http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (7): 1335-1340, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.1335.1340

A Study of a New Visualization IDS from Macro and Micro View

[1,2]Zhang Sheng, [1]Shi Ronghua and [1]Zhou Fangfang
[1]School of Information Science and Engineering, Central South University, Changsha 410083, China
[2]Modern Educational Technology Center, Hunan University of Commerce, Changsha 410205, China

Abstract: With more and more volume, velocity and variety (3Vs) of data generated from modern day networks, Visualization methods are used to quickly and effectively identify network attacks and abnormal events. Considering the characteristics and defeats of current working visualization systems, A new type of intrusion detection system, IDS Viewer, a system based on the radial panel visualization technology, has been introduced and developed. With a main focus on improvement of user experience, decrease of image occlusion and situation awareness, analysts can utilize fast recognition ability of human abstract thinking, in order to assess the network security situation from macro view and find the pattern of attack from micro view, which can tackle the weakness of the traditional intrusion detection systems.

Key words: Visualization IDS, radial panel, user experience, occlusion, situation awareness

INTRODUCTION

According to the Symantec report (Symantec, 2012), Symantec has blocked a total of over 5.5 billion malware attacks in 2011, there is an 81% increase over 2010. In China, the network security environment is deteriorating and it urgently needs new safety tools and technology to restrain and reduce network information security threats.

Intrusion Detection System (IDS) monitors network traffic and suspicious activity. In addition, it alerts the system or network administrator for security concerns. Traditional IDS has the following challenges: such as (1) Cognitive burden is heavy, (2) Lack of user interaction, (3) Lack of holistic network understanding, (4) Poor response on attacks, (5) Lack of ability of proactive defense and prediction , etc. With more and more volume, velocity and variety of intrusion attacks, Tradition IDS is facing more severe challenges.

Network security visualization is a new research field of information visualization (Becker *et al*., 1995; Fortier and Shombert, 2000). Using the model and structure of the human visual acquisition capacity, it can present abstract network data as the graphic image and help analysts to analyze network situation, identify network unusual activities and forecast network security event trends.

This study developed a novel radial panel system and used visualization methods to analyze and research intrusion alarm. The visualization system tries to diagnose the network security from the macro and micro view. The main aims of this study are on improvement of user experience, decrease of image occlusion and enhancement of situation awareness.

RELATED RESEARCH

Snort view (Koike and Ohno, 2004): Using scatter plots and symbols, it was suitable for small networks, which was designed to help administrators in judging false detection, detecting the implicit attack and attack sequence.

IP Matrix (Koike *et al.*, 2005): Using scatter plots and color maps, it was used to detect the spread of the virus welhia and sasser.d.

IDS Rainstorm (Abdullah *et al.*, 2005): using the scatter plot, it was used to discover unusual network events, worm propagation and botnets.

Vizalert (Livnat *et al.*, 2005): Using radial panel, it was designed to improve users' ability to identify critical network anomalies more quickly in order to reduce the impact and severity of network attacks.

Avisa (Shiravi *et al.*, 2010): Using radial panel and heuristic functions, it was designed to assist in comprehending IDS alerts and detecting abnormal pattern activities within a network.

These visualization systems have made remarkable achievements for different applications. However, overall speaking, the visualization system needs to be strengthened in the following aspects (Shiravi *et al.*, 2012): Reduce image occlusion (such as Snort View and

Corresponding Author: Zhang Sheng, School of Information Science and Engineering, Central South University, Changsha 410083, China

IP Matric), improve scalability (such as Snort View, IDS Rainstorm and Avisa), enhance the user experience (such as Vizalert), increase situation awareness and protect privacy, etc.

USER INTERFACE OF VISUALIZATION IDS FRAMEWORK

The quality of user Visual interface directly affects the user experience. Visual design involves the screen layout, color and information message arrangement, etc.

