Security Visualization with FloVis

Teryl Taylor, Diana Paterson, Joel Glanfield, Stephen Brooks, Carrie Gates and John McHugh
Agenda

- Need
- Approach - FloVis Framework
- Activity Plot
- FlowBundle
- NetBytes Viewer
- Conclusions and Future Work
Need

- Multiple organizations being monitored
- Flow level data only – highly aggregated
- Over 1 billion flows per day
- > 16 million IP addresses
- Too few analysts
- No time for training

* Looking for the monkey in the boat.
Approach

- Take a visual analytics approach to investigating data
Approach
Approach

- Create a visualization suite:
  - to help identify intrusive patterns
  - to obtain a general understanding of the network
- Develop a generic framework to support multiple visualizations and the ability to easily add more
- Investigate and apply new visualization techniques to deal with typical problems of current techniques
- Closer integration (but not dependent) with the SiLK tool suite
System Requirements

- Use SiLK data
  - So, unidirectional flow data only

- Scalability – 1.5 billion flows per day!

- Ability to detect patterns that are *not* detected currently through other means
  - E.g., NOT scans! 😊
FloVis Framework

Plugin

EventManager

Chooses Plugin

Generates Event

NetBytes Viewer Plugin
FlowBundle Plugin
Activity Viewer Plugin
Framework Interface

Creates

PanelContent: NetBytes, FlowBundle, Activity Viewer