

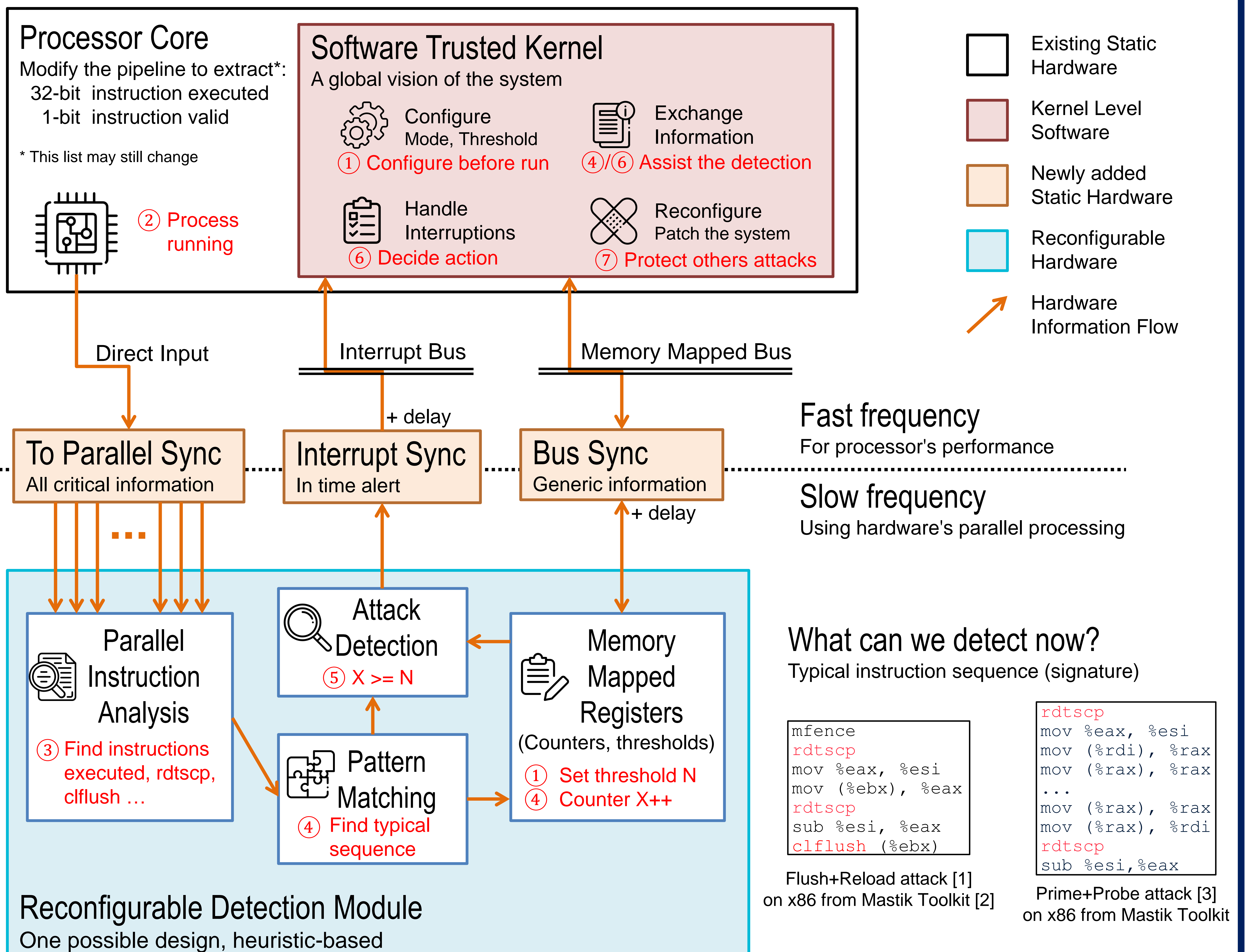


Context & Motivation

-  **Attacks:** Software-based attacks that exploit hardware microarchitectural properties
Cache side-channel attacks, Spectre and Meltdown, Rowhammer ...
-  **Defenses:** 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)

REHAD (REconfigurable Hardware for Attacks Detection)

Runtime monitoring • Low-frequency detection • Hardware & software hybrid • Instruction-based • No user program modification



Implementation

Platform: ML605 dev board (Virtex-6 FPGA)
Processor: Orca (32-bit, RISC-V)
Rocket-Chip (64-bit, RISC-V)
Resources: ~ 220 LUTs, ~ 70 FFs for Detection
~ 220 LUTs, ~ 730 FFs for Synchronization

Future Work

- > Run benchmarks with Linux on FPGA?
 - Measure false positive
- Other structure of Detection Module: Machine Learning based?
 - Where reconfigurable is better than reprogrammable
- Other attacks: Spectre? ROP? Malware signature?

References:

- [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.
[2] Y. Yarom, "Mastik: A Micro-Architectural Side-Channel Toolkit," 2016. <https://cs.adelaide.edu.au/yval/Mastik/>
[3] D. A. Osvik, A. Shamir, and E. Tromer, "Cache Attacks and Countermeasures: The Case of AES," in Topics in Cryptology CTRSA 2006, vol. 3860. Berlin, Heidelberg: Springer, Feb. 2006, pp. 1–20.
[4] Icons made by Freepik, srip, Kirqshqstry, Pixel perfect from www.flaticon.com