U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Verify: Energy Delivery Systems with Verifiable Trustworthiness

Oak Ridge National Laboratory (ORNL)

Stacy Prowell

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

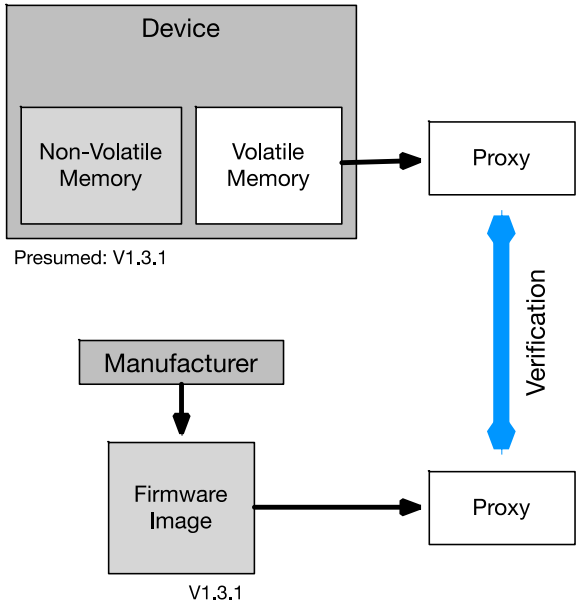
Summary: Verify

Objective

- *Automated*, *remote* verification of the integrity of the firmware of energy delivery system (EDS) devices, focusing on *volatile memory*

Schedule

- FY 2018 – FY 2020 (Delayed start until 3/2018)
- Team formed; Q1 / Q3 Hardware acquired; Q2 / Q3 Extraction; Q3 / Q4
- Provide a tool to verify the integrity of firmware used in EDS devices, without taking the equipment out of service



Total Value of Award:	**$ 800K**
Funds Expended to Date:	**% 53**
Performer:	**ORNL**
Partners:	**TDI Technologies, Inc.** **Electric Power Research Inst.** **Electric Power Board, Chattanooga** **FoxGuard, Inc.** **Intel** **Schneider Electric** **Tennessee Tech University**

Advancing the State of the Art (SOA)

- Current SOA varies for devices; remove device from service, have device self-report, reinstall firmware
- This does not detect compromises which modify volatile memory but leave stored firmware intact
- Our approach necessarily varies by device, so we picked a set of representative devices:
  - SEL RTAC (Linux), Allen-Bradley PLC, Schneider Sage RTU (VxWorks), C-RIO
  - Remotely *sample* memory using debugging command (PLC)
    Sample memory using a host-based plugin with integrity checking (Linux, VxWorks)
  - Leverage ORNL's prior work on **Akatosh**; a system for memory checkpointing and rollback of devices
- Detect compromises that *do not touch* stored firmware; avoid taking device out of service
- Verification of both volatile memory and firmware provides a strong guarantee that the device is not compromised, and can also provide forensic information when a compromise is detected

Challenges to Success

Connection to remote device

- Partnering with TDI to leverage ConsoleWorks to connect to remote devices

Memory image extraction

- Images can be too large to transfer; exploring hashing and sampling methods

Validation of the image

- Working with FoxGuard to establish a baseline and then compare

Progress to Date

Major Accomplishments

- Survey on SCADA forensics submitted for publication: “Tools, Techniques, and Methodologies: A Survey of Digital Forensics for SCADA Systems”
- All hardware and software configured, agreement in place with Schneider
- Collaborations established; working on (1) extraction of data using PLC debugging, and (2) memory extraction using Akatosh client on other platforms

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Initially the tool will be software available to run on ConsoleWorks (vendor), but we expect to define a standard software client to perform trusted memory sampling (OEM)
- Establish collaboration with Electric Power Board of Chattanooga (already in discussion on demonstration), with EPRI, and with NRECA to promote industry acceptance

Next Steps for this Project

Approach for the next year or to the end of project

- Demonstrate extraction of memory from all devices of interest
- Establish a trust anchor for each device to prevent spoofing; for instance using an externally-provided random seed or other method, along with some proof-of-work
- Develop the “gold standard” for each comparison
- Demonstrate *verification* of a memory sample / image, and *detection* of compromise of a device