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

KISS: Keyless Infrastructure Security Solution

Pacific Northwest NATIONAL LABORATORY

A trustworthy path to cyber resiliency for energy delivery systems

Energy delivery systems (EDS) operating at the grid's edge require unprecedented levels of security and trustworthiness to verify the integrity of data and manage complex, transactive, and distributed energy resource (DER) exchanges. Grid edge devices lack visibility, control, and security to conduct real-time energy transactions with the required security, speed, and scale. This project develops a keyless infrastructure security solution (KISS) to increase the trustworthiness, integrity, and resiliency of EDS. KISS delivers the first blockchain-based prototype to continuously monitor and autonomously verify energy exchanges; constructs a plugin for blockchain smart contracts to maintain ordered and timestamped data blocks that cannot be retroactively modified; and verifies that KISS can validate transaction data and rapidly detect data anomalies. KISS uses private blockchain technology with proof-of-authority consensus to provide an atomically verifiable cryptographic distributed ledger to increase the trustworthiness, integrity, and resiliency of EDS data stored in an energy management system historian and data-in-transit between a distribution management system and an EDS device. KISS secures the EDS supply chain at the grid's edge by enhancing the cyber security integrity features in the EDS and VOLTTRON™ platform (a Department of Energy supported open source platform for distributed sensing and control) by providing integrity violation and tamper detection capabilities for application, configuration, and endpoint telemetry services.

KEY TAKEAWAYS

- Uses private blockchain for secure operational technology configuration management and supply chain security
- Autonomously detects data anomalies and normalizes evidence across a unified timeline for incident analysis
- Provides real-time response to unauthorized attempts to change critical energy delivery system data, configurations, applications, appliances, and sensors

OUTCOME

KISS developed the first blockchain for cybersecurity alpha prototype to perform a proof of concept for continuously monitoring and autonomously verifying data exchanges at the grid's edge. The technical products of the KISS project includes: two filed patents pertaining to the core components of data-at-rest and data-in-transit security, and the supply chain security and auditing architecture; the paper "Enabling Secure Grid Information Sharing through Hash Calendar-based Blockchain Infrastructures" presented at the 2019 Resilience Week; a demonstration video; and three design architecture reports "Security Trust Analysis of Blockchain for Energy Cybersecurity," "Complex Grid Communications Architecture using Blockchain," and "VOLTTRON™ to Private Blockchain Integration: Specifications and Requirements."

PARTICIPANTS	ROLE
Pacific Northwest NATIONAL LABORATORY	Co-developed the VOLTTRON™ plugin to work with existing Guardtime blockchain capability and tested prototype trustworthiness and integrity of data-at-rest contained within the EMS historian.
guardtime	Co-developed the VOLTTRON™ plugin to work with their existing blockchain capability.
WASHINGTON STATE UNIVERSITY	Tested prototype trustworthiness of data-in-transit between DMS and endpoint devices.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Sri Nikhil Gupta Gourisetti
Principal Investigator
Pacific Northwest National Laboratory
509-375-7350
srinikhil.gourisetti@pnnl.gov

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

Period of Performance: September 2017 – September 2020

Total Award Value: $1,048,528
DOE Share: $1,048,528
Cost Share: $0

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