demonstrate the proposed approach using Locked Shields 16 CDX network traffic. Implications of this study and future case study are discussed.

Keywords: visualization, decisionmaking, mental model, analysts, virtual reality, cybersecurity

1. Introduction

The quantity of information collected by network monitoring tools has increased steadily in parallel to the society's growing dependence on information technology (Kaisler, et al., 2014). The use of monitoring tools to maintain Cyber Defense Situational Awareness (CDSA) is a prominent task among cybersecurity analysts who work in a Security Operations Center (SOC) or Network Operations Center (NOC). One way to potentially mitigate the increasing workload of the cybersecurity analyst is to visualize the network architecture and types of data traversing through it. Typical dashboard charts and graphs (e.g., line charts, node diagrams, etc.) could overlay this architecture. However, visualizing data acquired from a wide range of sources on charts and graphs in isolation may stymie the rapid acquisition of information about changing network behaviors because: (i) graphs and charts have limited scalability for networks complexity and size, (ii) commonly user graphs/charts often fail to account for the highly dynamic nature of the cyber environment, and (iii) detection of threats demand the ability to notice and highlight small anomalies that tend to disappear when visualizing large volumes of data (Schoenwaelder, et al., 2007). What is needed is a set of new types of graphs and charts, called visualizations herein, which flex with the changing parameter space while pictorially representing of dynamic, evolving network behavior. The purpose is to expedite analyst's situation awareness by designing a visualization that reflects the analyst's mental model of the network environment.

Anecdotally, the common NOC/SOC analyst's workstation often includes command line tools juxtaposed to dashboard tools; some dashboards allow the user to interact (e.g., filter, drill, etc.) with the data depicted in the chart or graph. Dashboards usually provide an array of two-dimensional (2D) graphs and charts that summarize different types of network data. Network data has a high-parameter space and is often multidimensional, leaving the dashboard designer to fit multidimensional network data into 2D visualizations. If NOC/SOC analysts have multidimensional mental models network behaviors, then some conversions of 2D may occur. This conversion renders a measurable perceptual lag and often augments subjective mental workload. The goal of this study is to design a visualization aligned with analyst's mental model of the network environment, which facilitates a faster and more accurate detection of network behavioral change (Kandel, et al., 2012). Our approach is to utilize a virtual environment to create new 3D visualizations with the capacity to encode a panoply of data parameters into depth, spatial and temporal cues.

In this study, we describe the development of a 3-dimensional (3D) visualization technique for CDSA. First, we describe the technique and application architecture. Then, we demonstrate how it can be used by network operators to obtain and maintain CDSA using data from the Locked Shields 2016 cyber defense exercise as an

example. Finally, we discuss the integration of this visualization with a virtual reality, interactive environment as well as plans for future evaluation.

2. Human visual perception

The human visual system has a finite amount of visual attention resources used to view the data presented on a computer screen (Schneider, Dumais, & Shiffrin, 1982). Hence, the human visual system is one of the major bottlenecks of information flows between a computer system to a human analyst (refer the Communication–Human Information Processing (C–HIP) model for details (Dejoy, et al., 1999)). Because of this bottleneck, the veracity and comprehensiveness of a human analyst’s mental model about a network event is directly impacted by perceptual bottlenecks. A *mental model* is internal, cognitive representation of the environment based on the acquired information. Then, these models can provide ways to describe, explain, predict, and, sometimes, control the phenomena (Gentner & Stevens, 1983); (Johnson-Laird, 1983) and they are built through direct perception of the environment. Hence, the design of data visualizations can impact the accuracy of an analyst’s mental model development and sustainment (Paradice & Davis, 2008).

Coding information can be used to reduce the chances of perceptual bottlenecks. Visual information can be efficiently augmented in reasoning processes based (See (Paivio, 1991) for an overview on dual-coding and (Baddeley, 2012) for a review on working memory). Furthermore, information can be presented to the analyst in more than one sensory modality to maximize the amount of information perceived in a time epoch. In Human Computer Interaction research, codes are stimuli that represent the smallest unit of information communicated. For example, visual codes within a scatterplot are size, color, shape, proximity, among others. These visual codes are relevant to 2D visualizations but ‘depth’ may be an additional code in 3D environments that can be populated with additional data parameters and impact the interpretation of other codes like proximity. A group of codes representing a large amount of information can be configured to create a visual pattern, which can then be perceived rapidly. This visual pattern, according to Gestalt Psychology, is called *emergent features* (Treisman & Paterson, 1984) because the meta-data patterns emerge from the display of raw data. Meta-data patterns can form the basis of human mental models that analysts use when searching for expected patterns of malicious network behavior as well as represent normal network behavior. Gestalt laws of perception (e.g., Laws of Proximity, Closure) (Ehrenstein, et al., 2003) characterize the natural ways humans perceive information groupings that the interface designer can capitalize on. Poor designs that violate the Gestalt laws of perception could force the analyst into controlled and deliberated processing that consumes attention resources (Schneider, et al., 1982).

Depth perception is facilitated with a set of monocular and/or binocular visual cues that could provide additional codes to depict network information. Monocular depth cues (i.e., light and shading, relative size, interposition, blur, texture gradient, and aerial perspective linear perspective) (Lebreton, et al., 2012) allow for a 3D depiction in a 2D plane (i.e., a page or photograph). These kinds of “3D in 2D” visualizations using monocular cueing were called “perspective views” (Ellis, et al., 1987) or “pseudo 3D” (Lange, et al., 2006). Binocular depth cues use stereopsis to present objects to the viewer that seem to ‘pop out’ from the visual scene. Visualizations with binocular depth cues are called “real 3D” (Lange, et al., 2006). Visual perception of natural 3D scenes is afforded by monocular and binocular depth cues working together (Lee & Lee, 2015).

Perspective (Foyle, et al., 2005) is another 3D technique and design principle which can hamper perception in 3D visualization environments. Upon entering a 3D environment, the analyst is perceiving the environment through the avatar’s eyes or perceiving via a top-down view looking at an avatar that represents themselves. The terminology describing perspectives is non-standard and sometimes obtuse. Human factors research defines *allocentric* views (Klatzky, et al., 1998), also called “through the window” (Brown, 1994) view, as one in which the observer is watching themselves through a viewpoint outside of the body. For example, an avatar representing a human has an allocentric view if the controller manipulates the avatar by watching it from behind. Allocentric is used interchangeably with *geocentric* or *exocentric* views (Klatzky, et al., 1998) or *plan* views (Foyle, et al., 2005). Plan views are allocentric perspectives in which the human is looking down from a higher altitude. Contrast this with *egocentric* views (Klatzky, et al., 1998), also called *immersive* (Brown, 1994) or *inside perspective* (Bryant & Tversky, 1999), such that the controller is seeing the virtual environment through the eyes of the avatar. The type of perspective used for a particular task has been shown to lead to human perceptual and spatial memory errors (Klatzky et al., 1998).

The advantages and disadvantages of depicting data using 3D compared to 2D displays has been studied and debated for decades with no clear resolution. With the rise of more sophisticated augmented reality environments, modern visualization research has re-vamped. The advancement of computing provides some explanations to the discrepancies between recent and dated studies of human performance with 3D visualizations (Smallman, et al., 2001). In some cases, 3D is advantageous because of a lower interpretive effort of perceived 3D information, given the human visualization system is designed to see in 3D (Dennehy, et al., 1994); (Smallman, et al., 2001). Furthermore, 3D visualizations potentially can display more codes with depth cueing compared to 2D displays. However, these benefits are couched in the type of work tasking required to complete with the visualization. Tasks such as altitude extraction, geo-spatial maneuvering, and navigation improve with 3D displays (Burnett & Barfield, 1991) while, there are tasks and environments for which the 2D displays are more advantageous than 3D displays (see (St. John, et al., 2001).

In sum, prior research indicates that while 3D visualizations in virtual reality environments afford more codes to use to depict data, the ways in which those codes are arranged using Gestalt's laws, emergent features and perspectives, determines how best to maximize the amount of data perceived. Communication from the interface to the human analysis involves the clear mapping between a mental model of the data that is expected to be reviewed, and the manner the data is depicted in the visualization (Ehrenstein, et al., 2003). The 3D objects we design must fit the typical mental model building inherent in network defense job tasking. To our knowledge, no prior research has identified whether computer network defense analysts are re-visualizing alphanumeric network data in geospatial patterns in their minds. Furthermore, we have no clarity whether training an analyst to build their mental models on 3D representations of alphanumeric network data will be advantageous to performance. These are assumptions we are exploring in our research. Although prior research has described basic Computer Network Defense (CND) operations and job tasking (D'Amico, et al., 2016) (D'Amico, et al., 2005), their findings are relatively generic to ascertain analyst mental models to build 3D visualizations from. Some preliminary research (Perl & Young, 2015) has attempted to document analyst's mental models, but the granularity of the models was too coarse to guide the development of 3D visualizations.

Based on discussions with subject matter experts, we hypothesize that akin to self-morphing graph structures often used to make sense of new datasets, the relations in data that cybersecurity analysts are after with their mental models to distill information, are more related to distinct data-shapes that arise while working with the datasets that analysts are using to solve the task at hand. While analyzing different datasets during incident response or other tasks. To verify this hypothesis a 3D environment and data-shapes was created, that and can be observed and manipulated by analysts using devices providing them stereoscopic view of those shapes.

3. Virtual data explorer

Initially, the OpenGraphiti (Reuille, et al., 2015) (<http://www.opengraphiti.com/>) platform was used to develop 3D visualizations, but due to lack of compatibility with motion controllers (i.e., input devices) Thus we used Unity 3D game engine to create a dedicated environment called Virtual Data Explorer (VDE, <https://coda.ee/vde>) which allow for motion controllers to interact as input devices for Oculus Touch controllers (Unity 3D, 2017) or the Microsoft Mixed Reality headset with their appropriate controllers (Microsoft, 2017). VDE is currently an academic prototype platform for building 3D data-shapes for data visualizations. The VDE affords 3D data visualizations by exporting rendered stereoscopic images to a Virtual, Augmented or Mixed Reality Head Mounted Display (HMD) to create an illusion for the user of immersion to virtual space, containing data-shapes consisting of the data that the user wishes to analyze. Technically a HMD is a set of screens; each screen rendering one of the pair of stereoscopic image per eye to provide vision for binocular depth cueing.

