Summary

Stephen Brooks, Carrie Gates, John McHugh
Conclusions

- FloVis is an extendable framework for network security visualizations
- Integrates with SiLK
- Currently FlowBundle, NetBytes Viewer, Activity Plot
Benefits

Gain Insight
- Better understand own network
- Recognize when something has changed
- Know when 1 org is different from others

Easily detect new patterns / attacks
- Take advantage of people’s strengths
- Do not waste people’s time
Future Work

• Further integration with SiLK (possible toolbox)
• Always looking for new visualizations
  • Metrics for prioritizing visualization development
• Test on other networks
• User feedback and user studies
• Develop open source release of framework and visualizations
Acknowledgements

- Ron McLeod of Telecom Applications Research Alliance (TARA)
- CA Labs
- Natural Science and Engineering Research Council of Canada (NSERC)
- Dalhousie University
Related Work: Connection Based

- Rumint/VisFlowConnect
  - Parallel axes graphs
- VISUAL
  - Modified node-link graph
- Flamingo
  - 3D quad tree based parallel axis
- TNV
  - Focus + context connections
- SeeNet
  - Geographical node-link graph.
Related Work: Matrix/Scatter plot

- 2D/3D matrices mapping IP octets/ports/packets:
  - Koike et al. in their 2005 paper “Visualizing Cyber Attacks Using an IP Matrix”
  - Spinning Cube of Potential Doom (Lau)
  - PortVis (McPherson et al.)
  - NVisionIP (Lakkaraju et al.)
  - Heatmaps (Wright et al.)
References


References


