ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

NetVis: Visualization Tool Based on Treemap

Mrs.Hemlata.A.Shinde
Lecturer AISSMS's Polytechnic, Pune.
hemlatakadam.it@gmail.com

Abstract

In this paper a new visualization tool based on hierarchy map, which is called NetVis, is introduced to combine the network security technique and universal network management together in an included visualization. NetVis is planned in 2D view.

Index Terms-NetVis,Network Security,Security Threats,Treemap,Prefuse

INTRODUCTION

With the explosion of the public Internet and e-commerce, private computers, and computer networks, if not adequately secured, are increasingly vulnerable to damaging attacks. Hackers, viruses, vindictive employees and even human error all represent clear and present dangers to networks. And all computer users, from the most casual Internet surfers to large enterprises, could be affected by network security breaches. However, security breaches can often be easily prevented. The Internet has undoubtedly become the largest public data network, enabling and facilitating both personal and business communications worldwide.More and more communication is taking place via e-mail; mobile workers, telecommuters, and branch offices are using the Internet to remotely connect to their corporate networks; and commercial transactions completed over the Internet, via the World Wide Web, now account for large portions of corporate revenue.

Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. With the rapid development of Internet and the expanding application fields of network applications, it is not enough to maintain the network security only depend on those professional network technical administrators. NetVis, is introduced to bind the network security technique and general network management together in an integrated visualization. NetVis is designed in 2D view.

NETWORK SECURITY

Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used. The current development in network security is not very impressive. Originally it was assumed that with the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development taking place in the same technologies being currently used.Combined use of IPv6 and security tools such as firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding intellectual property for the near future.

NETWORK SECURITY THREATS

Threats to network security usually fall into one of two main categories – logic attacks or resource attacks.Logic attacks, as the name implies, is an exploitation strategy used to bend any weakness within the system to will. These weaknesses can include anything from software vulnerabilities, like backdoors, to security lapses in code. The aim is to break into the system, either to crash it or to grant access to an unauthorized individual.

SECURITY TIPS

1. Encourage or require employees to choose passwords that are not obvious.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2. Require employees to change passwords every 90 days.
3. Make sure your virus protection subscription is current.
4. Educate employees about the security risks of e-mail attachments.
5. Implement a complete and comprehensive network security solution.
6. Assess your security posture regularly.
7. When an employee leaves a company, remove that employee's network access immediately.
8. If you allow people to work from home, provide a secure, centrally managed server for remote traffic.
9. Update your Web server software regularly.
10. Do not run any unnecessary network services.

TREEMAP

Treemaps are ideal for displaying large amounts of hierarchically structured (tree-structured) data. The space in the visualization is split up into rectangles that are sized and ordered by a quantitative variable.

The levels in the hierarchy of the treemap are visualized as rectangles containing other rectangles. Each set of rectangles on the same level in the hierarchy represents a column or an expression in a data table. Each individual rectangle on a level in the hierarchy represents a category in a column. For example, a rectangle representing a continent may contain several rectangles representing countries in that continent. Each rectangle representing a country may in turn contain rectangles representing cities in these countries. You can create a treemap hierarchy directly in the visualization, or use an already defined hierarchy. To learn more, see the section To Create a Treemap Hierarchy.

A number of different algorithms can be used to determine how the rectangles in a treemap should be sized and ordered. The treemap in Spotfire uses a squarified algorithm.

The rectangles in the treemap range in size from the top left corner of the visualization to the bottom right corner, with the largest rectangle positioned in the top left corner and the smallest rectangle in the bottom right corner. For hierarchies, that is, when the rectangles are nested, the same ordering of the rectangles is repeated for each rectangle in the treemap.

For example, a rectangle representing a continent may contain several rectangles representing countries in that continent. Each rectangle representing a country may in turn contain rectangles representing cities in these countries. You can create a treemap hierarchy directly in the visualization, or use an already defined hierarchy. To learn more, see the section To Create a Treemap Hierarchy.

A number of different algorithms can be used to determine how the rectangles in a treemap should be sized and ordered. The treemap in Spotfire uses a squarified algorithm.

PREFUSE TOOLKIT

Prefuse is a framework for building interactive information visualization applications using Java. It provides flexible data structures for:

- importing and storing the data
- mapping the data to visual elements
- adding direct manipulation interaction

The entire Prefuse toolkit is written in Java 1.4, using the Java 2D graphics libraries. It is licensed under a BSD license, and can be freely used for both commercial and non-commercial purposes.

PREFUSE'S FEATURES

- Table, graph, and tree data structures supporting arbitrary data attributes, data indexing, and selection queries, all with an efficient memory footprint.
- Components for layout, color, size, and shape encodings, distortion techniques and more.
- A library of controls for common interactive, direct-manipulation operations.
- Animation support through a general activity scheduling mechanism.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- View transformations supporting panning and zooming, including both geometric and semantic zooming.
- Dynamic queries for interactive filtering of data.
- Integrated text search using a number of available search engines.
- A physical force simulation engine for dynamic layout and animation.
- Flexibility for multiple views, including "overview+detail" and "small multiples" displays.
- A built in, SQL-like expression language for writing queries to prefuse data structures and creating derived data fields..

