NetSecRadar: A Visualization System for Network Security Situational Awareness

Fangfang Zhou, Ronghua Shi, Ying Zhao*, Yezi Huang, Xing Liang

School of Information Science and Engineering, Central South University, Changsha, China
{zff,shirh,zhaoying, huangyezide,liangxing}@csu.edu.cn

Abstract. Situational awareness is defined as the ability to effectively determine an overall computer network status based on relationships between security events in multiple dimensions. Unfortunately, as the lack of tools to synthetically analyze the security logs generated by kinds of network security products, such as NetFlow, Firewall and Host Security, it is difficult to monitor and perceive network security situational awareness. Information visualization allows users to discover and analyze large amounts of information through visual exploration and interaction efficiently. Even with the aid of visualization, identifying the attack patterns from big multi-source data and recognizing the abnormal from visual clutter are still challenges. In this paper, a novel visualization system, NetSecRadar, is proposed for network security situational awareness based on multi-source logs, which can monitor the network and perceive the overall view of the security situation by using radial graph. NetSecRadar utilizes a hierarchical force-directed graph layout for arrangement of thousands of hosts to better use the available screen space, and provide the method to quantify the dangerous levels of the security events, and find the correlations of security events generated by multi-source logs and perceive the patterns of abnormal in situational awareness, and synthesizes interactions, filtering and drill-down to understand the detail information. To demonstrate the system's capabilities, we utilize the VAST Challenge 2013 as case study.

Keywords: Network Security, Situational Awareness, Information Visualization, Radial graph.

1 INTRODUCTION

With the size and complexity of networks continuously increasing, network security analysts face mounting challenges of securing and monitoring their network infrastructure for attacks. This task is generally aided by kinds of network security products, such as NetFlow, firewall and Host security system. As the number of security incidents continues to increase, this task will become ever more insurmountable, and perhaps the main reason that the task of network security monitoring is so difficult is the lack of tools to provide a sense of network security situational awareness that defined by the Department of Homeland Security as

"the ability to effectively determine an overall computer network status based on relationships between security events in multiple dimensions."[1]

The fields of statistics, pattern recognition, machine learning, and data mining have been applied to the fields of network security situational awareness [2]. Although new systems, protocols and algorithms have been developed and adopted to prevent and detect network intruders automatically. Even with these advances, the central feature of Stoll's story has not changed: humans are still crucial in the computer security process [3]. Administrators must be willing to patiently observe and collect data on potential intruders. They need to think quickly and creatively.

Unlike the traditional methods of analyzing network security textual log data, information visualization approach has been proven that it can increase the efficiency and effectiveness of network intrusion detection significantly by the reduction of human cognition process [4]. Information visualization cannot only help analysts to deal with the large volume of analytical data by taking the advantage of computer graphics, but also help network administrators to detect anomalies through visual pattern recognition. It can even be used for discovering new types of attacks and forecasting the trend of unexpected events. Current research in cyber security visualization has been growing and many visual design methods have been explored. Some of the developed systems are IDGraphs [5], IP Matrix [6], Visual Firewall [7] and many others.

Even with the aid of information visualization, there are still complex issues that network security situational awareness is difficult to describe, because the security events are hard to quantify, the terminology and concepts become too obscure to understand, and large number and scope of the available security multi-source data become a great challenge to the security analysts.

In this paper, a novel visualization system, NetSecRadar, is proposed which can real-time monitor the network and perceive the overall view of security situation and find the correlation of dangerous events in logs generated by multi-source network security products using radial graph that is aesthetically pleasing and has a compact layout for user interaction. The system utilizes multi-source data to analyze the irregular behavioral patterns to identify and monitor the situational awareness, and synthesizes interactions, filtering and drill-down to detect the potential information.

The rest of this paper is organized as follows. Related work is discussed in Section 2 and the design of the visualization system is presented in Section 3. In Section 4, two examples are analyzed by using our system. Finally conclusion and the future work are shown in Section 5.

2 RELATED WORK

As the development of network application and technology, network security events like illegal access, DDoS attack and worm spread etc become more and more serious. A mass of security equipments, like firewall, IDS and anti-virus, are widely used in monitoring networked systems, and numerous approaches, like

statistics, machine learning and data mining, are deeply focused to identify anomalies [2]. However, when network security analysts face large quantities of networks events, the most difficulty question they have to answer is "How can I get an effective assessment of the global network security condition based on those events?" Bass [8] introduced situation awareness into the field of network security. After that, Network Security Situation Awareness (NSSA) became a new research field which determined the current status of all network assets based on tremendous network events in support to the further operations.

