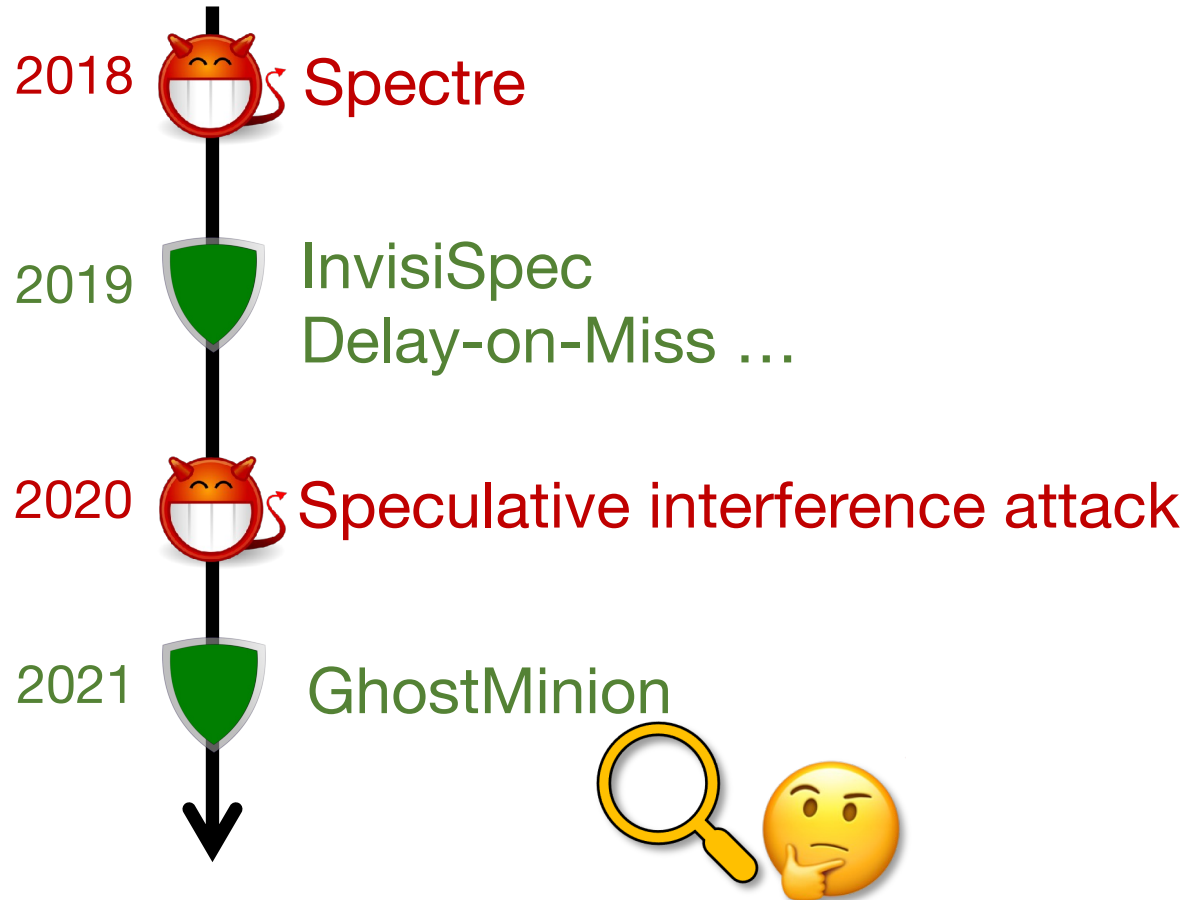


# **Pensieve: Microarchitectural Modeling for Security Evaluation**

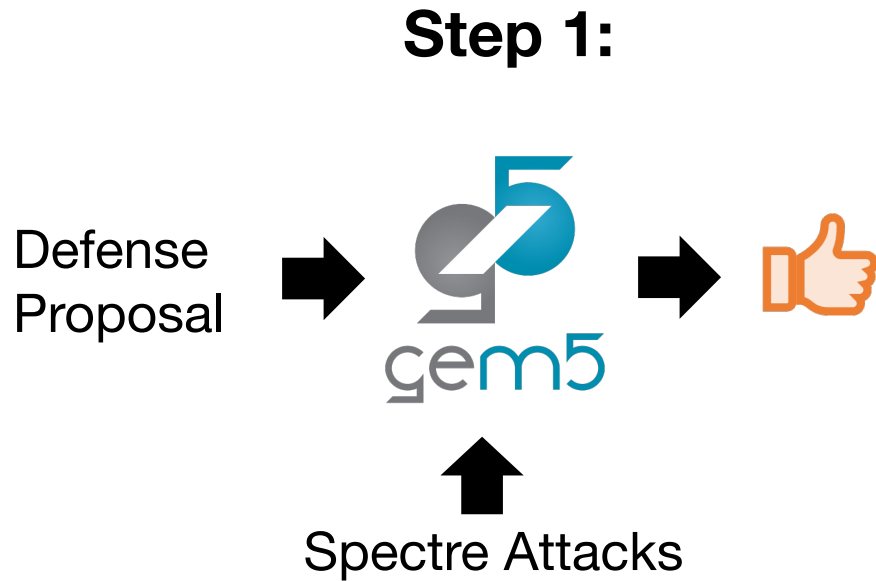
**Yuheng Yang, Thomas Bourgeat, Stella Lau, Mengjia Yan**



