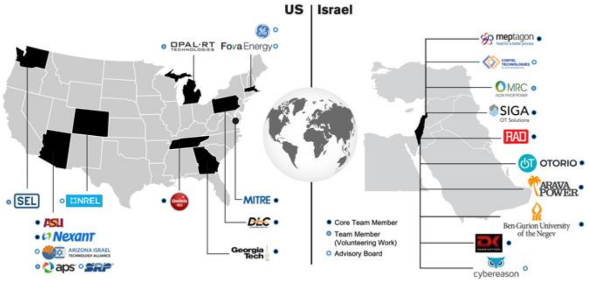
BIRD
Israel-U.S.
Binational Industrial Research
and Development Foundation



U.S.-Israel Energy Center

Converging Cybersecurity Solutions for Energy Systems to Practice

Attack Hypotheses Generation and Targeted Data Collection for Threat-Hunting Using Multi-Level Threat Intelligence Knowledge Graph

Rami Puzis

Ben-Gurion University

July 5, 2022, 7:00 - 8:00 pm, Israeli time

(12:00-1:00 pm EST, 9:00 am-10:00 am AZ Time)

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

Abstract: Threat hunting relies on cyber threat intelligence to perform active hunting of prospective attacks instead of waiting for an attack to trigger some pre-configured alerts. Cyber threat intelligence on past attacks may help with attack reconstruction and the prediction of the course of an ongoing attack by providing deeper understanding of the tools and attack patterns used by attackers. We present AttackDB, a multi-level threat knowledge base that combines data from multiple threat intelligence sources to associate high-level ATT&CK techniques with IT artifacts specified in behavioral malware reports. AttackDB helps with both inference of hypothetical Indicators of Attack (IoAs) - sets of TTPs presumably associated with an ongoing attack - and data collection targeted to confirm or refute a large set of hypotheses. The attack hypothesis generator relies on knowledge graph traversal algorithms and a variety of link prediction methods to automatically infer the IoAs from a set of observable artifacts. Targeted data collection is modeled as a multi-armed bandits (MAB) problem to balance between exploration and exploitation of the collected data while searching for forensic information related to the yet unknown attack.

Bio:

Dr Rami Puzis is a Senior Lecturer (Assistant Prof.) at the Department of Software and Information Systems Engineering at Ben-Gurion University. Rami has graduated BSc in Software Engineering and MSc and PhD in Information Systems Engineering. Rami was a post-doctoral research associate in the Lab for Computational Cultural Dynamics, University of Maryland. His main research interests include network analysis with applications to security, transportation network, social networks, computer communication, and biology. Over the past years, Rami has managed research projects funded by Deutsche Telekom AG, Israeli Ministry of Defense, Israeli Ministry of Trade and Commerce, and leading industries in Israel. His recent research projects have focused on threat hunting and threat intelligence, cyber-physical and cyber-biological security, and disinformation in social networks.