Post-Quantum

Cryptography Conference

Crypto Agility by Design: Securing PQC with Updatable HW/FW Co-design

Octavian Maciu

Hardware Product Manager at PQShield

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

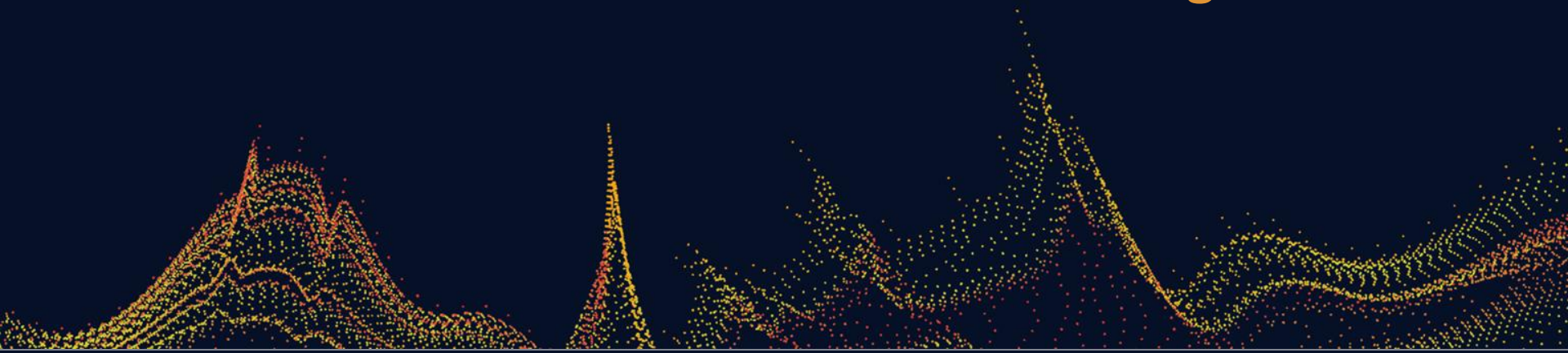
PKI Consortium

PKI Consortium
PQC Conference

PQSHIELD

The Power of Co-Design: Why a Hybrid Hardware/Software Approach is Essential for Post-Quantum Security

Octavian Maciu - HW Product Manager



Speaker: about me

Octavian Maciu
octavian.maciu@pqshield.com
Linkedin

- 2014 Université de Strasbourg:
  M.Sc in Microelectronics
- 2014-2017 CNRS:
  Research in ultra-fast image sensor design
- 2018-2025 Qualcomm:
  Cryptographic Management Unit owner inside Qualcomm's integrated secure element (SPU)
- 2025 PQShield:
  Hardware Product Manager

A Stable Past, An Uncertain Future: classical asymmetric cryptography (ex.RSA,ECC) enjoyed stable implementations with ‘predictable’ side-channel risks

The quantum threat shatters this stability

We cannot rely on static, immutable defenses anymore

The ability to securely evolve both hardware and software is a critical to protecting your investment

The Danger of Static Defenses

- **Immutable Software:** **Checkm8** exploit in the unpatchable bootrom.
- **Static Library:** **EUCLEAK** vulnerability in a non-updatable cryptographic library.
- **Hardware Logic:** **Caliptra** side-channel leak from a hardware accelerator.

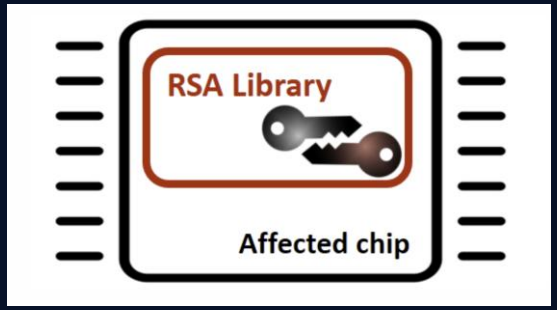
The true enemy isn't hardware; it's immutability.

The ROCA vulnerability

Affected millions of TPM chips, authentication tokens and smart cards worldwide

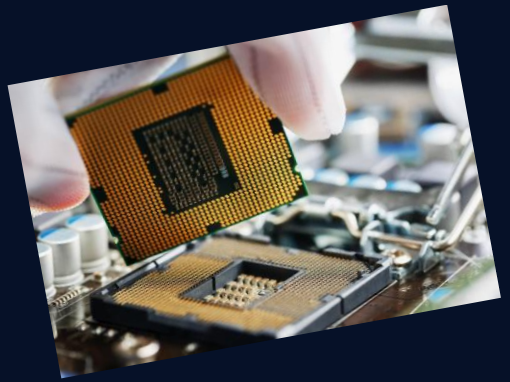
TPMs with updatable firmware could be patched in the field

However, Devices which lacked this mechanism required a costly 18-month-long physical replacement program



The true costs of immutability aren’t just financial; it's a massive logistical burden and an erosion of trust

Accelerating Security Responsiveness



Hardware-Only: A flaw found late means a multi-million dollar, 6+ month delay for a new silicon "tape-out"

Co-Design: A flaw can be mitigated by developing and testing a firmware countermeasure in days or weeks, leading to a more robust product at launch

The Advantage of a Dynamic Defense

Patch Vulnerabilities: Instantly fix the next ROCA or EUCLEAK

Counter Physical Attacks: Deploy new firmware countermeasures for side-channels.

Future-Proof for PQC: Stay crypto-agile, adapting to new standards and research without replacing hardware

PQC today

NIST Standards: ML-KEM, ML-DSA and SLH-DSA

Hardware Implementations: Are just appearing now

Future Standards: HQC, FN-DSA and others are coming...

No one size fits all like before

In the PQC era, resilience is just as important as prevention

A New Attack Surface…

Standards are not implementations

High-Assurance is back to Day One

Likely that many first-generation PQC implementations will be found vulnerable

Agility is the only defense against the unknown

The Best of Both Worlds: A Symbiotic Defense

The Hardware's Role:

- Provides the immutable Root of Trust
- Physically protects keys and logic that secure the firmware update mechanism

The Firmware/Software's Role:

- Provides the intelligent, adaptive defense layer
- Evolve and protect the hardware from threats it was never designed to face

The End of Stability: Why PQC Demands a New Approach

The **quantum threat** marks the end of a long era of cryptographic stability via perfected RSA/ECC implementations

The PQC Frontier: A New, unexplored world through algorithms like ML-KEM and ML-DSA.

Side-channel: attack surface is largely unknown territory.

Conclusion

The New Reality: The PQC transition is a dynamic, uncertain process where static defenses are guaranteed to fail.

The Path Forward: The only viable strategy is a resilient platform built on the synergy of trusted hardware and securely updatable firmware.

It behooves us to build dynamic, future-proof security platforms to protect our customers today and for the quantum future to come