Network security visualization is a growing community of network security research in recent years. More and more visualization tools are designed to help analysts cope with huge amount of network security data. Hence the demand of visualization techniques has stretched into each step of situation awareness research like situation perception, situation comprehension and even situation prediction. NVisionIP [9] and VisFlowConnect [10] take the lead in introducing visualization technology into NSSA, NVisionIP uses multi-level matrix graphs in status analysis of a class-B network by using NetFlow logs, and VisFlowConnect is a visualization design based on parallel axis technology to enhance the ability of an administrator to detect and investigate anomalous traffic between a local network and external domains. The Intrusion Detection System (IDS) is the most popular application that reports a variety of network events taken for the important input data of NSSA, IDS RainStorm [11], SnortView [12] and Avisa [13] are typical visual analysis tools that help administrators to recognize false positives, detect real abnormal events such as worm propagations and Botnet activities and make a better situation assessment. However, those visual systems based on a single kind of logs such as NetFlow log or IDS log are obviously insufficient. To achieve situational awareness BANKSAFE [14], a scalable and web-based visualization system, analyzes health monitoring logs, Firewall logs and IDS logs in the same time, and Horn [15] uses visual analytics to support the modeling of the computer network defense from kinds of raw data sources to decision goals.

Radial visualization is an increasingly popular metaphor in information visualization research because of its aesthetic appeal, its compact layout, and its interaction ability. LiuHe [16] presents a radial visualization system to reveal the characteristics of trip or road taken by taxi drivers, and Contingency-Wheel [17] is a visual analytics system which discovers and analyzes nontrivial patterns and associations in large categorical data by using the metaphor of wheel. In the field of network security visualization, there are many tools using radial graph such as Radial-Traffic-Analyzer [18], Avisa [13], and FloVis [19] etc. VisAlert [20][21] is a radial paradigm for visual correlation of network alerts and situation awareness from disparate logs. It's very good at dealing with three attributes of network security event, namely: What, When, and Where, and this paradigm facilitates and promotes situational awareness in complex network environments by visual analytics of events correlation. IDSRadar [22] presents a novel radial visualization framework to analyze source IPs, destination IPs, alert types and time of IDS alerts. Moreover, it utilizes five categories of entropy functions to quantitatively

analyze irregular behavioral patterns. There are two problems in VisAlert and IDSRadar. One is the lack of host automatic layout based on network topology to deal with the change of the host number and the growing network. Another one is visual clutter issue raised by too much straight lines appearing in the same time. To address those problems and provide a better visual tool for network events analysis and security situation assessment, the following describes our approach carefully.

3 NetSecRadar VISUALIZATION SYSTEM

3.1 Information to be visualized

The users of our visualization system for network security situational awareness are network security analysts or administrators, who use network security products to observe network status, detect any abnormal behavior, analyze the reasons behind it and report the dangerous as soon as possible. The following fundamental questions are needed to be addressed by themselves,

- "Is anything bad occurring in the network?" (using of automated tools to distinguish suspicious behavior requiring further investigation),
- "Where is something bad occurring in the network?" (spatial assessment of macro/micro assets),
- "When did bad events first occur in the network?" (temporal assessment of activity),
- "How is something bad occurring in the network?" (mechanism of attack).

It is difficult for network security analysts to answer the questions because the mass amount of the log data generated by kinds of network security products, about a few GB a day, makes them boring; a large percent of false positive, more than 90%, makes them confused; the lack of correlation analysis among the network security products makes them low efficiency. In this paper, the data source of our visualization system comes from multiple sources, such as NetFlow, Firewall and Host security log. The following information of the logs is essential for our visualization system.

- **NetFlow:** A network flow is an abstraction of a sequence of packets between two end points. A Cisco NetFlow is defined as an unidirectional NetFlow that is identified by the following unique keys: timestamps, source IP address, destination IP address, source port, destination port, protocol type, TOS (type of service), and the amount of traffic, etc.
- **Firewall:** A firewall is used by a network security system to control the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed to go through or not, based on a rule set. A firewall establishes a barrier between a trusted, secure internal network and another network. The firewall logs includes properties, such as timestamp, syslog

priority (information or warning), operation (Built, Teardown or Deny), protocol(TCP or UDP), source IP address, destination IP address, source port and destination port, Direction(inbound or outbound).

- **Host Health Status Log:** The security log records events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files. Multiple entries may be recorded if a particular action creates multiple security events. The host security logs include properties, Timestamp; Data field entry contains the name of the type of data present and the value of the data. Typical values will include the username, the domain name, the IP address, the workstation name, or the port name.

The network security logs are saved as different file format and the same content of the logs, such as IP address, is recorded in different format and every record in the logs are sampled at different sampling time. So it is necessary for us to register the logs in sampling time and format before implementing our visualization system and MySQL database is utilized to save data from our registered multi-source logs for its quick and powerful queries.

