Visualizing Real-Time Network Resource Usage

Ryan Blue, Cody Dunne, Adam Fuchs,

Kyle King, and Aaron Schulman

University of Maryland,

Dept. of Computer Science

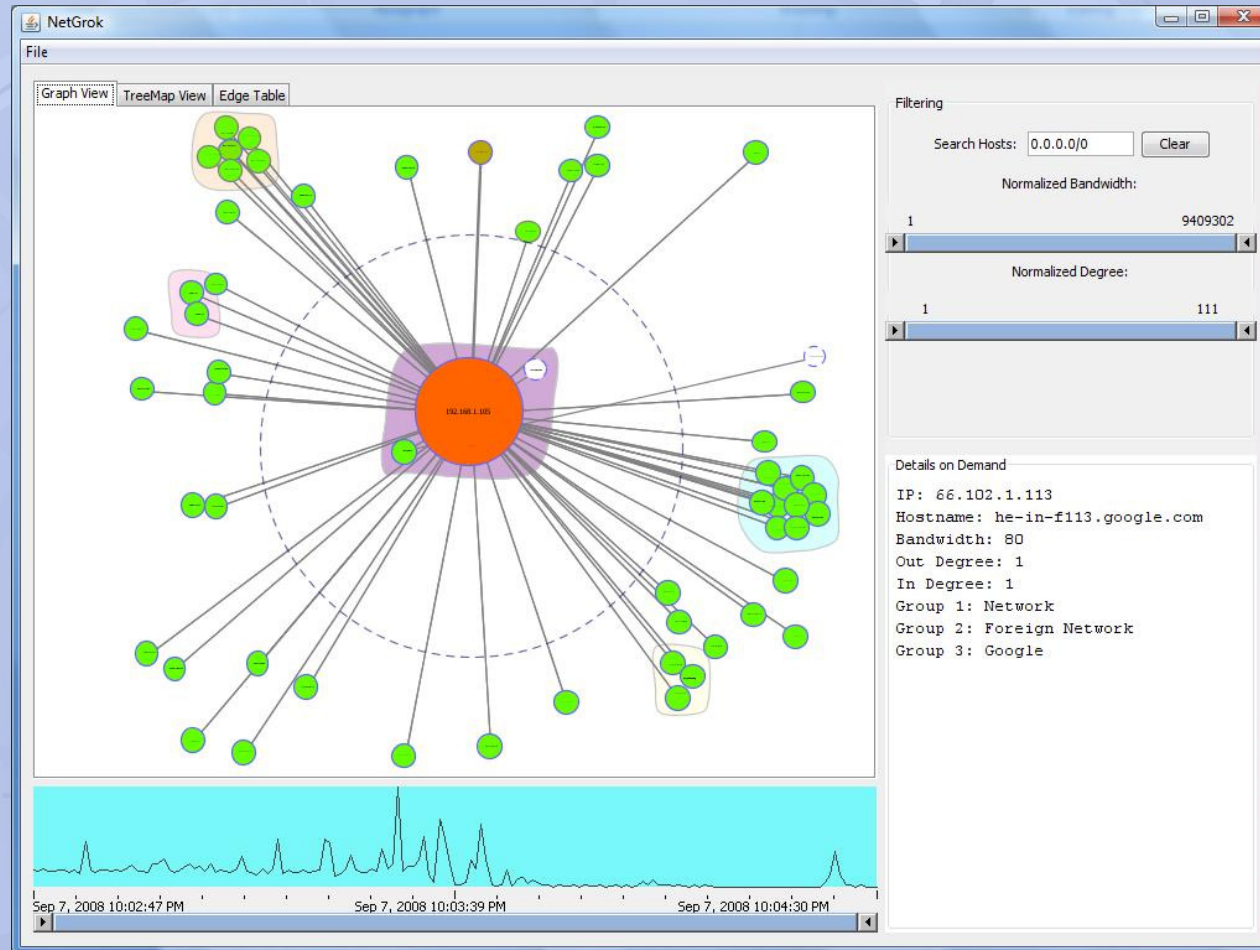Contact: cdunne@cs.umd.edu

Introduction

- Computer network data
  - Adversarial behavior
  - Configuration problems
  - Unfair resource usage
- Visualization tools
  - Too much data
  - Cluttered
  - Hard to follow
  - Primary tools are text based

Goals

- Real-time
- Visual stability
- Identify local systems
- Monitor behavior
  - Attacks
  - Topology changes
  - Unusual network usage

NetGrok

Contributions

- Hashed layout

- Grouped, home-centric layout

- Treemap links without occlusion

- Mouse-over and preferential edge display

- Visualization framework for real-time IP data

Implementation Details

- Java
- Prefuse toolkit
  - Custom data structures and visualizations
- JPCAP library
- Jigloo Eclipse plugin

Professional Feedback

- Expert user:
  - Use case meetings (2 x 1 hr + emails)
  - PCAP and live capture analysis (1 hr)
  - Likert scale questionnaire
- Positive:
  - Filter sliders, esp. time histogram
  - Intuitive layout and grouping
  - "NetGrok is excellent as a real-time diagnostic"
- Criticisms:
  - Transport layer data (TCP/UDP)
  - Dynamic grouping
  - Animations
  - Treemaps interesting but not intuitive

Future Work

- Age off old data

- More visualizations
    - Semantic substrates
    - Coarser views

- Personal security tool

Acknowledgments

- Professor Ben Shneiderman our advisor

- Brad Plecs our case study participant

- Thomas Lotze, Joonghoon Lee, Michael VanDaniker, Fatemeh Mir Rashed, Abigail Daken, Michael Lam, Huimin Guo, and Krist Wongsuphasawat our reviewers

Contact Info

- Website: www.cs.umd.edu/projects/netgrok/
- Email: cdunne@cs.umd.edu