Reconfigurable Hardware for Microarchitectural Timing Attacks

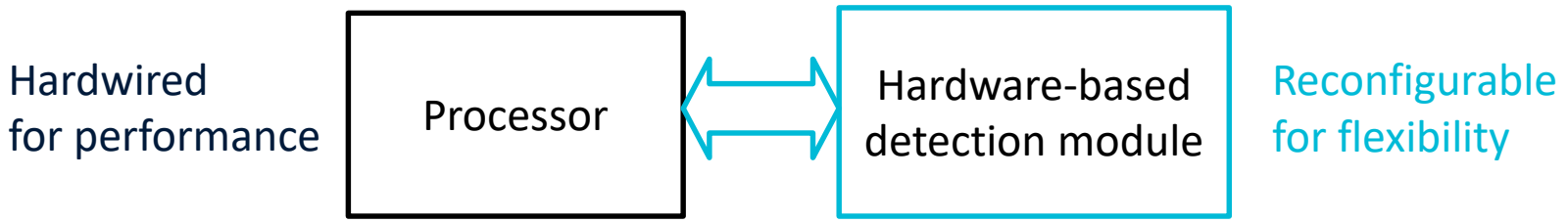
Yuxiao MAO
Vincent MIGLIORE
Vincent NICOMETTE

RESSI 2020

Motivation

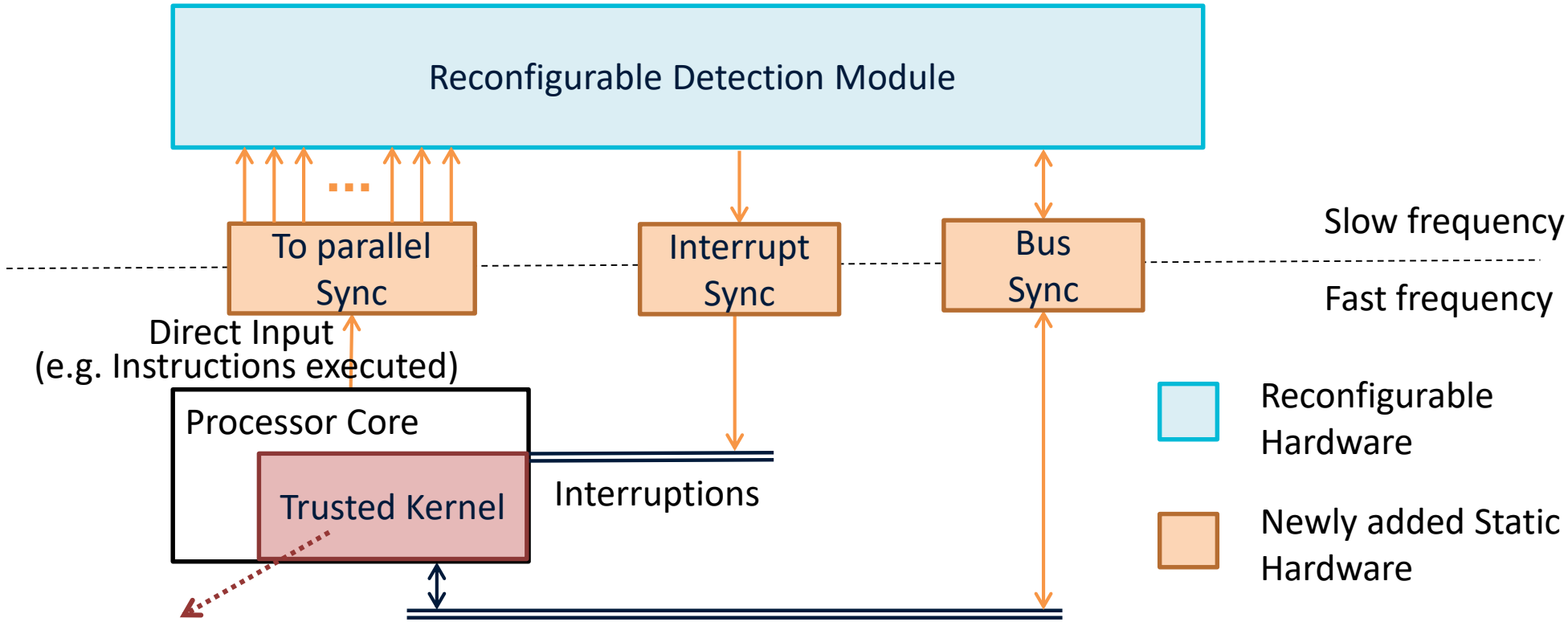
- Software-based attacks that exploit hardware microarchitectural properties
  - Cache side-channel attacks, Spectre and Meltdown, Rowhammer …
- Solutions proposed so far
  - Software (**Pros:** flexible. **Cons:** high overhead, difficulty of getting low-level information)
  - Dedicated hardware (**Pros:** fine tuned mitigation, efficient. **Cons:** impossible to adapt to new attacks)

