Cybersecurity for Energy Delivery Systems

Sandia National Laboratories in partnership with Lawrence Livermore National Laboratories, Washington Gas Energy Systems, Fort Belvoir, Chevron, Grimm, and Schweitzer Engineering Laboratories

Ensuring resiliency in energy and utility infrastructure through unpredictability and enhanced situational awareness in energy delivery system networks

Innovation

As critical infrastructure networks and control systems are upgraded and increasingly connected, system security is increasingly at risk. Energy delivery control systems traditionally have predictable communication paths and static configurations. Sandia's Artificial Diversity and Defense Security (ADDSec) project is developing solutions to introduce unpredictability and enhance situational awareness for vulnerable static energy delivery control systems, protecting them against cyber attack.

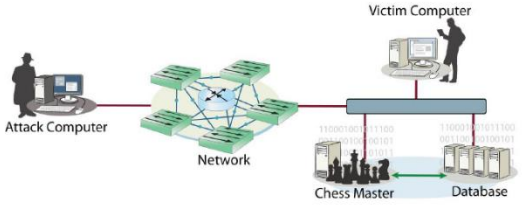
Outcomes

Technology Advancement

The ADDSec program has leveraged software defined networking to introduce random unpredictability into control system networks through three main components: network randomization, application library randomization, and machine learning based dynamic defense. Machine learning dynamic defense detects active attacks by recognizing patterns, providing situational awareness, and taking appropriate action when necessary.[1]

Impact

Research has resulted in a verified means for a resilient mechanism to support modern grid operation through creating complexity for adversarial attackers and detection capabilities for those attacks. Sandia, in conjunction with partner Schweitzer Engineering Laboratories, successfully employed testing at Fort Belvoir for ADDSec in which the technology defended Fort Belvoir's microgrid control system, detected abnormal behavior, and triggered a mitigation response. The demonstration has proven that the ADDSec technology can interoperate with commercially available products and be retrofitted into operating systems.[3]



Process demonstrating the security of legacy and modern systems by improving overall situational awareness and converting static systems into moving targets
[Image: Vicente Garcia. SNL][2]

"The detection and response capability of ADDSec provides a framework for Utility operators to proactively defend their networks against active threats in an automated fashion."

Adrian Chavez, Principal Member of Technical Staff / ADDSec Principal Investigator, Sandia National Laboratories[1]

Timeline[2]

October 2015: Project commences

July 2016: Initial Ft. Belvoir microgrid scenario developed

October 2016: Completed proof-of-concept demonstration

July 2018: Demonstration at Ft Belvoir microgrid for ADDSec certification

[1] DOE: energy.gov/sites/prod/files/2016/09/f33/SNL%20ADD%20Sec%20Fact%20Sheet%20September%202016.pdf

[2] SNL: energy.gov/sites/prod/files/2017/02/f34/SNL_ADDSec_Peer_Review_2016.pdf

[3] SNL. energy.sandia.gov/energy/ssrei/gridmod/grid-mod-newsletter/