Protection of a processor with DIFT against physical attacks

William PENSEC, Vianney LAPÔTRE, Guy GOGNIAT
Univ. Southern Brittany, ARCAD team, Lab-STICC, UMR 6285, France
firstname.lastname@univ-ubs.fr

Abstract

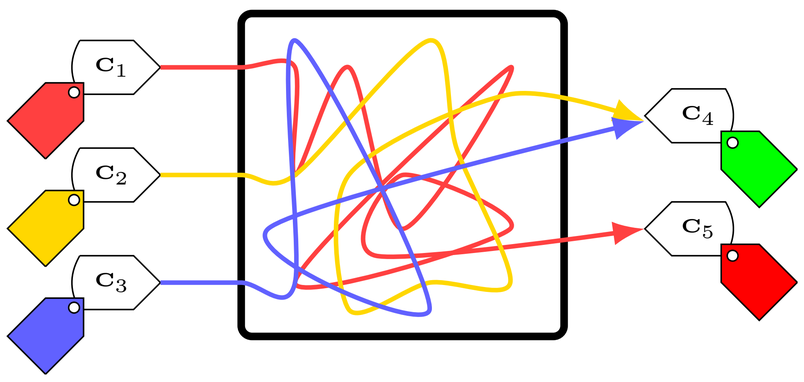
Internet of Things (IoT) devices are spreading massively in critical infrastructures like industry, smart cities, bio-medical devices, etc. Unfortunately, they also contribute to the increase of the attack surface of information systems, which represents a significant threat. A low-cost processor is usually a key element of IoT devices. Thus, it is necessary to build protection mechanisms taking into account performances, energy consumption and area.
Due to network connectivity and proximity to attackers, embedded systems face both software and physical attacks. Dynamic Information Flow Tracking (DIFT) techniques can detect various software attacks by attaching and propagating tags to information containers at runtime.
The goal of this project is therefore to design and evaluate a robust DIFT protection mechanism against both software and physical attacks (side channel analysis and fault injection attacks). This work relies on an open source RISC-V processor.

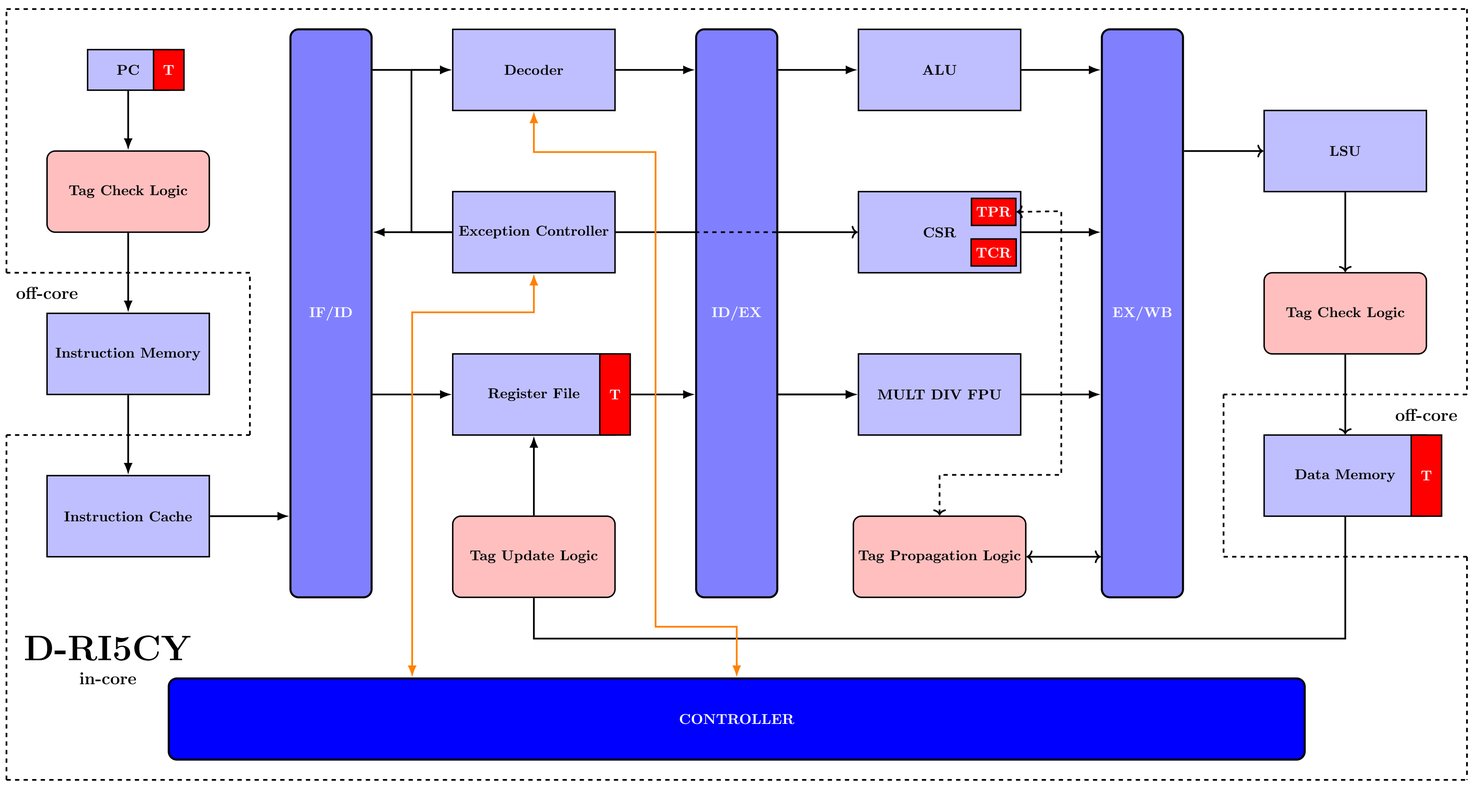
Information Flow Tracking in a RISC-V processor

