Vulnerabilities in Test Infrastructures

Paolo PRINETTO

Director
CINI Cybersecurity
National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

License & Disclaimer

License Information

This presentation is licensed under the Creative Commons BY-NC License

To view a copy of the license, visit:

http://creativecommons.org/licenses/by-nc/3.0/legalcode

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Goal

- Presenting:
  - some of most significant vulnerabilities introduced by test infrastructures
  - some possible attacks exploiting them.

Prerequisites

- Lectures:
  - *CS_1.4 – Vulnerabilities*
  - *HS_1.1 – The role of Hardware in Security*
  - *HW_S_0.7.1 – Hardware Testing -- Basic concepts*

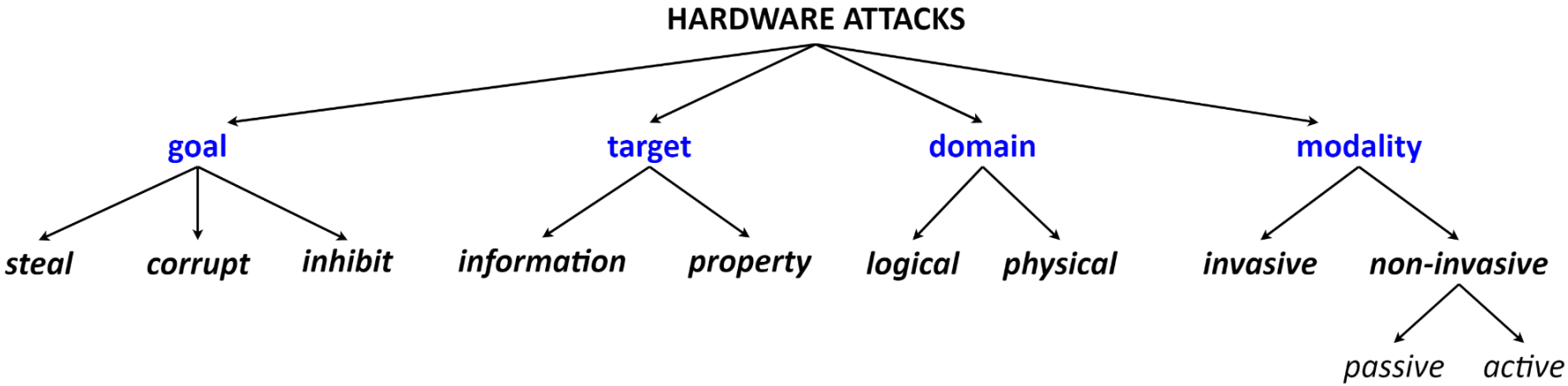
Outline

- Introduction
- Test Infrastructure based attacks
  - Scan chains
  - Standard IEEE 1149.1
- Fault attacks
  - ATPG

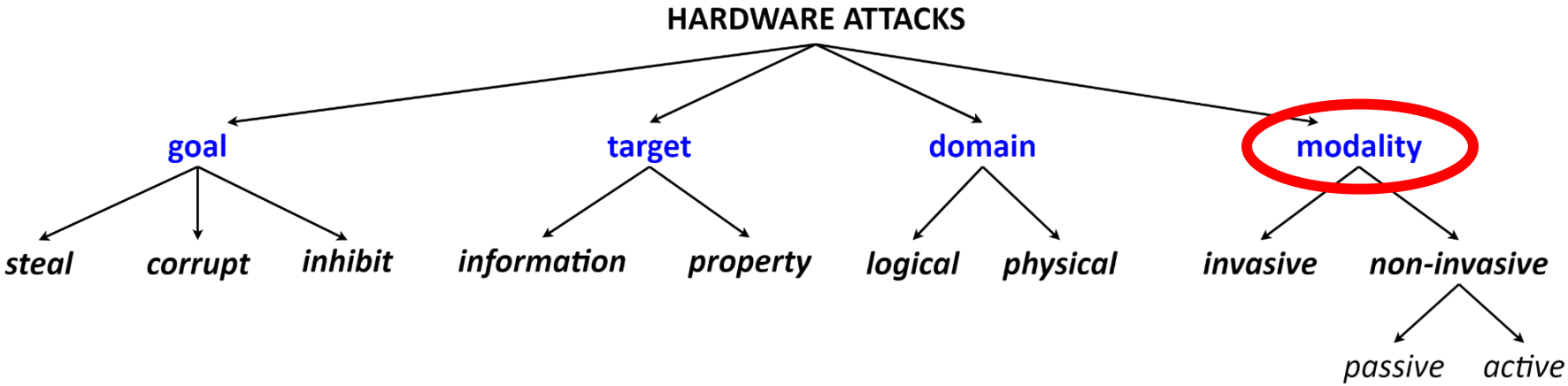
Outline

- Introduction
- Test Infrastructure based attacks
  - Scan chains
  - Standard IEEE 1149.1
- Fault attacks
  - ATPG

