The Role of Hardware in Security

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

Disclaimer

Acknowledgments

- The presentation includes material from
  - Nicolò MAUNERO
  - Gianluca ROASCIO

whose valuable contribution is here acknowledged and highly appreciated.

Goal

- Understanding why hardware plays a key role in the protection of any system.
- Introducing a clear distinction between the 3 main roles of hardware when dealing with security, and namely:
  - *Hardware Security*
  - *Hardware-based Security*
  - *Hardware Trust.*

Prerequisites

- None

Outline

- The role of Hardware in Security
- Hardware Security
- Hardware-based Security
- Hardware Trust

Why *Hardware* & *Security*?

- As with software, data and communication infrastructures, the hardware must be
  - *Designed*
  - *Built*
  - *Tested*
  - *Used*
  - *Maintained*
  - *dismissed*

considering possible cyber attacks and their consequences.

Motivations

- Hardware runs software and is, in fact, *the last line of defense*

Motivations

- Hardware runs software and is, in fact, *the last line of defense*

Consequences (1)

- If the hardware is corrupted, all the mechanisms introduced to make the software secure (at any level) may become useless

Important side effect

Consequences (2)

- Hardware runs software and is, in fact, *the last line of defence*
- A *trusted* and *secure* Hardware can effectively be used to protect other system components (e.g., software, data communication infrastructures)

What are we talking about

What are we talking about

- A multi-faceted reality

What are we talking about

- A multi-faceted reality

Belarusian National Library

Нацыянальная бібліятэка Беларусі

Национальная библиотека Беларуси

What are we talking about

- A multi-faceted reality

- A complex puzzle

Hardware & Security: a complex puzzle

- Hardware Vulnerabilities
- Hardware Attacks
- Hardware Trust
- Hardware Counterfeiting
- Hardware-based Defenses
- Security-oriented Architectures
- Built-in security features
- PUFs (Physically Unclonable Functions)
- …

For each tile, many dimensions

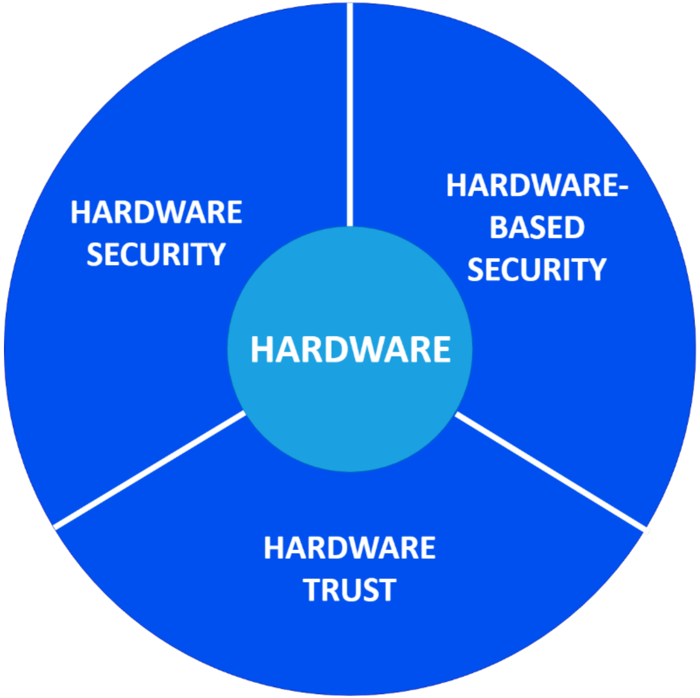
- *Technology*
- *Target abstraction level*
- *Types of components*
- *Application domain*
- *System complexity*
- *System criticality*
- …

The role of Hardware in Cybersecurity

- Trying to move from a *mess* to a more *rigorous view*, the role of Hardware in security can be seen as follows:

The role of Hardware in Cybersecurity

- Trying to move from a *mess* to a more *rigorous view*, the role of Hardware in security can be seen as follows:



Outline

- The role of Hardware in Security
- Hardware Security
- Hardware-based Security
- Hardware Trust

Hardware Security: What

- Refers to all those aspects of security (i.e., weaknesses, vulnerabilities, countermeasures) that concern *hardware components*, regardless their actual implementations, the exploited design tools, and the target abstraction level.

