CROSSCON: Interoperable IoT Security Stack for Embedded Connected Devices

Luís Cunha, Tiago Gomes
University of Minho, PORTUGAL

CROSSCON & (secure) Friends
RISC-V Summit EU 2024 - Side Event 1

RISC-V Summit EU 2024
24-28, June 2024, Munich, Germany

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

UNIVERSIDADE DO MINHO

Agenda

- CROSSCON Project
  - Motivations
  - Objectives
- CROSSCON Approach
- Development of the CROSSCON Security Stack
- Project Status & Roadmap
- Use Cases

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

CROSSCON

- **Project Name:** Cross-platform Open Security Stack for Connected Devices
- **Project Call:** HORIZON-CL3-2021-CS-01
- **GA Number:** 101070537
- **Budget:** 4.6M €
- **Duration:** 36 Months (Nov-2022 to Oct-2025)
  - **We are currently on M20**
- **Consortium:** 11 Members (8 countries)
- **Project Coordinator:** Hristo Koshutanski (ATOS)
- **Scientific Coordinator:** Bruno Crispo (UNITN)
- **Exploitation Coordinator:** Aljosa Pasic (ATOS)

Large Industry

Atos

Research Institutes and Universities

Università di Trento

Universidade do Minho

Julius-Maximilians-Universität Würzburg

Technische Universität Darmstadt

SMEs

SEARCH-LAB Security Evaluation Analysis and Research Laboratory

barbara

Beyond Semiconductor

3MDEB

CYSEC

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

Motivations

- **Current IoT device's landscape is quite fragmented…**
- **When it comes to security, it lacks:**
  - **Open-Source Hardware Solutions**
    - Most IoT solutions rely on proprietary hardware with closed-source licence, limiting innovation and collaboration between research teams;
  - **Root-of-Trust (RoT) sources and Chain-of-Trust (CoT) verification methods**
    - Compromising overall device's security
  - **Interoperability Between IoT Devices**
    - Security solutions are not interchangeable

- **Causing high engineering costs in developing Trusted Services**

- **While handling with several vulnerabilities in core Trust Components**

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

CROSSCON Objectives

- Design a new **open, modular, highly portable, and vendor independent** IoT security stack that can run on a wide range of embedded devices;
- Provide a stronger memory protection and isolation in both **new and existing TEEs** to mitigate the impact of current cybersecurity threats;
- Enhance common trusted services offered by TEEs, while providing new ones;

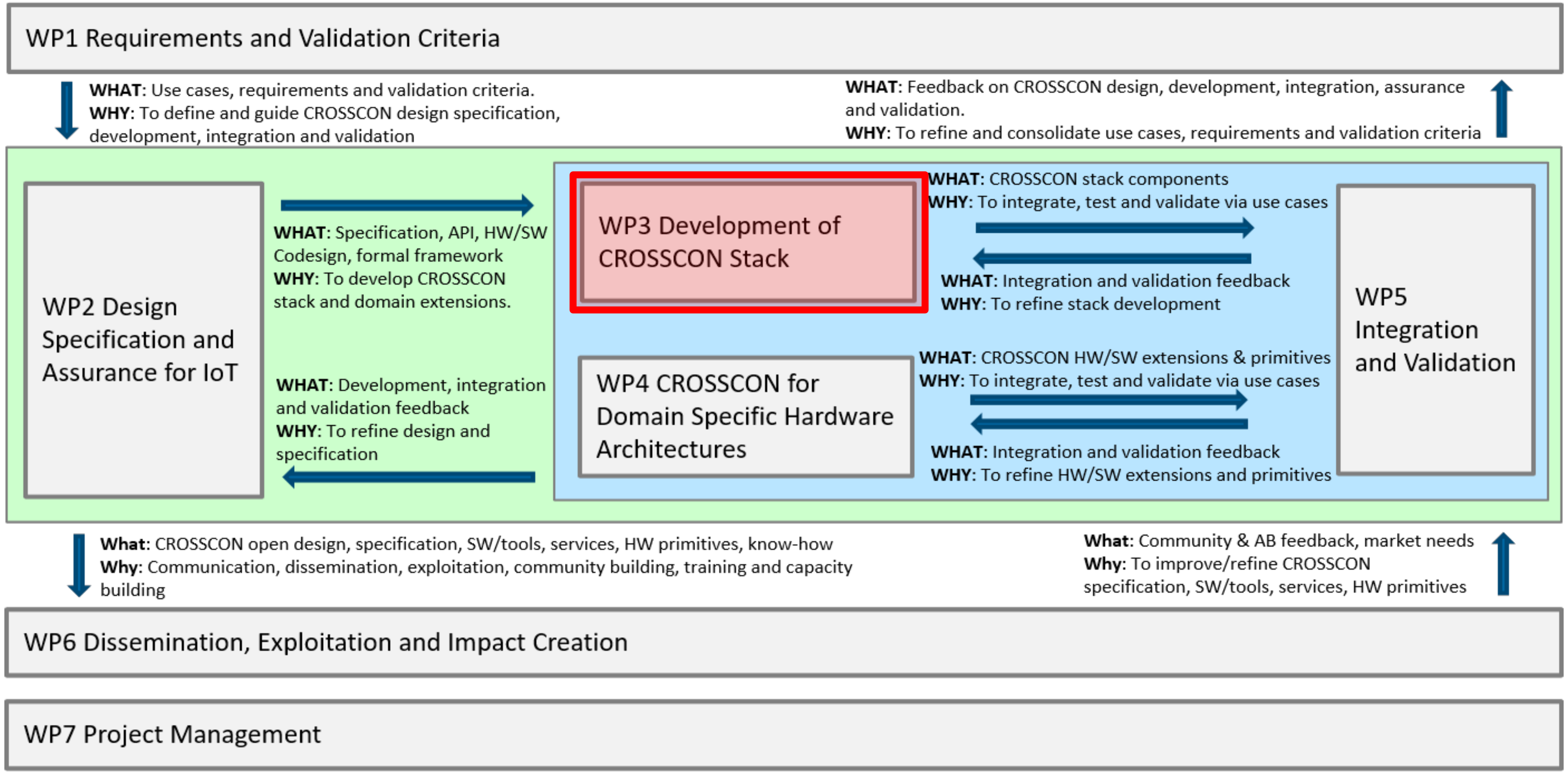
CROSSCON envisions a secure ecosystem where security starts at RoT and extends to all CoT components;

