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

Assured Cyber Supply Chain Provenance Using Permissioned Blockchain

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Mitigating cyber supply chain risks to guarantee energy delivery system component authenticity and security

This project leverages advances in blockchain technology to protect against critical risks to the cyber supply chain. As energy delivery system (EDS) networks become increasingly automated and reliant on smart device communication, they also become increasingly vulnerable to cyber security risks such as software counterfeits, unauthorized device production and sourcing, and the insertion of malicious software and hardware. The research develops permissioned blockchain-based techniques to certify the authenticity of EDS software/firmware at all stages of the cyber supply chain. The project delivers integrity mechanisms for permissioned blockchain platforms so that critical data remains secure even in the presence of data breach attacks. The team also investigates techniques to encourage widespread adoption of these systems across EDS vendors and operators.

KEY TAKEAWAYS

- Introduces a permissioned blockchain to the energy delivery system cyber supply chain
- Increases confidence in the authenticity and security of system software/firmware components
- Investigates game theory-based techniques to expand blockchain participation across vendors and operators

OUTCOME

This project develops and promotes the adoption of supply chain authentication tools for guaranteed EDS device security. End-users will be able to easily verify the authenticity of software/firmware in purchased electronic devices, reducing the risk of supply chain-based attacks on EDS infrastructure.

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.
OLD DOMINION UNIVERSITY	Lead institution; applies hyperledger methodology to problem of tracking software changes and provenance
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN	Partner institution; develops blockchain algorithms tailored to the domain context and software provenance validation
EPRI ELECTRIC POWER RESEARCH INSTITUTE	Industry collaborator; provides solution validation
RELIABILITYFIRST	Industry collaborator; publishes a joint paper
NRECA America's Electric Cooperatives	Engages stakeholders; provides solution validation

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Sachin Shetty
Site Lead, Associate Professor
Old Dominion University
757-686-6233
sshetty@odu.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