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

Cross-Layer Moving Target Defense to Hide Critical Targets from Attacks

SEEDS
CYBERSECURITY CENTER FOR
SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Using dummy traffic to hide critical targets from compromised internal nodes in substation networks

This project hides critical targets in electric substation networks from compromised internal nodes and protect them from further attacks. Specifically, the team studies how to add carefully controlled dummy traffic to a substation network to make critical target nodes indistinguishable from other nodes in network traffic patterns. Because adding dummy traffic increases the consumption of bandwidth, a dummy traffic generation scheme is carefully designed to achieve the desired defense performance.

KEY TAKEAWAYS

- Provides a solution for hiding critical targets from compromised internal nodes
- Prevents malicious actors from performing traffic analysis inside the network to identify critical targets for advanced attacks
- Compensates for traditional firewalls and intrusion detection systems that cannot detect passive espionage from an internal node

OUTCOME

This project delivers an algorithm for generating dummy traffic to hide critical targets in substation networks. Simulations show that this solution increases the bandwidth by 50% when providing reasonably good protection.

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.
UNIVERSITY OF ARKANSAS	Research, development, and testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Qinghua Li
Associate Professor
University of Arkansas
479-575-6416
qinghual@uark.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