Introduction to Security of Embedded Systems

Jean-Luc Danger

December 2019

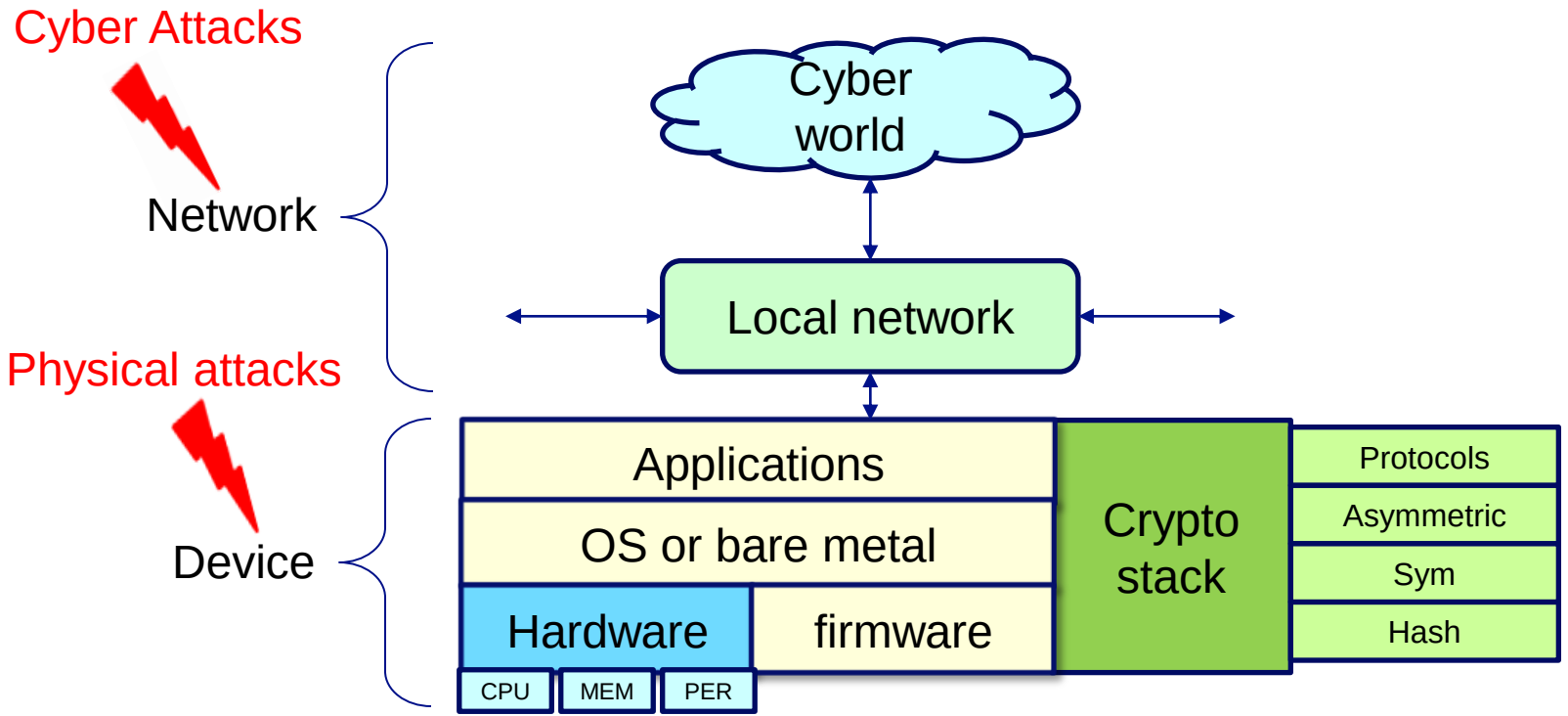
Outline

- Big Picture
- Attacks
- Hardware Protections
- Conclusion

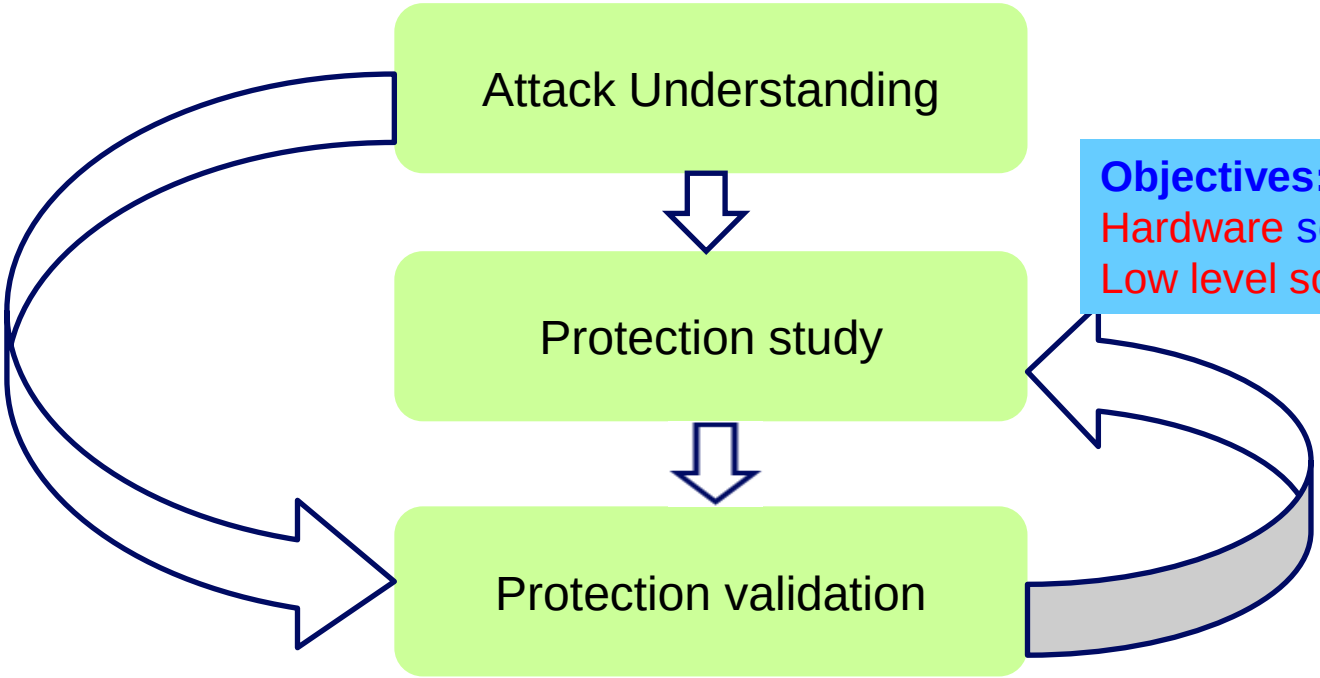
Embedded Systems Security

- **Embedded Systems Properties**
  - Dedicated computation
    - Mobiles, Set-top Boxes, Transport., Bank, Smart Home, …
  - Connected (IoTs)
  - High volume => Low-cost
  - Remotely and Physically accessible
- **Many security issues**
  - Remotely: Cyber Attacks
    - Software bug or misconfiguration => Software attacks by the network
  - Locally: Physical Attacks
    - Side-channel analysis
    - Fault injection attacks
    - Probing Attack
    - Reverse Engineering
    - Hardware Trojan Horses