Hardware Security: What

- “*Everything*” related to:
  - *hardware vulnerabilities*:
    - Their analysis, identification, detection, prevention, remediation, patching, …
    - prevention of their exploitation
  - *hardware attacks*:
    - Any technique and solution aimed at preventing, mitigating, defeating, making them ineffective, regardless the tools and the abstraction levels (e.g., software or any upper level) used to carry them out
  - *protection solutions*:
    - aimed at preventing hardware vulnerabilities and hardware attacks.

Hardware Security: What

HARDWARE SECURITY

HARD

- “*Everything*” related to:
  - *hardware vulnerabilities*:
    - Their analysis, identification, detection, prevention, remediation, patching
    - prevention of their expl
  - *hardware attacks*:
    - Any technique and solution aimed at preventing, mitigating, defeating, making them ineffective, reg or any upper level) used
  - *protection solutions*:
    - aimed at preventing hardware vulnerabilities and hardware attacks.

See lecture:

- *CS_1.4 - Vulnerabilities*

See lecture:

- *HS_1.3 - Hardware Attacks*

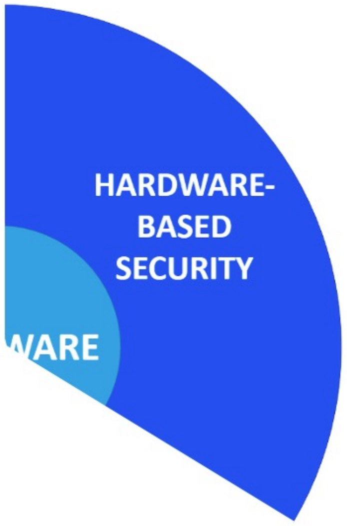
Hardware Security: When

- Hardware Security issues must be faced:
  - During the design and production phases (*Security-by-design*)
  - When hardware is already operating in the field.

Outline

- The role of Hardware in Security
- Hardware Security
- Hardware-based Security
- Hardware Trust

Hardware-based Security



- Refers to all those solutions aimed at resorting to hardware devices to protect the system from attacks that exploit vulnerabilities of *other* components of the system itself.

Remark

- To offer security features to upper layers, hardware itself must be secure at first
- From this point of view, *Hardware Security* play the role of a key *enabler* for *Hardware-based Security.*

Hardware-based Security Role

- *”Although hardware-based security is not a silver bullet, it does provide a “chain of trust” rooted in silicon that makes the device and extended network more trustworthy and secure.”*

[https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/intel-security-essentials-solution-brief.pdf]

Hardware-based Implementations

- Hardware-based Implementations can be clustered as:
  - *System level solutions*
  - *Architectural level solutions*
  - *Security-oriented components*
  - *Proprietary Solutions*
  - *Open Security Platforms*
  - *Built-in Security Features*

Hardware-based Implementations

- Hardware-based Implementations can be clustered as:
  - *System level solutions*
  - *Architectural level solutions*
  - *Security-oriented components*
  - *Proprietary Solutions*
  - *Open Security Platforms*
  - *Built-in Security Features*

System level solutions

- Two significant standards:
  - *Trusted Platform Module*
  - *Trusted Execution Environments*

System level solutions

- Two significant standards:
  - *Trusted Platform Module*
  - *Trusted Execution Environments*

Trusted Platform Module – TPM

- Standard guideline for developing chips with strong cybersecurity features
- Trustworthiness of TPM is based on different *Root of Trust* components and well-defined interactions among them

Root of Trust

- Component that needs to always behave in the expected manner because its misbehaviour cannot be detected

Root of Trust

- Trust in the *Roots of Trust* can be achieved through a variety of means including technical evaluation by competent experts.

