Continuous Security Monitoring Protocols and Architectures for Energy Delivery Systems

Adam Hahn, Chen-Ching Liu, Carl Hauser, Chih-Che Sun, Armin Rahimi

GOALS

Develop continuous monitoring techniques to improve EDS operator's awareness of their cyber infrastructure

- Continually monitor and measure system vulnerabilities, configuration errors, malicious events, and compliance with security policies
- Provide data analytics that aggregate and process a broad set of data sources to determine security concerns.
- Demonstrate the effectiveness of the technique against a variety of simulated attacks
- Test and verify the proposed technologies within realistic testbeds and in real-world systems

FUNDAMENTAL QUESTIONS/CHALLENGES

- Industry reports suggest 60% of attacks occur in minutes[1], but are not detected on average for 205 days[2]
- Cybersecurity assessments are costly and time consuming, preventing EDS operators from performing frequent security evaluations. While continuous monitoring technologies can provide EDS operators with more data, there remain critical questions:
  - What is most critical to the detection of unauthorized system access or misconfigurations?
  - What are the best analytical techniques to monitor large quantities of collected data?
  - Does the collection of security data have any negative impacts on the EDS system?
- ***Question:*** Can the process of assessing security and verifying that systems meet required security policies be automated and performed on a regular basis?

[1] 2015 Verizon Data Breach Investigation Report. Verizon.
[2] M-Trends 2015: A View from the Front Lines. Mandiant.

RESEARCH PLAN

This project will explore techniques to help EDS operators continuously monitor the cybersecurity of their systems through the following tasks:

Develop assessment techniques and protocols to collect security data

- Extend NIST's Security Content Automation Protocol (SCAP) to enable automated data collection
- Develop a continuous monitoring platform based on the ELK (Elasticsearch, Logstash, Kibana) stack to provide (i) data collection capabilities, (ii) data analysis algorithms, and (iii) visual dashboards

Explore assessment schedules to minimize the impact on the EDS

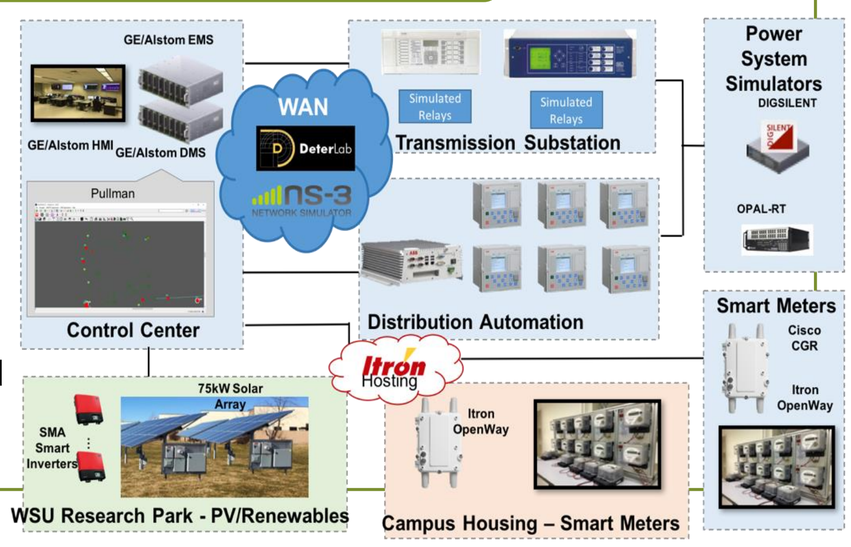
- Identify the impact of assessment operations (e.g., scanning) on a variety of EDS device

Develop analytical techniques to validate the system's current security baseline

- Correlated data from a variety of sources, including: assessment results, packet captures, netflows, IDS logs, and log files.

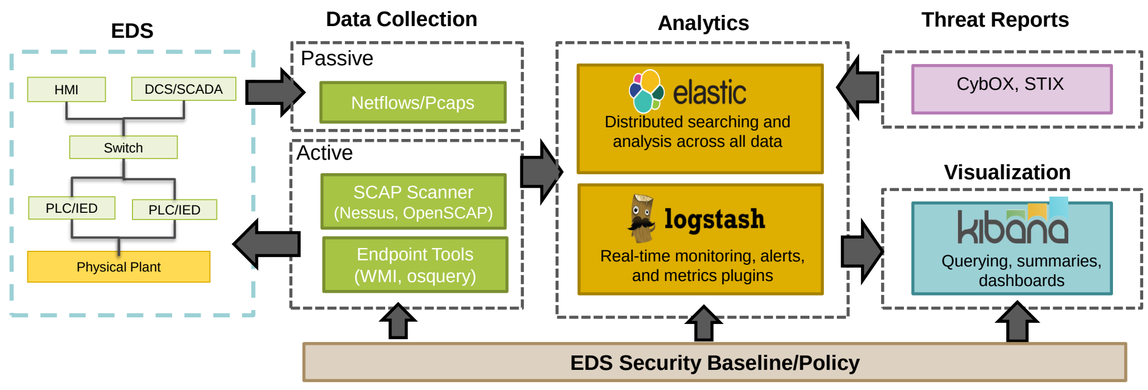
Test and validate the proposed techniques on various real-world devices

- Evaluate the proposed techniques against software platforms (e.g., EMS, DMS) and devices within the WSU Smart City Testbed and other CREDC testbeds.

