Deploying Intrusion-Tolerant SCADA for the Power Grid

Amy Babay, John Schultz, Thomas Tantillo, Samuel Beckley, Eamon Jordan, Kevin Ruddell, **Kevin Jordan**, and **Yair Amir**

Johns Hopkins University, Spread Concepts LLC, Resurgo LLC

JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

Distributed Systems
and Networks Lab
www.dsn.jhu.edu

Spread Concepts

Resurgo LLC

Intrusion-Tolerant SCADA for the Power Grid: Critical Need

- Supervisory Control and Data Acquisition (SCADA) systems: monitoring and control of critical infrastructure
- Must be constantly available and operating at expected level of performance
- Perimeter defenses are not sufficient against determined attackers
  - Stuxnet, Dragonfly/Energetic Bear, Black energy (Ukraine 2015), Crashoverride (Ukraine 2016)
  - Becoming a target for nation-state attackers

Translating Research into Practice

- Considerable research on intrusion-tolerant SCADA systems using BFT replication
  - PBFT applied to simulated grid
    - [ZV08] Embedded Software and Systems 2008
  - Prime integrated with Siemens product
    - [KGAWS14] IEEE Trans. Smart Grid 2014
  - SMaRt-SCADA: BFT-SMaRt integrated with EclipseNeoSCADA
    - [NGBN18] IEEE/IFIP DSN 2018
  - And more…

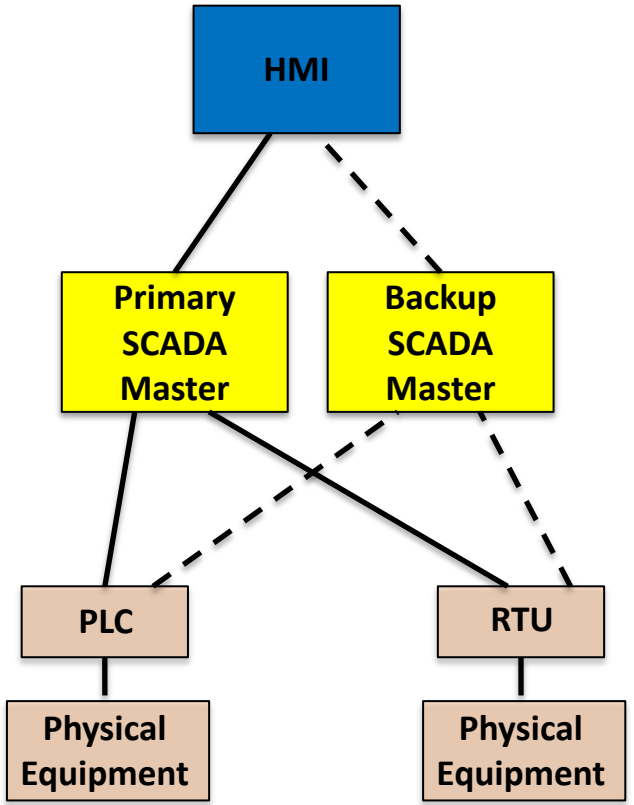
- Can these approaches be deployed in practice?
- Do they provide the promised resilience?
- How do we move toward an intrusion-tolerant power grid?

Roadmap

- Background: SCADA, Spire and MANA
- Red Team Experiment at Pacific Northwest National Labs (PNNL)
- Power Plant Deployment at Hawaiian Electric Company (HECO)
- Toward an Intrusion Tolerant Power Grid

