P3D: A Parallel 3D Coordinate Visualization for Advanced Network Scans

Troy Nunnally *, Penyen Chi *, Kulsoom Abdullah †, 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, pchi7, kulsoom, 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 network attacks increase in complexity, network administrators will continue to struggle with analyzing security data immediately and efficiently. To alleviate these challenges, researchers are looking into various visualization techniques (e.g., two-dimensional (2D) and three-dimensional (3D)) to detect, identify, and analyze malicious attacks. This paper discusses the benefits of using a stereoscopic *3D parallel* visualization techniques for network scanning, in particular, when addressing occlusion-based visualization attacks intended to confuse network administrators. To our knowledge, no 2D or 3D tool exists that analyzes these attacks. Hence, we propose a novel *3D Parallel* coordinate visualization tool for advanced network scans and attacks called *P3D*. P3D uses flow data, filtering techniques, and state-of-the art 3D technologies to help network administrators detect distributed and coordinated network scans. Compared to other 2D and 3D network security visualization tools, P3D prevents occlusion-based visualization attacks (e.g., Windshield Wiper and Port Source Confusion attacks). We validate our tool with use-cases from emulated distributed scanning attacks. Our evaluation shows P3D allows users to extract new information about scans and minimize information overload by adding an extra dimension and *awareness region* in the visualization.**

***Index Terms*—Stereoscopic 3D, Security Visualization, Parallel Coordinate**

I. Introduction

Network administrators are making strong efforts to monitor and protect their network and protect against malicious attackers. These attackers often use scanning and enumeration tools [1] to find more topology information and vulnerable services within a network. Moreover, these attackers attempt to deceive Intrusion Detection Systems (IDSs) and visualization tools by performing stealthy scans such as scanning from multiple hosts on a network, spoofing source and destination hosts, and adding noise (e.g., sending repetitive scans from dozens of spoofed IPs) to trigger false positives and generate misleading information [2]. If these scans are detected before a node is compromised, network administrators could use these scans as precautionary indicators for future attacks, reveal less information about their network, and prevent compromised networks. Furthermore, detecting unusual network behavior could unveil the presence of malicious software and indicate vulnerabilities and compromised machines within a network.

In the past, administrators examined and analyzed reconnaissance activity and behavior using textual representations [3]. However, as data volume increases and networks become more complex, the time span for analyzing data will 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 [4]. These visualization techniques take advantage of the visual system's ability to process large amounts of information in order to efficiently represent network characteristics. As a result, humans can efficiently recall and evaluate more visual representations and data more quickly and accurately than textual data, thereby, revealing the "Who, What, When, Where, Why, and How" behind network attacks in a form which can be easily presented to users.

Researchers are looking into visualizing multi-dimensional datasets using 2D visualization techniques including glyphs, color maps, parallel coordinate plots, histograms and scatterplots [5]. However, 2D visualizations of large data sets become occluded and overwhelming, vital data can be potentially overlooked, and common visualization trends can be lost [6]. Furthermore, 2D visualization techniques can cause an information overload rendering the visualizations useless. Some researchers addressed this issue using filtering techniques to remove unwanted data [7]. However, due to inaccuracies of these filtering techniques, significant data is inadvertently removed. Thus, researchers have considered other methods for expanding visualization techniques such as incorporating the z-direction [8].

The addition of the z-direction or depth for 3D allows n^2 more information to be visualized than its 2D counterparts [9], reduces clutter, results in clearer representations, and provides a more precise and accurate global view of the data's structure [10]. Moreover, it has been shown that 3D visualization demonstrates improved performance in spatial memory tasks when visualizing large sets of hierarchical data [11]. These attributes are beneficial when visualizing large IP address spaces and larger sets of data. However, one key challenge for implementing 3D security tools is that they must be designed to accurately depict objects in 3D space on an inherently flat 2D computer screen. Incorrectly portrayed objects are more prone to human error because network administrators would have difficulty formulating concise cognitive decisions. Currently, researchers are using *stereoscopic* 3D technologies to enhance 3D space and increase awareness in visualizations

978-1-4673-3122-7/13/$31.00 ©2013 IEEE

[12]. Network security could benefit from the creation of a stereoscopic tool to potentially help reduce error, enhance response rates, and increase awareness of peculiar activity. Accordingly, various industries such as gaming, television, computer-aided design, medical, and video graphics have started introducing numerous stereoscopic 3D technologies and these technologies are becoming more readily available. With the success of stereoscopic 3D in other areas, we believe that interface designers for network security systems should also begin considering and designing stereoscopic 3D tools for complex tasks, large node sets, and port scanning techniques. To the best of our knowledge, no tool exists that enables 3D stereoscopy for advanced port scans and visualization attacks.

