2010 Second International Conference on Computational Intelligence, Communication Systems and Networks

Expert-Aware Approach: A New Approach To Improve Network Security Visualization Tool

Doris Hooi-Ten Wong, Kok-Soon Chai, Sureswaran Ramadass, Nicolas Vavasseur
National Advanced IPv6 Centre (NAv6)
Universiti Sains Malaysia
11800 Penang, MALAYSIA
Email: {doris, kschai, sures, nicholas}@nav6.org

Abstract— **Nowadays, many computers have been infected with the computer anomalies or viruses. The availability of network security visualization tools greatly facilitate to detect, perceive and defend computer users from being affected by these anomalies. Many of the network security visualization tools are designed particularly for users with advanced network security awareness even though the tools are indispensable by various types of computer users. We proposed an expert-aware approach to designing a system which formulated with a large amount of network data or high-dimensional data and adaptive for different types of users. In the preliminary phase, we proposed and implemented initial pre-expertise classification system which provides a default setting for the expert-aware network security visualization tool. The tool will learn from continual user feedbacks in order to statistically satisfy the needs of majority tool users. The expert-aware approach looks at the users' expertise level in network security and adapts the visualization views that are best suitable for the user. Initial results of the implementation of the system show that it is capable of representing several of network security data not only on two-dimensional space on a computer but also beyond that space. Systems features, such as system effectiveness and efficiency of data visualization have been improved. Our experiments in a network lab suggest that the tool can be further improved as the tool for distribution to a wide range of computer user.**

Keywords-network security visualization tool, network security awareness, expert-aware approach, high-dimensional data, two-dimensional, effectiveness, efficiency.

I. INTRODUCTION

The evolution of hardware technology resulted in ton of data being captured and stored. Large volume of network security data is being requested by large amount of computer users. The network security data are represented to computer users by using different kinds of existing network security tools. Nowadays, many computers have been infected with the computer anomalies or viruses. The availability of network security visualization tools greatly facilitated to detect, perceive and defend computer users from being affected by these anomalies. This definitely entailed enormous network security tools to completely represent network security data to the computer users. However, many of the network security visualization tools are designed particularly for users with advanced network security awareness, although the tools are indispensable by various types of computer users. There are numbers of network security tools that perform network security data in their respective way such as, bar graph, pie chart and others data visualization techniques. The network security data are easily represented to users by using a bar chart or pie chart if they are a small amount, but very difficult to understand when the data structures become large [1]. An intelligence approach shall come into the priority in order to enhance the network security data visualization. An intelligence expert-aware approach works by representing the network security data in a more comprehensive way, effectively combining requirements from different types of experts on the network data.

In Section II of this paper, we presented related network security tools and problems. In Section III, we discussed the development of the expert-aware approach method. Finally, we discussed the expected results of the proposed method and discussions will be made in Section IV. Our future work will be discussed in Section V and following by a conclusion of the paper in Section VI.

II. RELATED NETWORK SECURITY TOOLS AND PROBLEMS

There are number of tools in the visualization area that have applied on the network data visualization. Commonly, network security data monitoring is the part that most of the visualization applications have focused on more compared with others. Information on malicious attacks that have been triggered on an abnormal detection device will be presented to the network administrator [2]. There are some other areas that visualization tools have focused on such as network intrusion detection. In this section, we discussed apparently five existing network security visualization tools such as, VISUAL, SCPD, PortVis, NVisionIP and VIAssist.

A. VISUAL

In order to rapidly aware with the security conditions of their network, Visual Information Security Utility for Administration Live (VISUAL) is a network security visualization tool that allows network administrators to examine the communication networks between internal and external hosts [3]. VISUAL applied the concept of dividing network space into a local and network address space and a remote network address space. In order to produce its data visualizations, data will be taken from the log files of Tcpdump or Wireshark. Previously, Wireshark was known as Ethereal [4][5] until Summer 2006 due to trademark disagreement. It is an open source tool which contributed to Unix and Windows, especially for network protocol analyser purpose.

