Cross-platform **O**pen **S**ecurity **S**tack for **Con**nected Device

D4.2 CROSSCON Extension Primitives to Domain Specific Hardware Architectures — Initial Version

Document Identification			
Status	Final	**Due Date**	30/04/2024
Version	1.0	**Submission Date**	30/04/2024

Related WP	WP4	**Document Reference**	D4.2
Related Deliverable(s)	D4.1	**Dissemination Level (*)**	PU
Lead Participant	BEYOND	**Lead Author**	Žiga Putrle (BEYOND)
Contributors	TUD, UWU	**Reviewers**	Bruno Crispo (UNITN) Shaza Zeitouni (TUD)

Keywords:
CROSSCON SoC, BA51-H, FPGA, FPGA TEE, Perimeter guard

Document Information

List of Contributors	
Name	Partner
Žiga Putrle	BEYOND
Tilen Nedanovski	BEYOND
Shaza Zeitouni	TUD
Lukas Petzi	UWU

Document History			
Version	Date	Change editors	Changes
0.1	24/04/2024	Žiga Purtle Shaza Zeitouni Lukas Petzi	Initial contributions.
0.2	28/04/2024	Žiga Purtle Shaza Zeitouni	Addressing review comments.
0.9	29/04/2024	Juan Alonso (ATOS)	Quality Assessment
1.0	30/04/2024	Hristo Koshutanski (ATOS)	Final version submitted

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Žiga Purtle (BEYOND)	28/04/2024
Quality manager	Juan Alonso (ATOS)	29/04/2024
Project Coordinator	Hristo Koshutanski (ATOS)	30/04/2024

Table of Contents

List of Acronyms

Abbreviation / acronym	Description
D4.1	Deliverable number 1 belonging to WP4
D4.2	Deliverable number 2 belonging to WP4
EC	European Commission
FPGA	Field-Programmable Gate Arrays
HW	Hardware
IoT	Internet of Things
MS8	8th Milestone
PG	Perimeter Guard
PMP	S-mode PMP
SoC	System-on-Chip
SPMP	S-mode Physical Memory Protection
TRL3	Technology Readiness Level 3
vFPGA	Virtual FPGA
WP	Work Package

Executive Summary

The deliverable D4.2 contains the initial implementation results of work done as part of WP4 described in D4.1 “CROSSCON Extensions to Domain Specific Hardware Architectures Documentation — Draft” [8]. It includes (1) the initial implementation of the CROSSCON SoC with BA51(-H) core and a prototype implementation of Perimeter guard, (2) a Spike (RISC-V) simulator extended with unified SPMP extension, (3) the initial implementation of Secure FPGA Provisioning system that can be used to establish virtual FPGA environments, and (4) a demonstrator showing how we can leverage PSA Crypto API to seamlessly use different cryptographic accelerators. The provided artifacts serve as proof of concept prototypes that demonstrate parts of developed solutions that will be extended and improved as part of the future work. This deliverable D4.2 contributes to the accomplishment of milestone MS4 “First version of the CROSSCON stack components and extension primitives, and testbed” with a targeted TRL3 of artefacts’ release according to the workplan.

1 Introduction

1.1 Purpose of the document

The document outlines the initial implementation results of work done as part of WP4 described in D4.1 “CROSSCON Extensions to Domain Specific Hardware Architectures Documentation — Draft” [8] and provides references to the project repositories that are included in this deliverable. Each of the repositories contains an extended description of the implemented solution, instructions on how to use it and related code / bitstreams. The provided prototypes demonstrate our work and will be extended and improved as part of the future work.

1.2 Relation to other project work

This document is closely related to the deliverable D4.1, “CROSSCON Extensions to Domain Specific Hardware Architectures Documentation — Draft” [8], as it contains the actual implementation results described in D4.1[8]. The implementation results serve as first prototypes of the work and are thus a necessary input for future development done in WP2, WP3 and WP4 towards MS8 “Final version of the CROSSCON stack components and extension primitives, and extended testbed”. Furthermore, through the implementation, new insights were acquired that are useful for further refinement of the CROSSCON Open Specification (D2.3) worked on in WP2. Additionally, the used development and runtime environment are necessary inputs for the integration and validation of the solutions as part of the WP5.

1.3 Structure of the document

The document is structured into several independent sections that are a part of chapter 2. Each section contains a short description of provided artifact with a reference to the repository that contains the extended description, the artifact itself and instructions on how to use it.

2 WP4: Extension Primitives Initial Version

Withing WP4, we aim to define and develop hardware-software extensions to improve the security of IoT devices and complement the CROSSCON Stack. As part of D4.2, “CROSSCON Extension Primitives to Domain Specific Hardware Architectures — Initial Version”, we provide the software / bitstreams of the initial, proof of concept, implementations of the developed extensions and related software together with their description and instructions on how to use them. The developed extensions and related documentation are accessible in the CROSSCON’s GitHub repository [1].

2.1 Task 4.1: Platform Security Architecture (PSA) Crypto API Demonstrator

CROSSCON aims to develop a unified software stack for resource-constrained IoT devices. As part of this effort, we seek to provide a unified interface for trusted services within CROSSCON to perform essential cryptographic operations. As IoT devices increasingly integrate domain-specific hardware components such as cryptographic accelerators, it is crucial for software stacks to incorporate these hardware components. An important task is to evaluate existing APIs to understand their versatility and potential for integration into the CROSSCON stack.

