3DSVAT: A 3D Stereoscopic Vulnerability Assessment Tool for Network Security

Troy Nunnally *, A. Selcuk Uluagac†, John A. Copeland*, and Raheem Beyah†
*CSC Lab., The School of ECE
Georgia Institute of Technology
Atlanta, GA 30332,USA
{troy.nunnally,jcopeland}@gatech.edu
†GT CAP Group, The School of ECE
Georgia Institute of Technology
Atlanta, GA 30332, USA
{selcuk,rbeyah}@ece.gatech.edu

***Abstract*—As the volume of network data continues to increase and networks become more complex, the ability to accurately manage and analyze data quickly becomes a difficult problem. Many network management tools already use two-dimensional (2D) and three-dimensional (3D) visualization techniques to help support decision-making and reasoning of network anomalies and activity. However, a poor user interface combined with the massive amount of data could obfuscate important network details. As a result, administrators may fail to detect and identify malicious network behavior in a timely manner. 3D visualizations address this challenge by introducing monocular and binocular visual cues to portray depth and to increase the perceived viewing area. In this work, we explore these cues for 3D network security applications, with a particular emphasis on binocular disparity or stereoscopic 3D. Currently, no network security tool takes advantage of the enhanced depth perception provided by stereoscopic 3D technologies for vulnerability assessment. Compared to traditional 3D systems, stereoscopic 3D helps improve the perception of depth, which can, in turn reduce the number of errors and increase response times of network administrators. Thus, we introduce a stereoscopic 3D visual Framework for Rendering Enhanced 3D Stereoscopic Visualizations for Network Security (FRE3DS). Our novel framework uses state-of-the art 3D graphics rendering to assist in 3D visualizations for network security applications. Moreover, utilizing our framework, we propose a new 3D Stereoscopic Vulnerability Assessment Tool (3DSVAT). We illustrate the use of 3DSVAT to assist in rapid detection and correlation of attack vulnerabilities in a subset of a modified local area network data set using the enhanced perception of depth in a stereoscopic 3D environment.**

***Index Terms*—Stereoscopic 3D, Security Visualization, Vulnerability Assessment Tool**

I. Introduction

Administrators are often given tasks to evaluate security risks and malicious activity of Internet Protocol (IP) traffic and logs from vulnerability scanners, intrusion detection systems (IDSs), firewalls, and host systems on a network. In the past, administrators examined and analyzed network activity and behavior using textual representations [1], [2]. However, as data volume increases and networks become more complex, textual representations and raw data become overwhelming, vital data could be potentially overlooked, and the time span for analyzing data could be lengthy.

Recently, researchers have attempted to convert abstract network data into visual representations in order to quickly discover and identify malicious activity and network behavior [3]. Network visualization takes advantage of the visual system's large spatial bandwidth in order to efficiently represent network characteristics. Moreover, this large spatial bandwidth significantly dominates other senses and the brain processes visual information in parallel, consequently increasing temporal bandwidth [4]. As a result, humans can efficiently recall more visual representations and evaluate large amounts of visual data more quickly and accurately than textual data.

2D visualizations produce representations on the x and y axes to identify, detect, and analyze malicious information. A large amount of work has been done in the area of visualizing IDS logs [5], [6], network management systems [7], [8], and firewalls [9] in 2D. However, as the amount of information increases, visualizing considerable amounts of 2D information can be perceived as cluttered and limited [10]. Thus, researchers address this issue by looking into methods for expanding visualization techniques to incorporate the z-direction [11], [12]. The addition of the z-direction or depth for 3D allows n^2 more information to be visualized than its 2D counterparts [13] and results in clearer representations [6], [10]. Furthermore, this reduction in clutter assists network security administrators in precisely identifying a substantial amount of malicious information and gaining a more precise and accurate global view of the data's structure. Moreover, it has been shown that 3D visualization increases awareness by allowing one to identify and recall more attributes based on spatial qualities [14] and demonstrate improved performance in spatial memory tasks when visualizing large sets of hierarchical data [15]. These attributes are beneficial when visualizing IP address spaces, Domain Name System (DNS) hierarchies, and categorization of network attributes. Also, network administrators can quickly recall attacks and attributes of attacks by using metaphorical 3D visualizations rather than textual representations. Users identify with metaphorical 3D interfaces since individuals naturally view the physical world in 3D. This concept is useful in network security visualization by metaphorically relating 3D objects to network properties. Harrop et. al. illustrate this concept by using 3D game engines to metaphorically represent real-time network monitoring and control [16].

The third dimension adds its own complications and complexities. One key challenge for implementing 3D security tools is that they must be designed to accurately depict objects

978-1-4673-1564-7/12/$31.00 ©2012 IEEE

in 3D space on an inherently flat 2D computer screen. If objects are portrayed incorrectly, the network visualizations are more prone to human error because network administrators would have a difficult time formulating concise cognitive decisions. In order to accurately depict depth on 2D screens, 3D interface designers use various psychological and cognitive properties to indicate depth. These cues help users easily locate, manipulate, and depict spatial relationships between objects. Some cues include shadowing, perspective, lighting, texturing, binocular disparity, and motion parallax [17]. Current 3D network security visualizations lack important depth cues and result in higher error rates and slower decision times. Research has shown that by introducing the major depth cue of binocular disparity, the visual cue for *stereoscopic 3D* applications, significant reduction in errors and enhanced response times compared to its non-stereoscopic 3D counterparts can be achieved [18]. It has also been shown that stereoscopic 3D is superior to any monoscopic viewing, and to any shadow condition, for enhancing accuracy positioning and resizing tasks of objects located in 3D space [19]. Thus, network security could benefit from the creation of a stereoscopic tool that could potentially reduce error and enhance response rates.

