Pensieve: Microarchitectural Modeling for Formal Security Evaluation

Yuheng Yang, Thomas Bourgeat, Stella Lau, Mengjia Yan

To appear at ISCA’23
Problem: the Cat-and-Mouse Game

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

New England Hardware Security Day 2023
Problem: Weak Security Evaluation

We need a principled, trustworthy security evaluation tool!

Step 1: Defense Proposal

Step 2: Spectre Attack

The defense works for all possible attack variations.
Challenge: Bridge the Gap

Defenses
- SafeSpec
- Delay-on-Miss
- invisSpec
- Muon trap
- GhostLoad
- GhostMinion

Model

Evaluation Tools
- JasperGold
- Coq
- Isabelle/HOL
- Rosette
- CVC5
- Boolector
- ACL2
- z3

Aligned with architectural design flow.
An architecture modeling method should be
1. Modular
2. Precise on describing timing behaviors
3. Represent a space of designs

Example: delay speculative requests
Pensieve Modeling

• Decouple timing and functionality using the hand-shaking interface
• Represent a space of timing behavior

An architecture modeling method should be
1. Modular ✓
2. Precise on describing timing behaviors ✓
3. Represent a space of designs ?
Uninterpreted Function (UF)

• A UF represents space of functions with the same input/output types
  • Example: \texttt{Bool UF(Bool, Bool)}
• UF helps us
  • state “what” affects the output,
  • abstract away the details on “how” the input affects the output
Pensieve Modeling: Using UF

• Examples:

\[
\text{Multiply\_req\_latency} = \text{UF} (\text{historyOf} (\text{in\_valid}))
\]
\[
\text{Multiply\_req\_latency} = \text{UF} (\text{historyOf} (\text{in\_valid, in\_operands}))
\]
\[
\text{Memory\_req\_latency} = \text{UF} (\text{historyOf} (\text{in\_valid, in\_addr}))
\]

Pensieve can use simple models to cover space of microarchitectures with complex timing behaviors
Pensieve Modeling

- Decouple timing and functionality using the hand-shaking interface
- Represent a space of timing behavior with uninterpreted functions

![Diagram showing the interaction between Func, Memory System, and UF (Uninterpreted Functions) with signals in_valid, in_ready, out_valid, out_ready, and addr, with timing signals and functional signals indicated.]

New England Hardware Security Day 2023
Pensieve finds **unknown** security vulnerabilities in the latest speculative execution defense, i.e., GhostMinion [2021]
New Attack on GhostMinion Summary

speculative interference attack

\[
\begin{align*}
y &= \ldots \\
\text{ld } y &\quad // \text{transmitter} \\
\text{if (false)} &\quad \text{ld sec } // \text{interfere}
\end{align*}
\]

new attack variant

\[
\begin{align*}
\text{if (true)} &\quad \text{ld y } // \text{transmitter} \\
\text{else} &\quad \text{ld sec } // \text{interfere}
\end{align*}
\]

Takeaway: Manual evaluation can easily be unsound, we need Pensieve, a trustworthy evaluation tool

New England Hardware Security Day 2023