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

Intel RARE Workshop 2023
Problem: Weak Security Evaluation

We need a principled, trustworthy security evaluation framework!

Step 1:
Defense Proposal

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

Spectre Attacks

"Piled Higher and Deeper" by Jorge Cham www.phdcomics.com
Pensieve’s Contribution

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

Security-Oriented Model

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

Model

Aligned with architectural 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: `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

#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 finds unknown security vulnerabilities in GhostMinion, the latest speculative execution defense
#1: Invisible Speculation

**GhostMinion**

if (false)
ld sec //transmitter

**Spectre v1**

**Insecure Baseline**

**Invisible Speculation**

Rest of Memory System

Rest of Memory System

Intel RARE Workshop 2023
Speculative Interference Attack

- **Younger** speculative loads interfere with **older** bound-to-commit loads.
- Many other contention structures: non-pipelined ALU, cache port, bank contention, network-on-chip, etc.

```plaintext
y = ...... //delay
ld y // transmitter
if (false)
  ld sec // interfere
```

Diagram:
- Younger speculative loads interfere with older bound-to-commit loads.
- Various contention structures include non-pipelined ALU, cache port, bank contention, network-on-chip, etc.

Intel RARE Workshop 2023
GhostMinion

#1: Invisible Speculation

#2: Prioritize Older Instructions through Timestamps

```
y = …... //delay 0
ld y //transmitter 1
if (false) 2
ld sec //interfere 3
```

Timestamp (based on decode time)
So Far …

2018
Spectre

2019
InvisiSpec
Delay-on-Miss …

2020
Spectre rewind
Speculative interference attack

2021
GhostMinion

Use Pensieve
## Pensieve Found A New Attack Variant

<table>
<thead>
<tr>
<th>Speculative load is older this time!</th>
</tr>
</thead>
</table>

### Code Snippet

```c
if (true)
    ld y // transmitter
else
    ld sec // interfere
```

### Timestamps

<table>
<thead>
<tr>
<th>Before Squash</th>
<th>After Squash</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

→ Speculative load can interfere with bound-to-commit load

---

Intel RARE Workshop 2023
New Attack on GhostMinion Summary

speculative interference attack

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

new attack variant

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

Takeaway: Manual evaluation can easily be unsound, we need Pensieve, a trustworthy evaluation tool
Checking Time and Scalability

- Microarchitecture Setup
  - 5 types of instructions
  - 4-entry register file
  - 4-entry data memory
  - 16-entry instruction memory
  - 8-entry ROB
  - GhostMinion defense

- Problem: Checking time increases exponentially as the number of simulated cycles increases

- Future work: Combine Penseive with more powerful formal verification backend
Pensieve Summary

• Pensieve provides a modeling principle that **aligns** with architecture design flow, and **links** computer architects to accessible formal-methods tools.
• Pensieve finds **unknown** security vulnerabilities in GhostMinion

![Diagram of security verification process]

**Security Property:** (Speculative Non-interference)

- Other security properties
- PAIE: Attack Program
- PASS: Security for k Cycles

**Verification Tools**

Intel RARE Workshop 2023