Labex UCN@Sophia

http://ucnlab.eu

Analyzing Security Properties at the Interface between HW & SW

Supervisors :

Ludovic Apvrille (Telecom ParisTech)

Aurélien Francillon (EURECOM)

Florian Lugou

florian.lugou@telecom-paristech.fr

The Goal

Formal Verification

Finding a modular approach to formally **prove** **security** properties of a piece of **software** running on a **custom** **hardware**.

Focus on Security

HW / SW Co-Designs

Adaptive Method

Why is it Challenging ?

Security

- Needs an **accurate** formal model of HW
- Possibilities of **abstraction limited**

Formal Verification

- **Limit approximations** as much as possible

Adaptive Method

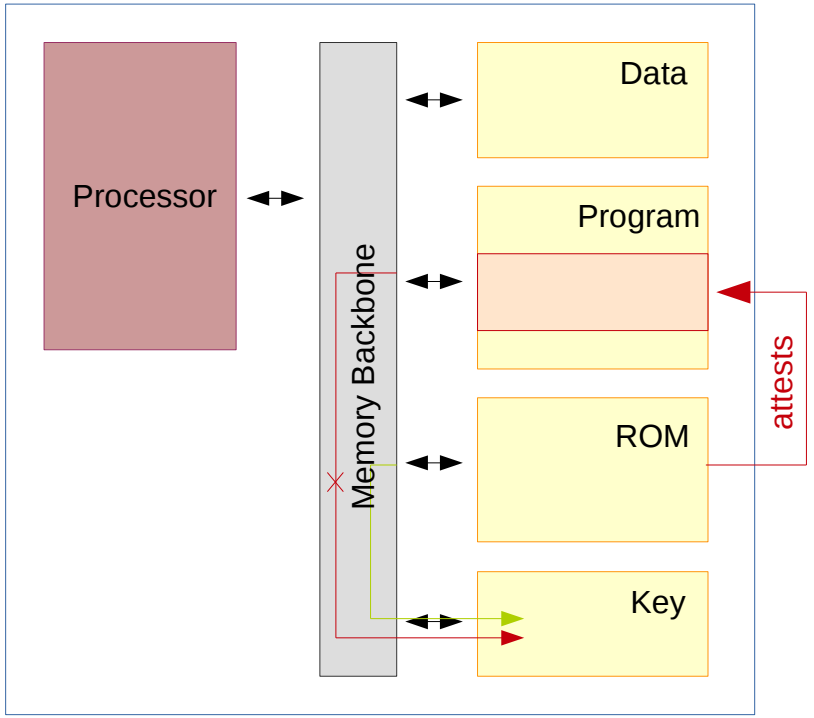
- **No hard-coded** HW model

HW / SW Co-Designs

- Different objectives, different abstraction levels, **different methods**
- HW and SW are **tightly coupled** in security designs

A First Approach

SMART




```
l2:
    cmp         r3,         r4
    jeq         l3
    mov.w       #0x0000,    @r4
    add.w       #1,         r4
```

.pv

ProVerif

```
Starting query not attacker(secret[])
RESULT not attacker(secret[]) is true.
```