The advantage of VISUAL is to provide a quick overview of the current and recent communication patterns among the

978-0-7695-4158-7/10 $26.00 © 2010 IEEE
DOI 10.1109/CICSyN.2010.64

monitored network. Administrators can specify their network and remote IP by using home and remote IP filter as shown in Figure 1. Based on the information provided by IP filter, administrators can identify any single external hosts that are connected with the number of internal hosts from a grid, which may be relevant to be used in their network. The grid represents home hosts; based on connection lines it allows the network administrator to check the total traffic that exchanged between home host and external host [3].

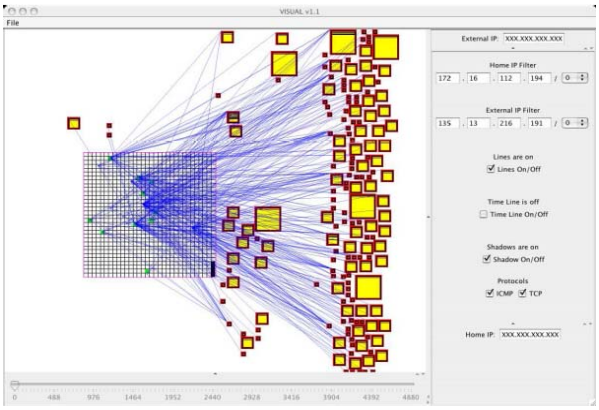

Figure 1. VISUAL is a tool that allows user to check communication network between internal and external hosts.

B. *Spinning Cube of Potential Doom*

One of the network security visualization tools that purposely designed for potential network professional, yet for beginner is Spinning Cube of Potential Doom (SCPD) [6]. It presented complicated security result for network professional and presented simple information on the network security frequency and threats extent to beginner. Figure 2 has shown the example of SCPD.

SCPD managed to provide a complete map of internet address space indicating the frequency and origin of scanning activity. User can be easily visualizing the sensor data from a large network. Rainbow color map has been applied in the cube colors dots of incomplete connections [6]. Vertical lines represented port scans on a single host while horizontal lines represented others scan across hosts..

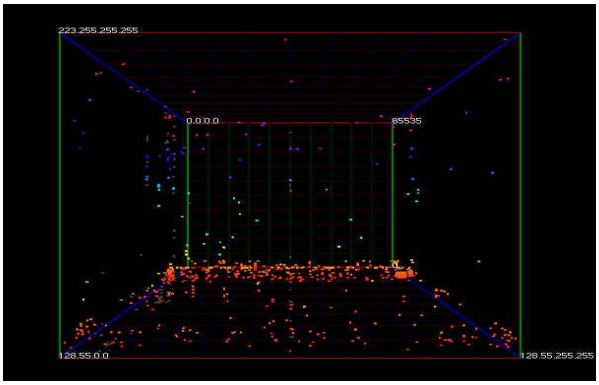

Figure 2. Network Security Tool - Spinning Cube of Potential Doom.

C. *PortVis*

Another network security visualization tool is PortVis [7] as shown in Figure 3. It was focusing on a single host at a time and doing the analysing on it. The main purpose of this tool is to present outside data entities to outside security specialists. Information such as each TCP port during a period of one hour is being visualised and large scale of security occurrence will be detected by PortVis. PortVis also allow for small scale security occurrence detection, which allowed for further investigation.

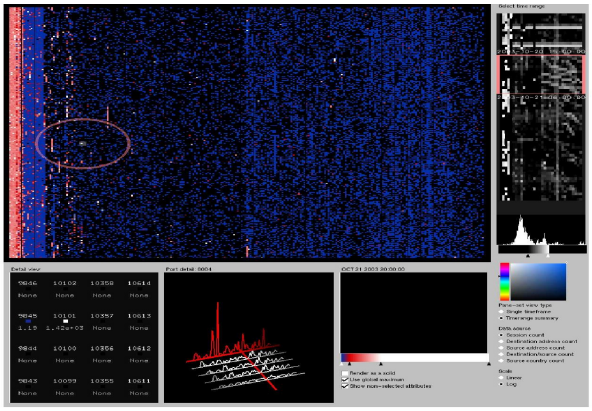

Figure 3. PortVis: Basic summary information from each TCP port during a period of one hour is visualized.

