NAV

Project Update

By: Meghan Allen
and Peter McLachlan

NAV Objectives

- Develop a tool for network visualization
  - Focus on common protocols:
    - TCP/IP
    - UDP/IP
    - ICMP
  - Within these protocols focus on common services
  - Focus on log files for now
- Intention is *not* to re-implement functionality in existing packet sniffers and protocol analyzers but to provide higher level information at-a-glance

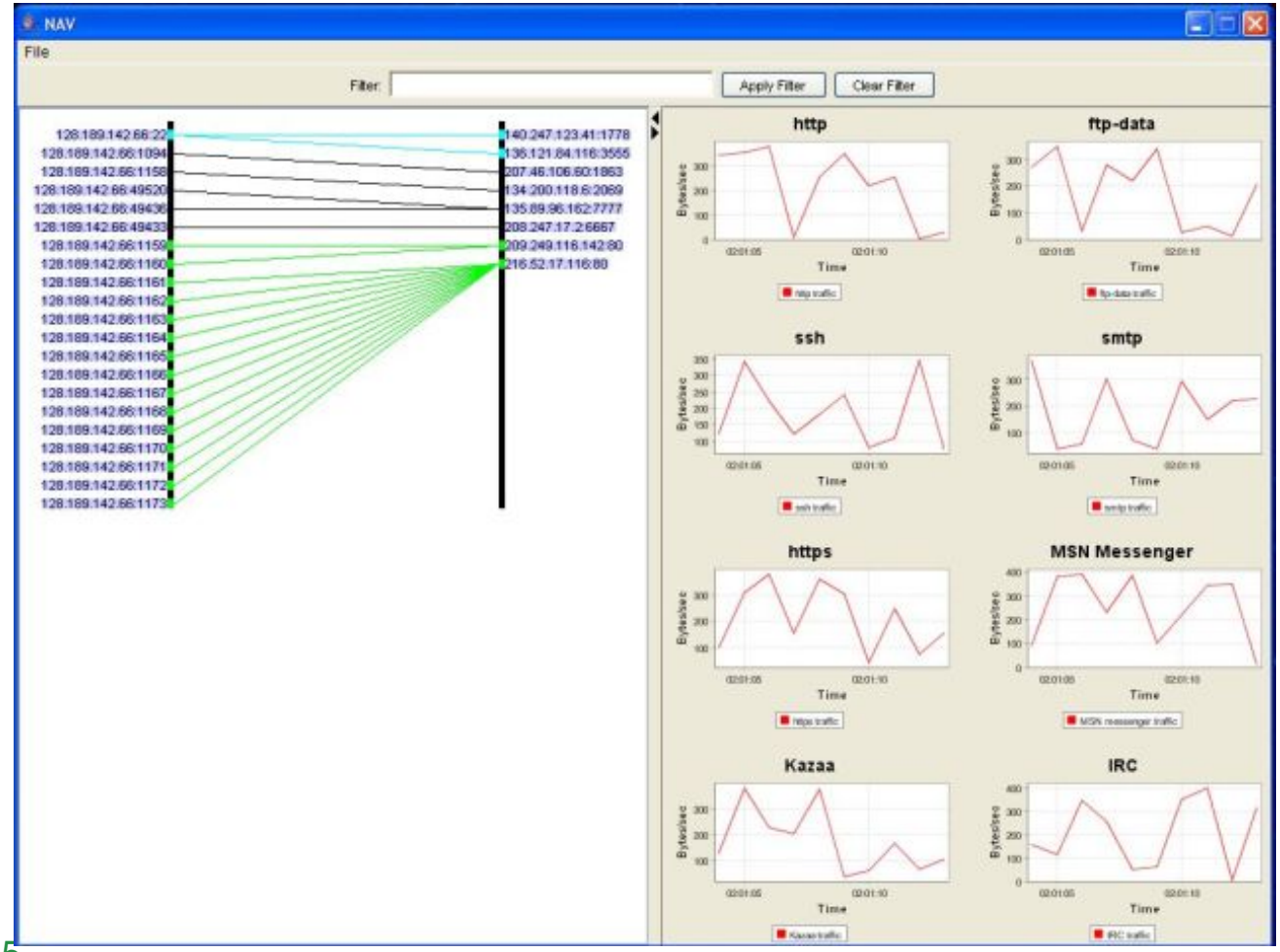
Scenario 1 – Enterprise Usage

- Security professionals need tools to help them manage the large volumes of traffic accessing their site
- They may be interested in seeing traffic access patterns, getting feedback on how heavily their site is being utilized, or doing post-mortem analysis
- The tool must allow for extensive filtering to display reduced data sets as well as provide means to ‘pop out’ important information