The type of data (network traffic, sessions and flows, but also application logs and process memory usage logs among others) we visualize can be static (logs, forensic evidence) or live-wire data. In the case of a live ingest, the characteristics of the data would be dynamic, however, our current prototype described herein is based off a static repository, as the added complexity of live ingest was not deemed necessary for initial testing of the usability of proposed 3D data-shapes. Note that VDE does not constrain the data-shape development to one type of environment; ingested data could be visualized as data-shapes in virtual-, mixed-, or augmented reality environments. The added benefit of using VR/AR is that 3D visualizations afford ample visual real estate to depict high-parameter (but originally non-spatial) data, allowing perception of numerous variables for each unit of observation. Each parameter can be encoded into visual codes like size, shape, color, and depth (Ware & Franck,

1996). For example, the perceived distance between observer and an object in the 3D virtual environment could represent a continuous value like total bandwidth usage, or number of bytes transmitted per unit of time.

Although using stereoscopic vision and motion cues to encode data have been found useful (Ware & Franck, 1996), it can be challenging to provide analysts with such technical capability that will make good use of humans' natural abilities. Unless analysts can immerse in and manipulate with the data-visualization environment intuitively, it may not be helpful in accomplishing their tasks; in addition, it is assumed that users must be able to use such environment without fatigue and simulator sickness (Kolasinski, 1995; Johnson, 2005), or as it's sometimes referred to – cybersickness.

Prior to current generation Graphics Processing Units (GPU), slow processing power created rendering lags that yielded visually mismatched orienting cues in the environment – this mismatch often led to user nausea. With the intensive development of the Interactive Entertainment Industry that has driven the market need, consumer grade GPU-s have become powerful enough to provide users with non-nauseating VR experiences, while being affordable enough to be used for our purposes. Recent GPUs with current generation HMDs significantly reduce the occurrence of visual lag, therefore reducing the chances of users' nausea.

There are also other factors that could cause unpleasant user experiences in VR. To minimize these effects, we've implemented a few methods in our environment to avoid such experiences. For example, while the user navigates the 3D space in avatar-less first-person perspective, we restrict the range of head movement during motion such that the user can only move in a linear direction towards the point of gaze, or away from it, sometimes referred to as "rudder head movement" (Unity 3D, 2017). The user of course has freedom to observe 360 degrees of the visual field (Kemeny, et al., 2017), only her movements are restricted to back-and-forth directions.

This approach allows us to immerse the user rather conveniently into the VDE environment, where she can, with hand and head gestures, roam around in 3D space to view the 3D data-shapes' visualizations from multiple vantage points, grab and interact with the visualization, experience, manipulate, and explore the data presentations that are dynamically created and adjusted to build situation awareness (in case of NOC/SOC analysts). Akin to self-morphing graphs (as implemented for example in OpenGraphiti (Reuille, et al., 2015)), VDE allows us to examine whether presenting data in 3D data-shapes and enabling interaction with its components could help analysts detect changes in network traffic (this method could also be extended to application logs and process' memory usage, for example). Furthermore, VDE allows us to evaluate whether deliberately structured visual data-shapes that are observed with stereoscopic HMD could enhance CDSA.

For the purposes of this study, we define:

- Dataset – values (e.g. IP addresses, their relations, connections, sessions etc.) collected from sensors, log files and network traffic monitors
- Data-object – one instance from dataset, that may be a key-value pair, set of values related to an event that caused a log-line or alert to be logged
- Data-shape – a specific form of data visualization, where pixels (that in collections represent nodes, connections etc.) are arranged so, that in the resulting visual data representation of the data-objects, visual objects are positioned according to their logical topology so, that the resulting 3D structure would relate to a specific task for which the NOC/SOC analyst is responsible for, and would be using that data-shape for (e.g. relate to hers mental model of the problem/hypothesis/situation)
- VDE scene – combined set of data-shapes, a meta-shape, that consists of spatially positioned data-shapes, that in combination enable to user to view relations between different data-shapes' nodes.

3.1 Data preparation

The ingested network traffic data used to demonstrate the 3D visualization was not live-wire data but a collection of data from the 2016 Locked Shields Cyber Defense Exercise (LS16) (NATO CCDCOE, 2016) (see <https://ccdcoe.org/locked-shields-2016.html>). This is an international cyber defense exercises with more than 550 participants from 26 nations. Participants were assigned roles in various teams, while most of them were

arranged into 20 defensive teams (Blue Teams) and one adversarial team (Red Team). In this exercise, the Blue Teams' goal was to maintain the availability and security of their networks during two days of the exercise.

Locked Shields' dataset was selected as it is relatively well documented, reasonably large (~20TB of PCAP files), has ground truth (what and when did Red Team members do) and there are 20 comparable networks that start out as identical but change as respective Blue Teams adjust them. IPv6 visualization was chosen for first VDE data-shape, as Blue Teams' ability to monitor and secure their IPv6 addresses was a relevant topic during this exercise.

A valuable advantage of LS16 dataset to researchers is the availability of knowledge about the network topology (of the Blue Teams' assets) and ground truth of Red Team actions – e.g., what and when did the Red Team members do during their attacks, and also the Blue Teams responses to adversarial activities (at least to some degree).

To prepare that dataset (IPv6 network traffic information) for 3D visualization, the packets captured (into PCAP files) during LS16 exercise were parsed with Bro IDS (<https://www.bro.org>) to get textual log files describing network connections between nodes (servers, workstations, network devices in Blue Teams' networks, and elsewhere in the "game network") that were observed in captured traffic. Textual log files were then queried with SpectX (SpectX, 2017) (<https://www.spectx.com>) to count the connections between devices to describe relations of nodes by coloring the edges (connections) between nodes according to the number of times those nodes were observed communicating – from transparent green to opaque green to red.

Based that data, VDE would then generate a virtual environment, with LS16 data visualization in it. For our first concept design we chose to visualize a network topology where the nodes (white spheres) represent devices like computer desktops, servers, switches or routers, and the edges (lines connecting spheres) represent the network traffic between those devices. VDE positions nodes according to their logical topology in their respective networks, visualized as data-shapes that are generated per every Blue Team. Such environment enables the user to immersively explore the data-shapes, its components using VR equipment. An example of a user exploring VDE environment composed of data-shapes visualizing LS16 Blue Teams' networks can be seen in a brief video released with this article (<https://coda.ee/iccws>).

3.2 Data-Shapes for visualizing logical topology of networked entities

When the user first enters the VDE, the viewer can look down at a ~30 degree angle at the scene that is positioned at such a distance, as to fit in the view. The floor of the VDE environment (in VR) is a dark patterned desert that continues until it meets a horizon line that delineates floor and skyline. The background environment is chosen such, that it would be unobtrusive to the viewer's task, while providing horizon for spatial orientation. Visualized data-shapes are floating well above the floor and a little below the horizon line, to ease its components' visibility (brighter objects against darker background).

Contrary to self-organizing graphs which are useful for initial examination of unknown datasets, our goal is to provide analysts with (the ability to create) data-shapes that would help them better comprehend datasets that are depicted as structures they can learn to know well over time. We propose creating data-shapes where networked entities (e.g. computers) are positioned according to their logical topology (e.g. computer or server groups and not only physical or functional topology) so, that the resulting 3D structure(s) would relate to a SOC/NOC analyst's task, which in this LS16 example would be to detect prohibited connections between Blue Team's network devices. Data-shapes as such are nothing new (Hurter, 2016), but few have tried to use stereoscopically perceivable 3D data-shapes for computer security (Payer & Trossbach, 2015).

One could consider following as prerequisite knowledge to the creation of the LS16 VDE scene, containing set of proposed data-shapes:

- Understand the principles of how does a computer network function; specifically, how such network is set up for Locked Shields exercise;
- Understand of the logical grouping of networked entities and their topology during Locked Shields; also understand networks (virtual entities) and this game's stakeholders' (physical entities) goals, e.g. Red vs Blue, but also Green, Yellow, White teams' functions;

- Understanding the expected behavior of the above actors and how it should reflect on network data
- Search for indicators, validate, visualize and act.

To create data-shapes for other datasets, a different set of knowledge is required, but can be acquired by mapping the mental models of the analysts who will be using these data-shapes.

To test the usefulness of using 3D data-shapes when encoding non-spatial data, networked entities were spatially positioned, considering their position in network topology, and more importantly, entities' affiliation to logical groups (by functionality (e.g. SCADA components), purpose (e.g. DMZ servers), risk exposure, OS etc.). This results in custom 3D data-shapes, that could be combined to a meta-shape (a VDE scene) representing larger whole of the LS network(s) that are of interest in our scenario. A meta-shape, VDE scene depicted in Figure 2 is the overall view of the percept the LS16 network traffic visualization makes from a distance.

As we have three axes available to encode data (we are not using time in this visualization scenario), we chose to use two of those to encode parts of network topology (subnet number (third octet in case of LS16) and entity's IP addresses' last octet or position in its subgroup) while the third axis binds to the functional or logical group of that entity. Using the common X, Y, Z referencing: within a data shape shown in Figure 1, the Y axis is the group number, the X axis is the subnet number (the team number) and the Z axis has no relevant values other than the IP addresses within a particular range cluster together (i.e., the IP addresses' last octet or position in its subgroup) along the Z-axis. A group number is assigned to a type of 6 functions the nodes or network devices perform. These groups are:

- 1. DMZ servers for email, WWW, DNS, NTP, and others
- 2. Office network with Domain Controller and workstations
- 3. Lab network for research and development
- 4. Control network for drone operators
- 5. Secure devices
- 6. Incident Command System (ICS) systems as the high level objective of the Red Team attacks

Groups contain nodes in their respective subnets, grouped vertically according to their logical positions in their functional groups (subnets). For example, Windows, Linux, OSX workstations are positioned onto separate layers to distinguish them visually in subnets 2 and 3, while Windows, Linux and other servers, networks devices, etc. are kept on the lowest group to distinguish intra-group traffic from inter-group traffic.

