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

Modeling Security Risk and Resiliency of Energy Delivery Systems Using Software-Defined Networks and Robust Networked Control Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Advancing energy delivery system resiliency through real-time system risk assessment and reconfiguration

The research team is operationalizing a software-defined networking-based (SDN) energy delivery system (EDS) controller to autonomously identify and contain false data injection attacks. The team formally models risk assessment and network diversity to assess the resiliency of EDS against zero-day attacks and quantify the impacts of various attack paths on EDS. The risk assessment model classifies attacks in terms of how severely they will impact the cyber-physical system's operation, which corresponds to a uniform scoring structure. The model also quantifies the security posture of the cyber-physical network at any given time, allowing SDN components to compare their individual security score to that of the overall system. When the EDS identifies scoring discrepancies, the SDN controller autonomously takes evasive action, such as enacting quarantine procedures, for affected system components. This program ensures continued operations of the power grid with minimal impact, even during active attacks.

KEY TAKEAWAYS

- Quantifies cybersecurity risks for energy delivery systems, allowing systems to identify and mitigate attacks quickly and autonomously
- Ensures seamless and continued operations of the power grid during false data injection attacks
- Implements software-defined networking for logical partitioning of energy delivery system communication infrastructure

OUTCOME

This project advances SDN implementations for EDS, making it possible to modify network configurations/topology in real time based on risk assessments of known or zero-day attacks. The advanced system modeling capabilities delivered by this research not only facilitate rapid response, but will also increase system state awareness, allow EDS operators to anticipate and analyze multi-stage attacks, and predict and prevent significant impacts.

PARTICIPANTS	ROLE
CREDC CYBER RESILIENT ENERGY DELIVERY CONSORTIUM	The CREDC performs multidisciplinary research & 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.
OLD DOMINION UNIVERSITY	Lead institution; develops domain-specific risk assessment models; develops and verifies attack detection algorithms
TENNESSEE STATE UNIVERSITY	Partner institution; provides student-supported development of models and algorithms
accenture	Provides a testbed for modeling technique development and tool verification
MidAmerican ENERGY OBSESSIVELY, RELENTLESSLY AT YOUR SERVICE®	Engages stakeholders

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Sachin Shetty
Site Lead, Associate Professor
Old Dominion University
757-686-6233
sshetty@odu.edu

Leehyun Keel
Site Lead, Professor
Tennessee State University
615-277-1611
lkeel@tnstate.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