CROSSCON: Interoperable IoT Security Stack - The RISC-V Opportunity

Sandro Pinto[*], Matjaz Breskvar[1], Tiago Gomes[*], Hristo Koshutanski[2], Aljosa Pasic[2], Piotr Krol[3], Emna Amri[4], David Puron[5], Zoltan Hornak[6], Marco Rovieri[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.

Introduction

The IoT landscape consists of highly heterogeneous devices, ranging from bare metal systems with a few kilobytes of RAM and limited or no security capability to devices equipped with powerful AI support and built-in hardware to implement the Root of Trust and Trusted Execution Environments (TEEs) [1, 2]. Such reality is the zeitgeist in the IoT, and it is still an open challenge to guarantee an acceptable level of security across the whole IoT spectrum.

CROSSCON aims to address all these issues by designing a new open, flexible, highly portable, and vendor-independent IoT security stack that can run across various edge devices and multiple computing architectures, including those built on RISC-V. As an open and interoperable security stack, there is a two-fold opportunity in RISC-V. Firstly, we believe we can contribute and help shape ongoing Trusted Execution and Confidential Computing activities and specifications. Secondly, RISC-V offers a unique opportunity to provide more robust security guarantees, by enabling unseen freedom to implement novel extensions and mechanisms at the hardware level [3].

The project will validate its approach in use cases dealing with trusted services for connected devices, including patches, security audits, commissioning and decommissioning, and secure authentication and communication. CROSSCON will provide the open specifications of the stack, interoperable with the (specs available in) RISC-V. Besides strengthening EU cybersecurity capacities, it will focus on community building, particularly with RISC-V International.

CROSSCON Security Stack

Figure 1 depicts the envisioned CROSSCON IoT security stack. Components in green extend interoperability across heterogeneous architectures (including RISC-V), offering a unified level of abstraction and enriching existing security features. To overcome interoperability issues, CROSSCON will provide the stack's top layers (i.e., the OS and applications) with a unified set of APIs to use TEE functionalities and trusted services. We expect to improve and enrich the traditional trusted services supported by existing TEEs and, in the case of RISC-V, to span the TEE guarantees from the CPU to the full SoC. Furthermore, since the Chain of Trust propagates on CROSSCON stack, relying ultimately on the Root of Trust, the security properties and guarantees offered by the stack design will be formally verified.

The RISC-V Opportunity

Standardization of Software Architectures for Trusted Execution. In contrast with other mainstream computing architectures (i.e., x86 and Armv8-A), RISC-V has no specific security-oriented extension for Trusted Execution at the ISA level. For example, Intel has SGX, and Arm has TrustZone. Existing TEE for RISC-V, e.g., KeyStone [4] and MulitZone [5], have been leveraging a very raw hardware primitive already embedded into the ISA for memory protection, i.e., the Physical Memory Protection (PMP). Notwithstanding, among the RISC-V Technical Working Groups and Special Interest Groups (SIG), there are already

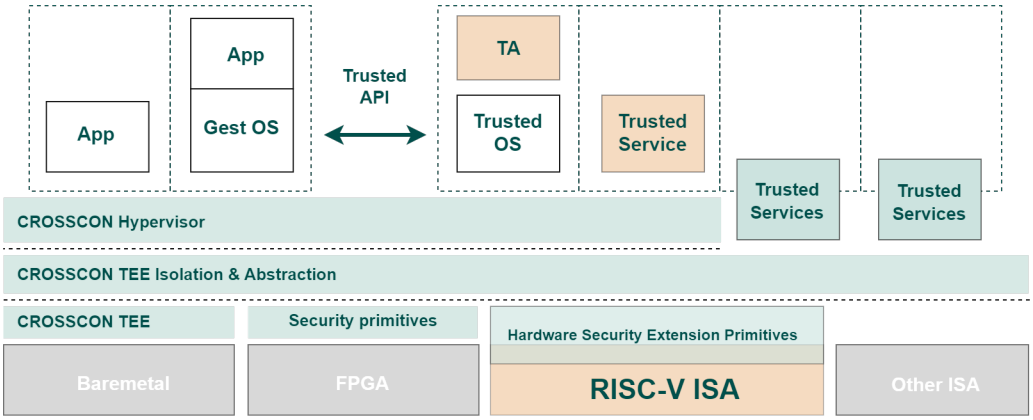

Figure 1: *Interoperable IoT Security Stack.*

ongoing activities to provide specifications for Trusted Execution and Confidential Computing, such as the CoVE [6] and Confidential Computing for IoT Devices [7]. Our goal here is multi-fold. First, engage with respective WG and SIGs. Second, participate and contribute to developing the specs, in particular by sharing requirements from the CROSSCON use cases and other TEE models. Finally, we plan to include support in the CROSSCON security stack for the different RISC-V TEE specs and architectures.

Development of Novel Security Hardware Extensions and Mechanisms. RISC-V offers a unique security opportunity at the ISA and hardware levels. One envisioned aisle of research and exploration involves leveraging the RISC-V ISA modularity to define new ISA extensions to accelerate at the application layer. There are already success stories in RISC-V, such as the XPULP ML extensions. In our case, we plan to provide ISA extensions for specific Trusted Services (derived from the use cases), e.g., hardware primitives for authentication services or Control-Flow Integrity enforcement. Secondly, CPUs are key but not the only security-relevant hardware component. The software usually interacts with many hardware devices and hardware accelerators (e.g., DMAs, crypto accelerators) that are relevant to the security of the applications/system. We plan to develop hardware security mechanisms that provide security guarantees to non-CPU hardware components similar to those offered to the CPU by the TEE. In particular, we plan to create a novel data-driven hardware-enforced separation model (and potentially other security-relevant property guarantees) targeting SoC interconnect, peripheral devices, hardware accelerators, and other domain-specific data flow processing hardware.

Roadmap and Conclusion

The 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: (i) an "horizontal" stream around the development of the heterogeneous and interoperable security software stack and (ii) a "vertical" stream towards security-oriented hardware extensions and domain-specific hardware architectures. All these activities will run toward the end of the project. We expect to engage with RISC-V International and contribute across the related WG and SIGs.

Acknowledgments

This work is supported by the European Union's Horizon Europe research and innovation program under grant agreement No 101070537, project CROSSCON (Cross-platform Open Security Stack for Connected Devices).

References

[1] Michele Grisafi et al. "PISTIS: Trusted Computing Architecture for Low-end Embedded Systems". In: *USENIX Security*. 2022.

[2] David Cerdeira et al. "ReZone: Disarming TrustZone with TEE Privilege Reduction". In: *USENIX Security*. 2022.

[3] Raad Bahmani et al. "CURE: A Security Architecture with CUstomizable and Resilient Enclaves". In: *USENIX Security*. 2021.

[4] Dayeol Lee et al. "Keystone: An Open Framework for Architecting Trusted Execution Environments". In: *Proc. of EuroSys*. 2020.

[5] Cesare Garlati and Sandro Pinto. "A Clean Slate Approach to Linux Security RISC-V Enclaves". In: *Embedded World Conference*. 2020.

[6] RISC-V AP-TEE Task Group. *Confidential VM Extension (CoVE) for Confidential Computing on RISC-V platforms*. 2023.

[7] Bicheng Yan et al. "Introducing RISC-V Confidential Computing for IoT Devices". In: *RISC-V Summit*. 2022.