Root of Trust - Role

- Is used as basic block for the construction of a *Chain of Trust*

TPM History

- Specification initially released by the *Trusted Computing Group* in 2003

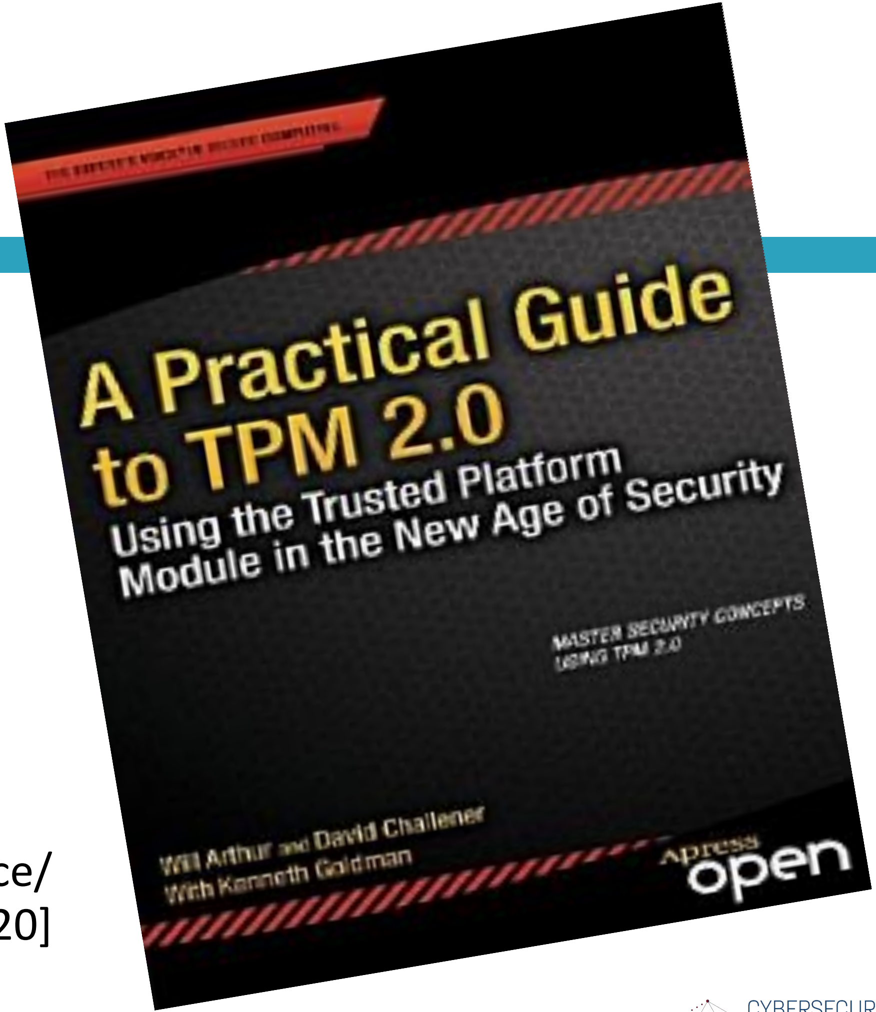
[https://trustedcomputinggroup.org/]

- The current version is TPM 2.0, which is standardized under ISO/IEC 11889

[https://www.iso.org/standard/66510.html]

[https://ebrary.net/24701/computer_science/a_practical_guide_to_tpm_20]

TPM 2.0



[https://ebrary.net/24701/computer_science/a_practical_guide_to_tpm_20]

System level solutions

- Two significant standards:
  - *Trusted Platform Module*
  - *Trusted Execution Environments*

Trusted Execution Environment

- TEE is a concept that provides a secure area of the main processor

  “to provide end-to-end security by protecting the execution of authenticated code, confidentiality, authenticity, privacy, system integrity and data access rights”

[Global Platform Device Committee, “EE protection profile,” version 1.2, Public Release, November 2014, Document Reference: GPD_SPE_021 https://csrc.nist.gov/publications/detail/fips/140/2/final]

Trusted Execution Environments

- TEEs are secure area of a System-on-Chip that guarantee code and data protection
- They typically offer the minimal security required by low-end, closed embedded systems, such as IoT and “bare-metal” (i.e., without any Operating System) solutions.

Hardware-based Implementations

- Hardware-based Implementations can be clustered as:
  - *System level solutions*
  - *Architectural level solutions*
  - *Security-oriented components*
  - *Proprietary Solutions*
  - *Open Security Platforms*
  - *Built-in Security Features*

