Continuous Security Monitoring Protocols and Architectures for Energy Delivery Systems

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

Researchers (WSU): Adam Hahn, Chen-Ching Liu, Chih-Che Sun, Armin Rahimi, Jin Young Lee, and James Halvorsen

Industry Collaboration:

- Siemens
- Currently seeking industry collaborators to help evaluate methods for collecting and analyzing available security data.

Description of research activity: This research activity explores methods to improve the collection and analysis of security data within an EDS, including attacks, system vulnerabilities, configurations, software versions, and account management. It explores how automated collection techniques currently used in the Information Technology (IT) domain (e.g., credentialed scanning) can be incorporated into a modern EDS environment. The project will align with current initiatives within the IT and Industrial Control System (ICS) domains in the development of continuous monitoring protocols, such as NIST's Security Content Automation Protocol (SCAP). The proposed techniques will be evaluated on realistic systems within the WSU smart grid testbeds, along with other CREDC testbeds. The techniques will be tailored towards AMI domains to develop an Anomaly Detection System (ADS) to detect abnormal behaviors in smart meters. A Temporal Causal Diagram (TCD) will be developed to help identify different types of attacks by analyzing the detected anomalies in a meter infrastructure. The completion of this task will identify new methodologies and techniques that will provide EDS owners with timely and accurate understanding of their system's security posture. Furthermore, it will attempt to introduce vendor-agonistic standards for continuous monitoring requirements to encourage interoperable vendor technologies in the future.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This activity specifically addresses the DOE Roadmap goal to "*Assess and Monitor Risk*"; specifically it enables the year 2020 goal that "continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators". The activity will help achieve these goals by evaluating current continuous monitoring techniques from IT environments within EDS systems, and developing new tools and techniques to improve the ability to monitor and assess systems.

Summary of EDS gap analysis: Currently there's an insufficient set of tools and technologies to monitor the security of EDS environments. Manual security audits are expensive and many auditing tools (e.g., port scanners, vulnerability scanners) are intrusive and can cause systems malfunctions. Additionally, manual tests can only be performed at periodic intervals, while system security posture changes frequently due to new vulnerability discoveries and system reconfigurations. This creates a strong need for more cost-effective, periodic, and repeatable approaches for security monitoring. This activity fills this gap by expanding and tailoring current IT continuous monitoring tools and protocols to the unique challenges of EDS. This task will (i) introduce a platform to integrate and analyze data from a variety of EDS platforms, (ii) develop tools to collect security data for EDS end-nodes, and (iii) evaluate these tools within the WSU Smart City Testbed.

Full EDS gap analysis: EDS environments utilize many unique software platforms, devices, and networks, a fact which complicates the process of monitoring and verifying system security policies. This task requires the collection of a variety of security information, including system configuration, accounts, password policies, patches, and anomalous events. However, manually performing this assessment is expensive and time consuming, therefore, techniques are required to automate this process. These challenges have been directly identified by the DOE Roadmap, which requests technology to perform "continuous security state monitoring of all energy delivery system architecture levels", along with NISTIR

7628 which recommends the implementation of continuous monitoring programs. Finally, NIST SP 1800-7A suggests that energy sector utilities require technologies to enable "increased real-time or near real-time cybersecurity monitoring [that] can enhance the resilience of their operations."

Bibliography:

- Jim McCarthy, et al. NIST Special Publication 1800-7A, "Situational Awareness For Electric Utilities." NIST/NCCoE. February 2017.
- "Roadmap to Achieve Energy Delivery Systems Cybersecurity," Department of Energy (DOE). September 2011.
- NIST Interagency Report 7628, "Guidelines for Smart Grid Cyber Security". NIST. August 2010.