Design and Implementation of the PHaSE Core

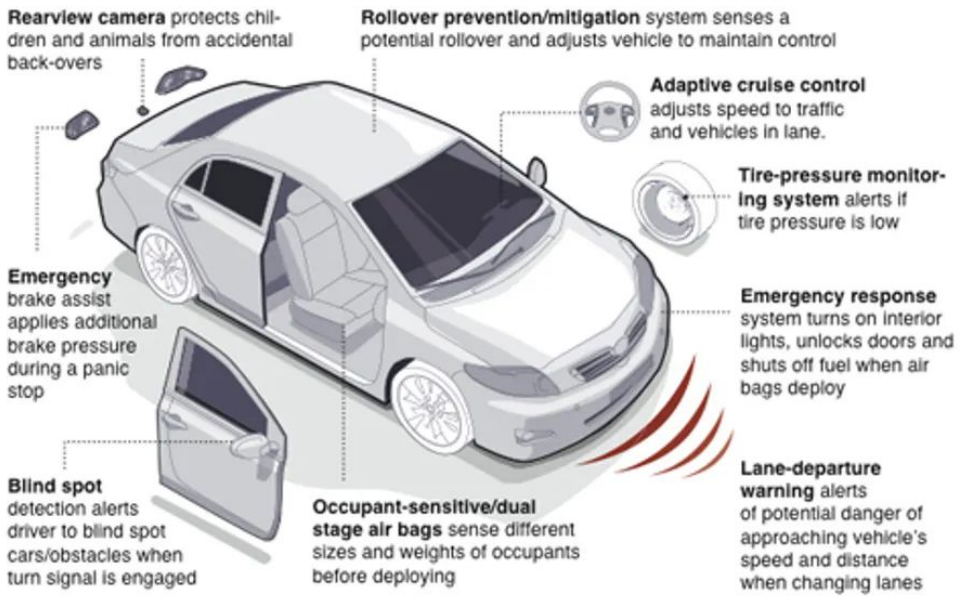
Establishing Hardware Roots of Trust for Safety-Critical Embedded Devices

Manoel Augusto de Souza Serafim

SBSeg24 SÃO JOSÉ DOS CAMPOS

UNIFESP

INTRODUCTION



- Authenticated Integrity
- Safety & Security
- Chains of Trust
- HRoT
- Conditional Control Flow
- Immutability
- Self-Tests (Weak)
- Revocation
- Cloning

TRUST

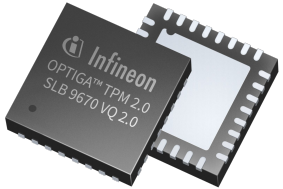
& the choice to be vulnerable.

- Risk & Trust boundaries?
- Trustworthiness?

RoT Storage (RoTS)
RoT Reporting (RoTR)
RoT Measurement (RoTM)

Severity/ Consequence (S)

Likelihood (L)	Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5



arm
TRUSTZONE

SOLUTIONS

CONTEXT

IBM

NIST’s post-quantum cryptography standards are here

A TPM chip is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and **malicious software is unable to tamper with the security functions of the TPM.** Jul 10, 2024

Microsoft Learn
https://learn.microsoft.com › hardware-security › tpm › t...

Trusted Platform Module Technology Overview - Microsoft Learn

Carnegie Mellon University — Search vulnerability notes

TCG TPM2.0 implementations vulnerable to memory corruption

REQUIREMENTS

Backward Compatibility
Supports legacy Line Replaceable Units (LRUs) without requiring major upgrades.

Security Through Transparency
Clear and verifiable security processes to enhance trust.

Future-Proof Design
Adaptable to address evolving threats and vulnerabilities.

Immutable Root of Trust
Ensures a tamper-proof foundation for security operations.

Resolder-Resistant Protection
Physical security measures to resist hardware tampering and resoldering attacks.

High Performance
Optimized for speed and low-latency cryptographic operations.