SCADA for the Power Grid: Basics

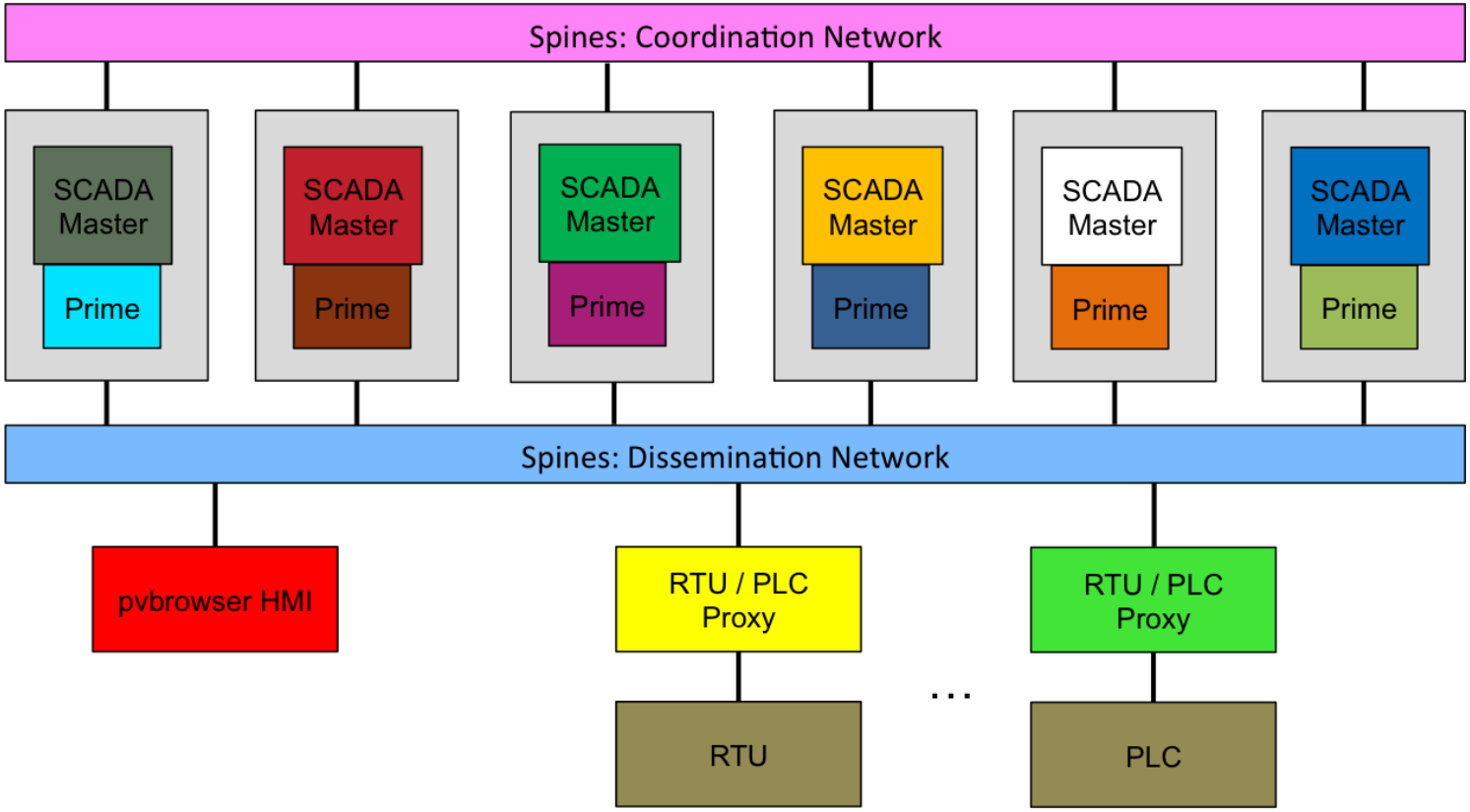
- Programmable Logic Controllers (PLCS) and Remote Terminal Units (RTUs) control power equipment
- SCADA Master provides central control
- Human Machine Interface (HMI) provides graphical displays for operator



Spire: Intrusion-Tolerant SCADA

- Spire: http://www.dsn.jhu.edu/spire/
  - First SCADA system for the power grid to withstand simultaneous system compromises and network attacks [BTAPA18] DSN 2018
- Intrusion-tolerant replication with latency guarantees under attack (Prime: [ACKL08] DSN 2008 / [ACKL11] TDSC 2011)
  - http://www.dsn.jhu.edu/prime/
- Compile-time diversity (Multicompiler)
  - https://github.com/securesystemslab/multicompiler
- Proactive recovery
- Intrusion-tolerant network (Spines: [OTBS+16] ICDCS 2016)
  - http://www.spines.org

Spire: Intrusion-Tolerant SCADA



MANA: Intrusion Detection for SCADA

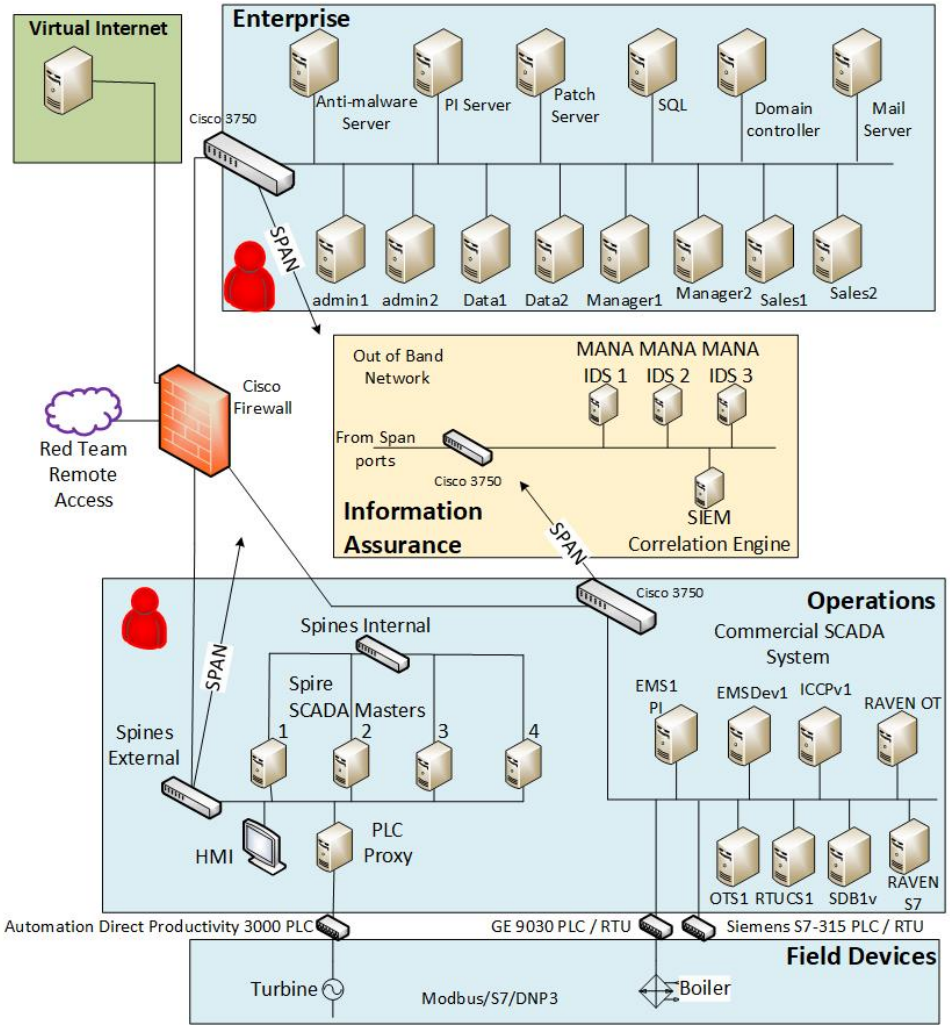
- Machine-learning Assisted Network Analyzer: http://themanalabs.com
- Non-invasive passive packet capture
- Trained on operations networks
- Alert Reader and Correlator (ARC): combines output of multiple machine learning algorithms to estimate alert confidence and reduce false positives
- First time intrusion detection deployed alongside intrusion-tolerant replication for SCADA

