Hardware Security in DRAMs and Processor Caches

Wenjie Xiong
Postdoctoral researcher at Facebook AI research
Work done at Yale University

My dissertation research aimed to:
- identify and mitigate security vulnerabilities in hardware design, e.g., covert channels
- leverage hardware features to enhance the system security, e.g., PUFs

Cache side and covert channel attacks are notorious for providing a high bandwidth communication channel that breaks the isolation between between different security domains. They have become a serious security threat.

Contributions

- Propose protocols for novel covert channels in the least recently used (LRU) cache replacement states.
- Demonstrate the LRU timing channel in Intel and AMD processors, showing high bandwidth.
- Demonstrate that PL cache, an existing secure cache designs cannot defend the new covert channel in LRU.

Evaluation

	Channel Type	Intel	AMD
Hyper-threaded	With Shared Memory	500Kbps	20Kbps
	Without Shared Memory	500Kbps	20Kbps
Time-sliced	With Shared Memory	2bps	0.2bps
	Without Shared Memory	--	--

Table 1. Transmission rate of LRU covert channels on Intel (Xeon E5-2690) and AMD (EPYC 7571) processors in both hyper-threaded setting and time-sliced setting.

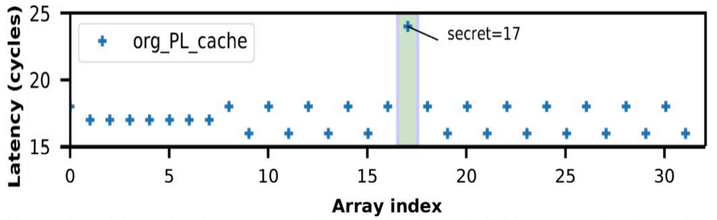

Fig. 1. Simulation results of the LRU attack in the original PL cache design in the gem5 simulator.

Covert Channel in Cache LRU States

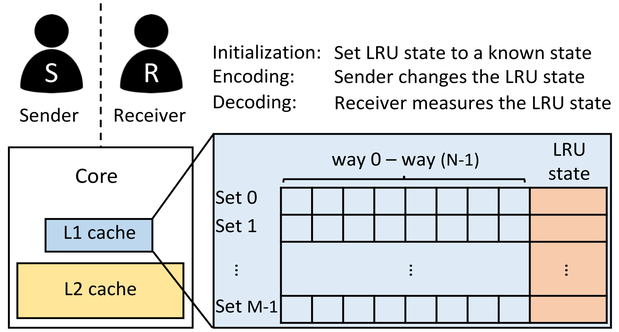

Fig. 2. Cache organization and the steps of the LRU timing-based side or covert channel.

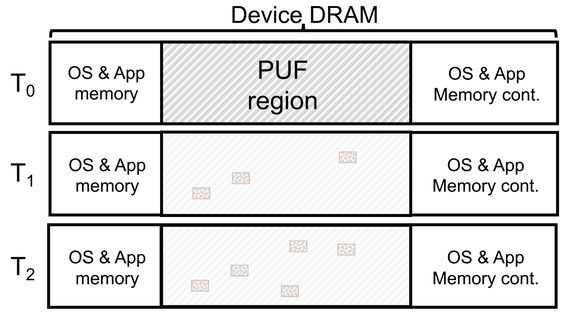

Fig. 3. DRAM PUFs responses overtime.

DRAM PUFs

References:
W. Xiong, J. Szefer, "Leaking Information Through Cache LRU States", HPCA 2020
W. Xiong *et al.*, "Run-time accessible DRAM PUFs in commodity devices ", CHES 2016
W. Xiong *et al.*, "Software Protection using Dynamic PUFs", TIFS 2019

Physically Unclonable Functions (PUFs) extract the unique and stable physical features from physical objects. Unclonability makes PUFs a primitive for authentication and key storage.

*Our **DRAM PUFs*** leverage the retention errors in DRAM. The locations of DRAM retention errors have unique pattern that can be used as PUF responses.

Contributions

Access DRAM PUF from unmodified, commodity devices; provide a system-level solution for querying the DRAM PUF at Linux runtime.

DRAM PUF characteristics

Jaccard index: $J(v_1, v_2) = \frac{|v_1 \cap v_2|}{|v_1 \cup v_2|}$

Robustness: Intra Jaccard index evaluates the differences between PUF responses from the **same** PUF. Ideally, $J_{intra} \approx 1$.
- Demonstrate the robustness under different **temperatures**.

Uniqueness: Inter Jaccard Index evaluates the differences between PUF responses from the different PUFs. Ideally, $J_{inter} \approx 0$.

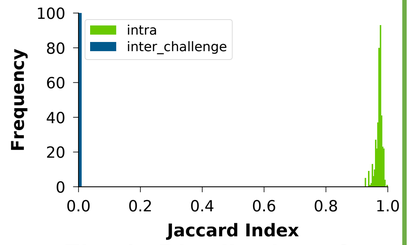

Fig. 4. Distribution of J_{intra} and J_{inter} of DRAM PUFs on Intel Galileo.

Applications

Design and demonstrate schemes for the following applications:
- Device authentication
- Key storage
- Dynamic software protection

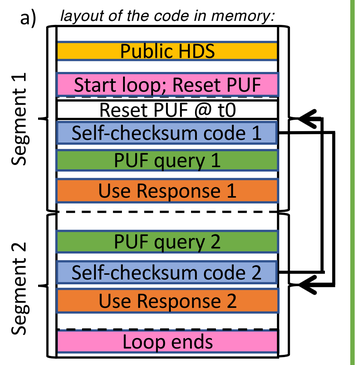

Fig. 5. Software Protection with PUF responses.