Related repo https://github.com/crosscon/crypto_API_demonstrator [2]. This repo contains an example of how the PSA Crypto API can be used to perform encryption and decryption with AES-128, as well as data hashing using SHA-256, on two different platforms, LPC55S69-EVK with ARM Cortex-M33 and ESP32-C3 with RISC-V microprocessor. Both devices are outfitted with hardware accelerators for these operations. The purpose of the demonstrator is not only to showcase the PSA Crypto API but also to provide guidance on how to configure the platform (e.g., by setting the correct compiler flags) to use or not use the available hardware accelerators without making changes to the actual code of the application itself.

2.2 Task 4.2: CROSSCON SoC – Initial Version

CROSSCON SoC is a system-on-chip (SoC) design, developed as part of the CROSSCON project, that provides a secure RISC-V execution environment for mixed-criticality IoT devices that require strong security guarantees, flexibility, small code size and low power consumption. The guarantees that the CROSSCON SoC can provide are strong software isolation (through virtualization-based trusted execution environments (TEEs)) with the ability to share hardware (HW) modules connected to the SoC interconnect between TEEs without compromising isolation guarantees.

Related repo https://github.com/crosscon/crosscon_soc [3].This repository contains the initial version of the CROSSCON SoC with (1) BA51-H core (highly configurable, low-power, deeply embedded 32-bit RISC-V processor with efficient virtualization support without virtual memory), (2) the first HW implementation of unified (2-stage) S-mode Physical Memory Protection (SPMP) RISC-V extension, and (3) a prototype implementation of Perimeter guard (PG), a HW module that can be used to share HW modules connected to the SoC interconnect between isolated domains.

2.3 Task 4.2: Spike (RISC-V) Simulator Extended with Unified SPMP Extension

Spike is a RISC-V ISA simulator [4] that provides a functional model for RISC-V cores and is generally considered as a golden model of the RISC-V specification. It allows one to run RISC- V programs with a variety of different RISC-V extensions, including the RV32I, PMP, and Hypervisor extension.

Related repo https://github.com/crosscon/riscv-isa-sim [5]. This repository contains the Spike simulator extended with a reference implementation of unified SPMP extension: one of the suggested approaches for how to extend the SPMP model [6], so that it can also be used by the hypervisor. The unified SPMP extensions was suggested to the RISC-V community as part of the CROSSCON project. The extended Spike can be used as a reference execution environment for the BA51-H core.

2.4 Task 4.3: Trusted Anchor for vFPGA – Initial Version

Field Programmable Gate Arrays (FPGAs) have become integral components in modern computing environments due to their adaptability and computing capabilities. As part of WP4, we explore the advancements and challenges in sharing FPGA resources among applications or users. Particularly, we are interested in extending trusted execution environment to FPGAs while providing IP protection for hardware designs configured on the FPGA.

Related repo https://github.com/crosscon/FPGA_TEE [7]. This repository contains the initial, proof of concept, implementation of Secure FPGA Provisioning system that provides secure FPGA-based acceleration and enable IP protection on FPGA-enabled SoCs within CROSSCON Stack. An important step toward this task is to design and implement the FPGA shell in the FPGA fabric, which is responsible for configuring the rest of the FPGA fabric at runtime. We provide a demonstrator, where the FPGA fabric is partitioned into two virtual FPGAs and the FPGA shell. The FPGA shell is responsible for partial reconfiguration of the virtual FPGAs at runtime with different accelerators through the internal configuration port.

3 Conclusion

This deliverable D4.2 contains the initial implementation results of the work done as part of WP4 described in D4.1 “CROSSCON Extensions to Domain Specific Hardware Architectures Documentation — Draft” [8]. The provided artifacts are an important and a necessary step towards developing a final version of the solutions as they require that the solutions are implemented and tried out, which provides an opportunity for evaluation. The artifacts will be refined and improved to achieve greater maturity and further extended with new functionality designed as part of the future work in WP4 aimed towards MS8 “Final version of the CROSSCON stack components and extension primitives, and extended testbed”.

References

[1] "**CROSSCON project GitHub repository**" [Online]. Available: https://github.com/crosscon. [Accessed April 2024].

[2] "**Crypto API Demonstrator**" April 2024. [Online]. Available: https://github.com/crosscon/crypto_API_demonstrator.

[3] "**CROSSCON SoC**" April 2024. [Online]. Available: https://github.com/crosscon/crosscon_soc.

[4] "**Spike RISC-V ISA Simulator**" [Online]. Available: https://github.com/riscv-software-src/riscv-isa-sim. [Accessed April 2024].

[5] "**Extended Spike (RISC-V ISA) simulator**" April 2024. [Online]. Available: https://github.com/crosscon/riscv-isa-sim.

[6] "**RISC-V SPMP Extension**" [Online]. Available: https://github.com/riscv/riscv-spmp. [Accessed April 2024].

[7] "**FPGA TEE**" April 2024. [Online]. Available: https://github.com/crosscon/FPGA_TEE.

[8] **CROSSCON** *"D4.1 CROSSCON Extensions to Domain Specific Hardware Architectures Documentation — Draft"*, Putrle Žiga, Zeitouni Shaza. 2024.