CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

Scalable Modeling of Network Flows [CLIQUE & Traffic Circle]

How much better could you defend your network if you knew how it looked and behaved?

Pacific Northwest National Laboratory
Daniel M. Best, Bryan K. Olsen

09/03/2013

Homeland Security
Science and Technology

Team Profile

Pacific Northwest National Laboratory

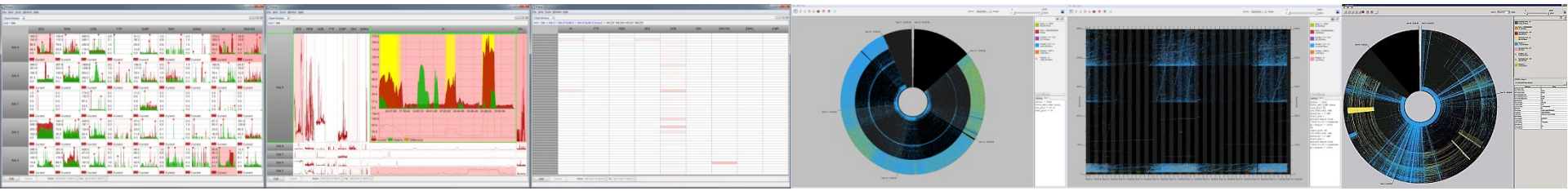
- Operated by Battelle since 1965
- Unique S&T strengths and capabilities
  - DOE's Cyber Intelligence Center
  - Control Systems Security
  - Component Security
  - Cyber Analytics
  - Bio-Inspired Cyber Security
  - Data Intensive Computing
- Mission-driven collaborations with government, industry and academia

Vision

PNNL will be recognized worldwide and valued nationally and regionally for leadership in science and for rapidly translating discoveries into solutions for challenges in energy, national security, and the environment.

