Il ruolo dell’Hardware

Indice

- Il ruolo dell'Hardware nella Sicurezza
- Hardware Security
- Hardware-based Security
- Hardware Trust

Indice

- Il ruolo dell'Hardware nella Sicurezza
- Hardware Security
- Hardware-based Security
- Hardware Trust

Perché *Hardware* & Sicurezza ?

- Così come avviene per il software, per i dati e per le infrastrutture di comunicazione, anche l'hardware deve essere *progettato*, *costruito*, *testato*, *utilizzato*, *supportato* e *dismesso* tenendo conto:
  - dei possibili attacchi informatici
  - delle loro conseguenze.

Motivazioni

- L’hardware permette l’esecuzione del software, ed è di fatto *l’ultima linea di difesa*

Motivazioni

- L’hardware permette l’esecuzione del software, ed è di fatto *l’ultima linea di difesa*

Conseguenze (1)

- Se l'hardware è compromesso, tutti i meccanismi introdotti per rendere sicuro il software (a qualsiasi livello) possono rivelarsi inutili

Effetto collaterale importante

- L’hardware permette l’esecuzione del software, ed è di fatto *l’ultima linea di difesa*

Conseguenze (2)

- Un hardware *fidato* e *sicuro* può essere utilizzato efficacemente per proteggere altri componenti del sistema (ad es., software, dati, comunicazioni)

Di che cosa stiamo parlando

- Di una realtà a più facce

Di che cosa stiamo parlando

- Di una realtà a più facce

- Di un puzzle complesso

Hardware & Sicurezza: un puzzle complesso

- Vulnerabilità Hardware
- Attacchi Hardware
- Hardware Trust
- Contraffazione dell'Hardware
- Difese basate sull'Hardware
- Architetture orientate alla Sicurezza
- Caratteristiche di Sicurezza *built-in*
- Physically Unclonable Functions (PUF)
- …

Per ciascun pezzo del puzzle, una varietà di dimensioni

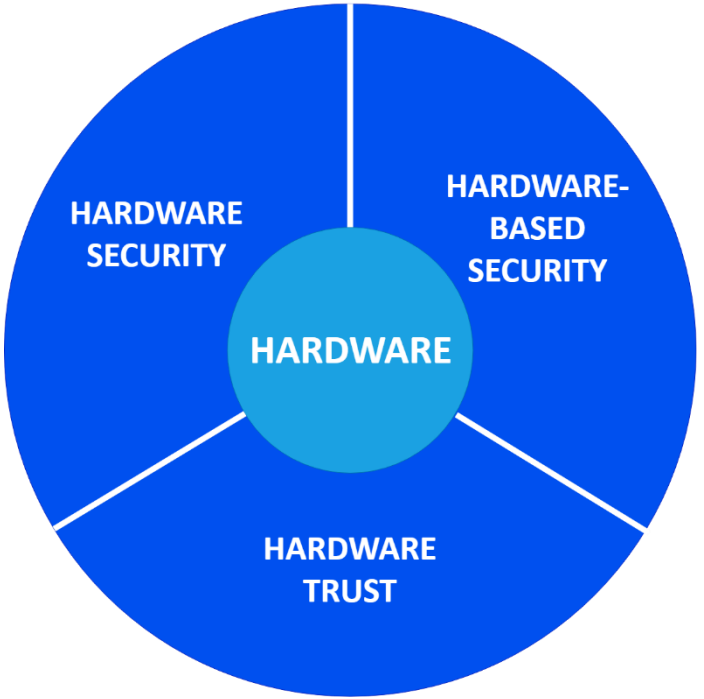
- *Tecnologia*
- *Livello di astrazione del target*
- *Tipologia dei componenti*
- *Dominio d'applicazione*
- *Complessità del sistema*
- *Criticità del sistema*
- *…*

Il ruolo dell'Hardware nella Sicurezza

- Passando a una visione più rigorosa, il ruolo dell'Hardware nella Sicurezza può essere visto come segue:

Il ruolo dell'Hardware nella Sicurezza

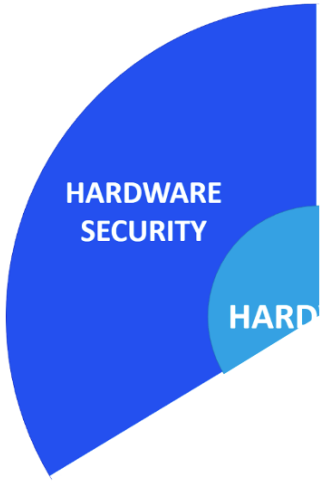
- Passando a una visione più rigorosa, il ruolo dell'Hardware nella Sicurezza può essere visto come segue:



Indice

- Il ruolo dell'Hardware nella Sicurezza
- Hardware Security
- Hardware-based Security
- Hardware Trust

Hardware Security: Cosa



- Tutto ciò che riguarda:
  - *vulnerabilità hardware:*
    - La loro analisi, identificazione, rilevamento, prevenzione, correzione, patch, ...
    - prevenzione del loro sfruttamento
  - *attacchi hardware:*
    - Qualsiasi tecnica e soluzione volta a prevenire, mitigare, sconfiggere, rendere inefficaci, indipendentemente dagli strumenti e dai livelli di astrazione (ad esempio, software o qualsiasi livello superiore) utilizzati per eseguirli
  - *soluzioni di protezione:*
    - volte a prevenire vulnerabilità hardware e attacchi hardware.

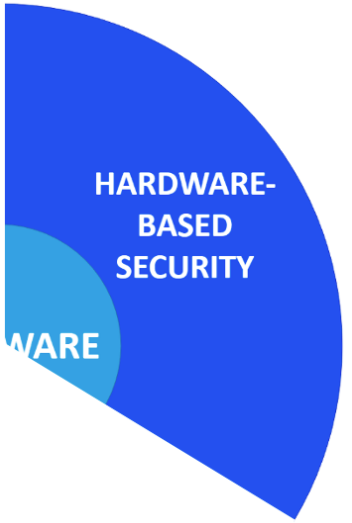
Hardware Security: Quando

- I problemi di sicurezza dell'hardware possono essere affrontati:
  - Durante le fasi di progettazione e produzione (*Security-by-design*)
  - Quando l'hardware è già in funzione sul campo.

Indice

- Il ruolo dell'Hardware nella Sicurezza
- Hardware Security
- Hardware-based Security
- Hardware Trust

Hardware-based Security



- Si riferisce a tutte quelle soluzioni che mirano a ricorrere a dispositivi hardware per proteggere il sistema da attacchi che sfruttano vulnerabilità presenti in *altre* componenti del sistema stesso.

Nota

- Al fine di offrire funzioni di sicurezza ai livelli di astrazione superiori, l’hardware deve essere “garantito” sicuro
- Da questo punto di vista, la sicurezza hardware svolge il ruolo di *abilitatore chiave* per la sicurezza basata sull'hardware.

Hardware-based Security: Ruolo

- *” Sebbene l’*Hardware-based Security *non sia la panacea, esso fornisce una “chain of trust” basata sul silicio e a esso “ancorata”, in grado di rendere più affidabili e sicuri i dispositivi e le reti.”*

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

Hardware-based Security: Implementazioni

- Le principali soluzioni di Hardware-based security possono essere raggruppate in:
  - *Soluzioni a livello di Sistema*
  - *Soluzioni a livello Architetturale*
  - *Security-oriented components*
  - *Soluzioni Proprietarie*
  - *Open Security Platforms*
  - *Built-in Security Features*

Soluzioni Proprietarie

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

Indice

- Il ruolo dell'Hardware nella Sicurezza
- Hardware Security
- Hardware-based Security
- Hardware Trust

Autenticità e Fiducia (Trust)

- *“Ci si può fidare di un'entità se questa si comporta sempre nel modo previsto per lo scopo previsto.”*

[D. Grawrock, Dynamics of a Trusted Platform: A building block approach. Intel Press, 2008]

