CROSSCON: INTEROPERABLE IOT SECURITY STACK

THE RISC-V OPPORTUNITY

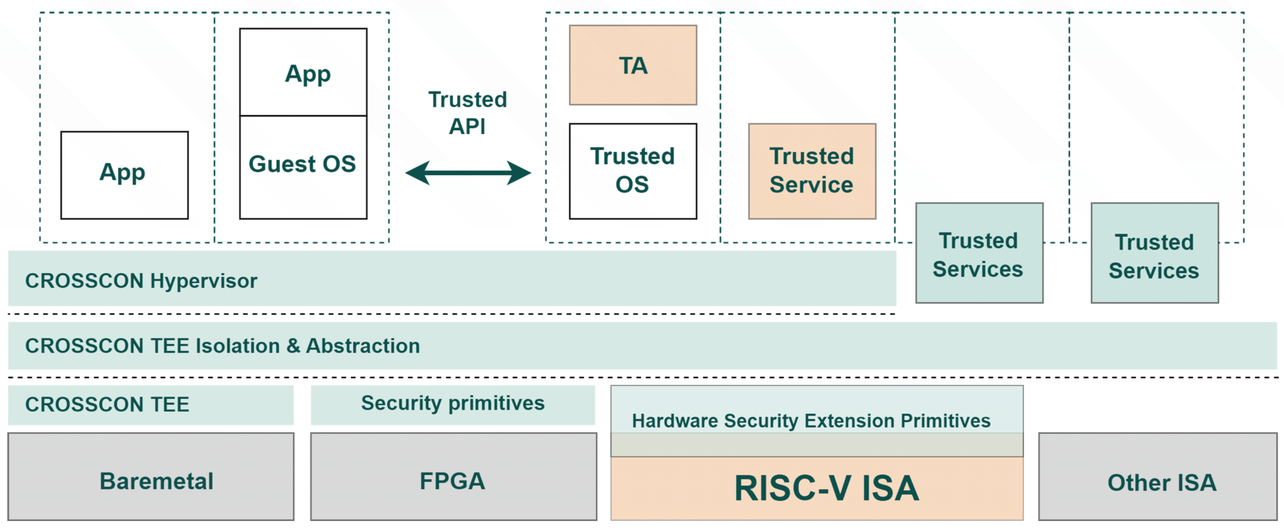
Sandro Pinto*, Matjaz Breskvar[1], Tiago Gomes*, Hristo Koshutanski[2], Aljosa Pasic[2], Piotr Król[3], Emna Amri[4], David Purón[5], Zoltan Hornak[6], Marco Roveri[7], Alexandra Dmitrienko[8], Ahmad-Reza Sadeghi[9], Bruno Crispo[7]

*Centro ALGORITMI/LASI - Universidade do Minho; [1]Beyond Semiconductor; [2]ATOS; [3]3MDEB; [4]CYSEC; [5]Barbara IoT; [6]Search-Lab; [7]Universita di Trento; [8]Universitat Wurzburg; [9]TU Darmstadt.

Abstract

CROSSCON is a 3-year, multi-million euro, Research and Innovation Action funded under Horizon Europe. The project aims to design a new open, modular, highly portable, and vendor-independent IoT security stack that can run on various devices using heterogeneous hardware architectures, including RISC-V. The Consortium sees in RISC-V a two-fold opportunity. Firstly, by aiming to develop an interoperable reference security stack, we believe we can contribute to the expected specifications of ongoing initiatives for Trusted Execution and Confidential Computing on Application processors (i.e., CoVE) and microcontrollers. Secondly, RISC-V offers a unique opportunity to develop novel security hardware extensions for software services, either by creating extensions directly to the ISA or developing non-ISA hardware mechanisms that support the efficient implementation of security guarantees at the application level.

CROSSCON Security Stack



CROSSCON Hypervisor

CROSSCON SoC

CROSSCON TEE

HW Security primitives

Trusted Services

To overcome current interoperability issues, CROSSCON aims at providing the stack's top layers (i.e., the OS and applications) with a unified set of APIs to use TEE functionalities and trusted services. CROSSCON also aims at improving and enriching the traditional trusted services supported by existing TEEs and, in the case of RISC-V, spanning the TEE guarantees from the CPU to the entire SoC.

RISC-V Opportunity

Standardization of Software Architectures for Trusted Execution

- Engage with RISC-V Working Groups (WG) and Special Interest Groups (SIG), e.g., AP-TEE and Trusted Computing.
- Contribute to developing the specs, in particular by sharing requirements from the CROSSCON use cases and other TEE model.
- Add support on the CROSSCON security stack for the different RISC-V TEE specs and architectures.

Development of Novel Security Hardware Extensions and Mechanisms

- Research potential ISA extensions for specific Trusted Services (derived from the use cases), e.g., hardware primitives for authentication services or Control-Flow Integrity enforcement.
- Develop hardware security mechanisms that provide security guarantees to non-CPU hardware components similar to those offered to the CPU by the TEE.

Road Map and Conclusion

The CROSSSCON project started in Q4 2022 by defining the requirements and refining the use cases. We are now working on the CROSSCON open specification. Activities will proceed next towards two streams of work:

- A "horizontal" stream around the development of the heterogeneous and interoperable security software stack;
- A "vertical" stream towards security-oriented hardware extensions and domain-specific hardware architectures.

We expect to engage with RISC-V International and contribute across the related WG and SIGs.

SCAN FOR MORE!

CROSSCON has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537.

contact@crosscon.eu

www.crosscon.eu