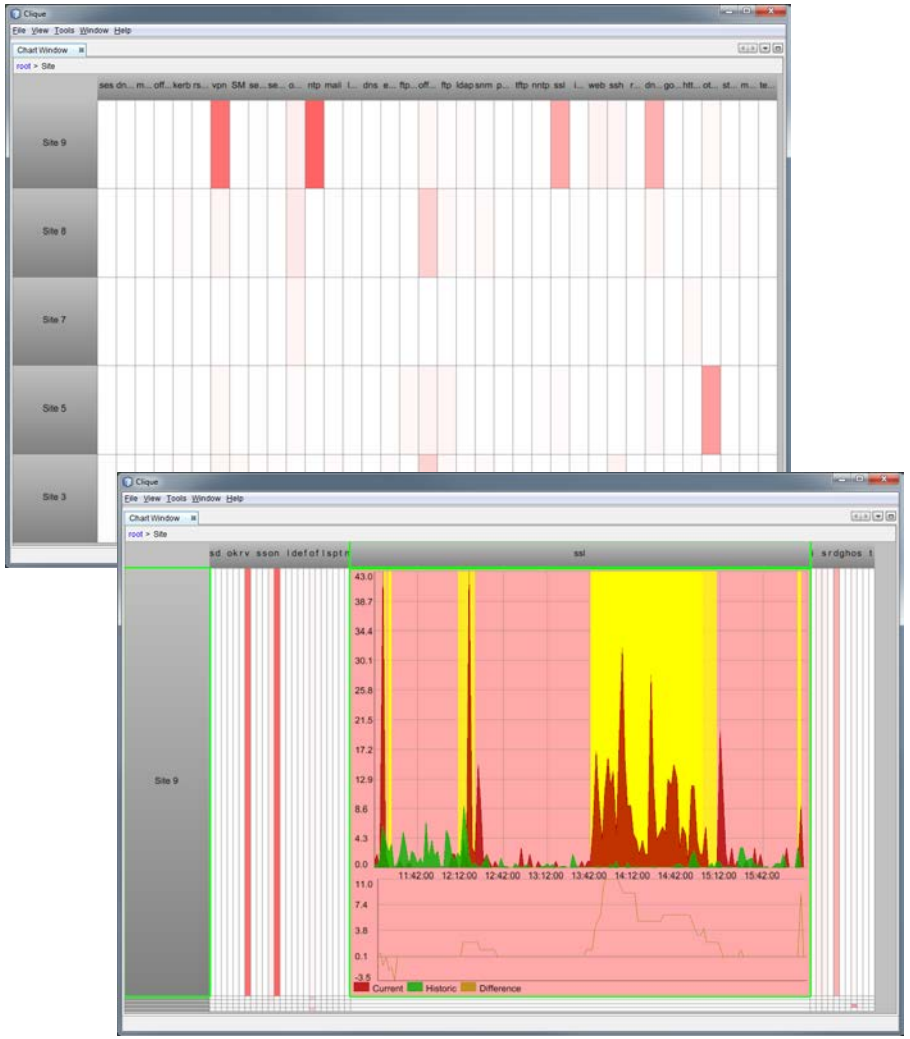
Customer Need

- **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



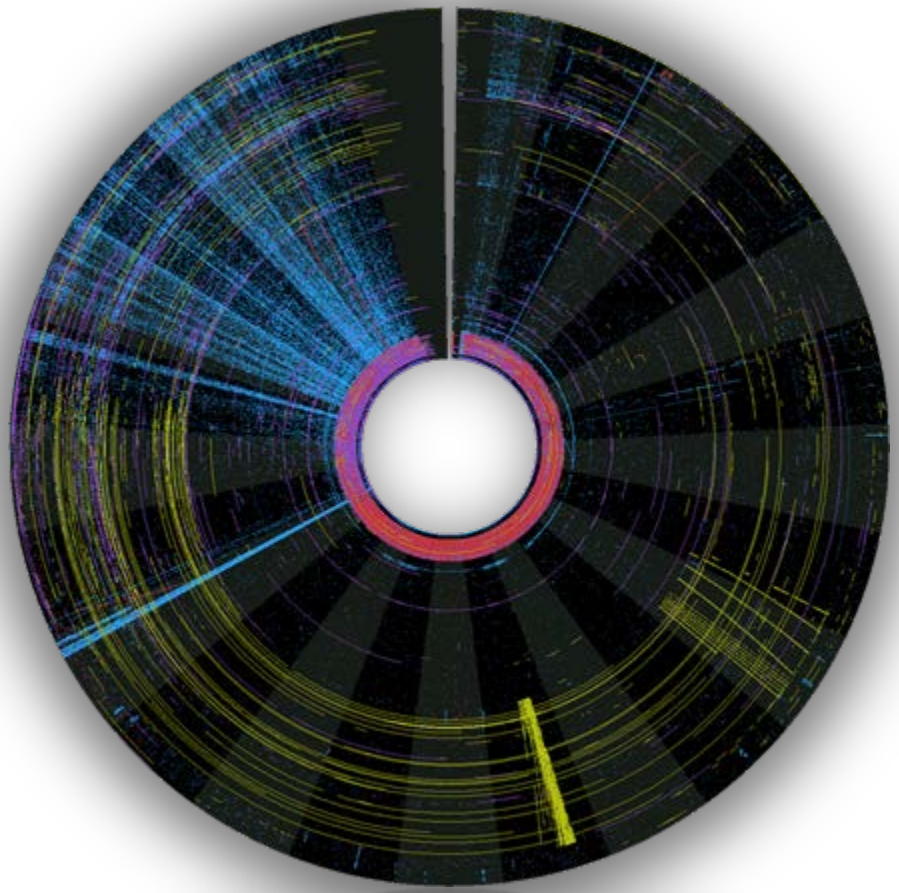
Approach : CLIQUE

- **Behavioral baselines for hosts or groups**
  - Compare minute of week with previous 3 weeks
  - Built for each group and category
  - Quick calculation of deviation from expected
- **Color indicates level of deviation**
  - Quickly alert analysts to off-normal behaviors
  - From site wide to individual hosts
- **Intuitive exploration of activity**
  - Progressive disclosure
  - Maintain context while exploring



