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

V-INT: Automated Vulnerability Intelligence and Risk Assessment

UNIVERSITY OF ARKANSAS

Targeted vulnerability mitigation using artificial intelligence and firewall analysis

This project researches, develops, conducts field tests, and commercializes an automated vulnerability intelligence and risk assessment toolset. V-INT assesses the risks of identified vulnerabilities by considering their reachability via the Internet in addition to traditional features, such as the known availability of exploit code. This provides more relevant risk assessment for electric utilities than current solutions, which often do not account for the operation environment and requires security operators to manually address the vulnerabilities. V-INT automates analysis to achieve better security at a lower cost. It automatically collects relevant asset, vulnerability, and firewall configuration data; identifies network services of assets affected by vulnerabilities that leverage natural language processing and machine learning; determines level of risk by considering the reachability of network services; and represents risk data to security operators with visualization techniques.

KEY TAKEAWAYS

- Identifies the small percentage of unsafe vulnerabilities by analyzing firewall configuration data
- Extracts vulnerable network services from the National Vulnerability Database using natural language processing
- Allows utilities to easily model how an adversary sees vulnerabilities in their infrastructure

OUTCOME

V-INT delivers a tested and validated cybersecurity product based on a library of over 100,000 vulnerability descriptions tagged for numerous network services. This increases security operator preparedness and informs and streamlines automated processes to enable more rapid response against the continuous flow of new software vulnerabilities.

PARTICIPANTS	ROLE
UNIVERSITY OF ARKANSAS	Leads the project and develops the natural language processing pipeline to extract network services from vulnerability descriptions and tie in vulnerability data with firewall configuration analysis from Network Perception's NP-View tool.
UA LITTLE ROCK	Performs the software engineering tasks with the University of Arkansas, develops asset feature extraction features and visualization tools.
np network perception	Provides its flagship product, NP Live, to parse firewall configurations into network attack graphs, and the Spartan tool provides asset vulnerability data back to NP Live for overlaying vulnerabilities on the network.
Electric Cooperatives of Arkansas — Your Local Energy Partners	Serves as a key partner in developing and field-testing artificial intelligence (AI) tools in vulnerability analysis to advance vulnerability risk identification.
VISTRA ENERGY	Serves as a key partner with Network Perception to provide expert decisions to enhance the use of AI in vulnerability management. Both Arkansas Electric and Vistra guide the toolset requirements and perform field tests.

CONTACT INFORMATION

Initial Leads:

Qinghua Li
Principal Investigator
University of Arkansas
479-575-6416
qinghual@uark.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

Period of Performance: September 2020 – November 2023

Total Award Value: $2,693,876
DOE Share: $1,919,954
Cost Share: $773,922

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