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

Remote Attestation Protocol Specification and Analysis

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Effective machine-to-machine authentication and resilient system design tools for operational technology networks

Remote attestation gathers evidence about a remote device and the software/firmware on it, analyzes that evidence to develop trust that it is who it says it is, and verifies that it contains the software, signature files, and configurations required to interact with it. Existing remote attestation technology was developed for and within the context of enterprise computing and is not optimized for operational technology (OT) constraints including real-time latency and cryptographic operations. This project formalizes the steps in a remote attestation protocol for OT verification. This formal language enables the analysis of the correctness, completeness, and security of the protocol to increase the level of trust between remote devices and the efficiency of enabling device-to-device processes. The research team also delivers advanced OT system modeling and simulation to explore whether a given remote attestation protocol violates the many unique constraints in an OT network. A model of a given system, along with the costs and frequency of the application of remote attestation policies, can be used during the protocol design phase to prune away designs that will violate OT constraints.

KEY TAKEAWAYS

- Formalizes language for validating device-to-device interaction across operational technology environments
- Develops modeling and simulation capabilities to support advanced, secure, and efficient system design
- Delivers open-source tools for large utility applications

OUTCOME

This project advances remote attestation for OT networks to significantly increase the trustworthiness of OT networks and operations. The project team will open source the language and analytical tools to enable any large utility to build efficient and transparent machine-to-machine authentication mechanisms into their OT environments.

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.
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN	Leads research, development, and testing
SEL SCHWEITZER ENGINEERING LABORATORIES	Researches techniques for machine-to-machine authentication and shares its algorithms for establishing peer-to-peer trust; provides practical expertise for limiting the scope of attestation protocols

CONTACT INFORMATION

Initial Leads:

David M Nicol
CREDC Principal Investigator
Director, Information Trust Institute
217-244-1925
dmnicol@illinois.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

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