Simplified Network Traffic Visualization for Real-Time Security Analysis

Matthew Dean and Lucas Vespa
Department of Computer Science
University of Illinois Springfield
Springfield, IL 62703

***Abstract*—Although traditional methods of network security analysis used in investigating network traffic and log files are essential to mitigating malicious network activity, these methods alone cannot keep up with constant increases in malevolent network traffic. Many visualization tools have been created as a supplement to traditional analysis and intrusion detection systems. Even though these tools are useful, each tool tends to have a niche use. Also, many network administrators fill dual roles as administrators and security analysts and have little time to learn different complex visualization tools. We therefore observe a need for a simple out-of-the-box solution for general network security visualization. We hope to fill this need with our tool called VNR, which in addition to its simplicity embeds transport layer data within visualizations allowing for better intra-host analysis. VNR can also be used for real-time or auditing purposes by configuring the amount of data visualized within specific time frames.**

I. Introduction

Malicious network traffic is increasing [1], including attacks on business networks, and also attacks originating from compromised hosts within networks. This increase in malicious behavior, along with other factors such as increasing network rates and increasing numbers of virtual and non-virtual hosts, makes a network security analyst's job very difficult. Traditional methods of network monitoring and log dissemination alone cannot keep up with demand for analysis. Alternative methods are required to aid in both real-time and log-based network security analysis.

Visualization tools [2], [3], [4], [5], [6] are a promising solution to the need for simplified analysis techniques, allowing analysts more freedom and a different perspective than traditional analysis. Many of these tools allow for several levels of data abstraction, permitting the user to drill down to packet level data if desired, or view high level visual data. There is a great deal of overlap between many visualization tools; however, each tool usually has some niche functionality.

As useful as network security visualization is to the analyst, there are some general problems that most visualization tools do not address. The following is a list of these problems, and possible solutions.

- $Problem$: Many analysts are not full time analysts, but rather admin/analysts who cannot devote their full attention to learning visual analysis tools, or for that matter, complex analysis techniques in general.
  - $Solution$: Create a basic, out-of-the-box visualization solution with functionality that is obvious to those with basic network knowledge.
- $Problem$: Many visualization tools utilize heavy abstraction, wherein, visualizations display only IP layer data if any data at all. Although this is useful for some analysis, transport and application layer data helps in detecting irregular behavior within single hosts.
  - $Solution$: Mix abstraction levels by embedding transport and/or application layer data across all visualized hosts, while still displaying IP layer host relationships.
- $Problem$: Grouping hosts based on internal/external status may focus an analyst's attention on external attacks. However, a great deal of malicious traffic may actually come from compromised hosts within a network, and internal IP ranges can be spoofed. These can be of greater concern than external attacks.
  - $Solution$: Treat all hosts equally in any graph-based visualization. Do not force groupings based on internal/external addresses.
- $Problem$: Many visualization tools are either too complex to visualize in real-time, or the amount of data visualized cannot be adjusted, such that real-time capture will yield useful analysis.
  - $Solution$: Simplify visualizations such that traffic can generally be process in real-time. Allow the user to adjust how many hosts will be displayed such that an accurate snapshot of current network traffic is visualized.

In this work we implement each of the above solutions in a network security visualization tool called VNR (Visualization of Networks in Real-time), a screenshot of which is shown in Figure 1. The visualizations and functionality of VNR need little explanation to those with fundamental network knowledge. VNR has basic grid and graph views which display IP layer relationships and transport layer information. Internal and external hosts are not forced to any locations or groupings. The visualizations are simple and old hosts fade from view by default, creating potential for real-time analysis. VNR also implements many traditional features such as details on demand and summary statistics.

The remainder of this paper is organized as follows. Section II presents related work in the area of network and security