D. *NVisionIP*

Besides that, Figure 4 shown the NVisionIP [8] is also a visualization tool that targeted to provide and improve the overall situational awareness of the network among network security administrators. A graphical representation of a class-B network and numbers of different views of the data will be presented to network security administrators. There are three main visualization views in a single application of NVisionIP, namely Galaxy, Small Multiple and Machine visualization views. NVisionIP targeted to improve the interactivity among this visualization views by allowing them to transferring data from one visualization views to other visualization views. Figure 4 showed the screen shot of NVisionIP.

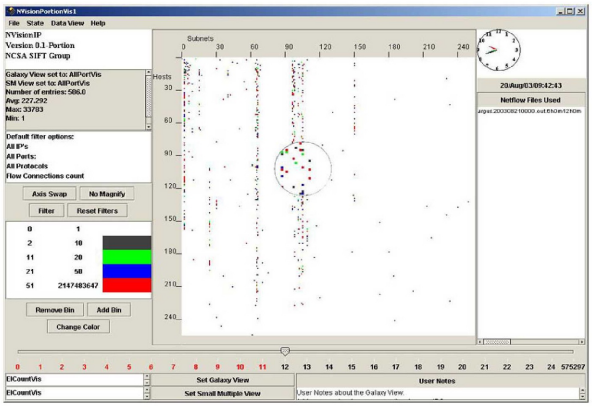

Figure 4. NVisionIP - A visualization tool to improve the situational awareness of security administrators.

E. VIAssist

VIAssist [9] as shown in Figure 5, provided a unified framework which to support and allow for different types of visualization tools to process and execute the same data source. There is also some other research mentioned and discussed the same architecture that is mentioned in [9].

Figure 5. Expert using VIAssist tool.

III. Development Of Expert-Aware Approach Method

We proposed an expert-aware approach to designing a system which formulated with a large amount of high-dimensional network data and adaptive for different types of users. In the preliminary phase, we were conducting a survey among different types of computer users and collecting data from them. Computer users provided us their requirement of network data. We construct a preface of an expertise classification system which provides a default setting for the expert-aware network security visualization tool. The system will learn from continual user feedbacks in order to statistically satisfy the needs of majority tool users. The expert-aware approach looks at the users' expertise level in network security and adapts the most comprehensive visualization views that are best suitable for the user.

Initial expertise classification system architecture on expert level-one also known as novice, level-two or intermediate and level-three or advanced will be discussed in the following subsections. The architecture is mostly based on the node concept. A node is an entity (a class, in our case with object-oriented programming) containing several elements such as, an icon (type depends on the programming language used), an x coordinates and a y coordinates as an Integer type (to localize the icon in the scene), some Strings containing the different IP addresses, a date type and also a list of nodes.

1) Details of Expert Level-One (Novice)

The expert level-one screen as shown in Figure 6 considers the user as a beginner in computer sciences, or at least someone who has very basic and common computer awareness. Based on the user requirements, system generates the initial screen for computer users, which are Figure 6 and 7. There are three types of data that will be shown on the expert level-one default screen:

a) Node: Composing the network represented by a machine icon, including IP addresses such as IP sources, IP destination and date of the analysis, displayed when mouse moving above the concerned node.

b) Address book: Containing every computer shown on the screen, allowing the user to have an overall view of who is connected on the network.

c) Worm detection: The system detects that any kind of worms is present on the network, it will immediately launch a pop-up window informing where that infection comes from. Plus, an icon will appear on the involved node to show that to the user in a more visual way.

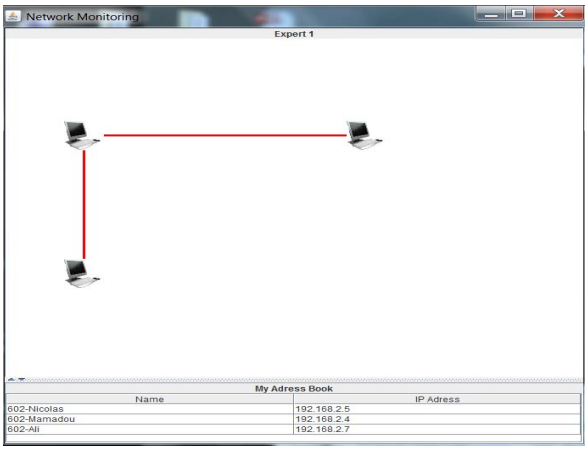

Figure 6. Expert level-one screen shot.

