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

Containerized Application Security for Industrial Control Systems (CAPSec)

Sandia National Laboratories

A software isolation, upgrade, and migration technology designed for industrial control systems

This project increases the resiliency of industrial control system environments against malware by using software containers to isolate individual applications from the rest of the system. Software containers are lightweight processing environments that include everything needed to run an application but are isolated from the rest of the system. By containing applications, targeted malware will have access to only the individual application's containerized environment, as opposed to the entire system. Fault-tolerant algorithms will be applied to each contained application to further secure individual applications from compromise. Containers also provide the ability to create a moving target defense for applications to easily and quickly migrate across systems within the network to avoid attacks. An open source container platform will be used to isolate applications, and orchestration technologies will manage connections between the containerized applications and the broader operating system. As an added benefit, containing applications also enables operators to securely and efficiently update software without system downtime. It is critical to ensure software is patched as soon as possible to improve the cybersecurity posture of energy delivery systems.

KEY TAKEAWAYS

- Automates detection, isolation, and survivability of a compromised application
- Provides fault-tolerant containers to increase industrial control system application resiliency
- Reduces time to upgrade applications while maintaining high availability and security

OUTCOME

This project proactively defends and upgrades applications by isolating them into containers to improve security, resiliency, and availability. The containerized environment impedes a malicious actor from moving between systems and applications, even if they are able to successfully gain unauthorized access to a vulnerable system component. Additionally, this solution is resilient against application crashes and maximizes service uptime.

PARTICIPANTS	ROLE
Sandia National Laboratories	Leads the CAPSec project; research and develop (R&D) a secure containerized reference implementation to upgrade energy delivery systems in real-time
Chevron	Provides R&D guidance so that the CAPSec technology can be applied in the oil and natural gas sector
GRIMM	Provides an independent third-party cybersecurity red team assessment of the CAPSec technologies
RDECOM CERDEC Night Vision & Electronic Sensors Directorate — Conquest of Darkness	Provides a microgrid testbed environment that the CAPSec reference implementation will be applied towards
Pacific Northwest National Laboratory	Performs R&D that leverages software-defined networking flow rules to initiate responses to mitigate threats detected from the containerized environments

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Adrian Chavez
Principal Investigator
Sandia National Laboratories
505-284-6664
adrchav@sandia.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: May 2018 – May 2021

Total Award Value: $2,500,000
DOE Share: $2,500,000
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