In this paper, we propose a novel visualization tool called *P3D*: A *P*arallel *3D* Coordinate Visualization for Advanced Network Scans which uses state-of-the art 3D graphics rendering and a novel 3D parallel coordinate visualization technique in identifying and analyzing distributed scanning attacks intended to thwart network administrators. We illustrate the use of P3D to assist in detection and increased awareness of distributed coordinate attacks. Moreover, by adding an extra dimension in the visualization, P3D prevents information overload and occlusion-based attacks, and administrators can extract new information about the scans. Using the enhanced perception of depth in a stereoscopic 3D environment, P3D includes a stereoscopic *awareness region* to help bring scans of interest to an administrators's attention without requiring filtering techniques so that significant data is not lost.

The rest of this paper is organized as follows. A background on visual cue theory, binocular disparity, and its relationship to port scanning is presented in Section 2. Next, related work is discussed in Section 3. We propose a methodology for P3D for assisting in detecting malicious scanning in local area networks in Section 4. Next, we validate P3D using various use-cases on a local area network, in Section 5. Finally, we conclude the paper and discuss 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, network parameters 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 visualizations are perspective, size, texture, occlusion, and shadows. Binocular disparity is a primary cue 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. As shown in Figure 1, 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 P3D when generating a 3D environment. Using binocular disparity, we can portray objects to be perceived as in front of the physical monitor. In P3D, the awareness region uses binocular disparity to portray scans in front of the monitor to prevent occlusion attacks from occurring.

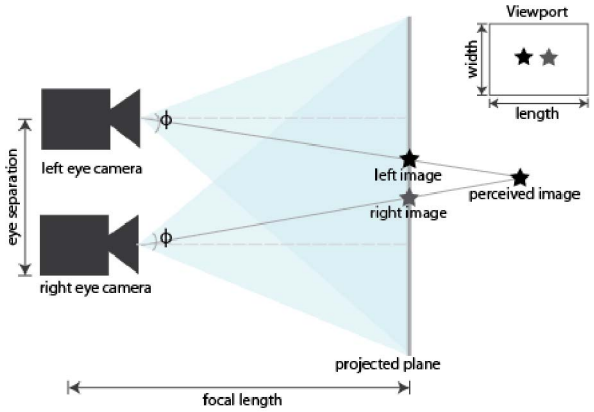


Fig. 1: 3D Stereoscopic rendering for an image using left and right image.

B. Scanning in Network Security

Attackers typically perform reconnaissance to gain information and intelligence about vulnerabilities in a network as a precursor to an attack. The addresses and ports scanned give insight into network details and services. If network Intrusion Detection Systems (IDSs) and visualization tools could quickly and accurately observe reconnaissance activities, measures can be taken to prevent network attacks. Attackers have been making visual detection of scans difficult. For instance, attackers can insert malicious data to reduce the effectiveness of a visualization system and overwhelm the administrator [2]. One such technique is an *occlusion attack*, which refers to attacks meant to obscure the display and hide malicious activity by overwriting old data with new data. As will be shown in Section V, P3D prevents certain occlusion attacks such as Port Source Confusion and the Windshield Wiper attack from occurring and still allows valuable information to be viewed.

III. Related Work

A. 2D Visualizations for Network Scanning

Existing 2D visualizations have been created to visualize network scans. Rumint [13] and parallel coordinate attack visualization (PCAV) [14] propose 2D Parallel Coordinates for detecting unknown large-scale Internet attacks including Internet worms, DDoS attacks and network scanning activities. PCAV uses hash algorithms to detect nine graphical signatures using a detection algorithm in addition to visual human monitoring. Some researchers use techniques such as brushing [15] to give some insight into the behavior of individual source

IP addresses. Brushing selects a specific coordinate or group of coordinates to focus on specific behaviors. However, brushing may become tedious when trying to select the behavior of one coordinate out of multiple coordinates. Scanveiwer [16] combines scatterplots, parallel coordinates, histograms and color maps into a single tool. However, occlusions due to large volumes of datasets result in cluttered visualizations and may cause data to be overlooked. In contrast to these techniques, P3D uses an awareness region mechanism to highlight important data and expand the visualization by using the 3rd dimension to help prevent occlusions.

B. 3D Visualizations for Network Scanning

Existing 3D visualizations visualize data from IDSs [17] using techniques such as iconic tree structures, bar charts [18], and 3D scatter plots [8]. 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.

PortVis [19] is a visualization tool that aids in detecting large-scale network security events and port activity. NetBytes Viewer [20] visualizes the historical network flow data per port of an individual host machine or subnet on a network using a 3D impulse graph plot. These tools only consider the 4-tuple: source IP, destination IP, source port, and destination port. Thus, these security events show a small amount of detail and only display the counts of activities rather than the activities themselves. Our tool enhances NetBytes Viewer by incorporating TCP fields such as RST, FIN, ACK, SYN and fragmentation bits. Various scanning events, such as stealthy intrusions at the firewall and IDS, can also be detected and identified.

The Spinning Cube of Potential Doom [8] 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. The color of the glyphs distinguishes the type of the connection (e.g., UDP or TCP). Their 3D scatter plots are useful in determining interesting patterns such as clusters or correlations for data using five parameters: source and destination IPs, source and destination ports, and connection type. Since the visualization is limited to five parameters, decoys cannot be detected without more parameters such as TCP flags and flow data. As a result, a deeper analysis of scanning behavior is not possible. P3D addresses these limitations by visualizing and incorporating more data, allowing it to help uniquely characterize port scans and further understand scanning activity. Additionally, P3D uses a stereoscopic region to increase awareness and reduce data overload.

IV. P3D Architecture

A. System Design

In order to display and detect stealthy scans, we have designed and implemented P3D. P3D uses the FRE3DS framework [21] to convert textual packet captures into a 3D visualization with stereoscopic 3D support and interactive techniques such as zooming and panning. The P3D system consists of 5 components: *Parser*, *Converter*, *Detector*, *Database*, and *Visualizer* as illustrated in Figure 2. Network packets are sent to the Parser. The Parser then extracts and filters relevant parameters from the packets and sends this data to the Converter. The data is filtered as follows: IP, Average Packet Size, Source and Destination Port, IP ID, Fragmentation bit, Timestamp, and TCP header flags such as SYN, FIN, URG, and PSH, and ACK. Extracting relevant data as opposed to storing entire network packets reduces data sizes and results in more efficient data management. The Converter converts the parameters from P3D Flow packets into the MySQL format and inserts them into a MySQL database.

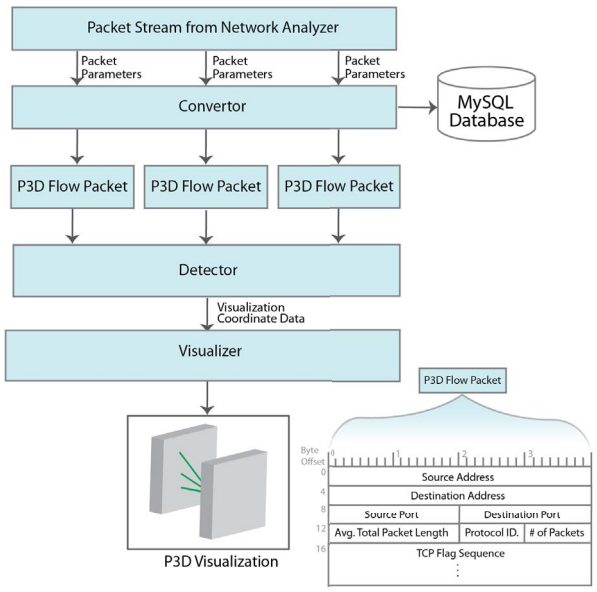


Fig. 2: System Design of P3D.