Architectural level solutions

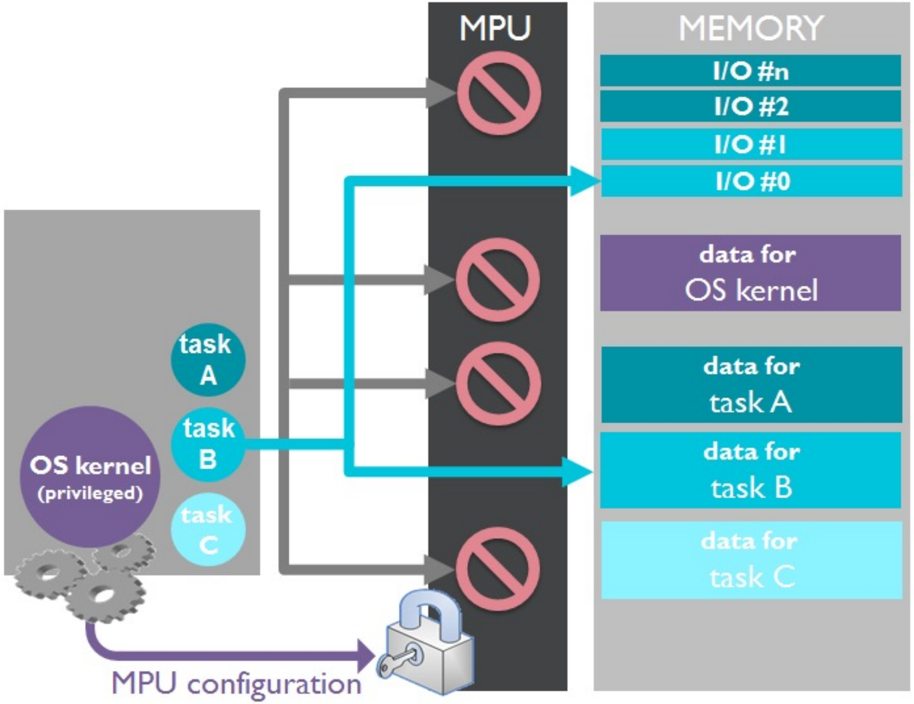
- General purpose *Design-for-Security* solutions adopted at the architectural level, mainly to improve the security of the CPUs and of the involved memories.

Architectural level solutions

- Examples include, among the others:
  - *Memory Protection Units*
  - *Shadow Stacks*
  - *Custom proprietary solutions*
  - …

Memory Protection Unit - MPU

- Present in a wider and wider number of processors
- Each memory page can be read, written or executed just by a predefined set of tasks/processes
- Access rights are decided by the kernel, which runs privileged
- Addresses sent to the memory are automatically processed by the MPU without the intervention of the kernel
- Violations cause the immediate abortion of the task



Hardware-based Implementations

- Hardware-based Implementations can be clustered as:
  - *System level solutions*
  - *Architectural level solutions*
  - *Security-oriented components*
  - *Proprietary Solutions*
  - *Open Security Platforms*
  - *Built-in Security Features*

Security-oriented components

- Set of custom, special-purpose components used for performing specific security-oriented operations, including:
  - *Hardware Cyphers*
  - *Smart Cards & SIM Cards*
  - *Secure storage devices*
  - *Random Number Generators*

Hardware-based Implementations

- Hardware-based Implementations can be clustered as:
  - *System level solutions*
  - *Architectural level solutions*
  - *Security-oriented components*
  - *Proprietary Solutions*
  - *Open Security Platforms*
  - *Built-in Security Features*

Proprietary Solutions

- *Intel® vPro® Platform*
- *AMD Secure Technology™*
- *ARM® TrustZone®*
- *Microsoft BitLocker*
- *Synopsys DesignWare® tRoot™*
- *Apple Secure Enclave Processor*
- *Google Titan*
- *Cisco® Trust Anchor*
- …

Hardware-based Implementations

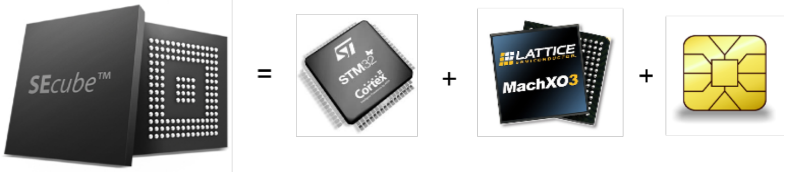
- Hardware-based Implementations can be clustered as:
  - *System level solutions*
  - *Architectural level solutions*
  - *Security-oriented components*
  - *Proprietary Solutions*
  - *Open Security Platforms*
  - *Built-in Security Features*