A Visualization IDS named IDS Viewer is designed by using popular radial panel as the interface graphics choice, as shown in Fig. 1:

- The system is made up by two main parts: the radial panel and internal curves. Radial panel has two arcs, the left side arc is used to display network alarm classification and alarm and the right side arc, the larger area, is used to display subnet (or custom packet) and host. The width of the arc shows the number of triggered alarm, the greater radian is, the more number of attack alarms
- Internal curve is used to display alarm details, one end of the curve points to alert, the other end points to the associated host. The thickness of internal curve indicates the number of the alarm, the thicker is, the more number of attack alarms
- The right three radial charts are supplementary to the main view, which, respectively, show the source IP, source Port and the type of alert information of the attack on the local host port
- All user interaction messages will not be displayed directly on the radiation graphic. When the user mouse clicks on the arc on the circle, alter message will appear on the left side message edit box

MACRO VIEW

IDS Viewer is used to monitor the entire campus network security situation. First, through the deployment of the security monitoring mechanism to capture the massive invasion and attacks in two days of the test, numerous invasions (520,000+records), which are grouped into 13 major categories and 62 subcategories, had been captured. Secondly, IDS Viewer was used to assess network security situation from a macro view.

Inner curve design: In order to obtain an appealing appearance of the graphics to users and minimize drawing complexity, the inner arc uses Bezier curve, defined as follows:

$$p(t) = \sum_{k=0}^{n} P_k BEN_{k,n}(t)\ t \in [0,1]$$
$$BEN_{k,n}(t) = C_n^k t^k (1-t)^{n-k}\ k = 0,1...,n \quad (1)$$

where, IDS Viewer uses Cubic Bezier curve (k = 3), when the period of time is shorter and the alerts are in a small number, the graph can display a clear and beautiful composition. In addition, it is easy to distinguish, as shown in Fig. 2a:

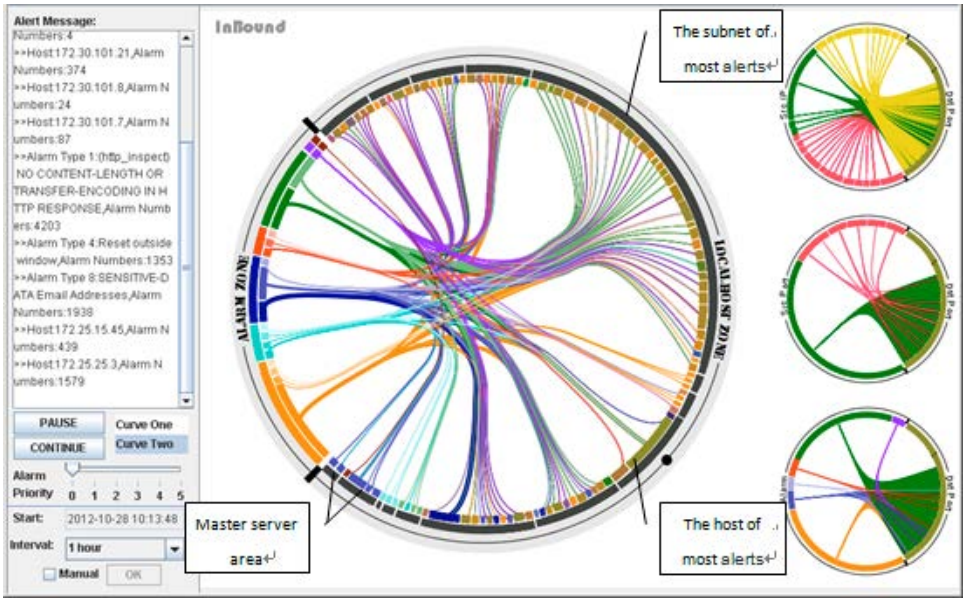

Fig. 1: IDS viewer interface and security situation assessment

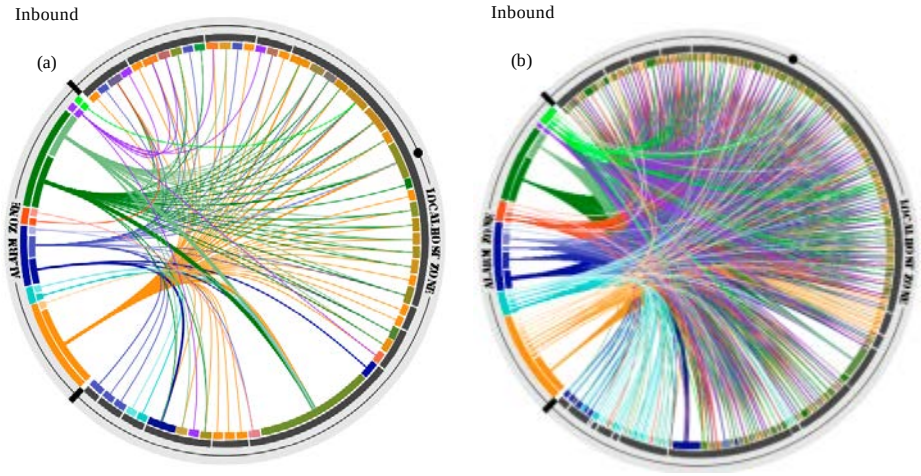

Fig. 2(a-b): Cubic Bezier curve with different lengths of time (a) 5 min (b) 12 h