Approach : Traffic Circle

- **Leverage human cognition to identify patterns**
  - Temporal cadence of traffic
  - View data in multiple ways
  - Identify “odd” features
- **Interact visually with massive amounts of data**
  - Up to hundreds of millions of rows
  - Highlight and filter data based on attributes
  - Zoom and select to explore
  - Statistics provided for selection



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**

Current Status

- **Pilot deployments**
  - National Biodefense Analysis and Countermeasures Center (NBACC)
    - Established January 2013
  - SciTech & Labnet data at DHS S&T
    - Established July 2013
  - National Collegiate Cyber Defense Competition (NCCDC) 2013
    - Deployed a network capture pipeline from the provided network tap

- **Traffic Circle and CLIQUE re-architecture**
  - Update code base to increase flexibility and robustness of the tool
  - Implement in a common architecture

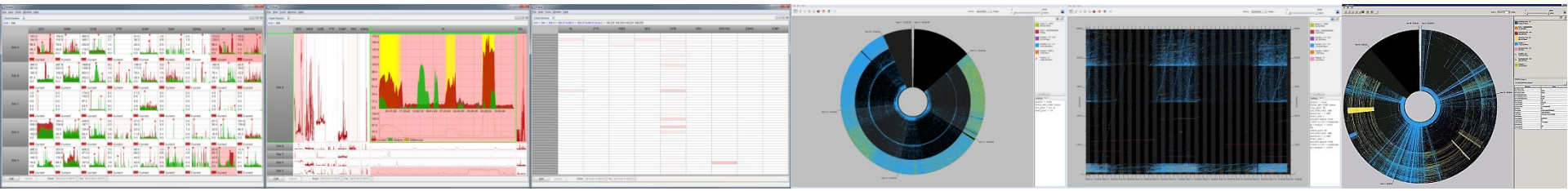
- **Commercialization roadmap**
  - Open source, Government Use, Licensing, or combination

Next Steps

- **Traffic Circle version 2**
  - Integrated environment with CLIQUE
- **Complete commercialization roadmap**
  - Begin transition to identified mechanism
- **Continued support of pilot activities**
  - NBACC, SciTech, and NCCDC
- **Identify organizations and funding for new pilot opportunities**
  - Expand deployments and operational utility
- **Quantify metrics through engagements with pilot partners and operational users**
  - Establish compelling benefits (return on investment)

Contact Information

- Daniel M. Best
  - Daniel.Best@pnnl.gov
  - Daniel.Best@st.dhs.gov
- Bryan K. Olsen
  - Bryan.Olsen@pnnl.gov
  - Bryan.Olsen@st.dhs.gov



Competition?

- **VisAlert [3]**
  - Network visualization tool that correlates alert logs using what, when, and where attributes
- **Portvis [4]**
  - Visualization of network communication data focusing on ports
- **Time-Based Network Visualizer (TNV) [2]**
  - Depicts network traffic by visualizing packets and links between local and remote hosts
- **VIAssist [1]**
  - 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**

Citations

1. Goodall, J. R., & Sowul, M. (2009). VIAssist: Visual analytics for cyber defense. *Technologies for Homeland Security, 2009. HST'09. IEEE Conference on* (pp. 143–150). IEEE.
2. Goodall, J. R., Lutters, W. G., Rheingans, P., & Komlodi, a. (n.d.). Preserving the big picture: visual network traffic analysis with TNV. *IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05).*
3. Livnat, Y., Agutter, J., Moon, S., Erbacher, R. F., & Foresti, S. (2005). A visualization paradigm for network intrusion detection. *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC* (pp. 92–99). IEEE. doi:10.1109/IAW.2005.1495939
4. Mcpherson, J., Krystosk, P., & Livermore, L. (2004). PortVis : A Tool for Port-Based Detection of Security Events.