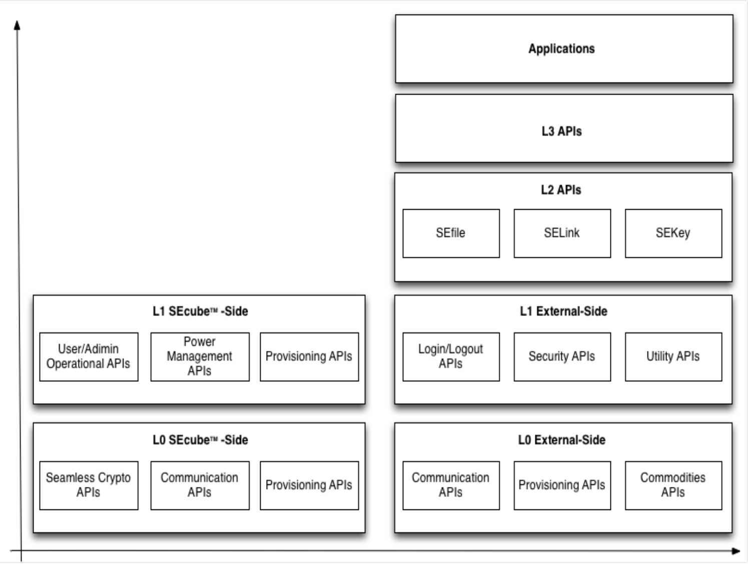
Open Security Platforms

- Platforms designed with cybersecurity in mind and packed with strong cybersecurity features:
  - Hardware accelerators for cryptography
  - Anti tamper
  - Secure boot process
- They include:
  - SE*cube*™
  - USB Armory

Hardware Platform – SE*cube*™

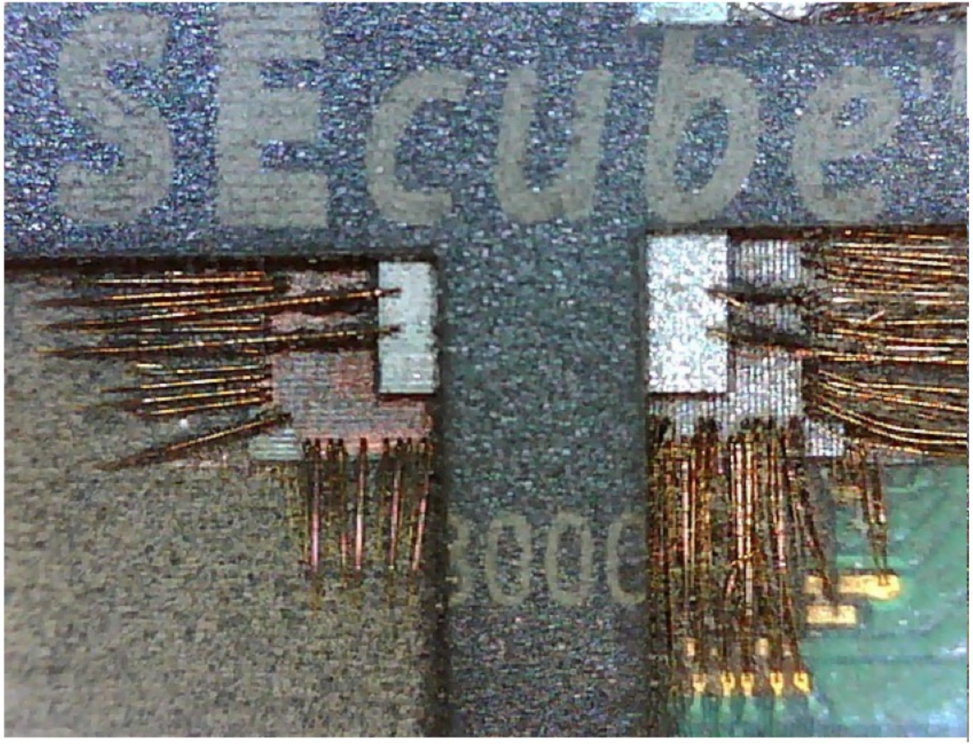
- System-In-Package developed by Blu5™ Group
  - Cortex-M4 microcontroller
  - Flexible and fast FPGA
  - SmartCard certified EAL 5+
- Strong Cybersecurity features and capabilities





[https://www.secube.eu/]

