IDSRadar: A real-time visualization framework for IDS alerts

Article *in* Sciece China. Information Sciences · September 2012

DOI: 10.1007/s11432-013-4891-9

5 authors, including:

Xiaoping Fan
Central South University
92 PUBLICATIONS **309** CITATIONS

SEE PROFILE

SCIENCE CHINA
Information Sciences

• RESEARCH PAPER • doi: 10.1007/s11432-013-4891-9

IDSRadar: a real-time visualization framework for IDS alerts

ZHAO Ying[1], ZHOU FangFang[1*], FAN XiaoPing[1,2], LIANG Xing[1] & LIU YongGang[1]

[1]*Information Science and Engineering School, Central South University, Changsha* 410075*, China;*
[2]*Laboratory of Networked Systems, Hunan University of Finance & Economics, Changsha* 410205*, China*

Received November 5, 2012; accepted February 25, 2013

Abstract Intrusion Detection Systems (IDS) is an automated cyber security monitoring system to sense malicious activities. Unfortunately, IDS often generates both a considerable number of alerts and false positives in IDS logs. 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 and recognizing the false positives from a great number of alerts are still challenges. In this paper, a novel visualization framework, IDSRadar, is proposed for IDS alerts, which can monitor the network and perceive the overall view of the security situation by using radial graph in real-time. IDSRadar utilizes five categories of entropy functions to quantitatively analyze the irregular behavioral patterns, and synthesizes interactions, filtering and drill-down to detect the potential intrusions. In conclusion, IDSRadar is used to analyze the mini-challenges of the VAST challenge 2011 and 2012.

Keywords visual analytics, information visualization, cyber security, IDS log, entropy

Citation Zhao Y, Zhou F F, Fan X P, et al. IDSRadar: a real-time visualization framework for IDS alerts. Sci China Inf Sci, 2013, 56, doi: 10.1007/s11432-013-4891-9

1 Introduction

Intrusion Detection System (IDS) is a network security monitoring system that emits alerts when some predefined attack patterns (signature-based IDS) or potentially dangerous behaviors (anomaly-based IDS) have been detected [1]. One drawback of IDS is that the overwhelming number of alerts generated in a day will easily exhaust security administrators. Additionally, since signatures are not always written precisely enough, there are so many numbers of false positives in IDS alerts that distinguishing true alerts from them wears out security administrators [2].

Information Visualization is a promising solution to large data analysis because it utilizes the processing capabilities of the human visual system which allows users to see and understand large amounts of data at a glance, and visual analysis allows for perception of patterns that can lead to new insights to the underlying data by interaction. Current research in cyber security visualization has been growing and many visual design methods have been explored. Some of the developed systems are NVisionIP [3], IDS

*Corresponding author (email: zhouffang@gmail.com)

RainStorm [4], SnortView [5], VisFlowConnect [6], VisAlert [7] and many others. In general, the main focus is to achieve visual patterns of the true alerts and to help the analysts to explore them. Even with the aid of the visualization, identifying the attack patterns and recognizing the false positives from a great number of alerts are still challenges.

Radial visualization is an increasingly popular metaphor in information visualization. By using radial visualization, IDSRadar is a visualization framework to visualize a large number of Snort alerts which is able to monitor and analysis network security in real-time. The main reason of the prevalence of radial visualization is perhaps due to its aesthetic appeal, its compact layout, and its ability to put selectable data within easy reach for users [8]. Mansmann [9] develops a hierarchical sunburst visualization, which logically groups rules or object groups for firewall logs. The Sun metaphor shows an abstracted representation of the hierarchically grouped data. Furthermore, Alsallakh [10] uses a wheel metaphor to represent large categorical data to solve the problem of scalability. However, they both analyze the whole data set rather than considering the data with time changing.

In this paper, a novel visualization framework, IDSRadar, is proposed by using radial graph. It is able to monitor the network in real-time and perceive the overall view of security situation. The framework utilizes five categories of entropy functions to analyze the irregular behavioral patterns quantitatively to identify the false positives, and synthesizes interactions, filtering and drill-down to detect the potential intrusions.

The rest of this paper is organized as follows. Related work is discussed in Section 2 and the design of visualization framework is presented in Section 3. In Section 4, we detail the calculation of the entropy functions and perform a thorough analysis. In Section 5, two examples are analyzed by using our framework. Finally, conclusion and the future work are shown in Section 6.

2 Related work

Our IDS alerts visualization framework, IDSRadar, inspired by VisAlert [7], not only allows users to observe current and historical state of the network security, but also provides simultaneous representations of relevant entropies of IDS alerts and statistical information to make attacking patterns more clearly. The following are some visualization systems related to network security.

NIVA [11] is an early visualization system for intrusion detection data. The data comes from various intrusion detectors, and the system incorporates links and colors to signify attacks in a 3D graphical environment. The positions of nodes are calculated by gravitational theory, electromagnetics and fluid dynamics. The system fails when representing the alert data accelerated over one month.

SnortView [5] uses visualization to recognize false positives. The visualization system is composed of three main panels: the sources, alerts and destinations. SnortView uses a matrix view to display source IP of alerts over time. Alerts are drawn as glyphs with different services and protocols using a variety of shapes and colors. The system is limited to represent a large number of alerts.

IDGraphs [12] is an interactive visualization system designed to identify intrusive behavior by incorporating network flow. The flow-level traces with time were plotted on the horizontal axis and the aggregated number of unsuccessful connections was drawn on the vertical axis. The system also allows users to identify potential anomalies in an overview and analyze the details through interactively querying. However, the histographs is not so intuitive as we expected.

