Tool Update: High Alarm Count Issues in IDS RainStorm

Kulsoom Abdullah
Georgia Institute of Technology
Communications Systems Center
kabdullah.ece00@gtalumni.org

John A. Copeland
Georgia Institute of Technology
Communications Systems Center
john.copeland@ece.gatech.edu

ABSTRACT

We developed a tool to help network administrators deal with the large amount of alarms generated from network security appliances. It efficiently uses screen space representing a high number of IP addresses along with time sequence so that general alarm activity for a network can be visualized along with details, if desired. The tool was useful but encountered problems when there was a significant increase in the amount of alarms. The issues that resulted are addressed in this paper along with methods to ease them.

Categories and Subject Descriptors: C.2.0 [Computer Communication Networks]: General - Security and Protection; I.3.6 [Computer Graphics]: Methodology and Techniques - Interaction Techniques

General Terms: Performance, Design, Security, Human Factors.

Keywords: IDS alarm visualization, filtering network data, network security information visualization

1. INTRODUCTION

There are many innovative tools that visualize various network data types for security. The next stage is to incorporate more usability studies results to improve visualization tools and effectively deal with the growing and changing network that is producing more data.

Survey results presented in [2] showed that professional security analysts feel overloaded when alerts average 230 per hour. Information visualization has shown to help with the increasing amount of information users can handle versus traditional textual methods, but these visualization tools can also become useless as the number increases to greater amounts [3]. More user interaction and filtering functions are needed to help discover significant activity on a network.

Since our previous publication [1], we have developed more functions for our IDS alarm visualization tool, described in section 2. The tool has been ported to Java/OpenGL (JOGL) for better performance and flexibility.

2. FILTERING ON ALARM PARAMETERS

Filtering is needed to deal with occlusion, but it needs to be implemented in a way that will allow analysts to find information, especially when one does not always know what to look for or where.

VizSEC'06, November 3, 2006, Alexandria, Virginia, USA.
ACM 1-59593-549-5/06/0011.

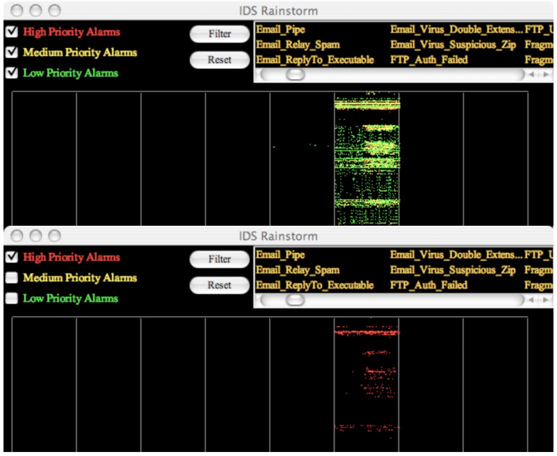


Figure 1: Filtering on high priority alarms.

2.1 Alarm Priority

Figure 1 shows high priority alarm filtering results. A clearer view is obtained, and taking care of alarms types separately is easier rather than analyzing them all at once.

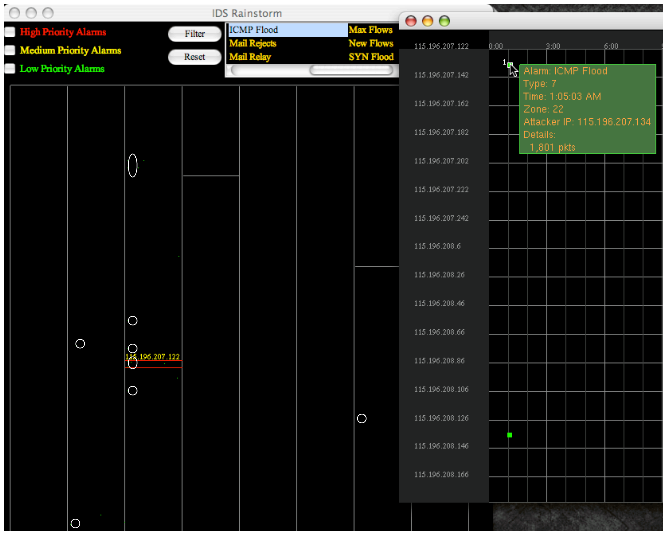
2.2 Alarm Type

Filtering on alarm type helps to pinpoint on a particular activity. Any alarms that you know are serious can be singled out and dealt with, like the Worm Activity alarm. It also helps find instances when a combination of alerts can signify one type of behavior, such as the SYN Flood and ICMP alarms. A machine that generates both these alarms 99% of the time has a virus or has been compromised. Being able to perform a Boolean OR function helps when just one alarm does not define the activity in question.