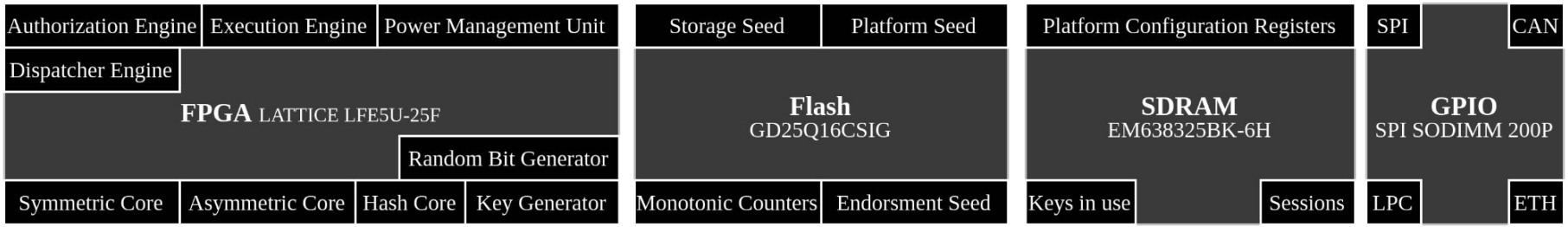
Interoperability
Replaces TPMs & Integrates with diverse hardware and software systems.

FIPS 140-3 Compliant
Meets standards for cryptographic hardware modules.

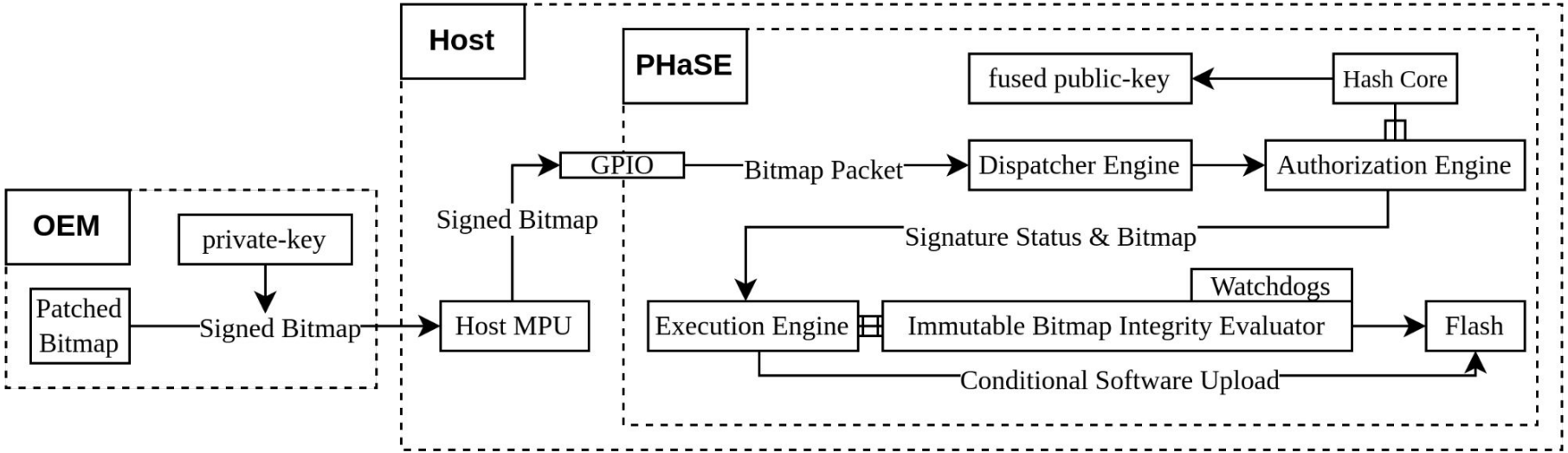
Efficient Patch Management
Supports updates and vulnerability patches without compromising security.