IP Matrix [13] uses a 2D matrix graph to represent IP space in Internet and the intranet. IDS alerts are drawn as colored pixels. The system shows its capability to detect the propagation tracks of a virus, such as Welhia and Sasser.D. A drawback of this system is that there are no host connections between Internet and the internal, which makes the system less intuitive.

Visual Firewall [14] is a network security visualization system with multi views for firewall operations, IDS alerts and overall network statistics. The real-time traffic view illustrates packets as dots, the packets flowing between hosts in the intranet and those in Internet. The statistics view illustrates the states of networks using histograms and alerts are displayed using colored lines. The authors believe that Visual Firewall can detect anomalous activities.

IDS RainStorm [4] is designed to visualize a flourishing number of IDS alerts generated from large networks. A main view of the system is depicted by eight vertical axes to represent a contiguous set of IP addresses and each horizontal axis associated with the vertical axes represents time. Alarms are represented as colored pixels. The system can detect abnormal network usages, worm propagations and Botnet activities.

VizAlert [15,16] is a radial paradigm for visualization of IDS alerts. The local network topology map is displayed in the center of the visualization system. The outer rings represent the various alert types. The rings width represents time and is divided into several periods. Each line connects a specific attack type on the outer ring to a source IP or target IP in the topology map to represent an alert. However, the source and target cannot be shown in a same view.

SpiralView [17] is a visualization system built on IDS to correlate security alerts with specific network applications. The main view is a spiral graph that depicts security events with their time of appearance. Alerts are illustrated as circles where color indicates alert type and size represents severity. The system can detect computers running malicious software in a network.

AlertGraph [18] is a 3D visual and alert classification system for Snort alerts. The advantages of the system are that it can highlight the true alerts from false positive alerts, and a large of number of alerts can be shown in a single view. However, interaction in a 3D space is not always easy.

Avisa [19] designs a radial graph to represent alerts and hosts. The alert types distribute on the top left corner of the ring, and the hosts in a network occupy the remainder of the ring. A spline which linked the alert type and the host represents an actual alert. The visualization system has a situation assessment component. However, the splines will cause clutter when there are more than hundreds of hosts and alerts.

3 IDS visualization framework

3.1 Information to be visualized

Our IDS logs come from two company networks monitoring by Snort. By investigating the IDS alerts, the following information is essential for analyzing and recognizing attack patterns [20].

- Timestamp of alert: The time of the recorded violation.
- Type of alert: The precise rule that is matched.
- Source IP: The address of potential attacker. The access from Internet is possible high risk.
- Destination IP: The address of the victim. The attacks to important systems, such as Web servers or Mail servers, are more dangerous than the access to clients.
- Source and Destination Ports: Network ports help to identify the services that are used in the observed attacks.
- Count of alerts: Sum of alerts in a time interval. The larger the sum of alerts is, the more dangerous the situation of network security is.

In addition, the following alerts are more likely to be considered as false positive detections according to network security experts' experience.

- Alerts which appear continuously: The alerts which appear continuously in the entire log are possible false positives.
- Alerts which appear many times: The alerts which appear many times in the entire log are more likely to be false positives.

3.2 Visual and interaction design

A network security visualization framework for a large number of IDS alerts has been developed by using radial visualization. Our design is composed of five main parts including servers and workstations, attack types, timeline and histogram, attack correlation and other information. The following are details of the visual and interaction design.

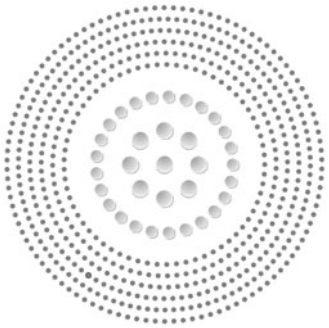

Figure 1 Arrangement of servers and workstations for a network.

Figure 2 Illustration for alert types.

3.2.1 *Servers and workstations*

Starting from the center part of the radial graph, shown in Figure 1, the nodes arranged in circles are servers and workstations of a corresponding corporate network. The bigger nodes are the servers with high priority in intranet, such as mail, file, website and database servers etc. Other nodes are individual workstations located in offices of the company. In the center of the alert type ring, the space is limited for many IPs, and the arrangement of all the IPs in concentric circles is one of the good ways to accommodate more IPs. The location of each node is ordered by its IP address, and generally those nodes, the IP address of which are in the same subnet, are arranged in the same circle or closer circles.

3.2.2 *Alert types*

The color band showed in Figure 2, formally known as the alert type band, is used to display IDS alert types. Each color represents each alert type since the color coding can ease visual correlation. The width of each color arc is corresponding to the percentage of the current alerts. The band will be updated in real-time while a new alert type is observed. At the same time, the escape mechanism will be set for alert types. When the number of alert types has already been larger than the threshold parameter, the alert types, which appear less, move in low frequency and never appear recently, will exit the drawing interface. The name of alert type will be shown on the arc if there is enough space.

3.2.3 *Timeline and histogram*

In our visualization framework, time is represented by animation, as shown in Figure 3. 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 in real time, and the height of the bar of the histogram represents the number of this alert type on the time span which can be minutes or hours tuned by the user. Most histograms in our examples are updated by every five minutes. The color of the bar is the same as that of the alert type, while the color of the bar of the histogram at current time is drawn in black.

In this occasion, the time is regarded as a discrete finite space. The bar of histogram will be overwritten from the beginning point of the arc once there is no more space to continue drawing along the alert type arc. The outer histogram represents the sum of all types of alert in a time span, and the color is the same as that of the overwhelming alert type.

