Interactive and Dynamic Visual Port Monitoring and Analysis

Robert F. Erbacher[1] and Menashe Garber[2]

[1]Utah State University, Dept. of Computer Science, UMC 4205, Logan, UT 84322
[2]University at Albany-SUNY, Dept. of Computer Science, LI67A, Albany, NY 12222

Abstract

Techniques in conjunction with an implemented environment are described for the visual monitoring and analysis of port activity. The goal is to provide the ability to detect anomalous or mischievous activity on an individual system basis. Such capabilities would allow individual users of systems to garner greater insight into the network activity of their system than is currently provided by typical tools, such as personal firewalls.

Keywords: Intrusion Detection, Visual Analysis, :Interactive Visualization

1. Introduction

In today's networked society new tools and techniques are needed to aid in monitoring computer systems to aid identification of unauthorized activity. Of particular interest for this research is the monitoring and analysis of individual computer systems. This is in contrast with the majority of prior work which has focused on networks of computer systems or servers. This work was motivated by the consideration of the lack of information provided by most personal firewalls and the need to provide additional feedback to individual users, e.g., home users.

The focus of the developed techniques and capabilities is to provide visual monitoring of individual computer systems. More specifically, we have developed capabilities for the real-time visual monitoring and analysis of port connections. The goal is to provide more information than is currently available, from event logs, as to the actual activity occurring and its implications.

2. Relation to Prior Art

In terms of visualization, many intrusion detection environments incorporate "odometer-like" scales or apply other techniques to represent system state [9]. This is embodied in the Hummer "perceived level of threat" [6] indicator. Earlier systems, such as DIDS [7], provided graphical representations in the form of color to indicate when a system had experienced a sequence of suspicious events. While useful, these approaches do not provide adequate information to aid diagnosis.

2.1. Intrusion Detection Systems

While many intrusion detection tools have begun to incorporate basic graphical user interfaces (BlackICE [10], RealSecure [11], Cisco Secure IDS [12], eSecure [13]) they fall short of providing effective visualization displays to aid in interpreting the generated information. For example, most of the tools will provide an indication when it received an unexpected packet. But was this an attack, a misdirected packet, a casual attack, or a real attempt to break into the system? These systems do not adequately provide the detail and event interrelationships needed to analyze the activity in the detail needed forensically.

2.2. Visualization systems

In contrast to intrusion detection, quite a bit of visualization research has been applied to network accesses. The principal body of work related to network intrusion is from the information exploration shoot-out, organized by Georges G. Grinstein and supported by the National Institute of Standards and Technology (NIST) [5]. In this project, researchers were given access to a data set consisting of network intrusions. The goal was to identify which researcher's techniques were effective at identifying the intrusions.

The previous work involving visualization related to networks emphasized network performance and bandwidth usage [2], even down to the router [2], individual packets [4], and individual e-mail messages [3]. The techniques developed for these purposes do not provide sufficient detail or handle sufficient numbers of nodes and attributes in combination for our needs. The work by Teoh et al [8] focuses on Internet routing data and thus is limited in its applicability in intrusion detection and will have no

```
$ ./viabi.exe a7.dump -D1 -M5

Finished Mode part!!

Parser done!
Done Parsing
1. \Device\NPF_{DFAF8CC5-48DB-499B-984C-A9D525FAB774}Dell Wireless WLAN 1450 Dual Band WLAN Mini-
PCI Card (Microsoft's Packet Scheduler)
2. \Device\NPF_{CF0698BE-2105-466B-8AAE-4F3276FE2264}Broadcom NetXtreme Gigabit Ethernet Driver
(Microsoft's Packet Scheduler)
3. \Device\NPF_{AF810396-6BA0-4594-A441-10CEBB346F3F}NET IP/1394 Miniport Reading Packets on
Device: Dell Wireless WLAN 1450 Dual Band WLAN Mini-PCI Card
(Microsoft's Packet Scheduler)
```

Figure 1: Network packet driver selection. –D1 specifies the first packet driver. This allows switching between multiple devices and interfaces.

applicability to forensics. The work by Eick et al. [3] strictly deals with e-mail and subsequently resolves many fewer nodes and attributes than is needed for intrusion detection. In terms of port monitoring, McPherson et al. developed a tool for the visualization of port activity which is geared more towards analysis of large scale systems and isn't geared towards the effective analysis of attacks on individual systems [1].

3. Configuration and Initialization

The discussed environment was developed under MS Windows using Cygwin, C++, OpenGL, WinPcap, and TclTk. The environment was developed in a system independent fashion and thus should be easily ported to other platforms. Upen execution of the environment the user must either select an interface at the command line or in response to a presented list of choices, figure 1.

4. Port Visualization

The port visualization technique, in its default mode, is shown in Figure 2. The display consists of four primary components: The interface at the bottom of the display, the legend at the top of the display, the four horizontal lines of target ports, and the bottom line (above the GUI), which represents time. Inbound connections are represented by drawing a ling from the appropriate temporal point on the bottom line to the relative position on the port lines for the target port on the given system. The port numbers are divided into four lines to more effectively segregate the large number of ports. An exponential distribution is used to be more representative of the volume of activity, sensitivity, and criticality of the individual port numbers, This results in the following distributions: 0-1999, 2000-9999, 10000-24999, and 25000-50000. Different colors are used for each of the major port connection types: blue for UDP and green for TCP.

When a new connection arrives, it is placed to the far right of the bottom line (the time line). This lines continuously shifts to the left to be representative of the passage of time. Thus, the oldest time points and their associated connection will eventually leave the display to the left. When the time point leaves the display area, the connections associated with that time point are removed entirely from the display. Thus, the monitoring environment provides a historical representation of connections activity, showing all activity that has occurred during a specified duration of time.

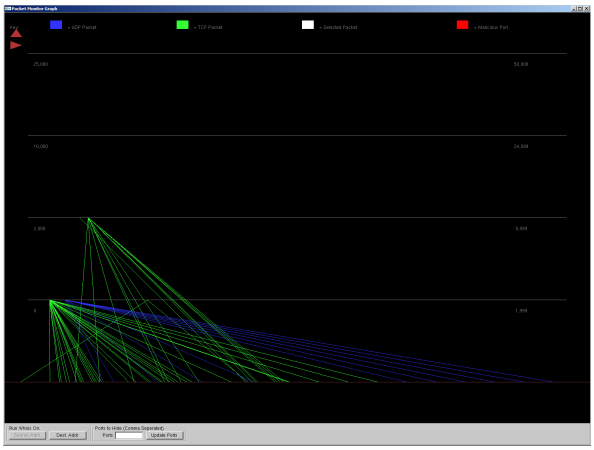

Figure 2: Initial port monitoring example. Lower port numbers are at the bottom of the display Line color is indicative of the type of connection with green representing TCP, blue represents UDP, white is a selected connection, and red is a connection to a known malicious port.

The two triangles in the top left corner of the display allows for the ordering of the port numbers to

be swapped and inverted. This modifies the display such that the lower port numbers are represented at the top of the display rather than at the bottom, figure 3. By inverting the display we in essence change the visual acuity of the active ports. For example, in figure 3 it can be easier to visually segregate connection information by moving the most frequently accessed ports to the top of the display, However, doing so increases the screen real-estate allocated to these connections, creating more collisions (intersections) than are exhibited in figure 2 and potentially occluding critical information from underlying port connections.

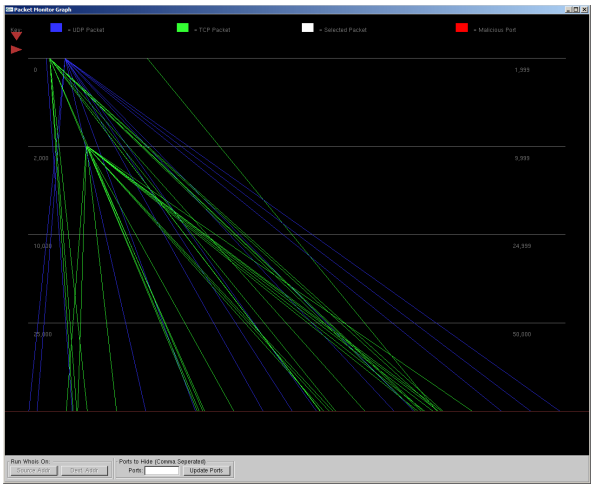

Figure 3: Alternative example with lower port numbers at the top of the display. Inverting the display in this fashion in essence inverts the visual attention focused on the individual connections, i.e., more emphasis is placed on the lower port numbers in this scenario.

