IMPROVING NETWORK MONITORING THROUGH CONTRACTS

Michael Collins

USC-ISI

mcollins@isi.edu

Top Level Ideas

- A network contract is a (hypothetical) traffic descriptor
  - Assets connecting to a network will provide a contract to a network monitoring system
  - The contract will describe “envelopes” of behavior under different circumstances: baseline traffic, traffic during software updates, times on, times off &c
- Contracts can empower operators to focus their attention on unknown or suspicious behaviors.
  - Human in the loop is important here
- Contracts will accommodate multiple states ranging from baseline behavior to maintenance to crises. Under different circumstances, different monitoring will be needed.

An Attention-Based Framework for Security Response

- SOC operators have a limited amount of time to process alerts
  - Current estimates are ~10 events per analyst-hour (EPAH)
  - This value is dwarfed by the number of alerts an enterprise receives per second
  - Operators need to be creative in order to constrain creative attackers
- To secure things in an attention-based framework:
  1. Work within organizational limits
  2. Given two options, pick the one that frustrates the attacker more
  3. Given two options meeting criterion (2), pick the option that lets operators manage more events

How Operators Spend Their Attention

- Validating alerts
  - Anomalous activity is not necessarily hostile
  - Hostile activity is not necessarily threatening
- Cross-referencing and comparing data from **multiple domains**
  - Network traffic x server log
  - Endpoint agent x network traffic
  - These comparisons are complicated and expensive under normal circumstances
- Networks are *contested* domains
  - Network instrumentation fails or is inadequate
  - Operators need fallbacks for failures in instrumentation
  - Any nontrivial network already has attackers operating in it

Why Anomaly Detection is Hard

- IDS mirrors artificial intelligence, early systems were expert systems, later systems have used current techniques: Bayesian networks, Neural Networks, Deep Learning, &c
- The results have been a mixed bag at best
  - The Internet changes over time and space
  - Individual sites lack sufficient data to train a model
  - Attackers adapt
  - Normal is not necessarily innocent
  - The base-rate fallacy is real
  - Operators are exhausted
- Security organizations are a cost center – they must *justify* their decisions

A Contract Mechanism

- Proposal: A contract consists of one or more traffic envelopes divided into different states
- The envelope consists of a number of traffic descriptors
  - Descriptors may include IP addresses, domain names and *indicators of compromise* (IOC)
  - Malware information sharing platform (MISP) from CIRCL is a good starting point for describing fields operators care about
- States describe different conditions under which traffic is allowed or expected
  - Example states: default, control, update, emergency patch
  - Imagine states as descriptive rather than proscriptive – if the "control" traffic is observed, this may annotate an event in a SIEM
- Potential contracts:
  - control: (DNS:www.virusupdate.com, 1x/day)
  - baseline: (netflow: host:*:*:80:tcp:(0,5MB):3600s)
  - baseline: (off,8PM:6AM)
  - baseline: *

The Necessity of Different States

- Monitoring needs to handle crises
  - Example: autoscaling time series visualizations isn't useful during a DDoS
    - Neither is full packet capture
- Common response to a security crisis is to reorganize monitoring – collect data from affected area, reroute traffic, &c
- By making these states *explicit*, we can consider the role of encryption and authentication under different conditions and crises
  - Our networks are neither homogeneous, nor homogeneously *pwned*

Contract to Monitoring

- Asset publishes contract to monitoring system
- Monitoring system may accept, reject or constrain contract
  - A contract may end up specifying asset-specific monitoring (e.g., I look up a DNS address checking the DNS server)
- Operators use contracts to extrapolate behavior
  - Asset explicitly violates contract (attempts contact with unexpected site)
  - Asset moves outside of boundaries temporarily (surge in traffic due to a large patch)
  - Asset provides *reasons* for why particular behavior is observed
- Driven by attention: monitoring and defense uses contracts to manage operator response, not as an automatic shutoff

Invitation To Discussion

- Three core ideas here:
  - Multiple states
  - Analyst attention/necessity of human in the loop
  - Supplementing anomaly detection with explicit behavioral envelopes
- Outstanding questions
  - What types of states are there?
  - More valuable for IoT?
  - Can monitoring mandate behavior to assets as part of negotiation, and what potential for abuse is there?