2018 ECE SPEAKER SERIES

ECE COLLOQUIUM

Daniel Genkin

Assistant Professor

University of Michigan
Department of Electrical Engineering
and Computer Science

Tuesday Dec 4, 2018 @ 1:00PM

ROOM CHANGE: Photonics Center, Room 906

Light refreshments will be available outside of 339 at 12:45PM

Meltdown, Spectre and Foreshadow: How a Small Side Channel Leakage Becomes a Big Problem

Abstract:

The security of a system is only as good as its weakest link. Even if the system's software is perfectly secure, security threats originating from the system's hardware are far from being properly understood. Side channel attacks extract secret information by exploiting delicate interactions between the system's software and hardware components (such as instruction timing and electromagnetic radiation). Despite being an active research area since the 90's, the systematic exploration of side channel leakage from complex devices has only begun recently, often with devastating security consequences.

In this talk I will cover the recent Spectre, Meltdown and Foreshadow attacks as well as their implications on the security of computer systems. The talk will be self-contained and include live demonstrations.

Biography:

Daniel Genkin is currently an Assistant Professor at the Department of Electrical Engineering and Computer Science at the University Of Michigan. Before that, he was a Postdoctoral Fellow at the University of Pennsylvania and the University of Maryland, where he was hosted by Prof. Nadia Heninger and Prof. Jonathan Katz. Previously he was a Ph.D student at the Computer Science Department in the Technion – Israel's Institute of Technology where I was co-advised by Prof. Yuval Ishai and Prof. Eran Tromer.

Assistant Professor Genkin's research interests are in cryptography and system security. He is interested in both theory and practice with particular interests in side-channel attacks, hardware security, cryptanalysis, secure multiparty computation (MPC), verifiable computation and SNARKS.

BU Department of Electrical & Computer Engineering