

Predicting hacker movement in an electric utility SCADA network

To: Secretary Granholm and distinguished members of the Secretary of Energy Advisory Board (SEAB):

Applied Controls Solutions, LLC appreciates this opportunity to provide information and a request to the SEAB for consideration during its July 26, 2023 meeting on the issue of developing technology to predict hacker movement in an electric utility SCADA network. SCADA networks are not just used in electric grids, but manufacturing like the new Wierton battery plant, water, pipelines, rail, etc.

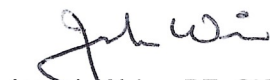
Work is ongoing in identifying cyber threats, vulnerabilities, and locating hacker penetration in an electric utility SCADA network. However, work needs to be done to predict hacker movements once the hacker is inside an electric utility SCADA network. The research on predicting hacker movement started in 2003-2007 when DARPA sponsored the development of advanced probabilistic methods including Bayesian Networks. In 2013-2016, the Missile Defense Agency (MDA) sponsored the development of probabilistic predictive algorithms for kinetic object tracking and forecasting, such as for missiles and drones. In 2022-2023 DOE sponsored a 9-month Phase 1 SBIR (I am a participant in this project) to perform a feasibility project to extend the MDA approach to predict the movement of a cyberthreat in an electric utility SCADA network. Both Sandia National Laboratory and Idaho National Laboratory (INL) personnel provided input on our Phase 1 project. Phase 1 is now complete, and the report has been delivered to DOE.

From the Phase 1 literature search, we found that in 2003, two independent papers from University of Texas and Georgia Tech proposed using Hidden Markov Models to predict the movement of a cyberthreat. In 2004, Georgia Tech advanced the approach to use Bayesian Networks. In 2006-2009, Tunisian researchers extended previous work. More disconcertingly, in **2014-2020, Iranian researchers further extended the previous work. This was the most recent and comprehensive work we could find.**

From our Phase 1 work, we found that Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) can't predict the future movement of a cyber intrusion that has successfully breached the electric utility SCADA network. We contacted leading US network threat and monitoring vendors about applying predictive future movement technology. However, we were informed by the cyber security vendors that they were not doing this work. Additionally, we contacted INL about using the SCADA Test Bed for simulations as part of the Phase 2 proposal.

Given the lead Iran has demonstrated from the open literature search, it is imperative to ensure that DOE funds this Phase 2 research as hackers have been in our electric grid networks since 2014. Yet, we have just been informed that our Phase 2 proposal was turned down by DOE.

Respectfully,



Joseph Weiss, PE, CISM, CRISC
Managing Partner, Applied Control Solutions, LLC
Joe.weiss@realtimeacs.com
(408) 253-7934

