Lightning Talk III [Engineering Design]

Project: Grid-SIEM

Team: Group 29

Ella Cook, Westin Chamberlain, Trent Bickford, Daniel Ocampo

Design Complexity

- Challenge
  - Power grids cover vast areas requiring oversight
  - Protecting the grid should not compromise speed or responsiveness
- Strategic placement of nodes
  - Strengthen grid by placing nodes in high-risk critical areas
  - Must secure the most area with minimal notes
- Meeting industry standards
  - Using and mastering SecurityOnion to implement solution
  - Utilizing Mitre Caldera to test and ensure robustness of our solution

Design Context

Area	Description	Example
Public Health, Safety, and welfare	Reliable electricity access will be possible with our project. As a result, the public will be able to live their lives normally with modern appliances and electronics	- Increasing security on power grids around the US preventing attackers and bad actors
Global, Cultural, and social	Once complete, our project will be usable by educational communities so they can learn about security	- Diagrams for our network - Implementation documentation for our software
Environmental	Indirectly effects energy consumption by reducing attacks on grids	- Defense against attackers
Economic	Potential costs for energy needed to run security software Less money spent on energy consumption by rogue actors	- Efficient coding and node usage - Strong security to deter attackers

Engineering Tools

- PyTorch software as a machine learning framework
- Security Onion open-source SIEM as a SIEM for our project
- Gravwell open-source option as another SIEM option for our project
- MITRE ATT&CK framework to keep track of and identify attacks that are being run against our power grid testbed
- Iowa State University PowerCyber testbed environment to simulate a power grid and its security

Design Visual and Description

- Senior Project focuses on adding the IDS Sensor and IDS Master to the PowerCyber environment
- DER Clients must also contain IDS sensors to monitor data
- IDS sensors will send data out of the DER Clients to the IDS master
- Meeting the requirement of securing the environment
- Our design will also include machine learning components that will be in the master node
- We will also be including another VM that will run attack scripts to verify the security

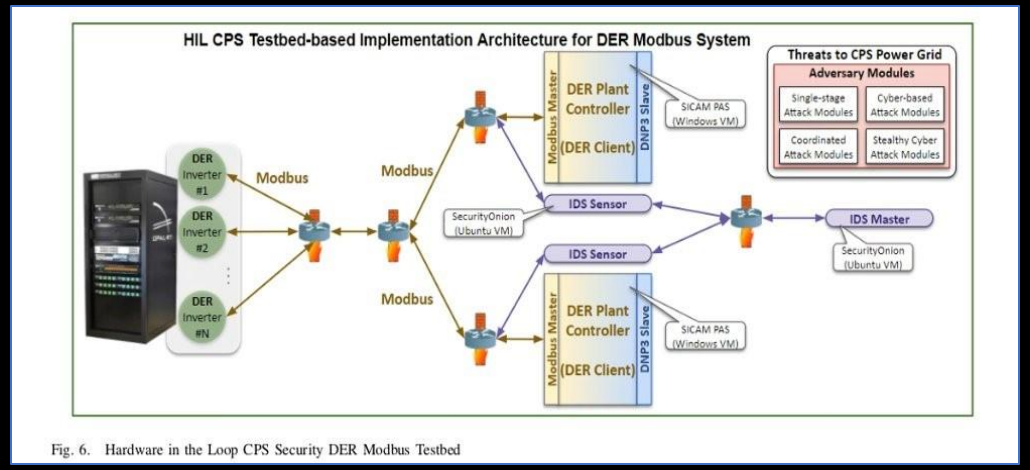

Fig. 6. Hardware in the Loop CPS Security DER Modbus Testbed

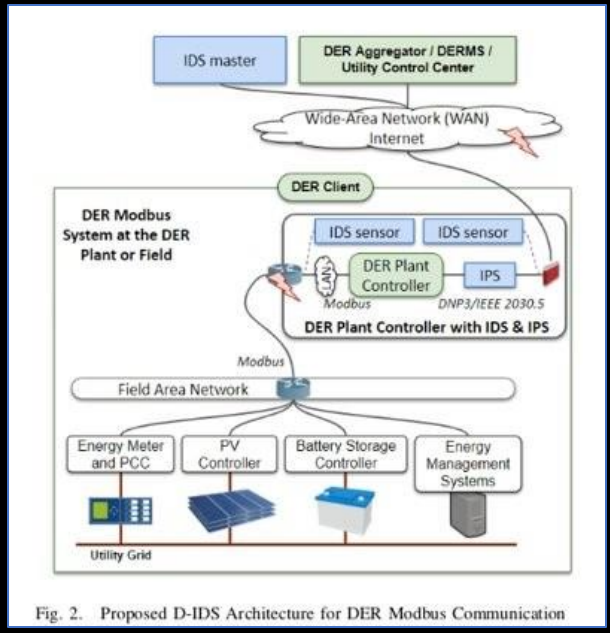

Fig. 2. Proposed D-IDS Architecture for DER Modbus Communication

Functionality

- This includes a dashboard displaying relevant activity within PowerCyber network.
- Info on latest incidents and alerts.
- ML capabilities called flows/playbooks will automate analyst actions.
- SIEM will have an uptime of 99.99% as required by an industrial control system.