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

D3.2 CROSSCON Open Security Stack – Initial Version

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

Related WP	WP3	**Document Reference**	D3.2
Related Deliverable(s)	D3.1	**Dissemination Level (*)**	PU
Lead Participant	UMINHO	**Lead Author**	Sandro Pinto
Contributors	UMINHO, UNITN, UWU, TUD	**Reviewers**	ATOS BIOT

Keywords:
CROSSCON Hypervisor, TEE Isolation, CROSSCON Trusted Services,

This document is issued within the frame and for the purpose of the CROSSCON project. This project has received funding from the European Union's Horizon Europe Programme under Grant Agreement No.101070537. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

The dissemination of this document reflects only the author's view, and the European Commission is not responsible for any use that may be made of the information it contains. This deliverable is subject to final acceptance by the European Commission.

This document and its content are the property of the CROSSCON Consortium. The content of all or parts of this document can be used and distributed provided that the CROSSCON project and the document are properly referenced.

Each CROSSCON Partner may use this document in conformity with the CROSSCON Consortium Grant Agreement provisions.

(*) Dissemination level: **(PU)** Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page). **(SEN)** Sensitive, limited under the conditions of the Grant Agreement. **(Classified EU-R)** EU RESTRICTED under the Commission Decision No2015/444. **(Classified EU-C)** EU CONFIDENTIAL under the Commission Decision No2015/444. **(Classified EU-S)** EU SECRET under the Commission Decision No2015/444.

Document Information

List of Contributors	
Name	**Partner**
Sandro Pinto	UMINHO
David Cerdeira	UMINHO
João Sousa	UMINHO
Luís Cunha	UMINHO
Bruno Crispo	UNITN
Michele Grisafi	UNITN
Marco Roveri	UNITN
Alberto Tachella	UNITN
Tommasco Zoppi	UNITN
Lukas Petzi	UWU
Peter Ten	UWU
Hristo Koshutanski	ATOS
Shaza Zeitouni	TUD

Document History			
Version	**Date**	**Change editors**	**Changes**
0.1	24/04/2024	João Sousa (UMINHO) David Cerdeira (UMINHO) Luís Cunha (UMINHO) Sandro Pinto (UMINHO)	Initial contributions.
0.2	30/04/2024	Sandro Pinto, João Sousa (UMINHO)	Final version for QA
0.9	30/04/2024	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	Sandro Pinto (UMINHO)	30/04/2024
Quality manager	Juan Alonso (ATOS)	30/04/2024
Project Coordinator	Hristo Koshutanski (ATOS)	30/04/2024

Table of Contents

List of Acronyms

Abbreviation / acronym	Description
D3.1	Deliverable number 1 belonging to WP3
D3.2	Deliverable number 2 belonging to WP3
EC	European Commission
IoT	Internet of Things
MS4	4th Milestone
MS8	8th Milestone
SoC	System-on-Chip
TEE	Trusted Execution Environment
FPGA	Field-Programmable Gate Arrays
PUF	Physical Unclonable Function
TRL3	Technology Readiness Level 3
WP	Work Package

Executive Summary

The deliverable D3.2 contains the initial implementation results of work done as part of WP3 described in D3.1 “CROSSCON Open Security Stack Documentation - Draft”. It includes (1) the initial implementation of the CROSSCON TEE Isolation, (2) CROSSCON Hypervisor, and (3) the status of CROSSCON Trusted Services, particularly the first proof of concept implementation of the PUF-based authentication service and initial version of Secure FPGA Provisioning. 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 D3.2 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 WP3 described in D3.1 “CROSSCON Open Security Stack Documentation - Draft” 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. The open-source reference implementation and related documentation will be accessible in the GitHub repository.

1.2 Relation to other project work

This document is closely related to the deliverable D3.1, “CROSSCON Open Security Stack Documentation - Draft”, as it contains the actual implementation results described in D3.1. 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

This document is composed of one chapter containing multiple sections. Each section contains a short description of a WP3 task with a reference to the respective repository. Each repository encompasses an extended description, the current implementation, and instructions on how to use it.

2 WP3: CROSSCON Stack Development

Within WP3, several tasks aim to develop essential components of the CROSSCON stack. The “D3.2 CROSSCON Open Security Stack – Initial Version” will provide the software, technical diagrams, and algorithms of the experimental proof of concept of the CROSSCON stack components developed by these tasks. The open-source reference implementation and related documentation will be accessible in the GitHub repository [1].

