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

Continuous Security Monitoring Protocols and Architectures for Energy Delivery Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Efficient, comprehensive, and vendor-agnostic security auditing tools for energy delivery system infrastructures

This research explores methods to implement cost-effective, automated, and continuous security auditing tools for energy delivery systems (EDS). Security audits require the collection of a variety of information, including system configurations, software versions, account management, password policies, and anomalous events. Manual audits are expensive and many auditing tools are intrusive and can cause system malfunctions. This team is exploring and evaluating automated techniques to improve the collection and analysis of security data within an EDS to detect anomalous behavior in system components. This includes the development and implementation of the Threat Observability & Monitoring Assessment Tool (TOMATo), which helps utilities identify security monitoring data sources that most efficiently detect attacks. This task identifies new methodologies and protocols that provide EDS owners with a timely and accurate understanding of their system's security posture.

KEY TAKEAWAYS

- Explores methods for security monitoring of EDS without impacting time-critical operations or system stability
- Improves the collection and analysis of security data within energy delivery system networks to identify vulnerabilities in system configurations and detect anomalous behavior
- Minimizes costs and increases efficiency of energy delivery system security audits

OUTCOME

This project assesses techniques to detect and analyze threats and abnormal behaviors in EDS operational technology networks as well as in the advanced metering infrastructure to efficiently and accurately identify different types of attacks. The resulting methodologies will introduce vendor-agonistic standards for continuous monitoring requirements to encourage interoperable vendor technologies in the future.

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.
WASHINGTON STATE UNIVERSITY	Leads research, development, and testing
MITRE	Provides access to MITRE ATT&ACK tool to integrate with TOMATo

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Chen-Ching Liu
Professor
Washington State University
509-335-1150
liu@eecs.wsu.edu

Adam Hahn
Site Lead, Assistant Professor
Washington State University
509-335-2343
ahahn@eecs.wsu.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