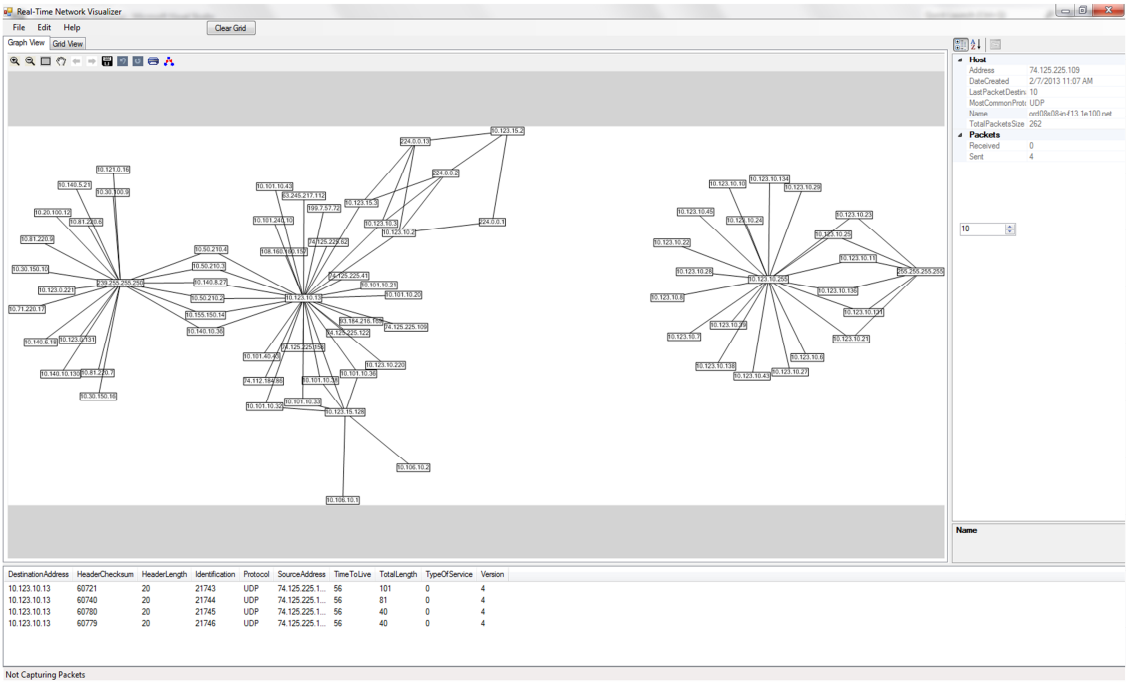


Fig. 1. VNR Screenshot

visualization. Section III summarizes VNR's design and basic functionality. Example uses of VNR for security and network analysis, and a further discussion of VNR are presented in Section IV. Conclusions are presented in Section V.

II. Related Work

A great deal of work has been done in the areas of visualization for networks [7], [8], [9] and security [10], [11], [12], [13]. Many tools for visualization have been produced, amongst which there is a great deal of overlap, with each tool having niche functionality. Most tools concentrate on visualizing trace files for better analysis, although some are designed for real-time analysis as well.

Specifically, in network visualization, TNV [4] displays a time-based matrix of host communications. TNV's matrix is detailed and gives the analyst many complex analysis tools. Several levels of granularity are displayed. Visual analysis of routing [5], [14] is another area of concern. BGPeep [5] is a visualization tool for BGP analysis. It presents a visual organization by IP space, using network address prefixes to categorize data. VisTracer [15] is a network tool to evaluate routing changes over time, and identify legitimate versus malicious route adjustments. Minarick and Dymacek [16] create a tool to use graphs to visualize netflow data. The graphs also include DNS name lookup and common port/service names for ease of understanding.

Even more specifically, network security visualization has been proposed to aid in the timely mitigation of network threats. Fligg et al [17] present an overview of network security visualization, specifically, the psychology of visualization and specific rules for efficiently utilizing particular space. Many visualization tools allow multiple levels of visual data abstraction, from high-level overviews to low-level details. TVi [18] reflects this functionality, implemented as a visual querying tool for network traces. Teoh et al [19] demonstrate how to perform visual analysis of log files as an alternative to traditional automated log analysis processes.

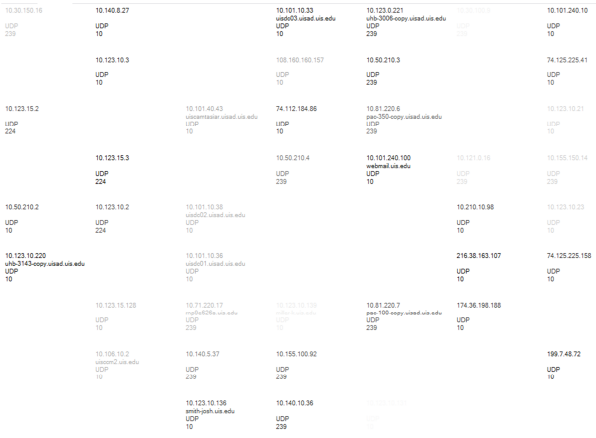
Because many visualization tools can help detect scans but not identify scan types, Muelder et al [20] create a methodology for further identifying scan characteristics, utilizing PortViz [3] and other tools. NFlowVis [21] uses a treemap visualization linked to attack alerts to analyze the validity of system alerts, as well as other analysis such as network service usage. Similar to NFlowVis, Garnet [6] uses a treemap to layout subnets, and then creates an attack graph which relates to the treemap. Musa et al [22] visualize Snort alerts in a 3D time-series graph. Netgrok [2] can visualize trace files by representing hosts in graph or treemap form.