But if observation time increases, such as 12 h, cubic curve will be occlusive because the curves are too many and overlap each other, as shown in Fig. 2b.

Reduce image occlusion

Method of improved curve: the same alarm source aggregates on the left side of the ring, the same host aggregates on the right side of the ring; the curve adopts the multi-segment fitting cubic Bezier curve, as shown in Fig. 3.

The key point of curve drawing lies in the choice of the control points, if the midpoint of the current host (alarm) angle is β, the midpoint of current subnet (alarm) angle is α, the circle radius is r, the alarm zone (host area) aggregation height is h and the aggregation width is d, the circle center coordinates is (0, 0) (which can be obtained through the two-dimensional coordinate change), then:

$$
\begin{aligned}
&P_0.x = r * \cos(\beta) P_0.y = r * \sin(\beta)\\
&P_1.x = r * \cos(\beta-\alpha) * \cos(\alpha) P_1.y = r * \cos(\beta-\alpha) * \sin(\alpha)\\
&\theta = \arctan\frac{r\sin(\beta-\alpha)}{r\cos(\beta-\alpha)-h} \lambda = \arctan\frac{d\sin\theta}{h+d\cos\theta}\\
&P_2.x = (\frac{d\sin\theta}{\sin\lambda}+h)\cos(\alpha+\lambda) P_2.y = (\frac{d\sin\theta}{\sin\lambda}+h)\sin(\alpha+\lambda)\\
&P_3.x = \frac{d\sin\theta}{\sin\lambda}\cos(\alpha+\lambda)\ P_3.y = \frac{d\sin\theta}{\sin\lambda}\sin(\alpha+\lambda)
\end{aligned}
\qquad (2)
$$

where, if the preceding control points of the two adjacent curves are P0-P3 and the following control point are P'0-P'3, then P3 and P'0 will be the same point. In order to make two segments of curve smoothly continuous, P2, P3 (P'0) and P'1 have to be on a straight line.

Although multi-segment fitting cubic Bezier curve has been used to reduce image occlusion, the image is still crowed for the period of time more than 1 day. The solution is data preprocessing, articles (Abdullah *et al*., 2005; Livnat *et al*., 2005; Shiravi *et al*., 2010), respectively, use heuristic algorithm, principal analysis algorithms and information entropy algorithm. The system adapts to the host alarm priority weighted algorithm. This algorithm takes source (destination) address and port, protocol, time stamp, data packets, number of attacks, harm extent of attacks and many other factors into account:

- W_{S_IP} and W_{D_IP} represent the weight factor of source IP address and destination IP address. if a certain range of hosts is under the focus, the weight of the area can be increased
- W_{S_port} and W_{D_port} represent the weight factor of the source and destination ports, ports are the logical interfaces which connect the computer to the external network. Focusing on different ports generally can be used to distinguish different types of attacks
- W_{Length} represents the weight factor of the data packet length. In certain network, attacks are disguised behind too long or short data packets
- W_{Alarm} represents harm extent weight factor which can be obtained from the traditional IDS system
- Abs represents the absolute number of attacks received by some hosts in the certain period
- ∑Abs represents the number of attacks received by all host of the period

Rel represents the number of attacks suffered by some host current relative to previous changed; ∑Rel represents all number of attacks current relative to previous changed, then:

$$
\begin{aligned}
Host_{priority} = &\sum(W_{S\_IP} + W_{D\_IP} + W_{S\_port} + W_{D\_port}) + \sum W_{Length}\\
&+\sum W_{Alarm} + Abs/\sum Abs + Rel/\sum Rel
\end{aligned}
\qquad (3)
$$

