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

Safe, Secure Autonomous Scanning Solution for Energy Delivery Systems (SSASS-E)

Pacific Northwest National Laboratory (PNNL)

David Manz, PM / Thomas Edgar, PI

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: Safe, Secure Autonomous Scanning Solution for Energy Delivery Systems - M617000284

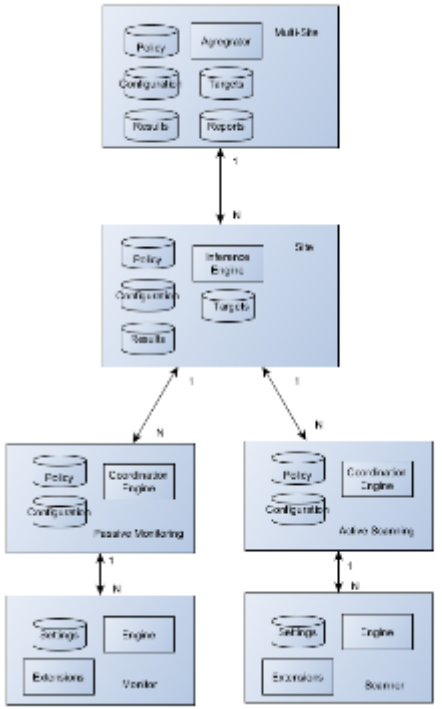
SSASS-E

Objective

- This novel solution will develop, validate, and verify an innovative safe scanning methodology, models, and architectures, and produce a prototype to transform the most widely deployed vulnerability scanner in the IT space to secure operational technology (OT) installed in critical energy infrastructure.

Schedule

- October 2017 – September 2020
- Phase 1 - Architecture and Process Design
- Phase 2 - Prototype Development
- Phase 3 - Laboratory Testing
- Phase 4 - Pilot Test



Total Value of Award:	**$ 2,500,000**
Funds Expended to Date:	**9%**
Performer:	**Pacific Northwest National Laboratory**
Partners:	**Tenable, UIUC, NRECA, Siemens, Chelan PUD**

Advancing the State of the Art (SOA)

- **Existing technology: 1) Does not provide continuous monitoring; 2) can cause disruption and degradation of service; and 3) does not provide combined vulnerability analysis and scanning across IT and OT enclaves.**
  - Lack controls on scaling approach based on risk profiles of OT environments
  - Lack inferential determination of equipment based on current evidence
  - Lack OT specific scanning approaches
- **Owners and operators of critical energy infrastructure need to improve methodologies and technology to safely and continuously scan EDSs for evolving or emerging threats, including the ability to scan OT, in addition to their other responsibilities in IT and IoT.**
  - Utilities need a way to discover all their critical cyber assets and manage vulnerabilities holistically.
  - Need ability to customize vulnerability analysis to their processes and risk stance
- **SSASS-E is designing a continuous monitoring solution that is safe, secure, and effectively eliminates blind spots in OT assets.**
  - Integrated passive monitoring and active scanning with EDS OT specific techniques
  - Probabilistic inferential device detection that provides:
    - highest confidence selection of device type: model, firmware, configuration etc.
    - Best scan type next to perform to improve confidence in device detection
  - Configuration detection and best practice guidance

Challenges to Success

Award of our contracts to our subcontractors is taking longer than anticipated.

- Milestones/deliverables require their input and they are unable to work with us until the contract has been awarded.

Large population of equipment types/variations to study for confidence in approaches

- Developed analysis of test population to provide understanding of our projects test coverage
- Will ensure laboratory testing of equipment of test pilot

Progress to Date

- **Intellectual Property Management Plan (IPMP)**
- **Subcontracts successfully executed**
  - Tenable
  - UIUC
  - Siemens
  - NRECA
  - Chelan PUD decided they did not need funds to participate.
- **Landscape survey completed**
- **Requirements gathering completed**
  - Gas Technology Institute consortium participation in utility questionnaire
- **Population selection and gap analysis whitepaper**
- **Drafted system architecture**
- **Begun collecting data for fingerprint analysis**

Collaboration/Technology Transfer

- Fingerprint Analysis study
  - Collect data
- Design Methodology and Architecture for Discovery in OT environments
  - Architecture design
  - Detection methodology leveraging different approaches
    1. Active scanning: interrogate and query a device;
    2. Passive scanning deep packet: given knowledge of protocol and system, infer information.
    3. Passive scanning header/ broadcast: listen for broadcast and multicast traffic
    4. Out of band: authenticated query of engineering access to device and existing or queried configuration files (active against engineering systems).
- Develop prototype capabilities that integrate with Tenable's platform
  - Integrates with Nessus Network Monitor, Nessus Vulnerability Scanner, and Nessus Enterprise
- Laboratory Test prototype
- Field test prototype at partner site
- Open source techniques and scripts

Next Steps for this Project

Short-Term Schedule:

- Finish collecting data for fingerprint analysis.
- Finish software architecture design.
- Design passive and active scanning approach.

Long-Term Schedule:

- Provide an improved solution for continuous monitoring and scanning of EDSs to support a new prototype of the SSASS-E platform.
- Validate and verify the solution, both methodology and technology, in a UIUC realistic test environment.
- Provide an improved nonintrusive methodology and solutions to vulnerability management. Supported protocols include relevant vendor- and utility-identified means of communication.
- Develop and prototype (in pilot) a platform for safe and secure autonomous scanning to improve active defense.