ISBN 978-1-84626-019-3
Proceedings of the 2009 International Conference on Information, Electronic and Computer Science
Qingdao, P. R. China, 14-15 November 2009, pp. xxx-xxx

Nebav: A visualization tool for monitoring large-scale network behaviors

Tao Li, Jian Gong
School of Computer Science & Engineering,
Jiangsu Province Key Laboratory of Computer Network,
Southeast University, Nanjing, P.R.China, 210096

Abstract. This paper proposes a visualization tool called Nebav (Network Behavior Visualization) to display behaviors of large-scale network.. Nebav draws a figure similar to Google Map to show the real-time behaviors of observed subnets. The historical time-diagrams of corresponding parameters drawn by RRDTool are produced at the same time. This paper presents a 2-D matrix which represents NetFlow numbers of ports of hot IP addresses. It combines temporal visualization with geographical visualization and logical visualization to help the security administrators to get full-round network situation awareness.

keywords: information visualization, network behavior, NetFlow

1. Introduction

When the units' number of observed network grows to large scale, take CERNET as an example, the number of access units rises to more than 1300 [1],it is insurmountable for the network administrators to gain an understanding of the current state of the network. Unfortunately, there is a severe lack of tools that can provide network administrators with the sense of situational awareness that they need. The best means of presenting a network administrator with enough data to form a cohesive picture of what is happening in their network is through the use of information visualization [2].

The three most common visualization views are: geographical view, logical view and temporal view. Each view has its own advantages and disadvantages. The geographical view is appropriate to show an overview of the behaviors of the observing network and connections among different units. The logical view is better to see detailed information of interested objects. The temporal view is useful to understand transitions of different network behaviors.

However, most of the existed visualization tools focus on single representation method. In this paper we present a visualization tool which integrates the three common views to observe large-scale network behaviors. The tool is called Nebav which is short for network behavior visualization. [1]

+ Corresponding author. Tel.: +86 02583794000-304; fax: +86 02584197050.
E-mail address: litaoseu@gmail.com.

2. Related Work

Nebav produces images of network behaviors in three different ways. This overall method of creating an image of network behavior is not wholly new; here is a sampling of systems that function similarly to Nebav in this respect:

·Mapnet [3] is a tool for visualizing the infrastructure of multiple international backbone providers simultaneously. Each backbone infrastructure is divided into a group of nodes (POPs) and pipes between these nodes, drawing them based on their geographical location on a map of the world. It has no logical or temporal visualization.

·PortVis [4] provides a 2-D matrix to represent packets number on each port. It permits analysts to discover the presence of any network security event that causes significant changes in the activity on ports. It is useful mostly for uncovering high-level security events. Security events that consist of small details are unlikely to be caught by using PortVis.

·VisFlowConnect [5] designs a parallel axes view which displays NetFlow[7] records as links between two machines or domains while employing a variety of visual cues to assist the user. It also provides filtering options to help the user to focus on his or her interesting flows. It does not provide detailed information, such as the source or destination unit, of a flow.

3. Implementation

3.1 System Architecture

Nebav is a sub module of NBOS(Network Behavior Observing System) which is designed for monitoring access units of CERNET. It is a web-based visualization tool which is based on BS architecture. The data sources of Nebav are NetFlows which are captured by a router on CERNET border and sent over UDP to a local server through a socket. By looking for a configuration table which maps IP addresses to unit names, we can classify NetFlows to different units. Other modules of NBOS parse and process NetFlows and store results into Mysql and RRDTool which will be visualized in three different views (Fig 1).