Recently, the gaming, television, computer-aided design, medical, and video graphics industries introduced stereoscopic 3D technologies to enhance the perception of depth. Also, auto-stereoscopic applications have been introduced in 3D smart phones and cameras. Auto-stereoscopic refers to using binocular parallax without special devices such as headgear or glasses. According to a *MarketsandMarkets*, a marketing research firm, global 3D technology-products and applications market is expected to reach $227.27 billion by 2016 [20]. Since the 3D market is growing tremendously in the upcoming years, 3D technologies are becoming more readily available, and security interface designers must begin considering and designing stereoscopic 3D tools for complex tasks, large node sets, and important vulnerability data. Currently, no tool or framework exists that allows 3D stereoscopy for network vulnerability data. This paper introduces a 3D stereoscopic tool - *3D Stereoscopic Vulnerability Assessment Tool* (3DSVAT) for analyzing vulnerability data and discusses a framework to assist 3D designers with creating future 3D stereoscopic tools.

The rest of the paper is organized as follows. Background on Visual Cue Theory and its relationship to network security visualization is presented in Section 2. Next, related work is discussed in Section 3. We propose a methodology and framework, FRE3DS, for assisting in situational awareness for vulnerabilities in local area networks in Section 4. Next, we propose 3DSVAT, our tool for assessing vulnerabilities on a local area network, in Section 5. Finally, we conclude the paper and discuss the future work in Section 6.

II. Background

A. Visual Cue Theory in Network Security

Monoscopic or non-stereoscopic 3D, hereafter known as 3D, refers to the depiction of a 3D environment using 2D perspective projections. Since displays are physically constrained to 2D projections, visual cues are required to adequately represent depth. Simply put, these cues create a perception of 3D objects on a 2D plane. When representing network security data, objects become 3D items such as spheres in 3D link graphs or points in 3D scatter plots. These cues are grouped into two categories: monocular and binocular. Monocular cues are depth cues that require only one eye to depict depth whereas binocular depth requires two eyes to depict depth. Some well-known monocular cues in network security are perspective, size, texture, occlusion, and shadows. If these cues are used correctly, then obscurities and confusion in network security visualization can be reduced. For example, if IP addresses are represented as spheres, and the size of the spheres represent the amount of data entering the node, the node's information cannot be accurately portrayed without a visual cue such as shadowing to denote where the object is in respect to other objects. 3DSVAT uniquely uses both monucular cues such as perspective, size, and occlusion and binocular cues such as binocular disparity to reduce error. Thus, allowing users to identify data more quickly and to accurately display complex information [21].

TABLE I: Visual Cues in Network Security

Utilization of Visual Cues in Network Security Tools	
Monocular Cues	***3D Visualization Tool***
Perspective	[16], [22], [23], [24], [25], [26]
Size	[16], [22], [25]
Texture	[16], [20]
Occlusion	[27], [16], [22], [23], [20], [24], [28], [25], [26]
Shadows	[16], [22], [20]
Motion Parallax	None
Binocular Cues	***3D Visualization Tool***
Binocular Disparity	[27]

Table 1 shows a collection of network security tools and their associated visual cues. Below is a explanation of both monocular cues and binocular.

- *Perspective* is the notion that parallel lines moving towards infinity converge to a point on a 2D plane. For example, parallel train track rails appear to meet at the horizon. Perspective is commonly used in network visualization to add more visualization data.
- *Size* refers to the relative position of the two objects of the same known size. If two objects are known to be the same size at the same distance and one object is positioned at a closer distance, the object's size appears to be larger relative to the other object.
- *Texture* represents the level of detail used to represent an object. As objects move closer, the texture becomes clearer but as objects move away, the texture appears obscure.
- *Occlusion* is the slight blocking of one object by another.
- *Shadows* occur when the shadow of an object is visible on the object or on different objects.
- *Motion parallax* refers to the spatial properties within motion. The movement of the camera or the object can give spatial properties about the 3D location of the object.

When an observer moves, absolute depth information of the distance can be determined from several stationary objects if the velocity and the direction are known. Closer objects appear to pass more quickly than objects further away.