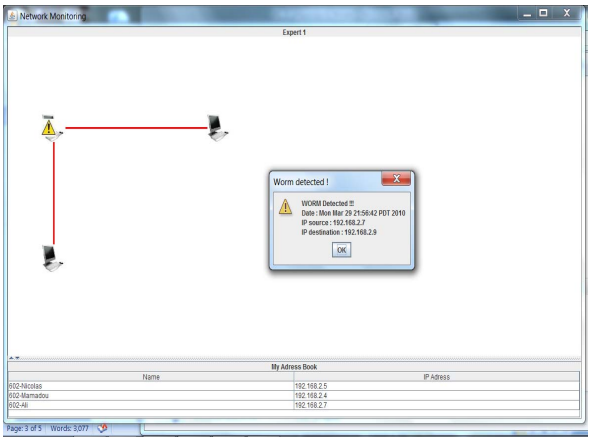

Figure 7. Expert level-one screen shot with worm detection alert.

2) Details of Expert Level-Two (Intermediate)

Figure 8 showed the screen shot of expert level-two. In this expert level, users consider as someone who has a little knowledge in computer sciences. Three new types of data have been added to the screen and some interactivity elements have been provided into this expert level. Animation features have been included in the development phase for expert level-two. The links between computers have been replaced by more complex entities exchanges.

a) Packets per sec: This information is represented by the speed of the packets coming from a computer to another. Faster is the packet between the two nodes, and higher is the packet per second value of the network.

b) Network utilization: This data is shown using the color of the packets, following this code: If it turns out that the network is subject to a high utilization, the color of the packets will be dark. And if the network is very poorly used, the color of packets will be slightly lighter.

c) Packets size ratio: It is represented on the screen by the size of the packets that are exchanged between two machines.

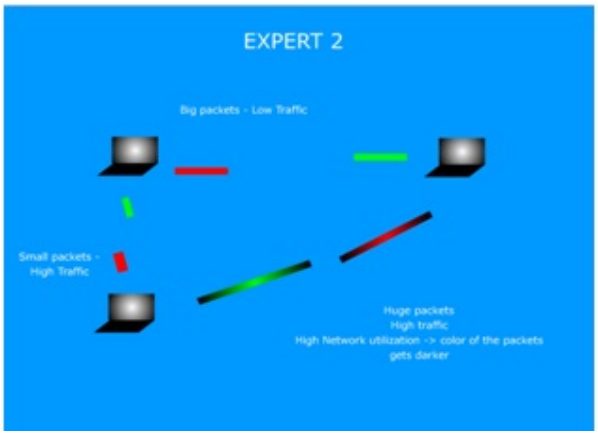

Figure 8. Expert level-two screen shot.

3) Details of Expert Level-Three (Advanced)

Computer user in expert level-three is expecting to have high awareness on network security data and network data. There are still ongoing processes to produce the comprehensive appearance. We proposed to include interactivity in these levels. Figure 9 shown the existing network security system screen shot that we will have it as reference, which going to be improve for expert level-three (Advanced).

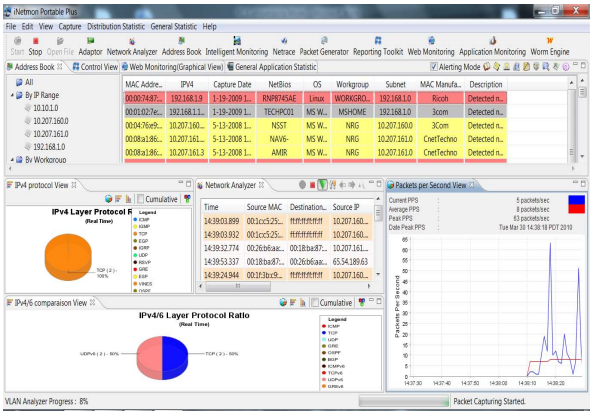

Figure 9. Existing expert level-three screen shot. (Source from iNetmon system [10])

