Operator Impressions of 3D Visualizations for Cybersecurity Analysts

Kaur Kullman[1], Noam Ben Asher[2], Char Sample[3]
TalTech University, Tallinn, Estonia, EU[1]
ORAU, Oak Ridge TN, USA[2]
ICF Inc. Columbia, MD, USA[3]

Abstract: Cybersecurity analysts ingest and process significant amounts of data from diverse sources in order to acquire network situation awareness. Visualizations can enhance the efficiency of analysts' workflow by providing contextual information, various sets of cybersecurity related data, information regarding alerts, among others. However, textual displays and 2D visualizations have limited capabilities in displaying complex, dynamic and multidimensional information. There have been many attempts to visualize data in 3D, while being displayed on 2D displays, but success has been limited. We propose that customized, stereoscopically perceivable 3D visualizations aligned with analysts' internal representations of network topology, may enhance their capability to understand their networks' state in ways that 2D displays cannot afford. These 3D visualizations may also provide a path for users who are trained and comfortable with textual and 2D representations of data to assess visualization methods that may be suitably aligned to implicit knowledge of their networks. Thus, the premise of custom data-visualizations forms the foundation for this study. Herein, we report on findings from a comparative, qualitative, within-subjects usability analysis between 2D and 3D representations of the same network traffic dataset. Study participants (analysts) provided information on: 1.) ability to create an initial understanding of the network, 2.) ease of finding task-relevant information in the representation, and 3.) overall usability. Results indicated that interviewees indicated a preference for 3D visualizations over the 2D alternatives and we discuss possible explanations for this preference.

Keywords: visualization, cybersecurity, decision-making, data visualization, virtual reality.

1. Introduction

Cyber is the newest domain of war (Lynn, 2010), endowed with unique sensory characteristics that differentiate this warfare environment from kinetic-physical warfare (Gonzalez, Ben-Asher, Oltramari, & Lebiere, 2014). Cyber security analysts who are responsible for ensuring the security of networks and other assets, utilize a wide array of computer network defense (CND) tools, such as Security Information & Event Management (SIEM) that allow data from various sources to be processed and alerted on. CND tools allow analysts to monitor, detect, investigate and report incidents that occur in the network, as well as provide an overview of the network state. To provide analysts with such capabilities, CND tools depend on the ability to query, process, summarize and display large quantities of diverse data which have fast and unexpected dynamics (Ben-Asher & Gonzalez, 2015). Shneiderman (Shneiderman, 1996) provided a taxonomy depicting 7 human-data interaction task levels: 1.) gaining *Overview* of the entire dataset, 2.) *Zoom* on an item or subsets of items, 3.) *Filter* non relevant items, 4.) get *Details-on-Demand* for an item or subset of items, 5.) *Relate* between items or subset of items, 6.) keep *History* of actions and 7.) allow *Extraction* of subsets of items and query parameters. Traditionally, cyber defenders have used command line tools and alphanumeric data displays to execute these seven tasks. With the need for faster and more accurate situational awareness of increasing data volume, many CND products have integrated graphical user interface (GUI) and 2-dimensional (2D) data visualizations to expedite human information acquisition.

Visualizing multidimensional data on 2D screens bears several limitations. First, the resulting visualization after the dimensionality reduction methods have been applied will likely differ from the mental representation that the analyst had acquired upon reviewing the same data in numerical and textual data. Contextual information will likely be removed in the reduction process that could be crucial to the understanding of the situation and to identify relevant clues (Rajivan, Konstantinidis, Ben-Asher, & Gonzalez, 2016). Also, three dimensional visualizations may address some of the inherent limitations of 2D displays by aligning with the analysts' internal representation of their datasets, if the analyst naturally thinks about data in three dimensions. Users' interactions in VR (Virtual Reality) and XR (Mixed Reality) may also be more intuitive if users are expected to interact with the visualization in ways that humans manipulate objects in the physical world. This way we could harness the dexterity of human hand movement for interactions (Gershon, Klatzky, & Lee, 2014) if the tools used are capable enough, using haptic feedback to further advance users interaction efficiency (Gershon, Klatzky, Palani, & Giudice, 2016).

However, the scale, heterogeneity, and complexity of cybersecurity datasets continue to pose challenges for visualization and interaction designers (Reda, et al., 2013) despite the constant increase in computers' abilities to process and display more data on 2D displays. This could be because visualization designers lack an understanding of cybersecurity operations and network infrastructure to create an effective visualization for cybersecurity analysts. Yet, cybersecurity analysts who are familiar with the technical aspect of network monitoring do not have expertise in data visualization and human perception. The visualization designer might need to have dual expertise.

By providing a data visualization environment where minimalistic visual, audio and haptic cues are informing the user of what is happening in that environment, we allow the user to focus on the task. Furthermore environmental cues should be perceptible and clear to avoid user confusion. Visualization should be functional and available utilities should accurately convey their functions. Controls, navigation, interface, and all other interface conventions should be consistent. Users cognitive and physical workload must be minimized. Human errors should be anticipated and prevented if possible. The environment should be flexible to allow customization for personal preferences, cultural differences, color vision deficiency etc. (Hodent, 2018). We hypothesize that the analyst may find it intuitive to use a 3D representation of cybersecurity network data that is aligned with the above guidelines as well as the analyst's internalized understanding of the data. Intuitive interfaces may enable the analysts to explore and understand their environment more efficiently.

