PathScan: Finding the Attacker Within the Network

This document is approved for public release; further dissemination unlimited
PathScan: Finding the Attacker Within the Network

PathScan Analyzes the Behavior of Subgraphs of Communicating Computers for Anomaly Detection

**BACKGROUND & MOTIVATION**

Modern Anomaly Detection for Computer Networks Models Events Independently

- Identifying deviations from historic activity
- Does not ask about deviations among subgraphs of communicating hosts

**INNOVATION**

Analyzing subgraphs of communicating computers provides better signal-to-noise ratios.

- Lower false alarm rate
- Higher true alarm rate
- Better forensic information—providing a fuller description of the overall attack

**DESCRIPTION**

Detecting Advanced Persistent Threats (APTs) on operational networks in near real-time

- Statistical modeling of network behavior
- Fast, parallel subgraph enumeration,
- Examining billions of subgraphs within enterprise-level computer networks

**How it works:**

1) Large networks are broken into billions of small paths

2) Models of the historic behavior are compared with observed data on each path

\[ \lambda = -2 \log \left( \frac{\mathcal{L}(\theta(\gamma); X(\gamma))}{\sup_{\psi \in \Theta} \mathcal{L}(\theta(\gamma); X(\gamma))} \right) \]

3) Those paths which exceed a threshold of anomalosity (weirdness) are alarmed upon

**Assumptions & Limitations**

- Main limitation is often access to high-quality internal network data
- We provide expertise in collecting data to help new networks quickly get up to speed

**ANTICIPATED IMPACT**

Real-time detection of sophisticated adversaries traversal behavior on a network

**PATH FORWARD**

Implement outside LANL:

Prototype and beta test on external networks:

- Government and commercial

Validate and harden algorithms against broader sets of network data:

- Other Government
- Commercial: Financial industry, Oil & gas industry, entertainment industry, etc.

**Potential End Users:**

- All large IT networks (government and commercial) at enterprise level

**Point of Contact:** Mike Fisk

Advanced Computing Solutions Program Office

505-667-5119, mfisk@lanl.gov