A P3D flow packet is a compacted data format that contains information about a flow. A *P3D flow* is defined as a network connection between two nodes or a set of packets with the same source IP, destination IP, source port, and destination port. Within a P3D flow packet, a sequential record of TCP flags is recorded between the source and destination to help determine the type of scan or connection. Next, the P3D flow data is sent to the *Detector*. The Detector examines each flow packet and categorizes the connection as various scans such as FIN, ACK, SYN, and Ping scans. These scans are commonly used to bypass firewalls and subvert IDSs. Then, the Detector performs fixed-time detection and categorizes the scan by examining the flow packets between the two hosts. For example, if there are at least 15 destination ports scanned in 15 seconds, then the Detector categorizes the connection as an aggressive port scan. [1]

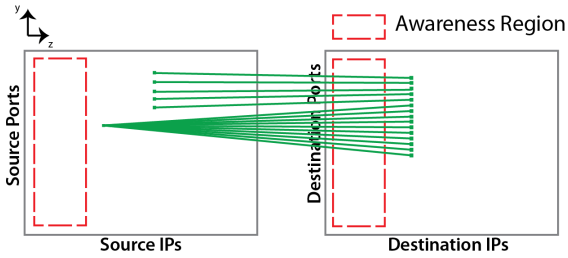
P3D uses the C++ Object Oriented Model-View-Controller paradigm for higher modularity and extensibility in the *Visual-*

[1]This rate is used commonly in IDS configurations such as Snort [22].

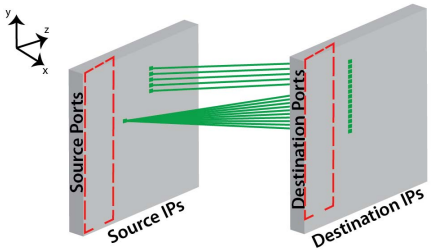
izer. We used a custom OpenGL class within a QT framework for its cross-platform capabilities. Therefore, it can compile and run on Windows, GNU/Linux and Mac OS X operating systems. We use the Framework for Rendering Enhanced 3D Stereoscopic Visualization (FRE3DS) [21]. This framework is useful for producing rapid customized 3D visualizations with stereoscopic support so that network administrators can easily and quickly develop various visualizations to efficiently investigate data. 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.

B. Visualization Design

Currently, no 3D or 2D visualization tool exists that prevents the occlusion-based visualization attacks discussed in this paper. Using 2D planes in P3D instead of 1D axes allows administrators to understand the relationship between source IP and source port. Figure 3 shows a 2D and 3D representation of P3D. Figure 3.a shows two adjacent planes to portray the relationship between source port, source IP, destination port, and destination IP.



(a) 2D representation of a single destination IP using planes.



(b) P3D scan to a single destination IP.

Fig. 3: P3D Visualization Design.

As shown in Figure 3.b, an aerial perspective of P3D is based on the x, y, and z coordinate systems consisting of two planes and colored links based on connections (e.g., green denotes TCP connect() call) between the planes. The aerial perspective allows users to use features such as pan, rotate, and translate to faster identify anomalies on the network than its 2D counterparts. One plane represents a range of source IPs along the z-axis and a range of destination ports along the y-axis, and the other plane represents a range of destination IPs and Ports. The ports range from 0 to 65535 and the IP range depends on the network. The Awareness Region is the stereoscopic portion of the visualization that appears in front of the screen. The colored (green) line denotes the TCP connection in a flow. For example, the color green means the source attempts to perform a TCP 3-way handshake. Figure 3b clearly shows that one source IP address is scanning from 5 source ports to 5 destination ports on a single destination IP as portrayed by consecutive horizontal lines and another source IP is scanning from one port to 5 destination ports as portrayed by a fan pattern. Such a scan goes undetected on most traditional visual IDS systems. In 2D Parallel coordinate systems, the relationship between source IPs, source ports, destination IP, and destination ports is lost. The 3D coordinate system design easily allows for the administrators to uniquely distinguish the scans from different hosts scanning from the same port and detect more advanced techniques such as occlusion attacks.

The 3D Visualizer creates the left and right cameras, off-axis frustum, and other components essential for rendering in an stereoscopic OpenGL environment. The 3D environment renders a stereoscopic visualization into two regions: the Coordinate Region (CR) and the Awareness Region (AR).

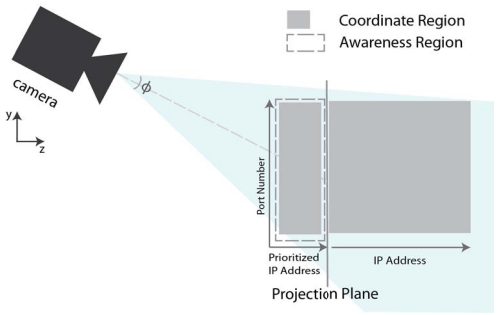


Fig. 4: Sideview of P3D.