Scenario 2 – Home use

- Many home users now have high speed access, often this access is shared
- Viewing internet access and bandwidth usage is a good way of detecting virus or spy-ware activity
- Users may also wonder “where is all my bandwidth going?” – our user interview demonstrated this need as the user was concerned when their bandwidth was being consumed by P2P applications run by their children
- ISP’s are increasingly implementing bandwidth caps – it is useful for users to visually see how much bandwidth they are using, when they are using it, and what services are consuming the most bandwidth

NAV Solution



Implementation

- Currently the services view is implemented using the JFreeChart [1] toolkit, the InfoVis [2] toolkit may be used instead
- Network packet capture and basic log file parsing is performed using the jpcap [3] native library interface to the pcap [4] packet capture library
- Wall view is implemented in Java 2D

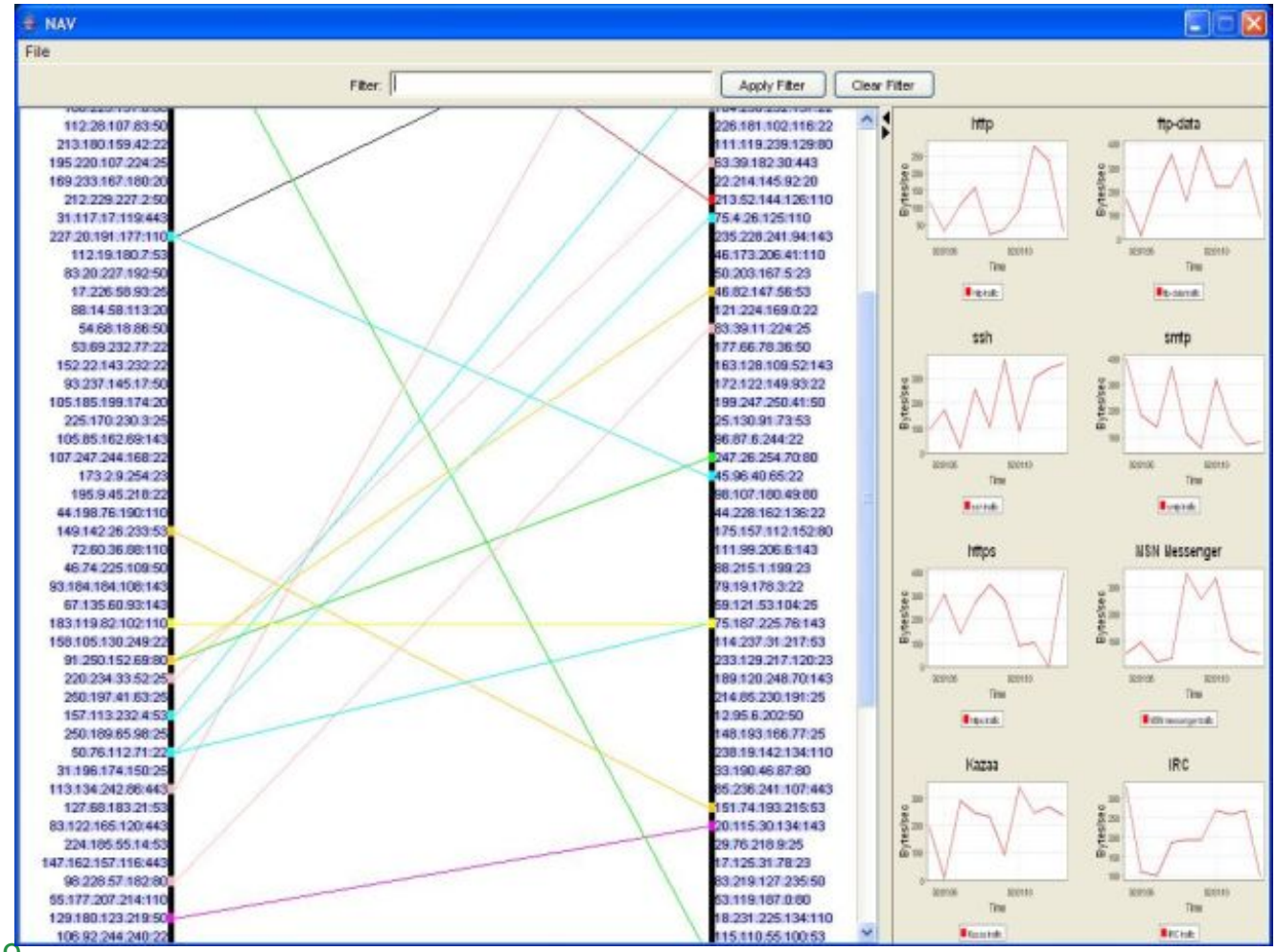
Scalability

- Both views
  - Dynamic filtering using sliders
  - Real-time analysis of data using capture interface
- Wall view
  - Bar graphs indicating total traffic transfer per host
  - Implement algorithm to minimize edge crossing
  - Ability to ‘collapse’ hierarchies of address and port ranges
- Services view
  - Logarithmic scaling of time axis
  - ‘Stretchable’ axis distortions