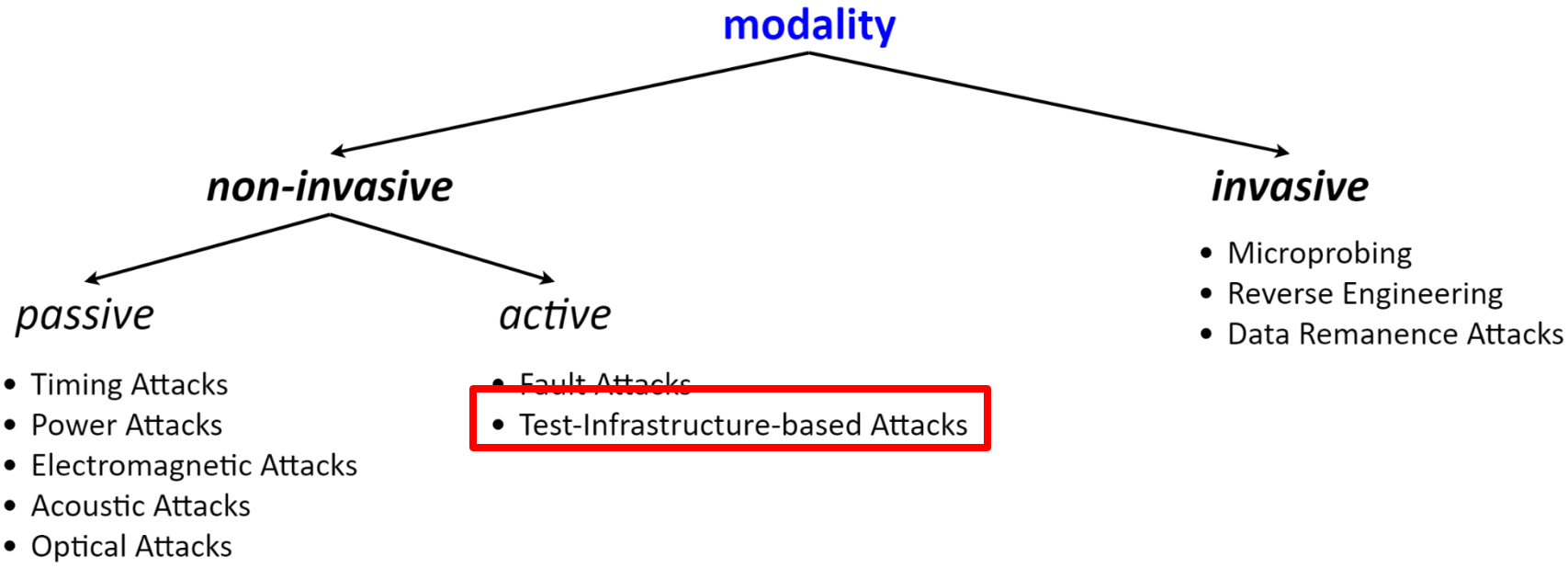
Hardware Attacks Taxonomy



Hardware Attacks Taxonomy



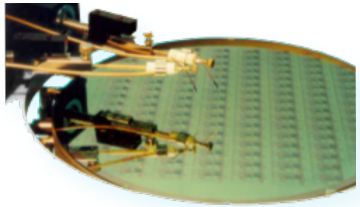
Hardware Attacks Modalities



Unprotected Test Infrastructures can Jeopardize the Security of the Entire System

Test vs Security

- Testing is mandatory to guarantee high quality of digital ICs
  - Increase controllability and observability



- On the contrary, security fears testability
  - Test infrastructures used for attacks

Do we need to test secure circuits?

