Passive Asset Dependency Discovery (CADDY)

TOM CARROLL

Asymmetric Resilient Cybersecurity Initiative Roadshow
May 12, 2017
Need

Perception

User-facing services

Reality

Support services

User-facing services
Commercial products are available, including:
- IBM Tivoli Application Dependency Discovery Manager (TADDM)
- ServiceNow Discovery

Academic literature details many approaches, such as:
- Sherlock
- Constellation
- NSDMiner
- Rippler

Unlike CADDY, these approaches:
- Identify **host** dependencies, but don’t provide a general approach to identify network **application** and **service** dependencies
- Require endpoint access, either via OS commands, agents, or other forms of instrumentation; or employ interventions that limit scalability and usefulness
- Are sensitive to uncontrolled network factors
Approach

CADDY

- Passive approach
- Takes standard network flow (works on other timestamped data)
- Requires no other impediments to discover and track dependencies
- Scalable
- Can be deployed centrally or distributed across an enterprise
**Approach**

- **TRANSFORM**: Flow information and other timestamped sources are mapped into event space
  - Clustering flows into event classes based on rules (networking principles) and minimal ML

- **ANALYZE**: Discover co-occurrences in event stream
  - Examine event class time series for relationships
  - Analysis based on ensemble model of statistical, signal processing, and machine learning approaches

- **ASSEMBLE**: Organize co-occurrences into recurrent temporal sequences
Benefit

- Tunable to your network attributes
- Field-tested in operational environments
- Operates over any timestamped event data
- Doesn’t require clock synchronization between data reports