Enhanced Situational Awareness for Advanced Threat Detection and Identification in IIoT (ESTATION)

Amin Hassanzadeh, Ph.D.
Accenture Technology Labs
ESTATION: A Holistic, Scalable, and Strategic IIoT Security Framework

To assess, prioritize, implement, and optimize security architecture and capabilities
Effective and Efficient Security Control Assignment in IIoT (ESCAN)

- **What** security capabilities are required?
- **Where** do we deploy security capabilities?
- **How** do we deploy security capabilities?

1. Enumerating traditional security controls
2. IIoT Architecture and functionality
3. Publicly available incident analyses
4. Conducting a gap analysis to determine the efficacy of security controls
Architectural View of ESTATION

On-the-edge Resource-aware Behavioral Intrusion Tolerance (ORBIT)

- The vast majority of these things won’t be in the cloud, they will be at the edge of the network—where the people are.
- IIoT will have enormous client-server interactions but it will have even more interactions among intelligent things at the edge of the network.
- Inefficient data communication to cloud for intrusion detection in large IIoT networks (communication overhead).
- Delayed data processing in real-time applications.

Optimal Security Function Distribution

Security Functions: Efficacy, Efficiency

Optimal IDS/IPS Function Distribution

ORBIT: On-the-edge Resource-aware Behavioral Intrusion Tolerance
Architectural View of ESTATION

Security Insight through Operational Telemetrics (SINOPTEC)

- ESCAN
  - Security Logs/Alerts
  - Telemetry Data
  - Anomaly Detection
  - Root Cause Analysis
  - Efficacy
  - Efficiency

- ORBIT
  - Optimal IDS/IPS Function Distribution

- IT Network

- OT Network

- SINOPTEC

- Data Driven Approach
  - Supervised Machine-Learning
  - Unsupervised Machine-Learning

- Model Based Approach
  - First-principle Model (physics laws)
  - Empirical Models (input-output data)

- Domain Specific Knowledge
  - Process Semantics
  - Physical Process Semantics
  - Supervised Machine-Learning
  - Unsupervised Machine-Learning

- Process Semantics used as domain knowledge (e.g., Bayesian Network)

- Human Error
- System Fault
- Cyber Attack
Architectural View of ESTATION

Event Correlation across Heterogeneous Operations (ECHO), Intelligence-Driven Threat Mitigation (IDTM)

**ESCAN**
- Efficacy
- Efficiency

**ORBIT**
- Optimal IDS/IPS Function Distribution

**IDTM**
- Cyber Threat intelligence Feeds (STIX Format)
- Preprocessing and Filtering
- Fusion & Aggregation
- Correlation & Pattern Extraction

**SINOPTEC**
- Anomaly Detection
- Root Cause Analysis

**OT Network**
- Telemetry Data

**IT Network**
- Security Logs/Alerts

Visualization of Complex Multi-domain IIoT Incidents
Architectural View of ESTATION

Industrial Security Agent Platform (ISAP)

- ESCAN: Cyber Threat intelligence Feeds (STIX Format)
- SINOPTEC: Anomaly Detection, Root Cause Analysis
- ORBIT: Optimal IDS/IPS Function Distribution
- IDTM: Preprocessing and Filtering, Fusion & Aggregation, Correlation & Pattern Extraction
- ECHO: Visualization of Complex Multi-domain IIoT Incidents

- ISAP:
  - Security capabilities for edge/field devices
  - Edge security control implementation customizable based on client risk posture, and gateway vendor-agnostic
  - Risk mitigation against, and reduction in data volume to, platform’s federated assets

Security Logs/Alerts

Telemetry Data
IIoT Security Orchestration

- Orchestrate complex automated security actions to improve situational awareness and real time mitigation capabilities
- Coordinate security processes and workflows across disparate security tools through infrastructure orchestration

Accenture Connected Security Solutions (ACCESS)
- ECHO, IDTM, ISAP/ORBIT
- Lightning Talk in TCIPG 2015
- Demo at Hannover Messe 2015

Enhanced Situational Awareness for Advanced Threat Detection and Identification (ESTATION)
- ECHO, SINOPTEC, ESCAN
- Submitted to DARPA RADICS BAA, 2016

- Six Pending Patents
- One journal and two conference papers accepted