- Of course, yes!
- In general, we have to guarantee high quality
- In particular, a defective secure device may jeopardize the overall security

Potential Avenues of Attack

- Among the plethora of test infrastructures, in the sequel we focus on
  - Scan chains
  - Standard IEEE 1149.1
  - JTAG infrastructures
  - ATPG

Outline

- Introduction
- Test Infrastructure based attacks
  - Scan chains
  - Standard IEEE 1149.1
- Fault attacks
  - ATPG

Issues

- In scan-based devices, the scan chains could provide a natural way to access the content of ALL the storage devices (flip-flops and registers) connected to a scan chain
- Thus, potentially scan chains can contain a secret (directly or indirectly):
  - Directly: the secret key itself
  - Indirectly: a value that is a function of the secret key (e.g., an intermediate value during the encryption process)

Scan-based attacks

- Goal: Retrieve embedded secret data
- HOW: Exploit observability and controllability offered by scan chains
- Principle: toggle the circuit between functional and scan modes

Red Teaming

- In some architectures, scan chains could:
  - Be hidden
  - Be accessible just via additional infrastructures, such as 1149.1 cells
  - Be managed via complex Scan compression Codec

https://www.youtube.com/watch?v=BTm9ExW5cLg

https://semiengineering.com/scan-compression-is-no-longer-about-compression/

Red Teaming – Vulnerability exploitations

1. Identify the target FFs that contain the secret to be stolen
2. Identify the scan chain SC to which the target FFs belong
3. Identify the precise time instant T in which the target FFs contain the secret.

Red Teaming – Vulnerability expl

1. Identify the target F
   stolen
2. Identify the scan cha
   belong
3. Identify the precise ti
   target FFs contain the

Red Teaming – Vulnerability exploitations

4. Run the circuit in *Normal mode* until the time T
5. Stop the circuit and switch it to *Test mode*
6. Scan out the content of the scan chain SC until the content of all the target FFs reach an output point you can observe

Red Teaming – Vulnerability expl

4. Run the circuit in *No*
5. Stop the circuit and
6. Scan out the content
   content of all the targ
   you can observe

Red Teaming – Vulnerability exploitations

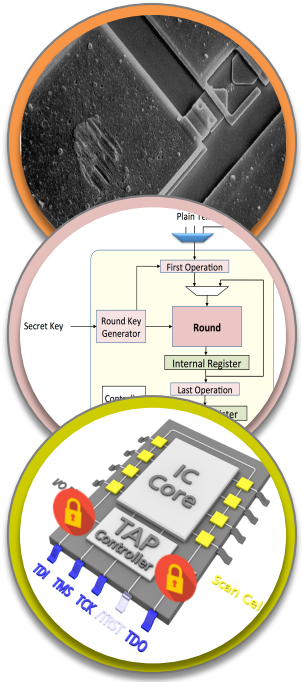
4. Run the circuit in *Normal mode* until the time T
5. Stop the circuit and switch it to *Test mode*
6. Scan out the content of the scan chain SC until the content of all the target FFs reach an output point you can observe
7. If Test decompressors and compressors are present, you have to previously reverse them.

Blue Teaming

- *Never let the scan chains freely accessible from the circuit pins !!*

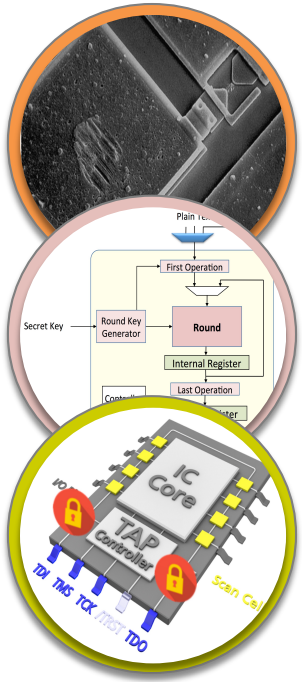
Blue Teaming

- Several countermeasures have been proposed, including:
  - Leave the scan chain unbound
  - Built-In Self-Test
  - Secure Test Access Mechanism
  - Scan Chain Encryption

