COLLEGE OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

Dissertation Defense

Ofir Weisse

Enabling Usable and Performant Trusted Execution

Monday, December 2, 2019
10:00 am – 12:00 pm
3725 Beyster Bldg.

ABSTRACT: A plethora of major security incidents---in which personal identifiers belonging to hundreds of millions of users were stolen---demonstrate the importance of improving the security of cloud systems. To increase security in the cloud environment, where resource sharing is the norm, we need to rethink existing approaches from the ground-up. This thesis analyzes the feasibility and security of trusted execution technologies as the cornerstone of secure software systems, to better protect users' data and privacy.

Trusted Execution Environments (TEE), such as Intel SGX, has the potential to minimize the Trusted Computing Base (TCB), but they also introduce many challenges for adoption. Among these challenges are TEE's significant impact on applications' performance and non-trivial effort required to migrate legacy systems to run on these secure execution technologies. Other challenges include managing a trustworthy state across a distributed system and ensuring these individual machines are resilient to micro-architectural attacks.

In this thesis, I first characterize the performance bottlenecks imposed by SGX and suggest optimization strategies. I then address two main adoption challenges for existing applications: managing permissions across a distributed system and scaling the SGX's mechanism for proving authenticity and integrity.

I then analyze the resilience of trusted execution technologies to speculative execution, micro-architectural attacks, which put cloud infrastructure at risk. This analysis revealed a devastating security flaw in Intel's processors which is known as Foreshadow/L1TF. Finally, I propose a new architectural design for out-of-order processors which defeats all known speculative execution attacks.

Chairs: Profs. Baris Kasikci and Thomas Wenisch