3.2.4 *Attack correlation*

An actual alert in IDS logs includes timestamp, alert type, source address and destination address. So we draw a triangle, which connects the source IP node, the 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 4. The color of the triangle is the same as that of the alert type. To distinguish the source IP and the destination IP clearly, a dash line is used to connect the destination IP node with the bar of histogram of the alert

(a) (b)

Figure 3 (a) Histogram of the amount of attacks grouped by alert types every five minutes; (b) outer histogram of sum of attacks over time.

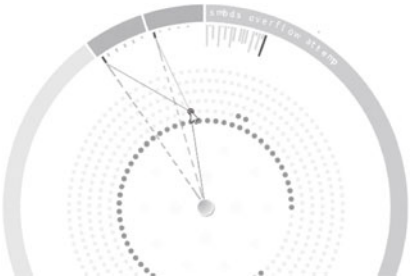

Figure 4 A triangle linked source IP, destination IP and alert type.

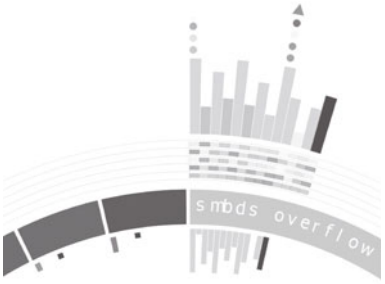

Figure 5 Other glyph of information visualization.

type. The nodes in an alert will be highlighted to differ from other nodes in the network. As shown in Figure 4, host launches two kinds of attack on the Firewall Server, and then through linking them, two Attack Correlation triangles have been formed. To avoid the visual clutter, the dash lines that link the alert types to the destination IPs will not be drawn in the overview graph. The triangles will be drawn by interaction.

3.2.5 *Other glyph of information visualization*

The outer ring shows statistical information to help network security administrator understand the Snort logs better. The outer histogram shows the sum of all alert types in a time span introduced in Subsection 3.2.3. The five tracks of mosaic represent respectively five categories of entropy functions which are alert type, source IP, destination IP, source port and destination port from inside to outside, to analyze uncertainty of the attack pattern and distinguish the false positives and real risks in a time span. The bigger the value of entropy is, the darker mosaic is, as shown in Figure 5.

Once a new alert type initially appears, a dot with corresponding color will be added on the top of the bar in the outer histogram. The triangle above the outer histogram is a mark representing a high risk in the time interval. The calculation of the risk parameter synthesizes the five categories of entropy functions and the number of alert types. When the parameter of risk is more than a threshold which is tuned by the user, the triangle will be marked on the time span.

3.2.6 *Interaction design*

Our visualization framework also provides users with interactively filtering by simply clicking on any of the hosts, servers, alert types, bars of histograms and tracks of entropy. The operations of zoom in, zoom out, play, stop, forward and backward are provided to help users to observe the situation of the network security. If an administrator, for example, wants to see the attacks of an alert type in a time interval, he just needs to click on the bar of alert type, as shown in Figure 6(b). If a workstation is clicked, the attacks related to it will be shown as Figure 6(c). When a user points to a highlighted node in an alert,

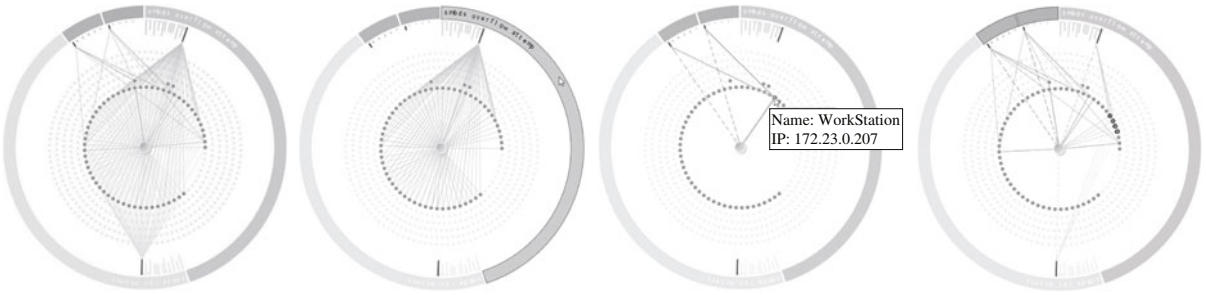

Figure 6 (a) Visualization of a network at one moment; (b) alerts filtered by the alert type; (c) alerts filtered by a host; (d) multi-selection.

the detail information about the host, such as host name and IP address, will be drawn, as shown in Figure 6(c). If you want to compare the attacks in this interval, multi-selection is provided, as shown in Figure 6(d). These pointing and clicking features allow users for a smooth, thorough analysis. An advantage of our visualization framework is its use of animation introduced in Subsection 3.2.3. In our case, animation is used to display the system transitions from one state to another, such as the distinct changes of alert types and the amount of alerts to perceive the dangerous behavior patterns.