3D SiP – An Example: SEcube™



Hardware-based Implementations

- Hardware-based Implementations can be clustered as:
  - *System level solutions*
  - *Architectural level solutions*
  - *Security-oriented components*
  - *Proprietary Solutions*
  - *Open Security Platforms*
  - *Built-in Security Features*

Built-in Security Features

- Functionalities present in most of modern microcontrollers
- Mostly introduced for safety
- A proper exploitation could significantly increase the system protection against the common threats in the embedded system landscape

Outline

- The role of Hardware in Security
- Hardware Security
- Hardware-based Security
- Hardware Trust

Trust

- “A trusted component, operation, or process is one whose behavior is predictable under almost any operating condition, and which is highly resistant to subversion by application software, virus, and a given level or physical interference.”

[ISO/IEC 24000]

Hardware Trust : Role

- Hardware trust mainly concerns *Hardware Authenticity*

Hardware Trust : What

- "*Everything*" related to:
  - *hardware counterfeiting*:
    - Counterfeiting types
    - Counterfeiters
    - Counterfeiting detection approaches
    - Counterfeiting consequences
  - *protection from counterfeiting*:
    - Any technique and solution aimed at preventing counterfeiting in all the stages of the product lifecycle.

Hardware Trust : What

HARDWARE TRUST

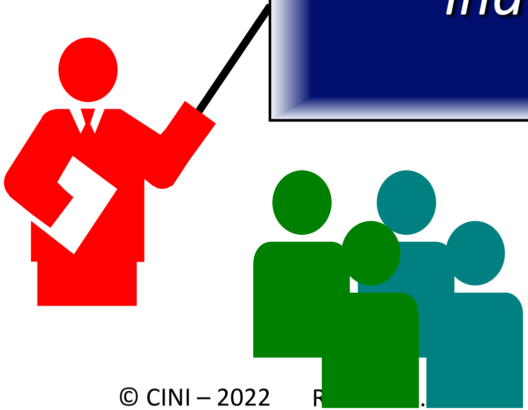
- *"Everything"* related to:
  - *hardware counterfeiting*:
    - Counterfeiting types
    - Counterfeiters
    - Counterfeiting detection app
    - Counterfeiting consequences
  - *protection from counterfeiting*:
    - Any techniqu
      the stages of the p

See lecture:
HS_1.5 - Hardware Counterfeiting

See lecture:
HS_1.6 - Physically Unclonable Functions - PUFs

Alarm

Counterfeiting of integrated circuits has become a major challenge in almost ALL industrial sectors !!



Counterfeiting

Causes

- The complexity of electronic systems significantly increased over the past few decades
- To reduce production cost, they are mostly fabricated and assembled globally

Counterfeiting

Causes

- The complexity of electronic systems significantly increased over the past few decades
- To reduce production cost, they are mostly fabricated and assembled globally

Consequences

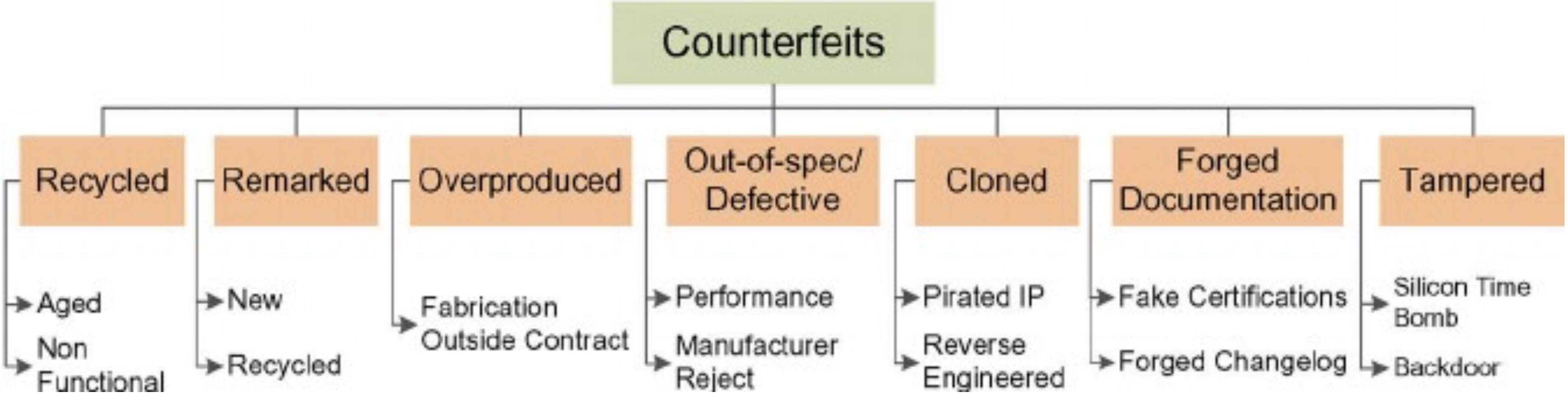
- This globalization has led to an illicit market willing to undercut the competition with counterfeit and fake parts

