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

Energy Delivery Systems with Verifiable Trustworthiness

OAK RIDGE National Laboratory

Protecting programmable logic controllers from fileless malware

Industrial control systems no longer operate in isolation but use other networks to facilitate and improve business processes, increasing their exposure to cyber threats. A significant threat is "fileless malware," where malware resides in device memory but does not leave persistent forensic traces in permanent storage. Fileless malware effectively bypasses detection by whitelisting systems and evidence is lost when the device is taken out of service for scanning. Malware can enter into the system via vulnerabilities or compromised firmware. This project enables the rapid, automated, and remote verification of the integrity of executable software on energy delivery system (EDS) devices without taking the device out of service and with minimal impact to device operation. By comparing the firmware in memory from EDS devices in service against a "gold standard," the team may identify vulnerabilities and present the results to system operators.

KEY TAKEAWAYS

- Verifies the integrity of loaded firmware used in energy delivery system devices without taking the equipment offline
- Detects fileless malware threats and runs on-demand assessments of executable memory content with minimal impact to the device performance and network bandwidth
- Provides utilities with an automated means for North American Electric Reliability Corporation critical infrastructure protection compliance testing

OUTCOME

This project provides a tool for automated scanning of firmware and comparison of programming on devices for vulnerability assessment and malware detection.

PARTICIPANTS	ROLE
Oak Ridge National Laboratory	Develops memory sampling technology
epb	Partners for technology demonstration
Schneider Electric	Advises on service development, demonstration, and distribution
NRECA America's Electric Cooperatives	Advises on service development, demonstration, and distribution
ISASecure®	Advises on service development, demonstration, and distribution
TVA	Partners for technology demonstration
GE	Partners and deploys solution to grid hardware

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Stacy Prowell
Principal Investigator
Oak Ridge National Laboratory
865-241-8874
prowellsj@ornl.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 – June 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