Title: Securing Processors against Side-Channel Attacks: CPU Caches, Schedulers, and Beyond!

Speaker: Professor Gururaj Saileshwar (University of Toronto)

Date and time: 18th October 2023 (Wednesday), 4:30 PM

Venue: Room 101, H R Kadim Diwan Building (KD 101), CSE Department

Abstract:

In recent years, microarchitectural side-channel attacks have emerged as a unique and potent threat to security and privacy. Identifying these side-channels is difficult as they often originate from undocumented hardware structures, which are hidden from the software. Moreover, their root-cause lies in crucial hardware performance optimizations, making low overhead mitigation challenging. This talk will focus on both discovery of new attacks and new low-cost defenses.

First, I will discuss CPU cache-side-channel attacks originating from cache-set conflicts. Such attacks can leak keys from encryption algorithms, cause privacy breaches like user activity fingerprinting, etc. Recently, many randomized cache defenses have been proposed as mitigations, but they have been broken by adaptive attacks. To fundamentally address this problem, we propose MIRAGE [Usenix Security 2021], a defense that eliminates set-conflicts with an abstraction of a fully associative cache. It achieves this practically with a set-associative design at less than 2% slowdown using Power-of-2-Random-Choices based load-balancing. While 2018 to 2020 saw 5 different defenses broken by 6 attacks, MIRAGE since 2020 has been unbroken.

Next, I will discuss a new side-channel vulnerability we discovered in AMD CPUs (Zen 2 & 3), called SQUIP [Security and Privacy 2023]. This work discovered a vulnerability with shared scheduler queues in multi-threaded AMD CPUs, which have been relatively unexplored. We reverse-engineered these CPU schedulers and demonstrated a side-channel attack exploiting scheduler queue contention that can leak a 4096-bit RSA key across SMT-threads. The vulnerability was acknowledged by AMD & assigne CVE-2021-46778.

Finally, I will conclude with a brief description of current work on DRAM Rowhammer attacks, automated side-channel detection & securing machine-learning models against hardware threats.

Speaker Bio:

Gururaj Saileshwar is an Assistant Professor at the University of Toronto, Department of Computer Science. His research bridges computer architecture and systems security, with interests including micro-architectural side-channels, DRAM Rowhammer attacks, and trusted execution environments. His work has received an IEEE HPCA Best Paper Award, an IEEE Micro Top Picks Honorable Mention, and his PhD dissertation has been recognized with an IEEE HOST Best PhD Dissertation Award and an IEEE TCCA/ACM SIGARCH Best Dissertation Award Honorable Mention. His work appears in computer architecture conferences like ASPLOS, MICRO, HPCA, and ISCA, and security conferences like USENIX Security, IEEE S&P and CCS.