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

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

**Focus on Security**

**Formal Verification**

**HW / SW Co-Designs**

**Adaptive Method**
Why is it Challenging?

Security

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

Adaptive Method

- **No hard-coded** HW model

Formal Verification

- **Limit approximations** as much as possible

HW / SW Co-Designs

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

SMART

Processor

Memory Backbone

Data

Program

ROM

Key

12:

cmp r3, r4
jeq 13
mov.w #0x0000, @r4
add.w #1, r4

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