

Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience

Quarterly Review Workshop IV Agenda

March 20 - 21, 2023

Israel Time: 7-9 pm

US Time: 1-3 pm (EST), 10am-12pm (AZ / Phoenix time)

Purpose of Quarterly Review Workshop

Welcome to the BIRD-ICRDE cybersecurity project workshop IV. We are delighted to have this opportunity to share with the consortium members some progress updates of this Israel-US binational joint project. The workshop will be on March 20-21. The Principal Investigator(s) of each task will present their research results and discuss plans for future quarters. The focus of the presentations would be on *tool development*, *integration*, demonstration of the *practical values and potential impact* of the research solutions for early cyberattack stages, and *commercialization* in collaboration with industry partners. The workshop will be conducted via zoom video conferencing and recorded for future reference. Please use the link below to join the workshop.

<https://asu.zoom.us/j/6712258140>

Agenda (Moderators: Yang Weng, Rami Puzis) (All times are in Israeli pm):

March 20 (Mon):

- 7:00-7:15 Task 11: AI based intrusion detection
Yisroel Mirsky (BGU), Ying-Cheng Lai (ASU)
- 7:15-7:25 Task 16: Reinforcement learning control for cyber physical systems
Ying-Cheng Lai (ASU)
- 7:25-7:45 Task 2: Digital rep. of physical processes & operational process modelling
Asaf Shabtai (BGU)
Task 10: Multi-layer anomaly detection framework, Robert Moskovitch (BGU)
Task 15: Self-healing and auto-remediation, Asaf Shabtai (BGU)
- 7:45-8:05 Task 3: Data collection and aggregation

Matan Dobrushin (OTORIO), Haim Beltran (Meptagon), Jonathen Myles / Avi Alon (Delek US)

- 8:05-8:30 Task 4: Multi-level threat intelligence knowledge base, Rami Puzis (BGU)
Task 12: Explainable cyber A.I. analytics, Liat Antwarg (BGU)
Task 6: Threat hunting, Rami Puzis (BGU)
- 8:30-8:50 Task 10: Multi-layer anomaly detection framework, Nir Nissim (BGU)
Task 12: Explainable cyber A.I. analytics, Nir Nissim (BGU)
- 8:50-9:00 Task 10: Multi-layer anomaly detection framework, Ron Insler (RAD)
- 9:00-9:10 Task 1: Realization of advanced energy management applications
Yang Weng (ASU), John Dirkman (Resource Innovations)

March 21 (Tue):

- 7:00-7:10 Task 18: Hardware-in-the-loop validation
Yang Weng (ASU)
- 7:10-7:35 Task 5: GANs for generating adversarial attacks
Task 8: Detect event mimicking attacks
Lalitha Sankar (ASU)
- 7:35-7:50 Task 7: Malware threats mitigation
Wenke Lee (GIT)
- 7:50-8:05 Task 9: False data injection
Hagai Galili, Ilan Gendelman (SIGA OT)
- 8:05-8:20 Task 13: Firmware verification
Yossi Oren (BGU)
- 8:20-8:35 Task 14: Cyberattack tolerance
Sukarno Mertoguno (GIT)
- 8:35-8:50 Task 17: ICS security by design
Dov Shirtz (BGU), Ron Insler (RAD)
- 8:50-9:00 Task 19: Innovation, education, coordination, and marketing programs
Dan Bloomberg (BGU)

ICRDE Management Team (Yang Weng, Rami Puzis, Aviad Elyashar, Chin-Woo Tan, Shuman Luo)

