Title: MI6: Secure Enclaves in a Speculative Out-of-Order Processor

Speaker: Arvind, Computer Science and Artificial Intelligence Laboratory, MIT

MI6 is an aggressive, speculative out-of-order processor to support Secure Enclaves, which restore the process isolation guarantees broken by recent attacks exploiting microarchitectural side-channels. Our threat model includes an untrusted OS and an attacker capable of mounting any software attack currently considered practical, including control flow speculation attacks such as Spectre. We model the performance impact of the hardware and software mechanisms added to support enclaves in MI6 through FPGA emulation on AWS F1 FPGAs by running SPEC CINT2006 benchmarks on top of an untrusted Linux OS. Security comes at the cost of 16.7% average slowdown for protected programs (MICRO 2019). Our open-source implementation will be auditable by the architecture and the security communities down to the hardware source code.

This work is done by Thomas Bourgeat, Ilia Lebedev, Andrew Wright, and Sizhuo Zhang under the supervision of Professor Srinivas Devadas and myself

Biography: Arvind is the Johnson Professor of Computer Science and Engineering at MIT. Arvind's group, in collaboration with Motorola, built the Monsoon dataflow machines and its associated software in the late eighties. In 2000, Arvind started Sandburst which was sold to Broadcom in 2006. In 2003, Arvind co-founded Bluespec Inc., an EDA company to produce a set of tools for high-level synthesis. Arvind's current research focus is to enable rapid development of embedded systems. Arvind is a Fellow of IEEE and ACM, and a member of the National Academy of Engineering and the American Academy of Arts and Sciences.