III. VNR Overview

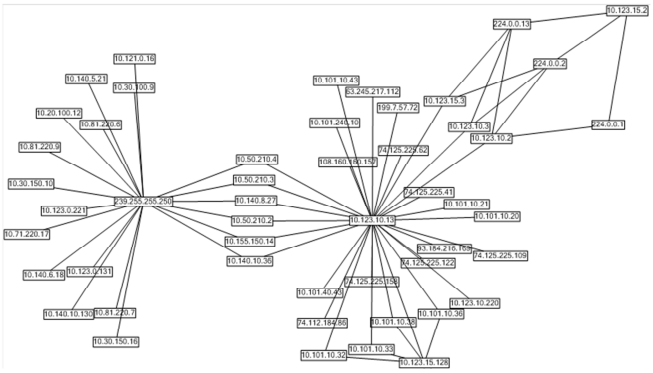
A. Overview

To facilitate easy evaluation of VNR's visualizations, two simple views are utilized, a grid view and graph view. Hosts communicating on the network are represented by a single element within each view. In grid view, these elements are cells, and each host is represented by a single cell. In graph view, the elements are vertices and each host is represented by a single vertex. Figure 2(a) shows the grid view and Figure 2(b) shows the graph view. Each view's output is simple to interpret allowing out-of-the-box analysis. Each element in either view displays multi-layer information about a host, allowing for intra-host analysis. Communicating hosts are connected by edges in the graph view.

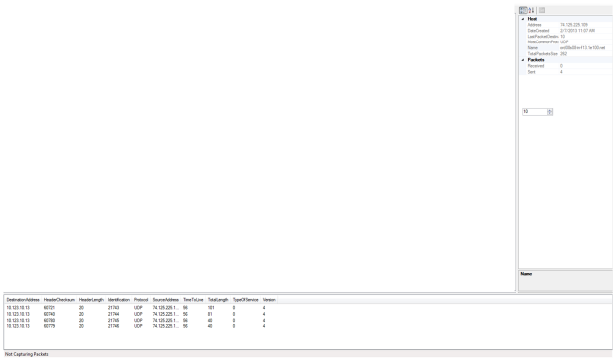
Hosts are selectable and details for a selected host are displayed in the details pane, an example of which is shown



(a) Grid View



(b) Graph View



(c) Details Pane

Fig. 2. VNR Views

in Figure 2(c). Each view displays x currently communicating hosts, where x is configurable and has a default value of 100 hosts. The value of x can be adjusted depending on the level of real-time analysis desired. It should be noted that VNR is not strictly a real-time tool. By increasing x to a very large value, VNR can be used for auditing and trace file analysis with many hosts.

Packet capture in VNR is achieved using PCAP.Net [23], a Dot Net wrapper for the popular WinPCAP libraries [24]. Microsoft C# [25] is therefore used for the application development. Graph visualization is performed using Microsoft Automated Graph Layout (MSAGL) [26], developed by Microsoft research.

B. Views and Features

a) Grid View: The grid view is a collection of cell elements, one for each of the x most recently communicating hosts. The host information includes network IP, packet counts, current embedded protocol and other configurable information. The simple layout and efficient use of space in the grid view allows maximum intra-host information to be displayed. This view is therefore especially useful for analyzing the behavior of individual hosts. Clicking a host in the grid view will update the details pane with information for the selected host. Older hosts slowly fade from the grid if no new traffic is received from them.

