International Journal of Smart Sensor and Adhoc Network

Volume 2 | Issue 4 Article 2

July 2012

# VISUALIZATION OF NETWORK TRAFFIC

SOWMYA C. L
*Department of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur*,
sowmyalnp@gmail.com

# VISUALIZATION OF NETWORK TRAFFIC

**SOWMYA C. L[1], C. D.GURUPRAKASH[2] & M.SIDDAPPA[3]**

[1,2&3]Department of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur
E-mail : sowmyalnp@gmail.com

**Abstract-** Network security in today's world is critical. System administrators must quickly perceive the security state of their networks, but they often have only text-based tools to work with. These tools often provide no overview that would help users grasp the big-picture.Network traffic visualization tools have successfully enabled security analysts to understand the nature of traffic present in a network. However these tools rely mainly on human expertise to discover anomalies in traffic and attack patterns.The visualization capability provided by Visualization tool allows an operator to assess the state of a large and complex network given an overall view of the entire network and filter/drill-down features with a friendly user interface that allows users to request more detailed information of interest such as specific protocol traffic flows.Visualization tool allows operators to detect and investigate anomalous internal and external network traffic. Visualization tool shows network events graphically. We model the network as a graph with hosts being nodes and traffic being flows on edges. We present a detailed description of Visualization tool functionality and demonstrate its application to traffic dynamics in order to monitor, discover, and investigate security-relevant events.

***Keywords*** *- Visualization, NetFlows, Parallel axes representation, Link based visualization, Security visualization, Network traffic visualization.*

## I. INTRODUCTION

Networks are becoming increasingly complex. Complexity is the enemy of security. Networks have become more complex in terms of size, topology, and especially traffic flows. Traffic flows are faster and the number of different applications generating flows grows continuously. While network traffic is an ideal place to monitor for security events since all security events leave some form of network trace, there is a major problem in that security events can also be concealed among the vast amount of legitimate traffic. It is often difficult to just to capture and store network traffic, so analyzing and detecting attacks in near-real-time with current command line driven text-based tools can be especially challenging for non-experts.

However, humans excel at visual processing and identifying abnormal visual patterns. Visualization is the act or process of interpreting in visual terms or of putting into visual form. A new definition is a tool or method for interpreting image data fed into a computer and for generating images from complex multi-dimensional data sets. Visualization tools can translate the myriads of network logs into animations that capture the patterns of network traffic in a sufficient way, thus enabling users to quickly identify abnormal patterns that warrant closer examination. Such visualization tools enable network administrators to sift through gigabytes of daily network traffic more effectively than searching text-based logs.

It is challenging to visualize all the information relevant to network and security administrators. We must be able to provide near real-time analysis. To deal with the storage and processing limitations, special data structures must often be created. Analysis is also complicated since not only must we show what is happening on each host, but we must visualize the relationships and interactions between all the hosts.

Visualization tool has these distinguishing features: (1) it uses animations to visualize network traffic dynamics and (2) it provides multi-level views of network traffic including an overview and drill-down views that allow users to query for details on-demand, and (3) it provides filtering capabilities to remove known legitimate traffic so as to focus on potential security events.

Although techniques to collect packets are important, the purpose and scope of collection have to be clearly described. As packets are collected in a single location, the location must satisfy the purpose and scope. Since network packets are digital signals transmitted by hosts, servers, network devices and others, it is important to understand the whole network structure. If the network is connected to the Internet, properties, such as the IP bandwidth of the collection location, type of the service, availability of VPN, rules of the firewall and network speed, have to be considered.

As packets are collected over a time period, details of the packets are analyzed by monitoring the time flow. For example, types of services used are achieved from the port information. The concentration and

distribution of services can be analyzed by investigating specific IP bandwidths. Therefore, packet data including IP or port data are analyzed in a binary or hexadecimal format. Due to the large amount of packets, wide IP bandwidths, and various services, acquiring specialized knowledge under limited time leads to serious analysis problems.

Extract IP addresses and ports from network packet files are used as Ethereal and Sniffer systems. After storing relevant traffic data, classification by session is performed and finally the amount of traffic that flows in is measured. Port scanning is the process that identifies listening ports of target systems. Attackers check if target systems are on and then look for open ports and find weak points to attack. Since the port scanning is highly likely to be a preliminary step of attacking, it is important to identify such attacks.