4 Entropy function

4.1 Definition of entropy

Information Entropy is a concept proposed by Shannon in 1948. Entropy is a measure of the uncertainty of a random variable. Let X be a discrete random variable with r states $x_i,\ i = 1, \ldots, r$, and probability function $p_i = P\{X = x_i\},\ x_i \in X,\ \Sigma p_i = 1,\ 0 \leqslant p_i \leqslant 1$. The entropy $H(X)$ of a discrete random variable X is defined as:

$$H(X) = -\sum_{i=1}^{r} p_i \log p_i. \tag{1}$$

The basic property of entropy is concave which allows us to use it in monitoring network security. If network state changes from normal to abnormal status, the entropy will be changed distinctly. This phenomenon can be applied to alert types, source IP, destination IP, source port and destination port. In [21], the Relative Uncertainty (RU) is defined as the standardized entropy.

$$\mathrm{RU}(X) = \frac{H(X)}{H_{\max}(X)} = \frac{H(X)}{\log(r)}, \quad 0 \leqslant \mathrm{RU}(X) \leqslant 1. \tag{2}$$

Obviously, if a observed value is 1, and the others are 0, i.e., $p(x_i) = 1$, $p(x_j) = 0$, $j \neq i$, $j = 1, \ldots, r$, for $x_i, x_j \in X$, then $\mathrm{RU}(X) = 0$. On the other hand, if all the observed values are uniform, it means that there is the highest level of variety in the observed data, and then it holds that $\mathrm{RU}(X) = 1$. In general, $\mathrm{RU}(X) \ll 1$ indicates that the data distribution is more skewed, and $\mathrm{RU}(X) \cong 1$ means that the values of the observed data are close to being uniformly distributed. Usually, the normal network visiting is random, so the number of visiting is distributed unevenly and the entropy and RU are low. If the amount of visiting, on the contrary, is distributed evenly in continuous time intervals, the cyber risk is very likely to have been generated during these time intervals and the entropy and RU are relatively high.

4.2 Evaluation

The attack pattern and situation awareness are analyzed by entropies of alert type, source IP, destination IP and ports in a time interval in real-time monitoring. An example of evaluation of entropy of alert type to explore the attack patter is shown as follows.

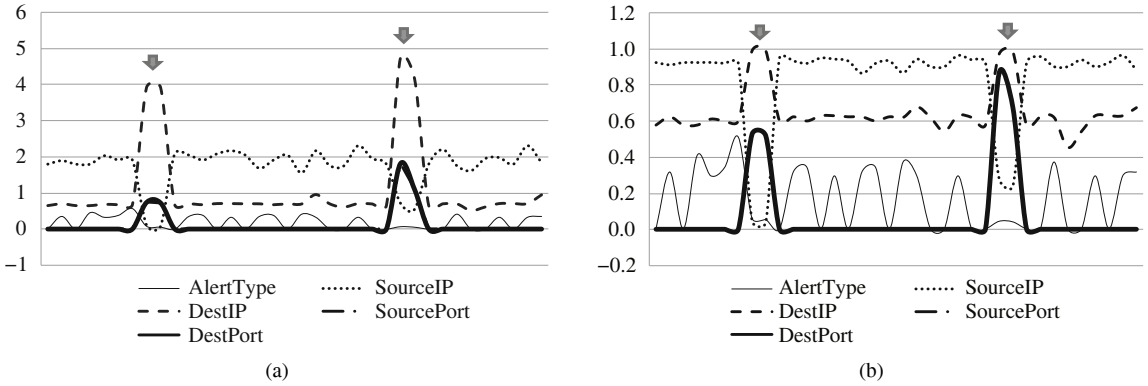

Figure 7 (a) Five categories of entropy; (b) five categories of standard entropy.

Let alert type be a discrete random variable, known as A, if four types of alert, $a_i,\ i = 1 \sim 4$, are observed in a time span $t_j,\ j = 1, \ldots, \infty$, and the amount of each alert occurred is $n_i,\ i = 1 \sim 4$, the probability $p_i,\ i = 1 \sim 4$ of each alert is calculated by equation

$$p_i = \frac{n_i}{\sum_1^4 n_i}, \quad i = 1, 2, 3, 4. \tag{3}$$

The entropy and the standardized entropy respective are

$$H(A) = -\sum_{i=1}^{4} p_i \log p_i, \quad \mathrm{RU}(A) = \frac{H(A)}{\log 4}. \tag{4}$$

The entropy of address for source IP or destination IP or source port or destination port in a time interval has the similar processing, which firstly counts the number of different types, and then counts the number for each type, and calculates the probability for each type by (3), finally the entropy and the standard entropy can be calculated by (1) and (2). All categories of the entropy to analyze the attack can also be synthesized. An example is shown in Figure 7 (a) and (b), we synthesize five categories of the entropies mentioned before and find out two risky moments marked with arrows. The attack pattern is that a few of source IPs attack a large number of destination IPs with ports in these two time span. The similar trends from the standard entropy are shown.

5 Results and analysis

The IDS alerts visualization framework, IDSRadar, is implemented by Qt and OpenGL. Generally, IDS alerts are captured by Snort which is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. At first, IDS logs are saved into MySQL database, then IDSRadar reads IDS data, such as source IPs, destination IPs and alert types, in every time interval which can be tuned by users, and calculates the statistical information of attacks, such as the amount of every kind of alerts in every time interval, or the accumulated amount of attacks in all of the time intervals. And then, IDSRadar renders the IDS alerts and the statistical information into the glyphs which we have designed. The network administrators can observe the overview of the situation of network security from the outer histogram and the detail information in the radial graph. If users find some potential risks, they can play backward to the time interval which they are interested in. Furthermore, users can zoom in, zoom out, or click the host to check source IP, destination IP and alert type. Then users can find when the attacks began, who the attackers are, and who the victims are. At last, users can decide what they should do to prevent the further attacks. In this section, IDSRadar is used to analyze mini-challenges of IEEE VAST challenge 2011 and 2012.

