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

Security Patch Automated Remediation Tool Analyzing the NVD (SPARTAN)

SEEDS
CYBERSECURITY CENTER FOR
SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Using artificial intelligence to automate and optimize security vulnerability and patch management in energy delivery systems

This project uses artificial intelligence techniques to automate and optimize risk analysis and decision making in vulnerability and patch management. First, it develops a tool for automated remediation analysis based on vulnerability features and asset features, which can recommend remediation decisions for vulnerabilities such as patch immediately, mitigate immediately, and patch-in-cycle. Second, it develops a technique for analyzing the risks of vulnerabilities by learning from expert assessment. Third, it develops a technique that can automatically find mitigation information for vulnerabilities from online resources, such as the National Vulnerability Database (NVD). These techniques can expedite vulnerability remediation and mitigation, reduce security risks, and save operation cost.

KEY TAKEAWAYS

- Automates vulnerability remediation decisions to ensure service reliability
- Compiles vulnerability mitigation information from the National Vulnerability Database to conduct efficient and effective risk assessments
- Minimizes overall security risks and costs associated with vulnerability management

OUTCOME

Experiments using two real vulnerability and patch management datasets showed that the remediation analysis tool can predict remediation decisions with 97%-99% accuracy. Additional experiments, using a 2017-2020 vulnerability dataset, showed that the mitigation information localization tool can achieve 92%-95% accuracy. The techniques developed in this project can save an estimated thousands of person-hours for an electric utility.

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	Develops methods for remediation action analysis, mitigation information localization, and risk analysis; software implementation and testing
UA LITTLE ROCK	Develops methods for risk analysis; user interface design; software implementation 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