System administrator can make use of the online network visualizing process to trace suspicious network activities or potential attacks to the network system. By applying visualization technique, the network analyst can examine the entire network traffics and discover the characteristics of traffic.

Most of the visualization techniques exist in generating the captured network data into informative graphical 2D or 3D view and to improve decision making and organization management performance.

Visualization tool is its ability to display a large amount of data and highlight unusual behaviors in two dimensional views that are easily readable. Obviously, three dimensional views would provide additional information compared to those that are two-dimensional (hereafter respectively called 3-D and 2-D views). However, to observe such 3-D views we have to project them down onto a 2-D visual aid (e.g., a screen or paper). Two main issues are raised by this dimensionality reduction, namely disorientation and occlusion. Disorientation means that the position of the plotted data is not clear and the values corresponding to the plots are difficult to retrieve. Occlusion occurs when plots hide one another, so information is omitted from view. These two problems are well-known in the field of computer vision, and a common solution is to display several 2-D projections instead of a single 3-D view.

### 1.1 Objective

Visualization is a technique to graphically represent sets of data. When data is large or abstract, visualization can help make the data easier to read or understand.

The objective of this project is to develop a technique for visualization of network traffic. The network traffic visualizing method is the main goal to be achieved. It visualizes network traffic flow using NetFlow source data. It detects and investigates anomalous internal and external network traffic. The tool provides multi level views of network traffic. Tool process network log records in real time.

Although visualization makes the analytical process more convenient, complex graphics makes the process difficult to conduct. By using simplified graphics network traffic can be easier to conduct because it is more understandable. Through logging network traffic will provide back tracking an incident of network to determine the source. Therefore the network traffic should be logged periodically and on demand for this purpose.

### 1.2 Motivation

Network attacks are a serious problem that network attacks cost businesses an estimated $666 million in 2003. There are a variety of network traffic visualization tools available, each focusing on a different level of network abstraction. Previous work focuses on representing activities occurring on machines while tool focuses on network flows between machines.

This project is motivated by concern of network security by system administrator and visualizing capability of network state. The text based tool, which perceive security state of network are not useful for users to grasp the big picture.

## II. LITERATURE SURVEY

Linkages between different hosts and events in a computer network contain important information for traffic analysis and intrusion detection.

"Home-Centric Visualization of Network Traffic for Security Administration" [5] and "Combining Visual and Automated Data Mining for Near-Real-Time Anomaly Detection and Analysis in BGP" [10] focus on visualizing linkages in a network.

"Home-Centric Visualization of Network Traffic for Security Administration" presents a VISUAL(Visual Information Security Utility for Administration Live), visualization tool. It focuses on visualizing linkages in a network. Rapidly perceive the security state of their network. Use a matrix visualization technique combined with a simple graph drawing technique. The prototype whose design and testing is discussed in this paper is called Visual Information Security Utility for Administration Live (VISUAL). VISUAL aids network administrators by showing a graphical, home-centric overview of their network. Aside from seeing abnormal traffic, VISUAL allows network administrators to develop an accurate mental model of what is normal on their own network so that they can diagnose problems better. VISUAL's design follows "Overview first, zoom and filter, then details

on demand." We wish to display an overview of network traffic for a small to mid-size network. We show a home-centric, internal vs. external perspective of the network. "Elisha: a Visual-based Anomaly Detection System" [12] the authors present a visualization of network routing information that can be used to detect inter-domain routing attacks and routing misconfigurations.

In "A Visual Exploration Process for the Analysis of Internet Routing Data",[13] they go further and propose different ways of visualizing routing data in order to detect intrusions."NVisionIP", [9] a security visualization tool that shows network traffic flows from a host-centric view. The visualization approach behind NVisionIP is to present an overview first, zoom and filter capabilities next, and then details on demand. In the overview/galaxy view, NVisionIP represents an entire class B IP address space 64,000 hosts on one screen with attributes highlighted such as traffic volume, number of connections and port or protocol activity-color and shape representations can be chosen by users on demand. Drill-down views to a subnet small-multiple view and an individual machine view allow operators to make analytical observations of flow activity.

## III. PROBLEM STATEMENT

Network is becoming complex in terms of size, topology and network traffic flow. So it is important to maintain the network secure. System administrator must maintain their system secure from network attacks.

Previously text based tools are used to monitor the network but it is difficult for non experts to analyze and detect attacks.

