Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

Safeguarding Cyber Systems with Visualization

Traffic Circle and CLIQUE

CHALLENGE

Protecting communications networks against attacks that aim to steal information, disrupt order, or harm critical infrastructure requires the collection and analysis of staggering amounts of data. The ability to detect and respond to threats quickly is a paramount concern that spans government, utilities, financial and private sectors. These organizations share a common burden of identification of threats buried within billions of network transactions each day. To better equip analysts, state-of-the-art data intensive visual analytics tools are needed to address the unique challenges within cyber security.

CAPABILITY

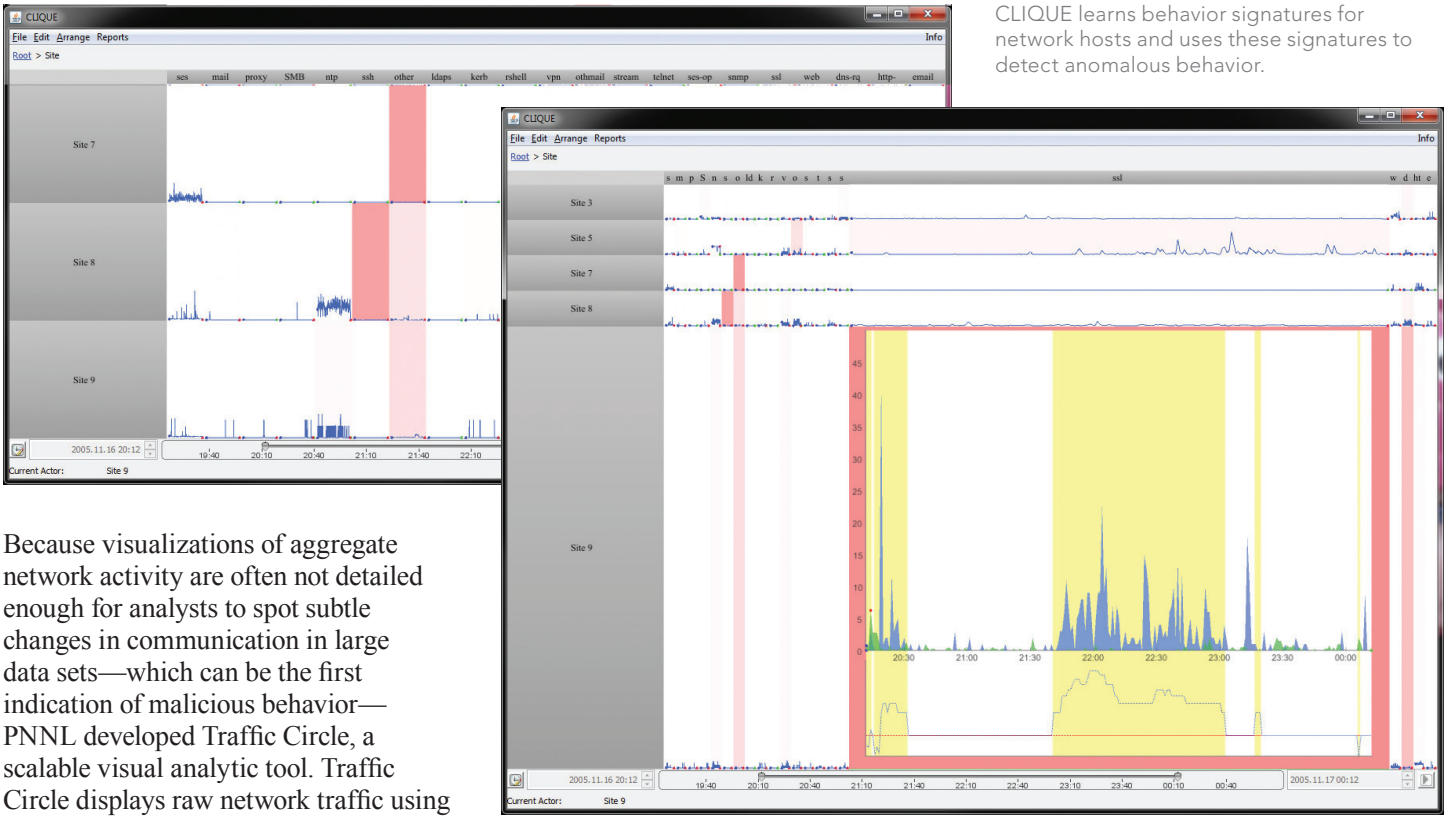
Researchers at the Pacific Northwest National Laboratory have developed two innovative visual analytics tools, which can leverage data intensive architectures that enable analysts and provide visibility and command of their data in ways not previously possible. Together, the tools support an investigative workflow.

PNNL's scalable cyber visualization tools offer insight into massive, streaming data sets, helping users discover early indicators of potentially malicious activity.

The Correlation Layers for Information Query and Exploration (CLIQUE) tool displays high-level overviews of network traffic using a new behavioral model-based anomaly detection technique. The CLIQUE system builds models for learning and classifying expected behavior of individual hosts on a network and compares these modeled behaviors to current data to generate early indicators of "non-normal" network activity.

The effectiveness of CLIQUE is enhanced by visualization features that allow the analyst to compare the anomalous activity to normal conditions. Users can navigate through their data temporally, viewing time periods as short as a few minutes or as long as several weeks. CLIQUE models help analysts to see departures from normal behavior at any time scale. Analysts also can drill down to view detailed displays of network activity and spot the machines, buildings, sites, or other sources of traffic behaving anomalously.

U.S. DEPARTMENT OF ENERGY



CLIQUE learns behavior signatures for network hosts and uses these signatures to detect anomalous behavior.

Because visualizations of aggregate network activity are often not detailed enough for analysts to spot subtle changes in communication in large data sets—which can be the first indication of malicious behavior—PNNL developed Traffic Circle, a scalable visual analytic tool. Traffic Circle displays raw network traffic using multiple time-based views and supports hundreds of millions of communications events in a single view. Traffic Circle enables analysts to view individual communication patterns that appear suspicious.

Like CLIQUE, Traffic Circle accommodates streaming data. As new network transactions occur, Traffic Circle displays them on a moving timeline. Via the Traffic Circle "time wheel," analysts can dynamically zoom through data spanning months or years in just seconds. The tool also allows for sophisticated filters that highlight important patterns in the traffic.

IMPACT

The interoperability between Traffic Circle and CLIQUE enables users to readily move data from one program to another at their desktop, allowing users to move seamlessly from high-level views of billions of transactions in CLIQUE down to detailed representations in Traffic Circle. The result is significantly improved situational awareness of network activity, which provides more efficient investigation to support prevention, response, and mitigation of harmful attacks.

CONTACT

Daniel Best
Pacific Northwest National Laboratory
P.O. Box 999, MSIN J4-32
Richland, WA 99352
Phone: (509) 372-6728
daniel.best@pnnl.gov

vis.pnnl.gov

ABOUT PNNL

Interdisciplinary teams at Pacific Northwest National Laboratory address many of America's most pressing issues in energy, the environment and national security through advances in basic and applied science. PNNL employs 4,600 staff, has an annual budget of nearly $1 billion, and has been managed for the U.S. Department of Energy by Ohio-based Battelle since the laboratory's inception in 1965.

www.pnnl.gov

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

PNNL-SA-75320