CS773 Project Proposal

Hybrid Cache Architecture for Comprehensive Security

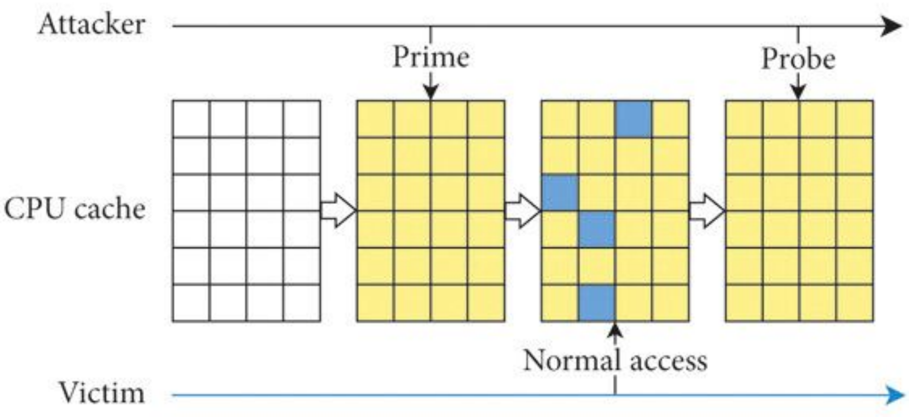
SM Arif Ali, Soumik Dutta, Arnab Bhakta

Team Gandiva

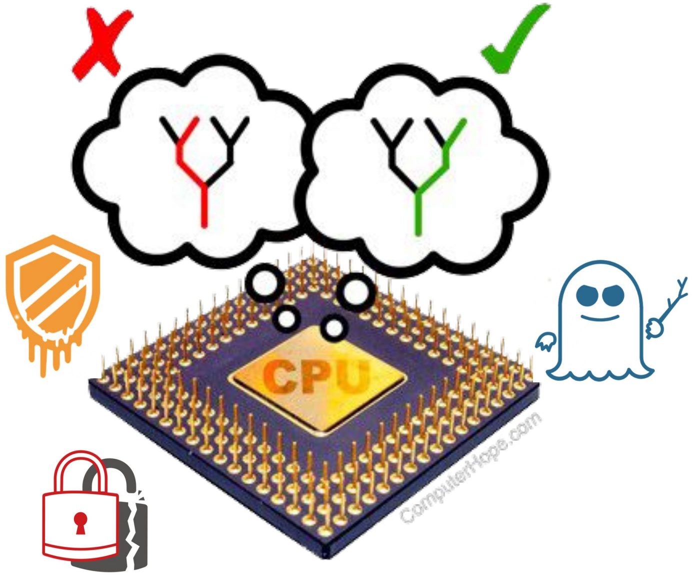
23m0822@iitb.ac.in, 23m0826@iitb.ac.in, 23m0835@iitb.ac.in

Problem statement

Modern processors are vulnerable to two major classes of attacks



Conflict based attacks



Transient execution attacks

To create an unified solution to defend against **both attack types** keeping performance-security tradeoff in mind

Prior Works

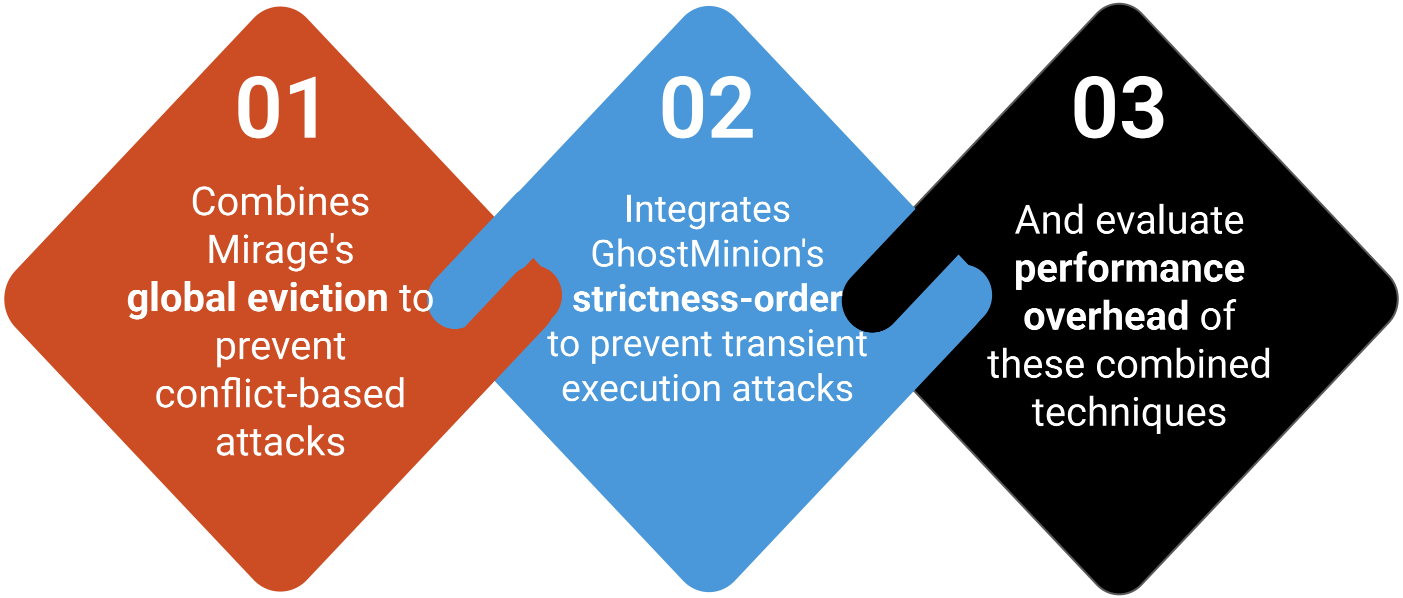
MIRAGE: Mitigating Conflict-Based Cache Attacks with a Practical Fully-Associative Design
USENIX Sec ‘21

GhostMinion: A Strictness-Ordered Cache System for Spectre Mitigation
MICRO ‘21

Combining them could provide comprehensive security but requires careful integration

Goal of the Project

Design a **hybrid cache architecture** that:



01

Combines Mirage's **global eviction** to prevent conflict-based attacks

02

Integrates GhostMinion's **strictness-order** to prevent transient execution attacks

03

And evaluate **performance overhead** of these combined techniques

Metrics of interest: IPC, MPKI

Plan for checkpoint-I

- Setup gem5 simulator and run MIRAGE artifact (Soumik)
- Run GhostMinion artifact (Arif)
- Performance evaluation of individual techniques on SPEC2017 & GAP workloads(Arnab)

Plan for checkpoint-II

- Design the integration of the combined technique (Soumik)
- Implement the integration in gem5 simulator & try possible optimisations as outlined in the papers (Arif)
- Measure performance overhead of the integration on SPEC2017 & GAP workloads(Arnab)

Github link

- https://github.com/sammagnet7/cs773_CompArch-Perf-Security.git