Mini-challenges of IEEE VAST Challenge 2011 and 2012 provided many Snort IDS logs and Firewall logs, in which unusual events and malicious attacks are occurring. Participants were asked to design

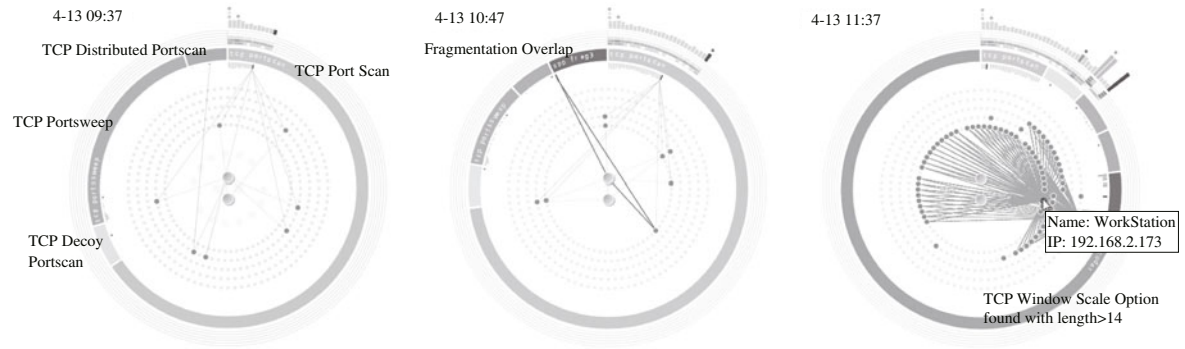

Figure 8 Visualization of three stages. (a) The snapshot at around 9:35 at the first stage; (b) Fragmentation Overlap initially appeared at the second stage, and a complete triangle is found, the host with IP 192.168.2.154 and DNS server communicate duplexing; (c) the third appearance of TCP Window Scale Option at the third stage and the source IP is 192.168.2.173.

situation awareness interfaces that would aid security analysts in identifying and preventing attacks. There are about 30 thousand IDS alerts in 3 days provided by VAST Challenge 2011, and 40 thousand IDS alerts in 3 days provided by VAST Challenge 2012. Those datasets can be dealt with in real time by using our visualization framework, and the time of all kinds of operations is 1 s or so. A detailed analysis process is as follows.

5.1 VAST Challenge 2011

In the first day of three days from VAST Challenge 2011. One of the first visible trends in the outer histogram from our radial framework is that the outer histogram in green is smooth in most situations, which represents "TCP Port Scan" with low risk. In addition, there is a large amount of "TCP Window Scale Option found with length > 14" with high risk occurred in three time intervals. Furthermore, the whole day can be classified into four noteworthy stages through analyzing the alert types, IPs and ports.

Stage1 (From around 8:40 on April 13): At the beginning, from around 8:40 to 10:40 on April 13, four kinds of port scan with low risk are observed, as shown in Figure 8(a). The sources of the port scan are always hosts, and the destinations are Internet Web Server or DNS server or both with the port 0. Although an attacker often uses different port scanning techniques and tools to determine operating system types and versions and also uses application versions to determine possible effective attack vectors that can be used against the target host, so many TCP port scans are distributed in the whole day that most of them can be considered as false positives.

Stage2 (From around 10:40 on April 13): The second stage begins at about 10:40 when Fragmentation Overlap initially appears. This alert is generated when the frag3 preprocessor has detected an anomalous network traffic which is the fragment overlapped another fragment. This is an indication of anomalous behavior between networked assets. From Figure 8(b), an overview of this moment, there is a complete triangle, since the workstation 192.168.2.154 and DNS Server communicate duplexing in the same moment which means the fragment overlaps.

Stage3 (From around 11:10 on April 13): In the third stage, there are overwhelming numbers of "TCP Window Scale Option found with length > 14" in three time intervals, at around 11:10, 11:15 and around 11:35, as shown in Figure 8(c). This event means snort decoding preprocessor have detected an anomalous network traffic, such as a worm. This behavior cannot be detected by firewall because it only happens in subnet, which reflects the fact obviously that the attacker and the victim are hosts in intranet. Furthermore, three hosts which launched a large number of attacks are 192.168.2.171, 192.168.2.172 and 192.168.2.173 respectively. They launched almost 3000 times of attacks to hundreds of hosts through port 50050 in a short time.

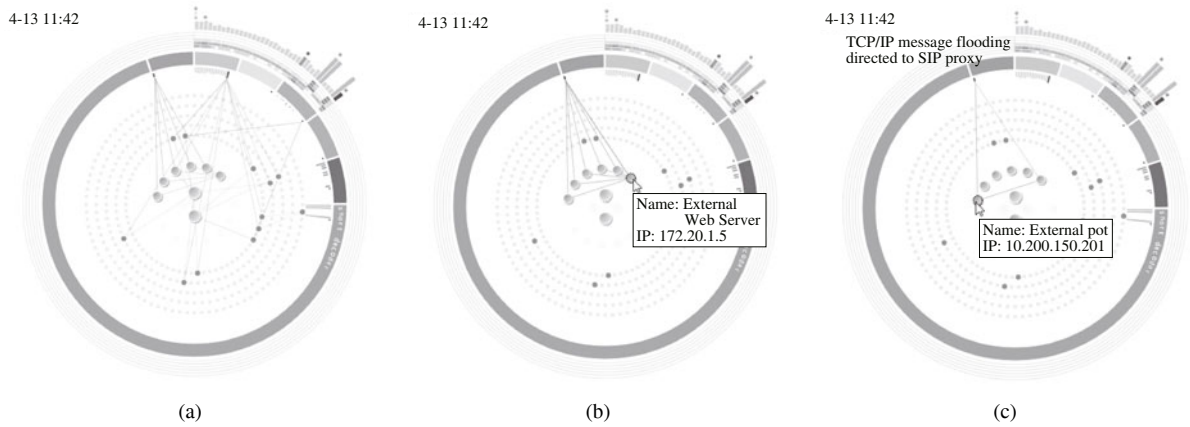

Figure 9 Visualization of the fourth stage. (a) SIP initial appearance; (b) the victim is External Web Server, 172.20.1.5; (c) one of the attackers 10.200.150.201.