3.2 Visual and Interaction Design

The visualization system for network security situational awareness has been developed by using radial visualization. Figure1 illustrates the design of our system, which is composed of two areas, the radial visualization area and the interactive control panel. The radial visualization area includes four parts, servers and workstations, network security events, histogram of event counts and events correlation. The interactive control panel provides the network security analysts with the function of parameter setting and selecting. The following are details of the design.

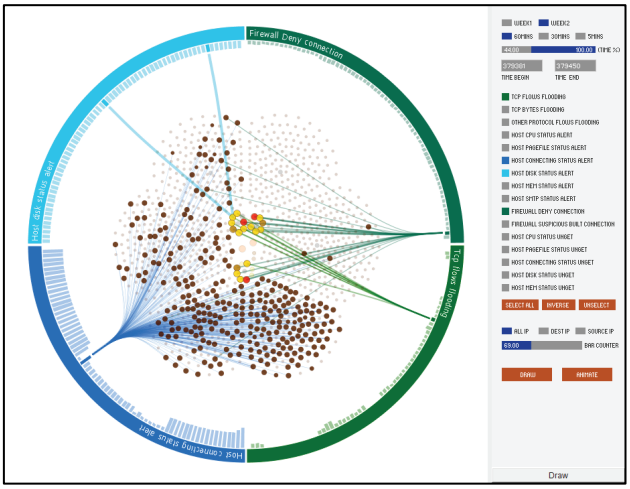
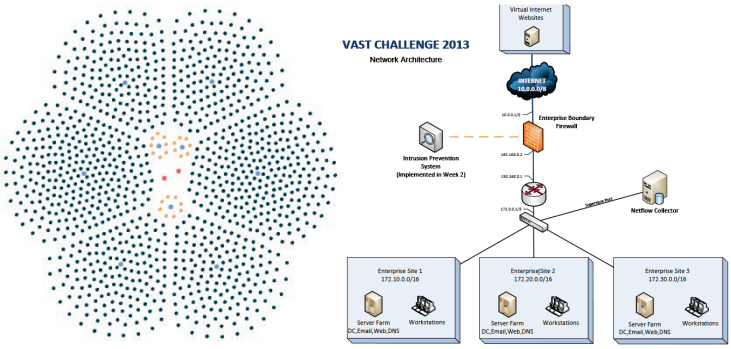


Fig. 1. Design of our visualization system

Servers and Workstations.



(a) (b)

Fig. 2. (a) Servers and workstations arranged by hierarchical force-directed layout algorithm; (b) A network topology in the VAST challenge 2013

In the center part of the radial graph, shown in figure 2 (a), the colored nodes arranged by force-directed layout algorithm are servers and workstations of a corresponding corporate network, shown in figure 2 (b), which is composed of more than one thousand workstations and about ten servers, routers and switches. The force-directed algorithm is an undirected graph layout calculated by all attraction and repulsion forces contained within the structure of graph itself, rather than relying on domain-specific knowledge. Graphs drawn with these algorithms tend to be esthetically pleasing, exhibit symmetries, and produce crossing-free layouts for planar graphs.

In this paper, we developed a hierarchical force-directed graph layout to better exploit the available screen space. Firstly, one thousand workstations and the servers in the corporate network are classified into two classes, the high priority class and the normal priority class. The high priority class includes servers with high priority, such as firewall server, core server, routers of servers and workstations; the normal class includes normal servers and normal workstations. Then in a first step of our hierarchical force-directed algorithm, servers and routers in the high priority class are arranged constrained in a circle using force-directed algorithm, the routers of workstations are constrained on a circle, such as blue nodes on circle shown in figure 2 (a), and the routers of servers, the firewall server and core server are distributed near the center of the circle, such as blue nodes and red nodes in the center of the circle. After the nodes of routers in blue and servers in red get balanced, the user can close the force among them and interactively move the nodes to a better position. In the second step of our layout algorithm, the workstations or servers with normal priority in the sub-intranet, which are nodes in green or in orange, will be arranged around their routers which are other nodes in blue, by the second hierarchical force-directed graph algorithm considering all attraction and repulsion forces among nodes in the normal priority class rather than the high priority class. Finally, one thousand workstations are symmetrically distributed around the circle like petals, and severs are near the

center like stamen. Our hierarchical force-directed layout algorithm and flexible interaction can help get a compact and beautiful effect of layout.

Network Security Events.
The colored arcs of the ring, shown in figure3, are known as the network security event types, such as firewall deny connection ring in orange, host CPU states alert ring in blue and TCP flows flooding in green. The security event types can be any dangerous behavior in firewall, NetFlow and host security logs and are set by network security analysts and are listed on the control panel. The event types will be drawn uniformly on the ring when they are selected according to the interest of the analysts, because there is limited area on the ring and are too many event types. The width of arc for every event type on the ring, L_e, can be calculated by:

$$L_e = L_r / N_e \tag{1}$$

L_r is the perimeter of the ring, N_e is the number of selected event types.

