Proactive Response Strategy for Energy Delivery Systems

Website: http://cred-c.org/researchactivity/proresponse

Researchers (Illinois): Mohammad Noureddine, Atul Bohara, Brett Feddersen, and William H. Sanders

Industry Collaboration:

- OSIsoft LLC
- Currently seeking collaborators from industry, power utilities, or national labs to pursue the possibility of deploying some of our algorithms or information on the kinds of monitors typically deployed in an EDS setting. Contact Mohammad Noureddine and Atul Bohara to discuss how you can engage or collaborate with our research team.

Description of research activity: Intrusion resilience in energy delivery systems preserves service during intrusions. In EDS, the fast-spreading intrusions lead to degradation in availability and integrity, causing wide-spread reduction in service. In this activity, we design theoretically proven proactive response strategies that use alerts from system-level sensors. The alerts are generated by monitoring algorithms that detect anomalies in behavior, degradation in EDS services, and commonly known attacks. The monitoring algorithms fuse heterogeneous sensory data from multiple levels of abstraction. The proactive response algorithms are required to be distributed, with proven safety invariants. A system protected with proactive response algorithms would detect attacks, contain an intrusion and run the system, possibly in a degraded state, until recovery is possible. This system reduces the manual load of monitoring alerts by human operators and provides semi-automatic response suggestions. This work is part of a larger effort at Illinois in the field of intrusion resilience through response and recovery, supported by multiple sponsors. In this research effort, we focus on problems specific to the energy delivery systems and develop algorithms suitable for EDS constraints.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This activity directly maps to the Manage Incidents goal in the Roadmap. In this activity, we develop methods that detect malicious cyber events and responds to adapt the system to contain attacks, while keeping an acceptable level of service, and finally recovering.

Summary of gap analysis: The severity and number of intrusions on computer networks are rapidly increasing. Preserving the availability and integrity of networked power delivery systems in the face of those fast-spreading intrusions requires advances not only in detection algorithms, but also in intrusion resilience and automated response techniques. Briefly, in this activity, the ultimate goal of the intrusion-resilient system design is to adaptively react against malicious attacks in real-time, given offline knowledge about the network's topology, and online alerts and measurements from system-level sensors, and physical sensors.

Full EDS gap analysis: Energy delivery systems are vast systems with a large number of computing devices that provide control and monitoring. A cyber-attack on those devices can disrupt services by either changing the control functions or influencing human actors to make wrong decisions. Due to the size of EDS, monitoring and response cannot be handled manually by human operators, as the human actors will be overwhelmed by the number of events and alerts. Moreover, the size of the system will prevent human actors from making truly optimal response decisions that take the whole system state into consideration. This activity addresses the gap in managing cyber incidents and responding to them as they unfold in real-time. Specifically, the activity will start by providing situational awareness through detection and cyber-physical state estimation. In the second step, the activity finds methods for threat containment, remediation, and recovery. The process is to be enables the goals in the Electricity Subsector Cybersecurity Capability Maturity Model Version 1.1 which in (7.7) starts by detection, escalations, response, continuity of service, and management.

Bibliography:

- Energy Sector Cybersecurity Capability Maturity Model (ES-C2M2)

- Intro to the NISTR 7628
- “Roadmap to Achieve Energy Delivery Systems Cybersecurity”, 2011
- RRE: A Game-Theoretic Intrusion Response and Recovery Engine. S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley. (13ZON02) IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, February 2014, pp. 395-406.
- Learning Process Behavioral Baselines for Anomaly Detection. A. M. Fawaz and W. H. Sanders. (16FAW03) Proceedings of the 22nd IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2017), Christchurch, New Zealand, January 22-25, 2017, to appear.