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

Early Insider Threat Detection

SEEDS
CYBERSECURITY CENTER FOR
SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

A deep learning-based prototype system that characterizes, captures, and analyzes insider threats in utility communication networks

This project develops novel multi-time series analysis technologies and builds a prototype system to characterize, detect, interpret, and mitigate dynamic insider threats. The developed technology combines temporal point processes and recurrent neural networks and has a two-level structure that effectively models activity times, activity types, session durations, and session intervals information. It is capable of capturing a general nonlinear dependency over the history of all activities of an individual.

KEY TAKEAWAYS

- Overcomes the reliance on alarms and manually generated features in threat detection technology
- Addresses dynamic insider threats that evade detection based on traditional predefined signatures
- Increases raw data processes capabilities and improves threat detection accuracy

OUTCOME

This technology addresses key challenges in insider threat detection: heterogeneous data, time dynamics, and no or few labeled insider threat records in training data. The team conducted evaluation using two datasets, the CERT Insider Threat Dataset and the UMD Wikipedia Vandal detection dataset. The resulting model outperformed state-of-the-art baselines such as One-class SVM and Isolation Forest. This research was presented at the 2019 IEEE Big Data Conference and the NeurIPS 2019 Learning with Temporal Point Processes Workshop.

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, implements, and tests algorithms to detect insider threats

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Xintao Wu
Principal Investigator
Professor
University of Arkansas
479-575-6519
xintaowu@uark.edu

Qinghua Li
Co-Principal Investigator
Associate Professor
University of Arkansas
479-575-6416
qinhaul@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