The Virtualized Cyber-Physical Testbed for Machine Learning Anomaly Detection: A Wind Powered Grid Case Study
DANIEL L. MARINO et al.
URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9611286

Main idea:

a. Develop virtualized Cyber-Physical system/testbed
b. Simulate a wind powered grid
c. Simulate cyber attacks
d. Collect network data of the attacks
e. Feed the network data to tain ML models
f. Use the trained ML models to detect future anomalies/attack

Cyber Physical System:

a. Cyber part: Regular network, working over TCP/IP with regular hosts and attacker hosts
b. Physical part: Industrial part with sensors
c. Interface between cyber physical: protocols like DNP3

The experiments in this paper were run on a single laptop with 32GB of RAM, and an Intel(R) Xeon(R) CPU E3-1505M v6 @ 3.00GHz, with 4 CPU cores (8 threads).

For windfirm simulation:
Cyber model consists of these hosts 1) a data historian, 2) a DNP3 outstation for the Wind Turbine, 3) a DNP3 outstation for data measured from the grid, 4) a cyber sensor, and 5) a malicious device.
Physical model consists of The Wind Farm DFIG Phasor Model provided by MATLAB Simscape Electrical.
Protocol for communication is DNP3.

3 scenarios considered:

a. Baseline scenario: no attack, regular traffic
b. Malicious Cyber Disturbances: Three attacks are launched one after the other: IP scan, ping sweep, and port scan. The attacks are launched using nmap and hping3.
c. Malicious Cyber Physical Disturbances: Pitch angle attack. The malicious device sends a DNP3 command that enables manual mode and sets the pitch angle to zero.

Wireshark is used to analyze captured network traffic data. nmap and fping were used to launch reconnaissance attacks, which simulate how an attacker would act when attempting to gain information about the computer network. Finally, Scapy is a library for network packet analysis and manipulation.

ML algorithms used for training models: Isolation Forest, Local Outlier Factor (LOF), OneClass SVM (OCSVM), and Autoencoders (AE).

HoneyICS: A High-interaction Physics-aware Honeynet for Industrial Control Systems
Marco Lucchese et al.
URL: https://dl.acm.org/doi/pdf/10.1145/3600160.3604984

Main idea: honeypot for ICS settings instead of just regular networks. Doing it in simulated cyber physical system.

Honeypots are computer security systems hosting virtual environments, which can emulate hardware and software devices and can be used to decoy attackers away from the real system, to educate staff, and to study attack patterns in order to select appropriate mitigation.

The setup aims to be equipped with an advanced monitoring system and physics-aware, particular focus on these two aspects. Physics-awareness means the attacker should receive consistent feedback from a (possibly simulated) manipulated physical process.

It is actually a cyber physical system. And the physical system is simulated.

HoneyICS components: PLCs, HMIs, communication networks, and a physical plant. Honeypots can be accessed by an attacker either via the Internet, through exposed PLCs and/or HMIs, or via a (compromised) VPN.

Architecture: As a use case, a honeynet inspired by Lanotte et al.'s system, consisting of a network of three PLCs to control a simplified version of the Secure Water Treatment system (SWaT) has been considered (simplified version of it actually).

Implementation: Does not use physical devices, but rather relies upon existing simulation frameworks: Honeyd, HoneyPLC , OpenPLC (physics aware experiment), ScadaBR (for HMI), and Simulink . As for industrial network protocols we emulate Modbus. As to scalability and reconfigurability, each component of our honeynet is deployed in a dedicated Docker container running either Ubuntu 18.04 LTS or NGINX base images.

Attack 1: Both PLCs and HMIs are exposed (and hence accessible) on the Internet. DoS on pump governed by PLC to achieve tank overflow.

Attack 2: the HMI is exposed on the Internet. a MITM attack exploiting *authenticated arbitrary file upload* vulnerability CVE-2021-26828 of ScadaBR to gain complete control of the HMI.

Attack 3: honeynet is under a compromised VPN. Stealthy DoS attack. Done using a script that keeps transmitting a Modbus packet, with function code read analog input register 0x04, on port 502/TCP, to read the PLC register associated with the level of tank.

Data of real world attack were collected using these two (well known??) experiments/conventions: Shodan's Honeypot tag Experiment and Internet Exposure Experiment.

There are some comparisons with other experiments in terms of features, not quantitative attack related data.