For example, to find suspicious connections inside a LS16 Blue Team's network, entities were first positioned according to their subnet and then by their functional groups—servers, network devices, workstations (distinguished further by their type (Windows, Linux, OSX)), and SCADA components among others (see Figure 1). The third dimension is entity's sequential position inside of its subgroup (often the last octet of its IP address). Because the designated functions (and therefore behavior) of the entities in same functional group should be similar, it is beneficial for the analyst to have them close together, while still being spatially distinguishable to quickly diagnose which group and which member to focus on.

At the start of the exercise, there were 20 functionally identical Blue Teams' networks, whose entities should have been communicating identically, but as the exercise advanced, the Blue Teams' networks' behavior (in this case, entities' activity and relative connections / edges) deteriorated from each other's. Each Blue Team's network had 68 preconfigured nodes, and the teams could add two virtual machines per their specifications.

Entities that fell outside of the known functional groups were positioned to three cube-shaped matrixes: i) entities with public IP addresses (simulated in-game internet); ii) entities that had IP addresses in Blue Teams' internal address ranges, but which were not preconfigured prior to game; and iii) entities that had IP addresses in Blue Teams' internal address ranges, were not preconfigured before the game, and did not follow the Locked Shields' addressing logic (for example, those that had letters in IPv6 address). Before positioning entities to those groups, these were sorted by their IP address.

