Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

Passive Asset Dependency Discovery (CADDY)

CHALLENGE

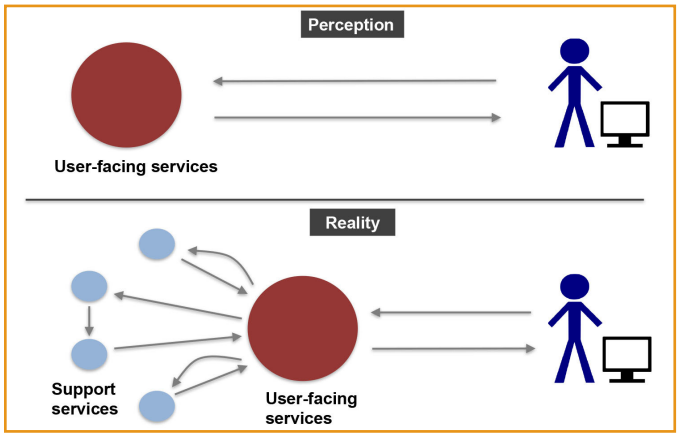
With virtualization and the "bring your own device" trends on the rise, cyber environments are becoming increasingly more fluid. The transient nature of such environments coupled with the complex dependencies of cyber assets present a unique challenge to network defenders and IT managers alike – making sure that when one asset moves, all the pieces it's connected to also move. This challenge is present in a number of situations, in conflict and in natural progression of systems.

Network service and application dependency discovery is essential for enhancing enterprise IT visibility and facilities infrastructure changes, problem diagnosing, and proactive defenses

APPROACH

Currently, there are methods which allow a user to infer which processes depend on each other. However, most are active methods, requiring a change to the network messaging format or network stack. In these cases, only processes which have also changed their network stack will be visible, leaving a huge number of processes and dependencies undiscovered.

The advantage of CADDY is that it looks for co-occurrence of activity on the network and infers those connections in real-time with statistical probability. CADDY does not require the system to change in any way. Once CADDY creates the model of dependencies, the business model can be overlaid to determine which assets and dependencies are the most critical. By linking business processes with their supporting cyber assets, CADDY improves the quality and speed of defenders' situation assessment and management.



Systems are often thought to have simple relationships, but in reality, dependencies are very complex and in some cases surprising. It is essential to discover what those dependencies are in order to make good decisions and have situation awareness.

METHODOLOGY

» **Transform:** Map network flow information and other timestamped sources into an event space

» **Analyze:** Detect and identify event co-occurrences in the event space temporal structure

- Analysis based on an ensemble of signal processing, machine learning, and statistical approaches

» **Assemble:** Organize co-occurrences into recurrent temporal sequences (RTS).

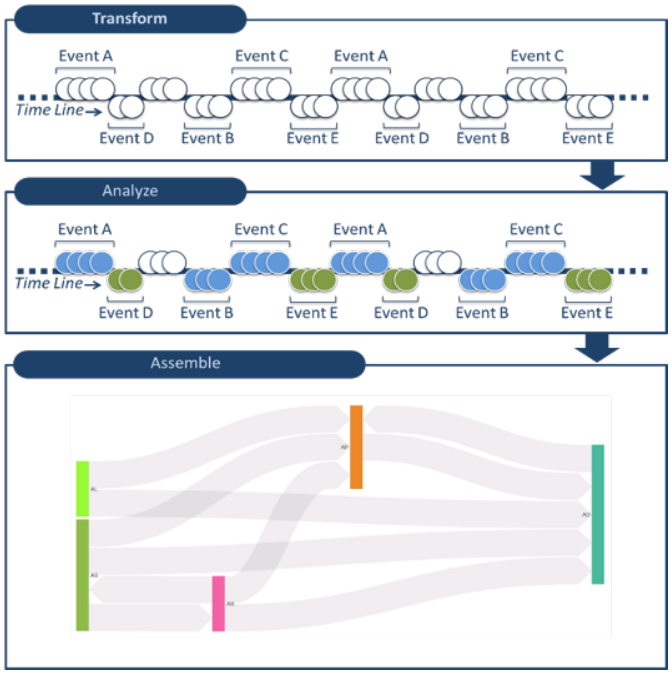
- RTS generalizes repeated observations of co-occurrences

IMPACT

CADDY improves situational awareness for practitioners, increasing response speed and minimizing mistakes by continuously discovering asset dependencies and ensuring information remains relevant as the network changes. Information such as triage, battle damage self-assessment, business continuity, and investments are based on criticality, thus significantly enhancing the defender's perspective with business knowledge.

Applications of CADDY include:

» **Cyber conflict.** CADDY gives you a heads up cyber awareness so that you can maneuver quickly in a cyber conflict.



The event analysis and recurrent pattern discovery approach comprises three stages: transform, analyze, and assemble. The recurrent temporal sequence results describe the dependencies between applications and services.

» **Changing dependencies.** Using CADDY as an alarm can help indicate when someone changes a dependency

» **Critical infrastructure.** Discovering the relationships between the IT systems that critical infrastructure rely on allows users to find unknown dependencies.

Contacts

Tom Carroll
Principal Investigator
(509) 371-6731
thomas.carroll@pnnl.gov

Chris Oehmen
Initiative Lead
(509) 375-2038
chris.oehmen@pnnl.gov

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965