As shown in Table 1, many security tools use monocular cues. However, a small number of tools currently use binocular cues. Examples of binocular cues include *binocular disparity*, *convergence*, and *accommodation*. Accommodation refers to the physical adjustment of the ciliary muscles in the eye when moving the focus on particular objects. When focusing on far objects, the lens decontracts and increases the focal length. Convergence is the inward movement of the eyes in an effort to maintain a single binocular vision of an object. Binocular disparity, also called binocular parallax, uses the notion that each eye within the visual system views two slightly unique retinal images. When the brain processes these images, it appears to give the illusion of depth. Binocular disparity enhances the perception of depth. *Due to these depth illusion qualities, binocular disparity can be used for network security in situations where monocular depth cues do not adequately reveal enough information about the network's security posture.* Binocular disparity is a primary physiological characteristic that enables the stereoscopic viewing of objects within a limited distance and is widely used for portraying virtual objects (e.g., images on a computer screen) in real 3D space. On the other hand, using accommodation and convergence to portray virtual objects in real 3D space is a challenge. As will be explained later, 3DSVAT uses binocular disparity to enhance vulnerability awareness and decrease response times for detecting vunerable nodes.

B. 3D Stereoscopic Overview

The stereoscopic rendering environment consists of two cameras: the right eye camera and the left eye camera. The usage of cameras is commonly used to create the environment in all 3D stereoscopic applications including 3D movies and 3D software. Each camera is separated with the average eye separation of 6.2 centimeters to mimic the average human eye separation. The cameras are positioned parallel to each other and perpendicular to the projection plane. In stereoscopic 3D, both the projection plane and the viewport are considered as the physical monitor. Likewise, the width and length of the viewport represents the length and width of the computer screen in pixels.

Before each visualization is rendered, each camera creates an off-axis frustum with the projection plane. The viewing angle or fovy of the camera is denoted by the lowercase ϕ symbol as shown in Figure 1. The distance between the camera and the projection plane is the focal length. The left and right cameras produce a left and right image, respectively. As shown in the above figure, the left and right images are two slightly unique perspectives of one image and this image is perceived to be behind the screen. This concept is used in both the FRE3DS framework and 3DSVAT tool when generating a 3D environment.

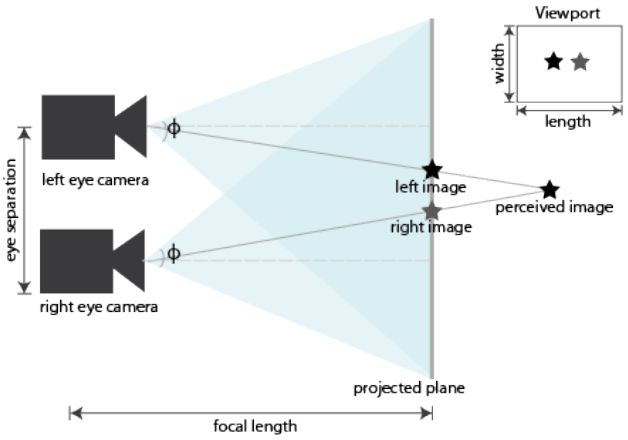

Fig. 1: 3D Stereoscopic rendering for an image using left and right image.

III. Related Work

A. 3D Security Visualization

Existing 3D visualizations have been created to visualize data from IDSs [28] using techniques such as iconic tree structures, bar charts [22], and 3D scatter plots [11]. In addition, researchers have used various techniques to represent a larger number of attributes such as the size of a packet's payload in bytes, the number of packets, and interarrival time. The primary benefit of these visualizations is that they adequately portray generalizations of a network's behavior. However, they do not consider the error due to small subtleties in various attributes that could potentially be addressed using stereoscopic depth cues. Visual Autonomous System Topology (VAST) [24] uses link graphs to extract information from Border Gateway Protocol (BGP) routing messages to assist in understanding topological properties of the Internet and Autonomous System (AS) behavior. VAST uses quad-tree based visualizations to represent Autonomous System Numbers (ASNs) on a 3D plane. This tool successfully shows leaks from one AS to another. When a large number of ASes are present, it is a challenge to determine the depth of an ASN due to lack of visual cues. VAST can use our framework to more accurately distinguish the depth between ASes when large amounts of ASes are present.

Scapy's trace 3D function [29] visualizes a 3D traceroute representation based on a linked graph. Likewise, Ipv6World [29] uses a similar method to visualize an IPv6 topology. Both Scapy 3D and Ipv6world portray a Python-based 3D linked graph using Real-time 3D visualization of linked graphs (RT3DG) with a fluid friction force physics engine. The Spinning Cube [11] visualization uses 3D scatter plots to represent network activity on three axes: the destination IP of the local network on the x-axis, the destination port on the y-axis, and the source IP on the z-axis. We can contribute to these tools by uniquely considering vulnerability scans or correlating the vulnerabilities across these networks. Papadopoulos discusses CyberSeer [27], a desktop interactive immersive auto-

stereoscopic 3D environment. The environment is integrated with multi-channel immersive sound to enhance security awareness. It introduces a 3D auto-stereoscopic environment to analyze spatial information for intrusion detection [27]. Compared to this tool, we introduce a framework that will allow better integration with other tools to produce a more wholelistic 3D stereoscopic toolset.

Nessus 3D [30] uses a top-down approach of the security vulnerabilities. This node-based visualization assists in showing the number of vulnerabilities per node, TCP and UDP blacklisted connections, and patch updates. Our tool differentiates itself by correlating vulnerabilities of multiple nodes across multiple exploits and groups the vulnerabilities for simpler evaluation. Thus, giving administrators a better depiction of the overall vulnerabilities of the network and therefore, the opportunity to prioritize patch updates. Furthermore, our tool possesses a 3D stereoscopic component, which more accurately portrays large datasets and reduces response time in detecting extremely vulnerable hosts.

