HACK MY CHIP:
A RED TEAM BLUE TEAM APPROACH FOR SOC SECURITY

David HELY
Grenoble INP–Esisar LCIS, Valence
david.hely@grenoble-inp.fr

NANOELEC.
Institut de recherche Technologique Nanoelec

UNIVERSITÉ Grenoble Alpes

LCIS
Laboratoire de Conception et d'Intégration des Systèmes

Grenoble INP

Red Team vs Blue Team

- What is this approach?
  - Given a System
    - The Red Team develops attacks
    - The Blue Team develops countermeasures
  - In order to define and validate:
    - New security test-benches
    - New countermeasures

What is **not** this approach?

- A hacking competition on commercial/industrial products
- A promotion of hacking

Why such an Approach?

- **Security exploits are sensitive**
  - Few « real world » attacks and secure system are available
  - A need for security test suites
- **Hacking is a « dynamic » activity**
  - New exploits/attacks are frequently created
  - This requires recurrent update of security testbench
- **Students are creative and enthusiastic**
  - Challenging security issues may arise
- **Pedagogic approach**
  - Practical way to get hands on Security Issues
  - Motivating and Challenging for students

CSAW: Embedded System Challenge (1)

- International Student Competition based on the Red Team/Blue Team Approach
- Participation of Esisar Students
- 2016 subjects: **Secure Processor Design**

CSAW: Embedded System Challenge (2)

Objectives:

- Demonstrating software vulnerabilities on a given processor system:
  - OpenRISC
- Modifying the processor hardware in order to secure it against such attacks:
  - How hardware can Thwart software vulnerabilities?

CSAW: Embedded System Challenge (2)

- Hardware mitigations for memory corruption and control flow integrity attacks in Embedded Systems
- System Baseline
  - OpenRisc based Embedded System running Linux on an FPGA
- Red Team:
  - Design software exploits for Linux programs running on an OpenRISC system
- Blue Team:
  - Design and Implement hardware-based mitigations for the OpenRISC processor to protect against different exploitation methods

CSAW: Embedded System Challenge (3)

- Evaluation:
  - Practical Evaluation
    - Each team plays both roles
    - Attacks are played on each secure embedded system
    - A team scores when its attack succeeds or when its defense resists
  - Evaluation by a panel of industry expert
    - Each teams presents the solution in front of a panel of industry expert judges which evaluates the countermeasures based on:
      - Cost, performance, integration, efficiency…

CSAW: Embedded System Challenge (4)

- Outcomes:
  - A practical Evaluation Platform for Embedded System Security Design :
    - A set of exploits for evaluation
    - Different countermeasures designed and Evaluated
    - Ready to use for both Research and Teaching Activities
  - From an Academic point of view:
    - Valuable Experience in embedded System Security for the students
    - New materials for teaching Activities
    - New Materials for On-going and Future research
  - From an industrial Point of view
    - Identification of promising students
    - Access to the platforms and associated materials

LCIS
Laboratoire de Conception et d'Intégration des Systèmes

Grenoble INP ESISAR

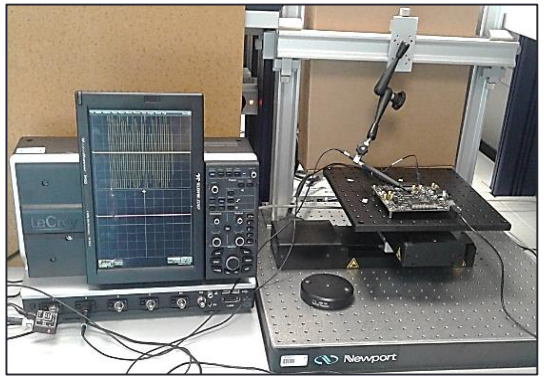
esynov

UNIVERSITÉ Grenoble Alpes

INP

Existing/On-Going Platforms (1)

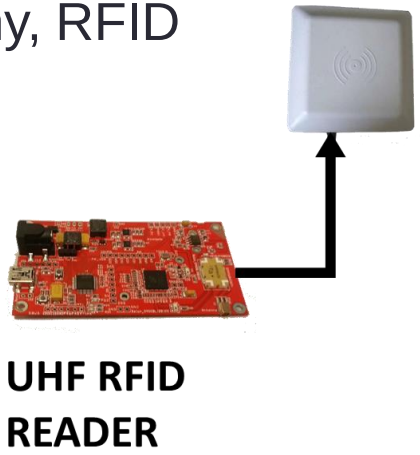
- Side channel Attacks
  - EM and Power Analysis
  - Different Ciphers: AES, DES, ECC, PRESENT
  - Different Implementations: SW and HW

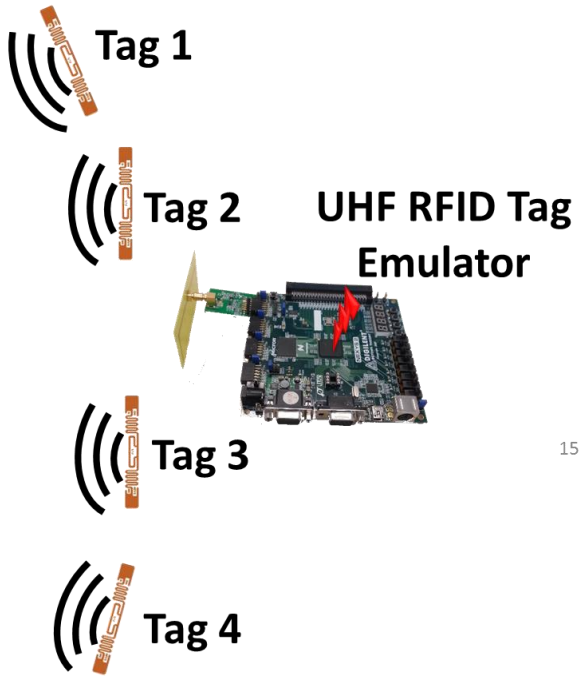


- Fault Attacks
  - Simulation based Fault Injection
  - Work on both models and countermeasures

Existing/On-Going Platforms (2)

- Secure RFID
  - In System Evaluation of Secure RFID protocol
  - Lightweight Cryptography, RFID Robustness





15

- Secure Processor Design
  - SoC Lifecycle Security
  - HW support to SW security

Conclusions

- Such Platforms and Activities are essential for Teaching and Research in the fields of IoT security in order to :
  - Promote hardware security issues and solution in modern IoT devices
  - Support solutions development (Research and Technology Transfer)
  - Keep Defense Designers up to date of hackers capabilities
  - Perform in System Evaluation of hardware based security solutions