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
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
- GhostMinion
- GhostLoads

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

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
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: `Bool UF(Bool, Bool)`
- UF helps us
  - state “what” affects the output,
  - abstract away the details on “how” the input affects the output

Unspecified function body represents `AND`, `OR`, and `...`
Pensieve Modeling: Using UFs

• Examples:

\[ \text{Multiply}_\text{req}_\text{latency} = \text{UF}(\text{historyOf}(\text{in}_\text{valid})) \]
\[ \text{Multiply}_\text{req}_\text{latency} = \text{UF}(\text{historyOf}(\text{in}_\text{valid}, \text{in}_\text{operands})) \]
\[ \text{Memory}_\text{req}_\text{latency} = \text{UF}(\text{historyOf}(\text{in}_\text{valid}, \text{in}_\text{addr})) \]

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

speculative interference attack

\[
y = \ldots \\
ld y // transmitter \\
if (\text{false}) \\
ld \text{sec} // \text{interfere}
\]

new attack variant

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

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