Pensieve: Microarchitectural Modeling for Security Evaluation

Yuheng Yang, Thomas Bourgeat, Stella Lau, Mengjia Yan
Problem: the Cat-and-Mouse Game

- 2018: Spectre
- 2019: InvisiSpec
  - Delay-on-Miss …
- 2020: Speculative interference attack
- 2021: GhostMinion

ISCA 2023
Problem: Weak Security Evaluation

We need a principled, trustworthy security evaluation framework!

Step 1:
Defense Proposal

Spectre Attacks

Step 2:
The defense works for all possible attack variants.

We need a principled, trustworthy security evaluation framework!
Pensieve’s Contribution

Defenses
- SafeSpec
- InvisiSpec
- GhostMinion
- GhostLoads
- Delay-on-Miss

Model

Security-Oriented Model

Aligned with architectural design flow.

Formal Tools
- JasperGold
- Rosette
- CVC5
- Coq
- Isabelle/HOL
- Boolector
- ACL2
- Z3

ISCA 2023
Defense Design Flow

A modeling method should be:
1. Modular
2. Precise on describing timing behaviors
3. Represent a space of designs
Pensieve Modeling

#1 Decouple timing and functionality using the hand-shaking interface
Uninterpreted Function (UF)

• A UF represents space of functions with the same input/output types

• Example: \texttt{Bool UF(Bool, Bool)}

Unspecified function body represents

\begin{itemize}
  \item \texttt{AND}
  \item \texttt{OR}
\end{itemize}
Pensieve Modeling

#1 Decouple timing and functionality using the hand-shaking interface

#2 Represent a space of timing behavior with uninterpreted functions

Pensieve uses **simple** models with **UF** to cover **space** of microarchitectures with **complex** timing behaviors
Pensieve Security Evaluation Framework

Micro-Arch Model → Model Checker → Security Property

(Speculative Non-interference)

FAIL: Attack Program
PASS: Security for k Cycles

Other verification tools

Other security properties

Pensieve finds **unknown** security vulnerabilities in GhostMinion, the latest speculative execution defense
GhostMinion prioritizes **smaller** timestamps

Original speculative interference attack

New attack variant found by Pensieve

**Takeaway:** Defenses should be driven by security properties, not by attack patterns

ISCA 2023
Pensieve Security Evaluation Framework

Security Property
(Speculative Non-interference)

Model Checker
FAIL: Attack Program
PASS: Security for k Cycles

Micro-Arch Model

Pensieve finds unknown security vulnerabilities in GhostMinion, the latest speculative execution defense