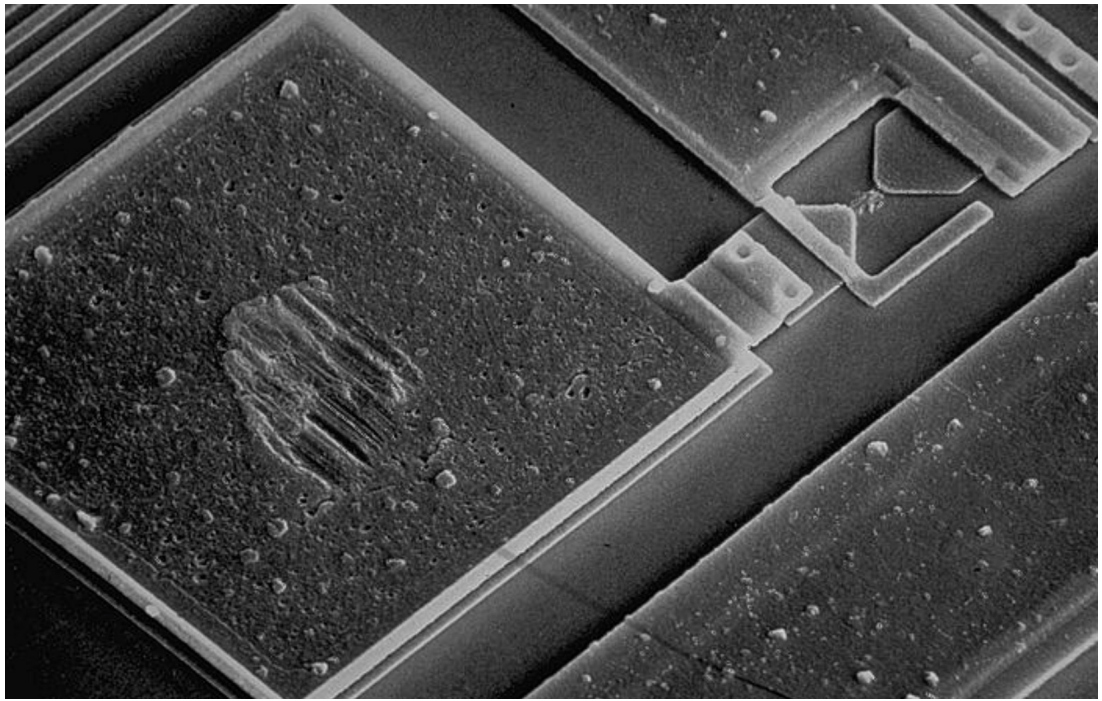


Blue Teaming

- Several countermeasures have been proposed, including:
  - Leave the scan chain unbound
  - Built-In Self-Test
  - Secure Test Access Mechanism
  - Scan Chain Encryption

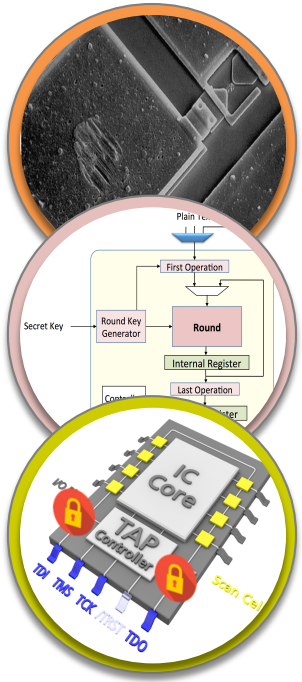


Fuses



Blue Teaming

- Several countermeasures have been proposed, including:
  - Leave the scan chain unbound
  - Built-In Self-Test
  - Secure Test Access Mechanism
  - Scan Chain Encryption



Built-In Self-Test (BIST)

- When possible, replace Scan Chains by BIST solutions.

Built-In Self-Test (BIST)

Pro's

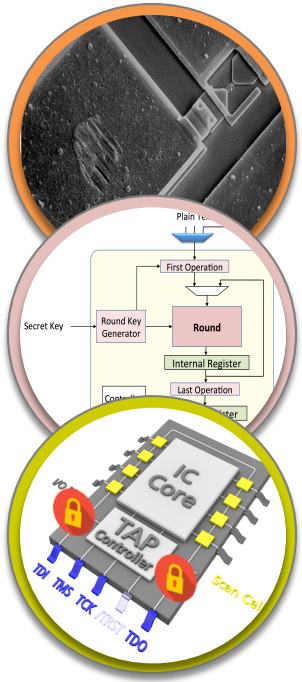
- Avoid scan-based testing
- Allow at-speed testing
- Reduced ATE costs