# Problem: the Cat-and-Mouse Game

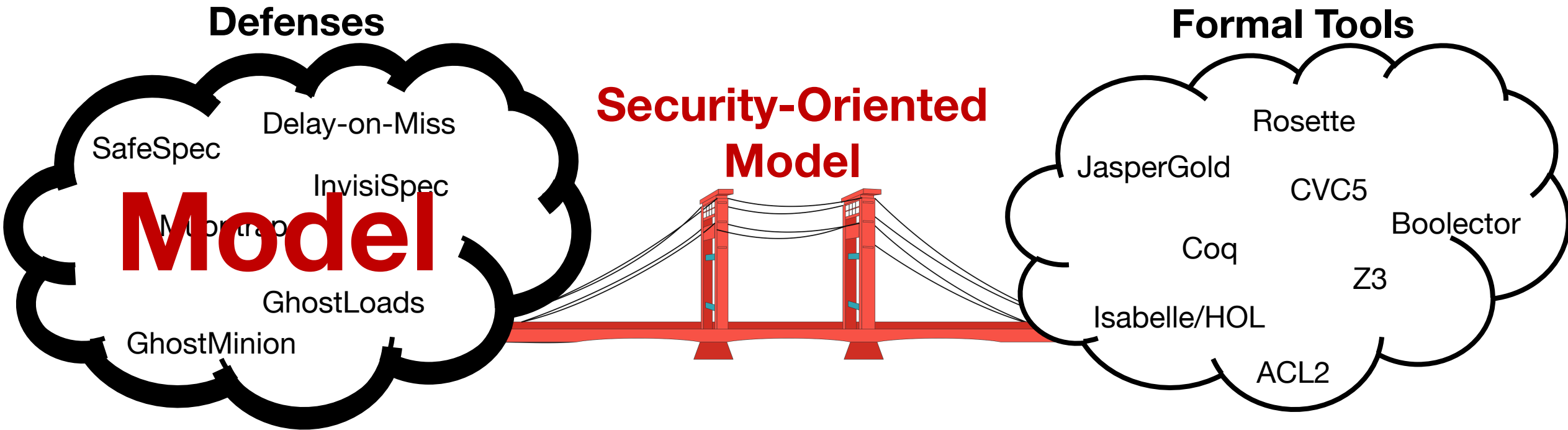


# Problem: Weak Security Evaluation



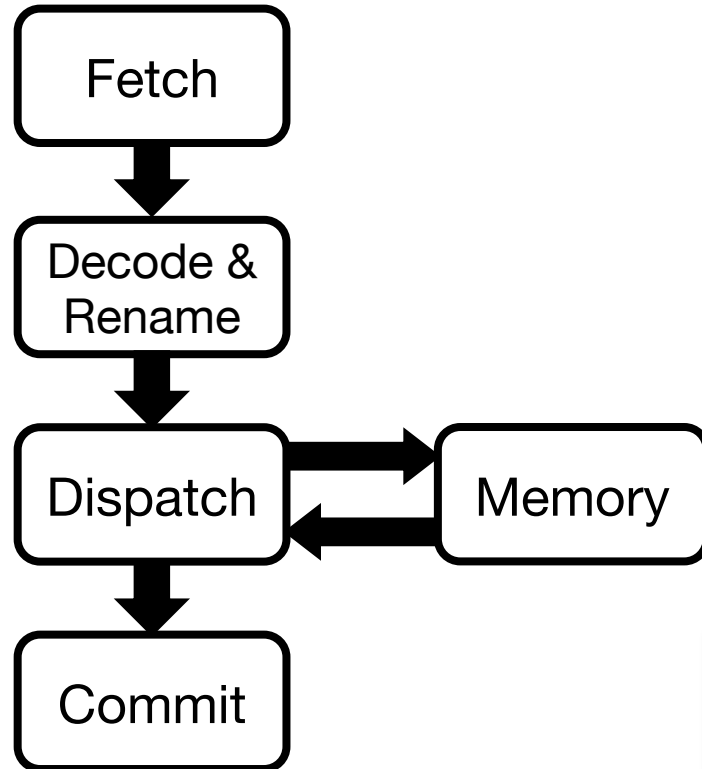
**We need a principled, trustworthy security evaluation framework!