5. Port Activity Analysis

Merely representing port connection information is insufficient for providing needed value. For this reason additional exploration and analysis capabilities are incorporated. This includes the ability to select hosts, retrieve feedback on a connection, and filter ports.

The ability to filter ports may be the most valuable capability as it allows the user to remove connections associated with a select set of ports. This allows connections to protected or unthreatening ports to be filtered. Additionally, ports with many connections that are leading to occlusion can also be filtered. This allows the user to control the visualization such that it will provide the most useful information both for that user and for the activity and analysis task at hand.

When a connection is selected, the connection will be highlighted in white. This highlight will remain until the connection is removed from the display or the user selects a different connection. This allows a connection to be followed over time and the analysis of the connection to be continued.

A second analysis capability is the ability to garner feedback as to the specifics of a connection. When the mouse is left hovering over a connection a popup will be presented showing specific detailed information as to said connection. This will include all of the most relevant information related to the connection, including: Source IP, Destination IP, Source Port, Destination Port, Connection Type, Connection Time Stamp, and Packet Length.

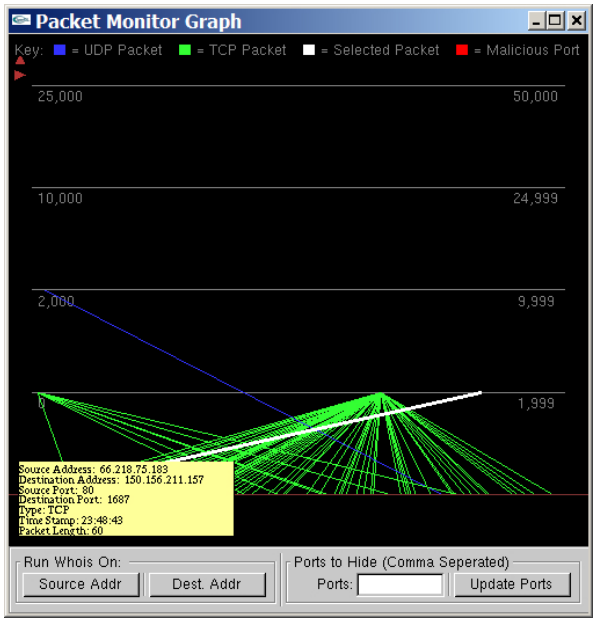

Figure 4: This example shows a selected TCP connection and the available feedback for such connections. Information provided includes: Source IP, Destination IP, Source Port, Destination Port, Connection Type, Connection Time Stamp, and Packet Length.

Additional information can be acquired by doing a whois lookup on a connection, either of the source IP or the destination IP, figure 5. This informational display can be critical when evaluating the meaning or intentions of the identified activity. In other words, we must examine the available information to determine if the activity is acceptable or malicious and the extent of needed response.

The combination of the provided capabilities provides a complete monitoring and analysis environment that allows the user to determine the meaning, threat, and criticality of identified activity. Employing this environment for the actual identification of malicious activities requires the identification of unusual activity, followed by the

analysis of said activity. Unusual activity that should garner interest can include access to known malicious ports, clusters of activity that deviate from normal activity, persistent or repeated connections to unexpected ports, etc. The concept of identifying activity that deviates from the norm is a typical concept that follows through much of the intrusion detection field but is also found to be very effective, powerful, and consistent.