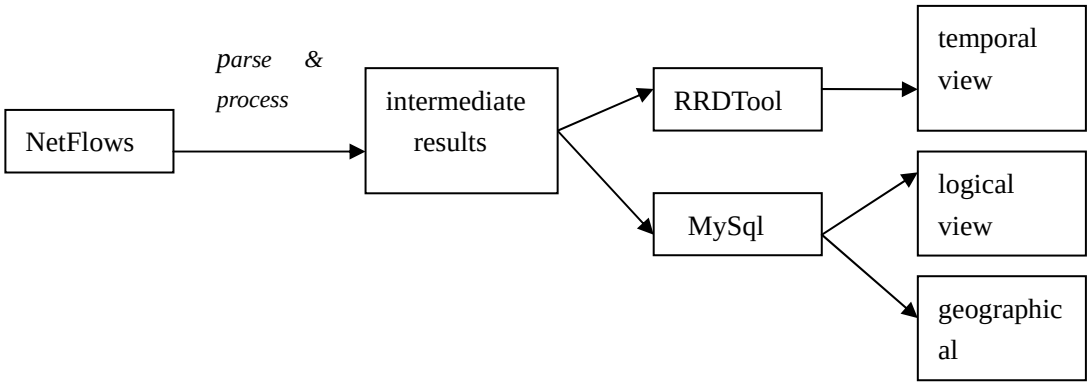

Fig. 1: Information Flow

3.2 Deployment Scenarios

3.2.1 Geographical View

The normal way to present subnets is by using tables which contain limited information in one or more pages. When the number of observing subnets increased, it is hard for the administrators to get their interested information at a glance. By using geographical map, the administrators can obtain an overview of the observing network promptly. As we known, Internet has a hierarchical structure. However, the existing visualization tools which use geographical map are static and can't show multi-level structure. We present a Google Map analogous view to show the state of observing network behaviors including security, threat, throughput and delay. Different behaviors are represented by different visualization characters, such as color, shape, thickness. By using the map, we can easily know the communication quality of different units, or which area is unsafe. By click on the hot area of the map, we can zoom in or out or drag to see units of different granularities such as country, province, city and university.

