Hybrid Intrusion Detection System for Smart Grids
Authors: Aneeqa Mumrez*, Hoomaan Khosravi, Ghada Elbez, Prof. Dr. Veit Hagenmeyer

Problem Statement
- Multiple communication protocols e.g. IEC 60870-5-104
- Extended interconnection
- Limitations
  - Signature based IDS
  - Specification based IDS
  - Anomaly based IDS
- Zero Day Attacks
- Fabricated Data with Legitimate Headers
- High False Alarm Rate

Prerequisites
- Signature based IDS
- Specification based IDS
- Anomaly based IDS

Features
- Cyber (IT)
- Physical (OT)
- Selection, prioritization and cross-validation

Techniques
- Anomaly based
- Signature based

Development and Implementation of Hybrid Intrusion Detection System (HIDS) Model

System Model
- Network Traffic (PcapNg)
- Data Configuration Files (SCL/SCD)
- Measurement Data

Hybrid IDS incorporates couple of attack detection approaches to improve detection rate, accuracy and efficiency.

Extension of Hybrid Intrusion Detection System with Intrusion Response System in KASTEL Security Lab Energy

Alerts generated by HIDS can be further utilized by Intrusion Response System (IRS) to produce responses nullifying or reducing the alteration done by an attacker.

Further Steps
- 01 Develop attack scenarios for the HIL architecture of lab
- 03 Select and test different models to be incorporated in the system
- 05 Integrate HIDS and IRS in KASTEL Security Lab Energy
- 02 Map features and deep packet inspection
- 04 Explore positioning strategies for HIDS in the system architecture

References: