OverFlow: An Overview Visualization for Network Analysis

Outline

- FloVis: crash course
- OverFlow
  - Motivation
  - Description
  - Case Study
- Future Work & Conclusions
FloVis: Crash Course

Network Visualization Framework
- Promotes extensibility
- Users create plug-ins
- Supports transitioning/pivoting
- Viz-to-viz communication
- Currently in progress...
Example: FlowBundle
FlowBundle: Drill down
Drill down: continued
Question!

What motivated the original query?

trial-and-error?

Hmmm... nothing here!

Nothing here either!

New data set

New data set

I hate this job...
OverFlow: Motivation

- We need a starting point
- We don’t want to go back to the data every time nothing is found worth investigating
  - (reduce “cognitive load” or “cognitive burden”)
- FloCon 2009: analysts described need to group IPs
  - Organizational groupings
  - Top-N lists
  - Etc.
OverFlow
Data Representation

Organize arbitrary network hierarchies:

- **By hand:**
  1. 192.168.0.0/16
  2. 192.168.2.0/24
  3. 192.168.5.0/24

- **Or:**
Visualizing Hierarchies
Visualizing Volumes
Visualizing Volumes
Visualizing Volumes
Visualizing Communications
Transitioning Over Time
Case Study

Network:
- /17
- Separated into 3 hierarchies:
  - Admin, Security, and wlan (public access)
  - 1 other group introduced for ‘outside’ IPs

Data
- Protocol/volume aggregates
  - SiLK tools used to generate protocol bags
Case Study

Should we drill down here?

Volume:BYTES

111.222.235.167
Case Study
Case Study

Unexpected SSH traffic
Case Study
FloVis: Context
Future Work
Conclusions

Two accomplishments:

1. Overview of network hierarchies
   - User-defined

2. High-level view of simple communication characteristics (e.g., volumes, connections)
   - Assists the analyst in focusing attention
Learn more...


http://www.flovis.net

QUESTIONS?