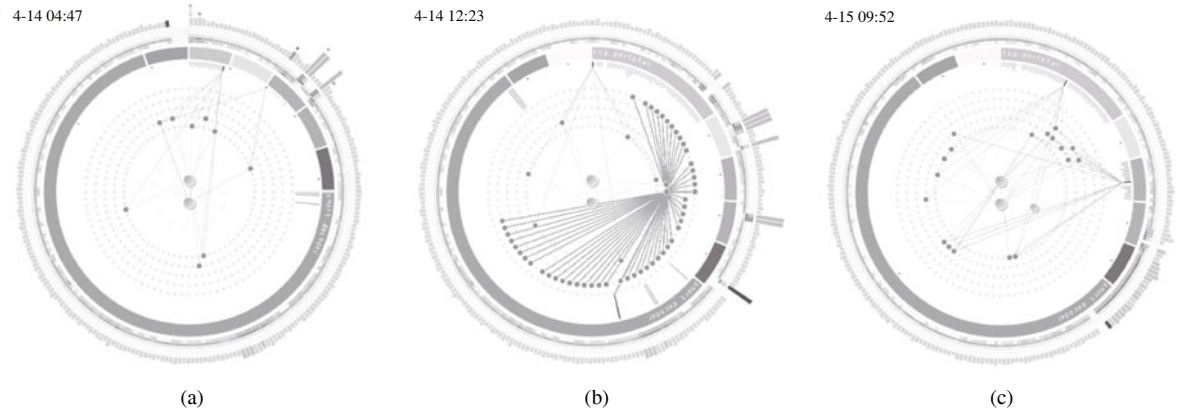

Figure 10 Overview of IDS alerts provided by VAST Challenge 2011. (a) Overview of the first day; (b) one of the "TCP Window Scale Option" attacking behaviors in the second day; (c) overview of April 15.

Stage4 (From around 11:40 on April 13): In the fourth stage, we observe SIP Proxy which is a classic Denial of Service attack on the corporation web server to disrupt communications, as shown in Figure 9. The victim is External Web Server 172.20.1.5 and the five attackers are external websites, 10.200.150.201, 10.200.150.206–10.200.150.209.

All day long, the entropy of this network shows the following characteristics: usually the entropy of alert type is not large, and the entropy of source IP is larger than that of destination IP, but the entropy of source port and destination port are pretty small. The reason is that, in most situations, there exists a small quantity of green attacks that are "TCP Port Scan" and this alert is usually launched by hosts without port information. At those three particular moments, the entropies of destination IP, source port and destination port increase suddenly, which represents that a few hosts attack numerous destination hosts through the same port in a short time.

The attacking behaviors in the second day and the third day had the similar patterns with the first day, as shown in Figure 10 (b) and (c). Computers continue port scanning in their own subnet. Hosts at 192.168.2.174 and 192.168.2.175 are involved in "TCP Window Scale Option" attack in the second day. This also indicates a problem within the network, such as a worm.

5.2 VAST Challenge 2012

The second example is from VAST challenge 2012. IDS Logs in two days are provided. Figure 11 (a) and (b) are the overviews of IDS alerts in the first day and the second day respectively. The outer histogram in the first day shows the irregular patterns, and that of the second day looks like more periodical. So the first day can be classified into four stages through analyzing the alert types and the frequency of the

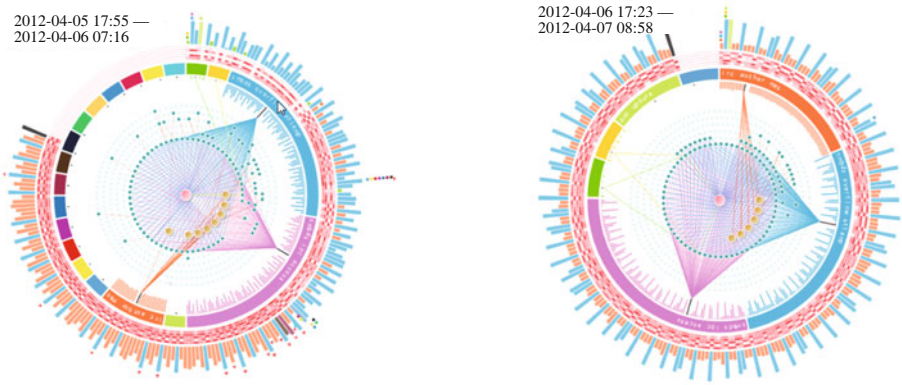

Figure 11 (a) Overview of the first day of IDS Logs provided by VAST Challenge 2012; (b) overview of the second day of IDS Logs.

