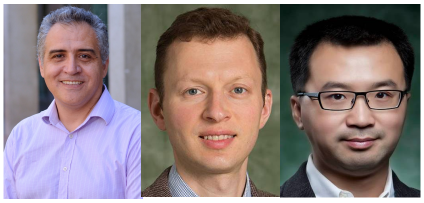
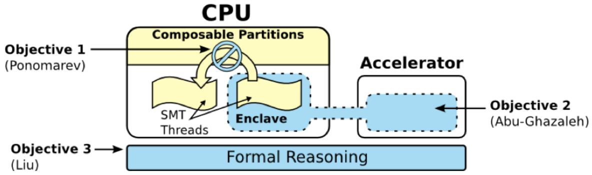
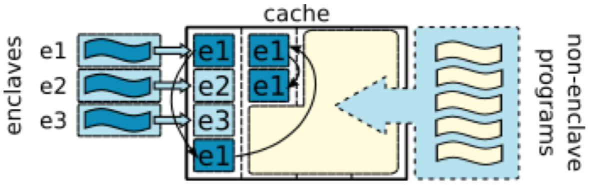
Collaborative Research: SaTC: CORE: Medium: Leakage-free Isolated Execution: Architectures and Security Models



Projects: CNS-1619322 (UCR) & CNS-1617915 (Binghamton)

PIs: Nael Abu-Ghazaleh (UCR), Dmitry Ponomarev (Binghamton), David Liu (Binghamton)





Key problems and challenges:

Key problem: Isolated execution systems are vulnerable to side-channel attacks.

Challenge 1: How to secure them with low performance impact and low complexity.

Challenge 2: How to build isolated execution environments in heterogenous systems.

Challenge 3: Understand how side-channel attacks manifest in heterogeneous environments

Scientific Impact:

The results of this project will help developers in building secure isolated execution systems that are immune to side-channel attacks.

So far, publications in several conferences – ISCA’21, SEED’22 and USENIX Security’ 22.

Key Innovations and Contributions:

- Create composable isolated partitions within hardware resources. Application to caches has been shown in USENIX Security’22 paper.
- Develop attacks to characterize the threat – in progress
- Develop models for secure isolated execution in heterogeneous systems – in progress.
- Develop formal analysis techniques to prove security. Demonstrated for caches in USENIX Security’22 paper

Broader Impact:

- The project advances the understanding of side-channel attacks and defenses in isolated execution environments, leading to more secure trusted execution systems.
- Several undergraduate students will be supported on the project.
- Materials in the security section of undergraduate computer architecture course will be enhanced.