NETVIS IMPLEMENTATION

We use Snort as a tool to monitor the network abnormalities and collect critical security data. In addition,NetVis also extract the related information from the huge department management data and personnel management data of this organization as part of its source data. The visualization interface of NetVis is developed by Prefuse. Prefuse is a toolkit for visualization which is written in the Java programming language using the Java2D graphics library . NetVis is designed under a simple philosophy: visualization generally flows from the highestlevel semantic constructs to the lowest-level semantic constructs So we used multi-view, Global View and Detail View to help analysts to identify and monitor the network security incidents.

GLOBAL VIEW

Although the traditional tree structure is good at representing hierarchical relationship, it doesn't gain the upper hand in network security visualization. Because tree structure often wastes a lot of screen space compared with its limited information. But treemap has resolved such defects well. Treemap can handle considerably more nodes, and they layout nodes using all of the available space. In network security visualization, treemap is undoubtedly considered as an intuitive and simple pattern. Anyway, treemap is not nothing left to desire because that it has weaken the advantages of traditional tree structure in reflecting hierarchical relationship. Based on the reasons above, we have connected the two tree patterns together in one interface, treemap for network state and traditional tree for organization management hierarchical structure, for the sake of combining the advantages of traditional tree structure in representing hierarchy and treemap in saving screen space. The two views communicate at any moment in order to learn from each other's strong points and close the gap. Even running in the same network, different departments have different security demands.

For example, the department which is in charge of finance or technology calls for much more strict safety requirements. So we should supervise those departments in different ways.

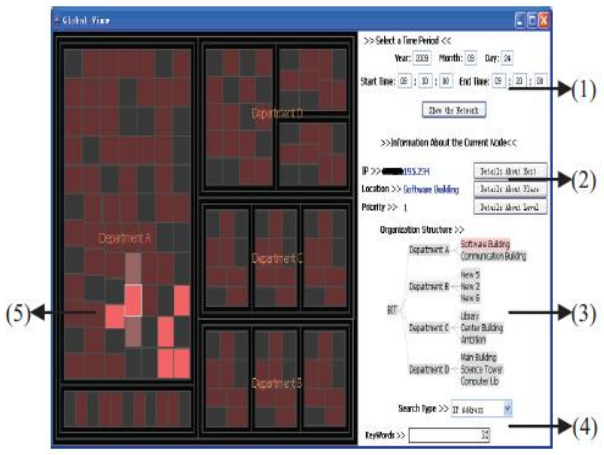

Figure 2.1 Global view

Figure 2.1 is the global view of NetVis. The left part of the frame is a treemap which expresses the network situation in a given organization. The leaves of treemap represent the hosts in the organization's network. These hosts are classified by the departments they belong to. The light-colored nodes show that there exist some alerts for this host in the network while dark-colored nodes means the host has no alert at all.When the user choose the exact time they are concerning about (See Figure 2.1(1)), the treemap will show the security situation in this selected time interval. The lighter the node shows, the weaker the host is. It means that the host will become

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

the weak link of network security very likely. The administrators should fix on such kinds of hosts immediately and pay more attention on them. Figure 2.1(2) describes the details of the host where the mouse is hovering over.Administrators can directly find the department and people in charge of the current host located. Accordingly they can notify the direct affiliated section or leader to pay attention to the warning as soon as possible, for the sake of increasing the efficiency of network management obviously. Figure 2.1(3) on the right is a tree graph of the given organization management hierarchical structure. When the mouse hovers on a specific leaf of the treemap, whose department correlated to the node of (3) will change its color. The more descriptive information of each item can be seen in the pop up windows in Figure 3.2 on clicking the corresponding button.

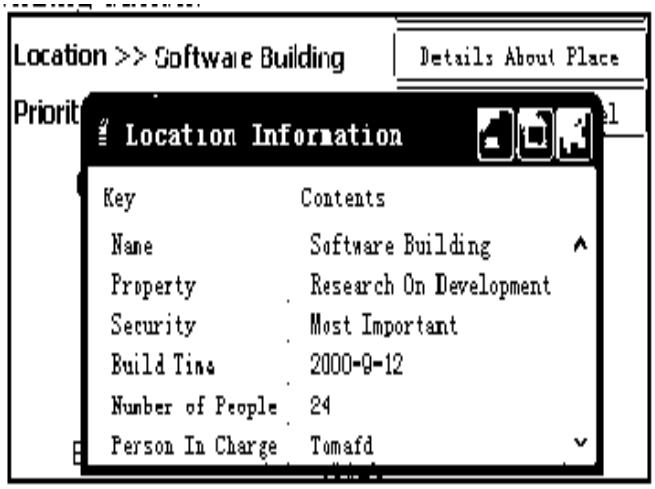

Figure 2.2 Description for different options

DETAIL VIEW

Figure 2.3 shows the detail Snort alert messages of the selected host in the network in the selected interval. It can be seen in the left radial node-link graph (See Figure 2.3(1)). The center node represents the focused warning host. The nodes around it are the hosts which have been suspected to be attackers of he focused host in or outside the organization network. The edges connecting the center node and nodes around describe their relationship. The color of the edge depends on the protocol of hosts' connection type, TCP or UDP.

