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

Advanced Networking Technology for Energy Delivery Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Engaging software-defined networks to undermine and expose malicious actors before an attack

Intrusion detection programs react after identifying the successful initialization of a cyberattack within an affected network. This project develops and demonstrates new tools and technology, called Raincoat, to disrupt the preparation of an attack strategy by a malicious actor. The researchers are combining advanced and validated software-defined network (SDN) implementations for the power grid with algorithms that continuously mislead an attacker into designing ineffective attack strategies. This approach exposes the attacker's presence within the system and prevents system damage. Raincoat supports an adaptive monitoring environment to enhance electric grid resiliency to variety of attacks.

KEY TAKEAWAYS

- Misleads would-be attackers into planning ineffective attack strategies
- Validates software-defined network implementations and intelligent security algorithms for electric grid application
- Eliminates the reliance on inefficient moving target and Honeypot defense mechanisms

OUTCOME

This project shifts electric grid security procedures from reactive to proactive. Raincoat-enabled SDN will enhance control efficiency, reduce operational costs, and increase the resiliency of energy delivery systems against accidents and cyberattacks.

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.
ILLINOIS	Leads research, development, and testing
SEL SCHWEITZER ENGINEERING LABORATORIES	Provides SDN-enabled switches for an experimental platform
Ameren ILLINOIS	Engages utility testbed stakeholders

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

David Nicol
Principal Investigator
Director, Information Trust Institute
Professor, University of Illinois
217-244-1925
dmnicol@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