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

Increasing Security in a Resilient Energy Delivery Infrastructure through the Analysis of Vulnerability and Exploit Markets

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Analyzing the buying and selling of vulnerability information to secure energy delivery systems

This research develops modeling and data analytics solutions for reducing the number of offensive vulnerabilities and limiting the exploits that affect energy delivery systems (EDS). The team will establish a bug bounty program to examine the offensive and defensive markets and their participants. Observing trends in the buying and selling of vulnerability information, mapping key players, and analyzing the structure of their interactions will aid in the development of policies for firms, states, and standards organizations. Understanding the benefits and limitations of both individual and collaborative vulnerability discovery programs is essential to the successful reduction of vulnerabilities and exploit capabilities in EDS. The research team is examining information sharing efforts and system simulation environments to streamline resource allocation decision making based on vulnerability market behaviors and threat intelligence.

KEY TAKEAWAYS

- Analyzes risk exposure for energy delivery systems and exploitation capabilities of potential attackers
- Examines the prevalence of zero-day vulnerabilities in energy delivery systems
- Establishes bug bounty and information sharing programs to improve energy sector threat intelligence

OUTCOME

This research develops an understanding of vulnerability markets and their effects on EDS cybersecurity requirements. The team will deliver comprehensive approaches for reducing vulnerabilities in EDS based on community-supported threat intelligence.

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.
Massachusetts Institute of Technology	Leads research, development, and testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Michael Siegel
Principal Research Scientist
Massachusetts Institute of Technology
617-253-2937
msiegel@mit.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