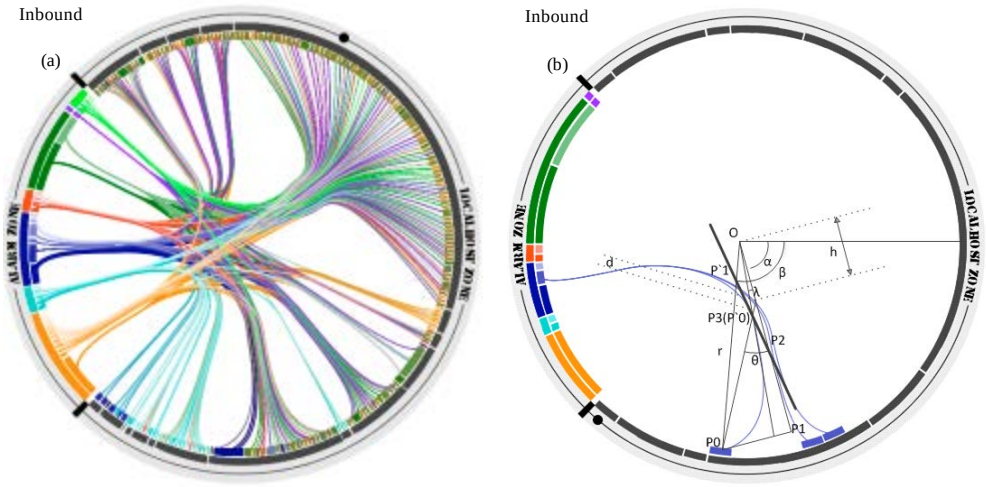

Fig. 3(a-b): (a) Multi-segment fitting cubic Bezier curve (b) Graphics rendering method

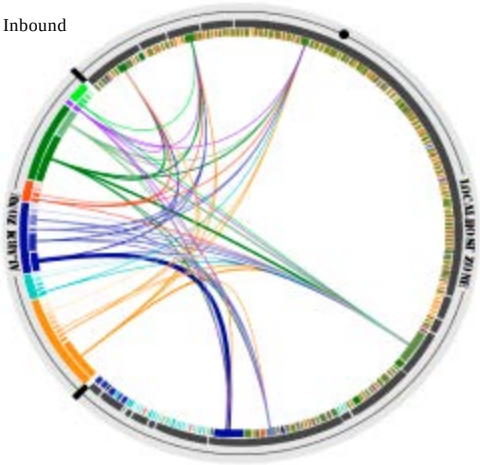

Fig. 4: Host alarm priority weighted graph

According to the formula 6, different security observation strategy can be designed to meet the needs of different observation angles. Figure 4 shows a processed graph which was improved weight factor of absolute number of attacks.

A case study of security situation analysis: Network security situation is to analyze the correlation among security data information, which has been massively obtained from network and construct these information in order to gain a macro view of network security situation. In a longer observation period of time (1 h), as shown in Fig. 1, the graph clearly indicates the most alarms subnet was 172.25.15.0 which serves for the library reading room. As a result of the Open University management, the library users have different backgrounds. This brings larger volume of attacks and alerts during that time period. The color of host is between brown and green, the alarms were mostly brown alert 1(No Content-Length or Transfer-encoding in Http Response) and green alert 8 (Sensitive-data E-mail Addresses). The most attacked host was 172.25.25.3, which is proxy Internet server for the classroom building. , The amount of attacks was 1584 and the majority of alarms associate with the type of alert 1 and 8. While the main server area of the school received less attacks, the main type of attacks concentrated on the blue-green alert 2 (PSNG_UDP_DECOY_ PORTSCAN) and dark blue alert 4 (Reset outside window). There was no indication of invasion success. The network security situation of this campus was stable and secure. The main server area is in a better situation, while the subordinate subnets, due to the lack of the necessary management or security measures, did not performance well. Improvement actions should be taken in place.

MICRO VIEW

In Macro View, the attention is on 3Ws, namely, the When, Where and What attributes. When refers to the point in time when the alert happened. Where refers to the local network and IP address. What refers to the type of the alert. These 3Ws help to capture the trend of the overall safety of the campus, but in order to get details of a specific invasion, it is not enough. Therefore, 3 supplementary views for IDS Viewer are introduced: Source IP vs. Destination Port, Source Port vs. Destination Port and Alarm types vs. Destination Port.

