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

GridTrust: Electricity Grid Root-of-Trust Decentralized Supply Chain Cybersecurity

Georgia Institute of Technology

Mitigating supply chain attacks with physics-based device authentication

Traditional supply chain protections include physical labels, patents, and information stored in a device's non-volatile memory, all of which are vulnerable to tampering. Recent advances in physically uncloneable functions (PUFs) provide physics-based generation of numbers that can be used in traditional security protocols, such as authentication and encryption, and enable highly secure device verification. Because PUFs are not controlled by software, they cannot be attacked by software. Implementing PUF-based security on electric grid components provides provable Root-of-Trust (RoT) technology that physically authenticates devices within cryptographic systems. This enables the implementation of systems and policies that improve the cybersecurity of the grid and its supply chain. GridTrust is a PUF-based cyber-physical solution that authenticates devices via physically provable unique identifiers tied to their RoT and a standard suite of encryption tools. The team is designing, demonstrating, and commercializing a framework to coordinate supply chain cybersecurity based on physically provable RoT. The resulting GridTrust Box can be installed within electric utilities to authenticate devices, making supply-chain attacks on the electric grid more difficult.

KEY TAKEAWAYS

- Leverages advances in physically uncloneable functions to introduce tamper-proof root-of-trust technology in electric utility devices
- Develops and validates the GridTrust Box to authenticate physical devices across electric grid infrastructures
- Commercializes and deploys a cyber-physical solution to mitigate supply chain attacks

OUTCOME

GridTrust minimizes the risk of cyberattack to electric utilities through supplier cyber-physical systems, enables stronger forms of hardware and software integrity and authenticity, and enhances supplier risk management and procurement controls.

PARTICIPANTS	ROLE
Georgia Institute of Technology	Coordinates general project management, as well as all GridTrust commercialization and demonstration tasks. Leads the research and development of GridTrust system architecture, hardware design and implementation, testing, and simulations.
Sandia National Laboratories	Develops the requirements on cybersecurity and supply chain security. Leads the emulation of GridTrust and substation hardening pathways.
PROTECT OUR POWER	Advises on grid supply chain and cybersecurity gaps. Identifies vendors and coordinates outreach and communications with industry stakeholders and GridTrust implementers.
OSIsoft.	Provides the mission-critical, real-time database, which is the core of the supply chain cybersecurity simulation environment. Offers expertise on protocol and data connectors for real-time control devices and advises on grid supply chain control systems.
Southern Company	Advises on grid supply chain cybersecurity and use cases. Coordinates the demonstration at the Georgia Power Research Microgrid.

CONTACT INFORMATION

Initial Leads:

Santiago Grijalva
Principal Investigator
Georgia Institute of Technology
404-894-2974
sgrijalva@ece.gatech.edu

Vincent Mooney
Co-Principal Investigator
Georgia Institute of Technology
404-385-0437
mooney@ece.gatech.edu

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: August 2020 – August 2023

Total Award Value: $3,049,673
DOE Share: $2,000,000
Cost Share: $1,049,673

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