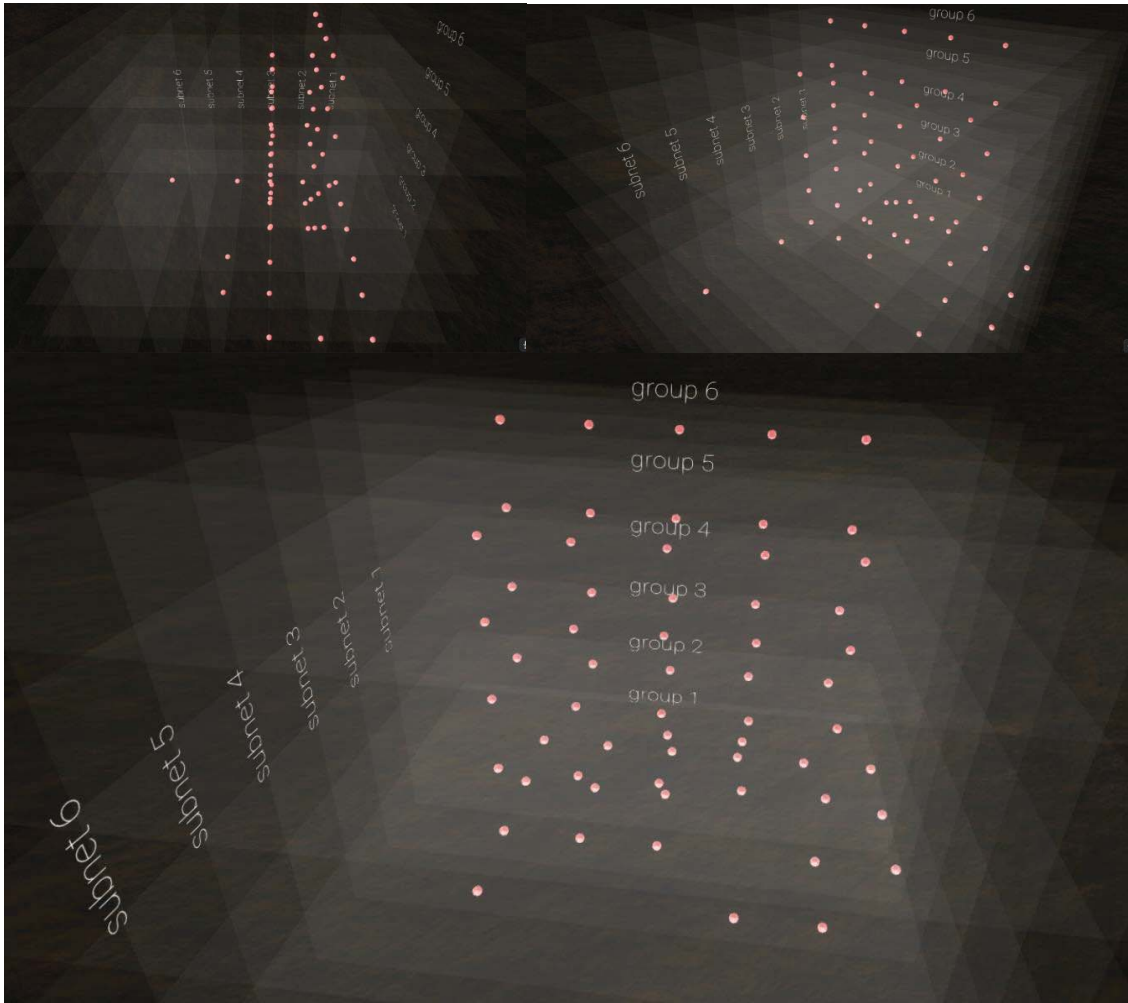


Figure 1: Viewing same data-shape from three different angles

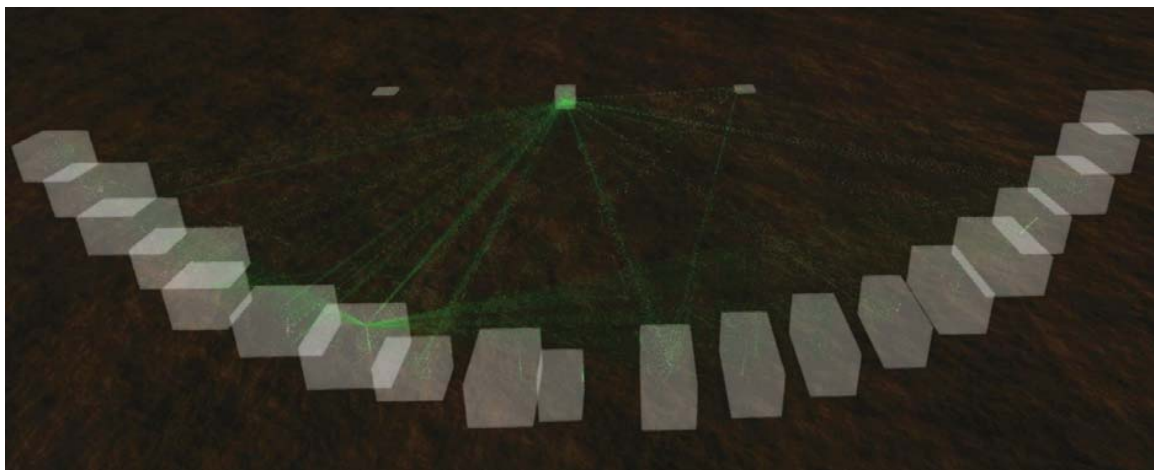


Figure 2: The analyst's initial view of the meta-shape of the Locked Shield dataset in the VDE

Teams' networks curved around three shapes containing external and/or potentially interesting hosts. All data-shapes contain the Blue Teams' systems with the same (or similar) layout as seen in Figure 1. From this broad view, an analyst who knows the logical positioning and internal functions of the Blue Team's networks' groups, subgroups and nodes may find anomalies to investigate further, which in this visualization scenario are connections (green edges) between different Blue Teams' systems. For example, the connections (green edges) originating from a host in the 7th team's network (7th data-shape from left) to other Blue Teams' systems should

not be happening. In addition, connections from the 11th team's network (11th cube from left) to hosts that were named unconventionally (so that they appear to be in the 11th team's IPv6 address range) should be examined by taking a closer look at the visualization (selecting specific host that seems to be trying to blend in and exploring its relations) or continuing exploration in textual logs. For a better understanding of this process, please see the videos (<https://coda.ee/iccws>).

Data-shapes were then spatially positioned to a meta-shape (as shown in Figure 2) to allow the user to take advantage of stereoscopic viewing and the sense of binocular depth that it provides. Several layouts were considered to minimize possible edge clutter and enable convenient distinguishability of intra- and extra-network connections.

Edges connecting the nodes were then added to the data-shapes, as prepared using the process described in subsection 3.1. From the initial vantage point user can distinguish edges that connect one Blue Teams' node(s) to those of other Blue Teams' internal nodes (mostly horizontal edges as opposed to vertical ones); on the other hand the edges connecting Blue Teams' internal nodes with entities in either of the three matrixes have different implications. Would an NOC/SOC operator have to evaluate a network from this view, she would want to see only i) Blue Team's first subnet (e.g. DMZ) nodes connecting to legitimate services located in "game internet" and ii) Blue Team's internal hosts communicating only to that same Blue Team's hosts. All other edges might need further examination.

3.3 Detecting abnormalities in traffic

In Figure 2, the vertical and diagonal lines that connect one node with multiple nodes in other Blue Teams' networks indicate a possible abnormality that should be investigated. Is it possible that the highlighted behaviors represent a compromised node in the Blue Team's network, which is used by a Red Team member to scan other Blue Teams' systems to find those that have not been correctly firewalled? Is it possible that some devices or tasks (e.g., network scans) were misconfigured, e.g., SYN packets were found in the traffic but not ACK or RST, meaning that the host did scan but could not connect to those hosts?