**

# Pensieve's Contribution



**Aligned** with architectural design flow.

# Defense Design Flow



Example: delay speculative requests

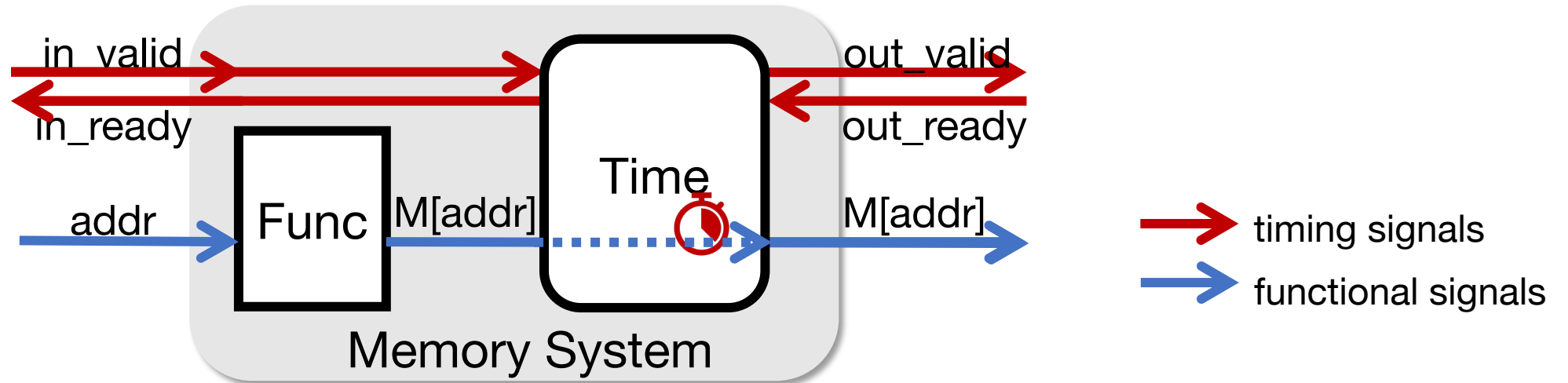


A modeling method should be:

1. Modular
2. Precise on describing timing behaviors
3. Represent a space of designs

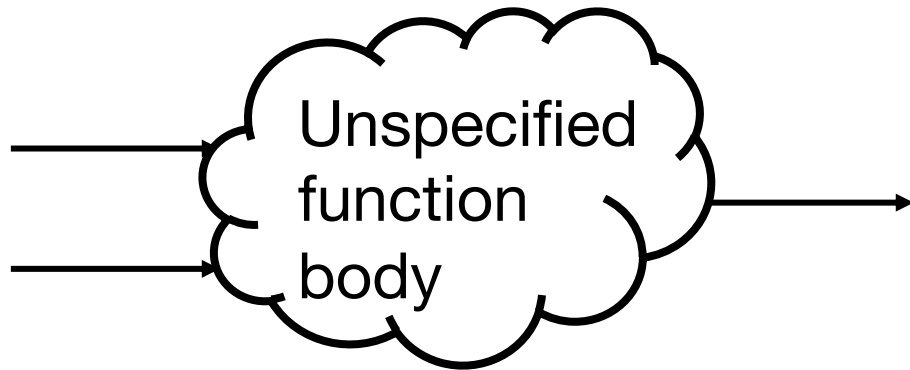
# Pensieve Modeling

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

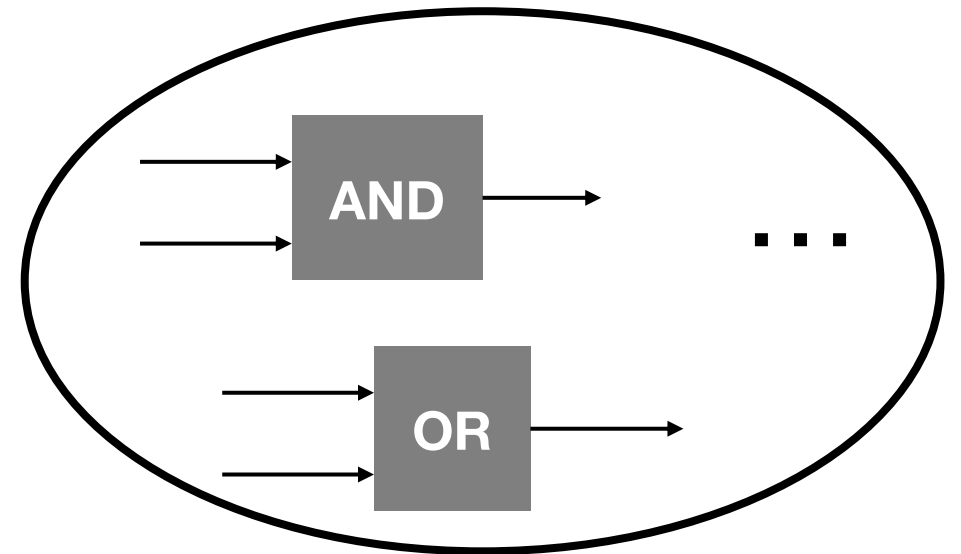


# Uninterpreted Function (UF)

- A UF represents space of functions with the same input/output types
- Example: `Bool UF (Bool, Bool)`



