NetSecRadar: A Real-Time Visualization System for Network Security
VAST 2012 Mini Challenge. Award: Honorable Mention for Interesting Use of Radial Visualization Technique
Ying Zhao, Fangfang Zhou*, Ronghua Shi
Central South University, Changsha, China

ABSTRACT
NetSecRadar is a visual analytics system to aid in monitoring the network security in real time and perceiving the overall view of the security situation using radial graph. At present, we use this tool mainly for IDS alerts to analyze the irregular behavioral patterns, and synthesize interactions, filtering and drill-down to detect the potential intrusions. In conclusion, we describe how this system was used to analyze the mini-challenges of the 2012 VAST challenge.

Keywords: Intrusion detection, security visualization, visual interfaces, real-time monitoring.

Index Terms: C.2.0 [Computer-Communication Networks]: General Security; H.5.2 [Information Interfaces and Presentation]: User Interfaces.

1 INTRODUCTION
Our network security analytics system is a combination of a large amount of network security information into a single view. At present, we use the system to monitor IDS alerts in real time and perceive the overall view of the security situation using radial visualization that is aesthetically pleasing and has a compact layout for user interaction [1]. The design of visualization system inspired by VisAlert [2] not only allows users to see multiple representations of the network state, but also provides simultaneous representations of statistical information to make attacking patterns more clearly.

2 VISUAL AND INTERACTION DESIGN
The radial graph, shown in figure 1, illustrates our system of initial design. It is composed of hosts, attack types, timeline and histogram, attack correlation and interaction. The following are details of the visual and interaction design.

2.1 Hosts and Alert types
In the center of the radial graph, shown in figure 2(left), the nodes arranged in circles are hosts of Bank of Money Regional Headquarters Network. The bigger nodes with red color are the servers with high priority, such as firewall, DNS, and Financial servers etc., in intranet. The yellow nodes are internet web sites. The green nodes that ordered by IP address are individual workstations located in offices of the company. The hosts with closer IP addresses, and possibly on the same subnet are arranged in same circle or closer circles.

The color band around the hosts showed in figure 2(left), formally known as the alert type band, is used to display IDS alert types. Each color is assigned to represent each alert type. The angle of each color arc is corresponding to the percentage of number of alerts. The band will be updated in real time while a new alert type observed. At the same time, the escape mechanism will be set for alert type. The alert types, which appear less, move in low frequency and never appear recently, will exit the drawing interface.

Figure 1: Initial design for our visualization system.

Figure 2: Arrangement of Hosts for a network and the color band for alert types(left); Histogram of attacks grouped by alert type every five minutes and outer histogram of sum of attacks(right)

2.2 Timeline and Histogram
In our visualization system, time is represented by animation, as shown in Figure 2(right). Animation can facilitate the perception of change over time. For example, the histogram below the alert type color arc is drawn clockwise along the alert type arc real-time.
2.3 Attack Correlation and Interaction

An actual alert in IDS can be drawn as a triangle, which connected source IP node, destination IP node and the top of the bar of histogram below the alert type in current time span, to represent an alert as shown in figure 3(right). The color of the triangle is the same as that of the alert type. To clearly recognize source IP and destination IP, we use a dash line to connect destination IP node to bar of histogram of alert type. The nodes in an alert will be highlighted to differ from the other nodes in the network. To avoid the visual clutter, the dash lines that link the alert types to destination IPs do not be drawn in the overview graph in figure 3(left).

Our visualization system also supports filtering by direct interaction with the user by simply clicking on any of the hosts, servers, alert types, bars of histograms. If an administrator, for example, would want to see the attacks launched by a workstation in figure 3(left), it would just need to click the node of workstation, and then the attacks related to it will be shown as figure 3(right). We can know that around 21:47 on April 5 when seven colored dots were drawn on the bar of outer histogram, some database visiting alerts were observed. Further, we find the attacker is 172.23.240.156, and the destination is firewall server. At the same time, the attacker also launched VNC Scan and SNMP request TCP to firewall server.

An advantage of our visualization system is its use of animation. In our case, animation is used not only to display transitions of one view to another, but to assist in highlighting system transitions from one state to another. Figure 4 shows the attacks from 17:20 on April 6 to 9:00 on April 7. We can see that there is periodicity for the sum of alerts and types of alert from the outer histogram.

3 Conclusion

We have presented a network security visualization system that can assist in comprehending IDS alerts and detecting abnormal pattern activities within a network. We have evaluated the system with real-world attacks and have shown how our system can be used to illustrate the attacks and visually correlate the events. In the future, we will extend the system to monitoring firewall log and other network security logs. Additionally, the scalability of the topology map will be enhanced especially when it is too big to fit into the inner circle. We also would like to extend the single view of radial graph to multiple views to show more details of the hosts. And further pattern analysis on individual host computer and individual risk will be performed.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant Nos 61103108.

References
