Network Security and Anomaly Visualization

VAST 2011 Mini Challenge #2

Qi Liao* Central Michigan University, USA
Lei Shi† IBM Research - China
Weihong Qian‡ IBM Research - China
Su Zhong§ IBM Research - China

ABSTRACT

Network security management requires both real-time situation awareness of the network in operation and detailed forensics of network events to understand the underlying causes of network security anomalies. In this VAST challenge, we present a visual analytic tool Network Security and Anomaly Visualization (NSAV) that can effectively provide overview+detail visualizations for the detection and analysis of network intrusions and attacks.

1 INTRODUCTION

In this challenge, the topology of network connectivity graphs are constructed directly from the firewall log, which is similar to the NetFlow data, where each line indicates one source IP address/port number pair having a established connection with a destination IP/port pair. Timestamps are recorded so that when investigators adjust the time slider in the visualization tool, the graphs can be dynamically filtered and interactively generated for more effective exploration. The novel part of this work is that these network graphs are then combined with other types of security anomalies such as firewall anomalies (activities beyond acceptable usage policy), intrusion detection system (IDS) snort, OS security event log and Nessus vulnerability scan data via events chaining based on the logical order of system timestamps. As a complement of flow data, security events as anomalies are rendered on top of the flow graphs. In the visualization, different icons (orange representing source and grey representing destination of anomalies) are used. For example, an orange *P* represents a machine generating port scan traffic while a grey *P* represents a machine being scanned. Generally speaking, the more anomaly icons a node gets, the more abnormal it is. The distribution of anomaly clusters can be quickly perceived through our tool as shown in the screenshots below. Finally, scatter views of anomaly events straightforwardly present the correlations among the security anomalies on different nodes for human analysis.

Our visualization tool was implemented in Java. The scatter view of anomaly events is extended from JFreeChart. The graph visualization of NSAV is extended from the Prefuse toolkit, which was selected due to its better customizability and extendibility for interactive visual analysis. Figure 1 shows an overview of the NSAV visualization tool. In the main view in the top-left, the tool shows the graph view of the host traffic connections extracted from firewall logs. Initially, an overview of all the connections is presented, the user could also click on one node to show the graph central to this node. In the right panel of the interface, the anomalies happened to the selected nodes are shown, with a textual list view in the top and a detailed temporal view in the bottom. In the bottom of the entire interface, there is a time slider. The user could manually select a time range and go deep to the graph and anomalies in the selected time range.

*e-mail: qi.liao@cmich.edu
†e-mail: shllsh@cn.ibm.com
‡e-mail: qianwh@cn.ibm.com
§e-mail: suzhong@cn.ibm.com

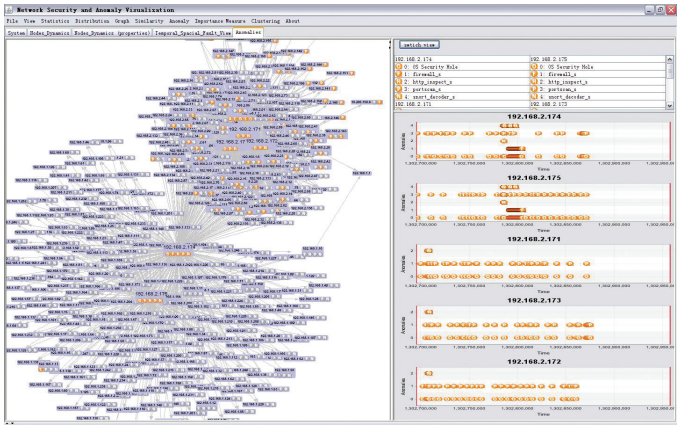

Figure 1: Situations with workstation 192.168.2.171 – 175. 171 – 173 and 174 – 175 have different anomaly patterns, including the bursty "snort_decoder" at the start and the continuous portscans. All 5 workstations have severe system security hole during the time.