Red Team Experiment

March 27 – April 7, 2017

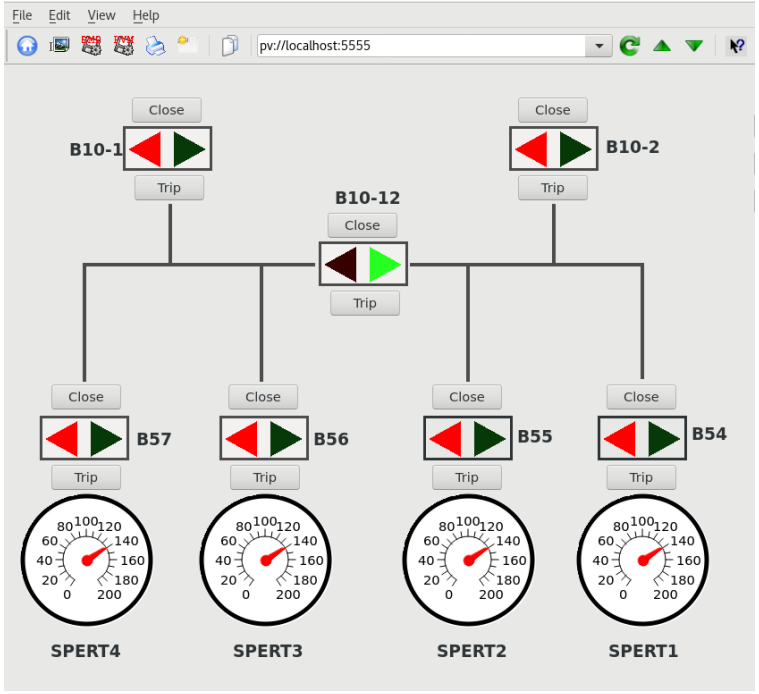
DoD ESTCP Red Team Experiment

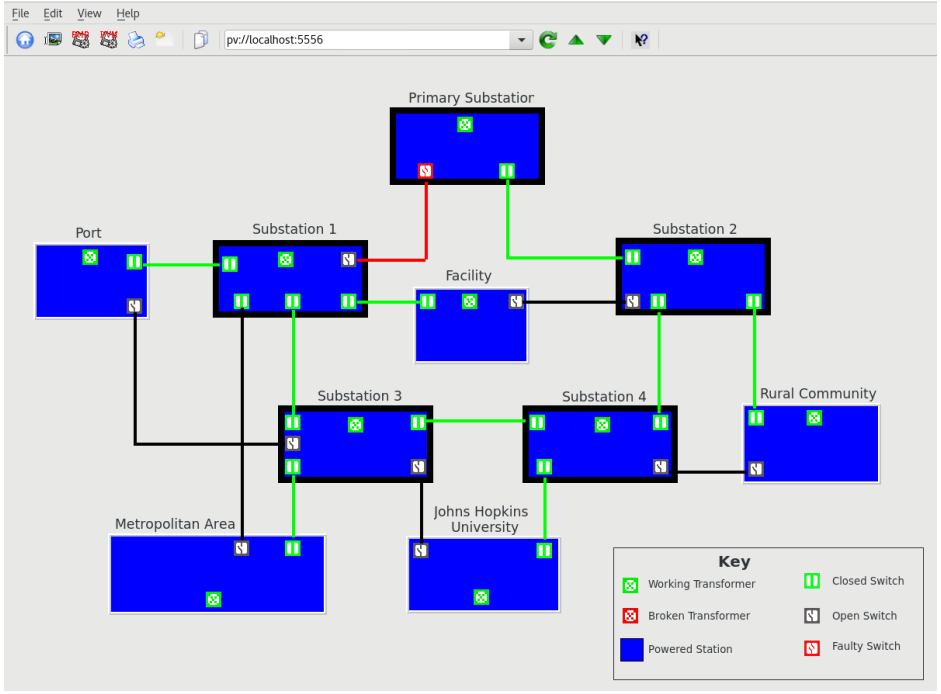
- Conducted at Pacific Northwest National Lab (PNNL)
- Power plant network architecture set up with input from Hawaiian Electric Company
- Parallel operations networks
  - NIST-compliant commercial SCADA system
  - Spire system
- MANA received input from each network
- Commercial system and Spire each attacked by Sandia National Labs red team