2. Visualization for Cyber Defense

Cybersecurity visualizations provide analysts with visual representation of alphanumeric data that would otherwise be difficult to comprehend due to its large volume. Such visualizations aim to effectively support analyst's tasks including detecting, monitoring and mitigating cyber attacks in a timely and efficient manner (Sethi & Wills, 2017). Cybersecurity specific visualizations can be broadly classified into three main categories: 1.) network analysis, 2.) malware and 3.) threat analysis, and situational awareness (Sethi & Wills, 2017). Timely and efficient execution of tasks in each of these categories may require different types of visualizations addressed by a growing number of cybersecurity specific visualization tools (Marty, 2008) as well as universal software with visualization capabilities like Tableau, MS Excel, R, Python, and D3 libraries (d3.js) among others. These tools could be used to visualize data in myriad of ways (Munzner, 2014) so that analysts could explore their datasets visually and interactively (Ward, Grinstein, & Keim, 2015). *Graphistry* is one recent example of a 2D force-directed graph visualization (Meyerovich & Tomasello, 2016) whose interface is easy to manage and visualization and is responsive to queries on massive datasets. These are crucial qualities for cybersecurity analysts, with emphasis on the importance of the low-latency between analyst's request for a change in visualization (change in filter, time window or other query parameters) and rendering of the visualized response from the system (Wu, Xu, Chang, Hellerstein, & Wu, 2018).

The usability of data visualizations for CND operations that have not been evaluated, may lead to low adoption rates by practitioners (Best, Endert, & Kidwell, 2014). The challenge in creating useful visualization for cybersecurity practitioners is in aligning data visualization experts' knowledge with cybersecurity analysts' needs and knowledge so, that the resulting visualizations would be useful for work tasking. A recent survey showed that 46% of 130 tools did not have any user-involvement in the evaluation phase (Sethi & Wills, 2017).

To achieve higher visualization adoption rates, analysts should have the ability to intuitively and iteratively adjust the visualizations to suit with their changing needs (Kirk, 2016). Datasets used in cybersecurity operations are often multi-dimensional and analysts would either have to scale down the number of dimensions viewed at one time to be able to use 2D & 3D visualizations, or combine multiple 2D visualizations displaying different dimensions of the same dataset in a single dashboard. This requires the designer to properly encode variables (dimensions) into shapes, colors, sizes among others. The viewer has to translate that shape into spatial perception and compare it to her internal understanding of the data, to decode the meaning of the visualizations; a task that may be non-trivial (Ehrenstein, Spillmann, & Sarris, 2003). There have been numerous attempts to employ 3D visualizations for cybersecurity data that are displayed on 2D computer screens with varying degrees of success. Such visualizations sometimes use monocular depth cues (Lebreton, Raake, Barkowsky, & Le Callet, 2012) and object movement to convey the 3D shape of the visualization; advantages and disadvantages of which were thoroughly discussed in our previous paper (Kullman, Cowley, & Ben-Asher, 2018). VIDS (Shearer & Edwards, 2018) provides an interactive 3D environment for visualizing network and alert (or other) data in 3D shapes, whereby users can seamlessly switch styles and layouts to dynamically shape their data and easily adjust their viewpoint (Gaw, 2014). Real-time 3D visualization engine DAEDALUS-VIZ allows operators to grasp visually and in real-time an overview of alert circumstances, while providing highly flexible and tangible interactivity (Inoue, Suzuki, Suzuki, Eto, & Nakao, 2012). InetVis (van Riel & Irwin, 2006) allows the user to allocate source and destination IPv4 addresses to X and Z axis, while destination ports are being allocated to the Y axis on a 3D cube. To understand the shape of the cube and detect the positions on Z axis, user must manually change the viewpoint with mouse. Shoki (Berry, n.d.) allows the user to define what values are plotted on which axis, while the screen is divided to four squares, three of them showing each axis in 2D, while the fourth square displays the cube as a 3D object.

Due to the emergence of commodity VR devices, multiple data visualization tools have implemented support for VR headsets, that are capable of 6 degrees of freedom (6DOF) movement of the user's viewpoint, allowing the observer to perceive the depth of the visualization stereoscopically, avoiding the mental work needed to convert 2D images to 3D. OpenGraphiti (Reuille, Hawthorne, Hay, Matsusaki, & Ye, 2015) enables provides customizable graphs, along with querying and filtering capabilities. However, OpenGraphiti does not provide 3D VR interaction capacities. However, V-Arc (Maddix, 2015) enables the positioning of data in a predetermined layout, data selection and color-coding amongst other capabilities. Virtual Data Explorer (VDE) is a VR tool that allows users to collaborate while investigating 3D data visualizations, to find anomalies in a variety of cybersecurity-related datasets (U.S. ARL, 2018). For our research herein, we used VDE (see 3.4), because it enables the user to perceive the spatial layout of the topology based on observed network traffic, while the resulting visualization can be augmented with additional data, like TCP/UDP session counts between network nodes (Kullman, Cowley, & Ben-Asher, 2018). Due to the 6DOF of Oculus Rift VR headset (OVR) used for this study, VDE also allows us to test the usefulness of stereoscopically perceived depth-cues (contrary to monocular depth-cues on flat screens) for encoding data.

3. Method

To understand whether stereoscopically-perceivable 3D data-shapes representing a complex computer network's topology is usable, we conducted semi-structured interviews with 10 subject matter experts working as cybersecurity analysts (as suggested in (Ward, Grinstein, & Keim, 2015)). Included in the usability assessment, we asked analysts about whether network behavior is understandable, helpful and useful for cybersecurity analysts' tasks.

