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

Lightweight, Delay-Aware, and Scalable Cryptographic Services for Smart Grid Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Securing smart grid communications with advanced and proven cryptography

Smart grids are vulnerable to false message injection, fake measurements, and tampering with command and control information. Existing security mechanisms are either not scalable, too slow, or too costly for smart grid application, causing a critical lack of real-time authentication and data integrity verification within these systems. This project introduces a suite of very fast, scalable digital signatures that can meet the needs of smart grids. The research team is designing and validating lightweight cryptographic schemes, creating an open-source cryptographic framework, and developing educational course modules to facilitate widespread application.

KEY TAKEAWAYS

- Develops and validates an open-source cryptographic framework for fast and scalable smart grid security

OUTCOME

This research produces an open-source cryptographic solution that offers advanced security to smart grid infrastructures and has broad applicability to other domains with time-critical needs such as vehicular networks, wireless sensors, and air drones.

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.
Oregon State University	Leads research, development, and testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Attila Yavuz
Assistant Professor
University of South Florida
813-974-0419
attilaayavuz@usf.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