

Network Analysis Visualization (NAV)

Meghan Allen and Peter McLachlan
December 15, 2004

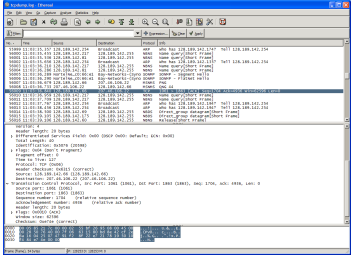
1

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

2

Ethereal



3

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

4

Related work

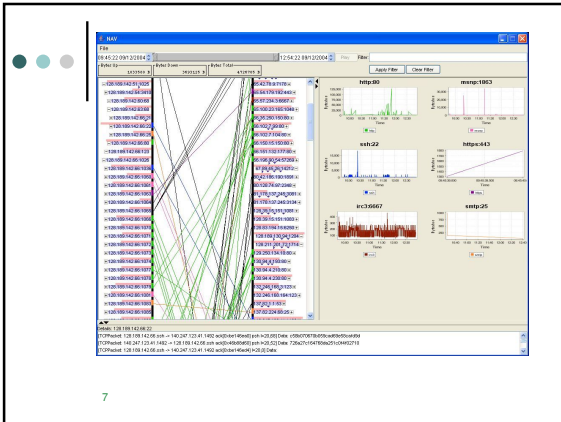
- Visual Information Security Utility for Administration Live (VISUAL) [1]
- PortVis [2]
- NVisionIP [3]
- The Spinning Cube of Potential Doom [4]

5

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

6



7

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

8

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

9

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

10

Evaluation

- Strengths
 - Good overviews of the information
 - Quickly shows active services that consume network resources
- Weaknesses
 - Performance/Scalability
 - Application is not feature complete

11

Future work

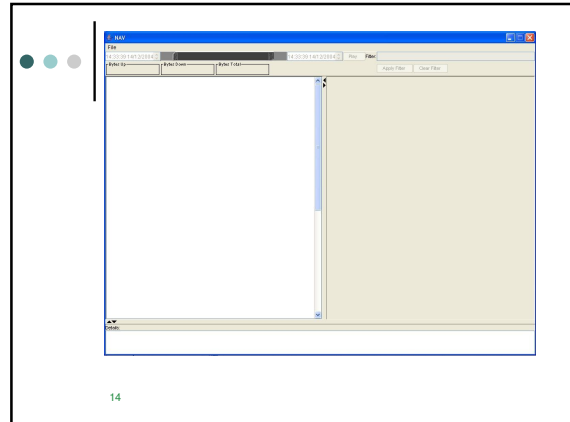
- Intrusion detection
- DNS recognition for IP addresses
- Expanded preferences
- Detect unexpected traffic
- Animation of connections on the wall view

12

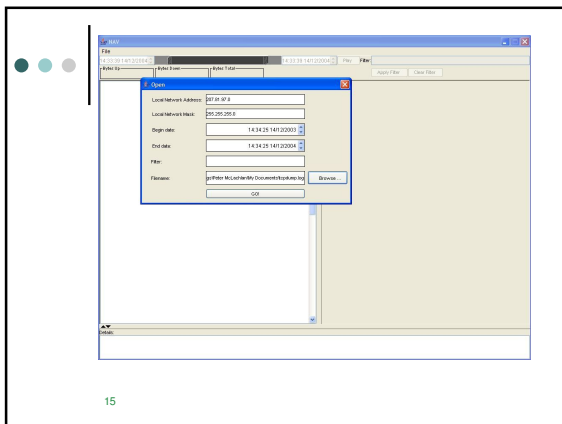
References

- [1] R. Ball, G. A. Fink and C. North, Home-centric visualization of network traffic for security administration, VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 55-64, 2004
- [2] K. Lakkaraju, W. Yurcik and A. J. Lee, NisionIP: netflow visualizations of system state for security situational awareness, VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 65-72, 2004
- [3] S. Lau. The Spinning Cube of Potential Doom. Communications of the ACM, pages 25-26, 2004.
- [4] 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.

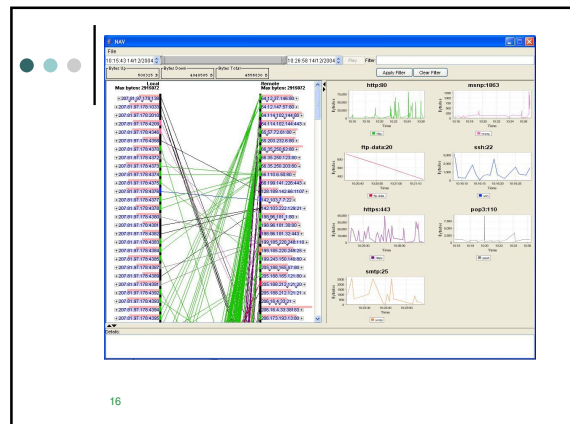
13



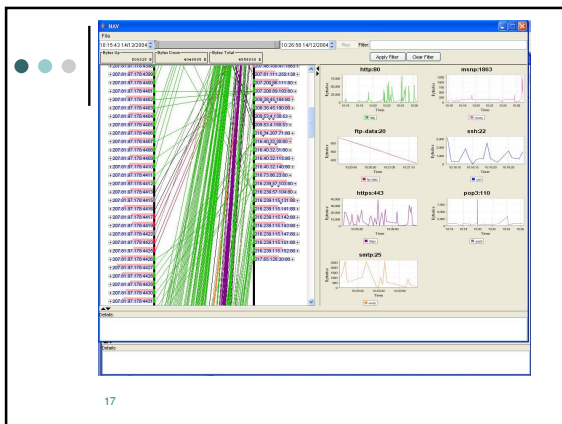
14



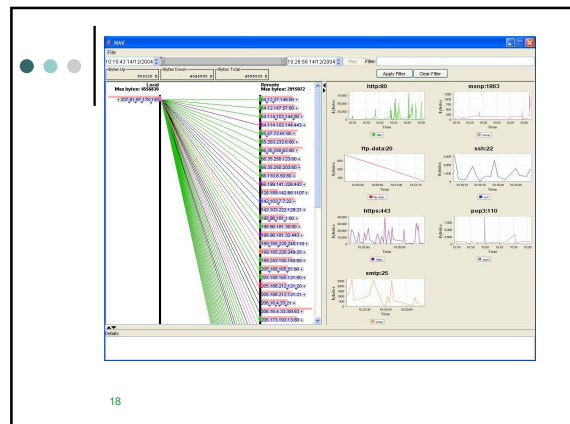
15



16



17



18

