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

Increasing Cyber-Resilience of Large-Scale and Long-Lived Energy Delivery Infrastructure

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Preventing and mitigating cybersecurity risks in energy delivery infrastructure

As energy sector infrastructure transforms to massively distributed networks of low-powered, embedded, and long-lived network edge devices, security becomes more difficult to ensure and maintain. The penetrate and patch approach that kept computers secure will no longer work when devices become too long-lived, too cheap, too invisible, and too numerous. This makes energy delivery systems (EDS) especially vulnerable to zero-day attacks as new components are introduced into systems. Also, legacy systems are vulnerable since they are no longer updated, patched, or maintained by vendors, as embedded devices age. The research team analyzes current coding practices and protocol standards to identify fundamental sources of vulnerabilities, develop new methods to reduce or eliminate them, and evaluate the effectiveness of mitigation strategies by modeling the attack risk and potential damage in infrastructure.

KEY TAKEAWAYS

- Addresses critical security concerns introduced by the distribution of embedded energy delivery system devices
- Prevents the installation of vulnerable system components and mitigates identified risks
- Evaluates the efficacy of security tools and procedures across expansive and variable infrastructure

OUTCOME

This research contributes to a culture of security across EDS vendors and operators by developing an understanding of how EDS remains vulnerable to attack, fostering resiliency. The models developed help EDS operators reduce system vulnerabilities and become more effective at mitigating identified risks across complex infrastructures.

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.
Dartmouth	Lead institution; leads analysis of industry specific protocols and development of secure parsers for each.
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN	Partner institution; provides support for the development of secure parsers
AUTOMATAK	Industry partner (industrial cybersecurity consultant)
DOVER ENERGY AUTOMATION	Industry partner
GE	Collaborator on security-aware protocol parser
SEL SCHWEITZER ENGINEERING LABORATORIES	Industry partner (leading substation equipment vendor)
WATERFALL Stronger Than Firewalls	Industry partner

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Sean W. Smith
Site Lead, Professor
Dartmouth College
603-646-1618
sws@cs.dartmouth.edu

Sergey Bratus
Research Associate Professor
Dartmouth College
603-646-2206
sergey@cs.dartmouth.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