Con's

- Area overhead
- Fault coverage
- Diagnosis

Blue Teaming

- Several countermeasures have been proposed, including:
  - Leave the scan chain unbound
  - Built-In Self-Test
  - Secure Test Access Mechanism
  - Scan Chain Encryption

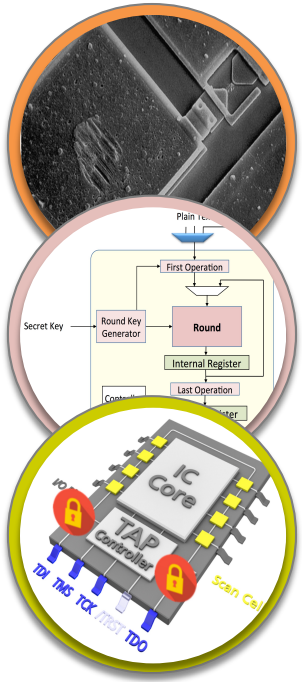


Secure Test Access Mechanism

- Drawbacks:
  - Authentication (expensive)
  - No in-field debug/diagnosis
  - Not easy to integrate in design flow

Blue Teaming

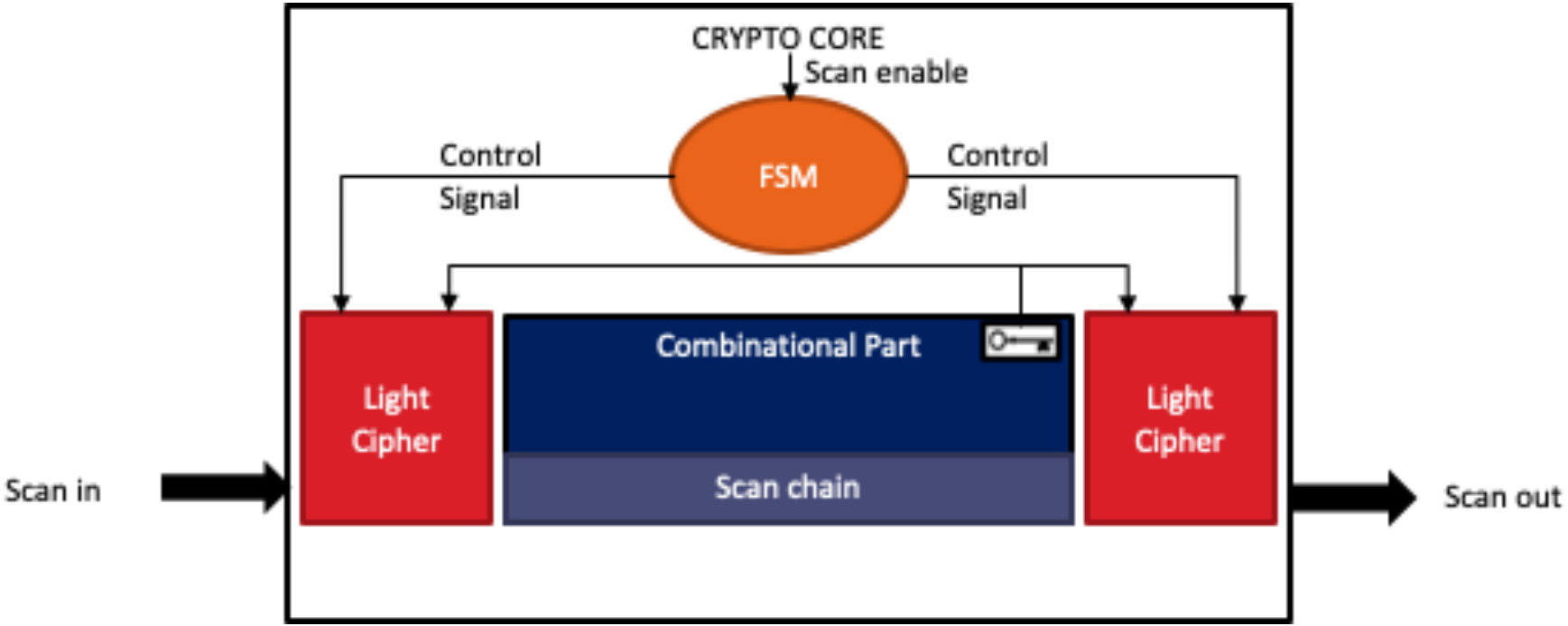
- Several countermeasures have been proposed, including:
  - Leave the scan chain unbound
  - Built-In Self-Test
  - Secure Test Access Mechanism
  - Scan Chain Encryption