3.1 Participants

Ten cybersecurity analysts (Mean age = 36.5yr., 20% females) were interviewed in a semi-structured format. All participants work as cyber security practitioners, having 2 months to 10 years of experience in the field (Mean = 4.5 years). Participation was voluntary and these volunteers were not compensated for their time.

3.2 Materials

The network traffic data used during the interviews was part of the NATO CCDCOE CDX Locked Shields 2018 (LS18) "Partner Run" (LS18PR) dataset. This dataset includes 23 defensive teams' (Blue Teams, BT) networks, an offensive (Red Team, RT), infrastructure support (Green Team), situational awareness (Yellow Team) and the managing team (White Team) nodes and traffic. During LS18 exercise the network included more than 4000 virtual machines, with about 2500 attacks executed by the Red Team against all Blue Teams combined. LS18PR function was to test Read Team' and infrastructure' readiness. Distinct of the main event, LS18 that ran for 2 days (2x7 hours), LS18PR ran for 7 hours, during which only few Blue Team networks were attacked and defended, while the rest of the networks were running as usual. Hence LS18PR dataset provides the ability to observe networks in their "normal" as well as "under attack" and "compromised" states during the same time.

The time-window for the network sessions used in the visualizations shown to the participants was set to 40-minute periods. For data preparation, Moloch (https://molo.ch/) was used to process the LS18PR packet data (PCAP). The resulting data and metadata was stored in an Elasticsearch server to allow dynamic querying. Kibana (https://www.elastic.co/products/kibana) was used to generate dynamic and interactive 2D visualizations based on the data stored in Elasticsearch server. VDE queried the Elasticsearch server for session counts between entities and presented the information using Oculus Rift (https://www.oculus.com/rift/) VR headset (OVR) while an Oculus Touch controller (OTC) was used to interact with the VDE. The controller allowed users to move around the virtual space (by changing their viewpoint), select different groups of objects (e.g. connections from/to a Blue Team), grab a network node to alter its position (and better perceive the destinations of the connections that this node had) and query additional information about the node (e.g. it's IP addresses).

3.3 Procedure

Upon arrival to the interview, participants were asked about their cybersecurity expertise, experience with 2D and 3D visualizations, as well as gaming preferences. Gaming preferences were discussed to build the rapport and understand interviewee's level of experience in cybersecurity. Below is a list of the basic questions asked in this introduction portion of the procedure. Participants provided open ended answers that were documented by the experimenter.

1. What are your favorite console / computer games?
2. Have you used Moloch and / or Kibana before?
3. Have you experienced Virtual, Augmented or Mixed Reality before?
4. Do you have formal education on IT and / or cybersecurity?
5. What area do you specialize in cybersecurity?
6. How long have you been working on your current specialty; on cybersecurity?

Then, participants received a short briefing about the purpose of the study and an overview of the dataset. They were shown a printed diagram (see Figure 1) illustrating the network topology of a single blue team network. Based on the diagram, participants were asked to consider, what (textual and visual) tools they would prefer to use to learn that network's topology to acquire situational awareness.

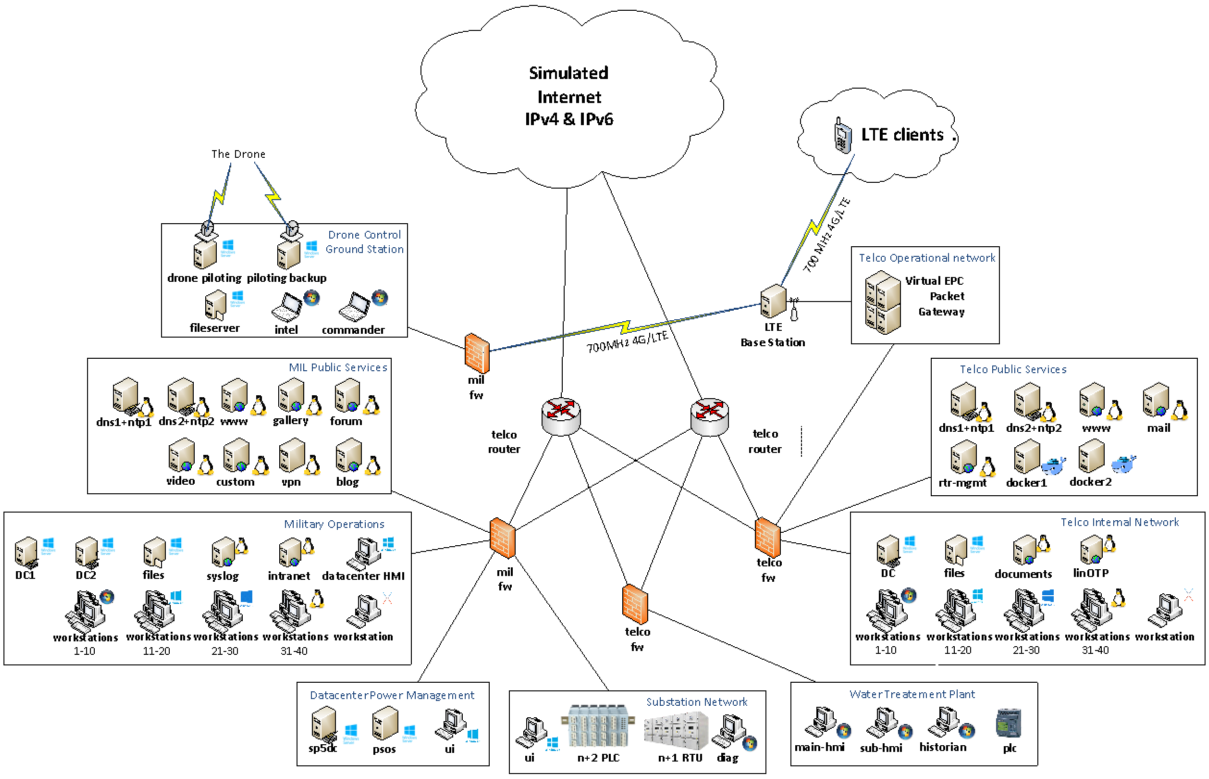
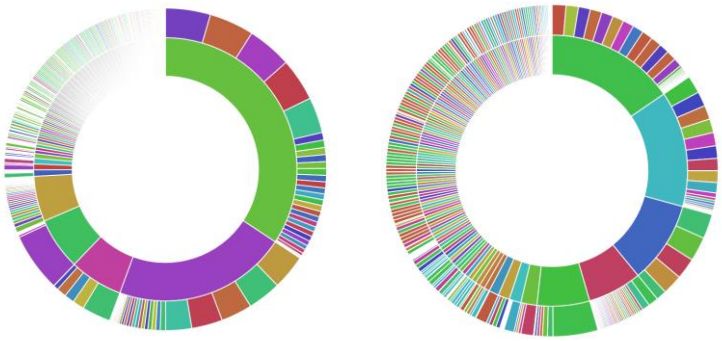