Hardware Trust : Cosa

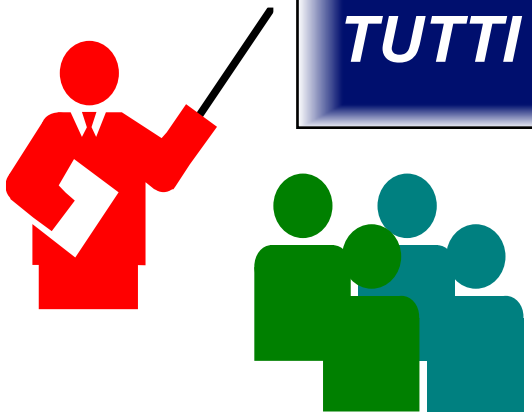
- “*Qualsiasi cosa*” relativa a:
  - *Contraffazione dell’hardware* :
    - Tipi di contraffazione
    - Contraffattori
    - Approcci al rilevamento delle contraffazioni
    - Conseguenze della contraffazione
  - *protezione dalla contraffazione* :
    - Qualsiasi tecnica o soluzione volta a prevenire la contraffazione in tutte le fasi del ciclo di vita del prodotto.

Hardware Trust: Ruolo

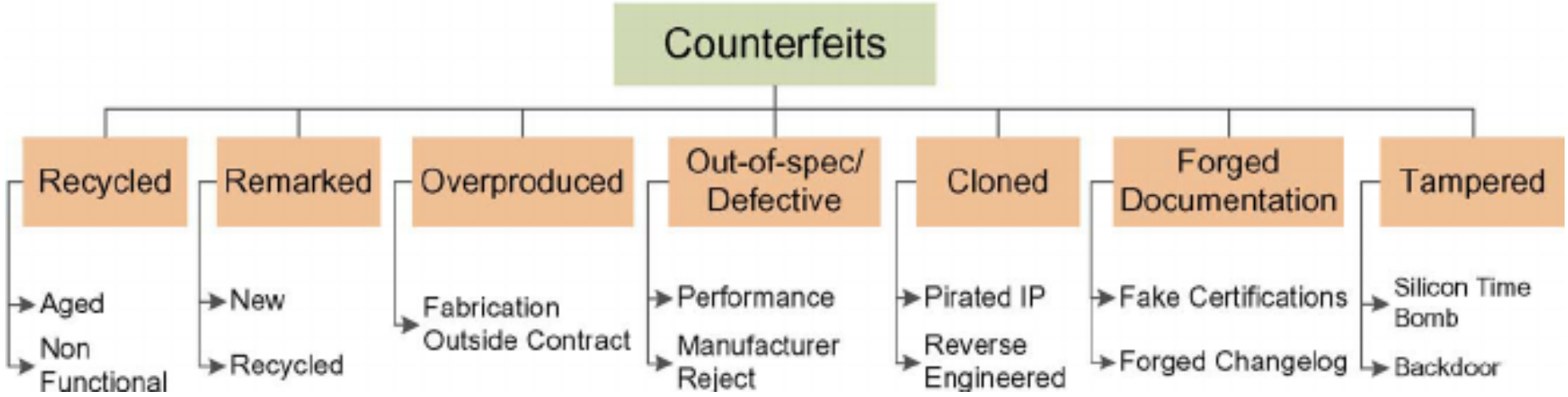
- Hardware trust
  riguarda principalmente
  Autenticità.
- Le component Hardware di un Sistema Informativo devono provenire da entità che siano in grado di dimostrarne, al di là di ogni ragionevole dubbio, la originalità e genuinità.

Allarme

La contraffazione di circuiti integrati è diventata un grande problematica in quasi TUTTI i settori industriali !!