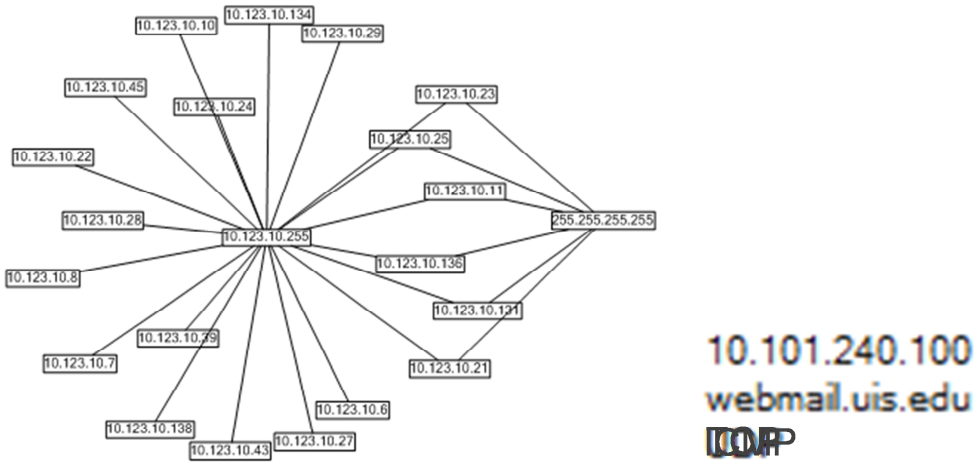
b) Graph View: The graph view displays each host element (vertex), and also connects communicating hosts. The hosts present in the graph view are synced with the grid view. Clicking a host in the graph view displays details for the selected host.

c) Details Pane: Packet level and summary information are displayed for each host in the details pane. Some of the information displayed includes individual packets sent and received by the selected host and summary information such as the majority embedded protocol, the time the host first appeared, host name and size of communicated data.

IV. Discussions

Figure 3(a) shows what a simple NMAP network scan looks like in VNR. A quick appearance of a one-to-many host relationship demonstrates a scan of a subnet. Although, this is only one very obvious use of VNR, more subtle variations of this can help identify scans that might go undetected otherwise. Once a potential scan is visually detected, more information about individual hosts can be gathered from the grid view and details pane.

Figure 3(b) shows what a scan of an individual host looks like in the grid view. Typically, in the grid view, the protocol, port and other fields tend to seemingly remain static due to communications of one type. However, during a scan, some fields will look as if they are flashing. This demonstrates a



(a) NMAP scan of a network.

(b) NMAP scan of a host

Fig. 3. VNR Visualizations

rapid change in values which indicates a potential scan. The image in Figure 3(b) is created artificially from a base screen shot of the grid view. to demonstrate what this activity looks like. We had to create the image because it is impossible to take a screen shot while the screen is refreshing. A great deal of malicious activity shows up as rapidly changing fields in the grid view, and can be a starting point for detecting malicious activity. Other methods of detecting malicious behavior are also present in the grid view.

The visualizations in VNR can be used to identify many other types of scans and general malicious activity. Any information that rapidly changes within the header fields of two communicating hosts will be detected by an analyst using VNR. In addition, all many-to-few communication relationships will be exposed to the analyst. In addition, traditional packet level and summary analysis can still be utilized due to the details on demand ability of VNR. VNR can also be used for auditing of large recorded network trace files for non real-time analysis. This allows for a more detailed investigation of network behavior.

In the future, besides the ability to drill down to details, we will also include the ability to jump back to host level from the details level. For example, if an analyst clicks a host to view packet level details and subsequently notices a suspicious address in the recorded packets for that host, the analyst will simply be able to click on that suspicious address and the host associated with the address will become the selected host in the current grid or graph view. This will allow an analyst to easily follow audit trails in real-time or while analyzing trace files.

V. Conclusions

In this work we have presented VNR, a network security visualization tool with easy to understand visualizations. VNR displays information from multiple network layers simultaneously and can be used for real-time or log analysis. We have demonstrated the functionality of VNR and shown its usefulness for detecting malicious network activity. We believe that tools like the one presented in this work are an essential step in mitigating future network threats, and that VNR is a positive augmentation toward generalized use of network security visualization tools.

References

[1] M. Kowtko, "Securing our nation and protecting privacy," in *Systems, Applications and Technology Conference (LISAT), 2011 IEEE Long Island*, May 2011, pp. 1 –6.

[2] R. Blue, C. Dunne, A. Fuchs, K. King, and A. Schulman, "Visualizing real-time network resource usage," in *Proceedings of the 5th international workshop on Visualization for Computer Security*, ser. VizSec '08, 2008, pp. 119–135.

[3] J. McPherson, K.-L. 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*, 2004, pp. 73–81.

[4] J. Goodall, W. Lutters, P. Rheingans, and A. Komlodi, "Preserving the big picture: visual network traffic analysis with tnv," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, October 2005, pp. 47–54.

