University of Colorado Boulder

CASM: A Generalizable and Accessible Security Metric to Evaluate Security of Cache Architectures

Phaedra Sophia Curlin, Tamara Silbergleit Lehman

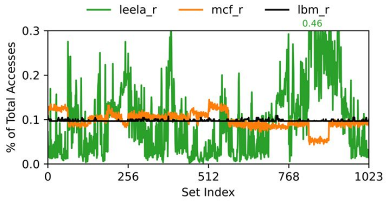
Motivation

- Cache attacks are a threat
- Many secure cache architectures proposed to mitigate
- Difficult to compare designs security-wise
- Cache security metrics proposed but lack:
  - *Generalizability* – attack-independence, framework agnostic
  - *Accessibility* – security and non-security experts can reason about security

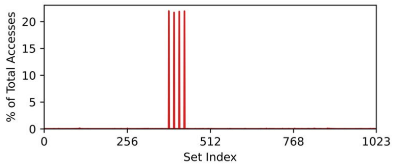
Behavioral Observations of Cache Attacks

- Benign programs spread uniformly across sets[1] and ways
- Cache attack repeatedly re-accesses small number of sets/blocks

Benign Programs



Flush+Reload Attack



Cache Access Security Metric (CASM)

- Indexing function should spread accesses uniformly across sets
  - Optimal performance + decouple index from cache access
- Compare empirical distribution of set accesses to uniform one

n: epoch
s: cache set
i_u: uniform prob.
i_e: empirical prob. of accessing index

$$Ent_i(n) = \sum_{s \in S} i_u(s) \log_2 \frac{i_u(s)}{i_e(s)}$$

- Eviction policy should consider all blocks set as an equally likely candidate for eviction

n: epoch
s: cache set
w: way
W_s: associativity
e_e: empirical prob. of evicting way

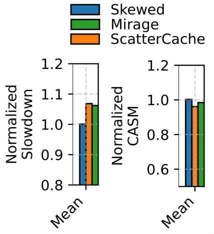
$$Ent_e(n) = 1 - \frac{1}{S} \sum_{s \in S} \sum_{w \in W_s} \frac{e_e(s) \log_2 e_e(s)}{\log_2(W_s)}$$

- Combine indexing and eviction entropy into single metric

$$CASM = \widetilde{Ent_i} + \widetilde{Ent_e}$$

Findings

- Skewed associative[2] has best performance but worse security
- ScatterCache[3] provides better performance-security trade-off
- Mirage[4] provides slightly higher performance



[1] M. Hill and A. Smith, "Evaluating associativity in CPU caches," IEEE Transactions on Computers, 1989.
[2] A. Seznec and F. Bodin, "Skewed-associative caches," PARLE '93 Parallel Architectures and Languages Europe. 1993.
[3] G. Saileshwar and M. Qureshi, "MIRAGE: Mitigating Conflict-Based Cache Attacks with a Practical Fully-Associative Design," USENIX Security Symposium, 2021.
[4] M. Werner, T. Unterluggauer, L. Giner, M. Schwarz, D. Gruss, and S. Mangard, "ScatterCache: Thwarting Cache Attacks via Cache Set Randomization," USENIX Security Symposium. 2019.