1st Workshop on Formal Methods-based Deep Learning for Industrial Control Systems Security

Overview

This workshop will explore the amalgamation of formal verification methods and deep neural networks for securing Industrial Control Systems (ICS). The recent rapid advances in deep neural network (DNN) technology have drawn in many ICS security designers and operators to adopt the technology for addressing ICS security issues. Although promising in other applications, incorporating DNN for ICS security is more challenging because of the DNN models' limitations on explainability and predictability. Unseen input may cause the unexpected output of DNN models, which can induce severe consequences to the corresponding physical processes. While formal verification is a well-established field promising strong guarantees for safety, security, and reliability, and has been successfully applied to ICS security in the past, the approach is susceptible to scalability and cost issues. This workshop aims to further advance the intersection of formal methods and DNN and facilitate novel solutions that bring the two technologies together for solving complex problems in ICS security. We expect submissions to fall at the intersection of formal methods and DNN, and demonstrate the feasibility of the proposed research on ICS.

Topics of Interest

Topics of interest include, but are not limited to:

- Anomaly Detection for ICS using Formal Methods and DNN
- Formal Verification of DNN models for ICS
- Deep Learning-assisted Formal Verification of ICS
- ICS forensics using DNN and Formal Verification
- Risk Assessment of ICS based on Formal Verification and DNN
- ICS Adversarial attacks and defenses of DNNs using Formal Verification
- Formal Verification and DNN-based ICS software testing and fuzzing
- Intrusion Detection and Firewalls of ICS based on Formal Analysis
- ICS malware analysis using DNN and Formal Verification

Any submissions related to ICS security using Formal Methods are welcomed.

Submission deadline: March 7th, 2023, co-located with AsiaCCS 2023.

CFP: https://www.web-hosting.guru/