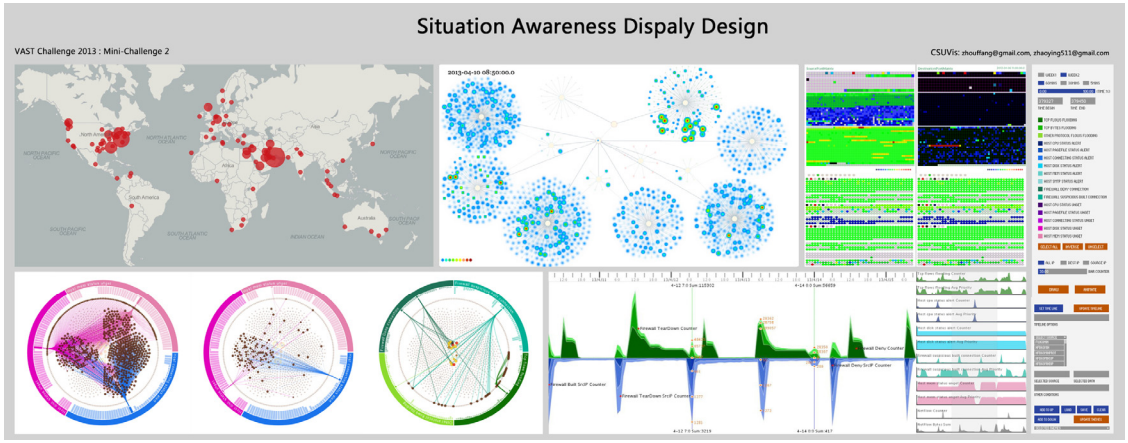
A Multi-View Visualization System for Network Security Situation Awareness

CSU-Zhao-MC2

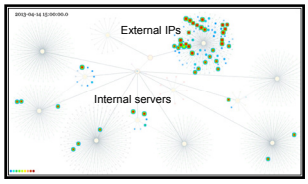
(Central South University, Changsha, Hunan, China)



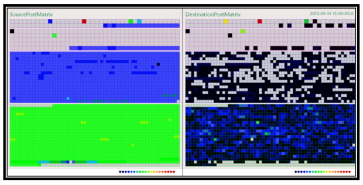
Storyboard

Stage1（Real-time monitoring）

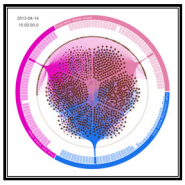
1: We find a hilighted circle in the map of our monitoring view which may belong to the network of BigMarketing Company.



2: Looking into the company network monitoring view, we will find this a traffic explosion as some external IPs raised a huge number of connections to port 80 of web servers.



3: Here is the port and ip matrix view. In this case, there over 60,000 source and destination ports and the level of flows data of these source ports are pretty regular.

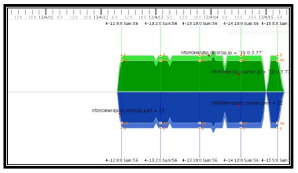


4: In the events monitoring view, near all internal workstations raised the host status alert.

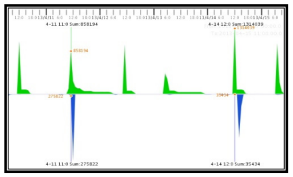
Conclusion 1: In this week, port 80 of internal web servers have received DDoS attack by over 20 external IPs through more than 60,000 source ports, which leads the abnormal of the internal network.

Stage2（History data analysis）

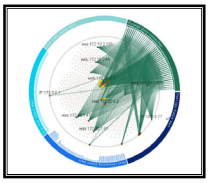
1: During this DDoS attack, there are eight hosts frequently accessing the port 22 of external IP, 10.0.3.77, and still keeping active after the DDoS attack.



2: By analyzing the history activity records of 10.0.3.77 in this week, we could find that eight internal hosts have accessed port 22 of 10.0.3.77 since 8:28 on April 12th.



3: Through the whole-week analysis on denied connection records of Firewall and on the time series record of Netflow, we could find that the denied connection have many climaxes while the records of Netflow reached peak twice, one of which is the DDoS attack near 14:00 on April 14th. Another attack happened at 11:00 April 11th.



4: In the history denied connection record of Firewall log, the preceding eight internal hosts and 10.0.3.77 appeared for many times.

Conclusion 2: In this week, the network of the company has received a large number of attacks, and the noteworthy part is that the firewall failed to resist twice, during which eight internal hosts accessed to external abnormal hosts frequently.