Counterfeiting

Lacks

- Deficiencies in the existing test solutions
- Lack of low-cost and effective avoidance mechanisms in place

Counterfeiting types



[Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris: "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", in Proceedings of the IEEE · August 2014 - DOI: 10.1109/JPROC.2014.2332291]

Problems of Recycled ICs

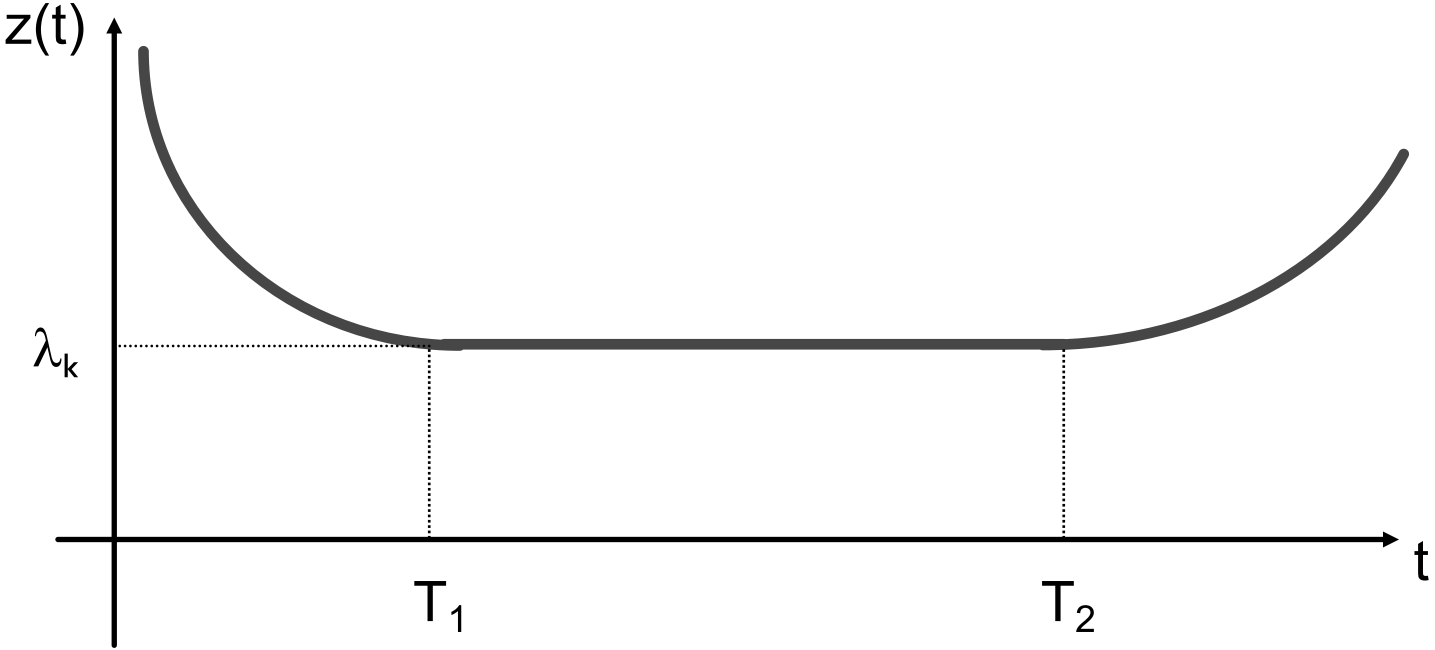
- Financial damage
- Safety
- Security

Problems of Recycled ICs

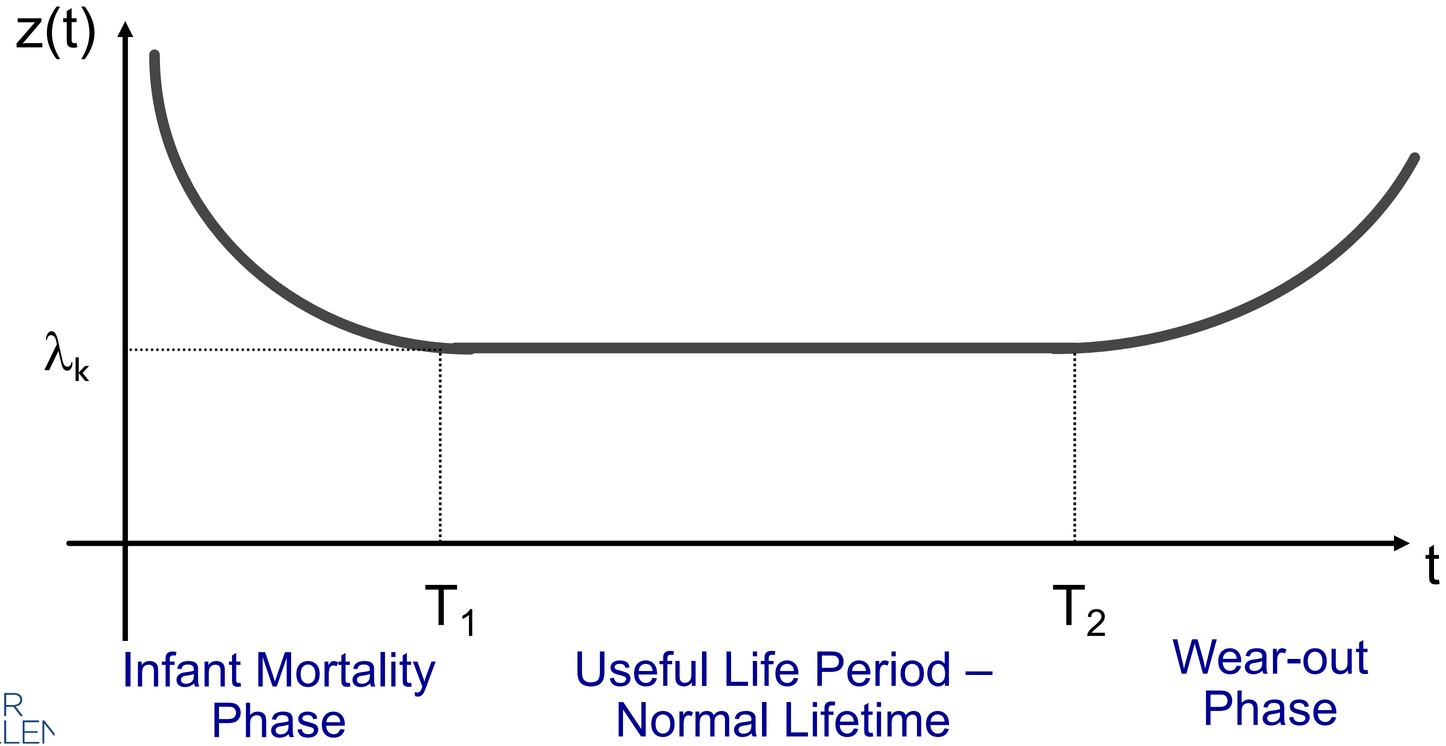
Safety

- Aging Phenomena (shorter lifetime)

Failure Rate Function
(Bathtub curve relationship)



Failure Rate Function
(Bathtub curve relationship)



Problems of Recycled ICs

Safety

- Aging Phenomena (shorter lifetime)
- Potential damage, due to the reclaiming process (removal under very high temperature, aggressive physical removal from boards, washing, sanding, repackaging, etc.)
- Lower performances

Problems of Recycled ICs

Safety

- Aging Phenomena (shorter lifetime)
- Potential damage, due to the reclaiming process (removal under very high temperature, aggressive physical removal from boards, washing, sanding, repackaging, etc.)
- Lower performances

Security

- Unpatched vulnerabilities

Paolo PRINETTO

Director
CINI Cybersecurity
National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it