DAguise: Mitigating Memory Controller Side Channels

Peter W. Deutsch*, Yuheng Yang*, Thomas Bourgeat, Jules Drea, Joel Emer, Mengjia Yan

1. SUMMARY

Problem: Contention in the memory controller can cause information leakage from a victim to an attacker.

Our Solution: Shape the victim’s memory traffic into a secret-independent pattern represented by an rDAG.

Evaluation: Compared to the state-of-the-art, DAguise achieves better security, performance, and has a lower profiling cost.

Generalization: Can be extended to other scheduler-based side channels, e.g.: SMT Port Contention
Network on Chip Contention

4. OUR SOLUTION: DAguise

DAguise: Shape memory requests to a secret-independent Directed Acyclic Request Graph (rDAG)

✓ Security
Shaping to a secret-independent defense rDAG makes victim request patterns indistinguishable
Defense rDAGs are public and are the only thing an attacker can recover

✓ Performance
Allows for dynamic sharing of memory resources in the memory controller

✓ Profiling Cost
Does not require knowledge of co-located applications

5. SECURITY

Simple Shaping Example
- Different victim request patterns are shaped to the same defense rDAG
- The shaper output is always the same, no matter the secret

Indistinguishability Property
Attacker’s response is independent from the victim’s request pattern

Formalize Using State Transitions

6. PERFORMANCE

Example: rDAG Adaptivity
- Shaper output can adapt to observed contention
- This allows for better bandwidth utilization

Example to Find Ideal Defense rDAGs

7. PROFILING

Goal: A defense rDAG should closely encapsulate the memory requirements of the victim

Low Profiling Cost
- Victim is profiled alone (since rDAGs can adapt to contention from co-running applications)
- Reduce search space by finding parameters for an rDAG template

Example to Find Ideal Defense rDAGs

8. GENERALIZATION

Scheduler-based Side Channels:
- Requests from different security domains enter a scheduler to access shared resources
- Shape the request pattern before entering the scheduler

Examples

SMT Contention
Network on Chip Contention

* Authors contributed equally