Figure 1. Simplified network topology diagram for traffic used in this study.

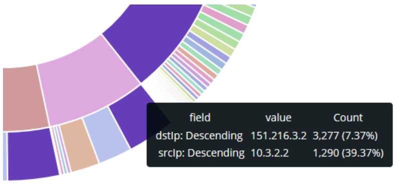


(a) (b)

Figure 2. *Radial 2D diagrams visualizing activeness of Blue Teams' internal nodes. Inner ring contains source addresses of the entities present in that Blue Team's network while the outer ring contains destination addresses of that same Blue Team's entities, with network connection sessions to that source address during a time-window.*

Following, the experimenter presented a 2D visualization of session counts between the different entities in the Blue Team's network as radial figures (Figure 2 using Kibana). As seen in Figure 2a and Figure 2b there is a difference of an actively attacked and maintained network (on the left) compared to another one with exactly the same topology and active services, while unmaintained and not attacked network (on the right).

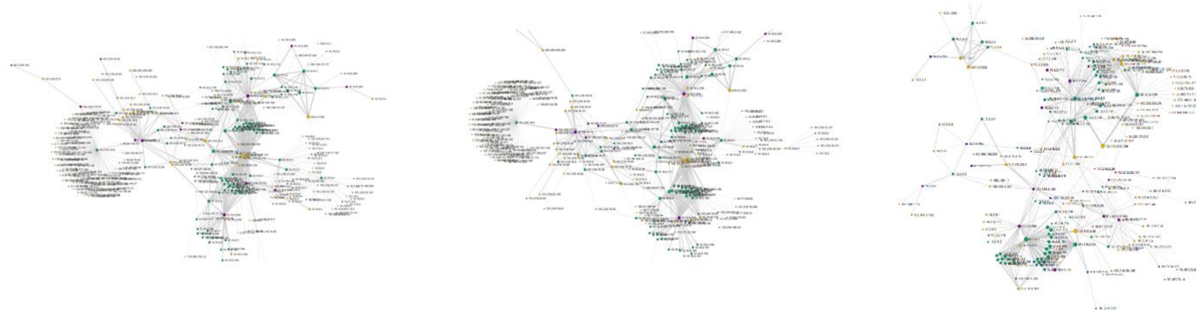
Size of a sector on Figure 2 represents the count of observed sessions. The radial diagram also indicated how many connections were initiated between the source and the inner ring, how many of those connections were targeted at the one represented in the outer ring, etc. The color of the session-count-block is randomly allocated to each node in that Blue Team network and does not have any relation to other networks. However, the color allocated to each node does allow the observer to find that same node in that same radial. The other sectors belonging to that same node are also highlighted by a mouse-over, which displays a popup detailing the IP addresses of source and its destination nodes and their session counts (see Figure 3).



field	value	Count
dstIp: Descending	151.216.3.2	3,277 (7.37%)
srcIp: Descending	10.3.2.2	1,290 (39.37%)

Figure 3. *Mouse-over example for selected data-point displayed in a popup window, with source IP address and observed session count (srcIp) and destination IP address with its respective session count (destIp).*

Participants were also shown a 2D visualization of a force directed graph (using Moloch) to provide another example of graphical representation of relations between networked entities (Figure 4).



(a) (b) (c)

Figure 4. *Network connections observed in the two unused BT (a) and (b) networks compared to a BT (c) networks that were actively engaged during LS18PR. Traffic observed during a set period of time is applied as pull strength of the edges between nodes, while nodes represent the hosts initiating and/or receiving connections, visualized on a 2D graph.*

Following the review of various 2D visualizations, participants were introduced to the VDE and the reasoning behind the spatial positioning of network elements in a 3D space. During this step, LS18PR networks were first shown as 3D shapes on a 2D display and once participants felt comfortable with their understanding of the 3D visualization as shown in VDE, they were fitted with an Oculus Rift VR Headset and Touch Controller. Participants were encouraged to explore the 3D display by changing their viewpoint while using VDE so that they could observe Blue Team networks from close distance (Figure 5) and would be able to read explanatory texts, reach out to grab the nodes, move those around, highlight nodes' features, select edges' groups and so on. After participants had familiarized themselves with the VDE environment and it's 6DOF "rudder head movement" (Pruett, 2017), they were asked to evaluate if and how such network topology visualization and its augmentation with additional data (e.g. network session counts) would relate to the 2D visualizations (Figures 2, 3, 4) and the print-out topology (Figure 1) shown to them before. Once the participant gained an understanding of a blue team's network, she/he was guided to adjust the viewpoint in VR so that all the LS18PR network components would be in the field of view. Then, the participant was asked to provide feedback and critique regarding the usability of VDE, subjective ease of stereoscopical perception of the 3D data shapes and her/his ability to acquire situation awareness with such tool.

