Passive Cyber Asset Dependency Discovery (CADDY)

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

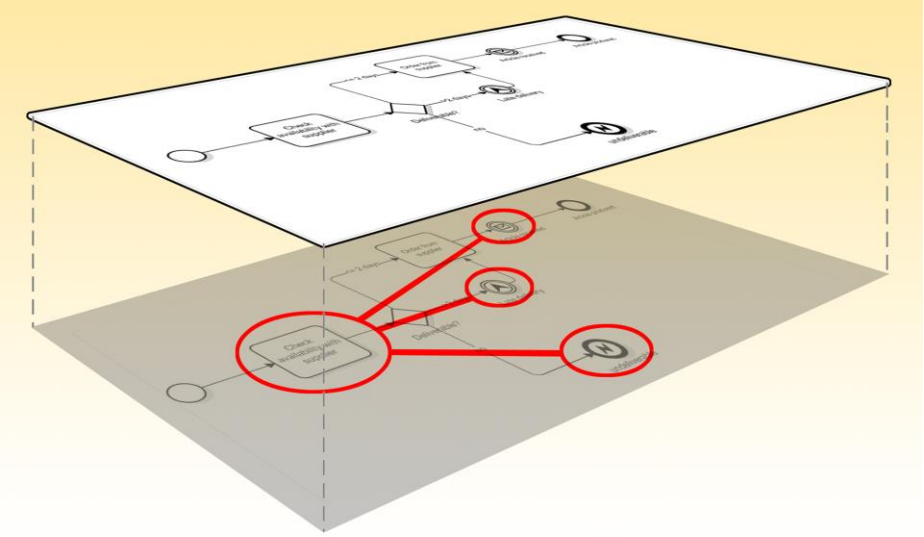
A (near) real-time enterprise introspection method for passively discovering cyber assets, identifying the functional relationships and dependencies between assets, and assessing the importance of the assets in terms of the business processes that they serve.

Challenge

Network service and application dependency discovery is essential for enhancing enterprise IT visibility and facilities infrastructure changes, problem diagnosis, and proactive defenses. While there are commercial products available and dependency discovery is an active area of research, current methods have significant limitations, including being host-centric, requiring endpoint support, and having inconsistent results.

Approach

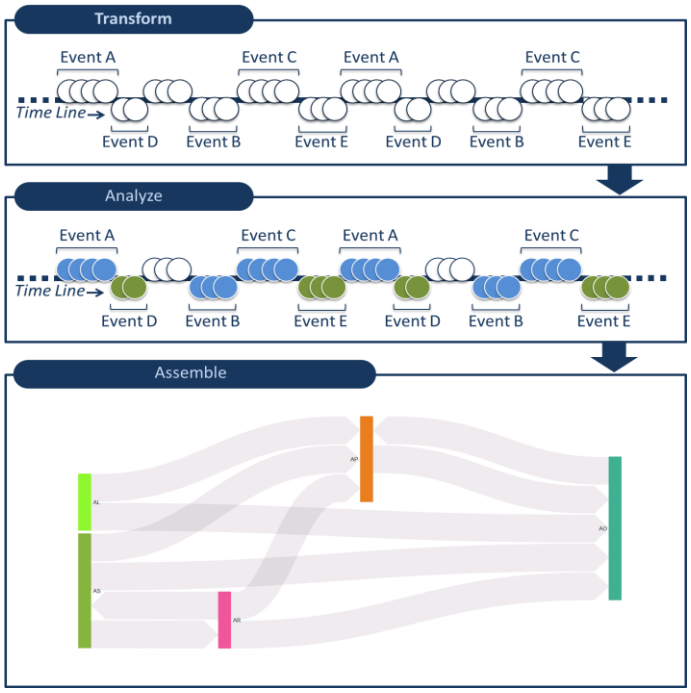
By linking business processes with their supporting cyber assets, CADDY improves the quality and speed of defenders' situation assessment and management. First, a network model of the functional associations between services is constructed by discovering recurring spatio-temporal patterns in the flow record set. These recurring patterns, which are identified using a machine learning-based deep learning workflow, arise due to the human- or machine-initiated machine-to-machine interactions that occur in the everyday operation of the enterprise. A business model, which has processes annotated with some of the essential services, is correlated to the network model to identify other process-essential assets. Asset criticality is then assessed as a function of business process importance.



The business model is correlated to the network model to identify the cyber assets that serve each business process; this relationship allows us to assess the importance to the enterprise of the asset

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



An overview of the approach for event analysis and recurrent pattern discovery

Impact

CADDY is a (near) real-time enterprise introspection method for discovering cyber assets, identifying the functional relationships and dependencies between assets, and assessing the importance of the assets in terms of the business processes that they serve. CADDY improves situational awareness for practitioners, increasing response speed and minimizing mistakes. This tool continuously discovers asset dependencies, 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.

ABOUT

The **Asymmetric Resilient Cybersecurity** Initiative

Researchers at PNNL are delivering the theory, processes, methodologies, and algorithms that will enable a resilient cyber infrastructure with an asymmetric advantage to thwart adversaries who seek to infiltrate and damage our national security through digital means. This exploratory science in Laboratory Directed Research and Development effort is made possible by the Pacific Northwest National Laboratory through funding provided by the U.S. Department of Energy.

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

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