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

Workshop on Visualization for Computer Security
September 15, 2008 Boston, MA

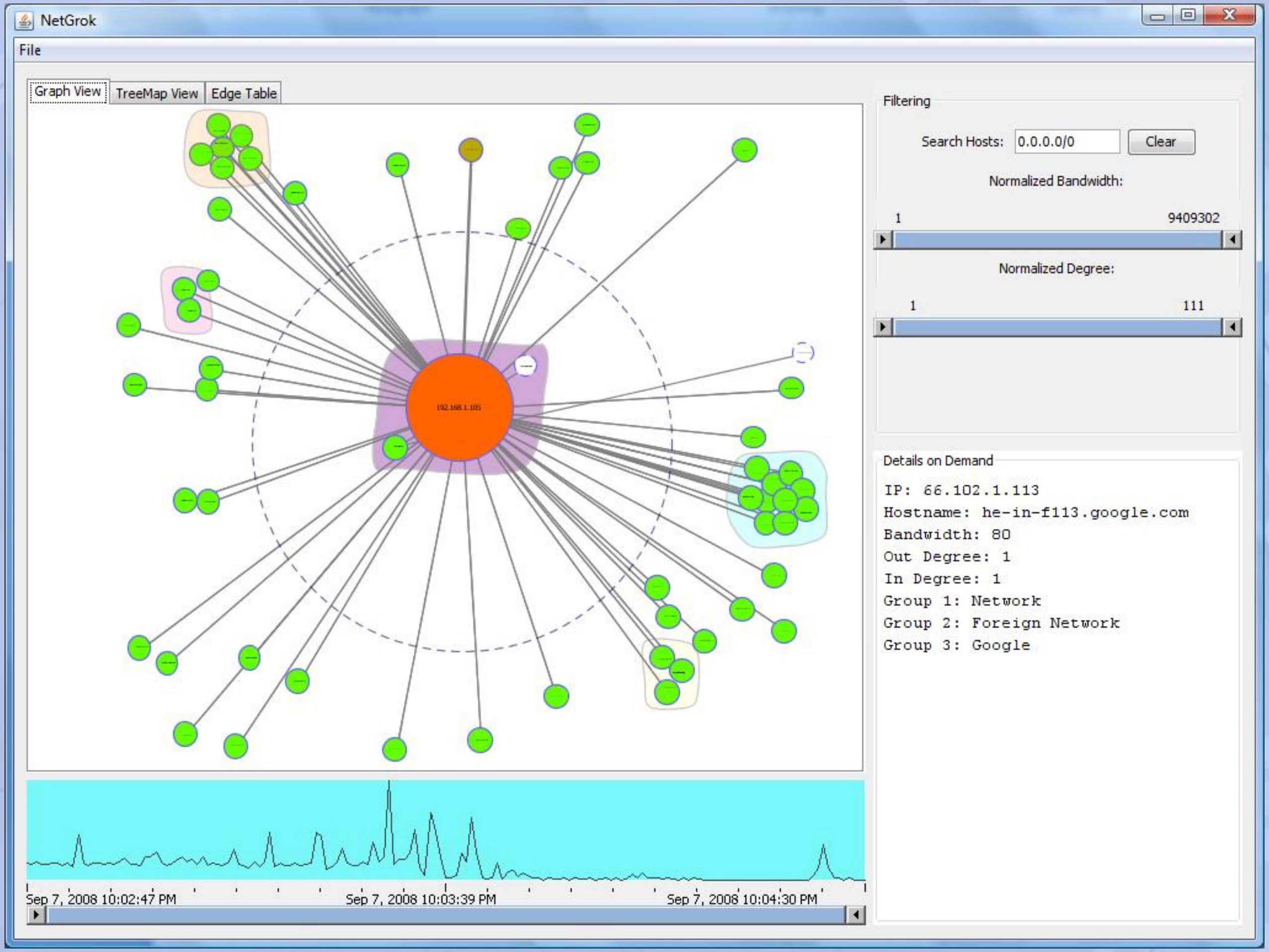
Introduction

- Computer network data is rich, and full of interesting patterns
  - Adversarial behavior
  - Configuration problems
  - Unfair resource usage
- Network administrators don’t typically use visualization tools
  - Too much data to see visually
  - Cluttered
  - Hard to follow
  - Primary tools are text based
- NetGrok brings new visualizations to network administrators

Goals

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

NetGrok



Search Hosts: 0.0.0.0/0

Normalized Bandwidth: 1 9409302

Normalized Degree: 1 111

Details on Demand

```
IP: 66.102.1.113
Hostname: he-in-f113.google.com
Bandwidth: 80
Out Degree: 1
In Degree: 1
Group 1: Network
Group 2: Foreign Network
Group 3: Google
```

http://www.youtube.com/watch?v=uCXPaNvI5Ok

Contributions

- Hashed layout for consistent node placement
- Grouped, home-centric network layout
- Treemap showing connections between nodes without occlusion
- Mouse-over and preferential display of edges reduces visual complexity
- Application of filter and selection widgets to network visualization
- Visualization framework for real-time IP data flows

Implementation Details

- Built in Java
- Visualizations and data store built primarily using the Prefuse toolkit,
  - Custom data structures and visualizations
- Packet capturing and PCAP file reading use the JPCAP library
- GUI constructed with Jigloo Eclipse plugin

Professional Feedback

- Expert user: Brad Plecs, Network Administrator for the CS Dept. at UMD
  - 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:
  - Needs to be aware of transport layer data (TCP/UDP)
  - Dynamic grouping
  - Animations are confusing, distracting, and slow
  - Treemaps interesting but not intuitive

Future Work

- Add support for aging off old data
- Add more visualizations
  - Semantic substrates for foreign host layout
  - Coarser views for larger data sets
- Personal security tool

Acknowledgments

- Professor Ben Shneiderman our advisor
- Brad Plecs for offering expert advice and participation in our preliminary case study
- Thomas Lotze, Joonghoon Lee, Michael VanDaniker, Fatemeh Mir Rashed, Abigail Daken, Michael Lam, Huimin Guo, and Krist Wongsuphasawat our class paper reviewers

Contact Info

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