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

Lightweight Key Management for Low-Bandwidth Legacy Environments in Smart Grid

SEEDS
CYBERSECURITY CENTER FOR
SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Achieving bandwidth-efficient symmetric key management using hash-chains for authentication

New security solutions designed for the smart grid typically do not consider the challenges of key management, where bandwidth limitations of the communication infrastructure largely depend on legacy technologies. As utilities incorporate Internet of Things (IoT) devices on top of this legacy infrastructure, bandwidth limitations become more restrictive. This project addresses the overhead of key management by developing a protocol that provides mutual authentication, key agreement, and key refreshment by utilizing a 0-Round Trip Time (RTT) message exchange scheme among field devices and the control center. This is the first 0-RTT scheme that combines dynamic hash-chains with Diffie-Helmann key exchange, while preventing any potential replay attacks, without bringing additional overhead. To further reduce the overhead, the team is adapting this scheme for User Datagram Protocol by incorporating efficient reliability features. The evaluation on both simulation and actual long-range testbed application shows that this scheme significantly outperforms other conventional approaches, such as Transport Layer Security (TLS), and is suitable for ongoing IoT and smart grid integration.

KEY TAKEAWAYS

- Integrates new secure communication protocols on legacy, low-bandwidth devices across smart grid infrastructure
- Minimizes overhead related to cryptographic key management
- Ensures time-sensitive data transfer between legacy devices without sacrificing security

OUTCOME

This project designs and implements a 0-RTT symmetric key management protocol for legacy power grid systems. The protocol achieves a 4-fold delay reduction compared to TLS, while resilient to all known types of cyberattacks. The concept is also applied to DNP3 authentication. The preliminary results of this project were published in the IEEE GLOBECOM 2019 communications conference and has been accepted as part of DOE Resilience Week 2020. The code is available to be deployed and used for real environments.

PARTICIPANTS	ROLE
SEEDS CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS	This project is part of the Secure Evolvable Energy Delivery Systems (SEEDS) academic consortium. SEEDS researches and develops innovative cybersecurity technologies, tools, and methodologies to advance the energy sector's ability to survive cyber incidents while sustaining critical functions.
FIU FLORIDA INTERNATIONAL UNIVERSITY	Research, development, and testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Kemal Akkaya
Professor
Florida International University
305-348-3017
kakkaya@fiu.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 SEEDS academic consortium, led by the University of Arkansas.

SEEDS Period of Performance: October 2015 – March 2022

SEEDS Total Award Value: $15,309,114
DOE Share: $12,226,504
Cost Share: $3,082,610

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