Embedded Systems Security

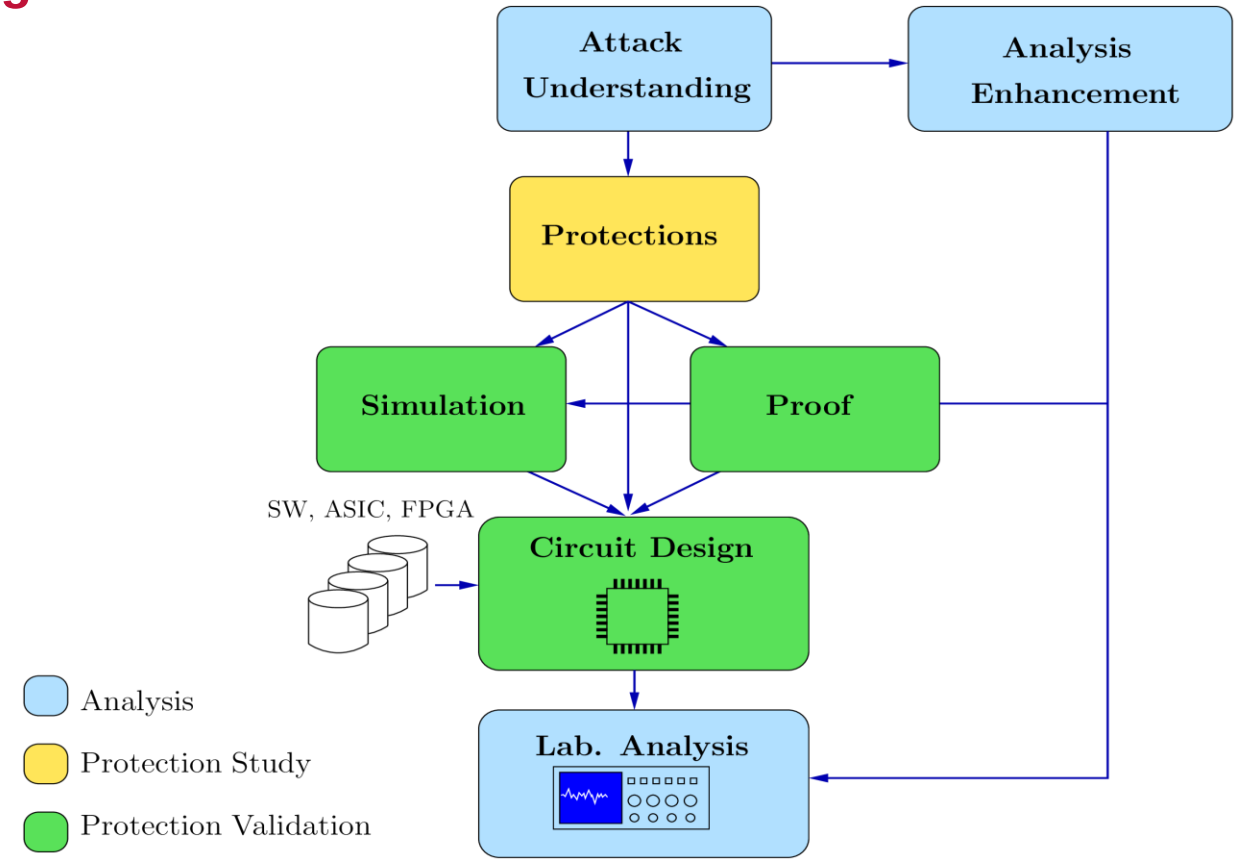


Challenges



Objectives: to use Hardware solutions or Low level software

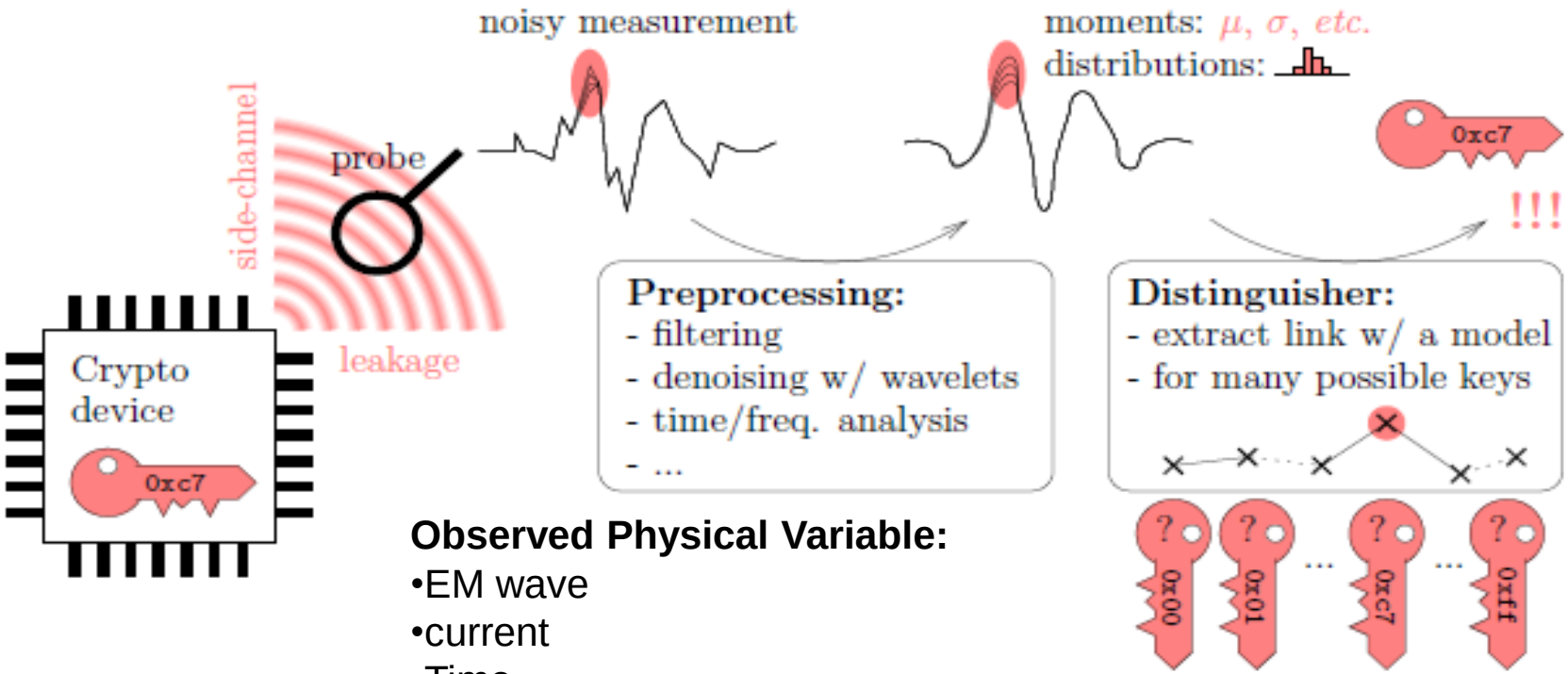
Big Picture


Attack Understanding
Analysis Enhancement
Protections
Simulation
Proof
SW, ASIC, FPGA