Port mapping algorithm: Viruses, Trojan attacks are diverse and the ports are key positions of all kinds of

invasion and attacks. Through statistical analysis, it was found that the attacks are mainly concentrated in two parts: the traditional ports (0 to 1024), such as port 80 (World Wide Web), port 21 (FTP service), port 25 (E-mail SMTP service), port 110 (E-mail POP3 service), these services have been used for many years; the second part is high ports (1024 and above), such as port 1433 (SQL Server), port 3389 (remote control), some popular virus backdoor ports, such as TCP 2745, 2946, 3127, 4168, 5554, 6129 , At the same time, it shows that in a continuous period of time, high port attacks are more concentrated and continuous. Therefore, in the supplementary view of local host port, different processing algorithms are used on the calculation of low port and high port angle.

Since the low ports range is relatively narrow and mainly for traditional services, the probability distribution of attacks complies with even distribution, which can treat equally on every port. The high ports range is wider, but the attack ports in a continuous time of period concentrate on a small area, which complies with the normal distribution. Based on the assumption that the high (low) port of start angle is ω, high (low) port of end angle is τ, port is the port number of attack, portH and portL are the maximum value and the minimum value of the fixed time period, P(x) is probability density for the attack, the attack's angle of the destination host port F(port) will be:

$$\begin{aligned}
&P(x)=\frac{1}{b-a}\quad port<1024\\
&b=1024\ a=0\\
&F(port)=\omega+(\tau-\omega)*P(x)*port\\
&P(x)=\frac{1}{\sqrt{2\pi}\sigma}e^{\frac{-(x-\mu)^2}{2\sigma^2}}\quad port\geq 1024\\
&\mu=(port_H+port_L)/2\ \sigma=(port_H-port_L)/2\\
&F(port)=\omega+(\tau-\omega)*\sum_{x=1024}^{port}P(x)
\end{aligned}\tag{4}$$

A case study of micro view: Different from the macro view, in order to have a deep observation on invasion details, It is necessary to reduce the period of observation time

