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

Data Sharing for Energy Delivery Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Engaging machine learning to enhance the security of threat information sharing between energy delivery systems vendors and operators

Data and information sharing are an effective strategy that can help reduce cybersecurity threats in energy delivery systems (EDS). By developing and sharing attack signatures with other EDS operators, proactive deployment of defenses can prevent the spread of a known attack. The Data Sharing for Energy Delivery Systems project focuses on investigating and developing secure, infrastructure-agnostic data and information sharing schemes for EDS based on the secure querying of machine learning (ML) classifiers. The goal of this project is to create mechanisms for protecting enterprise confidentiality including the development of ML models that protect training data and cannot be used to infer enterprise information or the EDS that generated the classifier. Overcoming classifier security obstacles will encourage more widespread and rapid threat and information sharing across EDS vendors and operators.

KEY TAKEAWAYS

- Develops a more comprehensive understanding, and proposes solutions to mitigate the risks, of data leakage associated with the sharing of machine learning threat classifiers
- Helps energy delivery system stakeholders such as utilities, equipment vendors, and security consultancies to securely and rapidly identify and mitigate emerging security threats
- Generalizes threat signatures to be applicable for all infrastructure topologies

OUTCOME

The research conducted through the Data Sharing for Energy Delivery Systems project will increase the security of threat information sharing through ML classifiers, making it faster and easier for EDS vendors and operators to monitor, identify, and mitigate security risks. This allows vendors to better manage current incidents and determine how changes to the underlying infrastructure and topology may help prevent future incidents.

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.
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN	Leads research, development, and testing
paloalto NETWORKS	Provides cybersecurity datasets and ML classifiers

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Carl Gunter
Professor
University of Illinois
217-244-1982
cgunter@illinois.edu

Nikita Borisov
Associate Professor
University of Illinois
217-244-5385
nikita@illinois.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