An Open-Source Trusted Execution Environment for Resource-Constrained RISC-V MCUs

Luís Cunha*, Daniel Oliveira, João Sousa, Tiago Gomes, Sandro Pinto

Centro ALGORITMI - UMinho

Abstract

This work presents the design and implementation of CROSSCON Baremetal TEE, an open-source Trusted Execution Environment (TEE) targeting resource-constrained RISC-V-based MCUs with support for Machine, (Supervisor,) and User modes. The CROSSCON Baremetal TEE leverages RISC-V's privilege levels and memory isolation primitives to enable multi-world execution while maintaining strong security guarantees at the least privileged level. So far, we have implemented and validated the system on Machine and User mode-enabled cores, running a set of low-level benchmarks and test applications. Future plans include extending the support to the Supervisor mode and open-sourcing all artifacts to foster collaboration within the RISC-V community.

Introduction

The Internet of Things (IoT) is experiencing exponential growth, with billions of connected devices already being used in various domains. Industry projections further highlight this trend; for instance, Business Insider Intelligence forecasts 64 billion devices by 2026 [1]. As these systems connect to the Internet, they face rising cybersecurity risks. As such, Trusted Execution Environments (TEEs) have become a key security layer on various platforms to protect sensitive services.

Although TEE technology, e.g., Arm TrustZone, is widely used in (embedded) application processor units (APUs), microcontroller units (MCUs) often lag behind. Many MCUs either lack essential security hardware primitives or fail to leverage them when available [2]. In response to these growing challenges, ARM pushed Trustzone-M technology with their Armv8-M MCUs. However, TrustZone-M is still limited to a dual-world architecture and has already revealed some vulnerabilities [2]. Nonetheless, this push forward from ARM highlights the lack of TEE architectures and specifications within the RISC-V ecosystem.

In this paper, we propose the CROSSCON Baremetal TEE, a novel open-source TEE implementation targeting resource-limited RISC-V-based MCUs with Machine, (Supervisor,) and User mode. Our solution aims to provide multi-world capabilities and core-level isolation by leveraging the different execution levels predicted in the RISC-V ISA and memory isolation hardware primitives. CROSSCON Baremetal TEE allows the creation of multiple and equally secure execution environments within the least privileged level. This work is core part of a multi-million EU-funded project, aiming at designing an open, flexible, highly portable and vendor-independent IoT security stack that can run across multiple hardware platforms.

Motivation

In the RISC-V ecosystem, the absence of standardized TEE architectures or specifications presents a significant challenge for the widespread adoption of TEE technologies. Unlike other architectures such as ARM, which has established TrustZone(-M), RISC-V lacks a unified approach. This results in fragmentation, with different vendors or organizations developing their own proprietary solutions, often without interoperability or clear security guarantees. Moreover, without standardized specifications, the design and implementation of TEEs in RISC-V are left open to inconsistencies.

An emerging solution to this is Worldguard, which provides a system-level approach to securing RISC-V designs. It offers hardware-enhanced software isolation, protecting against unauthorized access to memory or devices by software applications and other bus initiators. Nonetheless, despite the recent pushes towards Worldguard's ratification, the process is still in its early stages and more work is needed.

Similar works, like Multizone [3], provide hardware-enforced, software-defined isolation of multiple functional areas within a chip. Despite the similarities, we believe the novelty of our work is in the planned support of architectures with Supervisor-Mode, which Multizone lacks. Another line of work tackles the mentioned challenges but targets next-generation RISC-V MCUs, leveraging the Hypervisor extension and SPMP to provide secure execution [4]. None of the mentioned solutions offer out-of-the-box GlobalPlatform compliance which we aim to provide.

*Corresponding author: id11207@alunos.uminho.pt

Funded by the European Union under Horizon Europe Programme - Grant Agreement 101070537 — CrossCon. This work has been supported by FCT – Fundação para a Ciência e Tecnologia within the R&D Unit Project Scope UID/00319/Centro ALGORITMI (ALGORITMI/UM) and the Scholarships Project Scope SFRH/BD/00297/2023 and SFRH/BD/01007/2023.

Design and Implementation

We propose the CROSSCON Baremetal TEE, which aims to provide a multi-world architecture based on the zero-trust model, which dictates that every single software component, with the exception of the TEE kernel, cannot be trusted.

