Halfway Through: CROSSCON's Key Outcomes & Milestones

Towards an improvement in the security of a wide range of heterogeneous IoT devices, the CROSSCON project is designing a new open, flexible, highly portable, and vendor-independent IoT security stack that can run across multiple devices. Halfway through the project, several key milestones were already reached:

- ✅ Use Cases & Requirements Definition
- ✅ First version of CROSSCON Open Specification
- ✅ First version of the CROSSCON stack components

To fully understand the real-world impact of CROSSCON components, the project identified five crucial use-case scenarios: Device Multi-Factor Authentication, Firmware Updates for IoT Devices, Commissioning and Decommissioning of IoT Devices, Remote Attestation for Agricultural UAVs, and Intellectual Property Protection for Secure Multi-Tenancy on FPGA. Learn more about the uses cases in the CROSSCON website.

CROSSCON Open Specification is Ready (First Version)

To define the open specification of the security stack, CROSSCON analysed several architectures and security primitives, ranging from low-power microcontrollers (MCUs) to powerful aplication processors (APUs) with reconfigurable hardware. As a result, CROSSCON proposes an unified abstraction model encompassing various system stacks across different architectures, including Arm and RISC-V, leveraging different security primitives.

CROSSCON Components Available

First CROSSCON artifacts and demos are available in the official GitHub repository[1]. The initial release includes the TEE abstraction and isolation, the CROSSCON Hypervisor, new trusted services, TEE Toolchain, and a bare-metal TEE. Additionally, the project is designing its own SoC to enhance security, transparency, and flexibility over IoT devices' behavior.

✉ contact@crosscon.eu   🌐 www.crosscon.eu   🐦 @crosscon_eu   in in/crosscon