

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

Quarterly Review Workshop I Agenda

January 24, 2022

Israeli Time: 6-9 pm

US Time: 11 am - 2 pm (EST), 9 am - 12 pm (MST)

Purpose of Quarterly Review Workshop

Welcome to the BIRD cybersecurity project workshop I. We are delighted to have this opportunity to share with the consortium members some updates on the progress of this Israel-US binational joint project. The Principal Investigator(s) of each task will present their work and some initial results, if any, and discuss how their outcomes could be **integrated** with those from other tasks. A highly valued goal of this project is to evaluate the potential of commercializing the project outcomes and devise **commercialization plans** in collaboration with industrial partners. This will be elaborated in the presentations. The workshop will be conducted via zoom video conferencing and recorded for future reference. Please use the link below to join.

<https://asu.zoom.us/j/9723906777>

Agenda (Moderator: Yang Weng) (all times are in Israeli time):

Project tasks in progress:

- 6:00-6:10 Task 1: Realization of advanced energy management applications
John Dirkman (Nexant), Yang Weng (ASU),
- 6:10-6:25 Task 2: Digital rep. of physical processes & operational process modelling
Asaf Shabtai, Rami Puzis (BGU), Matan Dobrushin (OTORIO)
- 6:25-6:40 Task 3: Data collection and aggregation
Matan Dobrushin (OTORIO), Rami Puzis (BGU), Yang Weng (ASU)
- 6:40-7:05 Task 10: Multi-layer anomaly detection framework (15 min.)
Nir Nissim, David Tolpin (BGU), Ron Insler, Yuri Gofman (RAD)
Task 12: Explainable cyber A.I. analytics (10 min.)
Nir Nissim, Bracha Shapira, Antwarg Liat (BGU)

- 7:05-7:20 Task 4: Multi-level threat intelligence knowledge base (10 min.)
Adam Hahn, Marie Collins (MITRE), Bracha Shapira, Rami Puzis (BGU)
Task 6: Threat hunting (5 min.)
Rami Puzis (BGU)
- 7:20-7:40 Task 5: GANs for generating adversarial attacks (15 min.)
Task 8: Detect event mimicking attacks (5 min.)
Lalitha Sankar, Rajasekhar Anguluri (ASU), John Dirkman (Nexant)
- 7:40-7:55 Task 7: Malware threats mitigation
Wenke Lee, Moses Ike (GIT), Ron Insler, Yuri Gofman (RAD), Avi Alon,
Peter Weldon (Delek US)

Project tasks starting in 2022:

- 7:55-8:05 Task 9: False data injection
Hagai Galili, Ilan Gendelman, Adi Bartov (SIGA)
- 8:05-8:25 Task 11: AI based intrusion detection (10 min.)
Yisroel Mirsky (BGU), Ying-Cheng Lai (ASU), John Dirkman (Nexant)
Task 16: Reinforcement learning control for cyber physical systems (10 min.)
Ying-Cheng Lai (ASU), John Dirkman (Nexant)
- 8:25-8:35 Task 13: Firmware verification
Yossi Oren (BGU)
- 8:35-8:45 Task 14: Cyberattack tolerance
Sukarno Mertoguno (GIT), Ali Kazemi (Schweitzer Engineering Lab)
- 8:45-8:50 Task 15: Self-healing and auto-remediation
Asaf Shabtai (BGU)
- 8:50-8:55 Task 17: ICS security by design
Yuval Elovici (BGU)
- 8:55-9:00 Task 18: Hardware-in-the-loop validation
Yang Weng (ASU), Philippe Bisson (Opal-RT; advisory board member)
- 9:00-9:10 Task 19: Innovation, education, coordination, and marketing Programs
Dan Blumberg, Asaf Shabtai (BGU)
- 9:10-9:15 Closing Remarks
Yehuda Ayalon (Meptagon), Eynan Lichterman (BIRD Foundation)

BIRD Project Management Team

Yang Weng, Rami Puzis, Aviad Elyashar, Chin-Woo Tan, Shuman Luo, Oleg Brodt