Tipi di Contraffazione



[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]

Contraffazione

Cause

- La complessità dei sistemi elettronici è aumentata in modo significativo negli ultimi decenni
- Per ridurre i costi di produzione, essi sono principalmente fabbricati e assemblati a livello planetario

Contraffazione

Cause

- La complessità dei sistemi elettronici è aumentata in modo significativo negli ultimi decenni
- Per ridurre i costi di produzione, essi sono principalmente fabbricati e assemblati a livello planetario

Conseguenze

- La globalizzazione ha portato alla creazione di un mercato illecito finalizzato a distruggere la sana concorrenza con parti contraffatte e false

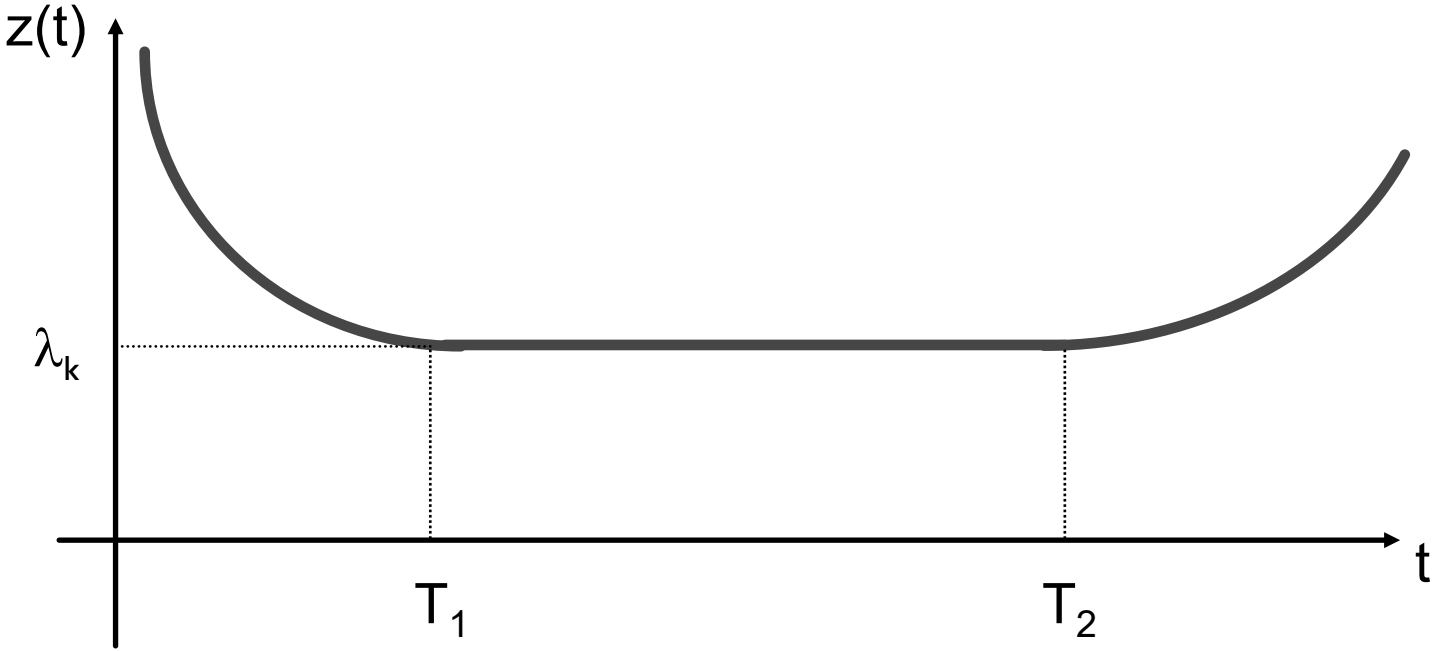
Problemi derivanti da dispositivi riciclati

Safety

- Fenomeni di invecchiamento (minor durata di vita)