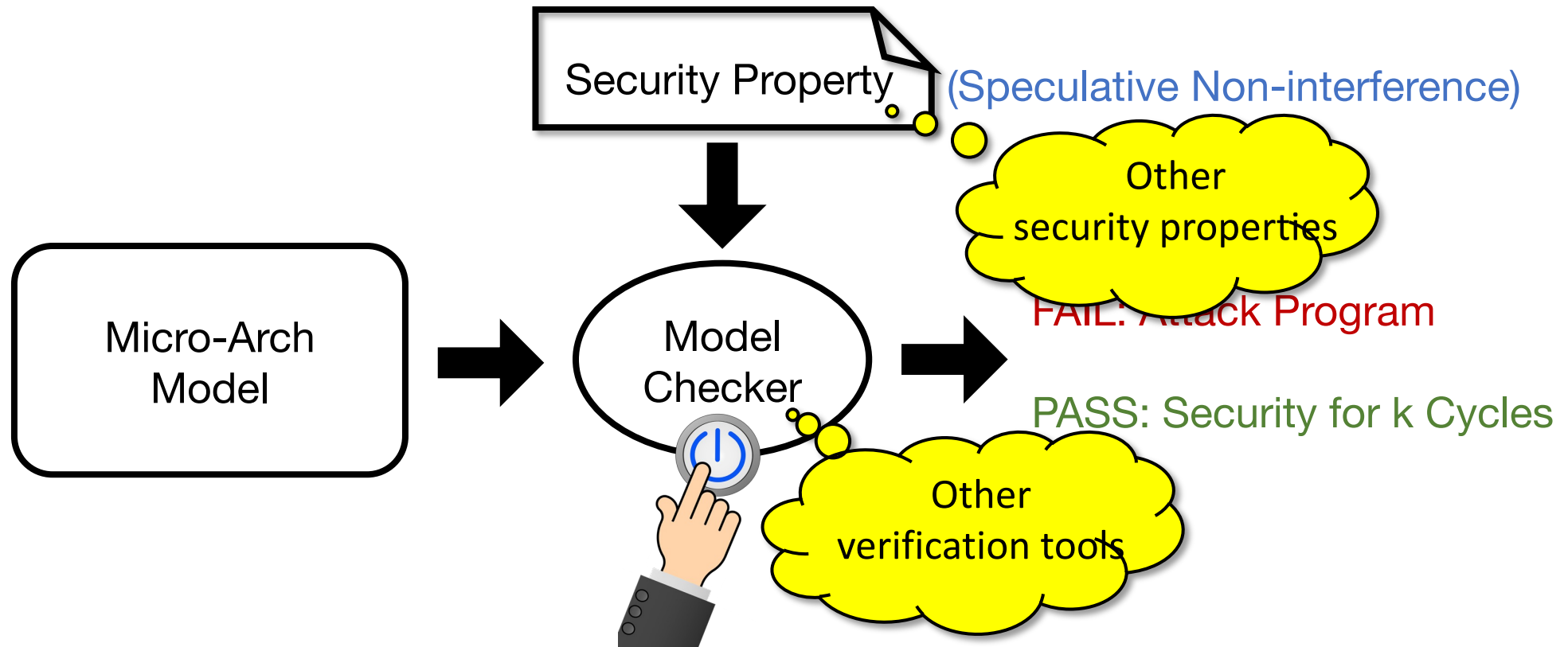
represents







# Pensieve Security Evaluation Framework




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

# Pensieve Breaks GhostMinion

GhostMinion prioritizes **smaller** timestamps

Timestamp  
(based on decode time)

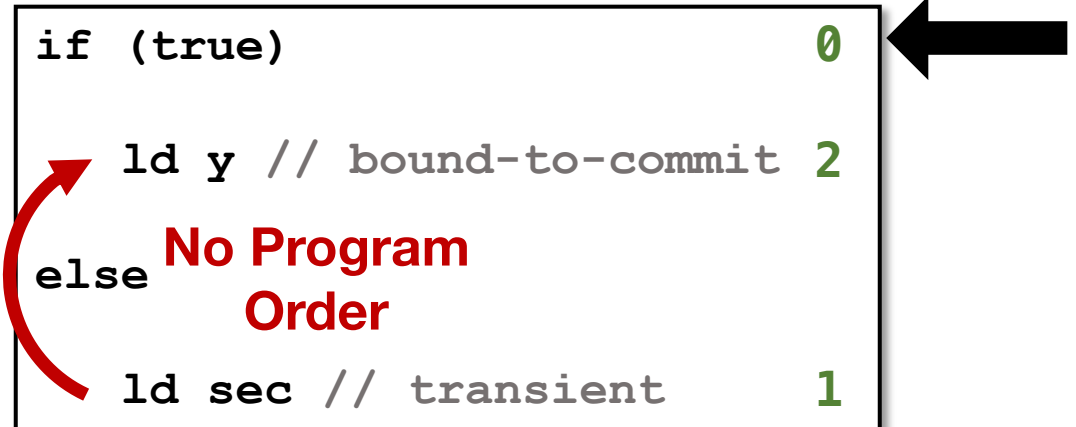
```
y = ..... // delay           0
ld y // bound-to-commit      1
if (false)                    2
ld sec // transient          3
```



