Situational Awareness Through Network Visualization
Pacific Northwest National Laboratory
Daniel M. Best
Bryan Olsen

11/25/2014
Introduction

Daniel Best – Cyber Security Researcher
• Visual Analytics Group
• Extensive application design and development experience
• Cyber security visual analytics research focus
• Graph analytics secondary research focus
• Founder of the Patchwork Cyber Analytics Pwnage Squad (PCAPS)

Bryan Olsen – Cyber Security Engineer
• Data Sciences & Analytics Group
• Research focus on enabling cyber analytics using high performance architectures
• Integration of visual analytic tools with parallel database architectures
• Research behavioral signatures of cyber attacks
• Applied OLAP techniques to cyber domain to enable high level trending and data exploration

Operated by Battelle since 1965
Unique S&T strength and capabilities
Mission-driven collaborations
Need

• Identify when network activity deviates from expected behavior
  – Is today different from yesterday?

• Explore large volumes of data to identify patterns, unexpected activity, and indicators of attack
  – Analyzing raw network flow records is infeasible

• Capabilities to assist in understanding of network and typical network communication patterns
  – Move away from reacting to the known, to exploring the unknown
Approach

• Combine summarization of behavior with scalable visualization of raw network flow
• Be adaptable to different networks (network flow format, database technology, etc..)

• Visualize normal vs. abnormal activity
• Configurable hierarchy of IP addresses for logical groupings
• Scale charts based on available space
  • More data as more space is available

• Visualize millions of network flows on one display
• Color encode traffic features for rapid identification of patterns
• Drill down from visual patterns to raw data
clique

- **CLIQUE builds behavioral baselines for hosts or groups**
  - A model of predicted activity based on past activity compared to current activity
  - CLIQUE helps visualize the deviation of an actor from this predicted activity.
  - Our models are built from connection-level variables rather than content – it’s fast.

- **Adaptive thresholds** alert analysts to off-normal behaviors, down to the level of the individual host.

- **Trade model expressiveness for ease of computation**
  - CLIQUE relies on counts (payloads, transactions, etc) that are quick to measure and easy to distribute
  - **Easy to compute** means we can also be flexible – users can ask for new models to be created on the fly
traffic circle

• A tool for **interacting** visually with **massive** log tables (up to hundreds of millions of rows)

• Useful for quickly identifying features and patterns
  – What does the normal pace of activity look like?
  – What sort of traffic does a sensor generate?
  – What “odd features” are in a log that we didn’t know to look for?
Benefits

• **Efficient identification of deviations from expected activity**
  – Shorten analysis time by highlighting what to look at first
  – Reduce the amount of data review required for deeper investigation
  – Understand typical network behavior patterns

• **Visually interact with network flow at scale**
  – Investigate millions of network flows at once
  – Expose features in traffic that would otherwise be missed
  – Gain deeper insight into communications

• **CLIQUE and Traffic Circle provide a means to understand an enterprise network and assist investigation**
Competition

- VisAlert: Network visualization tool that correlates alert logs using what, when, and where attributes
- Portvis: Visualization of network communication data focusing on ports
- Time-Based Network Visualizer (TNV): Depicts network traffic by visualizing packets and links between local and remote hosts
- VIAssist: Network and geospatial visualization operating on large multi-dimensional datasets for cyber defenders

We provide a behavioral investigation and network flow exploration process unlike our competitors.
Status

- Improving **clique**
  - Configurability through wizards
  - Greater flexibility for data sources
    - X and Y axis configurable
    - Category field selectable
- Migrating **traffic circle**
  - One environment to enable better workflow
  - Infrastructure in place
  - Initial view started
- Increasing user base
  - Added capability to view more than just network flow (SCADA, Financial, etc.)
Status

• Usability Assessment
  – Working on workflow and ease of use
  – Better menus and layout

• Testing
  – Automated user testing added to build server
    • User interaction scripted through Jelly
  – Red teaming planned when appropriate (Excelis)
Transition to Practice

• DHS S&T
  – Deployed for the past year
  – Used on a daily bases for operational tasks
  – Great feedback and first hand use cases

• NBACC
  – Deployed for the past year
  – Transitioning to greater usage

• Commercialization
  – Identified potential transition partner
Thanks

Daniel M. Best  
Cyber Security Researcher  
VISUAL ANALYTICS  
Phone: (509) 372-6728  
daniel.best@pnnl.gov

Bryan Olsen  
Cyber Security Engineer  
DATA SCIENCES & ANALYTICS  
Phone: (509) 372-6268  
bryan.olsen@pnnl.gov