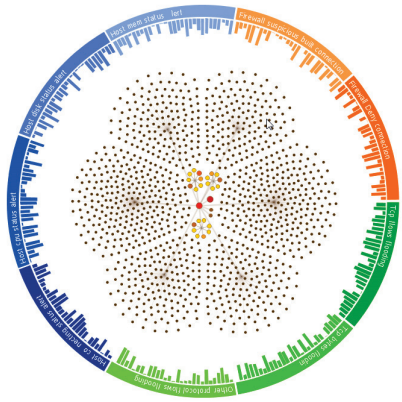


Fig. 3. The ring of event types and histogram of event counts

Three primary colors are used to visually distinguish the security events generated by different data sources, such as firewall in orange or NetFlow in green or host security logs in blue, and the intensity and saturation are used to differentiate the events from the same source, for example the color of Firewall Deny Connection is darker than that of Firewall Suspicious Built Connection. The color of every event type is set by users in advance, and the name of event type will be shown on the arc of the ring if there is enough space to better recognize event types.

Histogram of Event Counts.
The histogram inside the event types is drawn clockwise along the arc of the ring. The bars of the histogram have the same color with that of the event types, and the height of the bar of histogram of the particular color arc represents the amount of this event type happened or observed in a sampling time which can be minutes or hours tuned by the security analysts. The whole time span of the arc can be

also tuned by the security analysts. Our system will calculate the number and width of bars of the histogram, N_{bar} and W_{bar}, on arc according to the sampling time, t, the whole time span, T, and the width of the arc of event type, L_e .

$$N_{bar} = T / t; \tag{2}$$

$$W_{bar} = L_e / N_{bar} \tag{3}$$

The higher the bar is, the more dangerous the network security status is, and especially when several bars of event types are high at the same time. So the security analysts of network security can understand and analyze synthetically the network security trends according to events from the firewall, NetFlow and host security logs.

Events Correlation.

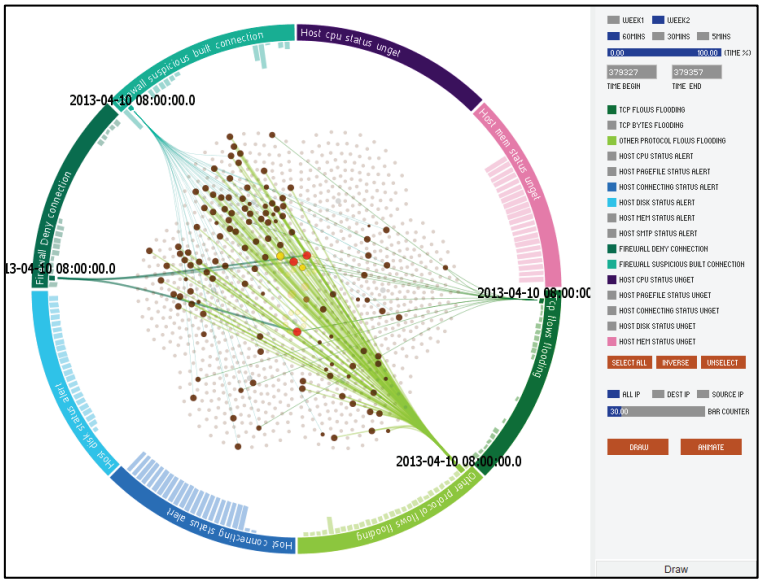


Fig. 4. Event correlation in a same time interval

A network security event includes timestamp, source address and destination address. When the dangerous status was found from the histogram, the security analysts would like to know the details of the dangerous information. So we draw a curve, which connects the top of the bar of the histogram where the event happened and the source address or destination address of the topology diagram in the center of the ring, shown in figure 4. The color of the line is the same with the color of the event type. The width of the curve is related to the dangerous level which is set by network security analysts in advance. Dangerous level of an event type is related to the hosts, for example when the number of Firewall Deny Connection to a server or workstation is more than a threshold, the server or work-

station is a dangerous host and would be connected by a thicker curve, and the node which represents the host is also bigger. The IP address of the host will be drawn when the dangerous node was clicked. The event correlation can help the network security analysts understand which nodes are dangerous attackers or victims. Moreover, to address visual clutter issue raised by too much straight lines appearing in the same time, we use curves to replace straight lines and implement the bundling effect

Interaction.