1) Coordinate Region: The Coordinate Region (CR) is used to detect stealthy scans, bogus scans, distributed scans and scans meant to bypass the firewall including SYN, ACK, and FIN scans by coloring the connection link. Using stereoscopic 3D, P3D is specially designed to handle more data than the traditional 2D plots.

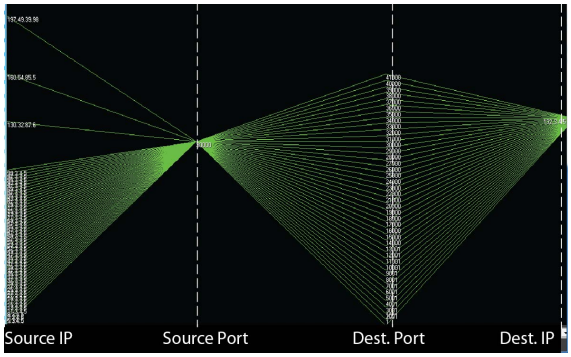
2) Awareness Region: The Awareness Region (AR) is a stereoscopic area that shows a subset of IPs with the highest priority. P3D uses a detection mechanism to determine interesting scans and prioritized IPs by analyzing the TCP/IP attributes in the flow. The detection mechanism visually groups nodes based on various categories: e.g., stealth SYN scanning, ACK scanning, and FIN scanning. Another option is grouping the nodes based into prioritized IPs. Since AR contains IPs and scanning categorization with the highest priority, stereoscopic technologies are used to enhance awareness of vulnerable nodes. These nodes' awareness is enhanced by positioning the nodes within the focal length into the AR. As a result, with stereoscopic technologies, the nodes within the AR are perceived in front of the physical screen. The groups of nodes allow the administrator to determine which nodes are scanning and being scanned within a network and distinguishes which nodes are potentially compromised.

V. Perfomance Evaluation

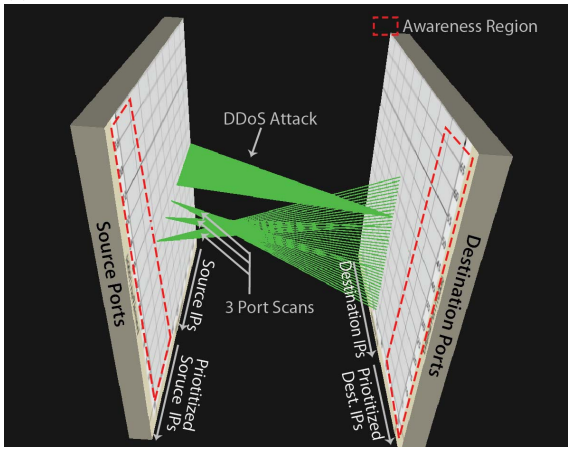
In this section, we evaluate P3D based on use-case scenarios for occlusion-based visualization attacks. Next, we discuss similarities and differences between 2D parallel coordinate visualization tool Rumint [13] and P3D. Rumint's 2D parallel coordinate technique is used for comparison because this technique, like P3D, has no theoretical limit in the number of network parameters that can be visualized. Additionally, 2D parallel coordinate visualization has, until P3D, led to a quicker understanding and a more informational graph over that of a 2D/3D scattered plot matrix [14].

A. Source Port Confusion Attack

One occlusion attack is source port confusion. 2D Parallel coordinate visualizations become confusing when multiple source nodes (with different IPs) share the same port [2]. This attack is important because it prevents users from understanding how each individual node is behaving on the network in comparison to other nodes.



(a) Rumint [13] 2D Source Port Confusion Visualization.



(b) P3D Source Port Confusion Visualization.

Fig. 5: Use Case 1: Source Port Confusion.

Most network scanner tools contain the ability to forge various packets (e.g., RST packets) from spoofed source and destination IP addresses as though they are coming from protected hosts behind the firewall. Although current visualization IDSs detect most script kiddies' scanning activity, more advanced attackers can use source port confusion attacks to perform distributed scans from botnets to subvert IDSs. These attacks fool most visualization systems by sending a mixture of bogus and real TCP connections.