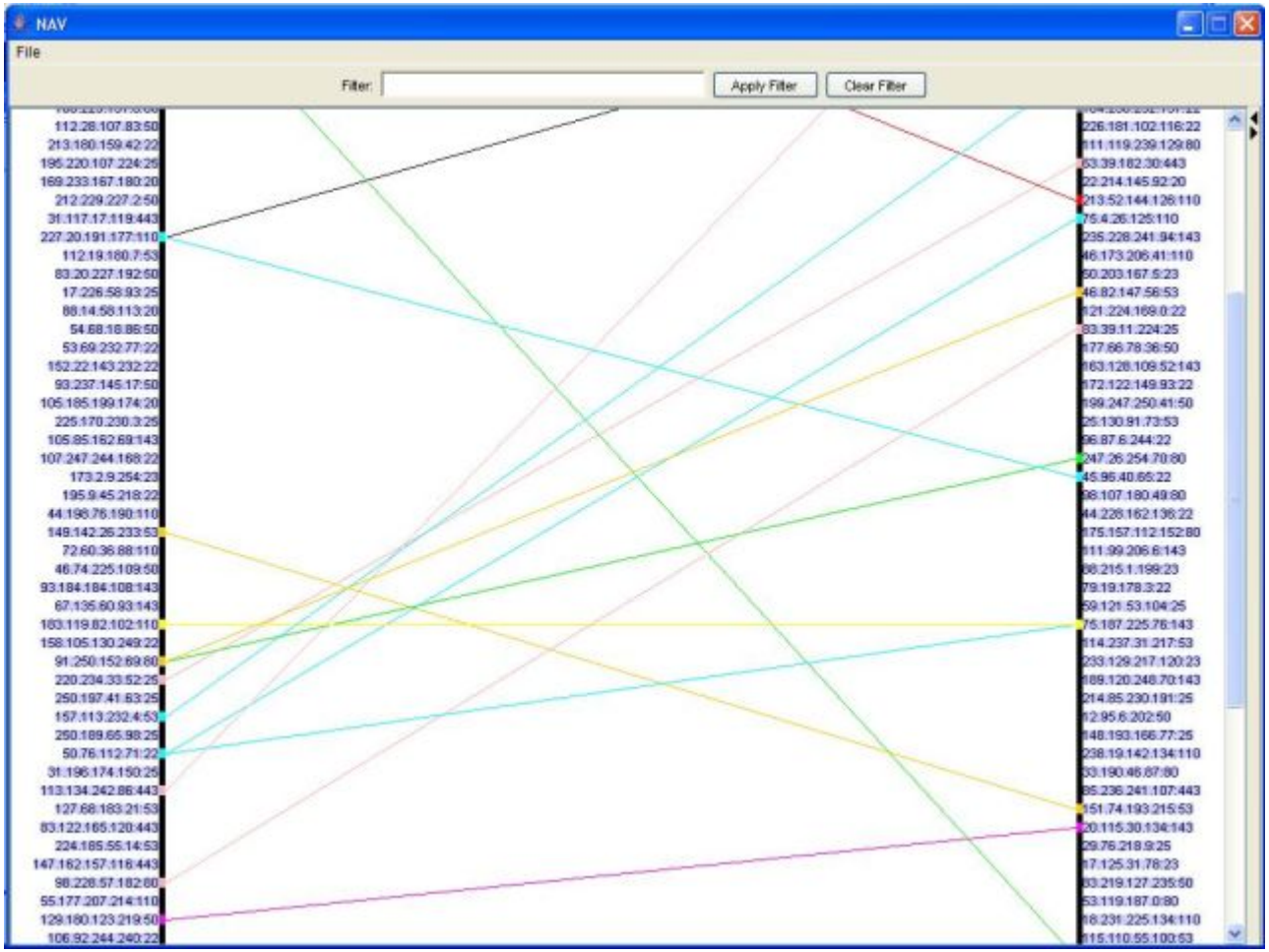
Interaction & Usability

- User preference dialogs, selecting services to be displayed, specify local IP ranges, display all local traffic
- User selectable color encoding for wall view
- Animation patterns in the wall view to show traffic flow
- VCR like ‘playback’ of the log files
- Allowing users to specify lists of hosts to which inbound connections are not expected
- Brushing and linking between the views
- Conceptual rudiments of intrusion detection

