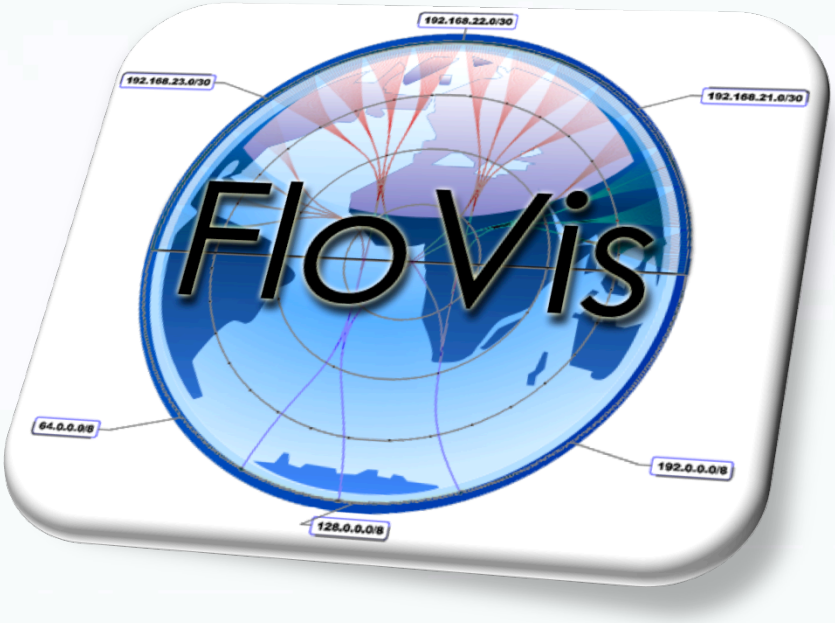


Summary

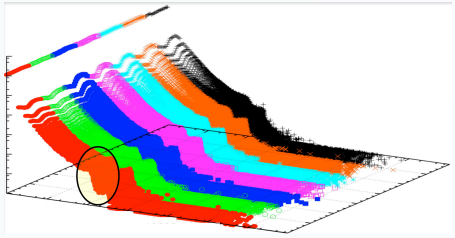
Stephen Brooks, Carrie Gates, John McHugh

Conclusions

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

Benefits

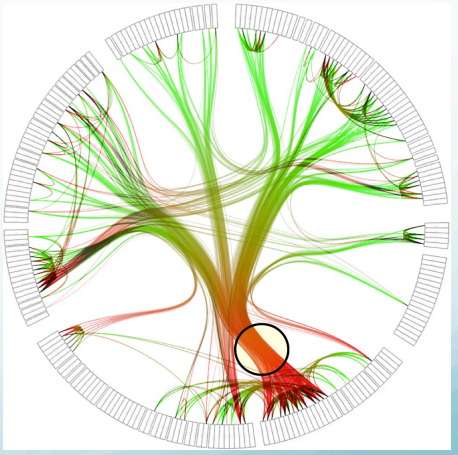
Gain Insight



- 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

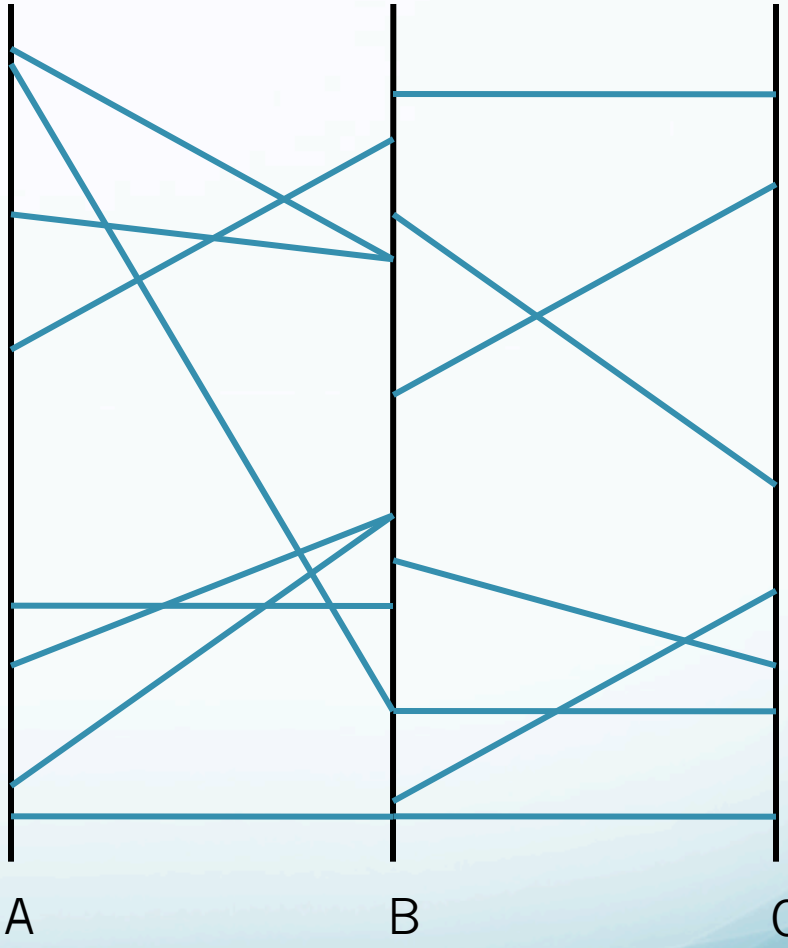
- Further integration with SiLK (possible toolbox)
- Always looking for new visualizations
  - Metrics for prioritizing visualization development
- Test on other networks
- User feedback and user studies
- Develop open source release of framework and visualizations