Our visualization system provides the network security analysts with interactively setting parameters, such as the whole visiting time span, T, and the sampling time, t, and also allows the security analysts to filter by simply clicking on any of the hosts, servers, event types and bars of histograms. If the analysts, for example, want to see the attacks of an event type in a time interval, it just needs to click on the bar of event type, as shown in figure5. If a workstation is clicked, the attacks related to it will be shown. When the analyst points to a highlighted node in an event, the detail information about the host, such as host name and IP address, will be drawn. If you want to compare the attacks in this interval, multi-selection is provided with. These pointing and clicking features allow users for a smooth, thorough analysis. Another advantage of our visualization system is its use of animation to display the system transitions from one state to another in the whole time span, such as the distinct changes of event types and the amount of events to perceive the dangerous behavior pattern.

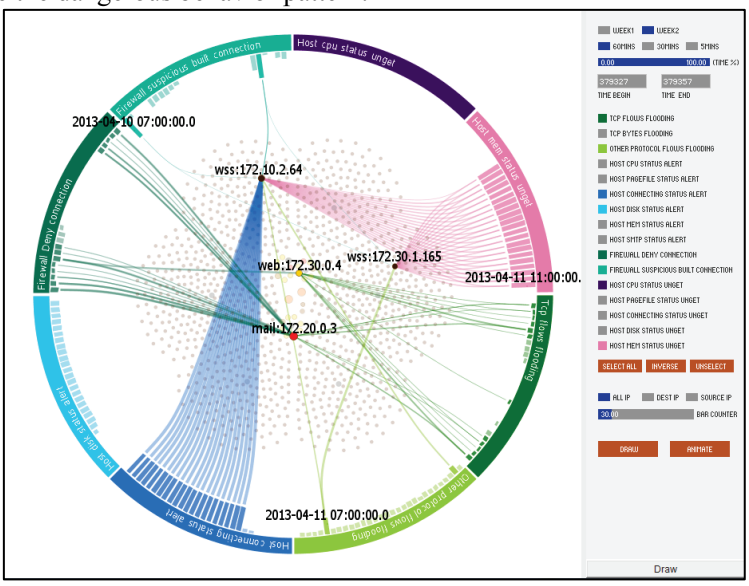


Fig. 5. Interaction in the visualization system

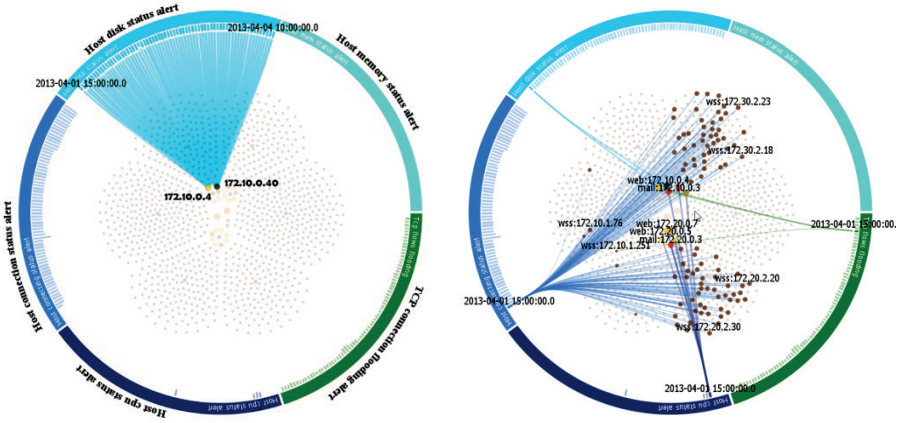
4 RESULTS AND ANALYSIS

The visualization system, NetSecRadar, is implemented by Processing in windows 7 on a PC with a 1.87GHz Intel Pentium(R) 4 CPU, 4 gigabytes of memory, a Ge-Force 8800 GTX graphics card. In this section, our visualization system is used to analyze mini-challenges of IEEE VAST challenge 2013. The challenge provides multiple network security data sources, NetFlow, Firewall logs and Host Health Status logs, in 2 weeks, from 2013-4-1 7:00 to 2014-4-15 7:00, and NetFlow and Firewall has 70 million and 16 million records respectively, and Host Health Status logs generated by BigBrother software has 55 million thousand records.

In the first case study, we selected five event types, TCP Connection Flooding alert in NetFlow log, and Host Disk alert, Host CPU alert, Host Connection problem and Host Memory alert in BigBrother log, from 2013-4-1 12:00 to 2013-4-4 6:00, sampled by one hour.

Firstly, we found two events with obvious features, shown in figure 6(a), in this time span. One is the Host Disk alert detected by BigBrother which has kept reporting from Web server 172.10.0.4 and Admin server 172.10.0.40 every hour，and we further found that both disks of the servers have been occupied over 90% in log file. Another is the Host Memory alert that has never been observed in this time span.

