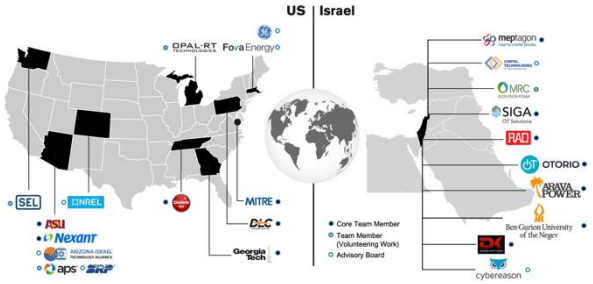

Converging Cybersecurity Solutions for Energy Systems to Practice

A SCADA-Physics Anomaly Correlation Technique

Moses Ike

Georgia Institute of Technology

January 10, 2023, 7:00 - 8:00 pm, Israeli time

(12:00-1:00 pm EST, 10:00-11:00am am AZ/Phoenix Time)

Link: https://asu.zoom.us/j/6712258140

Abstract: Modern Industrial Control Systems (ICS) attacks disrupt processes from infected Supervisory Control and Data Acquisition (SCADA) hosts, injecting semantic attacks that blend with noise. To detect these stealth attacks in practice, existing sensor tools lower their thresholds. However, since they cannot validate if their flagged attacks are actual attacks from SCADA or benign (e.g., faults), they raise high false alarms. To reduce false alarms, we propose a SCADA-Physics anomaly correlation technique that uses Physics to corroborate detected SCADA attacks. In SCADA, we use ICS conventions to select operational events to induce physical-bound API calls. It then analyzes their statistical dependencies to model SCADA semantics, which it uses for detection.

For Physics anomalies, we apply state-of-the-art Transformer neural networks in a novel way to rank important Physics relationships in sensor/actuator sequences and avoid sequential bottlenecks. Anomalies that show up at both SCADA and Physics are strong indicators of ICS attacks. To reduce false alarms, we can filter Physics anomalies that permeate from previous time windows (e.g., noise flares) before the SCADA anomaly.

Bio:

Moses Ike is a Ph.D. Candidate in the School of Cybersecurity and Privacy at Georgia Institute of Technology under the supervision of Prof. Wenke Lee and Saman Zonouz. Moses' research combines analysis of CPS behaviors at the SCADA host and physical processes to improve attack detection. Prior to joining Georgia Tech, Moses attended the University of Texas at Dallas, where he obtained his B.S. and M.S. degrees in Computer Science.