NJIT

NJIT Cybersecurity Research Center and Department of Computer Science

All Computers are Identical, and Other Lies we Tell Ourselves about Computer Design

Yossi Oren
Ben Gurion University of the Negev

Host: Reza Curtmola

Date: Monday, March 10, 2025
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
Zoom Link: https://njit-edu.zoom.us/j/99112675948?pwd=x7BrKFLwR6gFNes1KX4taiWF9JGwr6.1

Abstract:
Abstraction makes computer design elegant and powerful. It allows us to build complex systems while hiding unnecessary details. But what happens when these abstractions mislead us into making insecure systems? This talk explores some myths of modern computer design, including the comforting lie that all computers are identical, and shows how the gaps in these abstractions can lead to real exploits which affect user security and privacy. As is traditional in this field, the talk will conclude with a discussion of defenses and their drawbacks.

Joint work with Tomer Laor, Naif Mehanna, Vitaly Dyadyuk, Antonin Durey, Pierre Laperdrix, Clémentine Maurice, Romain Rouvoy, Walter Rudametkin and Yuval Yarom

Bio:
Twice-awardee of the NJIT-BGU Joint Seed Research Grant (together with Prof. Reza Curtmola and Prof. Nathan Malkin from NJIT), Prof. Yossi Oren (@yossioren) 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, and an M.Sc. in Computer Science from the Weizmann Institute of Science.

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.