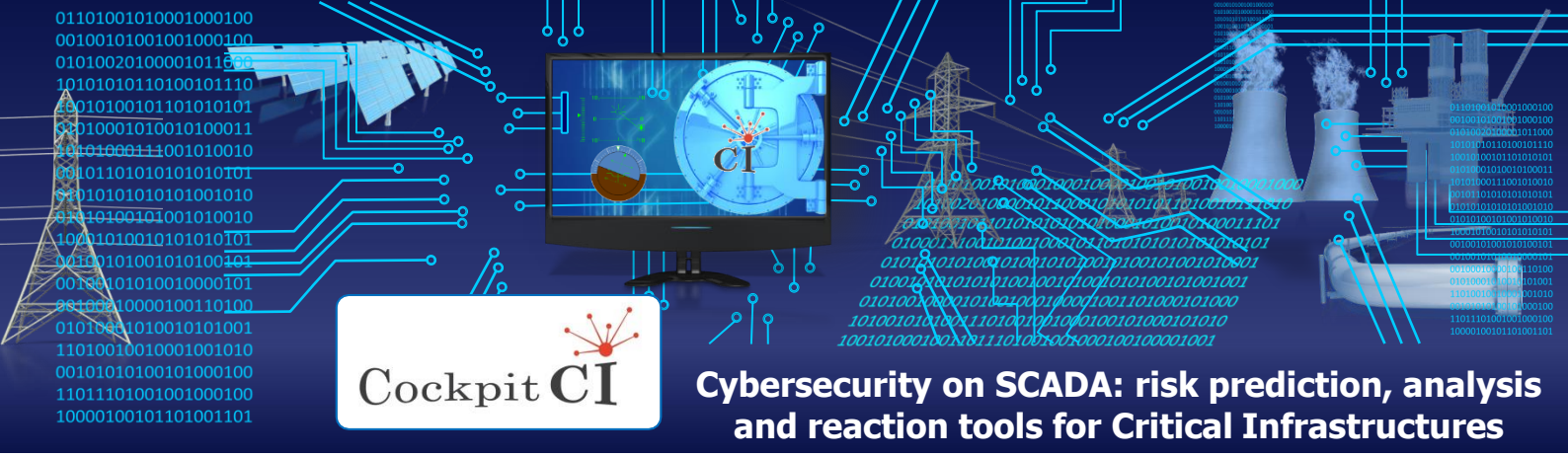


Cockpit CI

Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

Innovative system developed and by :

UNIVERSIDADE DE COIMBRA
FACULDADE DE CIÊNCIAS
E TECNOLOGIA

Main Functionalities

- Simulate a SCADA programmable control unit: *such as a Modbus Server*
- Simulate for the attacker all the behaviors of a real device
- Integrate a log events system and communication features to send collected information to a SOC
- Alert message in IDMEF standard
- Very unexpansive

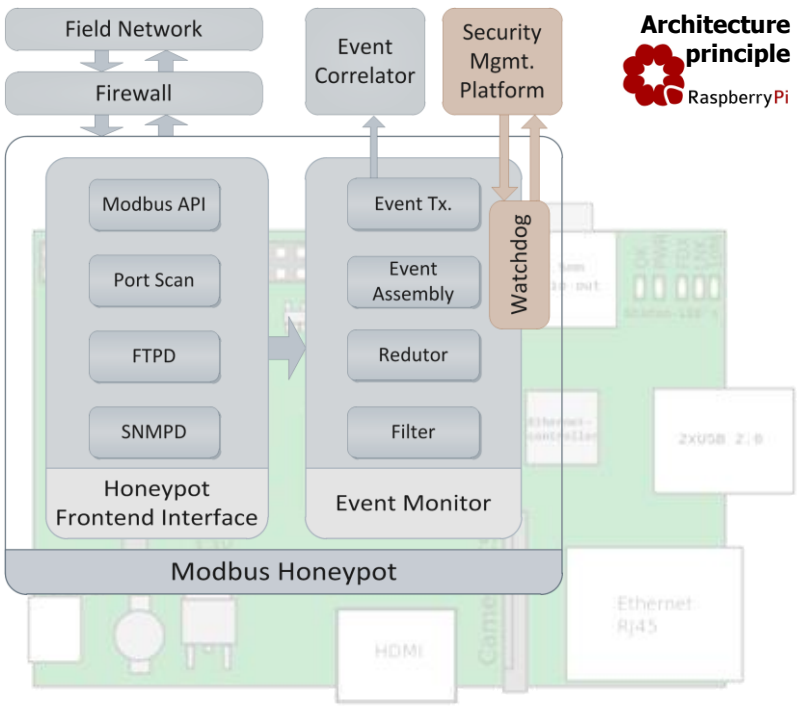
Operation Capabilities

- Master polling a PLC (Normal Operation)
- Network scan detection
- Modbus scan detection
- Modbus attack detection
- Very unexpansive

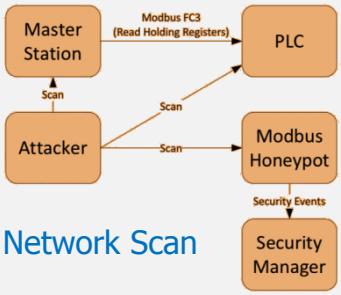
SCADA Honeypot

Type: *SCADA Security System*

Packaging: *Ready to use system embedded in Raspberry PI hardware*

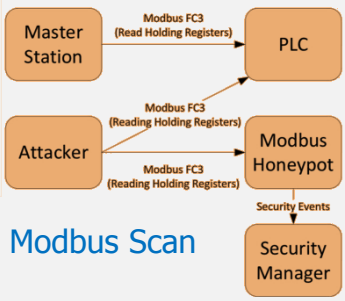


Functioning in detection mode



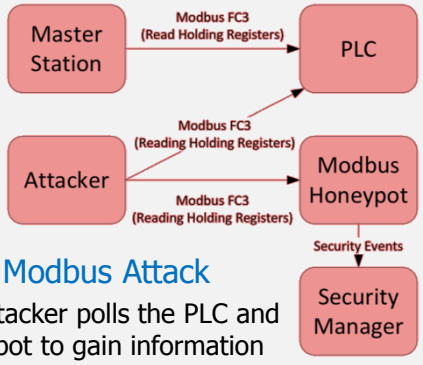
Network Scan

An attacker scans the network to discover devices to exploit.



Modbus Scan

The attacker scans the Modbus enabled devices (PLC and Honeypot) to gain information.



Modbus Attack

The attacker polls the PLC and Honeypot to gain information on the process or to alter its behaviour.

The honeypot detects the scan and sends an event to the Security Manager.

For more information contact Dr Paulo Simoes or Dr. Tiago Cruz