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101070537

CROSSCON Approach

7 Work Packages (WPs) allocated to different project leaders:

- WP1 Leader: ATOS
- WP2 Leader: UNITN
- WP3 Leader: UMINHO
- WP4 Leader: BEYOND
- WP5 Leader: SLAB
- WP6 Leader: ATOS
- WP7 Leader: ATOS



WP1 Requirements and Validation Criteria

WHAT: Use cases, requirements and validation criteria.
WHY: To define and guide CROSSCON design specification, development, integration and validation

WHAT: Feedback on CROSSCON design, development, integration, assurance and validation.
WHY: To refine and consolidate use cases, requirements and validation criteria

WP2 Design Specification and Assurance for IoT

WHAT: Specification, API, HW/SW Codesign, formal framework
WHY: To develop CROSSCON stack and domain extensions.

WHAT: Development, integration and validation feedback
WHY: To refine design and specification

WP3 Development of CROSSCON Stack

WHAT: CROSSCON stack components
WHY: To integrate, test and validate via use cases

WHAT: Integration and validation feedback
WHY: To refine stack development

WP4 CROSSCON for Domain Specific Hardware Architectures

WHAT: CROSSCON HW/SW extensions & primitives
WHY: To integrate, test and validate via use cases

WHAT: Integration and validation feedback
WHY: To refine HW/SW extensions and primitives

WP5 Integration and Validation

What: CROSSCON open design, specification, SW/tools, services, HW primitives, know-how
Why: Communication, dissemination, exploitation, community building, training and capacity building

What: Community & AB feedback, market needs
Why: To improve/refine CROSSCON specification, SW/tools, services, HW primitives

WP6 Dissemination, Exploitation and Impact Creation

WP7 Project Management

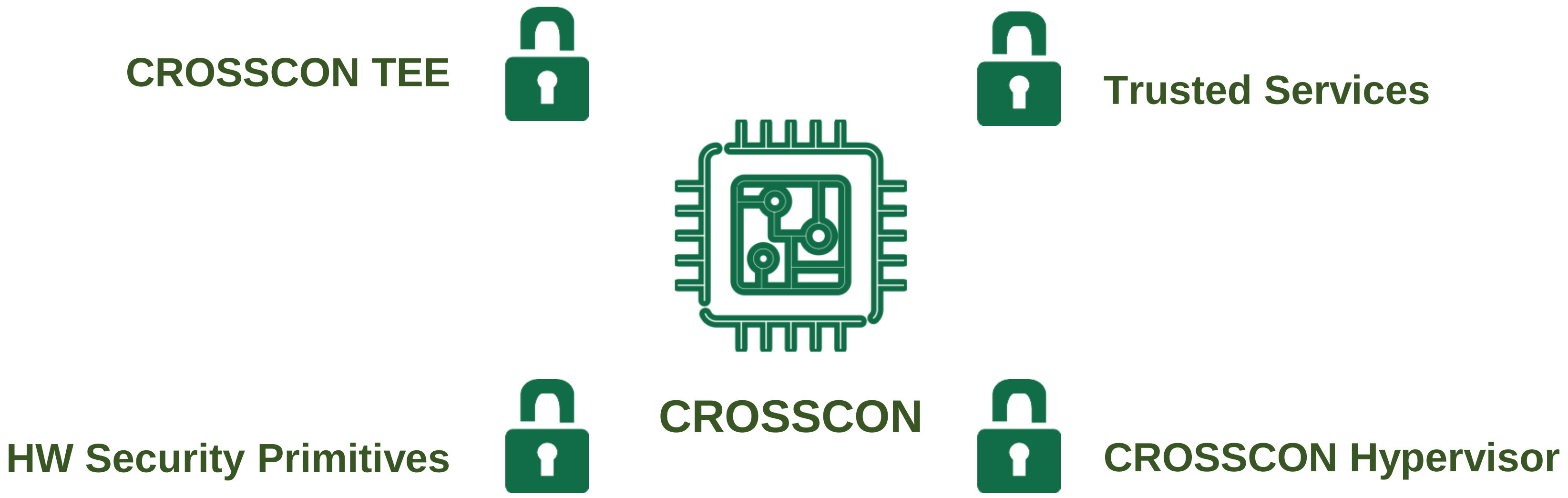
Workload allocation.

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

CROSSCON Security Stack Components

CROSSCON TEE to provide **suitability and interoperability** through isolation capabilities and covering several TEE models, architectures, and implementations;

Baseline Trusted Services: Control Flow Attestation; Firmware Update; Remote Attestation; Secure Boot; **New Trusted Services:** PUF-Based Authentication; MFA - Context-based Authentication;



CROSSCON TEE

Trusted Services

CROSSCON

HW Security Primitives

CROSSCON Hypervisor

Hardware security mechanisms that provide security guarantees to non-CPU hardware components;

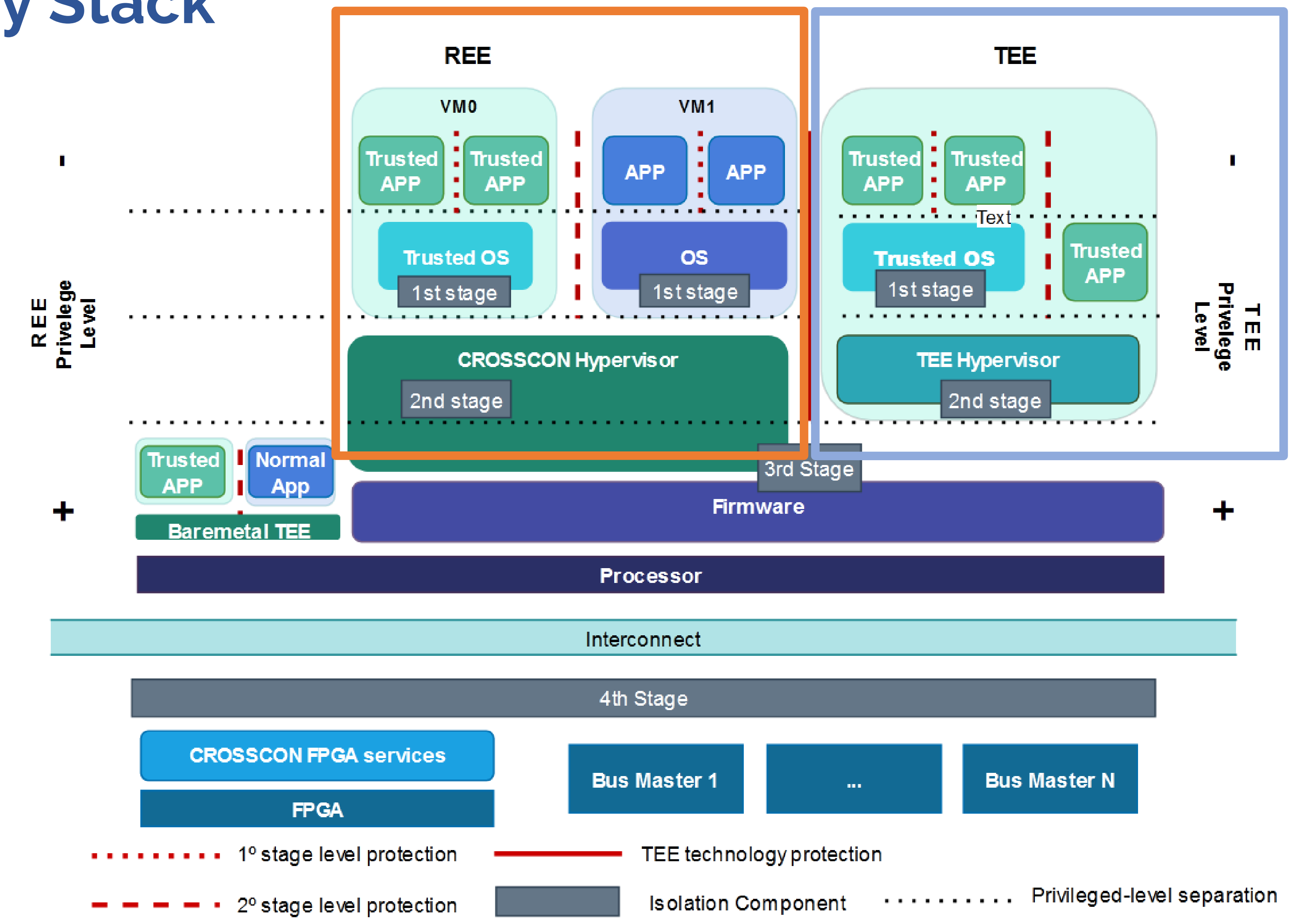
CROSSCON Hypervisor will be implemented based on Bao Hypervisor. Bao Hypervisor (Cross-Platform Open-source Static Partitioning Hypervisor);

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101070537

CROSSCON Security Stack abstraction model

Goals:

- Extend **interoperability** across heterogeneous devices;
- Offer a unified level of **abstraction** across **multiple hardware platforms**;
- Enrich existing **security** features by adding **new trusted services**;



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

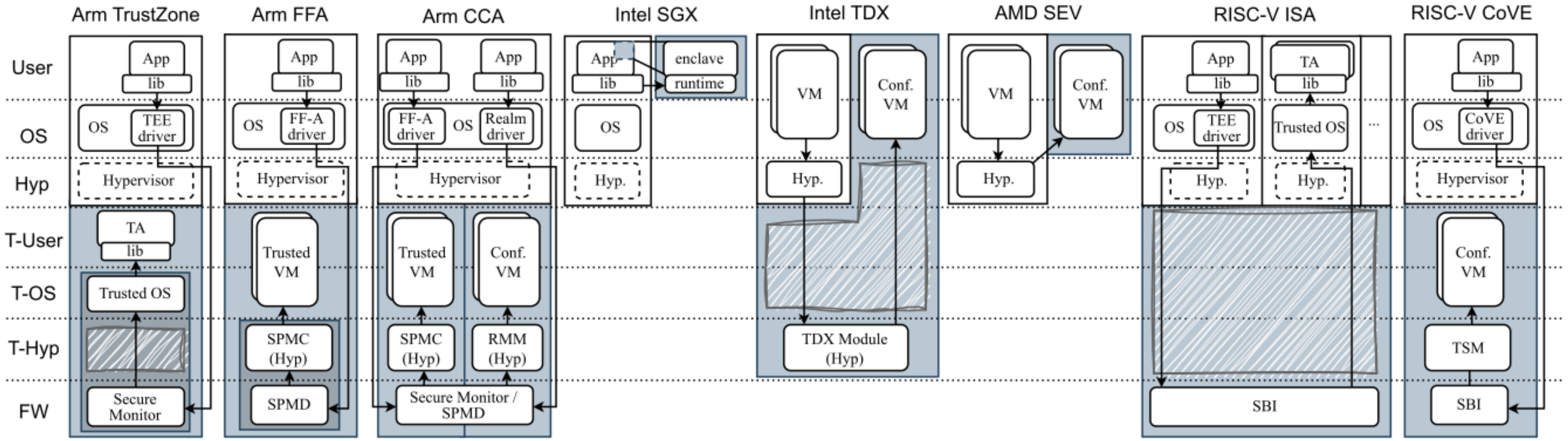
TEE Isolation and Interoperability – Limitations & Opportunity

TEE Isolation issues

- Architectural (TZ secure world excess of privileges)
- Implementation (secure monitor/trusted kernel/TAs bugs)
- Microarchitectural (side-channels)

TEE Interoperability issues

- Compatibility
- Reusability
- Fragmentation



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

TEE Isolation and Interoperability – CROSSCON Novelty

- **Virtualization-based TEE (AnyTEE)**

(Leveraging widespread HW virtualization Primitives)

- **Software-defined TEE**

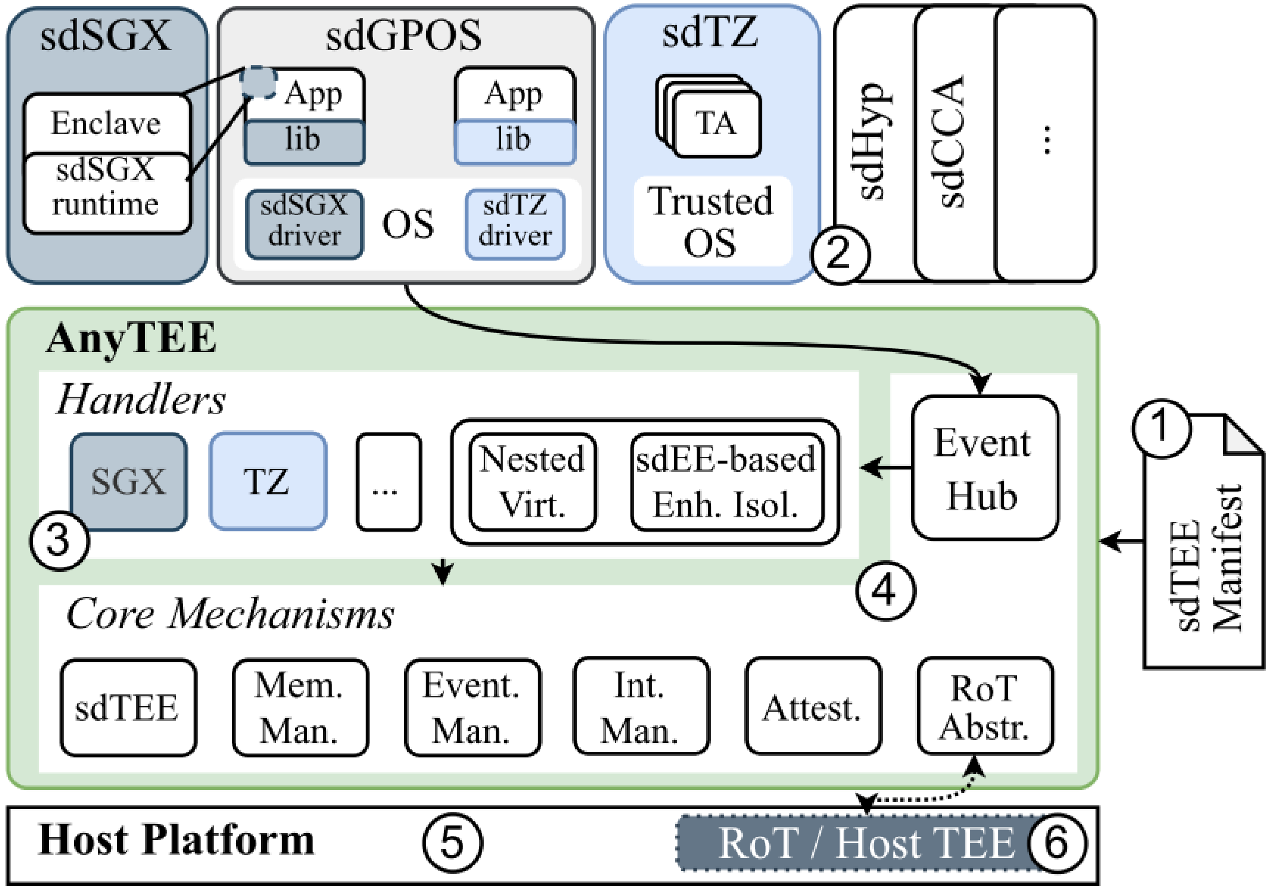
(TEE emulation and customization)

- **Multiple TEE Programming Models**

(Arm TrustZone, Intel SGX,)

- **Multiple Architectures**

(Arvm8-A, RV32/64H)

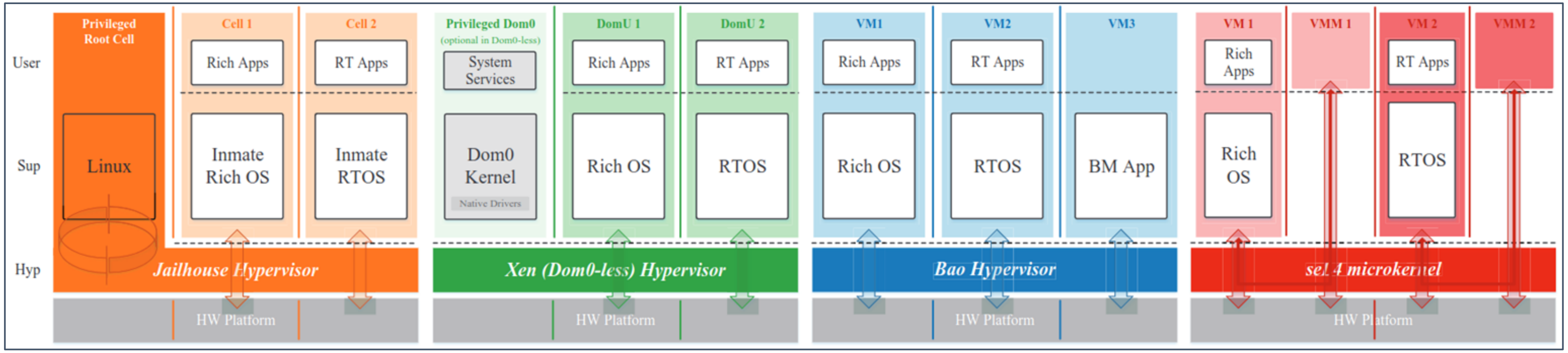


This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

CROSSCON Hypervisor – State-of-the-Art on SPHs

Analyzed:

- Jailhouse
- Xen (Dom0-less)
- Bao
- CAmkES (seL4)



Criteria: open-source and TCB size!

Conclusion:

Bao provides lower latencies, interference mitigation, smallest code base, and best scalability across Application, Real-Time and Microcontroller (WIP) class CPUs (from different architectures);

J. Martins and S. Pinto, "Shedding Light on Static Partitioning Hypervisors for Arm-based Mixed-Criticality Systems," in 2023 IEEE 29th Real-Time and Embedded Technology and Applications Symposium (RTAS), San Antonio, TX, USA, 2023 pp. 40-53.

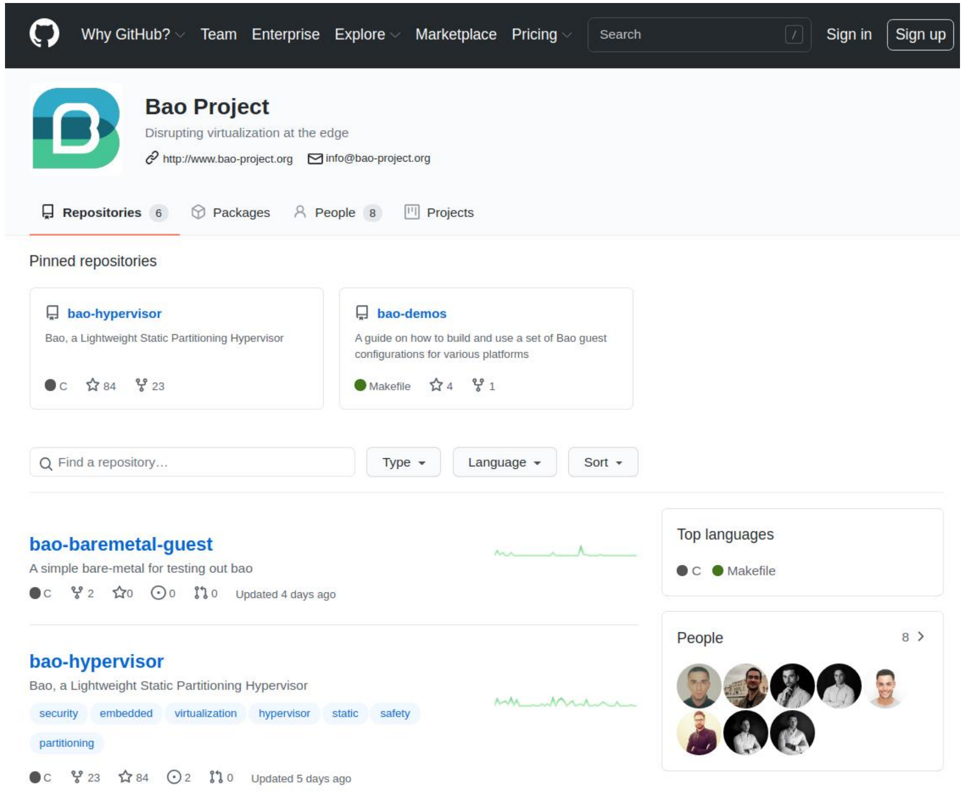
This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101070537

CROSSCON Hypervisor - Bao Hypervisor

https://github.com/crosscon

Fork from Bao Hypervisor

- Type-1 / Bare-metal
- Static Partitioning Architecture:
  - 1:1 vCPU-to-pCPU mapping
  - Static memory assignment
- Hardware-assisted
- Inter-VM communication
- Cache side-channel protection (cache-coloring)
- No Dependencies (libraries / OS)



Bao Project

Disrupting virtualization at the edge

http://www.bao-project.org info@bao-project.org

Pinned repositories

bao-hypervisor

Bao, a Lightweight Static Partitioning Hypervisor

● C ☆ 84 23

bao-demos

A guide on how to build and use a set of Bao guest configurations for various platforms

