Network Analysis Visualization (NAV)

Meghan Allen and Peter McLachlan
December 15, 2004
Problem

- Network traffic analysis is necessary for many home and corporate users
  - Security threats are on the rise on the internet
  - Users are interested in their bandwidth usage
- Analyzing network data is a difficult challenge
- Traditional network analysis software only provides detailed text based output
  - These packages do not provide an overview, or capabilities to pop-out important information
  - No dynamic filtering, static queries only
  - Finding specific events can be challenging
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>55999</td>
<td>11:03:35.357</td>
<td>128.189.142.254</td>
<td>Broadcast</td>
<td>ARP</td>
<td>Who has 128.189.142.147? Tel 128.189.142.254</td>
</tr>
<tr>
<td>56000</td>
<td>11:03:35.455</td>
<td>128.189.142.254</td>
<td>Name query [Short Frame]</td>
<td>ARP</td>
<td>Who has 128.189.142.147? Tel 128.189.142.254</td>
</tr>
<tr>
<td>56001</td>
<td>11:03:35.550</td>
<td>128.189.142.254</td>
<td>Name query [Short Frame]</td>
<td>ARP</td>
<td>Who has 128.189.142.147? Tel 128.189.142.254</td>
</tr>
<tr>
<td>56002</td>
<td>11:03:35.656</td>
<td>128.189.142.254</td>
<td>Name query [Short Frame]</td>
<td>ARP</td>
<td>Who has 128.189.142.147? Tel 128.189.142.254</td>
</tr>
<tr>
<td>56003</td>
<td>11:03:35.752</td>
<td>128.189.142.254</td>
<td>Name query [Short Frame]</td>
<td>ARP</td>
<td>Who has 128.189.142.147? Tel 128.189.142.254</td>
</tr>
<tr>
<td>56004</td>
<td>11:03:35.848</td>
<td>128.189.142.254</td>
<td>Name query [Short Frame]</td>
<td>ARP</td>
<td>Who has 128.189.142.147? Tel 128.189.142.254</td>
</tr>
<tr>
<td>56005</td>
<td>11:03:35.944</td>
<td>128.189.142.254</td>
<td>Name query [Short Frame]</td>
<td>ARP</td>
<td>Who has 128.189.142.147? Tel 128.189.142.254</td>
</tr>
<tr>
<td>56006</td>
<td>11:03:36.040</td>
<td>128.189.142.254</td>
<td>Name query [Short Frame]</td>
<td>ARP</td>
<td>Who has 128.189.142.147? Tel 128.189.142.254</td>
</tr>
</tbody>
</table>

**TCPdump:**

- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: DSCP (DSCP: default; ECN: dco)
- Total length: 40 bytes
- Identification: 0x507e (2054)
- Flags: 0x004 (Don't Fragment)
- Fragment offset: 0 bytes
- Time to live: 127
- Protocol: TCP (6)
- Head checksum: 0x8915 (Correct)
- Source: 128.189.142.66 (128.189.142.66)
- Destination: 207.46.106.22 (207.46.106.22)

**Transmission Control Protocol:**
Src Port: 1061 (IDLE), Dst Port: 1863 (IDLE), Seq: 1704, Ack: 4936, Len: 0
Source port: 1001 (1001)
Destination port: 1863 (1863)
Sequence number: 1704 (relative sequence number)
Acknowledgement number: 4936 (relative ack number)
Header length: 20 bytes
Flags: 0x0010 (ACK)
Window size: 65535 bytes
Checksum: Dc4e (Correct)
Objective

- Develop a tool for network visualization
  - Focus on common protocols and services
  - Focus on log files
- Our intention is to provide high level information at-a-glance
Related work

- Visual Information Security Utility for Administration Live (VISUAL) [1]
- PortVis [2]
- NVisionIP [3]
- The Spinning Cube of Potential Doom [4]
Solution

- NAV provides two overviews and a detail view
  - IP wall view displays connections between local and remote machines colour coded by port number
  - Services view contains a trellis structure of graphs displaying information based on the port number
- Users can dynamically filter on time
- Users can statically filter on a number of packet level details
IP wall view

- Displays connections between local and remote machines
- Ability to collapse and aggregate IP address ranges
- Allows connection hiding to avoid line snarls
- Displays total traffic per address/port pair
Service view

- Displays a graph for each pre-selected service only if data exists
- Graph displays traffic (bytes/s) against time
- Log based time axis can be toggled
- Service selection is user specified
Detail view

- Drag and drop from IP wall view or services view to display detailed packet information
- Displays packets for a single IP address or a single port number at a time
Evaluation

- **Strengths**
  - Good overviews of the information
  - Quickly shows active services that consume network resources

- **Weaknesses**
  - Performance/Scalability
  - Application is not feature complete
Future work

- Intrusion detection
- DNS recognition for IP addresses
- Expanded preferences
- Detect unexpected traffic
- Animation of connections on the wall view
References