3.4 Virtual Data Explorer

Virtual Data Explorer (VDE) was developed with the Unity 3D game engine to present users with stereoscopically perceivable data visualizations in VR and XR.

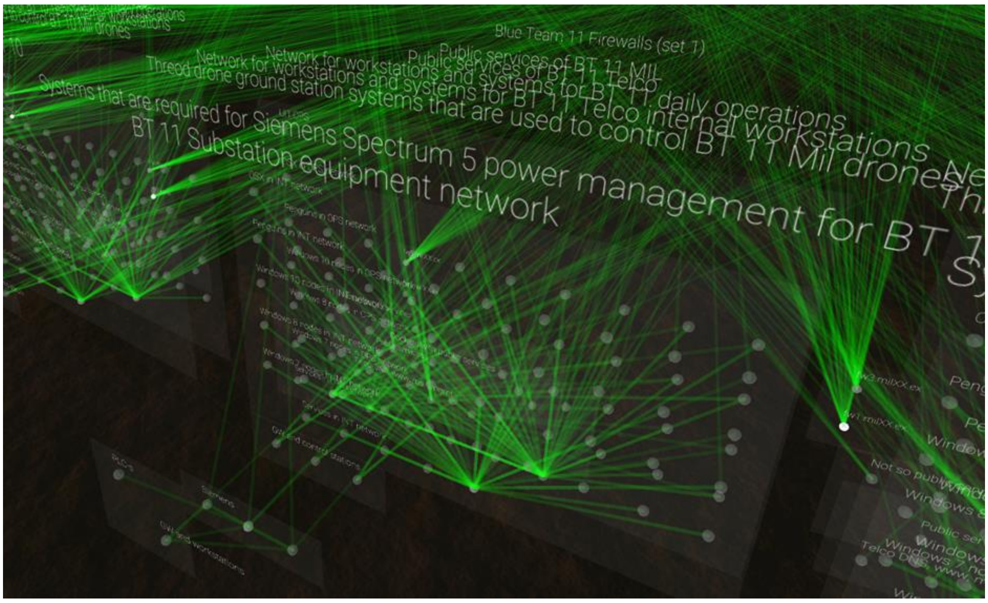

Blue Team 11 Firewalls (set 1)
Public services of BT 11 MIL
Network for workstations and systems for BT 11 Telco
Network for workstations and systems for BT 11 daily operations
Thread drone ground station systems that are used to control BT 11 Mil drones
BT 11 Telco internal workstations
Systems that are required for Siemens Spectrum 5 power management for BT 11
BT 11 Substation equipment network
Penguins in OPS network
Penguins in INT network
Windows 10 nodes in OPS network
Windows 10 nodes in INT network
PLCs
Siemens

Figure 5. *VDE 3D display of network topology and traffic focusing on a single Blue Team network topology ("Zoom" on "Details-on-Demand", per* (Shneiderman, 1996)*). Additional videos of VDE can be found: https://coda.ee/vde*

The VDE uses a predefined topology description (configuration) for the visualized network. Data-shapes were spatially positioned into a meta-shape (viewed from different angles as shown in Figure 6) to allow the user to take advantage of stereoscopic viewing that VR provides. Multiple layouts were considered to minimize possible edge clutter and enable convenient distinguishability of intra- and extra-network connections and nodes' relations. These 3D shapes are easily understandable in stereoscopically-perceivable VR headsets, while often cluttered and unusable on a 2D screen or on a printed paper.

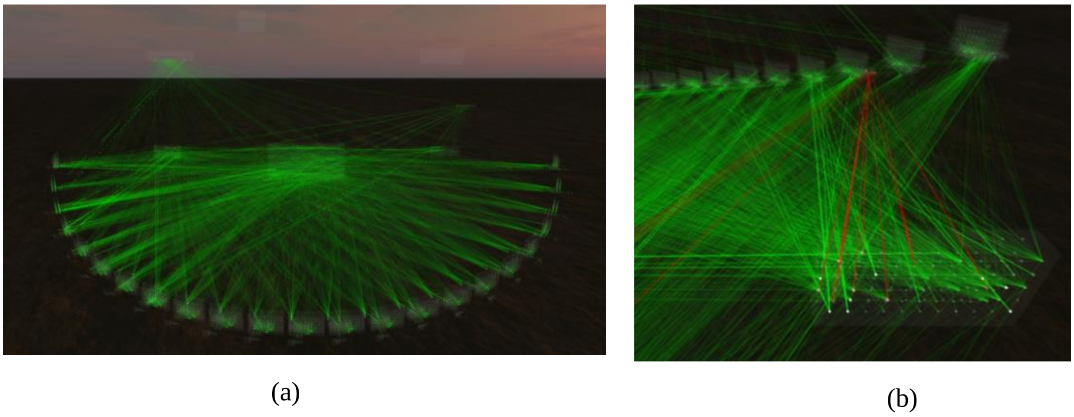


Figure 6. *3D display of LS18PR network topology and network traffic using VDE: (a) overall view of the meta-shape (“Overview”); (b), RT group (“Zoom”) with some added connections and selected (“Filtered”) edges colored red (“Relations”, per* (Shneiderman, 1996)*).*

VDE allows the spatial topology of the network to be augmented with additional data. For this study, the visualization was enriched with network session counts so, that the most popular connection (represented as a green line (edge) between the nodes that were observed connecting) was fully visible, while the least popular connection was almost transparent. User could add additional sessions using VDE menu system in VR, in which case the added edges were colored red until a next set of edges was added. Additional information about VDE design decisions can be found in our previous paper (Kullman, Cowley, & Ben-Asher, 2018).