Circuit Design
Lab. Analysis
Analysis
Protection Study
Protection Validation

Outline

- Big Picture
- Attacks
- Hardware Protections
- Conclusion

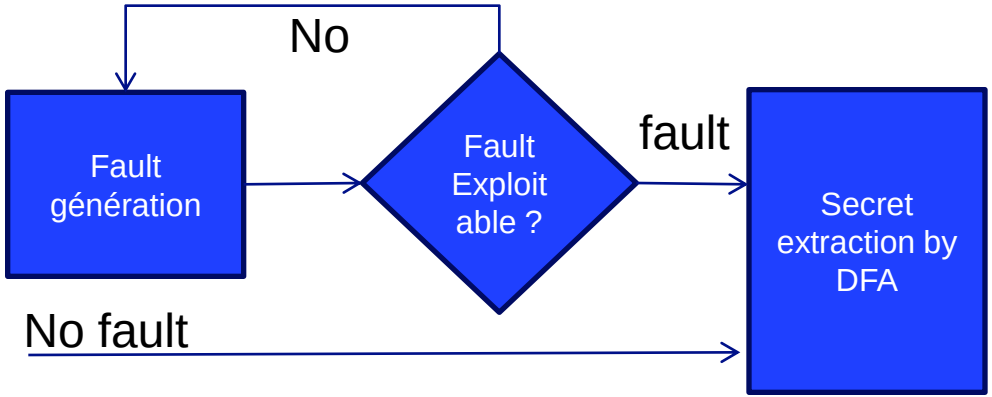
Side-Channel Analysis



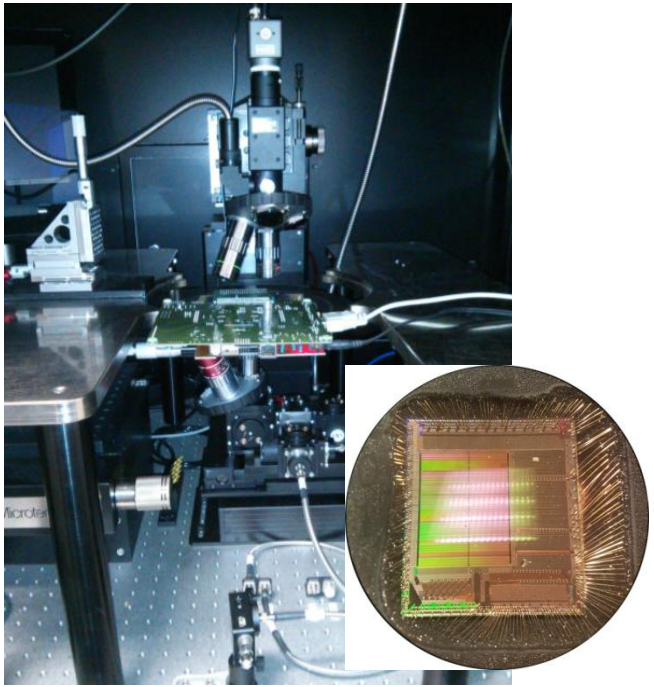
Observed Physical Variable:

- EM wave
- current
- Time

Fault Injection Attacks

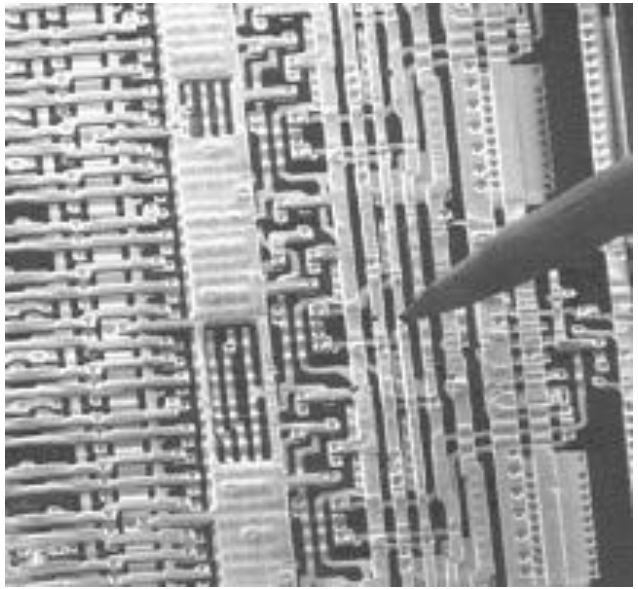


EM Injection

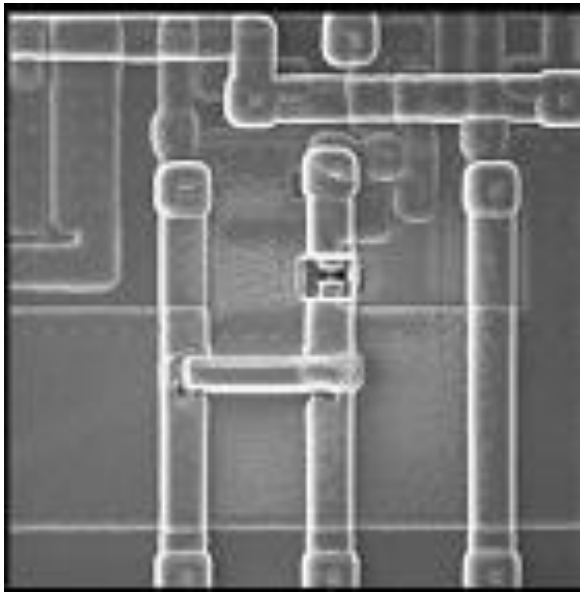


Laser Injection

Probing



Probing on PCB or circuit



FIB : Probing + modification

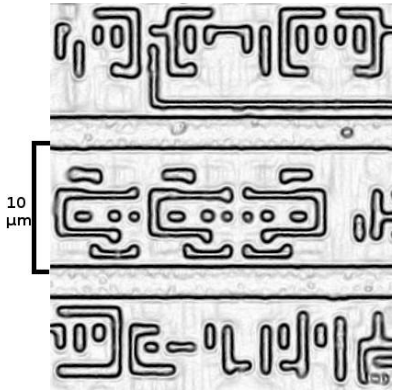
Highly invasive attack

Reverse Engineering

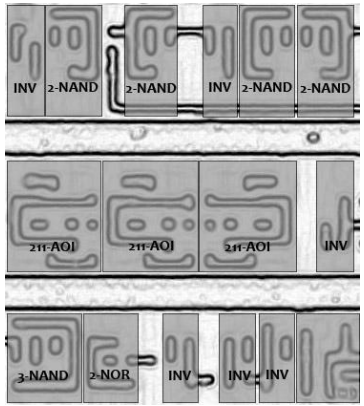
Delayering

Highly invasive attack

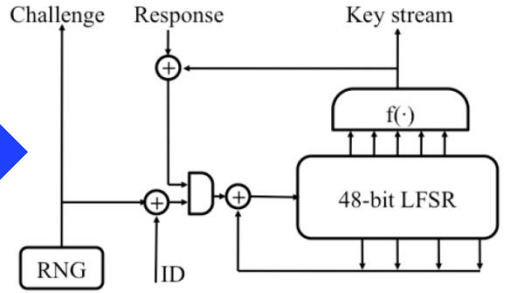
layout



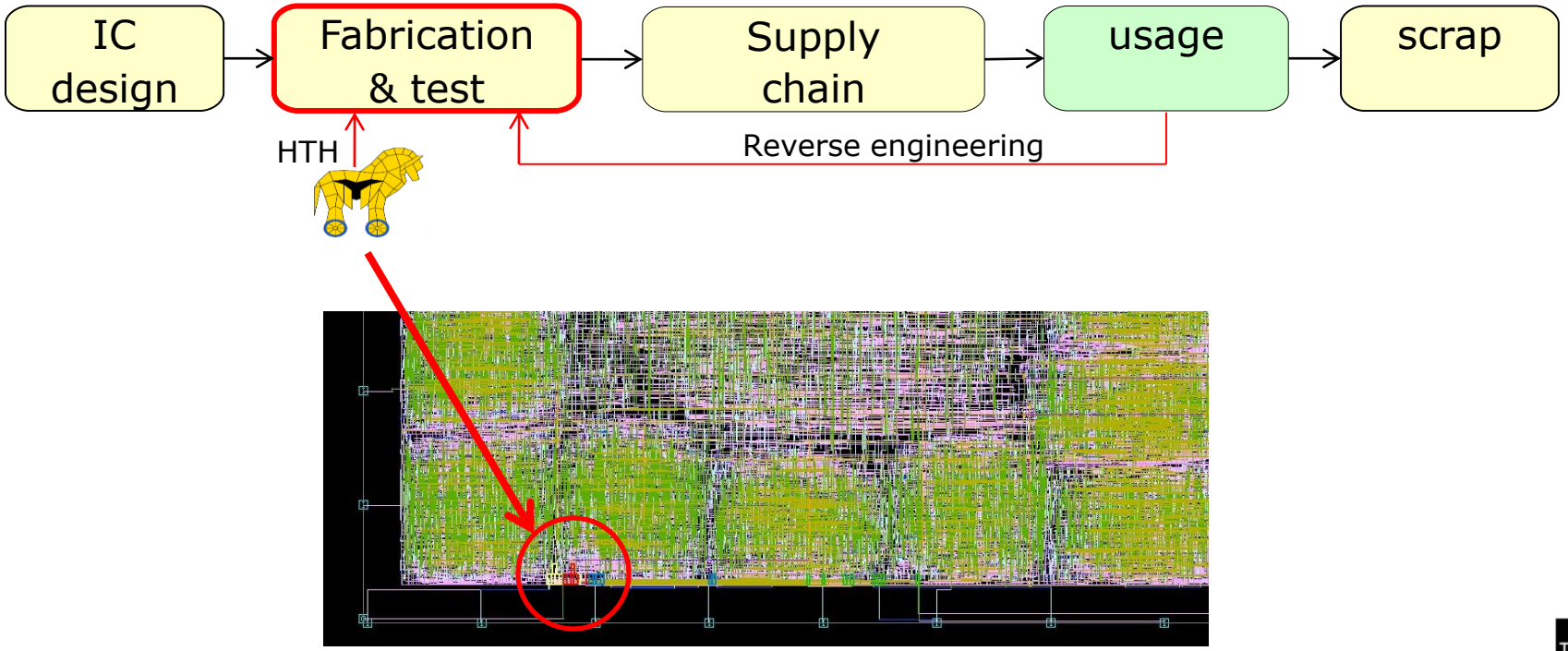
netlist



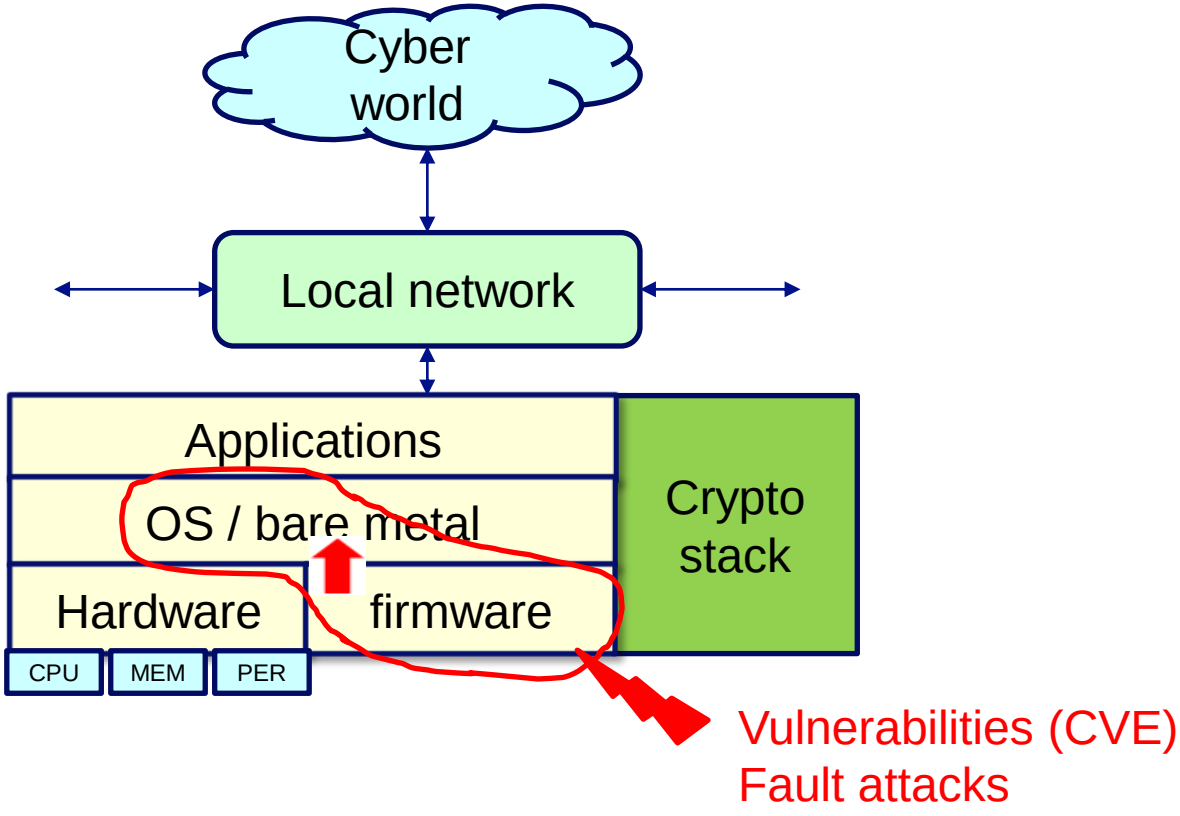
function



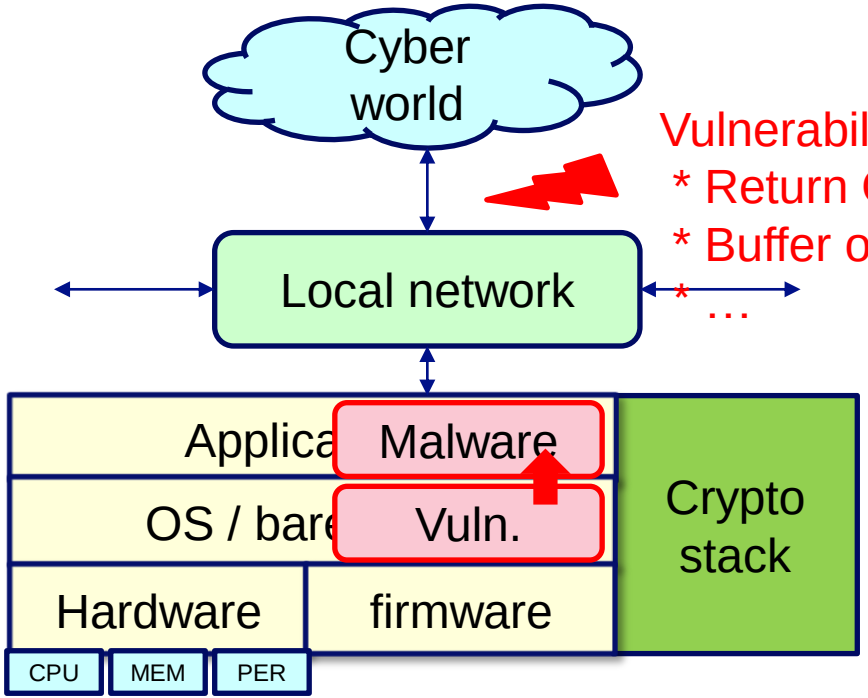