SCADA System Setup

- Scenario 1: 1 real PLC provided by PNNL, representing a field substation feeding power to four buildings
- Scenario 2: 10 PLCs emulated using OpenPLC, power distribution from 5 substations to 5 sites



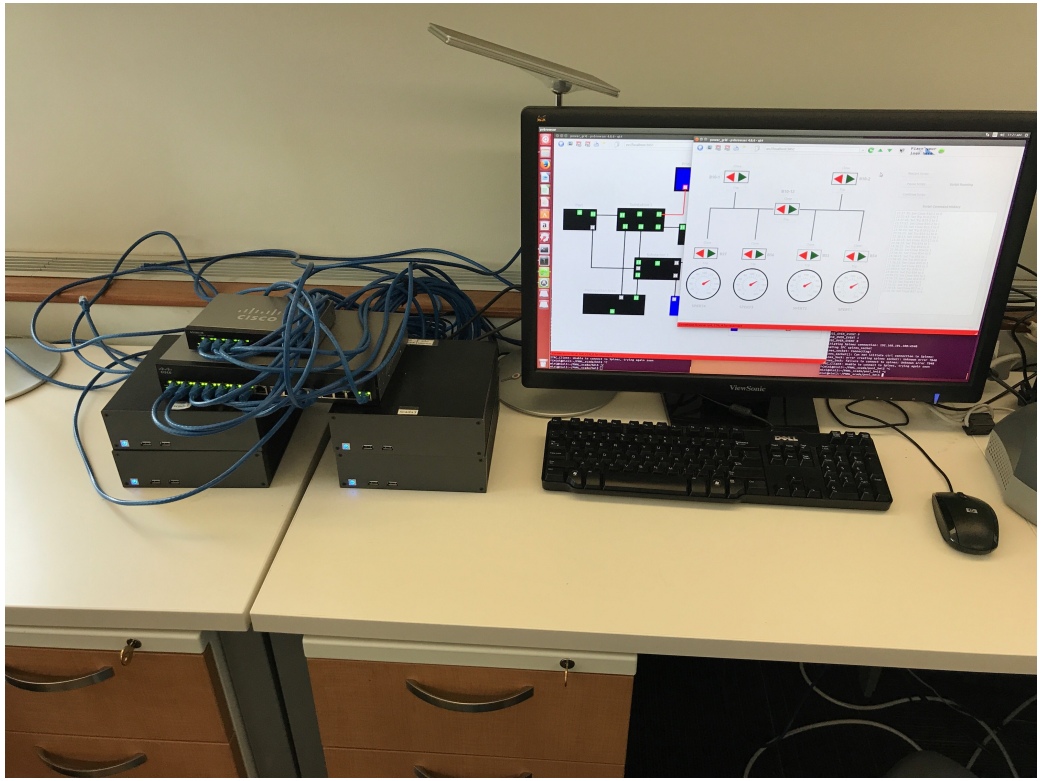


Preparing Spire: Beyond BFT

- Leveraged expertise running commercial cloud systems
- OS: Minimal CentOS server install
- Network setup
  - Host firewalls: only permit specific expected traffic (Spines)
  - Static mapping of MAC addresses to IP addresses on each host
  - Static mapping of MAC addresses to switch ports
- Network architecture
  - Isolated network for replication protocol
  - PLC Proxy

