Distributed Denial of Service Attack Animation

Areej Alghamdi
CIS 533
Class Project
Motivation and Project Idea

- Interested in scientific visualization and computer graphics
- Visual everything!
- Intersection of security and visualization. Animating a DDOS attack.
- Learned a lot: security, kinds of DDOS attacks, How?, weblogs, new information visualization tool, refreshing my web development skills and knowledge.
1. index.html
   - The html file that has my webpage code and has the scripts of the animation embeded in it.
   - I created this animation using d3.js.
   - “D3 helps you bring data to life using HTML, SVG, and CSS.”
   - It is javascript library to help manipulate and visualize documents through data-driven transformations.
   - I chose d3:
     - Visualize informational data
     - Graphical
     - Easy to view
2. logParser.py
   - This is a python script to parse standard apache weblog files and transform them to JSON files to read into the javascript and initiate the animation.
Design

Initial plan: a globe, with network requests presented as shooting segments! But..

I chose d3.force layout. Presenting the central node as the targeted server/website and linked to small nodes representing the web requests.
Limitations

• The project does not analyze weblog files and figure out the target. I have to specify the target.

• The data of is huge!

• JSON files are almost the same size as the weblog text files. My sample had (~17000 entries) for one month for a non commercial website(cs.uoregon.edu).

• The animation couldn’t handle more than 2000 node(web requests).
Future enhancements

• Optimize the speed of the animation to allow the visualization of more web requests if possible.

• Improve the design of the elements: ex. finalizing the attack with meaningful text

• Add stats of number of attacks by a certain user/ip.

• Add user field for uploading log files to parse and animate

• Combine all parts of the project into one component for ease of running
Demo

and

Q&A
Distributed Denial of Service Attack Animation using d3.js

MOTIVATION AND PURPOSE
The motivation is to create an animation for DDOS attacks given any weblogs file targeting a specific website/server in a graphical way that allow for user-interaction for the purpose of exploring and visualizing the event in a friendly and interesting manner.

DEVELOPMENT TOOLS
• Javascript using d3.js library. D3.js uses HTML, SVG and CSS to create data-driven transformations.
• Python script: to parse log files and generate JSON files of nodes and links to create and animate the attack.

DESIGN
• Central node: represents the targeted server/webstie.
• Small nodes surrounding the centreal node: representing the web requests from the different users/ips.
• Loading progress bar to show when it is ok click play and start the animation.
• Play, pause, and replay buttons to play, pause, and replay the attack respectively.
• Mouse hover over any small node show an information box presenting the current node’s details.
• Dragging event to any small node to explore it individually.
• The central node radiate as the attack is undergoing.
• When all nodes have targeted the central node. The central node is removed and replaced with “The server is down!!”