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

Secure Smart Metering Communications

SEEDS
CYBERSECURITY CENTER FOR
SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Significantly reducing distribution overhead for advanced metering infrastructures through cryptographic accumulator-based certificate management

As communication within advanced metering infrastructure (AMI) needs to be secured to protect user's power data, cryptographic key management becomes a challenge due to its overhead and the limited processing resources of smart meters. While using public keys eliminates some of the overhead, challenges remain regarding the management of certificates that store and certify public keys. In particular, the distribution and storage of certificate revocation lists (CRL) are major challenges due to the cost of distribution and storage across AMI networks, which have limited resources. To keep CRL distribution and storage costs effective and scalable, this project delivers two alternatives that will fit into smart grid environments: a distributed CRL management scheme that utilizes distributed hash trees and the deployment of cryptographic accumulators to reduce space requirements. The project team created a wireless mesh network testbed to implement and test these solutions. The results indicated that both approaches significantly outperform the current CRL approach, while the accumulator-based approach is ideal for minimizing distribution overhead.

KEY TAKEAWAYS

- Delivers a customized and efficient approach for certificate revocation list management
- Minimizes bandwidth requirements for maintaining certificate revocation lists across advanced metering infrastructures
- Ensures compliance with the National Institute of Standards and Technology's public key infrastructure security framework for distributed resources

OUTCOME

This project designs and implements two new certificate management techniques specifically geared for AMIs. The cryptographic accumulator-based approach achieved a tenfold reduction in distribution overhead, compared to the best existing approaches, while maintaining storage efficiency. This approach was patented by FIU. The results of this project have been published in two journals and three conference publications. The source code is available to be deployed and used in 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