SCATOPSY: Malware Threat Mitigation in ICS/SCADA Operations

Dr. Wenke Lee, Moses Ike
Georgia Institute of Technology
Jan 24, 2022

Georgia Tech

Objective

Detect Malware Activity in SCADA workstations (e.g., Human Machine Interfaces or HMI) by correlating malware execution-relevant datapoints in ICS host and network behaviors

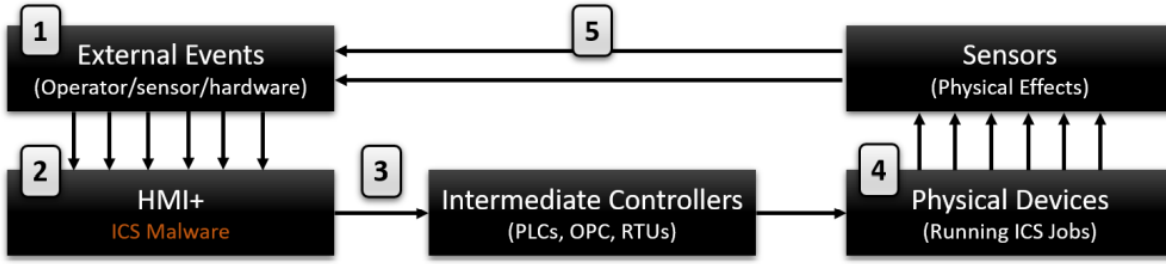


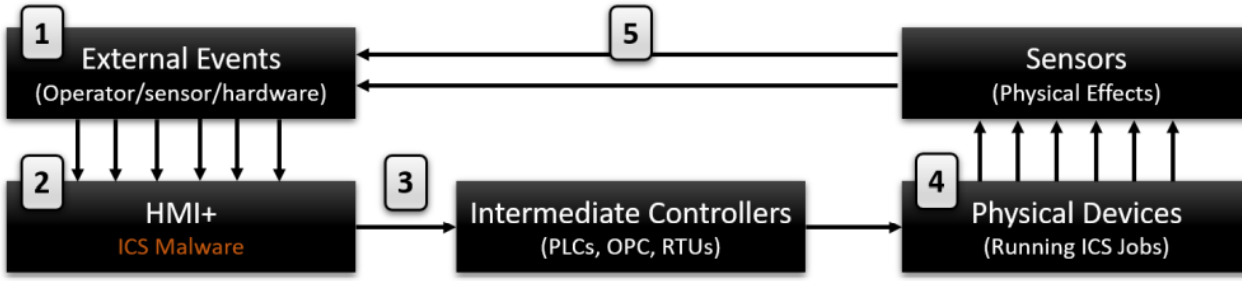
Figure 1: End-to-End ICS/SCADA process-control operation form a feedback control loop

- Observation/Insight
  - Unlike in Traditional IT, ICS/SCADA host operation is driven by ICS events (e.g., sensor measurements of physical process states)
  - To evade detection, modern ICS attacks stage and launch their payloads within these normal events to blend with benign SCADA host operations

  - Idea: Identify and model legitimate end-to-end SCADA behavior, which differentiate from attacker's malicious activities, enabling us to detect them

Georgia Tech

Approach and Challenges



- Build a baseline of legitimate ICS operation sequences 1-> 2-> 3
  - ICS Event -> SCADA Host Execution -> ICS Network Signal
  - Detect anomalous sequences in host execution and network activity
- Challenges:
  - I. Data Model for multi-dimensional sequences
    1. ICS Sensor Readings `<ICS parameter, state, timestamp>`
    2. SCADA Execution `<Process Activity/API call, Argument, timestamp>`
    3. ICS Network Signals `<ICS parameter, func_code, state, timestamp>`
  - II. Sequences may not be enough. Can be evaded by advanced malware ?
    - Additional physical properties/constraints may be needed
      - Statistical and Temporal behaviors

Georgia Tech

Initial Results

- Investigated the 2016 Industroyer Malware Attack on Ukraine Power Grid
  - Industroyer attacked circuit breakers and caused power outage
  - Analyzed Host and Network behaviors of the attack

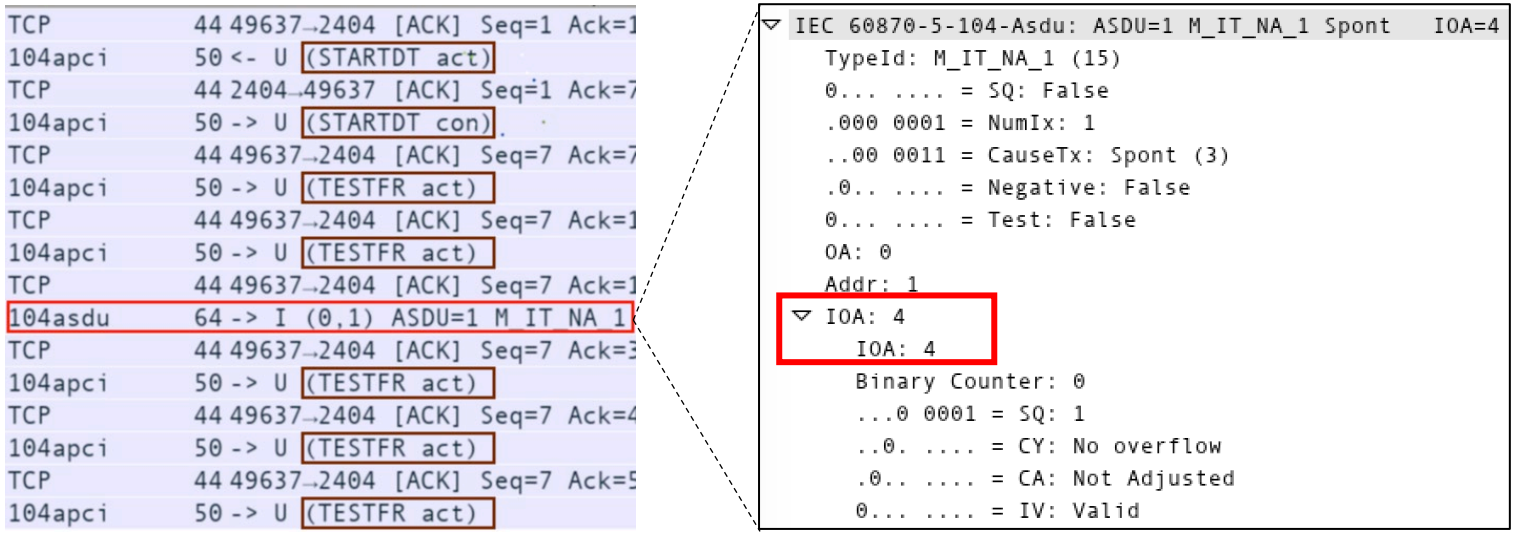


Figure 2: Industroyer Malware's ICS network behavior: Showing attack payload

Georgia Tech

Integration and Commercialization Plan

- Integration opportunities with RAD Gateway
- Commercialization based on further use case analysis
  - Distributed or centralized data collection and analysis?
  - Offline or online detection ?

Georgia Tech

Thank you

Questions ?

Georgia Tech