Abstract

The monitoring and analysis of computer networks to detect abnormal network behavior is a complex task for network administrators, which is assisted with the use of visualization analytics. In this work, we present a web-based implementation of the three-dimensional cube known as the Spinning Cube of Potential Doom using WebGL and the Three.js library. With this implementation, our goal is to provide an easy-to-use and accessible method for network administrators to visualize network traffic and detect abnormal behavior. This method allows for the efficient analysis and understanding of network data, and in our method, we implement a web version of the Spinning Cube of Potential Doom.

Problem

Given the complexity of monitoring network with large data sets, we are looking to provide efficient methods of analysis and visualization of network data through the web. This without the need of sophisticated hardware or software. In our method, we implement a web version of the Spinning Cube of Potential Doom.

Methodology

For the creation of the three-dimensional cube, we have used the 3D JavaScript library three.js, this library allows you to create 3D objects, camera manipulation, lights, scenes and other features.

• The first step is to create a scene.
• Second, we create a cube geometry to represent the network data through its axis. At the x axis we have the destination address, in y axis we put the ports and at the z axis we represent the source address.
• Finally, we create a particle system inside the cube where each particle represents a network flow.

Results

As a result we have a working version of the desired application providing an interactive web interface in which we use different JavaScript libraries to display NetFlow records through the web browser. At the moment we do some manipulations over the cube such as rotating it, and zoom in or out. Also, it is possible to filter the flows by source and destination IP address and to select the division of the network classes, and the user is allowed to select date and time of the flow, providing a wide and structured way to search.

What is a flow?

NetFlow is a service introduced by Cisco that allows system administrators to have a detailed record of the events on their network. A flow contains aggregated information of a network connection. Some of the data provided by a flow are:

- Source IP address: It is an address assigned to a node (computer) that is sending a packet through the network.
- Destination IP address: This address is used to know where is the data going to be sent.
- Destination Port: The port is an integer value between 0 and 65535 used to specify in what point (service) a packet is going to arrive. Each well known service use a designated port value like 80, 23, 22 for the HTTP, Telnet, and SSH services respectively.

As we can see in figure 1, we have the user interface where the cube is an additional component for a better comprehension of the data. The control panel at the right provide means to filter the data by source and/or destination IP address, or classes of networks, and by date and hour. Each point inside the cube represents a flow.

In the server side, we have a python script that verifies if the filename of the network flow is requested is valid. If not valid, it returns a signal to notify the user, otherwise, it parse all the data requested by the user and returns it back to the client side.

Conclusion

Given the structured implementation of this project and its successful results, we are contributing to innovation of applications directed to network monitoring through visual interfaces. In addition, we can easily manage and access the application. Based on the results that we have, we could use this application to monitor IP events to detect network or port scanning events, denial of services and other kinds of threats that often we see on a network. As a future project, this application will be attached as a network tool to the Toa Monitoring System.

Acknowledgements

First we would like to acknowledge to all the research lab members of Dr. José R. Ortiz Ubarri for their support. Also, we want to thank Dr. Humberto Ortiz Zuazaga for his comments and advices, and the HPCF for providing access to the University of Puerto Rico NetFlow data.

Bibliography