4. Results

Participants were asked for impressions on the technology, ideas or suggestions for modifications, should such a tool be made available for their tasking. All participants had used 2D visualizations, 6 had used Kibana, and 4 out had experienced VR prior to this study. Seven interviewees self-rated themselves as ‘experienced’ in playing computer games. All participants used command line interfaces or GUIs for tasks like querying NetFlow data, inspect captured packets, review incidents in SIEM, explore various configuration files of the routing and perimeter devices etc. Seven used Kibana and / or Excel for simple 2D visualization. All participants agreed that although printed or electronically provided 2D diagrams of the network topology would be helpful, topologies provided are usually outdated. Overall, there emerged a common process that analysts would have used to build their understanding of a network’s topology. First, analysts would build an understanding of what is “normal” in that specific environment and then find the behaviors that would need further investigation. In order to execute that process, the analysts begins by building filters on available data to exclude the findings that are deemed “normal” and continue fine-tuning that filter, while the analyst learns that network’s behavior and builds her/his internalized understanding of that datasets expected demeanor.

To the questions “How would you build the understanding of a network? How would you map the network topology?” participants responded with: “Textual logs from SIEM [or similar]”;”Textual tools”; “flow in Kibana, xflow, tcpdump”. “Whatever tools that are available. Textual mostly, if some visualization is available, then that too." To the question “How would you establish expectations regarding normal behaviors of the different entities in the network?” participants responded with: “I just read the logs [..]. Look in packets.”; “Check Ingress/egress points, what services are allowed through firewall, what VLANs&VPNs are in use.”; “filter logs, what type of systems are in these networks from SIEM. Use different filters and queries in Kibana.”; “Work through documentation, dive in, see configuration.”; “flow data, who’s talking to each other, as opposed to heading outside; I’ve used to bar graphs [..while trying to identify..] what IP’s are being hit, what hosts are endangered a lot in traffic. Usually I would likely see just textual lists of IP addresses, ports etc."; “Look at netflows, do a graph chart. Use excel, build bar graphs [and so on]"; “Use a sensor that sees all the traffic in this network, build a BPF to exclude things (ICMP, TCP, UDP) [from tcpdump] to see what’s left, what falls out, what ports and protocols, [..], to find what stands out, what weird ports are in use."

Once in the VDE VR environment, users had some trouble getting comfortable with the “rudder head movement” to roam around in the VR environment. Few participants found the rudder head movement intuitive to use. Learning to use this tool usually took between one to two minutes. Most problematic was the vertical movement. To execute vertical movement, users had to look straight up or straight down and move backwards or forwards to change their vertical viewpoint. However, one participant commented, "[moving around in this environment] is very natural to me". Only two participants reported feeling dizzy or having any simulator sickness/motion sickness symptoms during or after the session. The precision of depth perception or the predicting the physical distance of each virtual object from the self was highly variable. Most of the participants managed to grab and hold visualized entities easily, while others struggled. Further tuning of haptic and visual feedback is needed to improve interaction with 3D data representations.

Once the participants were comfortable with adjusting their position and viewpoint in the VR environment, all were able to observe the data-shapes and understand its relation to the network's textual and 2D visualizations they had seen moments before. Most participants stated that once the logical structure of the shapes positioned in VR had been understood, the topology of these networks became much clearer. Participants also understood the underling relations between 3D visualization and the textual / 2D representation they had seen previously:

- [P1]: "Does this [3D visualization] map back to the topology you saw on the paper before? *I think so, I mean I'd have to figure out where things are, but... [yes]*";
- [P6]: "*It is not how I thought about, but... [...] I think it would definitely be helpful, but it would take some re-learning, [e.g.] how to think visually. When you learn networking, then you're kind of trying to build this in your brain already. But then getting used to seeing this and not having to build your own picture. Like, training brain to think visually not only textually.*";
- [P4]: "*So this is what you showed [me] before on the network diagram [on paper]*? [...] *Yes, I like this. This is different than looking graphs on your computer screen.* [...] I take it you'd prefer this to the regular [tools]? *Yes, definitely*.";

Participants could "see" where "things" are in the network, helping them spatially perceive and understand the structure and topology of this computer network and networked entities' (nodes) positions and logical grouping inside that network ("Overview", as per (Shneiderman, 1996) taxonomy):

- [P1]: "*This agrees with me particular. I like visual. I always kind of visualize things, in a way like this. And this particularly agrees with me. That's very easy for me to understand.*";
- [P6]: "If you now look at this network diagram [printed on paper], does this looks familiar? *It is familiar, but very flat.* Would you prefer 3d? *Well, of course. This 2D looks like... why are we still using this.. it seems so.. like.. limited*.";
- [P2]: "*For our team this is a great representation of what we could use. This is a good representation of a network that would work for us. A way to visualize this and interact with."*;

