I. Why Do We Need Security Evaluation? 

The Endless Cat-and-Mouse Game

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

II. Challenge: Bridge the Gap

Defenses
SafeSpec
Delay-on-Miss
invisiSpec
Muontrap
GhostLyons
GhostMinion

Evaluation Tools
JasperGold
Rosette
CVC5
Coq
Isabelle/HOL
Boolector
z3

We Propose: A modeling approach aligned with how architects design defense.

III. Pensieve Microarchitectural Modeling

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

![Uninterpreted Function Diagram]

What is Uninterpreted function?

- A UF represents space of functions with 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
- Use UF to represent a space of timing behavior
  - Memory_latency = UF(history(in_valid, in_addr))

IV. Pensieve Security Evaluation Framework

- Security Property
- Micro-Arch Model
- PASS: Security for k Cycles
- FAIL: Attack Program
- Other verification tools

V. 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 Pensieve with more powerful formal verification backend

VI. New Attack Variant on GhostMinion

V-1. Spectre is MITIGATED by InvisiSpec

```plaintext
if (false)
  ld sec // transmitter
```

V-2. Speculative Interference Attack BREAKS InvisiSpec

(a) Pipeline view

(b) Memory traces

V-3. Speculative Interference Attack is MITIGATED by GhostMinion

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

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

"ld sec" is after "ld y" in program order

V-4. New Attack Variant BREAKS GhostMinion

```
if (true)
  ld y //transmitter
else
  ld sec //interface
```

V-5. Summary

No program order between "ld sec" and "ld y"