Hardware Trojan Horse



Secure Boot Attacks



Cyber Attacks



Vulnerabilites (CVE) =>
* Return Oriented Programming
* Buffer overflow
* …

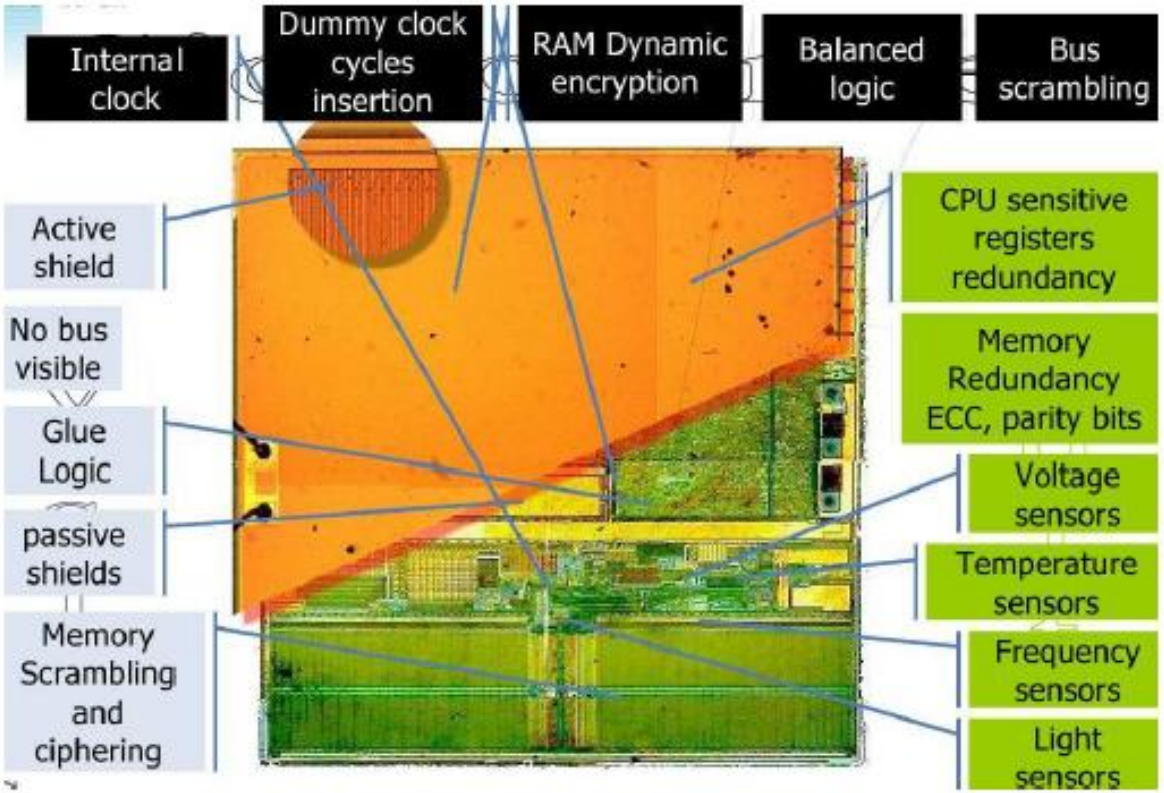
Outline

- Big Picture
- Attacks
- Hardware Protections
- Conclusion

Main Hardware Protections

- **Side-Channel Attacks**
  - Masking
  - Hiding (Obfuscation, DPL)
- **Fault Injection Attacks**
  - Sensors
  - Redundancy
- **Probing**
  - Secure bus
- **FIB**
  - Shielding
- **HTH**
  - Prevention, Detection
- **Secure Boot**
  - Strong authentication, PUF
- **Cyber Attacks**
  - Robust CPU

Smart Card Protections



Hardware Security primitives

- **Functionnal Blocks to be protected**
  - Cryptographic blocks
    - For confidentiality and integrity
  - TRNG
    - True Random Number Generator, for cryptographic keys
  - PUF
    - Physically Unclonable Functions, for authentication
  - CPUs
    - Against Cyber attacks (Control Flow Integrity CFI, Shadow stack, isolated execution)
- **Dedicated primitives for protections**
  - Fault Sensors
  - Shield
  - On–line checkers
    - entropy, security monitoring
  - Redundant structures
    - Coding, spatio-temporal duplication
  - Obfuscation structure
    - White Box implementation, noise generation

Outline

- Big Picture
- Attacks
- Hardware Protections
- Conclusion

Conclusion

- **Embedded Systems are very constrained devices**
  - Cost
  - Performances, real-time
- **And vulnerable to many attacks**
  - Connectivity => Cyber attacks
  - Physical access => Physical attacks
- **Compromise security / other constraints**
  - Necessity of low-cost yet secure primitives
- **Hardware protections allow to find good compromise**
  - Secure crypto-blocks, TRNG, PUF
  - Dedicated security primitives
  - Robust CPU against cyber attacks