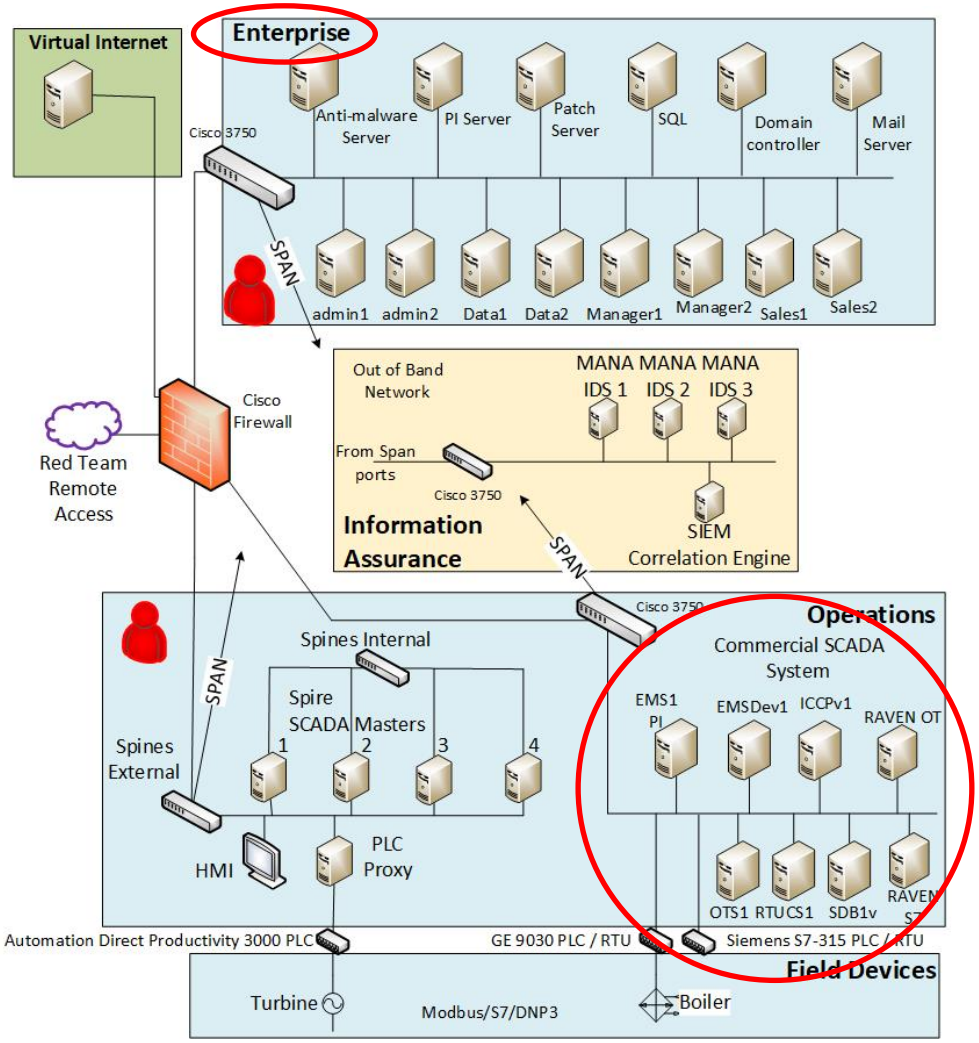
Spire in Action

- Spire as deployed in DoD ESTCP Experiment



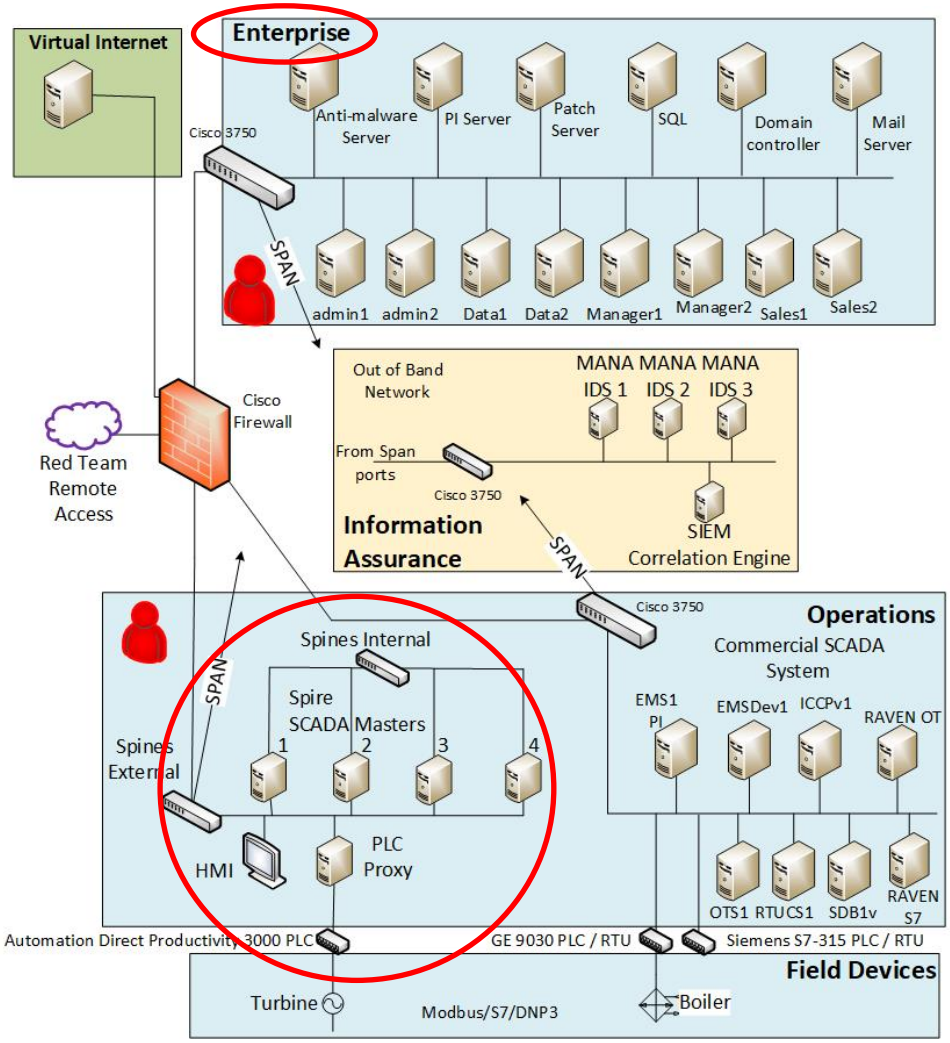
Commercial System Attacks

- Started from enterprise network
  - Goal: Establish baseline
  - Surprising result: access to operations network via MITM attack -> issued direct commands to PLC
  - Full control + damage to PLC: required firmware reinstall