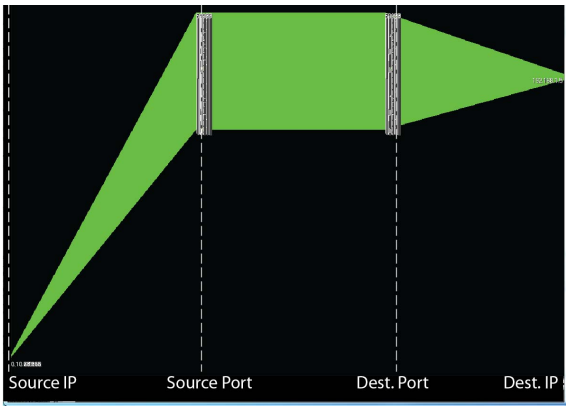
P3D allows users to distinguish the source and destination relationship between 4-tuple connections (source IP, source port, destination IP, destination port). This distinction allows administrators to quickly determine which host is sending malicious or benign data and prioritize the IP to prevent occlusion. For example, Figure 5 shows a simulated coordinated botnet attack of 100 nodes, ranging from 1.1.0.0 to 200.254.254.254, attacking destination IP address 132.3.4.5 on port 30000. In the 2D case [13], as shown in Figure 5.a, the visualization causes confusion and can be misleading because it is difficult to distinguish whether the scan is coming from one source host, multiple source hosts, or all source hosts. P3D (Figure 5.b) clearly shows that 3 IP addresses, 160.54.85.5 and 197.49.39.98, and 130.32.87.6 are performing scans while the other IPs are performing a Distributed Denial of Service (DDoS) attack on port 30000. In result, we can better pinpoint the behavior of individual targeted source IPs in the network than its 2D counterpart.

B. Windshield Wiper Occlusion Attack

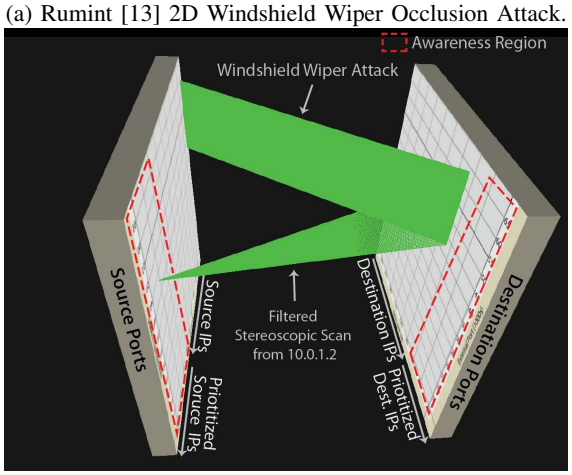
Another example of an occlusion attack is the Windshield Wiper attack [2], which attempts to completely obscure a visualization system's output by manipulating packet header fields in a coordinated way. Figure 6 is presented to better portray the detection of the extremely stealthy nodes within the visualization. This attack is created using a packet crafting tool hping [23] and each packet is generated using the equivalent source and destination ports from 40,000-60,000 on a 10.0.0.0 network. Figure 6.b shows a visualization of 10.0.0.0 LAN network using P3D. Within the P3D visualization in Figure 6.b, the Windshield Wiper attack is detected by a resulting diagonal rectangular pattern in the CR. Unlike in the port source confusion scenario, the Windshield Wiper attack can obscure a range of ports rather than one port. To perform such an attack, attackers send much more data onto the network than a source port confusion scenario on a network. For this reason, the Windshield Wiper attack is considered more data intensive. In result, the Detector applies a filtering algorithm to prioritize scans into the stereoscopic AR. This helps prevent data intensive occlusion attacks such as the Windshield Wiper attack while still maintaining other network activity without removing data. This region uses 3D technologies in the Visualizer to enhance the awareness of the scan by perceiving the scan in front of the computer monitor. Our visualization clearly shows a scan in the stereoscopic AR. On the other hand, in Figure 6.a, we applied a the same filtering algorithm to detect the prioritized IP and use brushing to portray the scan in blue. However, in the 2D case [13], *occlusion occurs and the scan from ip 10.0.3.34 in the 2D visualization is completely hidden.*

VI. Conclusions and Future Work

In this paper, we discussed the use of 2D/3D visualizations to analyze multidimensional data and introduced a format



(a) Rumint [13] 2D Windshield Wiper Occlusion Attack.



