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

Fast and Scalable Authentication in Energy Delivery Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Increasing smart grid security through low-overhead and scalable cryptographic solutions for energy delivery system domains

Within energy delivery system (EDS) infrastructure, expansive networks of interconnected devices collect and share critical information to maintain network operations, including ensuring high-quality and efficient service for consumers. This increases the attack surface, creating the need for fast and scalable authentication for these devices. However, existing encryption and authentication protocols that rely on public key infrastructure (PKI) require too much bandwidth and processing power for many smart grid devices such as sensors, actuators, and meters. In this project, the research teams investigate and validate affordable and scalable alternative solutions to traditional PKI for smart grid device security, communication validation, and identity authentication.

KEY TAKEAWAYS

- Enhances the security of smart device communication with minimal overhead
- Investigates new cryptographic key exchange strategies to simplify device authentication across large-scale energy delivery system infrastructures
- Promotes a culture of field device security for vendors and network operators

OUTCOME

This project delivers scalable cryptographic solutions for securing and authenticating communications between smart grid devices. This work reduces barriers to encrypting communication between smart grid devices and enhances the culture of security for EDS infrastructure vendors and operators.

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 the development of fast scalable authentication methods, inspired by Google's 'macaroons' concept
ILLINOIS	Partner Institution; leads the development of models of large-scale networks, which implement the macaroons-based methods
SDGE A Sempra Energy utility	Engages stakeholders
AUTOMATAK	Collaborates on Secure SCADA Protocol for the 21st Century (SSP21)
SCTE · ISBE Society of Cable Telecommunications Engineers International Society of Broadband Experts	Collaborates on Secure SCADA Protocol for the 21st Century (SSP21)
WATERFALL Stronger Than Firewalls	Provides consultations on Public Key Infrastructure (PKI) in EDS
GE	Collaborates on secure parser

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

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

David M. Nicol
CREDC Principal Investigator
Information Trust Institute, Professor
University of Illinois
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