Metior
A Comprehensive Model To Evaluate Obfuscating Side-Channel Defense Schemes

Peter W. Deutsch, Weon Taek Na, Thomas Bourgeat, Joel Emer*, and Mengjia Yan
MIT CSAIL, *MIT CSAIL/NVIDIA

ISCA 2023 - Session 1C
June 19th 2023
Side-Channel Overview

Victim’s Secret

Victim’s Modulation Pattern

Attacker’s Modulation Pattern

Shared Channel (e.g. Shared Cache)

Attacker’s Reconstructed Secret

Attacker’s Observation (e.g. # of Misses)
Side-Channel Defenses

Partitioning Defense Schemes
*e.g. Cache Partitioning*

- ** ✓ Completely Block Leakage**
- **✗ Poor Performance**

Obfuscating Defense Schemes
*e.g. Randomized Caches, Traffic Shaping, Noise Injection*

- ** 😞 Unclear Leakage**
- ** ✓ Reasonable Performance**
Analysis Example

Victim Modulation Patterns

Secret A Pattern

OR

Secret B Pattern

Attacker’s Modulation Pattern

Deterministic Cache

100% Distinguishibility 😈

Attacker’s Observations

Observation Probability

1

2

100%

Number of Attacker Misses
Analysis Example

Does adding non-determinism increase security? If so, by how much?

Victim Modulation Patterns
- Secret A Pattern
- OR
- Secret B Pattern

Attacker’s Modulation Pattern

Non-Deterministic Cache

Attacker’s Observations
- Number of Attacker Misses: 1
- Observation Probability: 100%
- Number of Attacker Misses: 2
- Observation Probability: < 100%

Distinguishibility < 100%?
What About the Attacker?

Victim Modulation Patterns
- Secret A
- OR
- Secret B

Attacker Modulation Patterns
- Strategy X
- OR
- Strategy Y

Non-Deterministic Cache

The attacker’s strategy is critical in understanding leakage
Metior

Prior Work: Customized modeling solutions for specific defenses and victims

Metior’s Goal: A unified solution for varying channels, victims, and attackers
Metior’s Unified Representation

Obfuscated side-channels can be represented as random variables and the relationships between them!
Metior’s Case Studies

Obfuscation Schemes
- Random Replacement
- Camouflage
- CEASER-S

Victim Applications
- RSA
- AES
- Document Compare

Attack Strategies
- Probabilistic Prime+Probe
- Cache Occupancy

Metior’s Unified Representation

S → Xv → Y → G

a
Case Study – Randomly Mapped Caches

Using Metior, we can explore the leakage of state-of-the-art randomized caches.

In doing so, we are able to:

Better understand the root causes of leakage

Demonstrate the importance of studying real victims
Case Study – Types of Attacks

We study two attacks

① Cache Occupancy
Random Addresses → Prime + Probe

② Probabilistic Prime + Probe (PPP)
Calibration → Eviction Set → Prime + Probe

Leakage Expectation: PPP > Cache Occupancy
Case Study – Results

Takeaway #1
Metior helps in understanding the root cause of obfuscating scheme leakage

Takeaway #2
Mitigations should broadly consider different dimensions of victim modulation patterns

RSA Encryption Victim
Secret 0 → 10 Cache Accesses
Secret 1 → 26 Cache Accesses

Probabilistic P+P ≈ Cache Occupancy!
Metior’s Key Contributions

① A unified model for representing and evaluating obfuscating defense schemes

② Multiple case studies revealing unintuitive insights into state-of-the-art victims, attacks, and defenses
Metior
A Comprehensive Model To Evaluate Obfuscating Side-Channel Defense Schemes

Peter W. Deutsch
pwd@mit.edu

Weon Taek Na
weontaek@mit.edu

Thomas Bourgeat
bthom@mit.edu

Joel S. Emer
jsemer@mit.edu

Mengjia Yan
mengjiay@mit.edu