- Given direct access to operations network
  - Disrupted and modified SCADA Master to HMI communication



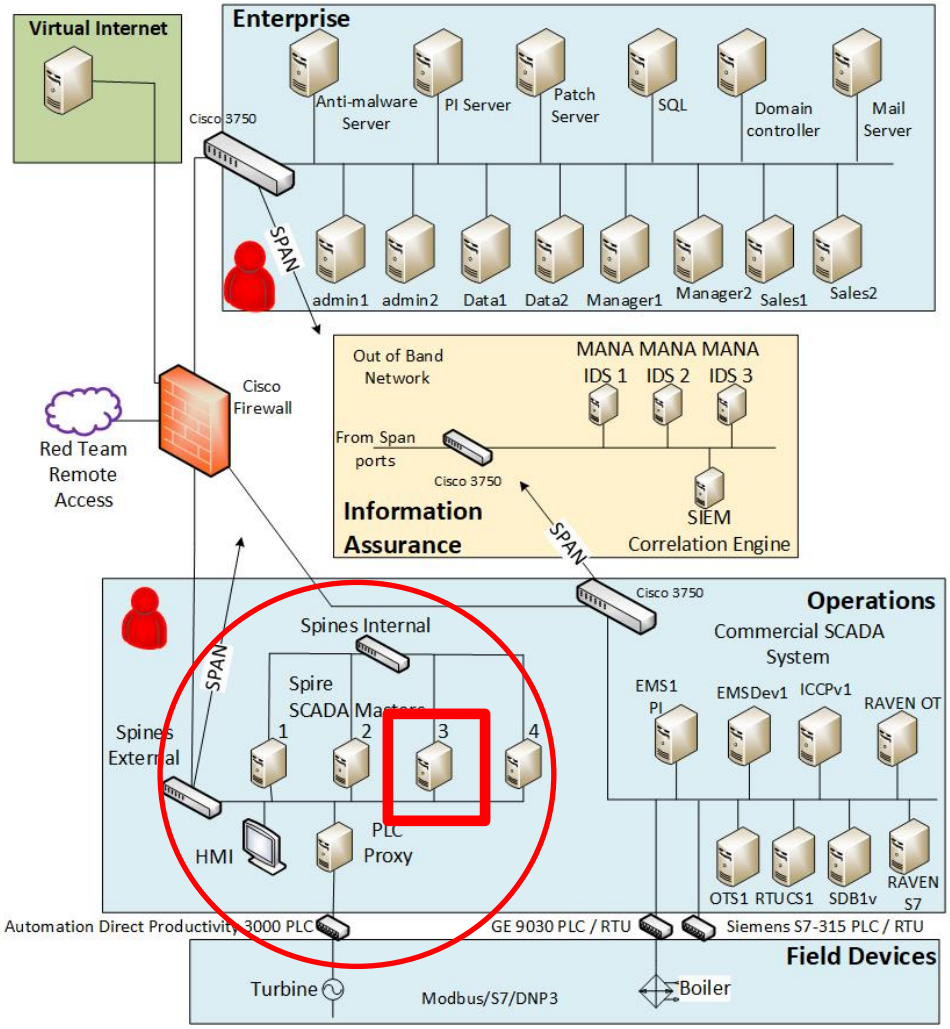
Spire System Attacks

- Started from enterprise network
  - No visibility; gave up after a couple hours
- Given direct access to operations network
  - 2 full days of network attacks (port scanning, ARP poisoning, IP address spoofing, DoS via traffic bursts, …)
- No effect on the system



