RadialNet

An Interactive Network Topology Visualization Tool with Visual Auditing Support

João Paulo S. Medeiros¹, Selan Rodrigues Santos²

<joaomeideiros@dca.ufrn.br>, <selan@dimap.ufrn.br>

¹Department of Computer Engineering and Automation – DCA
²Department of Informatics and Applied Mathematics – DIMAp
Federal University of Rio Grande do Norte – UFRN

Frascati, Italy, Oct. 2008
Motivation

- Data retrieval and visualization is a challenge for large networks;
- Data presentation is generally textual;
- Information Visualization can be applied to network related data;
- These techniques can be used to provide an effective network topology representation.
Introduction

Requirements
A network visualization tool must...

- Be able to represent large networks (more than hundreds of nodes);
- Provide mechanisms to navigate the network topology and its data;
- Afford a simple and complete (all data) visual representation;
- Get rid of or offer solutions for data occlusion.
Introduction

Related Work
There are problems with existing network visualization tools:

- fe3d: the three-dimensional approach implies data occlusion;
- Nagios: the radial visualization is good, but it lacks features;
- Cheops-ng: it is not based on solid information visualization techniques.
Nmap
Tool used to acquire network data. Features:

- Detect networks devices (routers, firewalls, wireless access points, ...);
- Detect remote operating system (OS fingerprinting);
- Perform Ports scan and service discovery (FTP, DNS, HTTP, ...);
- Discover Network topology (using Traceroute);
- Determine link latency and route disruption.
Visualization

Reference Model (Stuart Card)

Used reference model.
Reference Model (phases)

- Data Transformation
  - Data tables organized in variable types;

- Visual Mappings
  - Association between data tables and retinal variables;
  - Node-links diagrams (radial layout);
  - Visual marks + graphical properties;

- View Transformations
  - Navigation (animation, zooming, panning, reorganization of nodes);
  - Detail-on-demand;
  - Strategies to handle occlusion (filtering, fisheye distortion, subgraph collapsing).
The Application

http://www.dca.ufrn.br/~joaomedeiros/radialnet/
Some Features

- Open ports details;
- Filtered ports;
- Running services information;
- Detailed traceroute.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>State</th>
<th>Service</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>tcp</td>
<td>open</td>
<td>ftp</td>
<td>probed</td>
</tr>
<tr>
<td>21</td>
<td>state</td>
<td>open</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>state</td>
<td>reason</td>
<td>syn-ack</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>state</td>
<td>reason_ttl</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>service</td>
<td>product</td>
<td>bsd-ftp</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>service</td>
<td>name</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>service</td>
<td>hostname</td>
<td>cvs.openbsd.org</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>service</td>
<td>conf</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>service</td>
<td>ostype</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>service</td>
<td>method</td>
<td>probed</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>tcp</td>
<td>open</td>
<td>smtp</td>
<td>probed</td>
</tr>
<tr>
<td>53</td>
<td>tcp</td>
<td>open</td>
<td>domain</td>
<td>probed</td>
</tr>
</tbody>
</table>
Some Features

Collapsing (grouping) nodes.
Some Features

Fisheye based effect.
Case Study – Brazilian Universities

50 Brazilian universities (238 nodes).

- Node shape;
- Color and size;
- Line thickness;
- Icons;
- Orange lines;
- Dashed lines.
Case Study – Brazilian Universities

- Several hosts have security problems;
- All hosts have filtered ports;
- We can identify switches, routers and WAPs;
- Alternative routes;
- Hop counting;
- Network bottlenecks.
Case Study – Large Networks

Visualization of 1000 nodes.

To handle occlusion:
- Filtering;
- Subgraph collapsing;
- Fisheye distortion.
Final Considerations

Nmap/Umit Integration

- Radialnet was developed during Google Summer of Code 2007;
- Has been integrated to Umit (Nmap frontend);
- Added to Nmap/Zenmap.

Conclusion

- Information Visualization models and techniques can help network security management!

Future Work

- Perform a cross-referencing between captured data and NIST vulnerability database;
- Use other tools to acquire data can extend RadialNet applicability:
  - Network administration;
  - Load balancing analysis.
joaomedeiros@dca.ufrn.br