Then a sign of the first abnormal behavior in the Intranet was found in 15:00 2013-4-1. We found a few Host CPU alerts generated by Web and Mail Servers as well as many Host Connection problems caused by subnets 172.30.2.* and 172.20.2.*, at the same time, some TCP Connection Flooding from Web Sever 172.10.0.4, Mail Server 172.10.0.3and workstation 172.10.1.251, shown in figure 6(b).

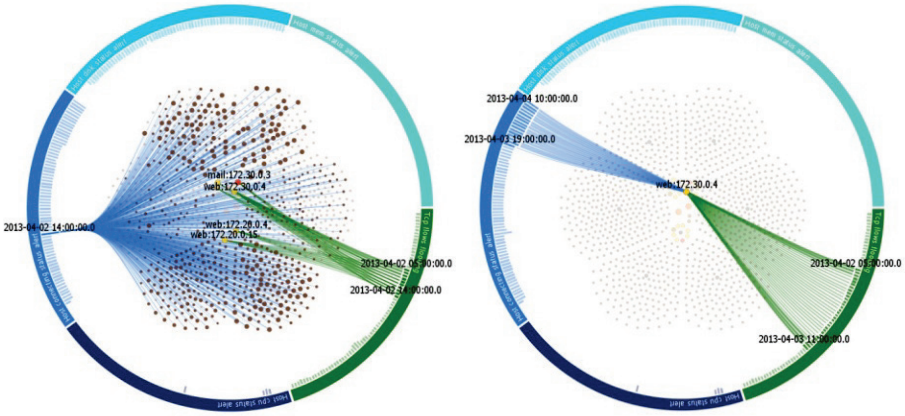


(a) (b)

Fig. 6. (a) Detail information of the Host Disk alerts from 2013-4-1 12:00 to 2013-4-4 6:00; (b) Correlation analysis of Host CPU alert, Host Connection problem and TCP Connection Flooding in 15:00 2013-4-1

In the morning of the following day, 2013-4-2, continuous warning of TCP Flooding alerts was generated by several servers, as shown in figure 7(a). From checking the NetFlow log, a DDoS attack was found. At 5:00 April 2nd, through over 60,000 source ports, ten external hosts like 10.6.6.14, 10.6.6.6, 10.6.6.13, 10.7.7.10 started the DDoS attack to port 80 of internal Web servers, and lasted to 14:00 April 2nd. The connection alert kept emerging in the Big Brother logs, and the number of the connection alert had a significant growth after the DDoS attack on April 2nd, so we can determine the DDoS attack that brought a great harm to the Intranet.

The most serious victim is server 172.30.0.4, as shown in figure 7(b), because it generated TCP Flooding alerts continuously from 2013-4-2 5:00 to 2013-4-3 11:00. Especially it suffered more serious attacks from 5:00 to 7:00 on 2013-4-2 and from 11:00 to 12:00 on 2013-4-3 for the thicker of the green curves. We also found that the server, 172.30.0.4 seemed to go down for the constant Host connection alarm since 2013-4-3 19:00.



(a) (b)

Fig. 7. (a) The network security situation under a DDoS attack on 2013-4-2; (b) Detail information about the most serious victim, server 172.30.0.4

We select another set of log data from 2013-4-12 13:00 to 2013-4-14 20:00, 4 event types are Denied Connection alert from Firewall logs, TCP Connection Flooding in NetFlow log, Host Disk problem and Host Connection problem from Host Health Status logs.

We could first find one server, 172.0.0.4, kept sending the Host Disk alert almost every hour, shown in figure 8(a). It seems that 172.10.0.4 kept reporting alert for two weeks while 172.10.0.40 got well in the second week.

From 5:00 to 22:00 on April 13, Web servers 172.10.0.4 and 172.10.0.8 raised lots of TCP Connection Flooding alerts and Firewall Denied Connection alert. At 15:00 on April 14, more web servers, such as 172.20.0.4 and 172.20.0.15 raised TCP Connection Flooding alerts, but no firewall warning was found on those web

servers at the same time, shown in figure 8(a). From 2013-4-13 5:00 to 4-13 22:00, Only a few workstations have Host Connection problem in BigBrother logs , shown in figure 8(b), but the number of the connection alert had a significant growth at 15:00 on April 14, shown in figure 8(c). Through further analysis of the log, over twenty external hosts IPs tried to attack web servers, and a massive number of TCP Flag exception packet sending from external IPs were denied by firewall, however, firewall failed to resist the attack by noon on April 14.