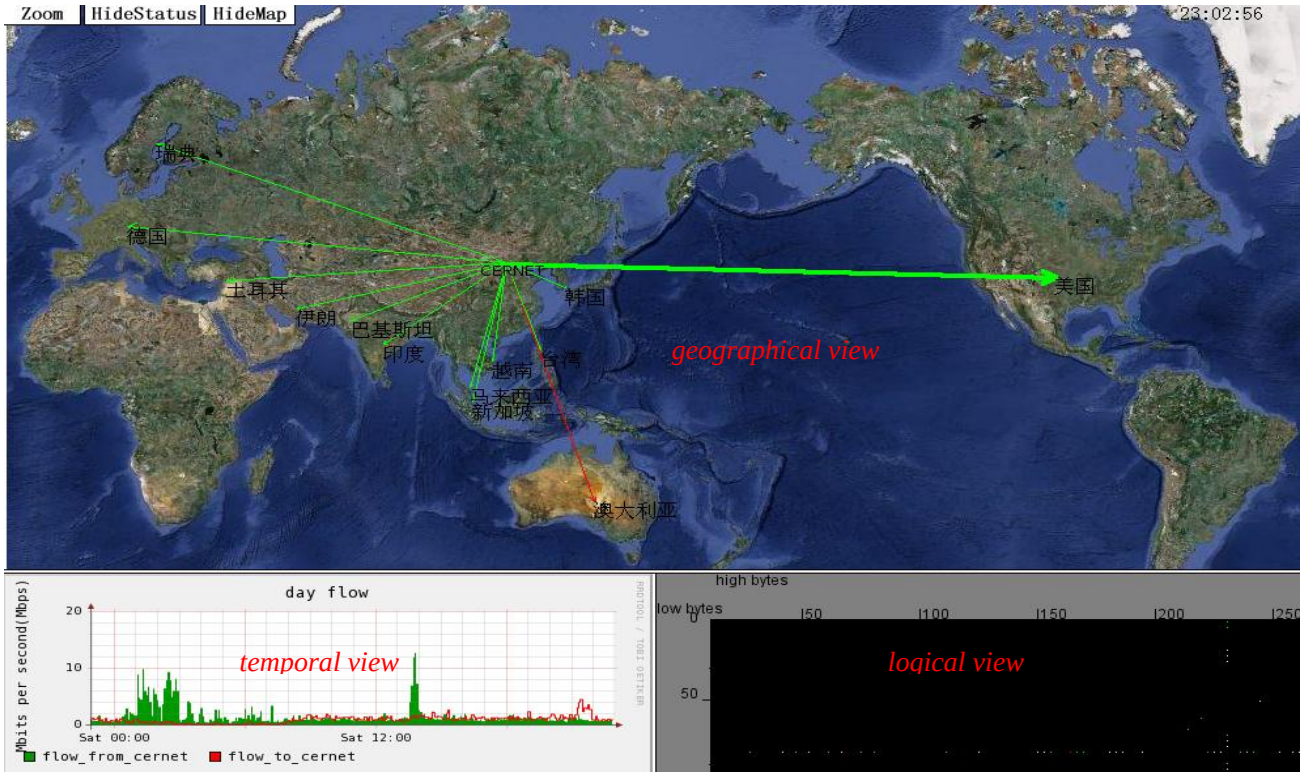

Fig. 2: Nebav Visualization

3.2.2 Temporal View

The temporal view is produced by RRDTool [7].In the time diagram, X-axis indicates time and Y-axis indicates, for example, the throughput of a unit which shows the transition of interested data.

3.2.3 Logical View

The above two views focus on the granularity of network segments. In fact, the targets of attacks are IP addresses. It is neither necessary nor practical to present information of each IP. As ports are the key targets of crackers, worms and viruses [4]. We focus on the 'key of key': the flow numbers through port of hot IP addresses (the addressed which have the most connections). Port Matrix is a 2-D matrix representation of units as shown partially in lower right part of Figure 2. In the section, the horizontal(X) axis indicates the low byte of the port number, and the vertical(Y) axis represents the high byte of the port number. The view consists of dots in a 256×256 grid for each of the 65,536 ports. The dot's location on the grid is calculated as follows:

$$x = port\_number \div 256$$
$$y = port\_number \bmod 256$$

The color of the port is determined by the number of NetFlows through it. By using this visualization, administrators are able to discover the presence of any network security event that causes significant changes in the activity on ports.

3.2.4 Integration

We provide a way to see the results of different visualization simultaneously to help the security administrators to compare information, make a right decision, and take an appropriate action. For example when the administrator clicks on a point on the logical visualization, the corresponding units are highlighted on the geographical visualization. When clicks on a behavior character of a unit on the geographical view, the temporal view of the behavior character is shown immediately.

4. Conclusion

As the dimension of network increased, network administrators have an urgent demand to understand the behaviors of network. The traditional visualization tools which base on single visualization view are not appropriate for this task. Nebav is a visualization tool integrates the three common views to observe large-scale network behaviors. Through the use of Nebav, the administrator will be able to understand the whole state of observing network or drill down to any interested area to know exactly what is happening.

5. Acknowledgements

This research is supported by the State Scientific and Technological Support Plan Project under Grant No.2008BAH37B04.

6. References

[1] Introduction to China Education and Research Network, http://www.edu.cn/cernet_jian_jie_1327/20060323/t20060323_91159.shtml

[2] Nahum Gershon, Stephen G.Eick,Information visualization,interactions,volume 5 Issue 2,1998

[3] Mapnet, http://www.caida.org/tools/visualization/mapnet/

[4] J.McPherson, K.Ma, P.Krystosk, T. Bartoletti , M.Christensen. PortVis: a tool for port-based detection of security events. Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, 2004

[5] X.Yin, W.Yurcik, M.Treaster, Y.Li, K.Lakkaraju, VisFlowConnect: netflow visualizations of link relationships for security situational awareness, VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security,2004

[6] RRDTool, http://oss.oetiker.ch/rrdtool/.

[7] Cisco IOS NetFlow, http://www.cisco.com/warp/public/732/Tech/netflow/index.shtml