Secure boot and root-of-trust for space-grade RISC-V systems

Petri Jehkonen and Kimmo Järvinen

Motivation

Space systems can be targets for remote attacks including malicious firmware updates and exploits against software vulnerabilities.

The secure boot ensures the integrity of the computing platform at boot.

The root-of-trust (RoT) is a component that is always trusted in a computing system. It is immutable and isolated component providing trustworthy cryptographic services and key management.

Post quantum cryptography

Quantum computers threaten the security of current asymmetric cryptography (RSA and ECC). This threat can be mitigated with post quantum cryptography (PQC) which are asymmetric cryptographic algorithms that are secure even against attacks with quantum computers.

NIST published final standards for three PQC algorithms in summer 2024: ML-KEM (key exchange), ML-DSA (digital signature), and SLH-DSA (digital signature).

Secure boot

Secure boot verifies digital signed binary images and ensures that they are allowed to be run by the processor only if the verification is successful.

Xiphera nQrux® Secure Boot uses ECDSA and ML-DSA signatures and SHA-3 for efficient secure boot solution designed particularly for space applications.

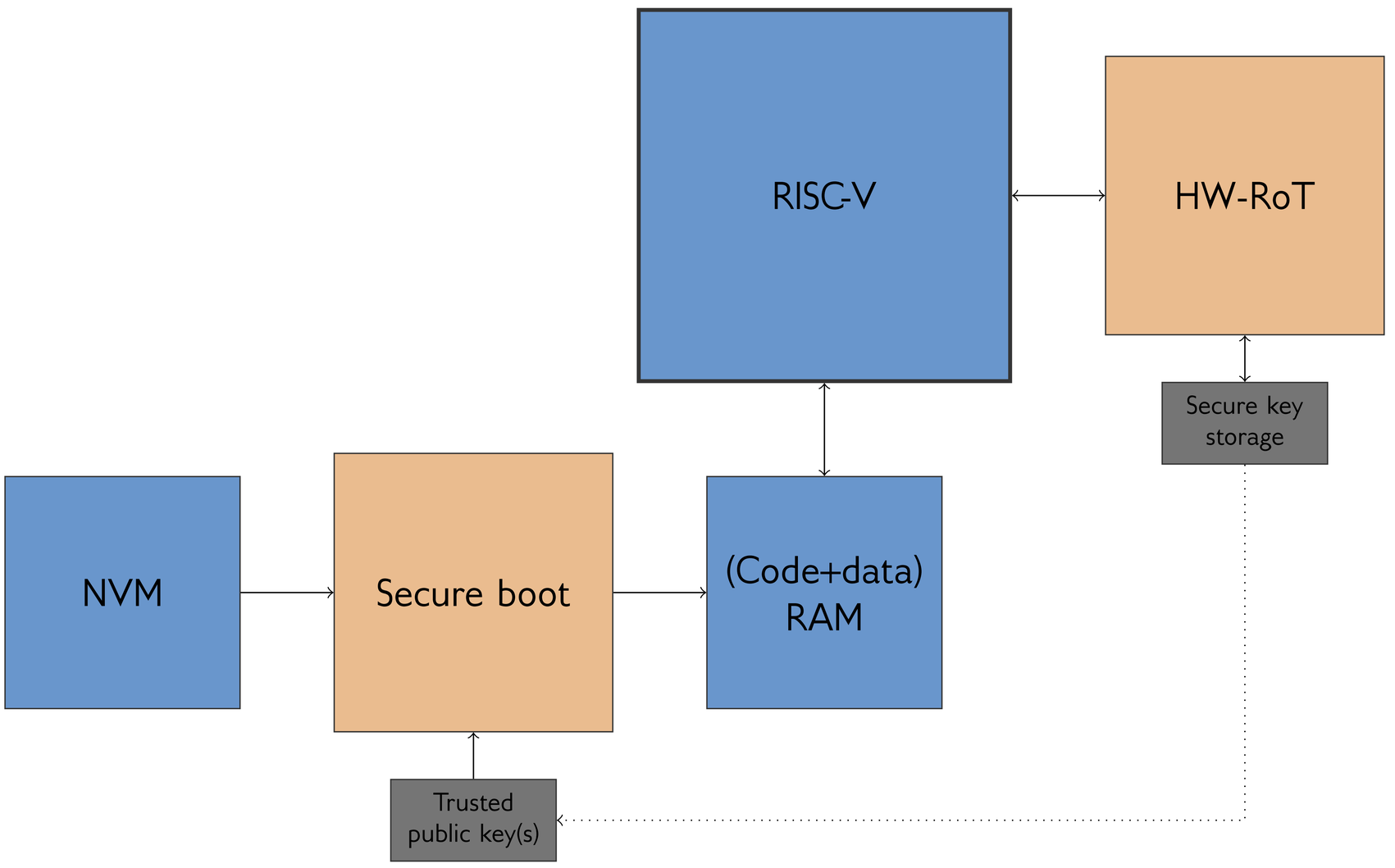
Hardware root-of-trust

HW-RoT is an isolated security domain in FPGA or ASIC (e.g. SoC) that operates as a trust anchor for the computing platform.

Xiphera has identified minimum viable RoT functionalities:
- Cryptographic services (ciphering, signing, rand. numbers, etc.)
- Unique device identity
- Secure key storage
- Access policies for different users
- Software API

Xiphera is developing a HW-RoT solution for space applications in an ESA project. (see: https://xiphera.com/xiphera-develops-quantum-resilient-hardware-security-solutions-for-space/).

Integration into a RISC-V system



Xiphera Oy, Tekniikantie 12, Espoo, Finland
firstname.lastname@xiphera.com

ESA Contract No. 4000145191/24/NL/KK/adu