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

Automated Network Access Policy Hardening

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

An open-source solution to identify risk exposure, modify network security, and strengthen access controls

Energy delivery system (EDS) operators manage large-scale and complex networks of inter-connected assets that must comply with best practices and be continuously monitored across multiple inter-meshed access control policies. This project introduces a solution to automate the hardening of network access policies. This project designs and implements an open-source software module that analyzes network topology, access control policies, and device-to-device connectivity maps to compute a network-wide risk exposure index. This index can be used to automatically identify and harden security policies to protect network assets against adversarial access via vulnerable lateral movement pathways within the network. Cybersecurity recommendations are ranked by the likelihood of the identified pathway to be exploited by an intruder. A policy optimization algorithm leverages firewall configuration best practices and externally provided vulnerability advisories to develop actionable improvement plans.

KEY TAKEAWAYS

- Identifies risk exposure caused by weak access controls within and between inter-connected assets across energy delivery systems
- Automatically hardens security policies to minimize adversarial lateral movement in the event of unauthorized network access
- Equips network operators with tools to measure progress towards implementing cybersecurity best practices

OUTCOME

This project better equips EDS operators and organizations to adopt a culture of cyber resilience across increasingly complex infrastructures. The open-source platform engages external inputs from across the energy sector to deliver and optimize measurable indices for determining progress towards the adoption of evolving best practices. This allows organizations to address and compare network architectures and access policies across different business units to ensure the implementation of critical access controls at large scale.

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
network perception	Provisions commercial offerings to generate inputs; provides in-kind technical support; and identifies potential customers for testing and evaluation of the developed tool

CONTACT INFORMATION

Initial Leads:

David M Nicol
CREDC Principal Investigator
Director, Information Trust Institute
217-244-1925
dmnicol@illinois.edu

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