[5] J. Shearer, K.-L. Ma, and T. Kohlenberg, "Bgpeep: An ip-space centered view for internet routing data," in *Visualization for Computer Security*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2008, pp. 95–110.

[6] L. Williams, R. Lippmann, and K. Ingols, "Garnet: A graphical attack graph and reachability network evaluation tool," in *Proceedings of the 5th international workshop on Visualization for Computer Security*, ser. VizSec '08, 2008, pp. 44–59.

[7] C. Kintzel, J. Fuchs, and F. Mansmann, "Monitoring large ip spaces with clockview," in *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, ser. VizSec '11, 2011, pp. 2:1–2:10.

[8] C. Horn and A. D'Amico, "Visual analysis of goal-directed network defense decisions," in *VizSec '11: Proceedings of the 8th International Symposium on Visualization for Cyber Security*, 2011, pp. 1–6.

[9] S. S. Kim and A. L. N. Reddy, "Netviewer: a network traffic visualization and analysis tool," in *Proceedings of the 19th conference on Large Installation System Administration Conference - Volume 19*, ser. LISA '05, 2005, pp. 18–18.

[10] L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, "Malware images: visualization and automatic classification," in *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, ser. VizSec '11, 2011, pp. 4:1–4:7.

[11] A. Singh, L. Bradel, A. Endert, R. Kincaid, C. Andrews, and C. North, "Supporting the cyber analytic process using visual history on large displays," in *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, ser. VizSec '11, 2011, pp. 3:1–3:8.

[12] R. Veras, J. Thorpe, and C. Collins, "Visualizing semantics in passwords: the role of dates," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec '12, 2012, pp. 88–95.

[13] L. Harrison, R. Spahn, M. Iannacone, E. Downing, and J. R. Goodall, "Nv: Nessus vulnerability visualization for the web," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec '12, 2012, pp. 25–32.

[14] S. T. Teoh, K.-L. Ma, and S. F. Wu, "A visual exploration process for the analysis of internet routing data," in *Proceedings of the 14th IEEE Visualization 2003 (VIS'03)*, ser. VIS '03, 2003, pp. 69–.

[15] F. Fischer, J. Fuchs, P.-A. Vervier, F. Mansmann, and O. Thonnard, "Vistracer: a visual analytics tool to investigate routing anomalies in traceroutes," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec '12, 2012, pp. 80–87.

[16] P. Minarik and T. Dymacek, "Netflow data visualization based on graphs," in *Proceedings of the 5th international workshop on Visualization for Computer Security*, ser. VizSec '08, 2008, pp. 144–151.

[17] K. Fligg and G. Max, "Network security visualization," *IEEE Network Special Issue on Recent Developments in Network Intrusion Detection*, Apr. 2012.

[18] A. Boschetti, L. Salgarelli, C. Muelder, and K.-L. Ma, "Tvi: a visual querying system for network monitoring and anomaly detection," in *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, ser. VizSec '11, 2011, pp. 1:1–1:10.

[19] S. T. Teoh, T. Jankun-Kelly, K.-L. Ma, and F. S. Wu, "Visual data analysis for detecting flaws and intruders in computer network systems," *IEEE Computer Graphics and Applications, special issue on Visual Analytics*, 2004.

[20] C. Muelder, K.-L. Ma, and T. Bartoletti, "A visualization methodology for characterization of network scans," in *Proceedings of the IEEE Workshops on Visualization for Computer Security*, ser. VIZSEC '05, 2005, pp. 4–.

[21] F. Fischer, F. Mansmann, D. A. Keim, S. Pietzko, and M. Waldvogel, "Large-scale network monitoring for visual analysis of attacks," in *Proceedings of the 5th international workshop on Visualization for Computer Security*, ser. VizSec '08, 2008, pp. 111–118.

[22] S. Musa and D. J. Parish, "Using time series 3d alertgraph and false alert classification to analyse snort alerts," in *Proceedings of the 5th international workshop on Visualization for Computer Security*, ser. VizSec '08, 2008, pp. 169–180.

[23] "Pcap.net," 2013, http://pcapdotnet.codeplex.com/.

[24] "Winpcap," 2013, http://www.winpcap.org/.

[25] "Microsoft visual studio express for windows desktop," 2013, http://www.microsoft.com/visualstudio/eng/products/visual-studio-express-for-windows-desktop.

[26] "Microsoft automatic graph layout," 2013, http://research.microsoft.com/en-us/projects/msagl/.