Participants admitted that they perceived the traffic "going" between nodes, referring to the edges representing the count of sessions observed between these two nodes ("Relations" of groups, subgroups and nodes, as per the taxonomy):

- [P1]: "*They are clearly grouped, and I can see exactly where everything is going [which node has been connecting to what other nodes].*"
- [P4]: "*This would help a lot. You can see the traffic leaving networks and so...*"
- [P5]: "*This makes a lot of sense to me. I really like the visualization. I can see.. there's the first firewall, DMZ.. I can kind of understand how the network is built...*"
- [P2]: "*This is useful... and this seems very utilizable. Useful in terms of what's reaching out to what. There's definitely usefulness in this for what we do here. [..] This makes much sense for what we do here in terms of usefulness and utility...*"

Participants recognized the advantages of using such visualizations could provide to transfer knowledge about specific networks from senior analysts to trainees:

- [P6]: "*Since I've been here for 4 years, I've trained about 80 people. I think if we'd have something like that from the start, it would change their whole perception of how to [think of networks] and jump start [their ability to work the networks]. [...] I think a lot of analysts would have different views, that would depend on their knowledge base and artistic side also. [..] When you're using tool like this, when you build your network diagrams, you would like to have same setup, that way [when] you're looking at them on a pdf, you'd have the same layout.*"

Participants suggested capabilities (see correlation with taxonomy, described in Introduction and (Shneiderman, 1996)), that they would like to have at their disposal:

- [P9]: "*This is awesome! [..] As an analyst I would want to see [in addition to the visualization] what's happening, the [textual] details. [..] It is cool; you could definitely do a lot with it. [..] This is one of the coolest things I've ever seen. But I do need [additional, textual] information. As an analyst, I could definitely use this. [..] I could probably play with this all day.*";
- [P1]: "*[It] would be nice to control how far apart they [nodes, groups] are. Would be easier to navigate between them. [..] [option to] change the icon of the node to something that would indicate the function of the entity. I would prefer to use colors for grouping the entities.*";
- [P3]: "*Color-code the layers in the network. Any host that is associated [has had sessions] with those should also be color accordingly. 6DOF movement should be available.*";
- [P6]: "*Lines should have arrows showing the direction of the sessions.*";

5. Conclusion

This study captured cybersecurity analysts' impressions of a network topology presented as a stereoscopically-perceivable 3D structure. Overall, the impressions towards stereoscopically-perceivable 3D data visualizations were highly favorable. Multiple participants acknowledged that such 3D visualizations of network topology could assist in their understanding of the networks they use daily. Participants expressed a wish to integrate such visualization capabilities in their workflow. Prior experience with 3D displays had no influence on user preferences, while participants with prior gaming experience adjusted quickly to the Oculus Touch motion controllers, suggesting that the relevant dexterity and muscle memory for gaming console controller usage helps users adjusting from those controllers to handling input devices for VR experiences. Further research is needed to understand what specific 3D data shapes would be useful and for which datasets (e.g. computer network topology) to create additional 3D visualization suitable for analysts' preferences and test the usefulness of those visualizations. Follow-up studies should evaluate operator performance in 3D environments.

6. Acknowledgements

For all the hints, ideas and mentoring, authors thank Jennifer A. Cowley, Alexander Kott, Lee C. Trossbach, Jaan Priisalu, Olaf Manuel Maennel. 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.

7. References

Arthur, K. W., Booth, K. S., & Ware, C. (1995, 7). Evaluating 3D Task Performance for Fish Tank Virtual Worlds. *ACM Transactions on Information Systems, 11*(3), 239-265. doi:10.1145/159161.155359

Aukstakalnis, S. (2017). *Practical Augmented Reality.* Addison-Wesley.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51-61.

Berry, S. P. (n.d.). *The Shoki Packet Hustler*. Retrieved from http://shoki.sourceforge.net/

Best, D. M., Endert, A., & Kidwell, D. (2014). 7 Key Challenges for Visualization in Cyber Network Defens. *In Proceedings of the Eleventh Workshop on Visualization for Cyber Security* (pp. 33-40). ACM.

Burnett, M. S., & Barfield, W. (1991). Perspective versus plan view air traffic control (ATC) displays - Survey and empirical results. *International Symposium on Aviation Psychology, 6th.* Columbus. Retrieved from http://adsabs.harvard.edu/abs/1991STIA...9244967B

Dennehy, M. T., Nesbitt, D. W., & Sumey, R. A. (1994). Real-Time Three-Dimensional Graphics Display for Antiair Warfare Command and Control. *Johns Hopkins APL Technical Digest, 15*(2), 110-119.

Ehrenstein, W. H., Spillmann, L., & Sarris, V. (2003). Gestalt Issues in Modern Neuroscience. In *Axiomathes* (pp. 433-458). Springer.

Gaw, T. J. (2014, 4). 3D Information Visualization of Network Security Event. Munice, Indiana, USA: Ball State University. Retrieved from https://pdfs.semanticscholar.org/f3fa/c8a059369b96202a70ceb19828c07444dc42.pdf

Gazzaniga, M. S., Ivry, R. B., & Mangun, G. R. (2013). *Cognitive Neuroscience: The Biology of the Mind, 4th Edition.* W. W. Norton & Company.

Gershon, P., Klatzky, R. L., & Lee, R. (2014). Handedness in a virtual haptic environment: Assessments from kinematic behavior and modeling. *Acta Psychologica*, 37-42.