One could argue that this kind of anomalous behavior would be blocked by the network devices' ACL rules, a myriad of "cybersecurity appliances" endorsed by cyber-insurance providers, or at least detected by conventional "cyber-devices" (e.g., IDS/IPS and firewalls). We argue, that while systems that help NOC/SOC personnel to protect their networks are a necessity, our adversaries will always find functionalities (weaknesses) in those systems that enable them to bypass those protections. Therefore NOC/SOC analysts will need to be able to creatively approach their datasets to find their adversaries attacks in novel ways, and we need to provide analysts with appropriate tools for those tasks. One such tool could be a system (ex. VDE) that would provide analysts' with environment where, using the same, similar, or improved structured data views to visualize familiar but dynamic datasets, the analyst could have different views of relevant datasets to find anomalies, which could be missed otherwise, would they rely on 2D and textual tools only.

4. Discussion and conclusion

This paper describes the theory and methodology used to develop a 3D visualization of network data. The selection of attributes, data-shapes and display aims to capture cybersecurity analysts' mental models enable the analysts to better understand their respective datasets. Following the development of the visualization, we are planning to conduct controlled validation study with experienced cybersecurity analysts and vulnerability analysts. We will be using a mixed method that begins with a set of qualitative task analyses while the participant is using the new visualization tool moving to quantitative behavioral studies. Our dependent measures are situation awareness content and accuracy, speed of SA acquisition, mental model accuracy.

We argue that there is a need for structured evaluation of visualizations that are comparable with the analyst's mental model. Current technology is capable of delivering the basic 3D visualization needs and this preliminary work demonstrates that through tight interaction with SMEs it is possible to identify core concepts in their mental models and transform them into Data-shapes. Further research is needed on how general are the Data-shapes over different types of networks, cyber operations, analyst past training and other individual differences. However, the benefits of harnessing human superior visual-perception to cyber detection can provide a much needed advantage to cyber defenders.

Acknowledgements

For all the hints, ideas and mentoring, authors thank Alexander Kott, Jaan Priisalu, Olaf Manuel Maennel and Lee Trossbach. This research was partly supported by the Army Research Laboratory under Cooperative Agreement Number W911NF-13-2-0045 (ARL Cyber Security CRA) and under Cooperative Agreement Number W911NF-16-2-0113 and W911NF-17-2-0083. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

References

- Baddeley, A., 2012. Working Memory: Theories, Models, and Controversies. *Annual Review of Psychology*, Volume 63, pp. 1-29.
- Brown, M. A., 1994. *Displays for Air Traffic Control: 2D, 3D and VR - A Preliminary Investigation*, London: Queen Mary & Westfield College.
- Bryant, D. J. & Tversky, B., 1999. Mental Representations of Perspective and Spatial Relations from Diagrams and Models. *Journal of Experimental Psychology Learning Memory and Cognition*, 25(1), pp. 137-156.
- Burnett, M. S. & Barfield, W., 1991. *Perspective versus plan view air traffic control (ATC) displays - Survey and empirical results*. Columbus, s.n.
- D'Amico, A., Buchanan, L., Kirkpatrick, D. & Walczak, P., 2016. Cyber Operator Perspectives on Security Visualization. In: *Advances in Human Factors in Cybersecurity*. s.l.:Springer, pp. 69-81.
- D'Amico, A. et al., 2005. *Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts*. s.l., s.n.
- Dejoy, D. M., Laughery, K. R. & Wogalter, M. S., 1999. Organizing theoretical framework: a consolidated communication-human information processing (C-HIP) model. Warnings and risk communication. In: s.l.:s.n., pp. 15-23.
- Dennehy, M. T., Nesbitt, D. W. & Sumei, R. A., 1994. Real-Time Three-Dimensional Graphics Display for Anti-air Warfare Command and Control. *Johns Hopkins APL Technical Digest*, 15(2), pp. 110-119.
- Ehrenstein, W. H., Spillmann, L. & Sarris, V., 2003. Gestalt Issues in Modern Neuroscience. In: *Axiomathes*. s.l.:Springer, pp. 433-458.
- Ellis, S. R., McGreevy, M. W. & Hitchcock, R. J., 1987. Perspective traffic display format and airline pilot traffic avoidance. *Human Factors*, Volume 29, pp. 371-382.
- Feltovich, P. J., Prietula, M. J. & Ericsson, K. A., 2006. Studies of expertise from psychological perspectives. In: *The Cambridge handbook of expertise and expert performance*. Cambridge: Cambridge University Press, pp. 41-67.
- Foyle, D. C., Andre, A. D. & Hooey, B. L., 2005. *Situation Awareness in an Augmented Reality Cockpit: Design, Viewpoints and Cognitive Glue*. Las Vegas, Proceedings of the 11th International Conference on Human Computer Interaction.
- Gentner, D. & Stevens, A., 1983. *Mental Models (Cognitive Science Series)*. s.l.:Lawrence Erlbaum Associates.
- Hurter, C., 2016. *Image-Based Visualization: Interactive Multidimensional Data Exploration*. s.l.:Morgan & Claypool.
- Johnson, D. M., 2005. *Introduction to and Review of Simulator Sickness Research*, Arlington: U.S. Army Research Institute for the Behavioral and Social Sciences.
- Johnson-Laird, P. N., 1983. *Mental Models*. s.l.:Cambridge University Press.
- Kaisler, S., Armour, F., Espinosa, A. J. & Money, W., 2014. *Big Data: Issues and Challenges Moving Forward*. Wailea, s.n.
- Kandel, S., Paepcke, A., Hellerstein, J. M. & Heer, J., 2012. Enterprise data analysis and visualization: An interview stud. *IEEE Transactions on Visualization and Computer Graphics*, 18(12), pp. 2917-2926.
- Kemeny, A., George, P. & Mérienne, F., 2017. New VR Navigation Techniques to Reduce Cybersickness. *Electronic Imaging, The Engineering Reality of Virtual Reality*, pp. 48-53.
- Klatzky, R. L. et al., 1998. *Spatial Updating of Self-Position and Orientation during Real, Imagined, and Virtual Locomotion*, s.l.: Sage Publications, Inc..
- Kolasinski, E. M., 1995. *Simulator Sickness in Virtual Environments*, Alexandria: United States Army Research Institute.
- Lange, M., Dang, T. & Cooper, M., 2006. *Interactive resolution of conflicts in a 3d stereoscopic environment for air traffic control*. Ho Chi Minh City, Vietnam, Vietnam, s.n.
- Lebreton, P., Raake, A., Barkowsky, M. & Le Callet, P., 2012. Evaluating Depth Perception of 3D Stereoscopic Videos. *IEEE Journal of Selected Topics in Signal Processing*, 6(6).
- Lee, K. & Lee, S., 2015. 3D Perception Based Quality Pooling: Stereopsis, Binocular Rivalry, and Binocular Suppression. *IEEE Journal of Selected Topics in Signal Processing*, 9(3), pp. 533-545.
- Microsoft, 2017. *Windows Dev Center, Motion controllers*. [Online] Available at: https://developer.microsoft.com/en-us/windows/mixed-reality/motion_controllers
- NATO CCDCOE, 2016. *Locked Shields 2016*. [Online] Available at: <https://ccdcoe.org/locked-shields-2016.html>
- Paivio, A., 1991. Dual Coding Theory: Retrospect And Current Status. *Canadian Journal of Psychology/Revue canadienne de psychologie*, 45(3), pp. 255-287.
- Paradice, D. & Davis, R. A., 2008. *DSS and Multiple Perspectives of Complex Problems*. s.l.:s.n.
- Payer, G. & Trossbach, L., 2015. The Application of Virtual Reality for Cyber Information Visualization and Investigation. In: *Evolution of Cyber Technologies and Operations to 2035*. s.l.:Springer, Cham, pp. 71-90.