● Makefile ☆ 4 1

bao-baremetal-guest

A simple bare-metal for testing out bao

● C 2 ☆0 0 0 Updated 4 days ago

bao-hypervisor

Bao, a Lightweight Static Partitioning Hypervisor

● C 23 ☆ 84 2 0 Updated 5 days ago

Top languages

● C ● Makefile

People 8 >

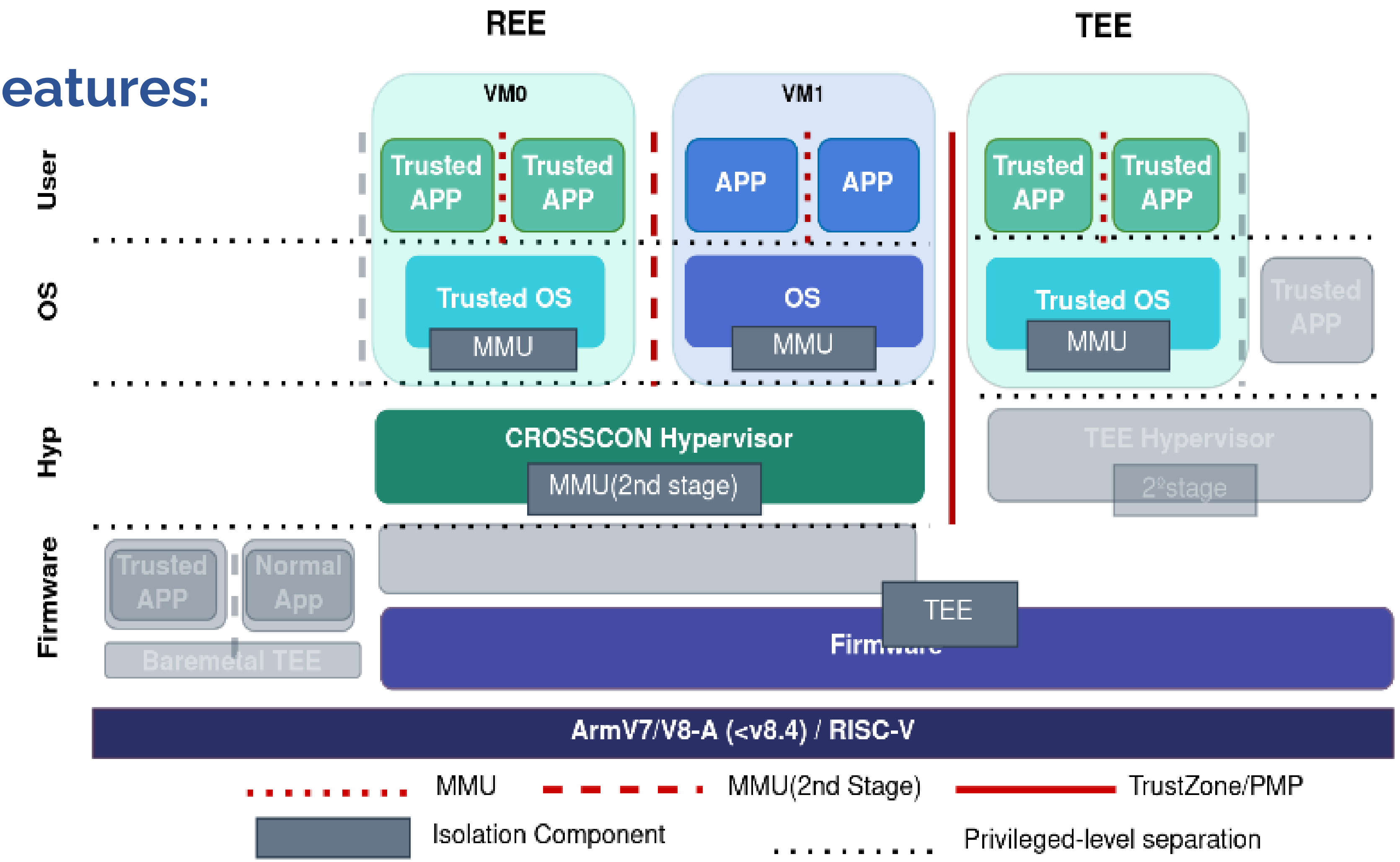
https://github.com/bao-project

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

CROSSCON Hypervisor

CROSSCON Hypervisor Features:

- Dynamic VM instantiation
- Per-VM TEE

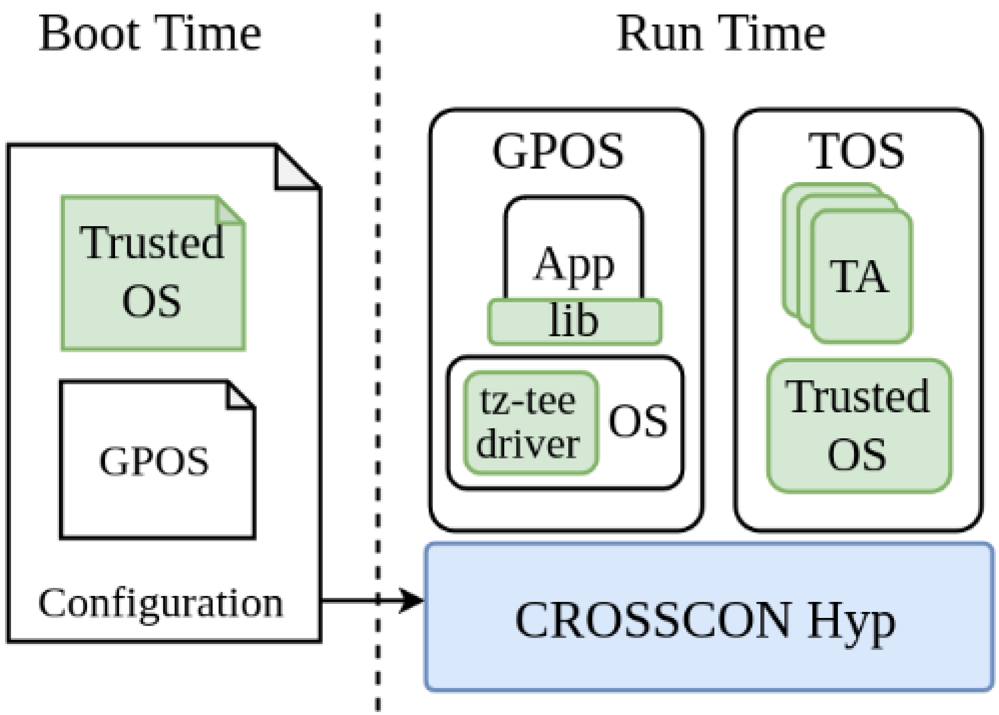


This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Project Status & Roadmap

Integration with the open-source trusted kernel OP-TEE (over Arm or RISC-V):

- OP-TEE follows the TZ programming model
- CROSSCON Hypervisor can host OP-TEE in a VM
- Two VMs: GPOS VM and Trusted OS VM (OP-TEE)
- It is possible to run OP-TEE out-of-the-box on Arm platforms without TZ (e.g, RPI4), or even RISC-V

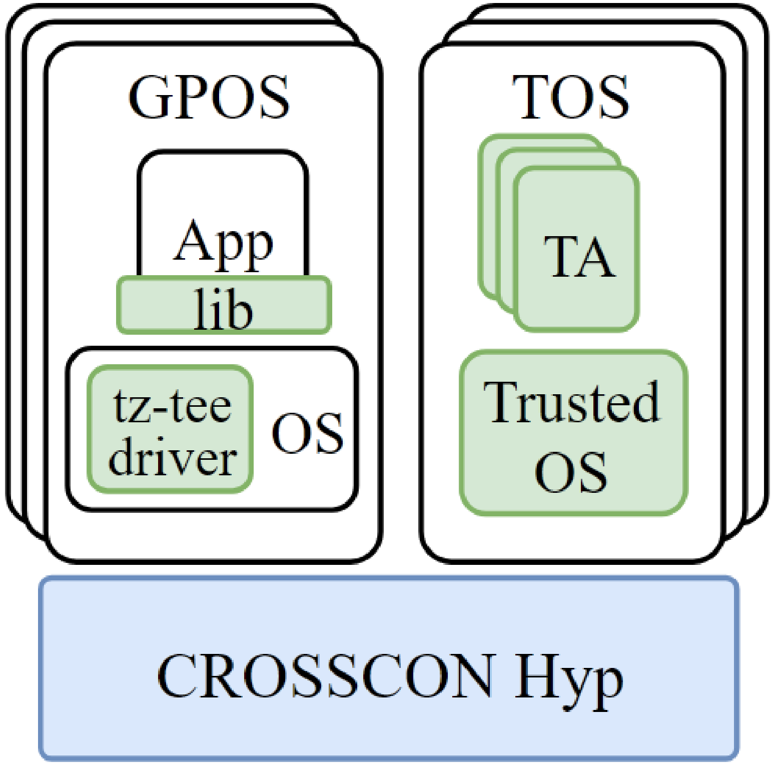


This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Project Status & Roadmap