➢ Our solution: REHAD (REconfigurable Hardware for Attacks Detection)



- Challenges
  - Frequency gap between the processor core and reconfigurable hardware
  - Covering as many attacks as possible
  - Amount and type of information exchanged between the processor and the detection module

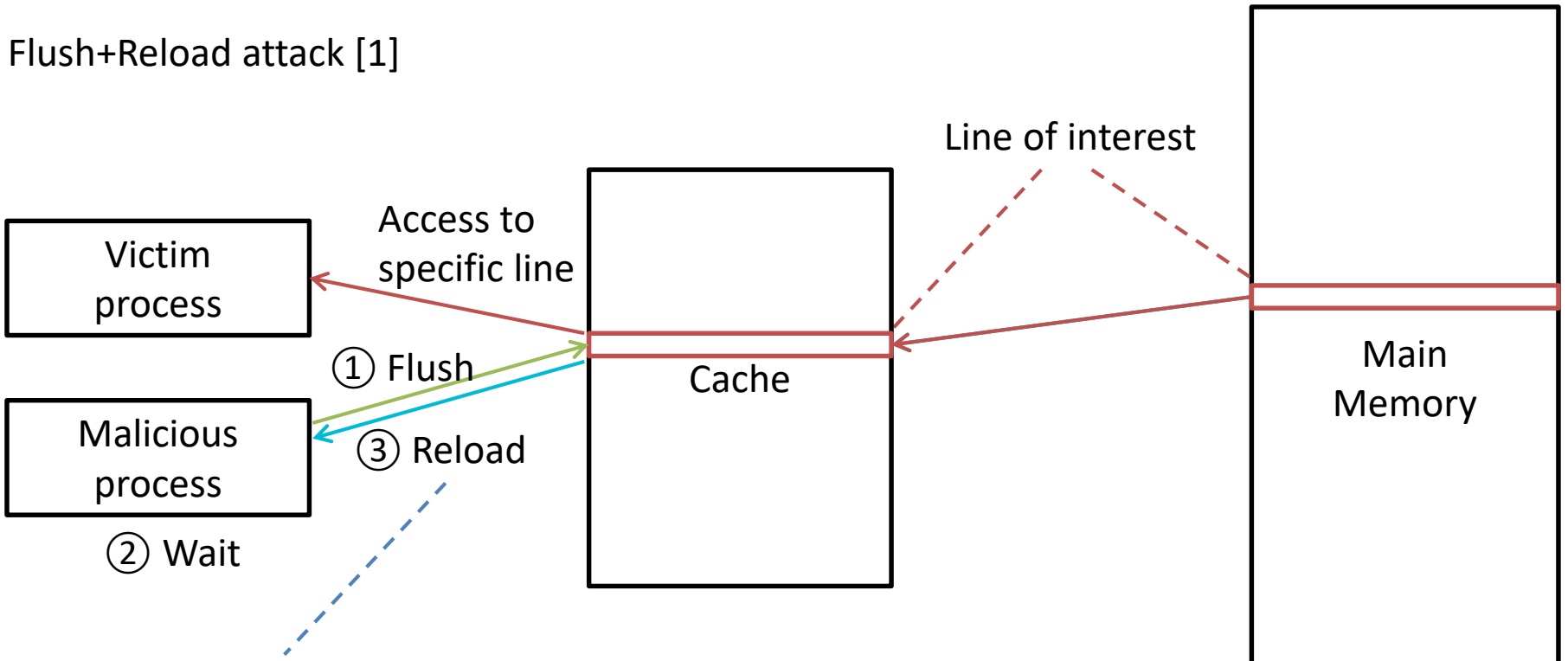
REHAD architecture



- Handles interruptions
- Configures
- Provides information
- Reconfigures

Implementation: Cache side-channel attacks

Flush+Reload attack [1]