2 EVENTS OF INTEREST

- Figure 1: The workstations 192.168.2.171-175 have severe security holes indicated by the Nessus network vulnerability scan report. These workstations also initiate various types of portscans, TCP communications anomalies and http attacks to the servers (192.168.1.*) and workstations (192.168.2.*).
- Figure 2: The workstations 192.168.2.11-138 continue to portscan server machine 192.168.1.2, 192.168.1.14, 192.168.1.6. Some of the workstations, including 192.168.2.68, 2.154, 2.33, 2.55, 2.147, 2.92, 2.28, 2.143, 2.17, 2.56, 2.51 initiate fragmentation overlap attack to 192.168.1.2 and 192.168.1.14 similar to teardrop attacks.
- Figure 3: The DC/DNS/DHCP server 192.168.1.2 (primary), 192.168.1.14 (secondary) and mail server 192.168.1.6 encounter continuous portscans and DoS attacks by both 192.168.2.11-138 (bots) and 192.168.2.171-175 (initiators). There are several high-risk OS security events on 192.168.1.2, the primary data server, including security log cleared event, more than 15 times logon attempts using explicit credential, more than 50 times operations on account domain objects (user, group, group policy container, etc.), more than 20 times validation of the credentials and two logon fails and one computer account change.
- Figure 4: The workstations 192.168.1.10-13 get continuous snort_decoder/http_inspect attacks and portscan by 192.168.2.174-175.
- Figure 5: The external web server 172.20.1.5 is intruded by 10.200.150.201 at port 3389. Then 172.20.1.5 attacks the internal web server 192.168.1.5 at port 445 (well-known Windows system flows to execute arbitrary code). 192.168.1.5 later gets many OS security events on logon failures.

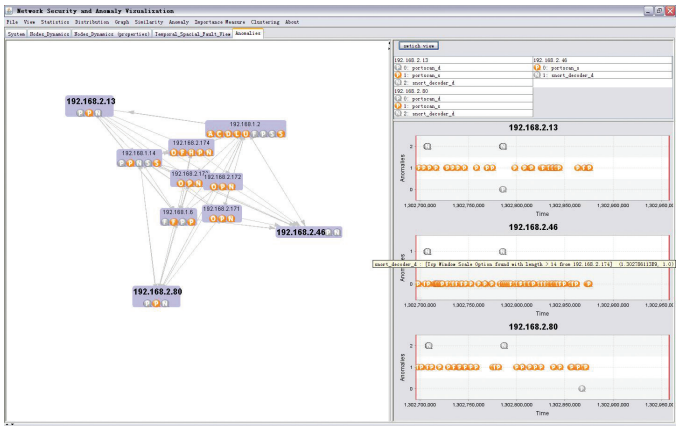

Figure 2: Situations with 192.168.2.11-138. These workstations are attacked on the morning of the first two days and continuously portscan 1.2/1.6/1.14 server machines.

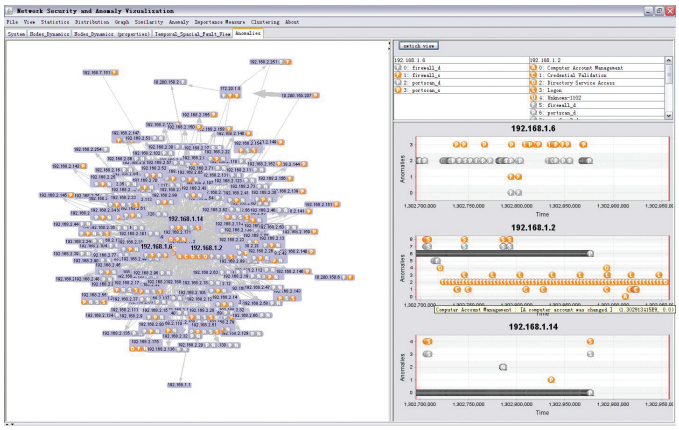

Figure 3: Situations with 192.168.1.2 / 192.168.1.14 / 192.168.1.6. 1.2 and 1.14 are troubled with all-time portscans and some teardrop attacks. DC 1.2 also has various system account high-risk operations identified by os security logs.