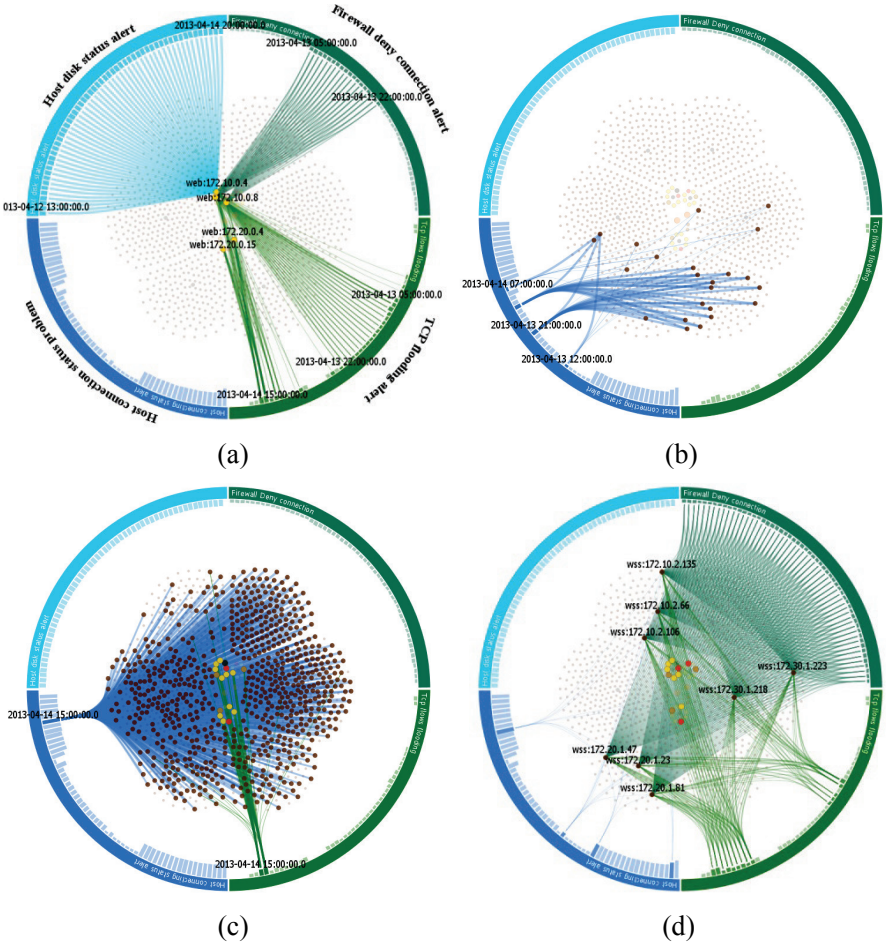


Fig. 8. (a) Detail information of workstations and servers from 5:00 to 22:00 on April 13; (b) Host Connection problem from 4-13 12:00 to 4-14 7:00; (c) Host Connection problem in 2013-4-14 15:00; (d) The workstations suffered Denny Connection and TCP Flooding

When observing all Firewall Deny alerts, eight internal hosts were suspicious. Not only a great number of Firewall Deny Connection events but also massive TCP Connection Flooding alerts were raised by them, shown in figure 8(d). After

examining logs for further diagnosis, beginning from 8:28 April 12th, and these eight internal hosts started accessing the port 22 of external host 10.0.3.77 regularly and the accessing number to 10.0.0.4~10.0.0.14 is much larger than that to other workstations. Hence these eight internal hosts are noteworthy.

5 CONCLUSION AND FUTURE WORK

In this paper a network security visualization system, NetSecRadar, is proposed to assist in monitoring and identifying abnormal pattern behavior based on multi-source logs in network security situational awareness by using radial graph. A hierarchical force-directed graph layout for arrangement of thousands of servers and workstations is proposed to better use the available screen space in the center of the radial graph, and a method of quantifying the dangerous levels of the security events is developed, and the correlations of security events generated by multi-source logs can be found by our graph design, and the interactions, filtering and drill-down, can help users understand the detail information of the events. We have evaluated the visualization system with attacks provided by VAST Challenge and have shown how our framework can be used to illustrate the attacks and visually correlate the events. In the future, we would like to extend the single view of radial graph to multiple views to show more details of servers and workstations. And further pattern analysis on individual host computer and individual risk will be performed.

ACKNOWLEDGMENTS

The authors wish to thank the anonymous reviewers for their comments. The authors would also like to thank the data providers, IEEE VAST Challenge. This work is supported by the National Natural Science Foundation of China under Grant Nos. 61103108, Hunan Provincial Science and Technology Program under Grant Nos. 2012RS4049, Hunan Provincial Natural Science Foundation under Grant Nos. 12JJ3062 and Postdoc Research Funding in Central South University.