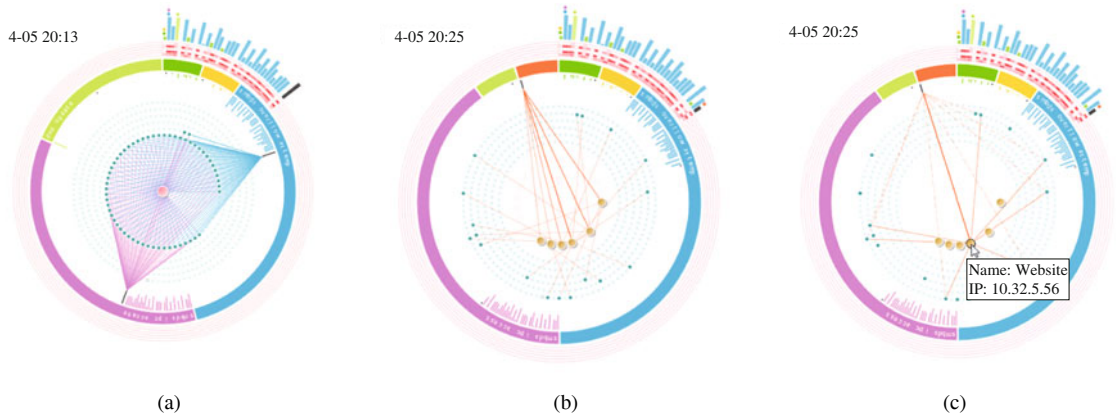

Figure 12 Visualization of the first and the second stages. (a) The snapshot of the first five types of alert all appeared at the first stage; (b) IRC initial appearance at the second stage and the attackers are websites in Internet and the victims are workstation in intranet; (c) the detail of IRC attacking.

attacking behaviors.

Stage1 (From 17:55 on April 5): At the beginning, there are five alert types with low risk observed. Especially, two alert types, "DS IPC Unicode share access" in pink and "DC Session Setup NTMLSSP Unicode asn1 overflow" in blue have the same behavior patterns, for example they both appear in every time interval, and the sources are the same hosts in intranet, and the destinations, DNS Server, are also the same, as shown in Figure 12(a), so most of them can be considered as false positives. The network is safe in the first stage.

Stage2 (From 20:25 on April 5): The second stage begins at 20:25 when "IRC authorization message" initially appears, as shown in Figure 12 (b) and (c). The sources of IRC are websites in Internet and destinations are workstations in intranet. IRC is a classic Botnet attacking. The attacker in Internet is called as Botnet Command and Control Servers (C&C servers), and the destination, the infected workstation, becomes a Botnet Client which sends the message that what type of computer it has infected to C&C servers. The C&C servers will command those Botnet clients to do something dangerous to the network, such as exfiltrating sensitive data by FTP and SSH or infecting more workstations to be Botnet clients. The C&C servers will communicate with Botnet clients frequently, so we can see the IRC attacks have lasted to the end of the second day since it initially appeared.

Stage 3 (From 21:40 on April 5): Around 21:40 on April 5 when seven colored dots are drawn on the bar of outer histogram, as shown in Figure 13, some database visiting alerts are observed, including "ET POLICY Suspicious inbound to MSSQL port 1433", "ET POLICY Suspicious inbound to Oracle SQL port 1521", "ET POLICY Suspicious inbound to mySQL port 3306" and "ET POLICY Suspicious inbound to PostgreSQL port 5432". Furthermore, we find the attacker is 172.23.240.156, and the destination is

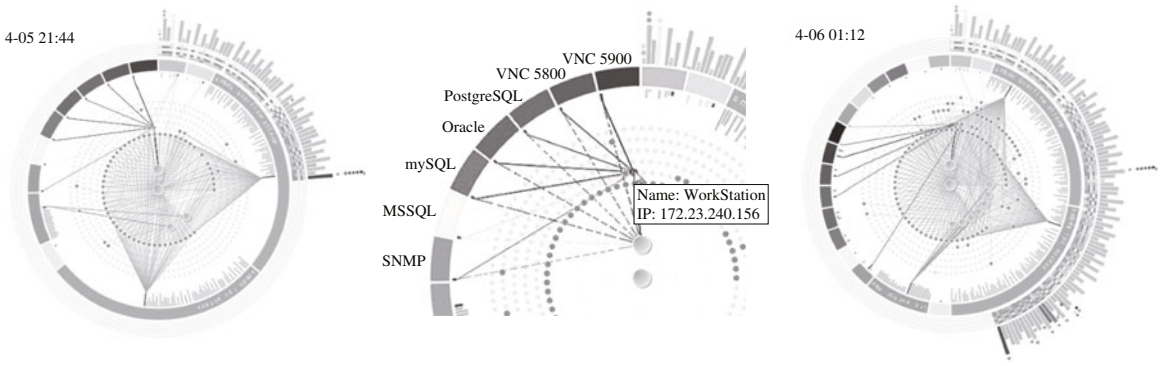

Figure 13 Visualization of the third and the fourth stages. (a) The snapshot when several database visiting behaviors at the third stage; (b) the detail of the database attacking behaviors. The attacker is workstation, 172.23.240.156, and the victim is firewall server; (c) the snapshot of IDS alerts at around 01:12 April 6 at the fourth stage. The amount of IRC is increasing gradually, so IRC appears in outer histogram regularly.

the firewall server, 172.23.0.1. At the same time, the attacker also launches "ET SCAN Potential VNC Scan 5800-5820", "ET SCAN Potential VNC Scan 5900-5920" and "GPL SNMP request TCP" to firewall server. Workstation, 172.23.240.156, has been infected to be a Botnet client and tried to visit sensitive data in the database.

Stage 4 (From 0:00 on April 6): A few high risky alerts, "ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection", "ET SCAN Potential SSH Scan OUTBOUND", "ET SCAN Potential SSH Scan", are observed, as shown in Figure 13(c). The Botnet clients attempt to leak data to Internet by SSH. The attackers in this time interval are 172.23.236.8, 172.23.231.69 and 172.23.234.58. The entropy of the alert type of this time interval is relatively high and unstable, so the triangles are marked on the bars of outer histogram. After that the amount of IRC increases gradually, the color of IRC appears in outer histogram regularly, which means the Botnet virus makes the network status worse.

