Real-Time Visualization of Network Behaviors for Situational Awareness

Daniel Best {daniel.best@pnl.gov}
Pacific Northwest National Laboratory

Shawn Bohn, Douglas Love, Adam Wynne, William Pike
Challenges to overcome

- Thousands of flow records per second
  - More network flow data than a human can possibly review
- Real-time availability
  - Knowing what is happening as it’s happening
- Making sense of it all
  - What is normal, is this activity expected?
Our contributions

► Traffic Circle
  ■ Visualization for situational awareness

► Correlation Layers for Information Query and Exploration (CLIQUE)
  ■ Network behavior visualization using LiveRac interface

► Middleware for Data-Intensive Computing (MeDiCi)
  ■ Data pipeline
CLIQUE: Find a starting point

- Behavior baseline for actors
  - Creates statistical model of what is normal for a given actor and category set
  - Visualizes the distance from normal activity
- Arbitrary actor hierarchy
  - Groups of IP addresses or just a single IP address
  - Analyst independent, can be shared
- Interactive interface which highlights thresholds and provides semantic zooming
CLIQUE: Behavior

Current

Web:  ABBCABABD
SSH:   BBBCCCAABA
FTP:   DDDDCDCDDB

Historic

Web:  ABBCABABD
SSH:   ABBCDCABA
FTP:   DDDDCDCDDB
Traffic Circle: Find understanding

- Interactive and scalable flow plot visualization
  - Capable of visualizing 100 Million + flow records
  - Allows exploration of the dataspace and draws out features
  - The more memory and pixels, the more the tool can display

- Layer style filters
  - Color encoding
  - Data hiding

- While listening to incoming flow records, Traffic Circle will spin clockwise on a heartbeat
Middleware for Data-Intensive Computing (MeDICi)

- Publish and subscribe event based system
  - Published to database in addition to tools
- Components are code base agnostic
  - Easily tie in modules needed for visualizations such as aggregators and statistical analysis
- Highly scalable
  - Best run of 2781 records per second (240 million per day) on a desktop workstation (Dell 7500)
Implemented MeDICi Information Framework
Future Directions

- Develop a predictive capability
- Explore extensions to other domains
  - Financial fraud detection
  - SCADA system reliability and security
- Enable heterogeneous data visualization
- Explore other behavioral trending algorithms
How to get in touch

Daniel Best
daniel.best@pnl.gov