B. 3D Stereoscopy Overview

A substantial amount of stereoscopic work has been done in the areas of human computer interaction (HCI) [19] and robotics [31], [32]. Currently, no research exists that uses stereoscopic 3D to provide situational awareness for vulnerable networks. In the field of HCI, researchers have found that stereoscopic 3D is superior to monoscopic viewing, with or without shadow conditions, for enhancing positioning and resizing accuracy and response time [19]. The use of stereoscopic 3D attributed to a 22% reduction time compared to the use of non-stereoscopic visualizations while performing positioning tasks. With stereoscopic 3D, individuals can perceive large amounts of visual information, especially if 3D binocular senses are present. Thus, network administrators can manipulate multidimensional data and transform it into a simplified representation for easy analysis. This visualization is useful in top-down network security tools, that give an overall state of the network and allows the user to manipulate views of data to analyze network data at different levels of granularity. Other stereoscopy work in HCI domain focuses on examining the human error and response times for tracing link-node graphs [18]. The work in [18] shows that 3D depth cues allowed participants to see paths in graphs containing 333 nodes with better than 92% accuracy. Also, it showed that stereoscopic conditions resulted in the shortest response times. Additionally, stereoscopic conditions possess substantially lower percent error than non-stereoscopic conditions for large node sets, particularly 333+ nodes for non-skilled users and skilled observers could see up to a 1000-node graph with less than a 10% error rate. This is an order of magnitude better than the error rate of 2D visualizations. Tracing node-link graphs is commonly used in network security visualizations such as those that visualize IPv6 topologies [22], [24], [29]. Other 3D stereoscopic techniques have been used in robotics, construction, and teleoperation applications (for performing dexterous tasks to control machines in real-time from a remote location). Within teleoperation applications, the remote operators were asked to achieve the requested pick-and-place task swiftly, without any collisions with obstacles. The results show that the operator saved more than 60% of his/her time when completing pick-and-place tasks with 3D stereoscopic visual feedback than its 2D monoscopic counterparts [31], [32]. Thus, 3D spatial positioning of objects can better portray using depth in 3D stereoscopic viewing in visual feedback systems. Our tool and framework take advantage of this HCI and robotic research and apply it to network security to help reduce human error and increase response times of network security administrators.

IV. FRE3DS: A Framework for Rendering Enhanced 3D Stereoscopic Visualization

A. System Implementation

The Framework for Rendering Enhanced 3D Stereoscopic Visualization (FRE3DS) uses rapid prototyping for 3D network security visualizations with stereoscopic support. This framework is useful for producing rapid customized 3D visualizations so that network administrators can easily and quickly develop various visualizations to efficiently investigate data.

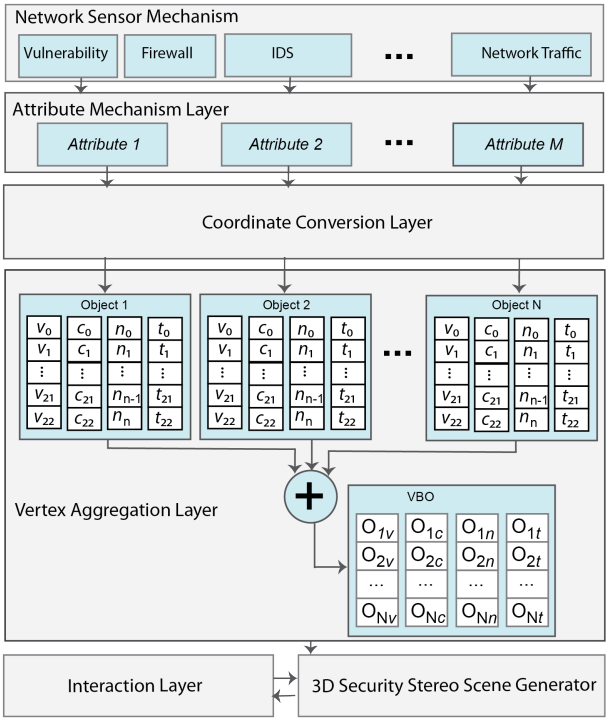

Fig. 2: FRE3DS Layer Model.

The framework uses the C++ Object Oriented Model-View-Controller paradigm for higher modularity and extensibility. We used a custom OpenGL 3D widget within a QT framework for its cross-platform capability. Thus, our framework compiles and runs on Windows, GNU/Linux and Mac OS X operating systems. To render the content in stereoscopic 3D, we used an Nvidia Quadro 2000, Nvidia RF 3D Vision Pro

Shutter Glasses, and a 120 Hz Asus 3D monitor for 60Hz screen rendering per eye as shown in Figure 3.

Fig. 3: Stereoscopic 3D Visualization Testbed.

The framework uses a layered approach. It takes as input raw data and outputs a 3D stereoscopic visualization. In the first layer, a sensor mechanism is used to collect data from various systems including vulnerability scanners, firewalls, IDSs, keyloggers and network traffic analyzers. Essentially, most network sensors can plug into our framework as modules for easy data visualization. The network sensor provides raw data to the *Attribute Mechanism Layer* (AML) that parses, filters, and stores relevant data such as firewall logs or port numbers as attributes into a storage location for quick and easy retrieval.