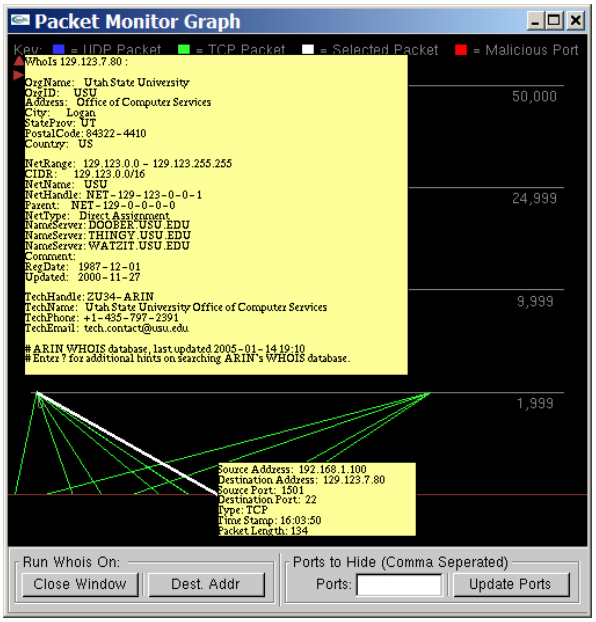

Figure 5: This final example shows both informational feedback of a selected node as well as the whois lookup of the destination IP. All information provided by whois is included in the large informational popup display.

6. Conclusions and Future Work

We have described a visualization technique and associated environment that allows for the monitoring of individual systems for potential security threats. The design of the environment allows for easy use by a wide variety of users. The incorporation of extensive interaction capabilities allows for the analysis of unusual activity identified within the visualization paradigm.

While the environment has proven capability it must be extended and enhanced to improve its representational capability. For example, in keeping with good visualization design we must attempt to reduce the amount of occlusion and intersecting lines. Additionally, we must examine the feasibility of incorporating the representation of additional monitored systems, rather than just a single system as is configured here.

7. References

[1] Jonathan McPherson, Kwan-Liu Ma, Paul Krystosek, Tony Bartoletti, Marvin Christensen, "PortVis: A Tool for Port-Based Detection of Security Events," Proceedings of CCS Workshop on Visualization and Data Mining for Computer Security, October 29, 2004.

[2] Kenneth Cox, Stephen Eick, and Taosong He, "3D geographic network displays," ACM Sigmod Record, Vol. 25, No. 4, pp. 50, December 1996.

[3] Stephen G. Eick and Graham J. Wills, "Navigating Large Networks with Heirarchies," In Visualization '93 Conference Proceedings, San Jose, California, pp. 204-210, October 1993.

[4] Deborah Estrin, Mark Handley, John Heidermann, Steven McCanne, Ya Xu, and Haobo Yu, "Network Visualization with Nam, the VINT Network Animator," IEEE Computer, Vol. 33, No. 11, pp. 63-68, November 2000.

[5] Georges Grinstein, "Workshop on Information Exploration Shootout Project and Benchmark Data Sets: Evaluating How Visualization does in Analyzing Real-World Data Analysis Problems," Proceedings of the IEEE Visualization '97 Conference, IEEE Computer Society Press, Phoenix, AZ, pp. 511-513, 1997.

[6] Polla, D., J. McConnell, T. Johnson, J. Marconi, D. Tobin, and D. Frincke, "A FrameWork for Cooperative Intrusion Detection," 21st National Information Systems Security Conference, pp. 361-373, October 1998.

[7] Snapp, S. et al., "DIDS (Distributed Intrusion Detection System) Motivation, Architecture and An Early Prototype," National Information Systems Security Conference, 1991.

[8] S.T. Teoh, K.L. Ma, and S. F. Wu, "Visual exploration process for the analysis of internet routing data," In Proceedings of the IEEE Conference on Visualization 2003, 2003, pp. 523-530.

[9] Vert, G., J. McConnell, and D. Frincke. "Towards a Mathematical Model for Intrusion," 21st National Information Systems Security Conference, pp. 329-337, October 1998.

[10] http://www.networkice.com/

[11] http://www.iss.net/securing_e-business/security_products/intrusion_detection/index.ph

[12] http://www.cisco.com/univercd/cc/td/doc/pcat/nerg.htm

[13] http://www.esecurityinc.com/