Original speculative interference attack

Timestamp  
(based on decode time)

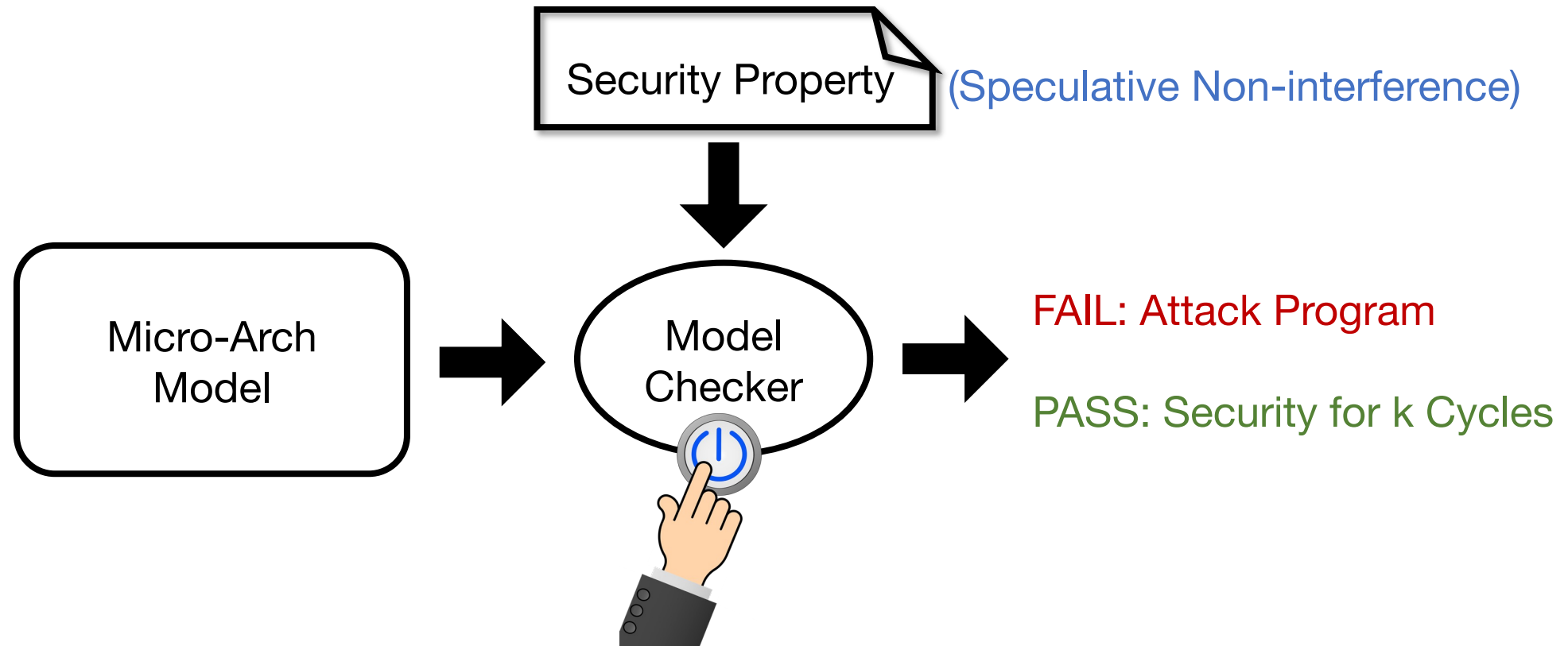
```
if (true)                      0
ld y // bound-to-commit      2
else No Program Order
ld sec // transient          1
```



New attack variant found by Pensieve

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

# Pensieve Security Evaluation Framework



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