(b) P3D Windshield Wiper Occlusion Attack.

Fig. 6: Use Case 2: Windshield Wiper Occlusion Attack.

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 visualization techniques aimed at understanding and analyzing scans or attacks used to mislead and overwhelm the user for large networks. P3D 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. P3D uses the FRE3DS framework [21] to reveal vital scanning characteristics of data and determine correlations between data and attacker nodes on a network. P3D is essential for strategically determining distributed coordinated attacks. Specifically, we showed that using P3D, it is less likely to obscure data through occlusion attacks particularly meant to visually overwhelm the user. In the future, we plan to apply our visualization design to the IPv6 address space, implement other depth cues, user interactions, and evaluate their effects on users.

REFERENCES

[1] J. Gadge and A. Patil, "Port Scan Detection," in *Proceedings of the IEEE International Conference on Networks (ICON)*, Dec. 2008, pp. 1–6.

[2] G. Conti, M. Ahamad, and J. Stasko, "Attacking Information Visualization System Usability Overloading and Deceiving the Human," in *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2005, pp. 89–100.

[3] 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.

[4] 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.

[5] D. Keim, "Information Visualization and Visual Data Mining," *IEEE Transactions on Visualization and Computer Graphics*, pp. 1–8, Mar 2002.

[6] 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)*, 2005, pp. 291–294.

[7] D. Stott, L. Greenwald, O. Kreidl, and B. DeCleene, "Tolerating Adversaries in the Estimation of Network Parameters from Noisy Data: A Nonlinear Filtering Approach," in *Proceedings of the IEEE Conference on Military Communications (MILCOM)*, Oct. 2009, pp. 1–7.

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

[9] C. Ware, *Information Visualization Perception for Design*. Morgan Kaufmann, 2004, vol. 1.

[10] 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.

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

[12] G. Hubona, P. Wheeler, G. 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.

[13] G. Conti and K. Abdullah, "Passive Visual Fingerprinting of Network Attack Tools," in *Proceedings of the ACM Workshop on Visualization and Data Mining for Computer Security(VizSEC/DMSEC)*, 2004, pp. 45–54.

[14] H. Choi, H. Lee, and H. Kim, "Fast Detection and Visualization of Network Attacks on Parallel Coordinates," *Computers and Security*, vol. 28, no. 5, pp. 276 – 288, 2009.

[15] H. Hauser, F. Ledermann, and H. Doleisch, "Angular Brushing of Extended Parallel Coordinates," in *Proceedings of the IEEE Symposium on Information Visualization (InfoVis)*, 2002, pp. 127–.

[16] Z. Jiawan, L. Liang, L. Liangfu, and Z. Ning, "A Novel Visualization Approach for Efficient Network Scans Detection," in *Proceedings of the International Conference on Security Technology (SECTECH)*, Dec. 2008, pp. 23 –26.

[17] I. Xydas, G. Miaoulis, P. 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.

[18] A. Oline and D. Reiners, "Exploring Three-Dimensional Visualization for Intrusion Detection," in *Proceedings of the IEEE Workshop on Visualization for Computer Security (VizSEC)*, Oct. 2005, pp. 113–120.

[19] J. McPherson, K. Ma, P. Krystosk, T. Bartoletti, and M. Christensen, "Portvis: A Tool for Port-based Detection of Security Events," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC)*, 2004, pp. 73–81.

[20] T. Taylor, S. Brooks, J. Mchugh, and S. Brooks, "Netbytes viewer: An entitybased netflow visualization utility for identifying intrusive behavior," in *Proceedings of the 2007 Workshop on Visualization for Computer Security (VizSec)*, 2008, pp. 101–114.

[21] T. Nunnally, A. S. Uluagac, J. Copeland, and R. Beyah, "3DSVAT: 3D Stereoscopic Vulnerability Assessment Tool for Network Security," in *Proceedings of the 37th IEEE Conference on Local Computer Networks (LCN)*, 2012.

[22] Snort. Snort. [Online]. Available: http://www.snort.orgt/

[23] S. Sanfilippo. (2006) Hping2. [Online]. Available: http://www.hping.org