Screenshot 2



Screenshot 3

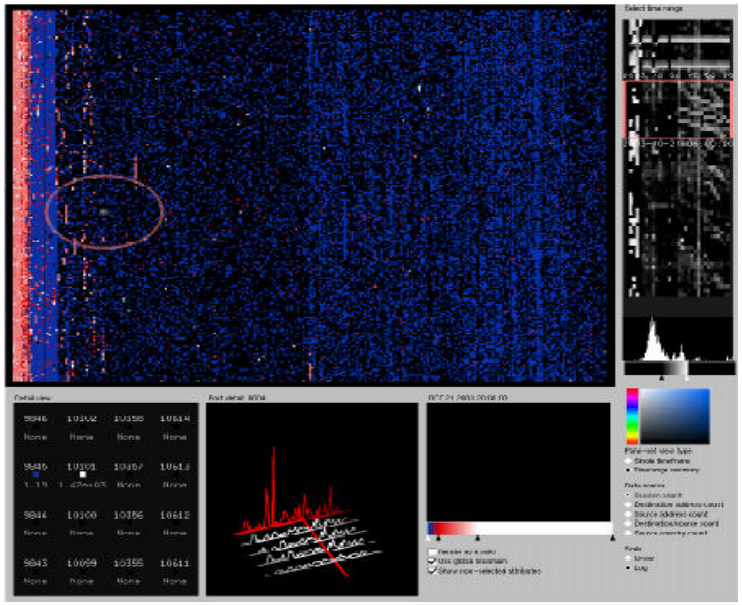


Challenges

- Poor documentation of the Infovis Toolkit; the Prefuse [5] package appears to have even less documentation
- jPCAP packet filtering does not have all the functionality we require
  - Dynamic filtering may not be able to use the native filtering interface
  - Filtering based on time is currently impossible
- Java does not support unsigned bytes and has poor support for bit level operations making filtering more challenging
- Neither implementer has extensive experience with graphics in Java
- Native library interfaces pose difficulties on diverse computing platforms (such as Sun workstations)

Related work: PortVis

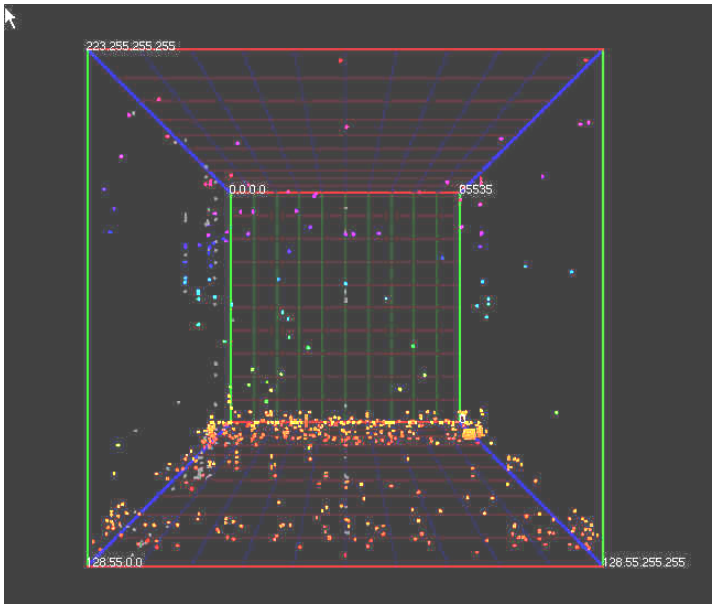
- PortVis [6] visualization of network ports published last month discusses displaying abstract security data



PortVis

Related work: Spinning Cube of Potential Doom

- Spinning cube of potential doom [7] provides an overview of the entire internet address space and aims to show malicious traffic by displaying incomplete connections (syn/fin scans)



Spinning Cube of Potential Doom

Bibliography

[1] jFreeChart. http://www.jfree.org/jfreechart/

[2] InfoVis Toolkit http://ivtk.sourceforge.net/

[3] jPCAP. http://jpcap.sourceforge.net/

[4] PCAP. http://www.tcpdump.org/

[5] Prefuse. http://prefuse.sourceforge.net/

[6] J. McPherson, K. Ma, P. Krystosk and T. Bartoletti and M. Christensen. PortVis: a tool for port-based detection of security events . Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 73-81, 2004.

[7] S. Lau. The Spinning Cube of Potential Doom. Communications of the ACM, pages 25-26, 2004.