Gershon, P., Klatzky, R. L., Palani, H., & Giudice, N. A. (2016). Visual, Tangible, and Touch-Screen: Comparison of Platforms for Displaying Simple Graphics. *Assistive technology: the official journal of RESNA, 28*(1), 1-6. doi:10.1080/10400435.2015.1054566

Gonzalez, C., Ben-Asher, N., Oltramari, A., & Lebiere, C. (2014). Cognition and technology. *In Cyber defense and situational awareness*, 93-117.

Hodent, C. (2018). *The Gamer's Brain; How Neuroscience and UX Can Impact Video Game Design.* CRC Press.

Hurter, C. (2016). *Image-Based Visualization: Interactive Multidimensional Data Exploration.* (N. Elmqvist, & D. Ebert, Eds.) Morgan & Claypool.

Inoue, D., Suzuki, K., Suzuki, M., Eto, M., & Nakao, K. (2012). DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System. *VizSec* (pp. 72-79). ACM.

Kirk, A. (2016). *Data Visualisation, A Handbook for Data Driven Design.* Sage.

Kullman, K., Cowley, J. A., & Ben-Asher, N. (2018). Enhancing Cyber Defense Situational Awareness Using 3D Visualizations. *Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018: National Defense University, Washington DC, USA 8-9 March 2018* (p. 369−378). Washington DC: Academic Conferences and Publishing International Limited.

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). Retrieved from http://ieeexplore.ieee.org/document/6269042/

Lynn, W. J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs, 89*(5), 97-108. Retrieved from https://city.rl.talis.com/items/71ACA705-9A0A-8C2B-EAD3-5FF314AAC847.html

Maddix, K. (2015). *Big Data VR Challenge – Winners!* Retrieved from Masters of Pie: http://www.mastersofpie.com/big-data-vr-challenge-winners/

Marty, R. (2008). *Applied Security Visualization.*

Meyerovich, L., & Tomasello, P. (2016). Display Relationships Between Data. *IQT Quarterly, 7*(4).

Munzner, T. (2014). *Visualization Analysis & Design.* A K Peters/CRC Press.

Payer, G., & Trossbach, L. (2015). The Application of Virtual Reality for Cyber Information Visualization and Investigation. In M. Blowers, *Evolution of Cyber Technologies and Operations to 2035* (Vol. 63, pp. 71-90). Springer. doi:10.1007/978-3-319-23585-1_6

Pruett, C. (2017, 05 17). Vision 2017 - Lessons from Oculus: Overcoming VR Roadblocks. Retrieved from https://youtu.be/swA8cm8r4iw?t=9m42s

Rajivan, P., Konstantinidis, E., Ben-Asher, N., & Gonzalez, C. (2016). Categorization of Events in Security Scenarios: The Role of Context and Heuristics. *Human Factors and Ergonomics Society Annual Meeting, 60*(1), 274-278.

Reda, K., Febretti, A., Knoll, A., Aurisano, J., Leigh, J., Johnson, A., . . . Hereld, M. (2013). Visualizing large, heterogeneous data in hybrid-reality environments. *IEEE Computer Graphics and Applications, 33*(4), 38-48.

Reuille, T., Hawthorne, S., Hay, A., Matsusaki, S., & Ye, C. (2015). *OpenDNS Data Visualization Framework*. Retrieved from OpenGraphiti: http://www.opengraphiti.com/

Schneider, W., Dumais, S. T., & Shiffrin, R. N. (1982). *Automatic and Control Processing and Attention.* Illinois: University of Illinois. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a115078.pdf

Sethi, A., & Wills, G. (2017). Expert-interviews led analysis of EEVi — A model for effective visualization in cyber-security. *IEEE Symposium on Visualization for Cyber Security* (pp. 1-8). Phoenix, AZ, USA: IEEE.

Shearer, G., & Edwards, J. (2018). *Vids: Version 2.0 Alpha Visualization Engine.* Adelphi: US Army Research Laboratory.

Shneiderman, B. (1996). The eyes have it: a task by data type taxonomy for information visualizations. *Proceedings 1996 IEEE Symposium on Visual Languages.* Boulder, CO, USA, USA: IEEE. doi:10.1109/VL.1996.545307

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), 51-57. Retrieved from http://journals.sagepub.com/doi/pdf/10.1518/001872001775992534

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, Spring*, 79-98. Retrieved from http://journals.sagepub.com/doi/pdf/10.1518/001872001775992534

U.S. ARL. (2018, 02 12). SEEING THE CYBERTHREAT. Aberdeen Proving Ground, Maryland, USA: U.S. Army Research Laboratory. Retrieved from https://dodstem.us/sites/default/files/lab-narratives/Seeing-the-Cyberthreat_0.pdf

van Riel, J.-P., & Irwin, B. (2006). InetVis, a Visual Tool for Network Telescope Traffic Analysis. *AFRIGRAPH 2006.* Cape Town: Association for Computing Machinery, Inc.

Ward, M. O., Grinstein, G., & Keim, D. (2015). *Interactive Data Visualization: Foundations, Techniques, and Applications, Second Edition.* A K Peters/CRC Press .

Ware, C., & Franck, G. (1996, 4). Evaluating Stereo and Motion Cues for Visualizing Information Nets in Three Dimensions. *ACMTransactions on Graphics, 15*(2), 121-140. doi:10.1145/234972.234975

Wu, Y., Xu, L., Chang, R., Hellerstein, J. M., & Wu, E. (2018). Making Sense of Asynchrony in Interactive Data. *JOURNAL OF LATEX CLASS FILES, 14*(8).