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

Evaluating Effectiveness of an Embedded System Endpoint Security Technology on Energy Delivery System Operational Technology: Defeating the Hackers of Industrial Internet of Things Devices

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Centralized lightweight security for vulnerable low-power devices at the edge of energy delivery systems

Industrial Internet of Things (IIoT) devices across energy delivery systems (EDS) are highly vulnerable to cyberattacks. These low-memory and low-power devices are unable to house the gigabytes of data and malware memory signatures required to operate antivirus software, leaving them highly susceptible to exploitation. The research team will bridge this gap by studying an embedded end-point security technology that was originally designed for the unique requirements of non-industrial enterprise IoT devices and customizing it for EDS. They will operationalize a lightweight command and control agent that fits on EDS endpoint devices to streamline IIoT device operating system updates without impacting EDS operations.

KEY TAKEAWAYS

- Develops endpoint device security for energy delivery systems based on proven enterprise solutions
- Implements security updates without impacting energy delivery system operations
- Efficiently collects and analyzes energy delivery system endpoint device data to adequately address security requirements

OUTCOME

This project overcomes deficiencies in existing IIoT security solutions, including vulnerabilities to control signal distortion, timing-based attacks, and inefficient and disruptive network traffic analysis-based programs. The developed tool allows all IIoT devices across NRECA member utilities to rapidly implement critical and verified security recommendations, regardless of endpoint hardware.

PARTICIPANTS	ROLE
CREDC CYBER RESILIENT ENERGY DELIVERY CONSORTIUM	The CREDC performs multidisciplinary research and development that focuses on the cybersecurity of energy delivery systems. The central project goal is to create an ecosystem where research results lead directly to the development of applications and methodologies, which are then validated in realistic contexts.
Massachusetts Institute of Technology	Leads research, development, and testing
SIEMENS	Engages industry stakeholders
Schneider Electric	Engages industry stakeholders
NRECA America's Electric Cooperatives	Collects and analyzes IIoT EDS data
Pacific Northwest NATIONAL LABORATORY	Provides industrial control system testbed
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN	Provides industrial control system testbed

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Michael Siegel
Principal Research Scientist
Massachusetts Institute of Technology
617-253-2937
msiegel@mit.edu

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

This is a subproject sponsored by the CREDC academic consortium, led by the University of Illinois.

CREDC Period of Performance: October 2015 – May 2022

CREDC Total Award Value: $28,099,258
DOE Share: $22,476,290
Cost Share: $5,622,968

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