CaSA: End-to-end Quantitative Security Analysis of Randomly Mapped Caches

Thomas Bourgeat, Jules Drean, Yuheng Yang, Lillian Tsai, Joel Emer, Mengjia Yan

Published at MICRO’20

[Logos for MIT, CSAIL, and NVIDIA]
Problem: Incomplete Security Analysis

• Cache side channels are a serious security threat

• Promising mitigation: randomly mapped cache

• The security property is not well understood
Key Insights: Telecommunication Analogy

• Contributions:
  • CaSA leverages concepts from telecommunications to enable quantitative analysis
  • An end-to-end communication paradigm to enable comprehensive analysis
  • New findings that refute common beliefs
Cache Side-channel Attacks

Victim code

If (secret==1) { foo = ldf 0x1000; }

0x1000

1-way Cache

Cache Line

Attacker code

While(1) { time(ld 0xf000); }

0xf000

Attacker monitor victim's behavior through cache conflicts.
Cache Side-channel Attacks

If (secret==1) { foo = ld 0x1000;}

While(1) { time(ld 0xf000); }

Using black-box mapping function increases the cost to build an Eviction Set to:
O(N) (with N the number of lines in the cache)
Security Metrics

• Community intuition on Security Metrics:
  • “How hard it is to build an eviction set” is a good quantitative notion of security

• State-of-the-art secure cache design approaches:
  • Dynamic mapping
  • Non-deterministic mapping

• Our work:
  • This security metric can be misleading
  • Both design approaches fail to provide security
Dynamic Mappings

• Common belief: attacks can not happen across epochs
• Dynamic remapping incurs performance overhead

\[ h_1 \quad \text{epoch 1} \quad h_2 \quad \text{epoch 2} \]

\( h \) beginning/end of an epoch
Non-Deterministic mapping

- Make conflict relationship between addresses non-deterministic

State of the art:
Non-deterministic + Dynamic mapping = Good security
Traditional Analysis

• Hard-conflict addresses:
  • Guarantee eviction
  • Difficult to obtain

• Soft-conflict addresses:
  • Easy to obtain
  • Need many of such addresses to reliably evict addresses

- Narrowly focus on eviction set construction and lose the bigger picture.
- Only want to create a one-to-one map from micro-architecture events to secret
End-to-end Communication Paradigm

• Leverage the concepts from telecommunication

• Trade-off between calibration and signaling
  • Long time on calibration $\rightarrow$ shorter time needed for signaling
  • Short time on calibration $\rightarrow$ longer time needed for signaling
New Security Metric

“How difficult to construct an eviction set”

End-to-end communication cost in **Calibration + Signaling**

Calibration
(i.e., Eviction set construction)

Eviction Addresses

Signaling
(e.g., Prime+Probe)

Signal Samples

Decode
Statistical Representation of Signals

• Signal: a random variable “X”
  • Describes the number of misses observed by the attacker
  • Follow a probability distribution

• Example:

<table>
<thead>
<tr>
<th>Victim accesses</th>
<th>Prob observing 0 miss</th>
<th>Prob observing 1 miss</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.75</td>
<td>0.25</td>
</tr>
<tr>
<td>No victim accesses</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

• Successfully covert the problem to a statistical analysis problem
  • How many samples are needed to distinguish the two distributions?
Two Insightful Findings

• Cross-epoch communication is possible

• Spending maximum resources on calibration is not the best strategy
Cross-epoch Communication

• In each epoch:

- one round of calibration
- one round of signal transfer
- beginning/end of an epoch
Cross-epoch Communication

Signals across epochs when attacking the RSA square-and-multiple function.

Cache configuration: 16 hash-groups / 1 way per hash-group/ 16k cache lines
Cross-epoch Communication

Cache configuration: 16 hash-groups / 1 way per hash-group/ 16k cache lines
Epoch size = 100*16K accesses

Cross-epoch communication works!
Trade-off between Calibration and Signaling

Spending the maximum amount of resources in calibration is not always the best strategy.

Cache configuration: 16 hash-groups / 1 way per hash-group/ 16k cache lines
Epoch size = 100*16K accesses
Conclusion & Long-term Impact

• Comprehensive security analysis for micro-architecture side channels should focus on end-to-end communication.

• CaSA formalize the analysis of micro-architecture behavior to the analysis of random variables.

  - Cache Occupancy Attack
  - Memory Controller
  - Front End
  - Execution Engine
  - ......