Scan Chain Encryption

- Encrypting scan chain content with a secret key
- Controllability and the observability:
  - Untouched if the secret key is known
  - Impossible to control or observe otherwise
- Constraints:
  - To modify the test vector and response offline

Architecture of a Scan Chain Encryptor



Outline

- Introduction
- Test Infrastructure based attacks
  - Scan chains
  - Standard IEEE 1149.1
- Fault attacks
  - ATPG

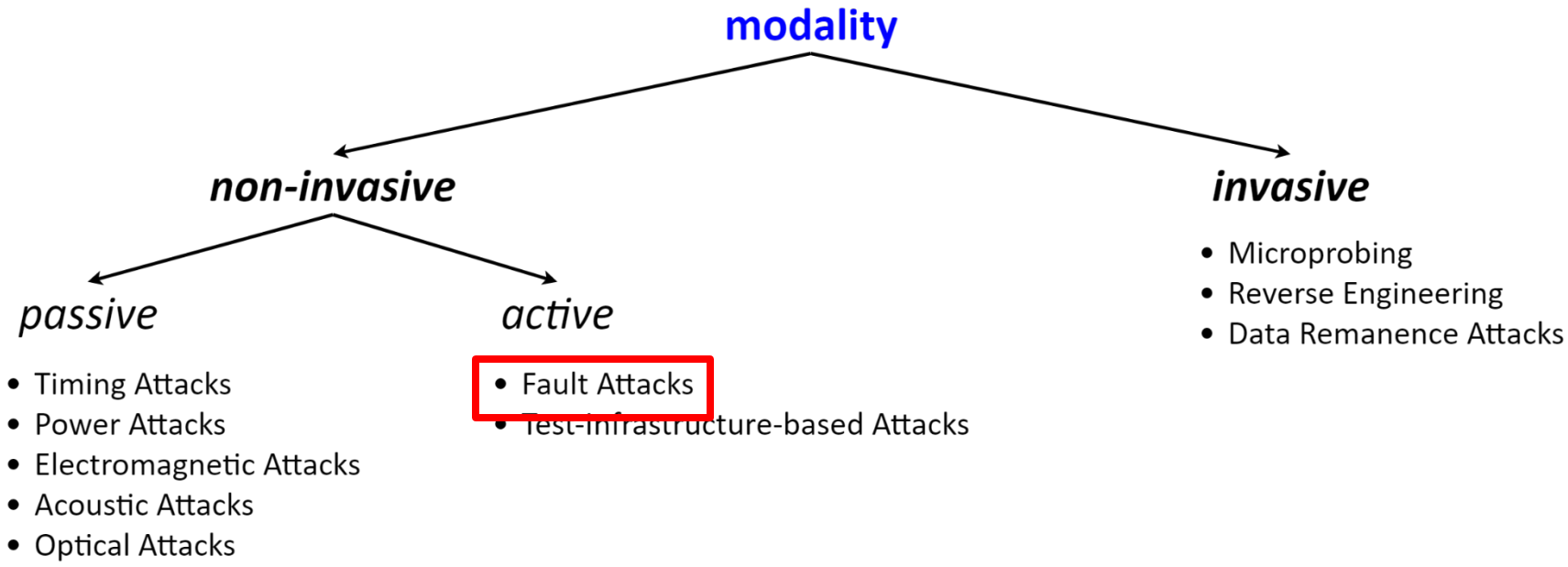
Red Teaming

- In 1149.1 compliant architectures, the Boundary Scan infrastructure may implement proprietary (or hidden) instruction(s) whose execution could enable you to access the internal scan chains.

Outline

- Introduction
- Test Infrastructure based attacks
  - Scan chains
  - Standard IEEE 1149.1
- Fault attacks
  - ATPG

Hardware Attacks Modalities



Conclusions on Testing

- Test of Secure devices is critical
- Test of Secure devices is possible (at higher costs)

- Nothing is perfect, solutions should be improved based on coming attacks!

Paolo PRINETTO

Director
CINI Cybersecurity
National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it