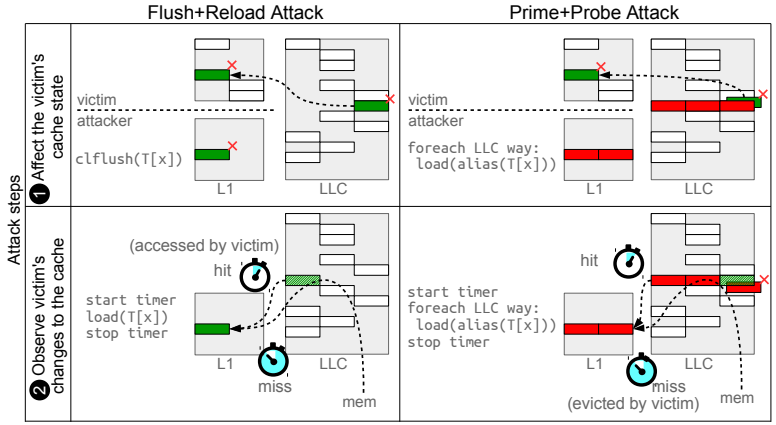
TWC: Small: Side Channels through Lower-Level Caches: Attacks, Defenses and Security Metrics

BINGHAMTON UNIVERSITY
State University of New York

UC RIVERSIDE UNIVERSITY OF CALIFORNIA

Challenges:

- How do we design systems to be resilient to side-channel attacks?
- Consider attacks on caches, branch predictors, GPUs and other shared resources.
- How to protect systems from transient execution attacks?



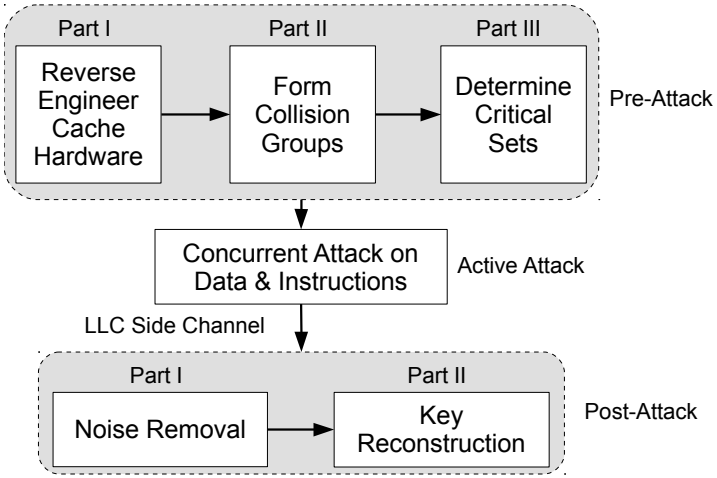
Scientific Impact:

• Published several papers in top computer architecture and security conferences (DAC'16, TACO'16, MICRO'16, CCS'16, DAC'17, MICRO'17, DAC'19, PACT'19)

• Developed side-channel attacks and defenses for caches and branch predictors, demonstrated covert channels through RNG, GPU and branch predictors. Attack on branch predictors was a precursor to Spectre attacks

Solutions:

- New side-channel attack on LLC (DAC'16, **Best paper nominee**)
- Relaxed Inclusion caches to protect LLCs (DAC'17)
- Jump-over-ASLR attack on branch predictor (MICRO'16). This work helped motivate Spectre attacks. Paper was presented at **Top Picks in Hardware and Embedded Security** Workshop.
- Covert channels through RNG (CCS'16), branch predictors (TACO'16) and GPU (MICRO'17)
- Principled approach to protect systems from transient execution attacks (DAC'19)
- Partitioned SMT design to protect from side channels through execution units (PACT'19, **Best paper nominee**)



Broader Impact:

- The project advanced the understanding of side-channel attacks on modern processors, uncovered several vulnerabilities and investigated new defenses. Our work was one of the motivations for development of Spectre attacks.
- Several papers received wide media coverage.
- Graduate seminar-style course on hardware and systems security has been designed and offered several times at UCR.
- Several PhD students and undergraduate students have been supported and trained. Two of the students (Dmitry Evtyushkin and Mehmet Kayaalp) became faculty members at the College of William & Mary and UNH respectively.

Project: CNS-1422401. Pis: Dmitry Ponomarev (Binghamton), Nael Abu-Ghazaleh (UCR). Email: dponomar@binghamton.edu, naelag@ucr.edu