Next, each attribute is sent to the *Coordinate Conversion Layer* (CCL). The CCL converts the security attributes into 3D environment coordinates. Each coordinate is determined by the type of visualization and depends on the visual representation for each attribute. Next, each coordinate is converted into objects. Objects are actually visual representations for a particular attribute such as cubes, lines, and planes. Each object contains a vertex array $v0, v1, \ldots, vn$, a color array $c0, c1, \ldots, cn$, a texture array $t0, t1, \ldots, tn$, and a normal array $n0, n1, \ldots, nn$ as in typical 3D graphics rendering. The vertex array consists of the vertices of objects being displayed. For example, if an IP source address is represented as a cube, then its vertex array contains 24 vertexes created from one (x,y, z) coordinate. The color array contains the color coordinates of the object. For example, a high threat vulnerability object can possess color coordinates as red.

The texture coordinates are coordinates for objects. Texture coordinates are beneficial when OS logos are textures on objects for OS fingerprinting. Normal coordinates are vectors that are perpendicular to the surfaces of the object and used to enhance lighting and shadowing depth cues. Each object is aggregated into a memory allocation array of vertex arrays and sent to the *3D Security Stereo Scene Generator* (SSG).

The SSG adjusts the OpenGL rendering pipeline using quad-buffer technologies. SSG takes the object data and passes it through the OpenGL rendering pipeline. The SSG generates two separate rendering pipelines for each eye. In addition, the SSG coordinates with the interaction layer to regenerate the screen based upon user input. The right and left visualizations are stored to a right and left back buffer. When the object is rendered to the page, the right and left back buffers swaps with the right and left front buffers. As a result, the security visualization is presented to the user. The pipeline creates two cameras, a left and right camera with a distance of 6.3 centimeters with off-axis frustums and the focal length positioned at the screen. If an object is positioned with a positive z-axis value, the object is positioned within the focal length of the user's eye and appears to be in front of the 3D monitor. We use this visualization concept to display vulnerable nodes in front of the monitor for rapid vulnerability detection. Moreover, the user can manipulate and interact with the 3D interface by zooming, panning, and selecting by taking the newly generated vertex data and passing it back through the pipelines.

V. 3DSVAT: 3D Stereoscopic Vulnerability Assessment Tool

A. Visualization Design

Currently, no visualization exists that focuses on 3D stereoscopic vulnerability correlations between nodes. Thus, we propose the 3D Stereoscopic Vulnerability Assessment Tool (3DSVAT), which assists in rapid detection of vulnerable nodes using severity level as a function of depth. Furthermore, 3DSVAT uniquely represents the network topology based on correlations of the vulnerable data for monitoring network vulnerabilities, management of patch updates, and correlating vulnerabilities and nodes on a local area network. Consequently, this tool is useful for network situational awareness.

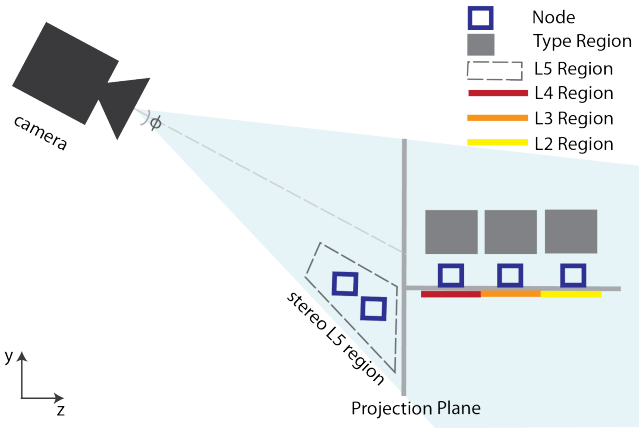

Fig. 4: Side View of 3DSVAT Visual Layout.

3DSVAT distinctly shows an aerial perspective visualization based on x, y, and z coordinate systems. This visualization uses the FRE3DS Framework to retrieve attribute input from the Qualys Guard Vulnerability [33] assessment tool. The

Attribute Mechanism Layer parses and filters the following relevant attributes: IP, OS, Vulnerability Severity Score, and the Common Exposure Vulnerability (CVE) identification number. Next, the CCL converts each attribute into 3D coordinates. The CCL converts severity scores into coordinates for bar graphs, OSes into textures, IP address into sets of cubes based on severity, and CVE identification numbers into scatter plots. The vertex aggregation layer combines these vertexes and passes them to the 3D scene generator. The 3D scene generator creates the left and right cameras, off-axis frustum, and other components essential for rendering an OpenGL environment. The 3D environment renders a stereoscopic visualization into three regions: the Grouped Vulnerability Region, Vulnerability Type Region, and Stereoscopic Region.

