Title: Side-Channel Attacks on Human Secrets

Speaker: Yossi Oren

Abstract: Side-channel analysis techniques have been traditionally applied toward the recovery of computer-related secrets such as cryptographic keys. Humans, however, also share secrets of their own with their computers – for example, their browsing habits, their political or religious beliefs, or sensitive information about their health. This secret information is increasingly vulnerable to emerging low-cost side-channel attacks that are highly scalable, employing malicious peripheral devices or turning components of a system against itself. There are countermeasures which can be applied to protect systems from the theft of human secrets via side channel attacks. These countermeasures, however, have different designs, and exact different costs, than those designed to protect against the theft of cryptographic secrets.

Bio: Yossi Oren is a Senior Lecturer 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 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). Twitter: @yossioren, Website: https://iss.oy.ne.ro