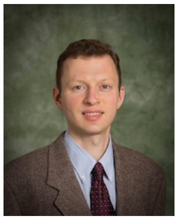
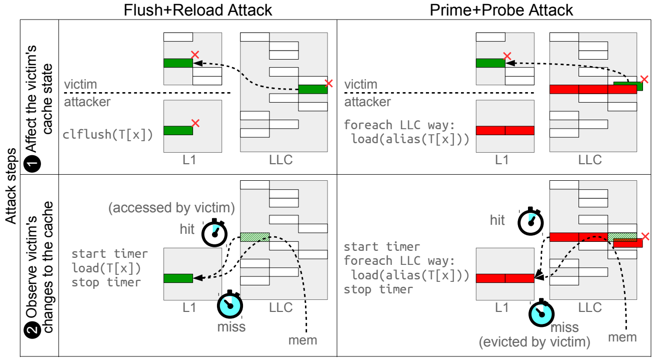
TWC:Small: Side-Channels through Lower-Level Caches: Attacks, Defenses and Security Metrics

Project: CNS-1422401

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



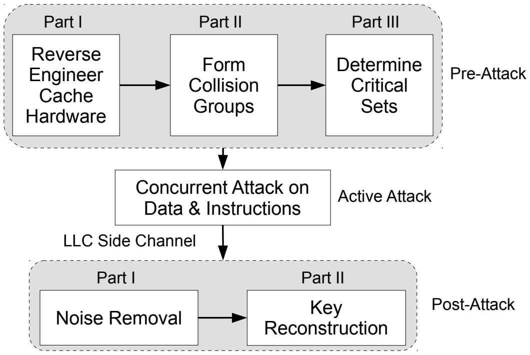


```
clflush(T[x])
```

```
foreach LLC way:
 load(alias(T[x]))
```

```
start timer
load(T[x])
stop timer
```

```
start timer
foreach LLC way:
 load(alias(T[x]))
stop timer
```



Key problems and challenges:

1) What are the challenges to LLC side-channel attacks and how to overcome them?

2) How can we design cache hierarchies immune to side-channel attacks?

3) What other processor resources are vulnerable to side and covert channels?

4) How can we protect systems from transient execution attacks?

5) How can we protect SMT processors?

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

Key Innovations and Contributions:

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

Broader Impact:

1) 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.
2) Several papers received wide media coverage.
3) Graduate seminar-style course on hardware and systems security has been designed and offered several times at UCR.
4) 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.