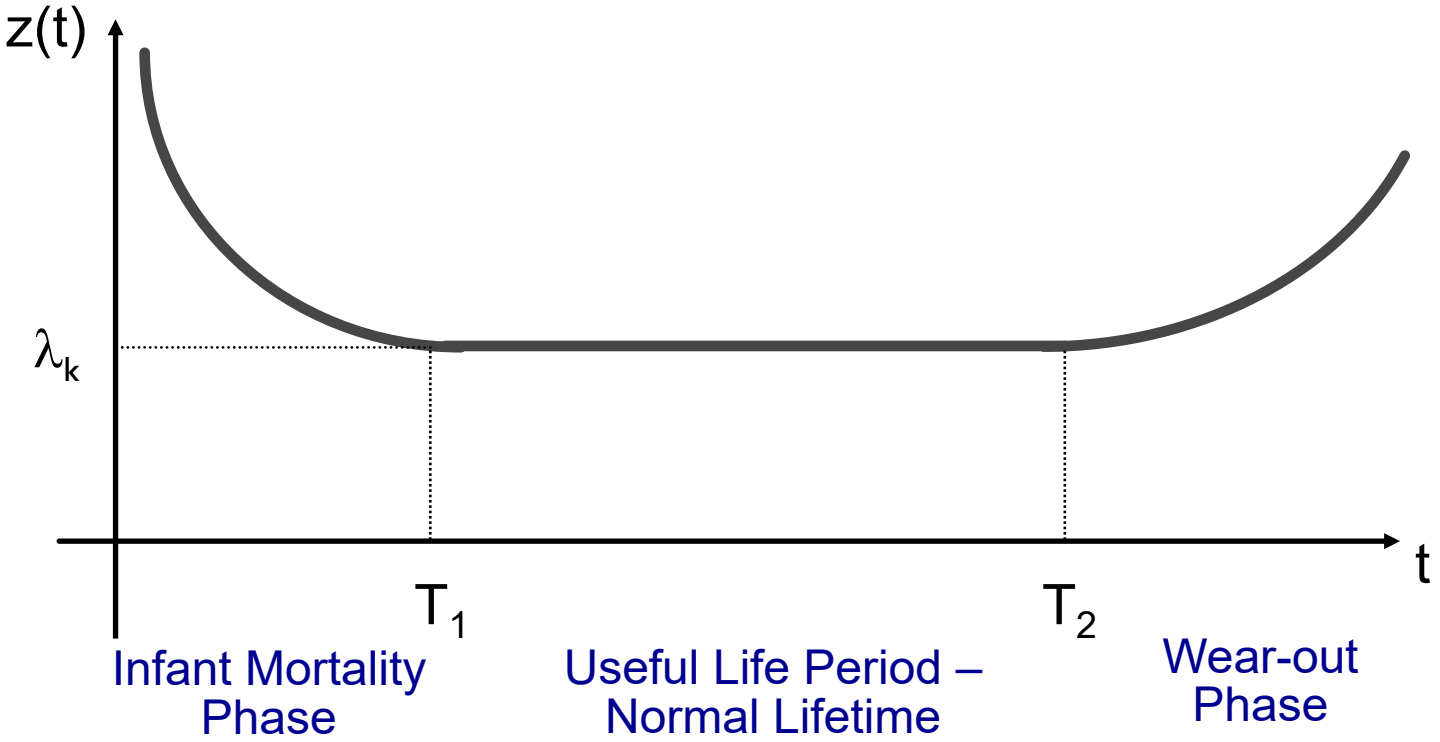
Failure Rate Function

(Andamento "*a vasca da bagno* - Bathtub curve)



Failure Rate Function

(Andamento "*a vasca da bagno* - Bathtub curve)



Problemi derivanti da dispositivi riciclati

Safety

- Fenomeni di invecchiamento (minor durata di vita)
- Potenziali danni, dovuti al processo di riciclaggio (rimozione ad altissima temperatura, rimozione fisica forzata dalle schede, lavaggio, levigatura, reimballaggio, ecc.)
- Prestazioni inferiori

Problemi derivanti da dispositivi riciclati

Safety

- Fenomeni di invecchiamento (minor durata di vita)
- Potenziali danni, dovuti al processo di riciclaggio (rimozione ad altissima temperatura, rimozione fisica forzata dalle schede, lavaggio, levigatura, reimballaggio, ecc.)
- Prestazioni inferiori

Security

- Vulnerabilità non “patch”-ate in modo adeguato