REFERENCES

1. United States Department of Homeland Security. Team Coordination Training, Student Guide, May 2004.
2. Li B, Springer J, Bebis G, et al. A survey of network flow applications[J]. Journal of Network and Computer Applications, 2013, 36(2): 567-581.
3. Li X, Wang Q, Yang L, et al. The Research on Network Security Visualization Key Technology[C]//Multimedia Information Networking and Security (MINES), 2012 Fourth International Conference on. IEEE, 2012: 983-988.
4. Hadi S., Ali S. and Ali A.G. A Survey of Visualization Systems for Network Security. IEEE Transactions on Visualization and Computer Graphics. 2012, vol.18, no.8, 1313-1329.

5. Pin R., Yan G., Zhichun L. and Yan C. IDGraphs: intrusion detection and analysis using histographs. IEEE Workshop on Visualization for Computer Security. (Minneapolis, Minnesota, USA, October 26, 2005). VizSEC05. IEEE Computer Society, 2005, 39-46.
6. Hideki K., Kazuhiro O., Kanba K. Visualizing Cyber Attacks using IP matrix. IEEE Workshop on Visualization for Computer Security. (Minneapolis, Minnesota, USA, October 26, 2005). VizSEC 05.IEEE Computer Society, 2005, 91-98.
7. Chris P. L., Jason T., Nicholas G., Raheem B., John A.C. Visual firewall: real-time network security monitor. IEEE Workshop on Visualization for Computer Security. (Minneapolis, Minnesota, USA, October 26, 2005). VizSEC'05. IEEE Computer Society, 2005, 129-136.
8. Bass T. Intrusion detection systems and multisensor data fusion[J]. Communications of the ACM, 2000, 43(4): 99-105.
9. Lakkaraju K, Yurcik W, Lee A J. NVisionIP: netflow visualizations of system state for security situational awareness[C]//Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. ACM, 2004: 65-72.
10. Yin X, Yurcik W, Treaster M, et al. VisFlowConnect: netflow visualizations of link relationships for security situational awareness[C]//Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. ACM, 2004: 26-34.
11. Kulsoom A., Chris L., Gregory C., John A. C., John S. IDS RainStorm: visualizing IDS alarms. IEEE Workshop on Visualization for Computer Security. (Minneapolis, Minnesota, October 26, 2005). VizSEC'05. IEEE Computer Society, 2005, 1-10.
12. Hideki K., Kazuhiro O. SnortView: visualization system of snort logs. The 2004 ACM work-shop on Visualization and data mining for computer security. (Washington, DC, USA, Oc-tober 25-29, 2004). VizSEC/DMSEC '04. IEEE Computer Society, 2004, 143-147.
13. Hadi S., Ali S. and Ali A.G. IDS alert visualization and monitoring through heuristic host selection. Lecture Notes in Computer Science. 2010, vol. 6476, 445-458.
14. Fuchs J, Keim D A, Mansmann F, et al. BANKSAFE: A visual situational awareness tool for large-scale computer networks: VAST 2012 challenge award: Outstanding comprehensive submission, including multiple vizes[C]//Proceedings of the 2012 IEEE Conference on Visual Analytics Science and Technology (VAST). IEEE Computer Society, 2012: 257-258.
15. Horn C, D'Amico A. Visual analysis of goal-directed network defense decisions[C]//Proceedings of the 8th International Symposium on Visualization for Cyber Security. ACM, 2011: 5.
16. Liu H, Gao Y, Lu L, et al. Visual analysis of route diversity[C]//Visual Analytics Science and Technology (VAST), 2011 IEEE Conference on. IEEE, 2011: 171-180.
17. Alsallakh B, Aigner W, Miksch S, et al. Reinventing the contingency wheel: scalable visual analytics of large categorical data[J]. Visualization and Computer Graphics, IEEE Transactions on, 2012, 18(12): 2849-2858.
18. Keim D A, Mansmann F, Schneidewind J, et al. Monitoring network traffic with radial traffic analyzer[C]//Visual Analytics Science And Technology, 2006 IEEE Symposium On. IEEE, 2006: 123-128.
19. Taylor T, Paterson D, Glanfield J, et al. Flovis: Flow visualization system[C]//Conference For Homeland Security, 2009. CATCH'09. Cybersecurity Applications & Technology. IEEE, 2009: 186-198.
20. Livnat Y, Agutter J, Moon S, et al. A visualization paradigm for network intrusion detection[C]//Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC. IEEE, 2005: 92-99.
21. Yarden L., Jim A., Shaun M. and Stefano F. Visual correlation for situational awareness.

IEEE Symposium on Information Visualization. (Minneapolis, Minnesota, USA, October 23-25, 2005). INFOVIS'05. IEEE Computer Society, 2005, 95-102.
22. Zhao Y, Zhou F F, Fan X P, et al. IDSRadar: a real-time visualization framework for IDS alerts[J]. Science China Information Sciences, 2013: 1-12.