BunnyHop: Exploiting The Instruction Prefetcher

Zhiyuan Zhang, Mingtian Tao, Sioli O’Connell, Chitchanok Chuengsatiansup, Daniel Genkin, Yuval Yarom
BunnyHop

We like shared resources!

Hey prefetcher, check an address.

BunnyHop: Translate Branch Predictor State to Cache State

Cache Attack. Okey-Dokey!
With the Power of BunnyHop

• Reverse Engineer
  • First work on Instruction Prefetcher
  • Branch Target Buffer
    • First work on Replacement Policy
    • First observation of two type branches: Long Branch & Short Branch

• Three Cool Attacks
  • Flush+Reload on Predictor: Learn same thread predictor state
  • Prime+Probe on Predictor: Learn cross-thread predictor state
  • Self-Eviction : Confuse the victim to evict its own data

More in the paper!
Self-Eviction: The Resident Evil

- Evict secret-dependent data from cache
- Poison the Branch Predictor
- Measure victim process

Cache Coloring

Poisoning

Guide

Prefetch

Any Instruction
Self-Eviction: The case of AES

![Graph showing Pearson Correlation vs Number of Ciphertexts with a correct guess of 0x30]
Summary

• Branch Predictor state can be leaked via cache state
• Reverse Engineer the Instruction Prefetcher
• Reverse Engineer the Branch Target Buffer
• Three attacks on Branch Predictor

https://github.com/0xADE1A1DE/BunnyHop