1) Grouped Vulnerability Region: The Group Vulnerability Region portrays grouped nodes by highest vulnerability score similar to the Qualys Guard Vulnerability assessment tool [33]. These groups of vulnerabilities are arranged from severity level 1 to 4. The levels are described below:

- A system is labeled as critical (level 4), denoted by the color red, if its vulnerabilities allow the compromise of highly sensitive information on a system.
- A system is labeled as serious (level 3), denoted by the color orange, if its vulnerabilities enable intruders to gain access to specific information, potentially misuse the host, or allow unauthorized use of services such as access to certain files, Denial of Service (DoS) attacks, or mail relay.
- Medium and minimal levels (Level 2/1), denoted by the color yellow, are triggered if the nodes' vulnerabilities enable intruders to collect specific information about the hosts, such as version of software.

The group of correlated vulnerabilities allows the administrator to determine which nodes are the most vulnerable on a network and most common vulnerabilities between nodes. Furthermore, this allows administrators to know which vulnerability to patch first. In addition to grouping, each node contains bar graphs showing the number of vulnerabilities of lower level grouped regions.

2) Stereoscopic Region: The Stereoscopic Region displays urgent level 5 vulnerabilities. The urgent level 5 vulnerabilities allow intruders to gain full control of hosts including full read and write access, remote code execution, and backdoors installations. Since urgent level 5, the highest severity level, contains vulnerabilities that pose the most serious threats, stereoscopic technologies are used to enhance awareness of vulnerable nodes. These nodes are positioned within the focal length. As a result, with stereoscopic technologies, the nodes within the Stereoscopic Region are perceived in front of the physical screen.

3) Vulnerability Type Region: The Vulnerability Type Region portrays how nodes in a grouped category correlate to specific vulnerabilities. A list of the common CVE identifiers is positioned horizontally along the y-axis and the number of nodes is positioned vertically along the z-axis. This region shows how specific vulnerabilities correlate to nodes on the network. For example, if there is only one point in the region, then all nodes share a single vulnerability. Furthermore, this section can be filtered based on types of vulnerabilities, such as buffer overflows or DoS attacks to introduce further details.

B. Implementation

The following figure shows a visualization of an 18-node LAN network using 3DSVAT. The vulnerability data is a subset of data taken from a large production network and modified to portray important capabilities of the 3DSVAT tool in a 192.168.3.0/24 subnet. This visualization shows some interesting correlations between the nodes and their vulnerabilities by introducing the z-direction. In contrast to 2D visualizations, this tool promotes scalability by visualizing multiple grouped LAN networks. In Figure 4, each node is grouped by the highest vulnerability level it possesses and is positioned along the z-axis. In this visualization, three nodes demonstrate level 5 vulnerabilities as the highest vulnerability level. Level 5 nodes are located in the stereoscopic region and when viewed with stereoscopic glasses, these three nodes (192.168.3.34, 192.168.3.78, and 192.168.3.84) are perceived to be in front of the monitor to increase the awareness of the network administrator.

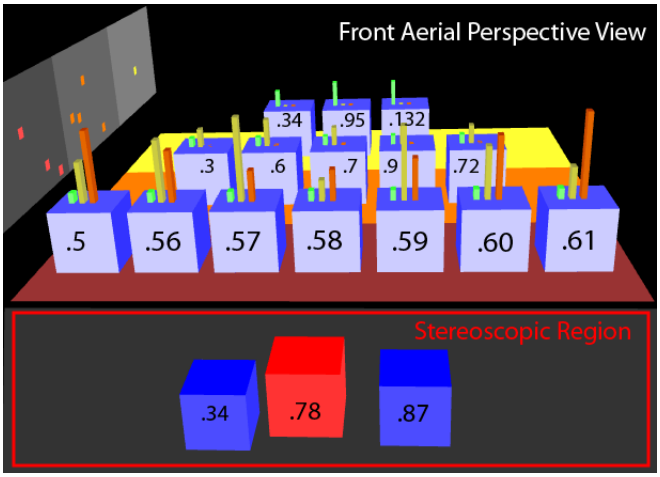

Fig. 5: 3DSVAT Aerial Front View Visualization for 18-node LAN.

A side view figure is given to better portray the location of the extremely vulnerable nodes within the visualization. Accordingly, they are perceived to be closer to the user. Also, as denoted in Figure 5, each node is categorized based on the highest vulnerability level it possesses. For example, 7 nodes possess level 4 vulnerabilities as the highest vulnerability level. Likewise, 5 nodes possess level 3 as the highest vulnerability level. If a level 5 node contains more than one vulnerability, the node is positioned closer to the user. The red node (192.168.3.78) represents a node where root access exploits can be quickly found by performing a simple Internet search. The red node list was compiled by comparing CVE data to well-known penetration testing sites.

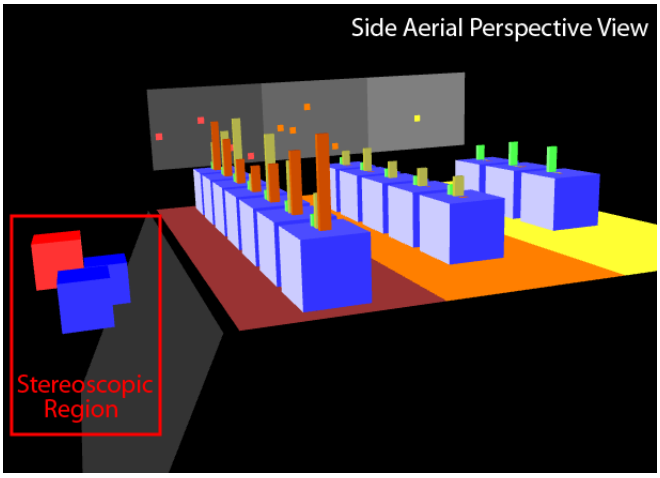

Fig. 6: 3DSVAT Aerial Side View Visualization.