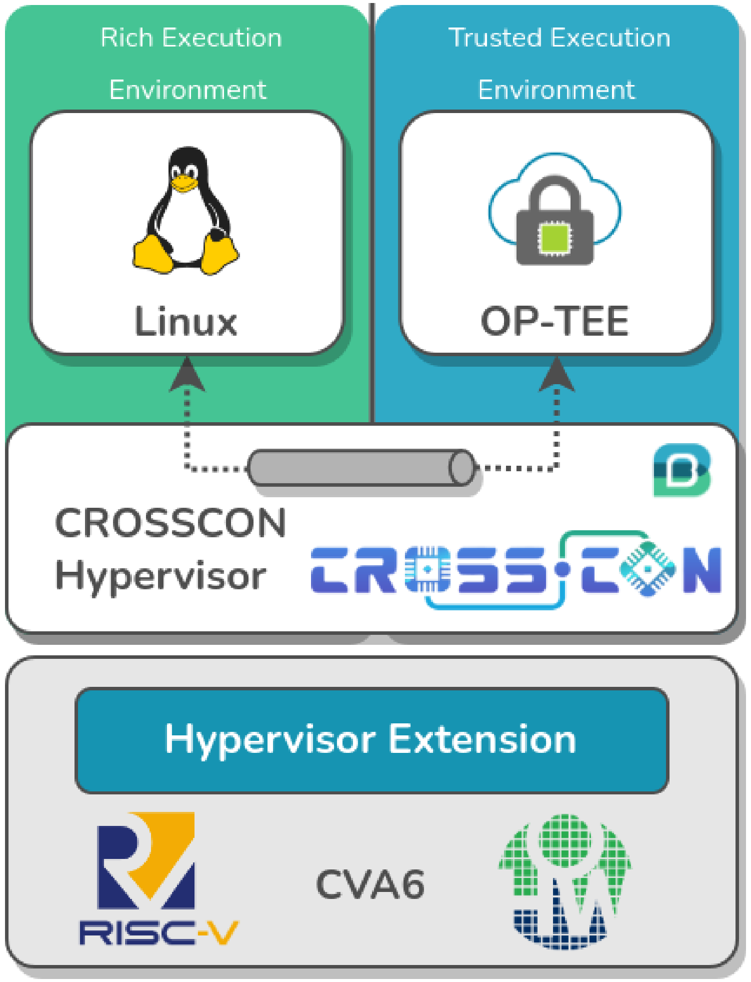
Integration with the open-source trusted kernel OP-TEE (over Arm or RISC-V):

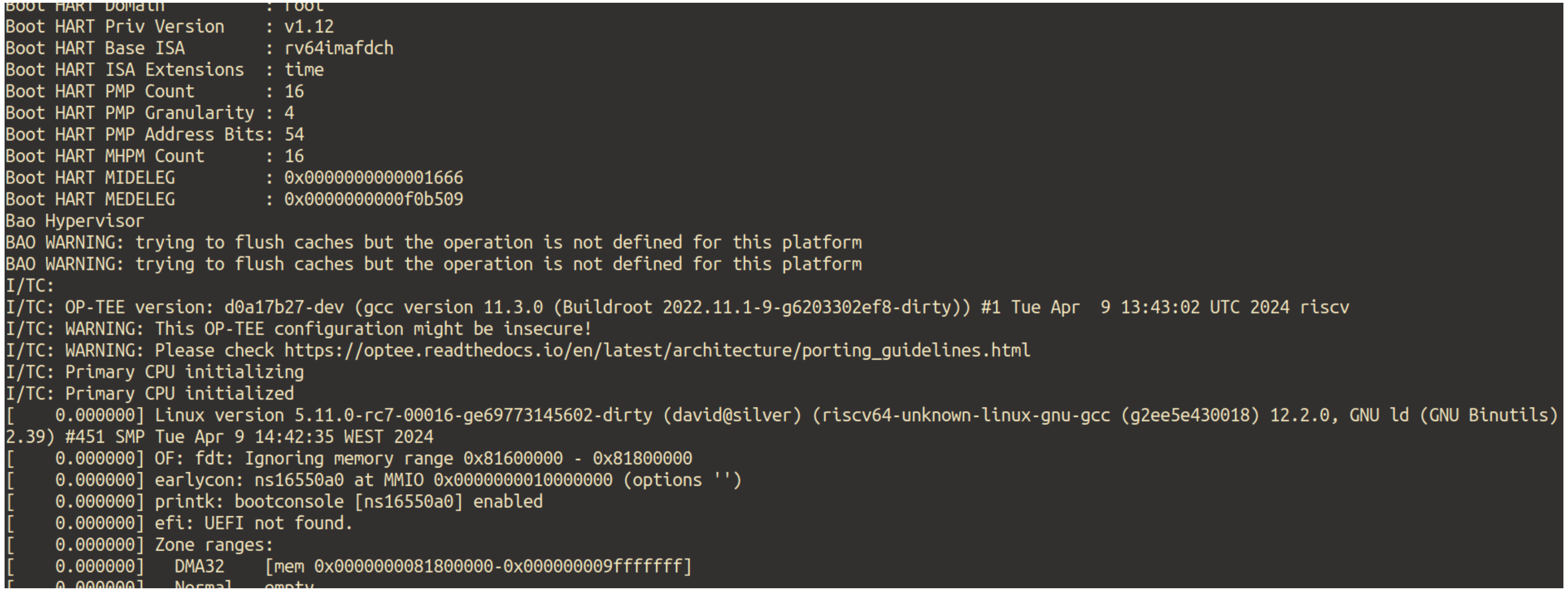
- OP-TEE follows the TZ programming model
- CROSSCON Hypervisor can host OP-TEE in a VM
- Two VMs: GPOS VM and Trusted OS VM (OP-TEE)
- It is possible to run OP-TEE out-of-the-box on Arm platforms without TZ (e.g, RPI4), or even RISC-V
- Enables per-VM TEE services, splitting a single TEE system into multiple isolated TEEs.



