Cesar Pereida García, Billy Bob Brumley, Yuval Yarom.

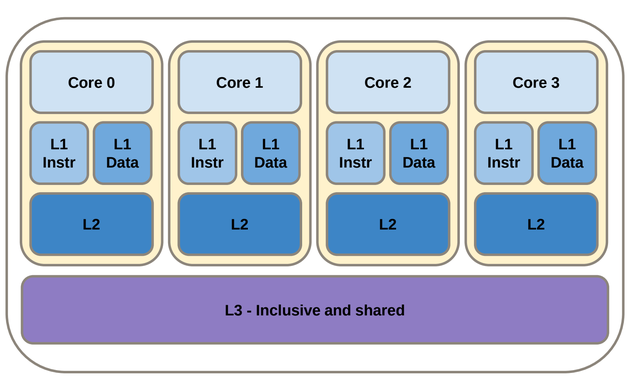
Let Me CLFLUSH Your Cache: Cache-Timing Techniques

➔Cache-timing attacks are a real threat due to library design problems and increased microprocessor architecture complexity.

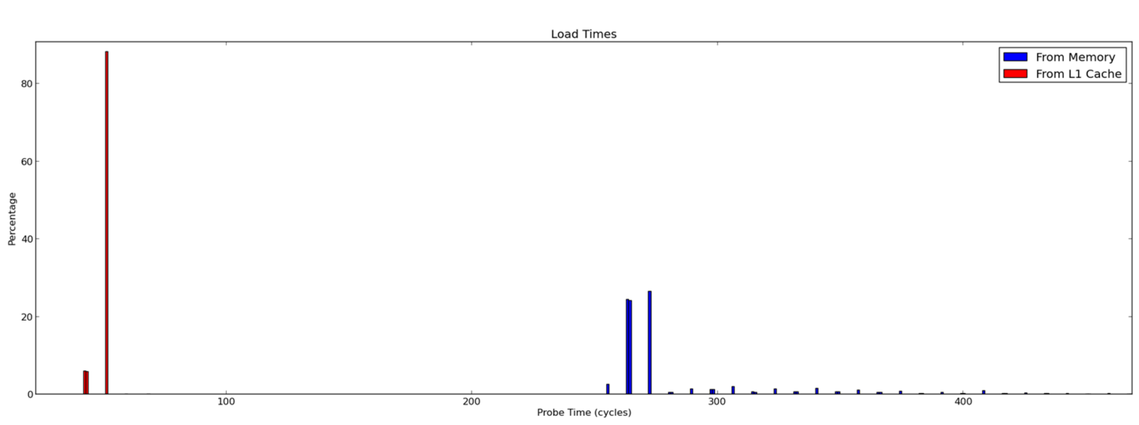
➔Improved attacks are possible combining different cache-timing techniques.

Flush+Reload Technique

- **Cross-core**, **cross-VM** asynchronous attack.
- Memory sharing between **victim** and **spy**.
  - Shared libraries.
  - Page de-duplication.
- **Last-Level Cache (LLC)** is the main target.
- **clflush** command gives high resolution.
- **Round of Attack:**
  - **flush** memory address.
  - **wait** for some time.
  - **reload** memory address.
- **Limitations:**
  - Requires **inclusive** caches (e.g. Intel).
  - Requires a method to efficiently flush cache for accuracy and resolution.



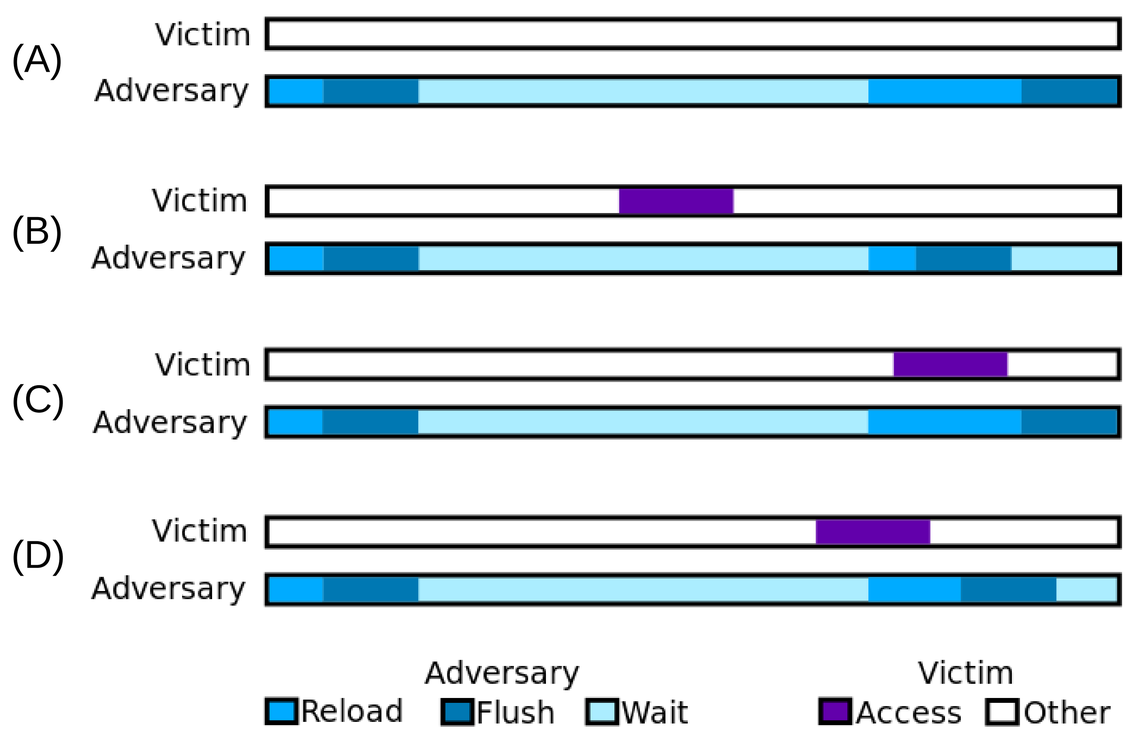
Typical Quad-Core Cache Architecture.



100,000 measurements: Loading time L1 vs Main Memory.

Performance Degradation Attack

- Amplifying the cache side-channel attack.
- Inclusive cache and memory eviction required.
- The goal is to negate cache benefits.
- Program-specific attack.
- Single and multi thread degradation attack.
- **Attack:**
  - **identify** **hot** memory addresses.
  - **evict** repeatedly.



Flush+Reload timing:
(A) No Victim Access (B) Victim Access (C) Overlap (D) Partial Overlap

Do you want to know more?

- Yuval Yarom and Katrina Falkner. Flush+Reload: a high resolution, low noise, L3 cache side-channel attack. In 23rd USENIX Security, pages 719–732, San Diego, CA, US, 2014
- Thomas Allan, Billy Bob Brumley, Katrina Falkner, Joop van de Pol, and Yuval Yarom. Amplifying side channels through performance degradation. IACR Cryptology ePrint Archive, Report 2015/1141, Nov 2015.