IV. Results And Discussions

Initial results of the implementation of the expert-aware approach for the network security visualization tool show that it is capable of representing several of network security data not only on two-dimensional space on a computer but also three-dimensional or even beyond that space. The tool able to represent different types of network data based on different types of users' requirements. Our proposed approach is tested with dataset which has been captured by using iNetmon system and system acceptance surveys have been conducted among the computer users (beginner, intermediate and advanced) to get the feedback from them in order to improve the approach. System features such as effectiveness and efficiency have been improved based on the survey result analysis.

The results from the survey also showed that the expert-aware approach that applied in network security is similar to some other existing network security data visualization tools, it lays out complicated network data on comprehensive representation, and added further advantage by making it possible to display very large volume of network security data by allowing the computer users clicking of node or other attributes, which can lead the computer user to more details and deep of the network. It also not only showed the small portion of network security data but all relevant data to different types of user.

V. Our Future Work

An expert-aware approach helps to lead the process of enhancing the network security data visualization. The approach should imply more technical programming in order to produce an innovative technique for data visualization purposes.

Other algorithms and projection techniques are being studied so as to obtain and produce a more robust algorithm to network data visualization. We believed that other system features, such as performance will be improved.

VI. Conclusion

In this research, we proposed and implemented an intuitive and new expert-aware approach for the network security visualization tools, which improved the existing network security visualization tools. Our approach focuses more in the multi level of users' requirement which is very limited in the existing network security visualization tools. Our experiments in a network lab suggest that the tool can be further progressed as the tool has a high potential in the visualization area to a wide range of computer users. The initial result showed that the expert-aware approach has the capability for intelligence adjustment change whenever network data are updated. It will also improve on performance, effectiveness, and efficiency of network data visualization. The developed network data visualization approach makes it a promising network data visualization tool for the future.

ACKNOWLEDGMENT

Doris Hooi-Ten Wong is grateful to National Advanced IPv6 (NAv6), Universiti Sains Malaysia (USM) colleagues for their willingness to spare and contribute their time, sharing their knowledge, support and many useful insights. Our special thanks to Institute of Postgraduate Studies (IPS), Universiti Sains Malaysia (USM) for their financial support by awarding Doris Hooi-Ten Wong the Fellowship Scheme.

REFERENCES

[1] Bruls S., M., Huizing, K., and Van Wijk, J., 2000. Squarified treemaps. In Proceedings of the Joint Eurographics and IEEE TCVG Symposium on Visualization (VisSym), 33–42.

[2] M. Allen, P. McLachlan, "NAV Network Analysis Visualization," University of British Columbia, [Online, 29 May 2009].

[3] R. Ball, G. A. Fink, and C. North, "Home-centric visualization of network traffic for security administration," VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 55–64. ACM Press, 2004.

[4] V. Jacobson, C. Leres, and S. McCanne, TCPdump public repository, http://kb.pert.geant.net/PERTKB/TcpDump, cited September, 2009.

[5] G. Combs. Ethereal downloadable at: http://www.ethereal.com/,cited September, 2009.

[6] S. Lau, "The Spinning of Potential Doom," Commun. ACM, 47(6):25–26, 2004.

[7] Jonathan McPherson, Kwan-Liu Ma, Paul Krystosk, Tony Bartoletti, and Marvin Christensen. Portvis: a tool for port-based detection of security events. In VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 73–81. ACM Press, 2004.

[8] Kiran Lakkaraju, William Yurcik, and Adam J. Lee. NVisionIP: net-flow visualizations of system state for security situational awareness. In VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 65–72. ACM Press, 2004.

[9] A. D. D'Amico, J. R. Goodall, D. R. Tesone, and J. K. Kopylec, "Visual discovery in computer network defense," IEEE Computer Graphics and Applications, vol. 27, no. 5, pp. 20–27, 2007.

[10] iNetmon, "iNetmon System," 2008, http://www.inetmon.com, Last Accessed December 2008.