In addition, the vulnerability type region demonstrates the specific vulnerabilities and how they correlate to the nodes in a group. For example, the yellow level 2 nodes 192.168.3.34, 192.168.3.95, and 192.168.3.132 share the same CVE-2002-0510 vulnerability type where all hosts are transmitting UDP packets with a constant IP Identification field. As a result, an attacker can fingerprint the operating system version and approximate kernel version of the three vulnerable systems. Within the level 4 nodes, multiple nodes share multiple vulnerabilities across multiple levels. Three level 4 nodes have vulnerabilities that can allow an attacker to use the NetBIOS access to steal a remote user list of authenticated accounts on the node, including guest accounts. In addition, level 4 nodes 192.168.3.6, 192.168.3.6.7 and 192.168.3.9 are susceptible to man-in-the-middle attacks. Moreover, the level 4 nodes contain a large number of orange bars. This illustrates that they also contain a large number of level 3 vulnerabilities. However, since there are seven nodes with level 4 vulnerabilities, a network administrator may decide to address the level 4 vulnerabilities first or the administrator may patch the level 5 nodes first to prevent computers from compromising the entire network. Nevertheless, this visualization allows the administrator to identify the best strategy possible, which complies with the security policies of the organization.

VI. Conclusions and Future Work

In this paper, we discuss the use of 2D/3D visualizations to analyze multidimensional data and format it into a form suitable for simplified human interpretation and analysis. Although there have been several studies on 2D/3D visualization techniques for network analysis, there has been little work on stereoscopic 3D techniques for network security visualization. FRE3DS allows administrators to absorb and perceive large amounts of visual information, particularly when the 3D senses are enabled by binocular vision. It renders both monocular and binocular depth cues to enhance the administrator's user experience, perform faster analysis of the network vulnerability data, reduce clutter, and increase efficiency. This framework is extremely beneficial in visualizing hierarchally spatial data such as subnets. The 3DSVAT tool uses this framework to reveal vital vulnerability characteristics of local area network data and determine correlations of vulnerability data between nodes. This is essential for strategically determining which node to patch first and rapidly determining highly vulnerable nodes on networks. In the future, we plan to adapt our visualization design to the IPv6 address space and the implementation of other depth cues and its effects on users. Also, we are interested in the implications of introducing head tracking in 300+ node visualizations. Overall, stereoscopic 3D visualizations in network security applications are promising for vulnerability awareness.

References

[1] S. Kakuru, "Behavior Based Network Traffic Analysis Tool," in *Proceedings of the 3rd IEEE International Conference on Communication Software and Networks (ICCSN)*, May 2011, pp. 649–652.

[2] S. Al-Mamory, A. Hamid, A. Abdul-Razak, and Z. Falah, "String Matching Enhancement for Snort IDS," in *Proceedings of the 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, Dec. 2010, pp. 1020–1023.

[3] J. Goodall, "Visualization is Better! A Comparative Evaluation," in *Proceedings of the 6th International Workshop on Visualization for Cyber Security (VizSEC)*, Oct. 2009, pp. 57–68.

[4] R. Friedhoff and M. Peercy, *Visual Computing*. New York: Scientific American Library, 2000, vol. 1.

[5] K. Abdullah, C. Lee, G. Conti, J. Copeland, and J. Stasko, "IDS RainStorm: Visualizing IDS Alarms," in *Proceedings of the IEEE Workshop on Visualization for Computer Security (VizSEC)*, Oct. 2005, pp. 1–10.

[6] H. Koike and K. Ohno, "SnortView: Visualization System of Snort Logs," in *Proceedings of the ACM Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC)*, 2004, pp. 143–147.

[7] Z. Kan, C. Hu, Z. Wang, G. Wang, and X. Huang, "Netvis: A Network Security Management Visualization Tool based on Treemap," in *Proceedings of the 2nd International Conference on Advanced Computer Control (ICACC)*, vol. 4, Mar. 2010, pp. 18–21.

[8] K. Lakkaraju, W. Yurcik, and A. J. Lee, "NVisionIP: Netflow Visualizations of System State for Security Situational Awareness," in *Proceedings of the ACM Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC)*, 2004, pp. 65–72.

[9] S. Krasser, G. Conti, J. Grizzard, J. Gribschaw, and H. Owen, "Real-time and Forensic Network Data Analysis using Animated and Coordinated Visualization," in *Proceedings fo the Sixth IEEE SMC Information Assurance Workshop (IAW)*, Jun. 2005, pp. 42–49.

[10] W. S. Ark, D. C. Dryer, T. Selker, and S. Zhai, "Representation Matters: The Effect of 3D Objects and a Spatial Metaphor in a Graphical User Interface," in *Proceedings of HCI on People and Computers*. Springer-Verlag, 1998, pp. 209–219.

