U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

SSASS-E: Safe and Secure Autonomous Scanning Solution for Energy Delivery Systems

Pacific Northwest NATIONAL LABORATORY

Safe and continuous scanning, analysis, and mitigation recommendations for energy delivery systems

Traditional information technology (IT) vulnerability discovery processes that actively transmit a broad range and large number of scans can cause service disruptions, degradations, and the potential for device failures. In response, industry largely relies upon manual system configuration documentation. This method quickly becomes a stale and passive monitoring process, which is limited in its capacity for asset and vulnerability discovery. Asset owners often need to implement multiple and separate services for vulnerability scanning and analysis capabilities. SSASS-E provides an improved methodology and technology for electricity and oil and natural gas asset owners and operators to continuously monitor Energy Delivery Systems (EDS) and critical IT/operational technology (OT) assets needed for reliable delivery of energy. It also produces a continuous monitoring solution that is safe, secure, and eliminates blind spots by identifying and analyzing transient mobile, virtual, cloud, IT, and OT assets. Utility operators will receive context-aware solution recommendations based on relevant and unique OT/EDS data sets.

KEY TAKEAWAYS

- Minimizes and optimizes the types and frequency of probes necessary for accurate asset and discovery of potential vulnerabilities
- Enables tuning of active scanning behavior to meet specific user risk profiles
- Conducts realistic and operational testing to deliver trustworthy, data-driven recommendations for industry decision makers

OUTCOME

This project provides improved non-intrusive methodology and solutions to vulnerability management and mitigation strategy identification. The toolset enhances cyber awareness and improves active discovery capabilities that will be made available for use by energy utilities nationwide.

PARTICIPANTS	ROLE
Pacific Northwest NATIONAL LABORATORY	Project lead; designs the integrates architecture of tools leveraging Tenable's NESSUS toolset and develops a prototype including open source and custom tools
tenable	Provides expertise in passive monitoring and active scanning techniques and support in using existing commercial tools
P.U.D. CHELAN COUNTY	Industry advisor and pilot partner
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN	Provides expertise in passive analysis and support in testing tools
NRECA America's Electric Cooperatives	Industry advisor
SIEMENS	Industry vendor advisor and support in testing tools

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

David Manz
Project Manager
Pacific Northwest National Lab
509-372-5995
david.manz@pnnl.gov

Thomas Edgar
Principal Investigator
Pacific Northwest National Lab
509-372-6195
thomas.edgar@pnnl.gov

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

Period of Performance: October 2017 – March 2021

Total Award Value: $2,500,000
DOE Share: $2,500,000
Cost Share: $0

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021