- Perl, S. J. & Young, R. O., 2015. *A Cognitive Study of Incident Handling Expertise*. Berlin, 27th Annual FIRST Conference.
- Reda, K. et al., 2013. Visualizing large, heterogeneous data in hybrid-reality environments. *IEEE Computer Graphics and Applications*, 33(4), pp. 38-48.
- Reuille, T. et al., 2015. *OpenDNS Data Visualization Framework*. [Online] Available at: <http://www.opengraphiti.com/>
- Schneider, W., Dumais, S. T. & Shiffrin, R. N., 1982. *Automatic and Control Processing and Attention*, Illinois: University of Illinois.
- Schoenwaelder, P. J. et al., 2007. Key research challenges in network management. *IEEE Communications Magazine*, 45(10), p. 104–110.
- Smallman, H. S., St. John, M., Oonk, H. M. & Cowen, M. B., 2001. Information availability in 2D and 3D displays. *IEEE Computer Graphics and Applications*, 21(5), pp. 51-57.
- SpectX, 2017. *Inertia in Processing Machine Generated Data*. [Online] Available at: <https://www.spectx.com/articles/processing-machine-generated-data>
- St. John, M., Cowen, M. B., Smallman, H. S. & Oonk, H. M., 2001. The Use of 2D and 3D Displays for Shape-Understanding versus Relative-Position Tasks. *Human Factors*, Volume Spring, pp. 79-98.
- The Bro Project, n.d. [Online] Available at: <https://www.bro.org/>
- Treisman, A. & Paterson, R., 1984. Emergent features, attention, and object perception. *Journal of Experimental Psychology: Human Perception and Performance*, 10(1)(12).
- Unity 3D, 2017. *Unity 3D Manual, Input for Oculus, Oculus Touch Controllers*. [Online] Available at: <https://docs.unity3d.com/Manual/OculusControllers.html>
- Unity 3D, 2017. *Vision 2017 - Lessons from Oculus: Overcoming VR Roadblocks*. [Online] Available at: <https://youtu.be/swA8cm8r4iw?t=9m42s>
- Ware, C. & Franck, G., 1996. Evaluating stereo and motion cues for visualizing information nets in three dimensions. *ACM Transactions on Graphics*, March.15(2).
- Wickens, C. D. & Hollands, J. G., 2000. *Engineering psychology and human performance*. Upper Saddle River: Prentice Hall.
- Young, I., 2008. *Mental Models: Aligning Design Strategy with Human Behavior*. s.l.:Rosenfeld Media.