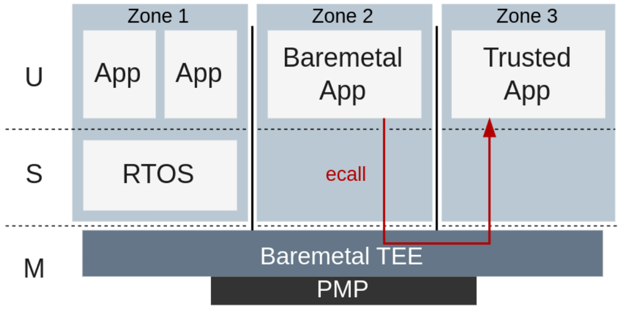

Figure 1: *CROSSCON Baremetal TEE architecture.*

Design Principles. As depicted in Figure 1, this solution leverages the RISC-V ISA privilege levels, as well as the PMP to provide separate and isolated worlds. Using these hardware features allows the CROSSCON Baremetal TEE to maintain a minimal implementation, reducing the system's attack surface.

Execution. At boot, the CROSSCON Baremetal TEE configures the PMP entries for the first world based on a configuration file and initiates its execution. Scheduling is managed using the *mtimer*, following a round-robin policy. At each scheduling point, four key actions take place: (i) the context of the current world is saved, (ii) a new world is selected for execution, (iii) the PMP is reconfigured to grant access to the memory regions of the new world, and (iv) the context of the new world is restored. Additionally, a world can issue an `ecall` to pass execution arguments and request the execution of a specific world, enabling standardized APIs such as the GlobalPlatform TEE API.

Discussion. Reconfiguring the PMP entries at each scheduling point can be expensive when considering world switching time; however, it increases the system's flexibility when the amount of entries is limited, allowing for more worlds and more protected regions per world. Nonetheless, the entries can also be pre-configured and just enabled/disabled for stricter real-time scenarios, with further testing needed for conclusions. Additionally, this design cannot protect the worlds against attacks from other bus initiators, e.g., DMA attacks. Although there are open implementations of bus-level controllers, such as the IOPMP [5], the specification has not yet been ratified, and commercial solutions are scarce. As highlighted, these system-level protections and TEE architectures are still missing in the RISC-V ecosystem, limiting the implementation of more secure low-level systems. Although they are not currently available, the CROSSCON Baremetal TEE could be extended to use these solutions to provide world isolation at the system level.

Status, Roadmap

To date, we have implemented the proposed solution to run on Machine- and User-mode enabled cores. We validated the behavior by running a set of low-level benchmarks and applications. We are now proceeding to a more empirical functional validation where we will run a bitcoin wallet, i.e., trusted application, alongside a client application. Next, we will assess the overhead of using the CROSSCON Baremetal TEE, which we predict will be negligible due to it being written in assembly. Finally, we will extend the system to run on Machine-, Supervisor-, and User-mode enabled cores.

Conclusion

In this work, we introduced CROSSCON Baremetal TEE, a novel open-source TEE implementation designed for resource-constrained RISC-V-based MCUs supporting Machine, (Supervisor,) and User modes. By leveraging RISC-V's privilege levels and memory isolation primitives, this TEE enables multi-world execution while maintaining strong security guarantees at the least privileged level. Our approach provides a lightweight yet effective framework for core-level isolation, addressing the growing need for secure execution environments in embedded systems. As part of the open-source focused CROSSCON project, we plan to release all implementation artifacts to foster collaboration within the RISC-V community, encouraging further research and development in the field of trusted execution for constrained devices.

References

[1] "Celebration of IoT Day 2020: How Open Hardware & Software Is Stimulating IoT Innovation". In: *RISC-V Blog* (2020).

[2] X. Tan et al. ""Where's the"up"?! A Comprehensive (bottom-up) Study on the Security of Arm Cortex-M Systems". In: *arXiv preprint arXiv:2401.15289,* (2024).

[3] Cesare Garlati and Sandro Pinto. "Secure IoT Firmware For RISC-V Processors". In: *Embedded World Conference.* 2021.

[4] Sandro Pinto et al. "Securing Embedded and IoT Systems with SPMP-based Virtualization". In: *RISC-V Summit Europe 2024*. 2024.

[5] Luís Cunha et al. "Open-source RISC-V Input/Output Physical Memory Protection (IOPMP) IP". In: *RISC-V Summit Europe 2024*. 2024.