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

Project Status & Roadmap





```
Boot HART Domain          : root
Boot HART Priv Version    : v1.12
Boot HART Base ISA        : rv64imafdch
Boot HART ISA Extensions  : time
Boot HART PMP Count       : 16
Boot HART PMP Granularity : 4
Boot HART PMP Address Bits: 54
Boot HART MHPM Count      : 16
Boot HART MIDELEG         : 0x0000000000001666
Boot HART MEDELEG         : 0x0000000000f0b509
Bao Hypervisor
BAO WARNING: trying to flush caches but the operation is not defined for this platform
BAO WARNING: trying to flush caches but the operation is not defined for this platform
I/TC:
I/TC: OP-TEE version: d0a17b27-dev (gcc version 11.3.0 (Buildroot 2022.11.1-9-g6203302ef8-dirty)) #1 Tue Apr  9 13:43:02 UTC 2024 riscv
I/TC: WARNING: This OP-TEE configuration might be insecure!
I/TC: WARNING: Please check https://optee.readthedocs.io/en/latest/architecture/porting_guidelines.html
I/TC: Primary CPU initializing
I/TC: Primary CPU initialized
[    0.000000] Linux version 5.11.0-rc7-00016-ge69773145602-dirty (david@silver) (riscv64-unknown-linux-gnu-gcc (g2ee5e430018) 12.2.0, GNU ld (GNU Binutils)
2.39) #451 SMP Tue Apr 9 14:42:35 WEST 2024
[    0.000000] OF: fdt: Ignoring memory range 0x81600000 - 0x81800000
[    0.000000] earlycon: ns16550a0 at MMIO 0x0000000010000000 (options '')
[    0.000000] printk: bootconsole [ns16550a0] enabled
[    0.000000] efi: UEFI not found.
[    0.000000] Zone ranges:
[    0.000000]   DMA32    [mem 0x0000000081800000-0x000000009fffffff]
[    0.000000]   Normal   empty
```

Try this demo:

☆ **https://github.com/crosscon**

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

Project Status & Roadmap

Next Steps:

- CROSSCON Stack development encompasses trusted services.

  - Trusted services complement existing platform mechanisms (e.g., secure boot, remote attestation, cryptographic and secure storage)

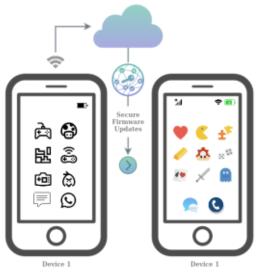
  - Next steps are design, implement, and validate: PUF- and context-based authentication, control flow integrity and secure firmware updates.

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

Use-Cases of the CROSSCON stack

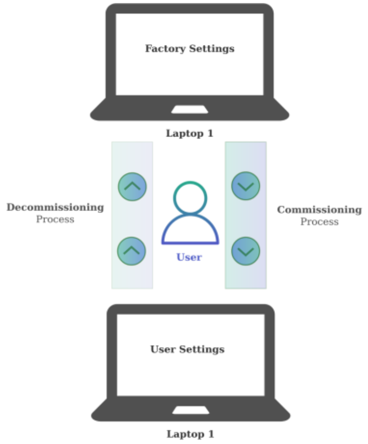
UC1: Device Multi-Factor Authentication

Introduce new authentication methods based on context and behavioral authentication



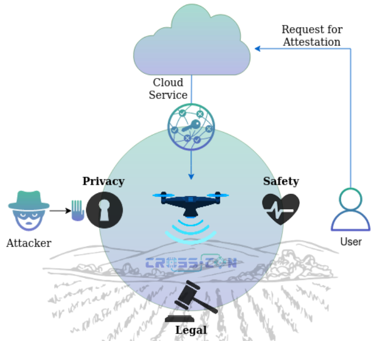
UC2: Firmware Updates of IoT Devices

Deploy secure firmware updates Over-The-Air (OTA).



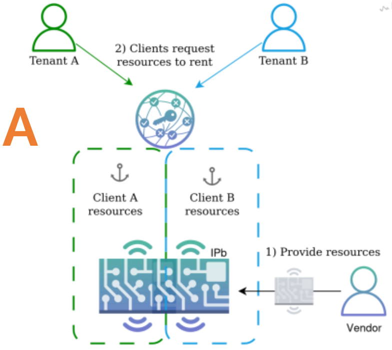
UC3: Commissioning and Decommissioning of IoT devices.

Implement robust commissioning and decommissioning procedures for applications, ensuring the highest levels of security and reliability in IoT device operations.



UC4: Remote Attestation for Identification and Integrity Validation of Agricultural Unmanned Aerial Vehicles (UAVs)

Provide secure remote attestation on agricultural UAVs.



UC5: Intellectual Property Protection for Secure Multi-Tenancy on FPGA

Provide secure multi-tenancy, assuring that the workload of one tenant cannot interact with others (or affect the hardware resources)

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101070537

Thank You!

Questions?

crosscon.eu
contact@crosscon.eu

Follow our project updates:

Atos

UNIVERSITÀ DI TRENTO

Universidade do Minho

SEARCH-LAB
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY

barbara

Julius-Maximilians-
UNIVERSITÄT WÜRZBURG

TECHNISCHE UNIVERSITÄT DARMSTADT

BEYOND SEMICONDUCTOR

3MDEB

CYSEC

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

Partners and roles:

Atos - Spain - Leader of the project / website / exploitation
UniTN - Italy - Leader of design and specifications / Security of Bare-metal devices
UniMINHO - Portugal - Development of the CROSSCON Stack
S-Lab - Hungary - Testbed creation / Validation activities
3mdeb - Poland - for KPI definition and validation criteria
CYSEC - Switzerland - to validate the operation scenarios and contributing through security related tasks
Barbara - Spain - Study the Use-cases of the project
UWU - Develop of new Trusted services
TUD - Germany - Cloud-based FPGA accelerators
Beyond - Slovenia - Security and hardware relates responsibilities. Involving RISC-V architecture

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