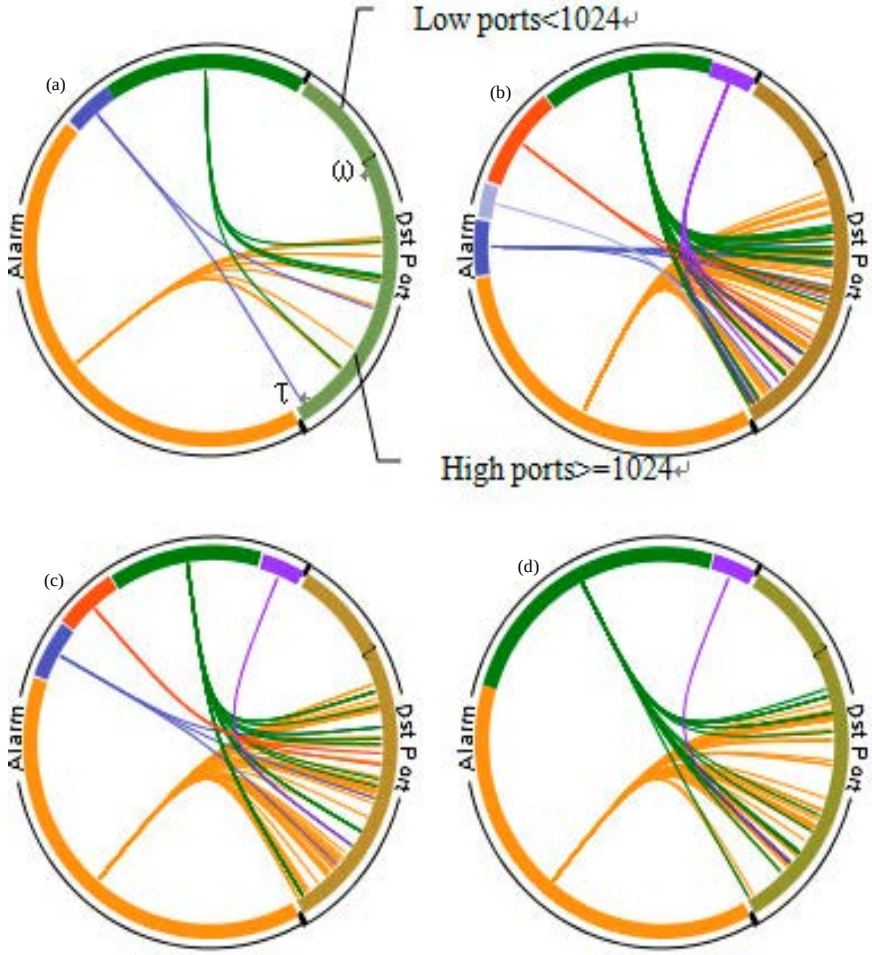

Fig. 5(a-d): Invasion Detail in the Micro view with different time spans (a) 10:40-10:50 (b) 10:50-11:00 (c) 11:00-11:10 (d) 11:10-11:20

(such as 10 min), as shown in Fig. 5a-d, which used four periods of time to analyze. It can be seen from 4 charts that the common attack sequence was alarm 1 (orange), alarm 4 (blue) and alarm 8 (green). And in the two periods of middle time, there was additional red attack 11 (Data sent on stream not accepting data), light blue 12 (Bad segment, adjusted size < = 0) and purple 14 (FILE-IDENTIFY Portable Executable binary file magic detected), that shows the intruder tried to attack the host through implanting executable binary code.

CONCLUSION

The first advantage of this system is situation awareness capability. The sheer volume of data generated from modern day networks and the high complexity of relations between data elements have proven traditional technologies as inefficient and inadequate for rising security situation awareness on a human analyst. this system applies real-time method and radial panel visualization technique to reduce user's cognitive load and increase situation awareness.

The second advantage of this system is reduction of image occlusion. The sheer amount of data in network security not only causes cognitive burden issues but also leads to the phenomenon of occlusion and overcrowding of displays. Interactions such as zooming, distorting, or filtering through dynamic queries on these calculated structural properties can lead to much deeper insight into the underlying patterns of the dataset. This system uses multi-segment fitting cubic Bezier curve and data preprocessing to reduce image occlusion.

The last advantage of this system is improvement of user experience. Security visualization systems should be designed around the explicit needs of security analysts and their requirements must be taken into account every step of the way. In order to improve user experience, this system use lots of algorithms, such as color mixing algorithm, multi-segment Bezier curve fitting algorithm and port mapping algorithms, etc to support.

REFERENCES

Abdullah, K., C.P. Lee, G. Conti, J.A. Copeland and J. Stasko, 2005. Ids rain Storm: Visualizing IDS alarms. Proceedings of the Workshop on Visualization for Computer Security, October 26, 2005, Minneapolis MN., USA., pp: 1-10.

Becker, R.A., S.G. Eick and A.R. Wilks, 1995. Visualizing network data. IEEE Trans. Visualization Comput. Graphics, 1: 16-28.

Fortier, S.C. and L. Shombert, 2000. Network profiling and data visualization. Proceedings of the IEEE Workshop on Information Assurance and Security, January 1, 2000, USA., pp: 166-169.

Koike, H. and K. Ohno, 2004. SnortView: Visualization system of snort logs. Proceedings of the ACM Workshop on Visualization and Data Mining for Computer Security, October 29, 2004, Washington, DC., USA., pp: 143-147.

Koike, H., K. Ohno and K. Koizumi, 2005. Visualizing cyber attacks using IP matrix. Proceedings of the IEEE Workshop on Visualization for Computer Security, October 26, 2005, Minneapolis MN., USA., pp: 91-98.

Livnat, Y., J. Agutter, S. Moon, R.F. Erbacher and S. Foresti, 2005. A visualization paradigm for network intrusion detection. Proceedings of the 6th Annual IEEE SMC Information Assurance Workshop, June 15-17, 2005, West Point, NY., pp: 92-99.

Shiravi, H., A. Shirav and A.A. Ghorbani, 2010. Ids alert visualization and monitoring through heuristic host selection. Proceedings of the 12th International Conference on Information and Communications Security, December 15-17, 2010, Barcelona, Spain, pp: 445-458.

Shiravi, H., A. Shiravi and A.A. Ghorbani, 2012. A survey of visualization systems for network security. IEEE Trans. Visualization Comput. Graphics, 18: 1313-1329.

Symantec, 2012. Internet security threat report. Volume 17, Symantec Corporation, Cupertino, CA., USA