[11] S. Lau, "The Spinning Cube of Potential Doom," *Commun. ACM*, vol. 47, no. 6, pp. 25–26, Jun. 2004.

[12] M. L. Huang, J. Zhang, Q. V. Nguyen, and J. Wang, "Visual Clustering of Spam Emails for DDoS Analysis," in *Proceedings of the 15th International Conference on Information Visualisation (IV)*, July 2011, pp. 65–72.

[13] C. Ware, *Information Visualization Perception for Design*. San Francisco, USA: Morgan Kaufmann, 2004, vol. 1.

[14] A. Carvajal, "Quantitative Comparison between the Use of 3D vs 2D Visualization Tools to Present Building Design Proposals to Non-Spatial Skilled End Users," in *Proceedings of the 9th International Conference on Information Visualisation (IV)*, Washington, DC, USA, 2005, pp. 291–294.

[15] A. Cockburn, "Revisiting 2D vs 3D Implications on Spatial Memory," in *Proceedings of the 5th Conference on Australasian User Interface*. Australian Computer Society, Inc., 2004, pp. 25–31.

[16] W. Harrop and G. Armitage, "Real-time Collaborative Network Monitoring and Control using 3D Game Engines for Representation and Interaction," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security (VizSEC)*. ACM, 2006, pp. 31–40.

[17] G. S. Hubona, P. N. Wheeler, G. W. Shirah, and M. Brandt, "The Relative Contributions of Stereo, Lighting, and Background Scenes in Promoting 3D Depth Visualization," *ACM Transactions on Computer-Human Interaction*, vol. 6, no. 3, pp. 214–242, Sep. 1999.
[18] C. Ware and P. Mitchell, "Visualizing Graphs in Three Dimensions," *ACM Transactions on Applied Perception*, vol. 5, no. 1, Jan. 2008.
[19] G. S. Hubona, P. N. Wheeler, G. W. Shirah, and M. Brandt, "The Relative Contributions of Stereo, Lighting, and Background Scenes in Promoting 3D Depth Visualization," *ACM Transactions on Computer-Human Interaction*, vol. 6, no. 3, pp. 214–242, Sep. 1999.
[20] E. Le Malécot, M. Kohara, Y. Hori, and K. Sakurai, "Interactively Combining 2D and 3D Visualization for Network Traffic Monitoring," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security (VizSEC)*, 2006, pp. 123–127.
[21] W. R. Hendee and P. N. T. Wells, *The Perception of Visual Information*. Springer, 1997.
[22] A. Oline and D. Reiners, "Exploring Three-Dimensional Visualization for Intrusion Detection," in *Proceedings of the IEEE Workshop on Visualization for Computer Security (VizSEC 2005)*, Oct. 2005, pp. 113–120.
[23] N. S. Team. Front End 3D (fe3D). http://map.gsfc.nasa.gov.
[24] J. Oberheide, M. Karir, and D. Blazakis, "VAST: Visualizing Autonomous System Topology," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security (VizSEC)*, 2006, pp. 71–80.
[25] Z. Jiawan, Y. Peng, L. Liangfu, and C. Lei, "NetViewer: A Visualization Tool for Network Security Events," in *Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC)*, vol. 1, April 2009, pp. 434–437.
[26] S. Krasser, G. Conti, J. Grizzard, J. Gribschaw, and H. Owen, "Real-time and Forensic Network Data Analysis using Animated and Coordinated Visualization," in *Proceedings from the Sixth IEEE Workshop on Information Assurance (IAW)*, June 2005, pp. 42–49.
[27] C. Papadopoulos, C. Kyriakakis, A. Sawchuk, and X. He, "Cyberseer: 3D Audio-visual Immersion for Network Security and Management," in *Proceedings of the ACM Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC)*, 2004, pp. 90–98.
[28] I. Xydas, G. Miaoulis, P.-F. Bonnefoi, D. Plemenos, and D. Ghazanfarpour, "3D Graph Visualization Prototype System for Intrusion Detection: A Surveillance Aid to Security Analysts," in *Proceedings of the 9th International Conference on Computer Graphics and Artificial Intelligence*, May 2006.
[29] RT Graph 3D. [Online]. Available: http://www.secdev.org/projects/rtgraph3d/
[30] Nessus 3D. [Online]. Available: http://www.tenablesecurity.com/
[31] W. T. Lo, W. K. Fung, Y. H. Liu, K. C. Hui, N. Xi, and Y. C. Wang, "Real-time Teleoperation via the Internet with 3D Stereoscopic Video Feedback," in *Proceedings of the IEEE International Conference on Robotics and Automation*, Apr. 2004.
[32] W. keung Fung, W. tai Lo, Y. hui Liu, and N. Xi, "A Case Study of 3D Stereoscopic vs. 2D Monoscopic Tele-reality in Real-time Dexterous Teleoperation," in *Proceedings of the IEEE International Conference on Intelligent Robots and Systems (IROS)*, Aug. 2005, pp. 181–186.
[33] QualysGuard. [Online]. Available: http://www.qualys.com/