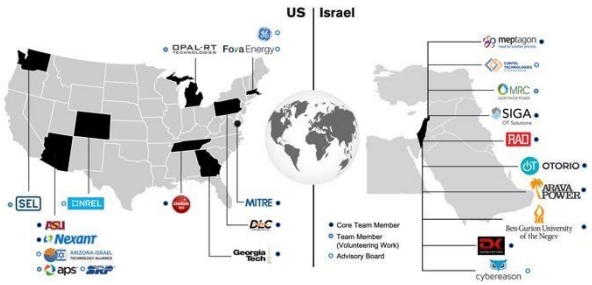

Converging Cybersecurity Solutions for Energy Systems to Practice

Safeguarding Embedded Controllers through Side Channel Analysis

Yossi Oren

Ben-Gurion University

February 20, 2023, 6:30 - 7:30 pm, Israeli time

(11:30-12:30 am EST, 9:30 am-10:30 am AZ / Phoenix Time)

Link: https://us02web.zoom.us/j/81690844393?pwd=ZDIwTTZrbFZQemtFM1hwTVhMV1NLQT09

Abstract: In today's interconnected world, Programmable Logic Controller (PLC) devices play a crucial role in controlling and automating critical processes across various sectors. This increased connectivity, however, also brings about significant security risks, including the threat of the PLC's control flow being subverted through malicious code injected by state-level actors. This talk will cover an exploration of the use of side channels for control flow monitoring. By analyzing subtle variations in system behavior, such as power consumption and electromagnetic radiation, these side channels can be effectively leveraged to infer control flow information, and thus identify potential attacks. To accomplish this, we employ the emitted signals to train a machine learning model, and evaluate our detector by simulating two different types of attacks: malicious code injection and sensitive data infiltration. Additionally, we provide a unique comparison between the power consumption and electromagnetic side channels, highlighting the primary benefits each signal type exhibits in terms of detecting and preventing attacks. The talk will also include a brief discussion about the possibility to use both channels as input for a multimodal ML model, and the common approaches for multimodal training. Finally, we'll talk about the commercialization aspects of our task.

Bio:

Yossi Oren is an associate professor in the Department of Software and Information Systems Engineering at Ben-Gurion University of the Negev, and a member of BGU's Cyber Security Research Center. Prior to joining BGU, Yossi was a Post-Doctoral Research Scientist in the Network Security Lab at Columbia University in the City of New York and a member of the security lab at Samsung Research Israel. He holds a Ph.D. in Electrical Engineering from Tel-Aviv University (thesis), and an M.Sc. in Computer Science from the Weizmann Institute of Science (thesis).

His research interests include implementation security (side-channel attacks, micro-architectural attacks, power analysis and other hardware attacks and countermeasures; low-resource cryptographic constructions for lightweight computers) and cryptography in the real world (consumer and voter privacy in the digital era; web application security). He has been recognized by The Register as a Top Boffin.