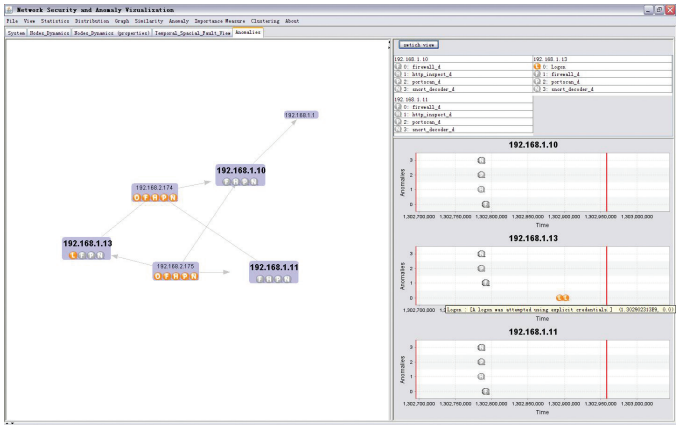

Figure 4: Situations with 192.168.1.10-13. 1.13 has logon attempts with explicit credential after attacked by 192.168.2.174-175 on 135/445/3389 ports.

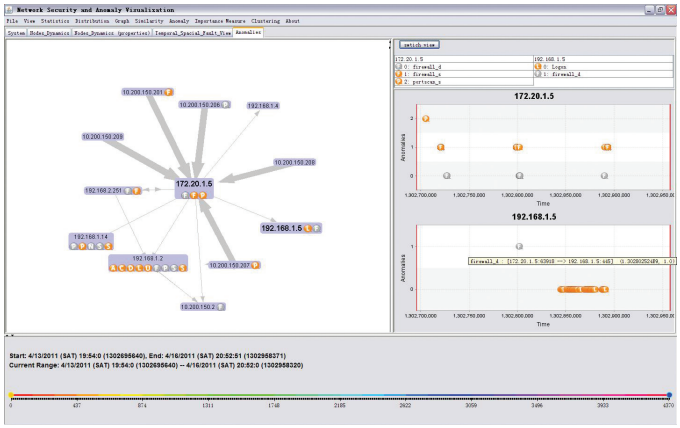

Figure 5: Situations with 172.20.1.5 and 192.168.1.5. 172.20.1.5 is the external web server connected with several external hosts (10.200.150.*). The web server is attacked from outside and then operated to attack the internal web server 192.168.1.5, leading to the logon fail security event on 192.168.1.5.

3 Timeliness

- The workstations 192.168.1.171-175 attack can be as early as 2011-4-13 12:00:00, when bursty "snort_decoder" attacks in the morning just finished and the portscans issued by the workstations are spotted. CNO member could recognize the event from both the traffic graph (e.g., 192.168.2.171 has a star connection graph, and the bursty transmission of "snort_decoder" and portscans indicated in the right anomaly temporal panel).
- The workstations 192.168.2.11-138 hijacks and portscans the servers (DDOS) and these malicious behaviors could link to the attack from 192.168.1.171-173 on the morning of 4/13/2011 and the attack from 192.168.1.174-175 on the morning of 4/14/2011.
- Detection of the DC/DNS/DHCP server 192.168.1.2/192.168.1.14/192.168.1.6 attacks can be as early as 2011-4-13 23:00:00, when the first logon attempt with explicit credential has been issued at 192.168.1.2.
- The attack on workstations 192.168.1.10-13 can be detected by the night of the last day, 2011-4-15 20:00:00, when two logon attempts with explicit credentials happened.
- The attack on the external/internal web server 172.20.1.5/192.168.1.5 can be detected at 2011-4-15 3:00:00, when the first logon fails are logged on 192.168.1.5.

4 Recommendation

First, the events discovered in Section 2 implies that the nodes 192.168.1.171-175 are sources of security attacks due to the operating system security holes so arbitrary code can be executed on the remote host. One recommendation that computer network operations (CNO) group at All Freight should give to the CEO is to immediately fix the security holes on these nodes (1.171-1.175). Policy should be made to ensure all hosts running on the network should be periodically updated and unpatched machines should not be connected to the cooperate network. For other packet-based attacks, routers can be configured to drop packets with invalid options.

While these suggestions may be helpful, there is no panacea for security problem. The most practical and important approach is being able to detect and find the sources/causes of security violations and anomalies if they happen. Visual analytic tools such as the one developed and presented in this article can be extremely helpful to network operators and administrators at enterprise networks like All Freight.