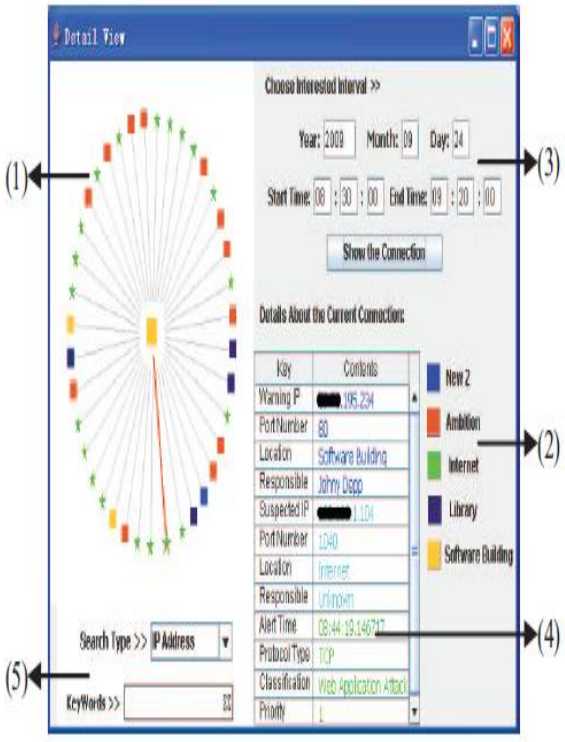

Figure 2.3 Detail view

The hosts in the same organization network are rendered as square glyph while the hosts in the Internet are rendered as star glyph. Colors of glyphs distinguish the departments they belong to. Figure 2.3(2) expresses those color samples of different departments. As in global view, the users can choose specific time interval in Figure 2.3(3). More details about each alert can be seen in the table like Figure 2.3(4),including IP address and port number of both sides, information about their location, alert time, priority and so on.

INTERACTION

The interaction elements are very important to an information visualization tool because it makes the information easily understood. NetVis provides many kinds of interactive components to facilitate the communication between user and data, as well as make it more easy and familiar for different kinds of administrators to manipulate. At present there are two main kinds of interaction operations: Selection and Searching Item.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Selection:

Selection is an important element of visualization interaction. As we mentioned above, users can fill the particular time interval in text field on both kinds of views, as Figure 2.1(1) and Figure 2.3(3). Then NetVis will rebuild the view in the selected period under the user's demands.

Searching Item:

Both global view and detail view of NetVis includes search components: ComboBox and TextField. Users can search for special graph items by describing the type and key words of the information they are seeking at the moment. This can be seen in Figure 2.1(4) and Figure 2.3(5).

CONCLUSION

The integrated visualization of network security technology and network management will become a popular trend in the future network development. It comprises the absolute network technique and flexible organizational analysis as a whole. Either from the perspective of security technology or of security management, it is a win-win means to play the greatest advantage of both sides. In the future research, we plan to add more information about organization management to the visualization and develop more interactive characters.

Meanwhile, we will improve more security feature and defensive means for the common network attacks, making it more available and helpful in the field of network security management.

BIBLIOGRAPHY

[1] J. McPherson, Ma K. L., Krystosk P., Bartoletti T., Christensen M.,"Portvis: A tool for port-based detection of security events," ACM VizSEC 2004 Workshop, 2004, pp.73-81

[2] D. Phan, J. Gerth, M. Lee, A. Paepcke, and T. Winograd, "Visual Analysis of Network Flow Data with Timelines and Event Plots," VizSEC 2007 Workshop

[3] Pearlman J, Rheingans P, "Visualizing Network Security Events Using Compound Glyphs from a Service-Oriented Perspective," VizSec 2007

[4] Jeffrey Heer, Stuart K. Card, James A. Landay, "Prefuse-A Toolkit for Interactive Information Visualization," CHI 2005 PAPERS: Interactive Information Visualization April 2-7 Portland, Oregon, USA

[5] Ryan Blue, Cody Dunne, Adam Fuchs, "Visualizing Real-Time Network Resource Usage," VizSec 2008, pp.119

[6] Muelder Chris, Ma Kwan-Liu, Bartoletti Tony, "A Visualization Methodology for Characterization of Network Scans," VizSec 2005

[7] http://www.cs.mun.ca/~hoeber/teaching/cs4767/notes/04-prefuse/