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

Ethereal

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