Different types of IFT:
- Static or Dynamic[1, 2]
- Software, hardware (in-core, off-core (dedicated CPU, co-processor)) or mixed

Three steps
- Tag initialization
- Tag propagation
- Tag verification

Levels of IFT
- OS level
- Application level
- Low level



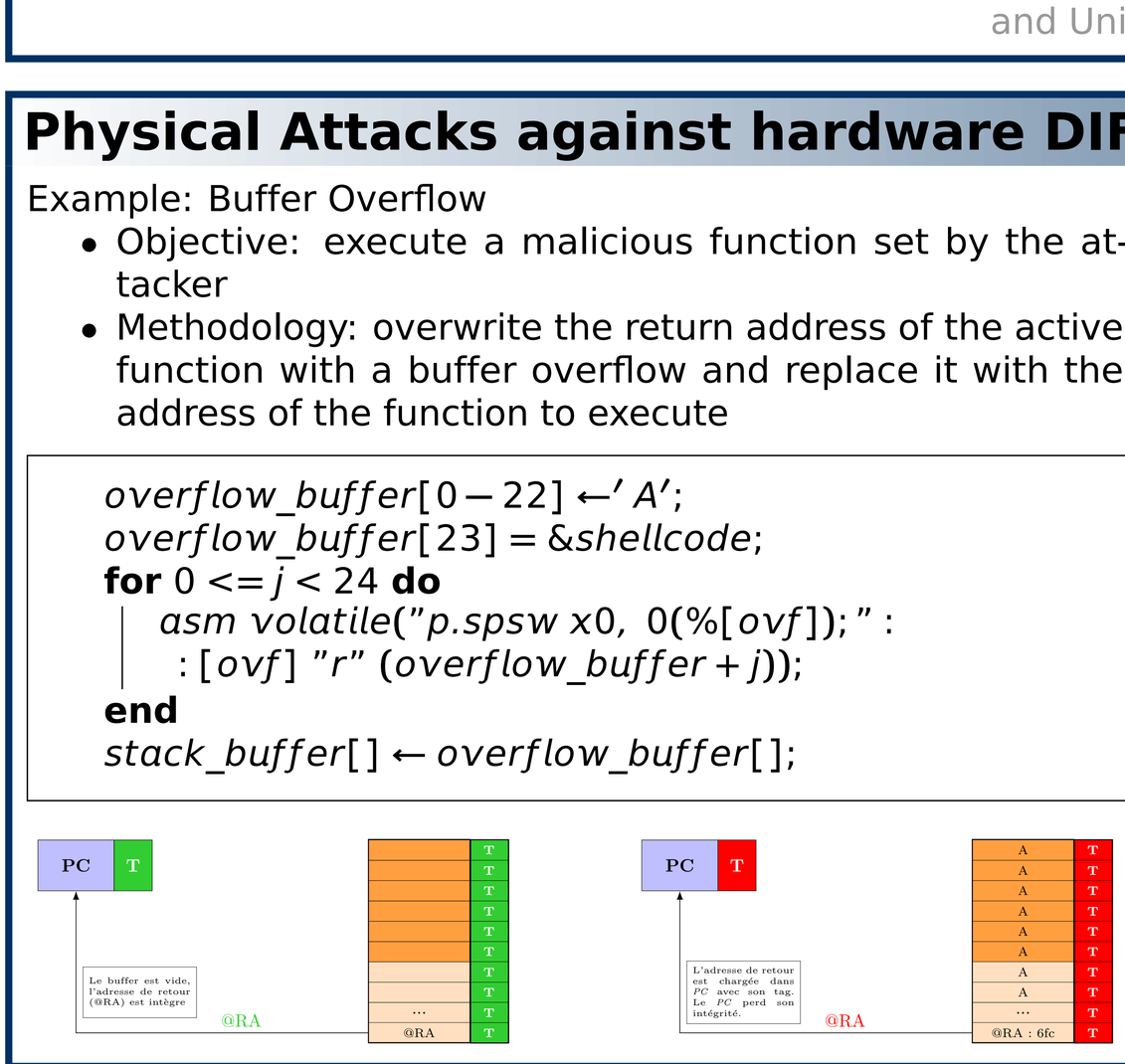


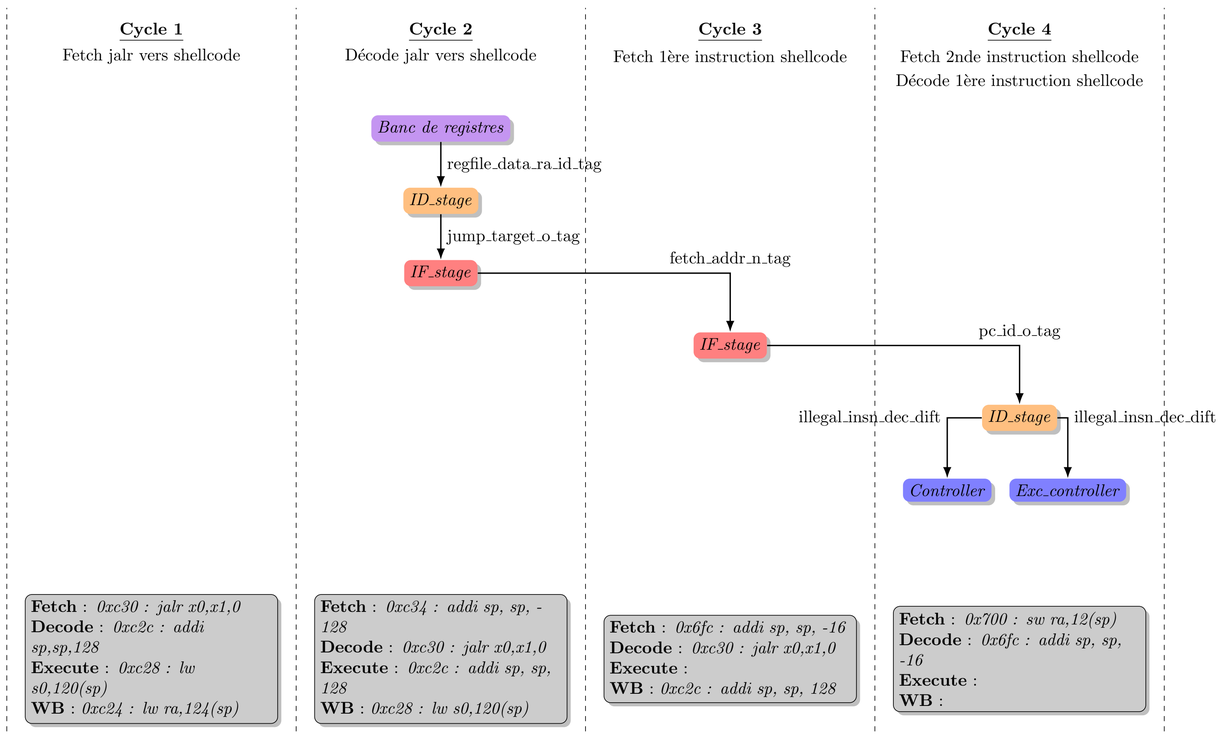
D-RI5CY[3] has been developed by researchers from Columbia University, New York, and University of Turin (Italy).

Physical Attacks against hardware DIFT

Example: Buffer Overflow
- Objective: execute a malicious function set by the attacker
- Methodology: overwrite the return address of the active function with a buffer overflow and replace it with the address of the function to execute

```
overflow_buffer[0−22] ←' A';
overflow_buffer[23] = &shellcode;
for 0 <= j < 24 do
    asm volatile("p.spsw x0, 0(%[ovf]);" :
      : [ovf] "r" (overflow_buffer + j));
end
stack_buffer[] ← overflow_buffer[];
```





Perspectives

- Study the impacts of physical attacks in hardware DIFT through fault injection campaigns (simulation and actual clock/voltage glitches or EM injections)
- Propose, develop and evaluate hardware countermeasures taking into account several constraints such as area, energy consumption, performance targeting a FPGA implementation

Bibliography

[1] W. Hu *et al.*, "Hardware information flow tracking," vol. 54, no. 4, May 2021, ISSN: 0360-0300. DOI: 10.1145/3447867. [Online]. Available: https://doi.org/10.1145/3447867.
[2] M. A. Wahab, "Hardware support for the security analysis of embedded softwares : Applications on information flow control and malware analysis," PhD Thesis, Centrale Supelec, Université Bretagne Loire, Dec. 2018. [Online]. Available: https://tel.archives-ouvertes.fr/tel-02634340.
[3] C. Palmiero *et al.*, "Design and implementation of a dynamic information flow tracking architecture to secure a risc-v core for iot applications," 2018.