Programmable Hardware

Siloed Engine



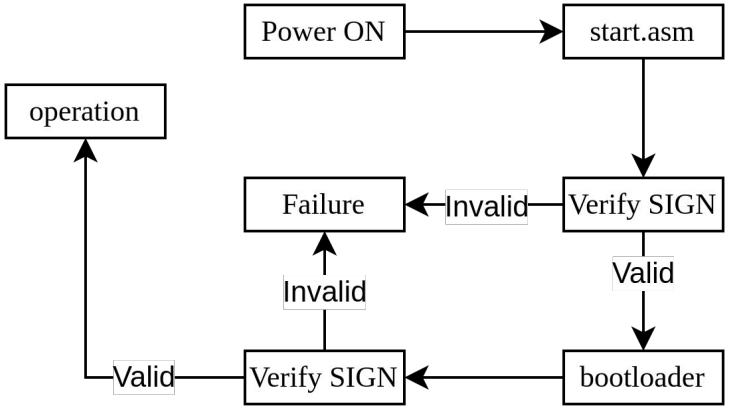
IAP


Host
PHaSE
fused public-key
Hash Core
GPIO
Bitmap Packet
Dispatcher Engine
Authorization Engine
OEM
private-key
Signed Bitmap
Signature Status & Bitmap
Watchdogs
Patched Bitmap
Signed Bitmap
Host MPU
Execution Engine
Immutable Bitmap Integrity Evaluator
Flash
Conditional Software Upload

SECURE BOOT

Validates images before they are allowed to execute.

- WORM
- SHA3... 2... 1
- RSA, ECDSA
- Time to ML-DSA & SLH-DSA?
- Cost?



BENCHMARKING

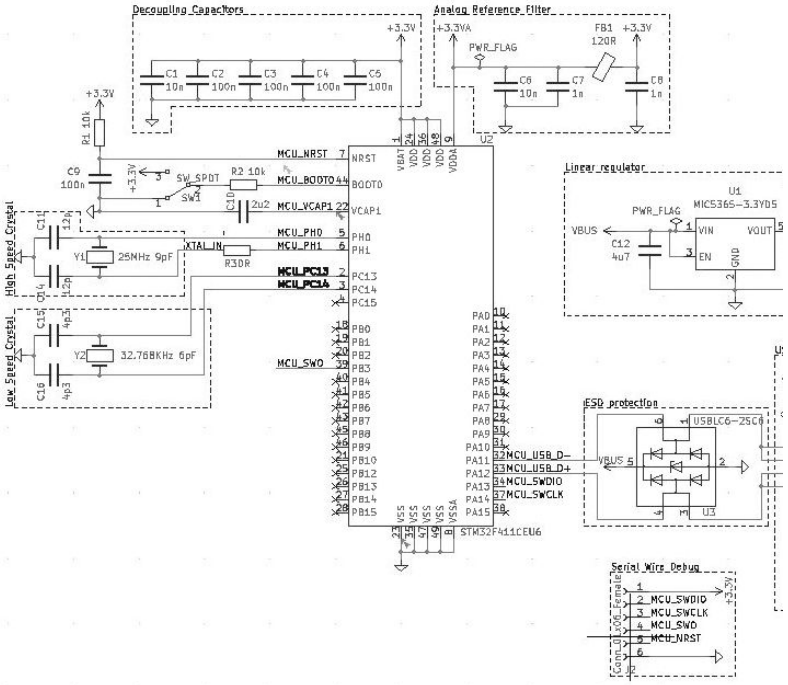
Table 1. Comparison of PHaSE Core and SLB 9670

Feature	PHaSE Core	SLB 9670
Construction	Sponge	Merkle-Damgard
Algorithm Considerations	Parallelizable in FPGA	No significant gains
Input	2MB Random Binary Image	
Hashing Time (ms)	48	944
Clock Speed	43 MHz Generated by PLL	43MHz
Number of Iterations	1000	

- No Fairness
- KECCAK
- Instruction vs Synthesis
- Monte Carlo
- SPI

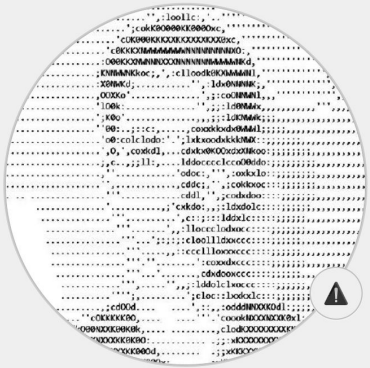
FUTURE WORK

- Power Analysis
- Mitigations as a Testable Requirement
- PCB Design
- **LoadVauIT32** Integration
- ML-DSA, SLH-DSA & ML-KEM



OBRIGADO!

semiotic.gitbook.io



Manoel Serafim
manoel-serafim

Q&A!