Title: Side Channel Attacks: How a Small Leakage Becomes a Big Problem

Speaker: Daniel Genkin

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 (such as PCs, servers and phones) has only begun recently, often with devastating security consequences. While originally considered a threat to cryptographic implementations, over the past 5 years side channel attacks have evolved, becoming a threat to the confidentiality and integrity guarantees of virtually every computer system.

In this tutorial, I will cover several recent side channel attacks on complex devices. This includes both physical attacks which exploit physical effects such as sound and electromagnetic radiation as well as microarchitectural attacks which exploit minute variants in instruction timing. Making things worse, I will show that side channel attacks are often subtle and unpredictable and can often defeat code carefully designed to resist them. Finally, I will conclude with recent attack on speculative execution (e.g, Spectre and Meltdown) as well as the Foreshadow attack on Intel’s SGX.

The talk will be self-contained and include live demonstrations.

Bio: Daniel Genkin is an Assistant Professor at the Department of Electrical Engineering and Computer Science at the University of Michigan. His research interests include cryptography and system security with particular interest in side-channel attacks, hardware security, cryptanalysis, secure multiparty computation (MPC), verifiable computation, and SNARKS. Before joining the University of Michigan, Daniel 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, Daniel obtained his Ph.D from the Computer Science Department in the Technion, where he was co-advised by Prof. Yuval Ishai and Prof. Eran Tromer.