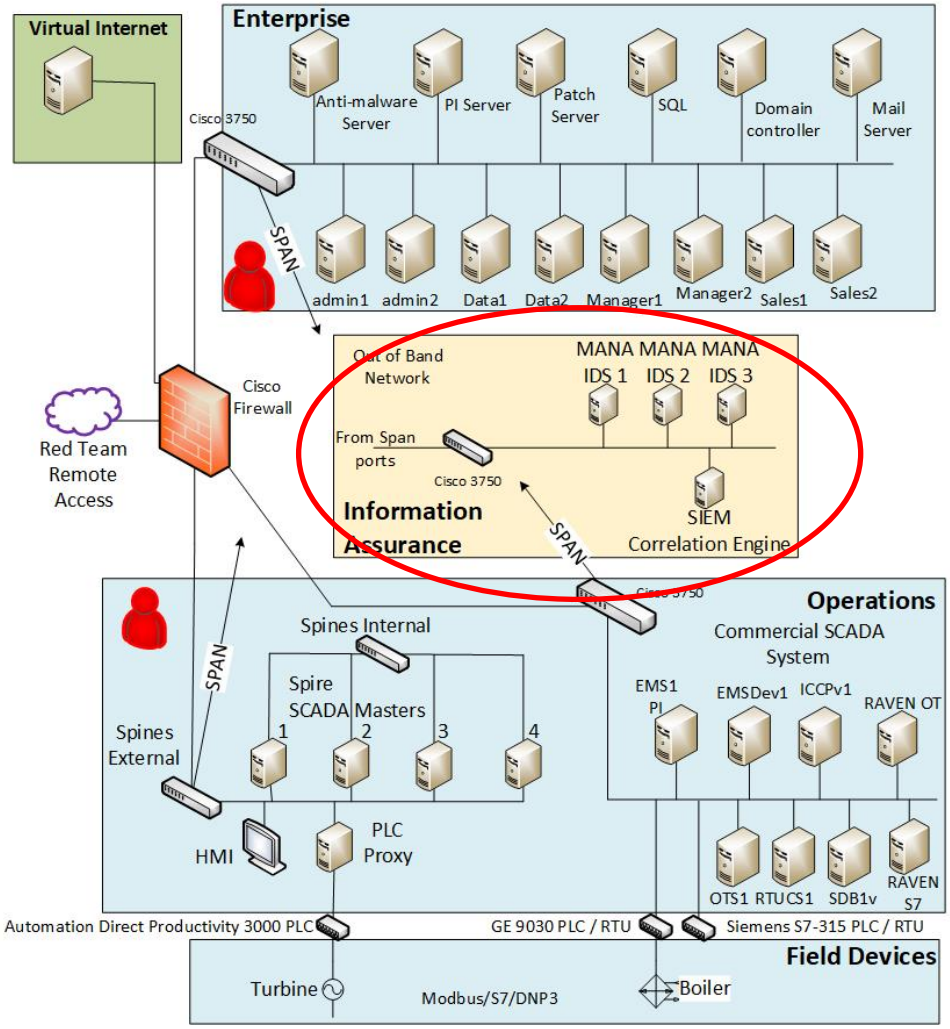
Spire System Excursion

- Excursion: Red team given access to SCADA Master replica
- User-level access
  - Stopped Spines daemon, launched modified version
  - Tried to escalate privilege
  - Patched running Spines daemon to attempt exploit
- Root access + source code
  - Primarily focused on Spines and fairness
  - Ran modified versions
- No effect on the system



MANA Experience

- Successfully detected 79% of attacks
- Dramatically outperformed signature (2% detection) and anomaly-based (28% detection) methods
- High false positives (~50%); motivated development of ARC correlation



DoD ESTCP Red Team Experiment: Lessons Learned

- Today's power grid is vulnerable
- Research-based intrusion-tolerant solutions can make a difference
- Intrusion-tolerant network + secure network setup (protected for 2 days); Intrusion-tolerant protocols (protected on 3rd day during excursion)
  - Evaluating relative importance of these pieces is future work

Hawaiian Electric Company Power Plant Deployment

January 22 – February 2, 2018

DoD ESTCP Power Plant Test Deployment

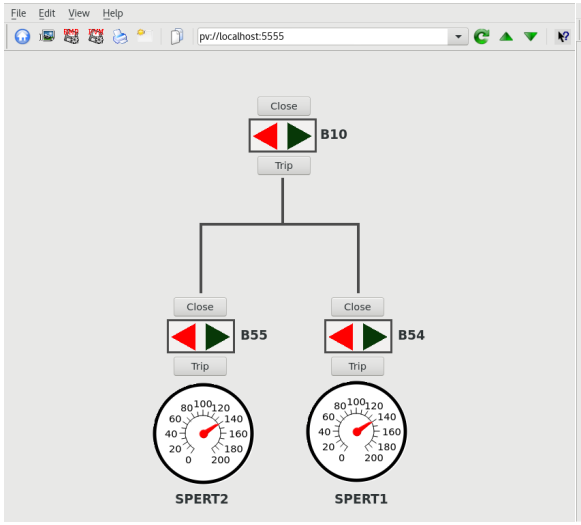
- Spire and MANA test deployment at Hawaiian Electric Company (HECO)
  - "Mothballed" Honolulu plant
- Deployment goals
  - Operate correctly in real environment without adverse effects
  - Meet performance requirements