Figure 11(b) shows the attacks from 18:50 on April 6 to 8:00 on April 7. There is periodicity for the sum of alerts and types of alert from the outer histogram. The three of most alert types are "GPL NETBIOS SMB IPC Unicode share access", "GPL NETBIOS SMB Session Setup NTMLSSP Unicode asn1 overflow attempt" and "ET POLICY IRC authorization message". The sources of the first two alerts are workstations in 172.23.0.X and 172.23.1.X, and the destination is DNS server. Both alert types are in low risk. The IRC alert shows that the external websites (C&C servers) in Internet constantly attack workstations in intranet. From analyzing the periodical behavior, almost 15 percent workstations have been infected by Botnet, so we can predict that the future situation of the network will be almost out of control.

6 Conclusion and future work

In this paper a network security visualization framework, IDSRadar, is proposed to assist in understanding IDS alerts and identifying the real abnormal pattern behavior in overwhelming false positives. Five catalogues of Entropy functions have been described how to analyze the attack pattern and recognize the false positives. We have evaluated the visualization framework 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, the scalability of the topology map will be enhanced especially when there are too many IPs 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 servers and workstations. And further pattern analysis on individual host computer and individual risk will be performed.

Acknowledgements

This work was supported by National Natural Science Foundation of China (Grant No. 61103108), Hunan Provincial Science and Technology Program (Grant Nos. 2012GK3166, 2012RS4049), Hunan Provincial Natural Science Foundation of China (Grant No. 12JJ3062), and Postdoc Research Funding in Central South University. The authors wish to thank the anonymous reviewers for their comments. The authors would also like to thank the data providers, IEEE VAST Challenge.

References

1 Marty R. Applied Security Visualization. Indiana: Addison Wesley Professional Indianapolis, 2008
2 Shin M S, Kim E H, Ryu K H. False alarm classification model for network-based intrusion detection system. Lect Note Comput Sci, 2004, 3177: 259–265
3 Lakkaraju K, Bearavolu R, Slagell A, et al. Closing-the-loop in NVisionIP: integrating discovery and search in security visualizations. In: IEEE Workshop on Visualization for Computer Security, Minneapolis, 2005. 75–82
4 Abdullah K, Lee C, Conti G, et al. IDS RainStorm: visualizing IDS alarms. In: IEEE Workshop on Visualization for Computer Security, Minneapolis, 2005. 1–10
5 Koike H, Ohno K. SnortView: visualization system of snort logs. In: The ACM workshop on Visualization and data mining for computer security, Washington, 2004. 143–147
6 Yin X, Yurcik W, Treaster M, et al. VisFlowConnect: netflow visualizations of link relationships for security situational awareness. In: the ACM workshop on Visualization and data mining for computer security, Washington, 2004. 26–34
7 Livnat Y, Agutter J, Moon S, et al. A visualization paradigm for network intrusion detection. In: the 6th Annual IEEE SMC Information Assurance Workshop, West Point, 2005. 92–99
8 Draper G M, Livnat Y, Riesenfeld R F. A survey of radial methods for information visualization. IEEE Trans Vis Comput Graph, 2009, 15: 759–776
9 Mansmann F, Gobel T, Cheswick W. Visual analysis of complex firewall configurations. In: Proceedings of the VizSec Symposium on Visualization for Cyber Security, Seattle, 2012. 1–8
10 Alsallakh B, Aigner W, Miksch S, et al. Reinventing the contingency wheel: scalable visual analytics of large categorical data. IEEE Trans Vis Comput Graph, 2012, 18: 2849–2858
11 Nyarko K, Capers T, Scott C, et al. Network intrusion visualization with niva, an intrusion detection visual analyzer with haptic integration. In: Haptic Interfaces for Virtual Environment and Teleoperator Systems, Orlando, 2002. 277–284
12 Ren P, Gao Y, Li Z, et al. IDGraphs: intrusion detection and analysis using histographs. In: IEEE Workshop on Visualization for Computer Security, Minneapolis, 2005. 39–46
13 Koike H, Ohno K, Koizumi K. Visualizing cyber attacks using IP matrix. In: IEEE Workshop on Visualization for Computer Security, Minneapolis, 2005. 91–98
14 Lee C P, Trost J, Gibbs N, et al. Visual firewall: real-time network security monitor. In: IEEE Workshop on Visualization for Computer Security, Minneapolis, 2005. 129–136
15 Livnat Y, Agutter J, Moon S, et al. Visual correlation for situational awareness. In: IEEE Symposium on Information Visualization, Minneapolis, 2005. 95–102
16 Foresti S, Agutter J, Livnat Y, et al. Visual correlation of network alerts. IEEE Trans Vis Comput Graph, 2006, 26: 48–59
17 Bertini E, Hertzog P, Lalanne D. Spiralview: towards security policies assessment through visual correlation of network resources with evolution of alarms. In: IEEE Symposium on Visual Analytics Science and Technology, Sacramento, 2007. 139–146
18 Musa S, Parish D J. Using time series 3D alert graph and false alert classification to analyze Snort alerts. In: the 5th International Workshop on Visualization for Computer Security, Cambridge, 2008. 169–180
19 Shiravi H, Shiravi A, Ghorbani A A. IDS alert visualization and monitoring through heuristic host selection. Lect Note Comput Sci, 2010, 6476: 445–458
20 Shiravi H, Shiravi A, Ghorbani A A. A survey of visualization systems for network security. IEEE Trans Vis Comput Graph, 2012, 18: 1313–1329
21 Xu K, Zhang Z L, Bhattacharyya S. Internet traffic behavior profiling for network security monitoring. IEEE/ACM Trans Netw, 2008, 16: 1241–1252