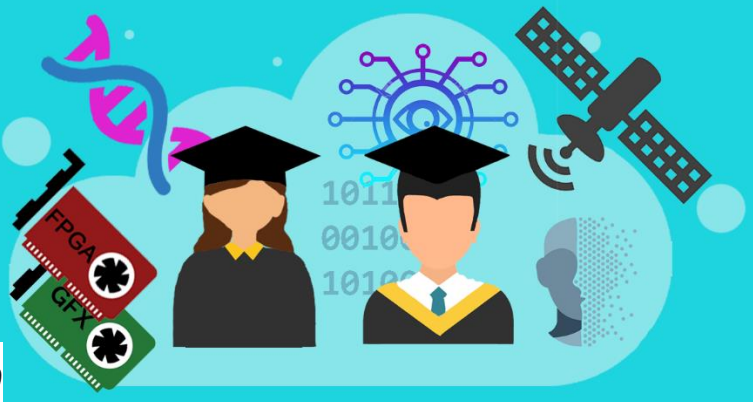
Diploma Thesis

Microproccessors and Digital Systems Laboratory

&

ETH zürich



Hardware-Software-OS Cooperative Techniques for Efficient and Secure Computing

Co-designing software, hardware, and the operating system is a promising approach towards (i) accelerating a wide spectrum of modern applications like graph analytics, generative AI, and recommender systems, (ii) designing intelligent and efficient OS policies like memory management, storage management, container spawning, and (ii) hardening system and processor security.

We are searching for students who are interested in any of these hardware-software-OS co-design research topics:

1. Hardware/OS co-design to enable efficient and secure memory and compute resources
   a. New out-of-the-box virtual memory designs with a focus on new memory trends like CXL memory pooling, processing-near-memory, processing-using memory, and in-storage processing
   b. Establishing new protection schemes against microarchitectural attacks that leverage the OS to introduce new vulnerabilities
   c. Design of specialized hardware to enable efficient system-level operations (e.g., context switching, spawning containers, spawning VMs)
   d. Design of data-centric and data-aware kernel-level memory and disk management operations
   e. Simulation and FPGA-based infrastructures to enable hardware/OS co-design studies

2. Designing software and hardware solutions to harden the security of emerging paradigms like processing-in-memory and in-storage processing

Requirements:

- Strong coding (mainly C/C++) skills
- Strong computer architecture and operating systems background
- Strong work ethic

Suggested readings:

[1] Konstantinos Kanellopoulos et al."Victima: Drastically Increasing Address Translation Reach by Leveraging Underutilized Cache Resources" MICRO 2023

[2] Konstantinos Kanellopoulos et al."Utopia: Fast and Efficient Address Translation via Hybrid Restrictive & Flexible Virtual-to-Physical Address Mappings" MICRO 2023

[3] Vijaykumar et al. "A Case for Richer Cross-layer Abstractions: Bridging the Semantic Gap with Expressive Memory" ISCA 2018

[4] Hajinazar et al. "The Virtual Block Interface: A Flexible Alternative to the Conventional Virtual Memory Framework" ISCA 2020

[5] Kanellopoulos et al. "Amplifying Main Memory-Based Timing Covert and Side Channels using Processing-in-Memory Operations" arXiv 2024

[6] Onur Mutlu, **"Intelligent Architectures for Intelligent Machines"** Invited paper in DATE 2021

If you are interested, please email:

Konstantinos Kanellopoulos, konkanello@gmail.com, https://konkanello.github.io/
Dimosthenis Masouros Ph.D.: (dmasouros@microlab.ntua.gr)
Prof. Onur Mutlu, omutlu@gmail.com, https://people.inf.ethz.ch/omutlu/
Prof. Dimitrios Soudris: (dsoudris@microlab.ntua.gr)