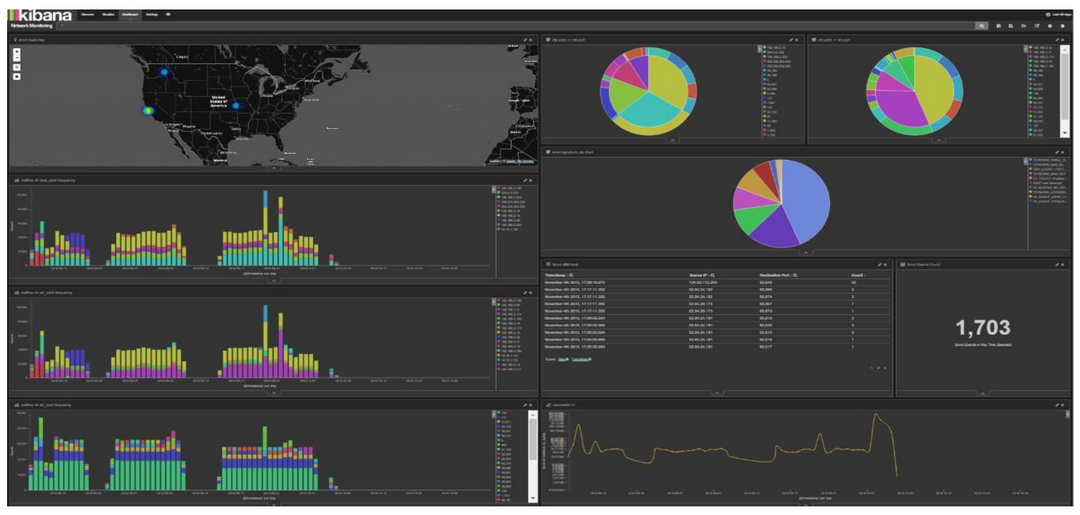


RESEARCH RESULTS

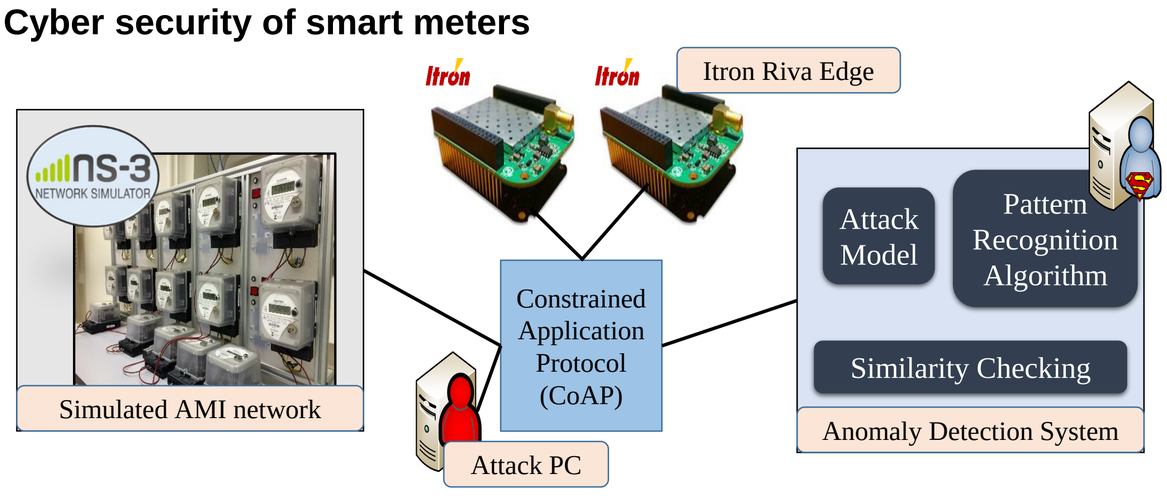
Continuous network monitoring infrastructure



Visualization



Cyber security of smart meters



BROADER IMPACT

- Provide utilities and other EDS operators with real-time awareness of their critical cyber assets, beyond traditional intrusion alerts
- Decrease the window of time between when a security incident occurs and when EDS operators identify the incident
- Reduce the cost and inconvenience of periodic vulnerability assessments
- Inform EDS operators with consistent evidence of their compliance with organizational or industry standard security policies

INTERACTION WITH OTHER PROJECTS

- The project will explore collaboration with other CREDC activities focusing on:
  - Detecting cyber attacks on systems and networks
  - Performing big-data analytics of cybersecurity events
  - Developing cyber-physical metrics for security
- This research will also explore industry collaboration to obtain inputs from both vendors and EDS operators on the feasibility of the proposed techniques

FUTURE EFFORTS

- Explore techniques to identify malicious activity on smart meters and other EDS systems, combining both network and host-based analysis.
- Implement algorithms to correlate event data and create baselines for expected and anomalous behavior
- Expand platform testing on other EDS environments and prototype systems with industry deployments

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY