TEL AVIV UNIVERSITY
Pursuing the Unknown

ICRC
Blavatnik Interdisciplinary Cyber Research Center

Yuval Ne'eman Workshop
for Science, Technology and Security
Tel Aviv University

Blavatnik ICRC (TAU) – UAEU Joint Research Workshop

Speakers from ICRC:

Name: Prof. Lior Wolf, Professor in the School of Computer Science at Tel Aviv University

Presentation Topic: Sample of never-before-presented projects from the Deep Learning Lab at Tel Aviv University

Short Bio: Lior Wolf is a full professor in the School of Computer Science at Tel-Aviv University, Israel and a research scientist manager at Facebook AI Research. He conducted postdoctoral research at prof. Poggio's lab at the Massachusetts Institute of Technology and received his PhD degree from the Hebrew University, under the supervision of Prof. Shashua. He is an ERC grantee and has won the ICCV 2001 and ICCV 2019 honorable mention, and the best paper awards at ECCV 2000 and ICANN 2016. His research focuses on deep learning for computer vision, audio synthesis, cyber, physics, and medicine.

Name: Prof. Yuval Shavitt, Professor of Electrical Engineering at Tel Aviv University

Presentation Topic: A deep learning approach for IP hijack detection

Short Bio: Professor of Electrical Engineering at Tel Aviv University. Before joining Tel Aviv University, he worked for four years at the Networking Center of Bell Labs, Holmdel, NJ. Has published seminal papers in the fields of caching, routing, IP hijack attacks, and network measurements. In 2004 he incepted the DIMES project for mapping the Internet infrastructure using thousands of lightweight software agents, which revolutionized the field of Internet measurement and mapping. Data gathered by DIMES was used by academies worldwide. In 2014 he established BGProtect, a company that uses the DIMES approach to protect nations and large organizations against IP hijack attacks and provide network infrastructure intelligence. Recenty, Prof. Shavitt was working on using deep learning solutions to network security problems, such as IP hijack detection and encrypted traffic classification.

Name: Prof. Itzhak Benenson, Geosimulation and Spatial Analysis Lab, Department of Geography and Human Environment, Porter School of the Environment and Earth Sciences, Faculty of Exact Sciences, Tel Aviv University

Presentation Topic: Bayesian positioning in mobile networks and its consequences for mobile privacy (for the full abstract please click here)

Short Bio: Dr. Itzhak Benenson is a Professor of Geography at the Department of Geography and Human Environment of the Porter School of the Environment and Earth Sciences, Faculty of Exact Sciences, Tel Aviv University, Israel, and a Head of the Geosimulation and Spatial Analysis lab there. His research includes study of the big urban data including smartcard and mobile phone data, modeling of urban transportation and transport behavior, and modeling of the urban land use and residential dynamics. Itzhak is an Associate Editor of the *Computers Environment and Urban System* journal and serves on several other editorial boards.

Name: Mahmood Sharif, Senior Lecturer, SCS, TAU (starting October, 2021)

Presentation Topic: The Security of Machine Learning in the Real World and Machine Learning for Personalized Security (for the full abstract please click here)

Short Bio: Mahmood Sharif is a postdoctoral researcher in the VMware Research Group. His research interests are primarily at the intersections of computer security and privacy with machine learning, specifically adversarial machine learning, and with human factors. Mahmood obtained his Ph.D. from Carnegie Mellon University, where he was affiliated with the CyLab Security and Privacy Institute. Mahmood is the recipient of two CyLab Presidential Fellowships and a Symantec Research Labs Fellowship. He will join the School of Computer Science at Tel Aviv University as a Senior Lecturer in Fall 2021.

Agenda:

We propose each speaker from each side will speak for 10 minutes. After both sides present their selected topics, we can leave time for discussion, questions and future steps towards joint research.

We would like to request that Prof. Lior Wolf will be the first speaker due to time limitations.