INSIDE – Enhancing Network Intrusion Detection in Power Grids with Automated Facility Monitoring

Motivation

Power Grids

- Vital part of a country's critical infrastructure
- Require special protection against sabotage
  - Physical protection, e.g., perimeter protection and access control
  - Cybersecurity protecting digital assets
- Intrusion Detection Systems (IDSs) enable early detection of malicious network activities
  - Industrial IDSs leverage context information regarding industrial processes and communication
  - Further context information is required to improve the accuracy of IDSs in power grids, particularly considering the many remote sites of power grids
- Enhancing industrial IDSs with automated facility monitoring
  - IDSs should react more sensitively to suspicious network activity resulting from unauthorized physical access, e.g., trespassing
  - Use output from automated Facility Monitoring Systems (FMSs) (e.g., video surveillance) to locate (on-site) origin of cyberattack

Threat Model

Assumptions

Limited Knowledge
- …about power grid & network structure
- E.g., an external maintenance engineer

→ **Local Access**
- Through a remote facility / substation
- E.g., a trespasser

↓

Preparations

Discovery
- Network reconnaissance through manipulated host

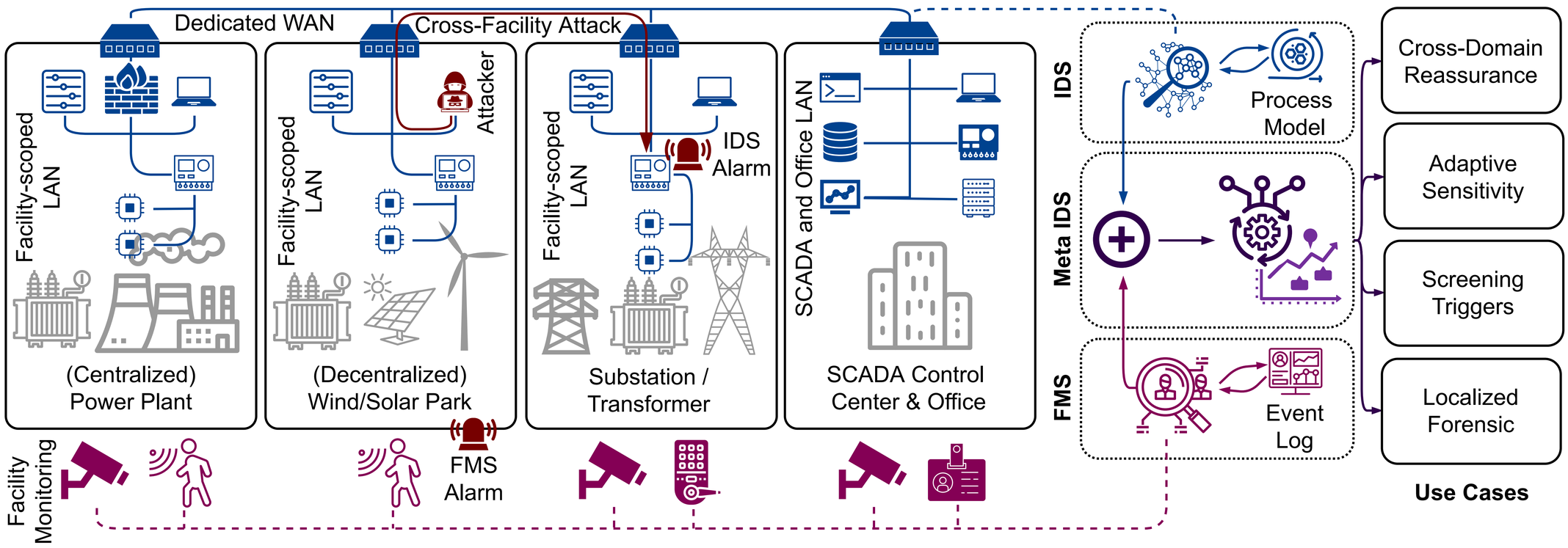
← **Lateral Movement**
- Using privilege escalation
- Attacking local host close to target

↓

Impact

Attacking Power Grid Control
- Manipulate monitoring & command pkts
- Maximize damage (e.g., induce blackout)

INSIDE: Combining Industrial IDS with Automated Facility Monitoring



Industrial IDS

- Leverages knowledge about physical processes to improve anomaly detection
- Non-invasive monitoring approach
  - IDS sensors use TAPs of switches for traffic capturing
  - Sensors are placed at strategically relevant switches
- Significant limitation: IDSs are unable to identify the origin of an attack

Facility Monitoring System

- Corresponds to an IDS for the physical world
- Detects security-related physical incidents, e.g.,
  - A maintenance engineer accessing a restricted area
- Various sensors throughout the power grid, e.g.,
  - Surveillance cameras, motion sensors, and digital keylocks
- Issues intrusion alarms, records facility accesses, and log how specific incidents were resolved

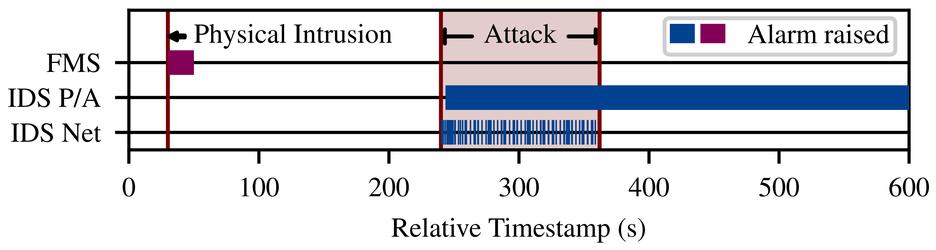
Meta IDS

- Aggregates the real-time results from the industrial IDS and the FMS for analysis
  - Identifies correlations between suspicious network traffic and physical accesses
  - Localizes origin of possible cyberattack
- Enables incident response team to determine if this is a false alarm or stop an ongoing attack

Attack Example: Industroyer

- Industroyer malware attacks multiple IEC 104-based RTUs
  - Attacker physically breaks into remote facility
  - Attacker issues control commands via manipulated host
    - Establishes secondary IEC 104 connections to the substation's RTUs
    - Opens circuit breakers to induce blackout
  - Effects visible in field measurements
- IDS and FMS alarm correlation
  - FMS (e.g., motion sensor) triggers during physical Intrusion at facility *F*
  - We evaluated two IDS variants: process aware (P/A) and network based (Net)
    - Both are able to detect the attack
    - **However: attack origin is hard to identify**
  - INSIDE: Correlate FMS alarm of facility *F* with IDS alarms to locate attack origin

FMS and IDS alarms during the Industroyer attack



Outlook

Use Cases

Cross-Domain Reassurance
- Combine reports of IDS and FMS
- Reduce false positives by increasing certainty about incident

Adaptive Sensitivity
- Increasing IDS sensitivity when the FMS triggers an alarm
- Improves reaction to smaller deviations

Screening Triggers
- Alarms trigger active system screenings
- Potentially deploy temporal IDS components in area of interest

Localized Forensics
- Use previous FMS alarms to identify the location of the attacking device
- Quickly respond & prevent more damage

Future Work

- Elaborate a prototype for a power grid simulation environment including FMS, IDS and Meta IDS
- Focus on the correlation between physical access violations and network traffic anomalies to reliably identify the attack's origin

We provide the PCAP files of the conducted attack at *https://wattson.it/ccs22*

Martin Serror, Lennart Bader, Martin Henze, Arne Schwarze, Kai Nürnberger

https://fkie.fraunhofer.de

Fraunhofer FKIE