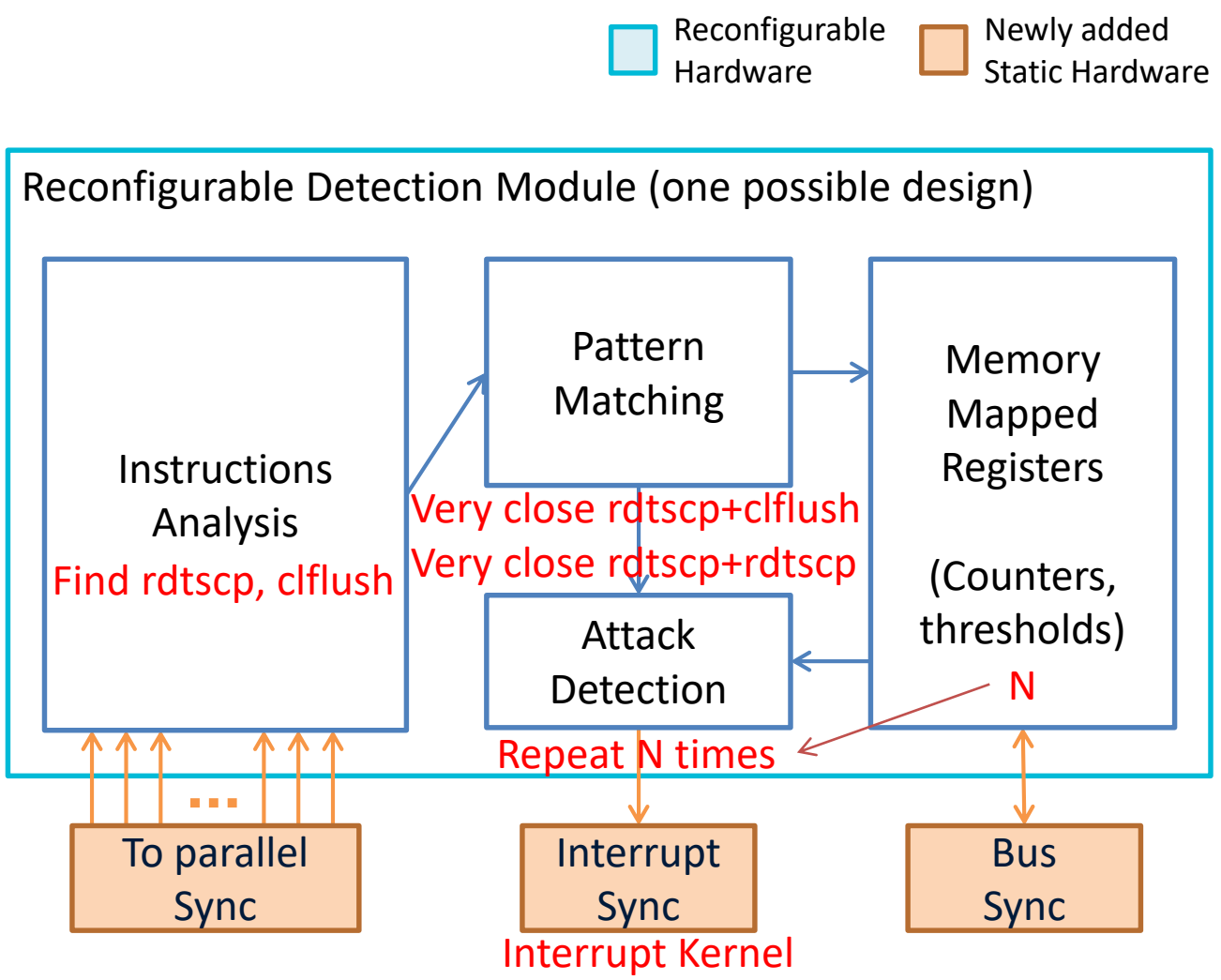
Measure time of [Reload]
If Victim accessed [line] => Fast
If not => Slow

[1] Y. Yarom and K. Falkner, "FLUSH+RELOAD: a High Resolution, Low Noise, L3 Cache Side-Channel Attack," in Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, Aug. 2014, pp. 719–732.

Implementation: Detect Flush+Reload

```
mfence
rdtscp
mov %eax, %esi
mov (%ebx), %eax
rdtscp
sub %esi, %eax
clflush (%ebx)
```

Flush+Reload attack
on x86 from Mastik Toolkit [2]



[2] Y. Yarom, "Mastik: A Micro-Architectural Side-Channel Toolkit," 2016. https://cs.adelaide.edu.au/yval/Mastik/

Future Work

- ✓ Basic Prime+Probe attack detection
  - Only need to reconfigure the Detection Module
- ✓ Move to Rocket-Chip softcore processor
  - Can be adapted to different processor cores
- ➢ Run benchmarks with Linux on FPGA
  - Measure false positive rate
- Other internal structure of Detection Module
  - Where reconfigurable is better than reprogrammable
- Other attacks
- …

Thank you. Questions?

Yuxiao MAO yuxiao.mao@laas.fr
Vincent MIGLIORE vincent.migliore@laas.fr
Vincent NICOMETTE vincent.nicomette@laas.fr

RESSI 2020