Threat Detection and Mitigation for IoT Systems using Self Learning Networks (SLN)

JP Vasseur, PhD - Cisco Fellow – jpv@cisco.com
Maik G. Seewald, CISSP – Sr. Technical Lead – maseewal@cisco.com

June 2016
Cyber Security Trend: Increasing Threat Surface

Threat Landscape 2016 (Cisco’s ASR)

- Emerging Hacker Industry: Cybercrime is lucrative
- Threat Automation and Scripted Attacks: Malware sophistication and ease of use has grown exponentially
- Large DDoS networks
- Attacks based on DNS for command and control
- Malicious Browser Extensions
- Aging network and computer infrastructure
- Growing complexity

For the success of IoT, it is essential to address an increasing threat surface!

ASR = Cisco 2016 Annual Security Report
Cyber Security Trend: Increasing Threat Surface
Example: Botnets and Data Ex-Filtration Techniques

- Size can range from thousands to millions of compromised hosts
- Botnet can cause DDoS & other malicious traffic (e.g.: spam) to originate from the inside of the corporate network
- C&C (C2) servers become increasingly evasive
  - Fast Flux Service Networks (FFSN), single or double Flux
  - DGA-based malware (Domain Generation Algorithms)
  - DNS/NTP Tunneling
  - Peer-to-Peer (P2P) protocols
  - Anonymized services (Tor)
  - Steganography, potentially combined with Cryptography
  - Social media updates or email messages
  - Mixed protocols
  - Timing Channels
Addressing the Threat Landscape
The Network as Sensor and Enforcer

Attack Continuum

BEFORE
Control
Enforce

DURING
Detect
Block

AFTER
Scope
Contain

A more adaptive security architecture to address the complexity of increasing connectivity and digitalization
Threat Intelligence, Detection and Awareness
Addressing the Threat Landscape
Visibility and Context Awareness

Attack Continuum

BEFORE
Control
Enforce

DURING
Detect
Block

AFTER
Scope
含

Firewall
VPN
Network Access Control
Posture Assessment

NG IPS
Anomaly Detection

Network Behavior Analysis
SIEM
Forensics

Advanced Protection using Machine Learning
Learning Machines
A true paradigm shift

Current Generation of Security Architectures and Products:
- Specialized Security gear connected to the network (FW, IPS, IDS)
- Heavily signature-based ... to detect known Malware
- Hardly adaptive
- Does not address the dynamics of these days attacks

SLN is Machine Learning based and pervasive

- Use of adaptive Machine Learning (AI) technology to detect advanced, evasive Malware: build a model of normal pattern and detect outlier (deviations)
- High focus on Zero-Day Attacks
- Use every node in the network as a security engine to detect attacks
- Complementary to all other technologies (FW, IPS, IDS)
Self Learning Networks
A true paradigm shift

**Signature-based (Firewalls):** traffic is normal *unless* matching known characteristics

**Dynamic Learning of anomalies (SLN):** Outperform conventional algorithms in presence of uncertainty, when complexity is too large (scale) and when adaptation is required.

This is a key requirement in IoT/IoE. We need predictive models for large scale networks to address:

- High performance and high resiliency
- Detection of disruptive subtle DDoS attacks
- New threats
SLN Architecture

- Orchestration of Distributed Learning Agents (DLAs)
- Advanced Visualization of anomalies
- Centralized policy for mitigation
- Interaction with other security components such as ISE and Threat Intelligence Feeds
- North bound API to SIEM/Database
- Evaluation of anomaly relevancy

- Sensing (knowledge): granular data collection with knowledge extraction from NetFlow but also DPI on control and data plane & local states
- Machine Learning: real-time embedded behavioral modeling & anomaly detection
- Control: autonomous embedded control, advanced networking control (police, shape, recoloring, redirect, ...)

© 2013-2016 Cisco and/or its affiliates. All rights reserved.
Self Learning Network
An Open Architecture (SCA)

Identity Services Engine
Context Enrichment: IP Address (key), Audit session ID, User AD Domain, MAC address, ESP Status, NAS IP & port, Posture, TrustSec information, Endpoint Profile Name

Syslog messages using both CEF/CIM formats pushing anomalies events into DB and SIEM

Various Source of Threat Intelligence: Talos (blacklists), Threat Grid (sandboxing), OpenDNS (AS, URL, historical association to domains)

API triggering Mitigation from external Sources such as Firewall, IPS/IDS; Abstracting networking complexity
SLN and Threat Detection
Clusters, Self Organizing Learning Topology and Anomalies

- Modeling mixed-behaviors unavoidably leads to hiding anomalies ...
- The fundamental idea of dynamic clustering is to “group” devices according to behavioral similarity
- Self Organizing Learning Topologies (SOLT): ability to build Virtual topologies used to learn models between dynamic clusters
  - Example: find a model for the traffic from cluster A to cluster B, for HTTP traffic
- What is an anomaly? An anomaly is the detection of a flow that significantly deviates from a model locally computed by a Distributed Learning Agent, on premise.
Threat Detection
Anomaly Detection: A paradigm change

Traditional Anomaly Detection Systems
Focus on Detection (wrong)
Core challenge is not Detection itself but Precision (avoid False Positive / Irrelevant alarms)

SLN Approach
Efficient detection and Precision
Make the Network learn from its own mistakes and eliminate False Positive!
Not a feature but an Architecture
Dynamic Learning of anomalies (SLN): mathematical models built on-line and deviation from these (constantly adapted) models lead to detection of anomalies
Conclusion

SLN

- Network Security as sound basis for a scalable IoT Security Architecture
- Visibility and Context awareness are key requirements for IoT Networks
- Security Intelligence is needed to address Threat Automation and Malware Sophistication
- Behavior Based Security using Learning Machine Technologies as next step in Security Technology - Complementary to existing technologies (FW, IPS)
- SLN is fundamentally a hyper-distributed analytics platform:
  - Goldmine of untouched data on networking gear (sensing)
  - Network learns and computes models on premise (analytics)
  - The Network adapts, modifies its behavior (control)
Thank you.