Thus visualization technique is used to analyze and detect attacks, which makes users to identify attacks easily by seeing patterns.

The title of the project is "Visualization of Network Traffic". The visualization technique monitors, analyzes the network traffic for attacks. Where visualization technique captures the network traffic and projects the data into graphical representation. Graphical representation can be 2D or 3D. Visualization technique enables user to understand the network anomalies and attack easily by using the graphical representation. By using visualization we can identify any anomalies in the network by seeing patterns in the graphical representation.

## IV. METHODOLOGY

In visualization of network traffic, it captures the network traffic and analyzes the captured network traffic. The traffic is captured in the form of packets. Thus packets information like source, destination address and port number, packet size, time of packet capture, protocol type used and some information about the packet are captured as network traffic flow. Then captured packets are analyzed. These analyzed packets are then sent to visualizer, which creates new image after some interval of time from the captured packet data. The visualization of network traffic flow can be done in real time also, i.e by capturing live network traffic and then analyzing the captured data and then viewing the captured data through visualizer.

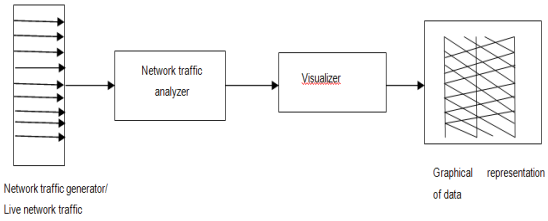


**Fig. 1: General architecture of visualization**

Firstly, it requires generation of network traffic flow then capturing the network traffic flow. Later analyzing the network traffic and then filtering the network traffic based on some parameters like source, destination address, port number, protocol and etc. Then filtered or analyzed packets can be visualized through visualizer, which presents the data in user understandable format, i.e in graphical representation. Store the captured data for future reference. Identify any anomalous traffic flow by examining the flow with stored data.

### Denial of Service Attack

In this case, an unfamiliar domain is generating a significant amount of traffic to multiple hosts on the local network. For example consider while traffic is capturing, at that time filtering is applied. i.e filter out all traffic except that on port 80. This reveals that a single domain is generating a large amount of traffic to many internal hosts on this port, suggesting that this external domain is contacting many local web servers. Thus many machines on the external network are heavily accessing a set of hosts on the local network. This type of pattern strongly suggests the occurrence of an attempted denial of service attack in progress on local web servers.

Visualization approach is capable of revealing a variety of network traffic patterns relevant to security. Here by using visualization we identify some variety of traffic patterns like Dos attack.

## V. CONCLUSION

Visualization tool for visualizing traffic flows on a network using NetFlow source data. This visualization framework is extensible to other domains beyond IP networks. Visualization tool can

visualize traffic in near realtime for security monitoring purposes.

Visualizing network traffic increases the ability to detect network anomalies or attacks.

Visualization tool enhances the situational awareness of a security administrator by providing an intuitive view of IP flows using link analysis. The primary graphical user interface to Visualization tool is a parallel axes view which is used to represent the source and destination of network traffic flows. A highlevel overview is provided first with the user able to drill down to lower level views for more resolution and details on demand. Filtering mechanisms are provided to facilitate either extracting known legitimate traffic patterns or highlighting flows of special interest.

## REFERENCES

[1] R. Ball, G. A. Fink, C. North, "Home-Centric Visualization of Network Traffic for Security Administration", CCS Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC), 2004.

[2] Kiran Lakkaraju William, Yurcik Ratna Bearavolu, Adam J. Lee, "NVisionIP: An Interactive Network Flow Visualization Tool for Security", National Center for Supercomputing Applications (NCSA) University of Illinois, Urbana-Champaign.

[3] Meghan Allen, Peter McLachlan, "Network Analysis Visualization", University of British Columbia Department of Computer Science.

[4] Sven Krasser, Member, IEEE; Gregory Conti, Member, IEEE; Julian Grizzard, Member, IEEE; Jeff Gribschaw, Member, IEEE; Henry Owen, Senior Member, IEEE, "Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization", Proceedings of the 2005 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY.

[5] K. Lakkaraju, W. Yurcik, A. Lee, R. Bearavolu, Y. Li, and X. Yin. NVisionIP: NetFlow Visualizations of System State for Security Situational Awareness. In ACM CCS Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC) held in conjunction with the 11th ACM Conference on Computer and Communications Security, 2004.