2.3 Filtering Summary

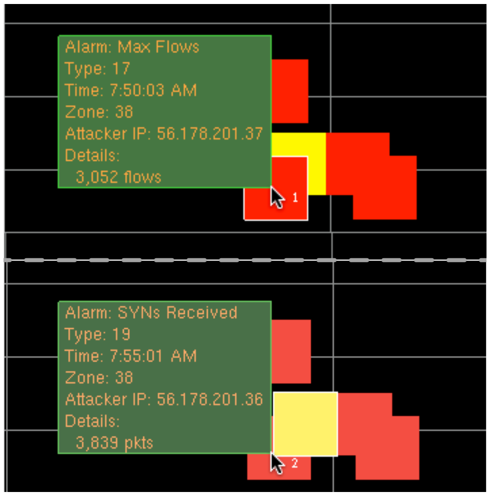
Unix functions like *grep* can be used on text logs for filtering, but this is tedious. Being able to filter while visualizing the data is easier and one can see an instant view of the filter result.

Figure 2 illustrates an example when both isolating an alarm helps to notice an important pattern. Shown in the figure are ICMP Flood alarms. There is not a great number but the majority of them appear to occur around the same time (see circled alarms). Upon closer investigation, it is found that seven of these alarms occurred at exactly 1:05:03 AM and two occurred at 1:10:05 AM. A new automated worm was discovered on these hosts.



Alarm: ICMP Flood
Type: 7
Time: 1:05:03 AM
Zone: 22
Attacker IP: 115.196.207.134
Details:
1,801 pkts

Figure 2: ICMP Flood alarm filtered. Alarms circled occurred simultaneously for those hosts.



Alarm: Max Flows
Type: 17
Time: 7:50:03 AM
Zone: 38
Attacker IP: 56.178.201.37
Details:
3,052 flows

Alarm: SYNs Received
Type: 19
Time: 7:55:01 AM
Zone: 38
Attacker IP: 56.178.201.36
Details:
3,839 pkts

Figure 3: Indexing through alarms that are overlapped. This is shown zoomed in for clarity.

3. ALARM GLYPH OCCLUSION

Increased alarm count can lead to overlap in the zoom view. The method implemented to deal with this uses left and right mouse clicks to index through any alarms or lines that overlap in the same spot (Figure 3).

4. IP ADDRESS LABELING OCCLUSION

The number of external IP addresses inevitably leads to overlap with the text labels on the right vertical axis in the zoom view. Highlighting the IP address label on a mouseover helps, but only when you mouseover a specific alarm. The technique implemented provides spacing between labels if collision occurs. Only unique IPs associated with alarms in the current zoom view are printed (Figure 4).

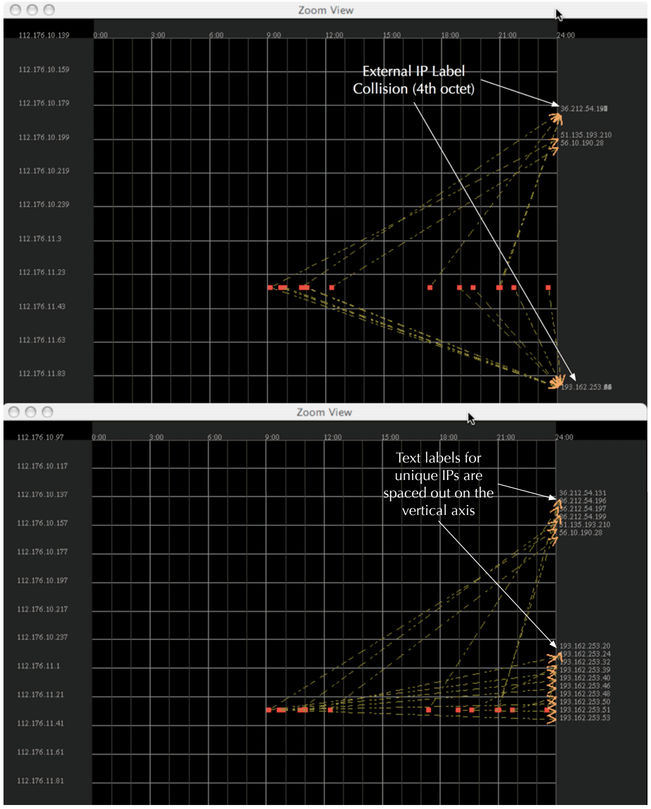


Figure 4: Before (T) and after (B) of IP address labeling techniques.

5. ACKNOWLEDGMENTS

Thanks goes to Greg Tedder for helping with the conversion to JOGL. Also to the Internet Security team at OIT at Georgia Tech for valuable feedback.

6. REFERENCES

[1] K. Abdullah, C. Lee, G. Conti, J. Copeland, and J. Stasko. Ids rainstorm: Visualizing ids alarms. In *IEEE Symposium on Information Visualization's Workshop on Visualization for Computer Security (VizSEC)*, pages 1–10, 2005.

[2] G. Conti, K. Abdullah, J. Grizzard, J. Stasko, J. A. Copeland, M. Ahamad, H. L. Owen, and C. Lee. Countering security information overload through alert and packet visualization. *IEEE Computer Graphics and Applications*, 2006.

[3] G. Conti, M. Ahamad, and J. Stasko. Attacking information visualization system usability: Overloading and deceiving the human. In *Symposium on Usable Privacy and Security (SOUPS)*, July 2005.