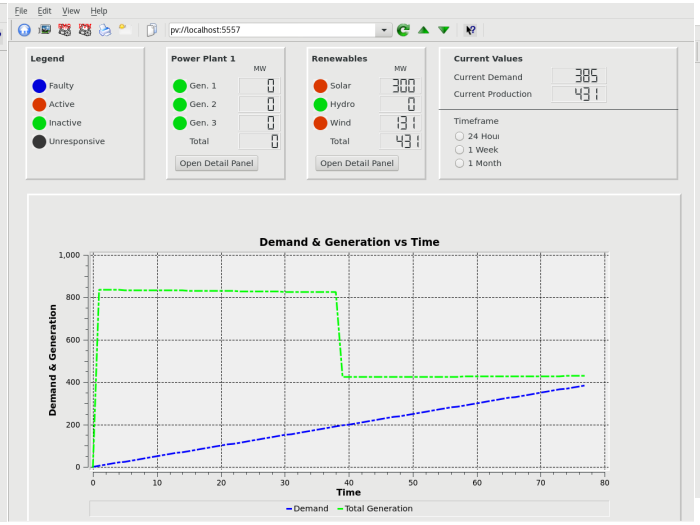
DoD ESTCP Power Plant Test Deployment

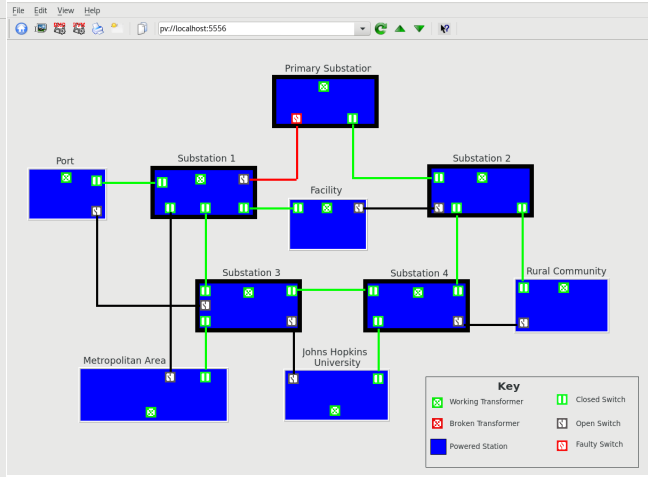
- Spire installed in Distributed Control System (DCS) room
  - Managed small power topology, controlling 3 physical breakers via Modbus PLC
- MANA deployed to monitor Certified Ethical Hacker (CEH) team activity

Spire Setup

- Spire HMIs placed in 3 locations throughout the plant: DCS room, control room, demonstration room
- 3 SCADA Scenarios: 1 with real PLC and physical breakers, 2 emulated with a total of 16 emulated PLCs

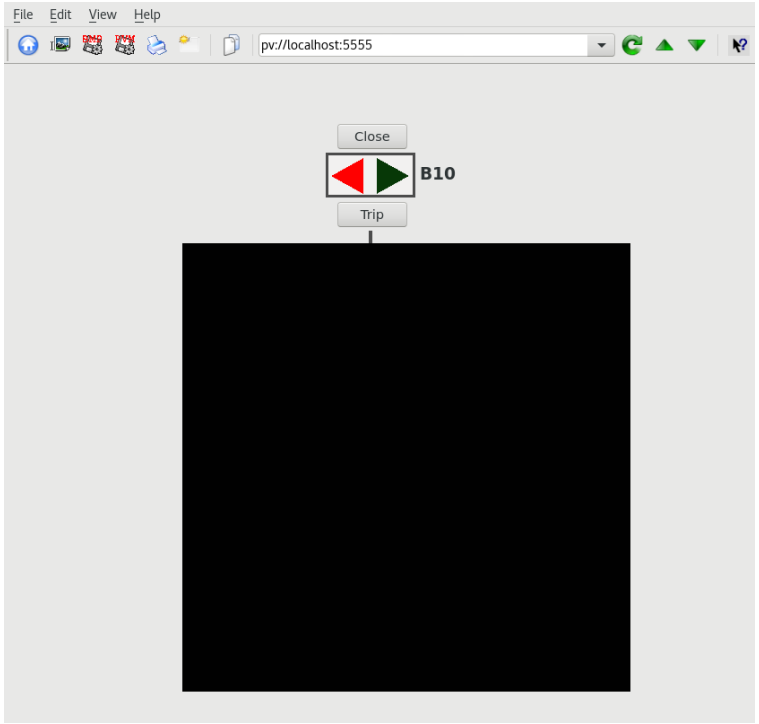






Deployment Results

- Ran continuously for 6 days without adverse effects on other plant systems
- With new correlation system, MANA detected all CEH attacks without false positives
- Timing experiment using sensor to measure HMI reaction time showed that Spire met latency requirements



Toward an Intrusion-Tolerant Power Grid

Takeaways: Technical

- Intrusion-tolerant solution substantially improves resilience compared to today's best practices
- Intrusion-tolerant replication is not sufficient on its own
  - Requires low-level secure network and OS setup to support assumptions
  - Network-level resilience is crucial: intrusion-tolerant network
  - Combining with intrusion detection and situational awareness increases utility

Takeaways: Transition

- Transition requires continued collaboration and further deployment experience
  - Power plant operations involve multiple complex subsystems, not only SCADA
    - Need close collaboration to understand and develop holistic architecture
  - Conservative ecosystem (with good reason!)
    - Incremental approach, continued trust-building
- Follow-up / ongoing discussions with Hawaiian Electric Company, Florida Power and Light, PJM
  - Considerable interest but long process