2.1 Task 3.1 - CROSSCON TEE Abstraction and Isolation – Initial Version:

The goal of this task is twofold. The first involves identifying potential gaps in the global platform internal core API specification. The second is enhancing TEE isolation capabilities by enabling the decomposition of trusted services into multiple isolated execution environments, i.e., multiple trusted OS instances.

CROSSCON TEE Isolation https://github.com/crosscon/CROSSCON-Hypervisor-and-TEE-Isolation-Demos [2]. This repo includes the source code of TEE isolation features to decompose trusted services from trusted kernels for APU devices. Currently it demonstrates the use of CROSSCON hypervisor to execute the OP-TEE trusted OS in a VM alongside a Linux VM in both RISC-V and Arm in their respective qemu-virt emulation platforms.

2.2 Task 3.2 - CROSSCON Hypervisor – Initial Version:

The goal of this task is to develop novel hypervisor mechanisms to address static partitioning hypervisor limitations, enabling dynamic VM creation and management, as well as per-VM TEE services support.

Related Repo https://github.com/crosscon/CROSSCON-Hypervisor[3]. This repo includes the source code of CROSSCON hypervisor. CROSSCON hypervisor is based on Bao static partitioning hypervisor to reach a broad range of devices and architectures. CROSSCON Hypervisor provides the following additional features compared to Bao: (i) dynamic VM Creation and management and (ii) per-VM TEE.

2.3 Task 3.3 - CROSSCON New Trusted Services:

The goal of this task is to define and implement new trusted services to enhance the security and functionality of the CROSSCON stack.

2.3.1 PUF Based Authentication – Initial Version

Related Repo https://github.com/crosscon/crosscon_puf_authentication[4]. This repository contains the initial, proof of concept, implementation of our PUF-based authentication service provided as part of the CROSSCON stack. The repository consists of three distinctive authentication schemes offering different functionality and security features.

2.3.2 Secure FPGA Provisioning – Initial Version

Related repo https://github.com/crosscon/FPGA_TEE [5]. 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.

2.4 Task 3.4 - CROSSCON Toolchain:

The goal of this task is to develop a toolchain to enable the implementation of an update mechanism that preserves the CROSSCON security and safety policies.

Related Repo https://github.com/crosscon/RIOT [6]. This repo includes a fork of the RIOT Operating System, integrated with an initial implementation of the new security update mechanism.

2.5 Task 3.5 - CROSSCON Baremetal-TEE:

The goal of this task is to design and develop a software-based TEE for the bare-metal devices. Given the high heterogeneity of bare-metal devices, we propose two different versions of the TEE: one compatible with MPU-enabled devices (MPU-version) and one with those devices lacking such a hardware (nonMPU-version). The TEE will ensure the basic security primitives such as privilege separation and memory isolation.

Related Repo https://github.com/crosscon/baremetal-tee [7]. This repo includes the source code of both versions of the CROSSCON baremetal-TEE.

3 Conclusion

This report presents the initial implementation of the work carried out in WP3 and detailed in D3.1 "CROSSCON Open Security Stack Documentation - Draft." In document D3.1, we comprehensively cover the CROSSCON Stack, encompassing CROSSCON TEE isolation, Hypervisor, Toolchain, Bare-metal TEE as well as five novel trusted services. However, it's important to note that some components have yet to attain TRL3 status. As a result, this document does not include repos on three of the novel trusted services: "Behavioural-based," "Control Flow Integrity," and "Remote Attestation." These artifacts are a crucial step toward the development of the final solution, as they require implementation and testing for evaluation. The artifacts will continue to be refined and improved to increase their maturity, and new functionality will be added as part of WP3's future work aimed at achieving 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] **“CROSSCON Hypervisor and TEE Isolation Demos,"** [Online]. Available: https://github.com/crosscon/CROSSCON-Hypervisor-and-TEE-Isolation-Demos. [Accessed April 2024].

[3] **“CROSSCON Hypervisor,”** [Online]. Available: https://github.com/crosscon/CROSSCON-Hypervisor. [Accessed April 2024].

[4] **“PUF-Based Authentication Proof of Concept Implementation,"** [Online]. Available: https://github.com/crosscon/crosscon_puf_authentication. [Accessed April 2024].

[5] **“Secure FPGA Provisioning,"** [Online]. Available: https://github.com/crosscon/FPGA_TEE. [Accessed April 2024].

[6] “**RIOT**” [Online]. Available: https://github.com/crosscon/RIOT [Accessed April 2024]

[7] “**Bare-metal TEE**” [Online]. Available: https://github.com/crosscon/baremetal-tee [Accessed April 2024]