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

MEEDS: Mitigation of External-Exposure of Energy Delivery System Equipment

Pacific Northwest NATIONAL LABORATORY

Leveraging vulnerability database search engines for energy delivery system detection, identification, and risk mitigation

Energy delivery system (EDS) devices are often inadvertently exposed to the Internet, which can be used by adversaries to enter the system, disrupt operation, and cause damage or injury. It is essential to monitor for and detect any exposed devices so that these threats can be mitigated. This project improves the cyber risk management process by proactively identifying, detecting, and responding to vulnerable EDSs inadvertently exposed to the public Internet. It helps determine relative risk and facilitates user mitigation of vulnerabilities with an easy-to-use tool. MEEDS builds upon existing vulnerability database technologies, such as Shodan, that collect information about critical systems that are publicly visible to the Internet. MEEDS has been demonstrated at a partner utility.

KEY TAKEAWAYS

- Delivers an effective, easy-to-use dashboard on externally exposed energy delivery systems and their published vulnerabilities
- Performs non-intrusive online detection and identification of energy delivery systems exposed to the Internet without degradation or disruption of services
- Distills cyber intelligence from multiple vulnerability databases to help operational technology-based facilities determine mitigation strategies for the exposed devices
- Applies adversarial tactics to increase cyber risk awareness for utility owners and operators

OUTCOME

MEEDS assists with improving cyber risk management of EDS by delivering a configurable and customizable dashboard summarizing identified concerns and creating a relative risk metric. MEEDS has been demonstrated to the National Rural Electric Cooperative Association with a planned pilot demonstration at multiple utility cooperatives. MEEDS' relative-risk assessment framework was accepted to the Hawaii International Conference on System Sciences 2020 conference. A patent related to MEEDS core building blocks and a copyright related to MEEDS software components (server and client) are in the filing process.

PARTICIPANTS	ROLE
Pacific Northwest NATIONAL LABORATORY	Designs and develops tool architecture and software application.
SHODAN	Provider of Shodan search engine for identifying internet-facing Operational Technology/Information Technology devices.
Hawaiian Electric	Utility advisor to the project.
NRECA America's Electric Cooperatives	Generates design requirements, performs document reviews and tool testing, and coordinates end-user participation.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Sri Nikhil Gupta Gourisetti
Principal Investigator
Pacific Northwest National Laboratory
509-375-7350
srinikhil.gourisetti@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 – July 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