Acknowledgements

- Department of Homeland Security under Contract No. N66001-08-C-2032.
- Ron McLeod of Telecom Applications Research Alliance (TARA)
- CA Labs
- Natural Science and Engineering Research Council of Canada (NSERC)
- Dalhousie University

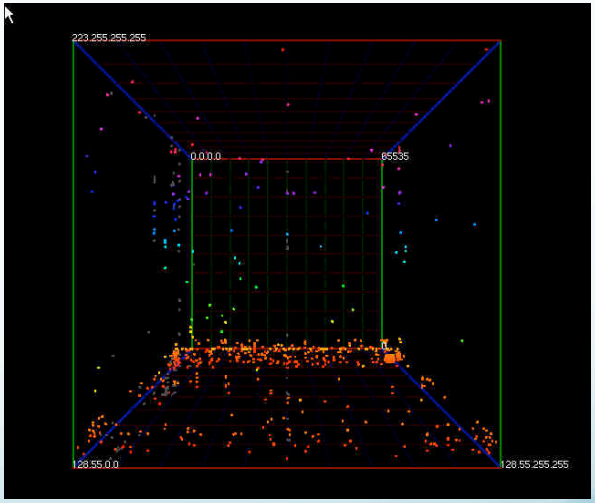
Related Work: Connection Based

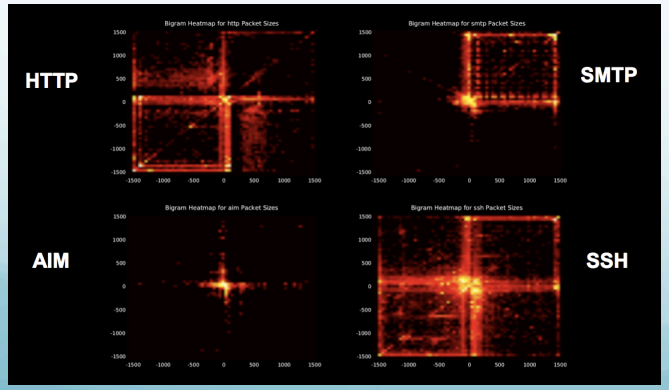
- Rumint/VisFlowConnect
  - Parallel axes graphs
- VISUAL
  - Modified node-link graph
- Flamingo
  - 3D quad tree based parallel axis
- TNV
  - Focus + context connections
- SeeNet
  - Geographical node-link graph.



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

- John R. Goodall, Wayne G. Lutters, Penny Rheingans, and Anita Komlodi. *Focusing on Context in Network Traffic Analysis*. IEEE Computer Graphics Applications, 26(2):72–80, 2006.

- Kiran Lakkara ju, William Yurcik, and Adam J. Lee. *NVisionIP: Netflow Visualizations of System State for Security Situational Awareness*. In VizSEC/DMSEC '04: Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, pages 65–72, Washington DC, USA, 2004.

- Koike, H., Ohno, K., and Koizumi, K. 2005. *Visualizing Cyber Attacks using IP Matrix*. In Proceedings of the IEEE Workshops on Visualization For Computer Security (October 26 - 26, 2005). VIZSEC. IEEE Computer Society, Washington, DC, 11.

- Stephen Lau. *The Spinning Cube of Potential Doom*. Communications of the ACM, 47(6): 25– 26, 2004.

- Jonathan McPherson, Kwan-Liu Ma, Paul Krystosk, Tony Bartoletti, and Marvin Christensen. *PortVis: A Tool for Port-based Detection of Security Events*. In VizSEC/DMSEC '04: Pro- ceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, pages 73–81, Washington DC, USA, 2004.

References

- J. Oberheide, M. Goff, and M. Karir. *Flamingo: Visualizing Internet Traffic*. In Proceedings of the 10th IEEE/IFIP Network Operations and Management Symposium, pages 150–161, 2006.

- Teryl Taylor, Diana Paterson, Joel Glanfield, Carrie Gates, Stephen Brooks, and John McHugh. *FloVis: Flow Visualization System*. To appear at the Cybersecurity Applications and Technologies Conference for Homeland Security (CATCH) 2009, Washington, DC. March 3-4, 2009.

- Wright, C. V., Monrose, F., and Masson, G. M. 2006. *Using visual motifs to classify encrypted traffic*. In Proceedings of the 3rd international Workshop on Visualization For Computer Security (Alexandria, Virginia, USA, November 03 - 03, 2006). VizSEC '06. ACM, New York, NY, 41-50.

- Xiaoxin Yin, William Yurcik, Michael Treaster, Yifan Li, and Kiran Lakkara ju. *VisFlow-Connect: Netflow Visualizations of Link Relationships for Security Situational Awareness*. In VizSEC/DMSEC '04: Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, pages 26–34, Washington DC, USA, 2004.