NEWSLETTER #4

CONTENTS:

"The CROSSCON stack provides an easy way to obtain an isolated execution environment that spans the entire hardware-software stack using simple hardware primitives available on most platforms."

- Žiga Putrle, Beyond Semiconductor

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

WP4 Leader Notes

Beyond Semiconductor

The CROSSCON stack provides an easy way to obtain an isolated execution environment that spans the entire hardware-software stack using simple hardware primitives available on most platforms.

June/2025

Dear Readers,

Welcome to the fourth newsletter of the CROSSCON project. Nearly three years have passed since the start of the project, and we are working with full steam ahead towards the latest version of the CROSSCON stack that we aim to deliver as part of the next milestone (Milestone 8) for internal validation. At the same time, we are already leveraging the stack in several pilot use cases to ensure that it includes all the necessary features. It is great to see everything coming together and being used in real-world use cases. Some of our work is already available on the project's GitHub page[1], so be sure to check it out.

Milestone 8 (MS8) is an important milestone for the project, as we aim to deliver most of the stack's functionality so that it can be further validated in the following months. The release will include all the major components of the stack that we have been working on as part of WP3 and WP4. This includes the CROSSCON Hypervisor, trusted services, CROSSCON SoC, Secure FPGA provisioning, and others.

As the stack's components continue to mature, it is encouraging to see how they simplify development when applied to real-world use cases, especially as the added security can have a minimal cost in terms of hardware resources and performance. The CROSSCON stack provides an easy way to obtain an isolated execution environment that spans the entire hardware-software stack using simple hardware primitives available on most platforms. Furthermore, the stack can leverage new hardware primitives that we have designed to improve isolation and provide additional functionality through trusted services. We are excited to continue validating the stack against the use cases to ensure that all the necessary features are there and are easy to use, which is vital for the adoption of the stack by the broader community. The validation effort is well underway as part of WP5.

Žiga Putrle

Software Engineer, Beyond Semiconductor

On the dissemination and research side, CROSSCON participated in several events, including Embedded World 2025, Crypto-Chipset Security Webinar, NECS Winter School 2025, WB3C Training on cybersecurity, and SWII 2024, while publishing several scientific papers. Read more about our work and events in this newsletter and on the website.

Žiga Putrle

[1] https://github.com/crosscon

Project Updates

CROSSCON Components

As we move forward with the development of the CROSSCON stack, we're preparing to deliver the first complete internal version of the CROSSCON components as part of Milestone 8. This section gives you an overview of the current status of some CROSSCON components.

CROSSCON Hypervisor

As mention in previous Newsletter versions, CROSSCON Hypervisor aims to provide interoperability and strong isolation across wide range of heterogeneours devices (from low-end to high-end devices) of multiple architectures (e.g., RISC-V and Arm).

Current Status:
In the first half of the project, partners worked towards implementing hypervisor for high-end devices by providing features such as (i) dynamic VM and (ii) per-VM TEE. Some demonstrations are on our GitHub page to showcase its functionalities for QEMU (RISC-V & Armv8-A), for RPI4B and ZCU102 platforms. An example of its use is demonstrated in the figure below.

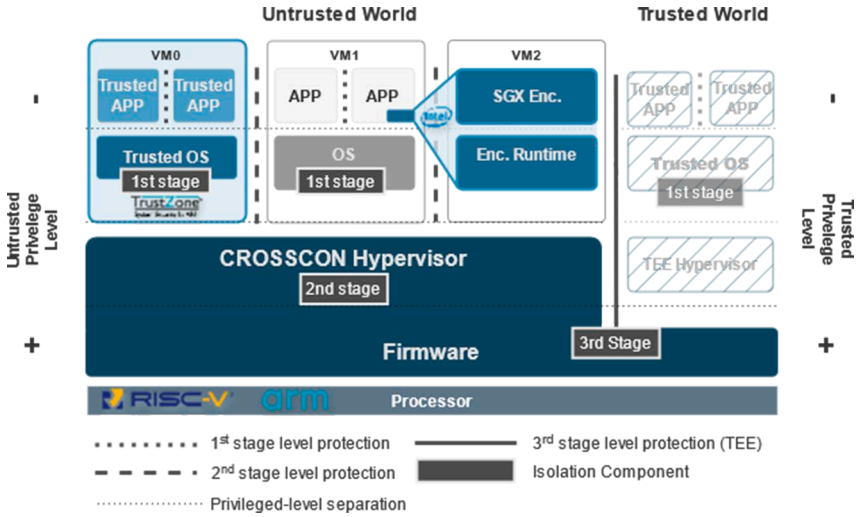


Figure 1: Unified security stack model with CROSSCON Hypervisor managing three VMs. VM1 runs a general-purpose OS, while VM2 and VM0 operate as Trusted Execution Environments (TEEs) based on different security models: Intel SGX and Arm TrustZone, respectively.

During last months, our partners have been working on CROSSCON Hypervisor for low-end devices. To enhance isolation and security guarantees, this version of CROSSCON Hypervisor uses dynamic reconfiguration capabilities of TrustZone-M controllers. Its main features are described below:

- Operates at the highest privilege level (secure privileged mode) on MCUs and relies on TrustZone-M hardware security primitives;
- Enables the creation of multiple domains in the Untrusted World, supporting not only standard applications but also TEE-based kernel components;
- Extends dual-world TrustZone-M implementations to provide multiple secure execution environments and enhanced TEE capabilities;
- Prevents privilege escalation and lateral movements across virtualized environments

Put your hands on CROSSCON Hypervisor here:
https://github.com/crosscon/CROSSCON-Hypervisor-and-TEE-Isolation-Demos

Project Updates

CROSSCON Components

PUF-based authentication service

CROSSCON is building a unified software stack for resource-constrained IoT devices, which includes a suite of modular trusted services. One of these trusted services is our PUF-based authentication service, which leverages Physical Unclonable Functions (PUFs) to give tiny devices a lightweight way to prove their identity.

Current Status:
As part of CROSSCON's efforts to provide modular and efficient trusted services, we're developing a lightweight authentication mechanism based on, e.g., Physical Unclonable Functions (PUFs). One of the services, known as AuthentiSafe, eliminates the need for centralized servers by combining PUFs with one-time signatures and distributed ledger technology. It was recently featured in a blog post[1] outlining its benefits and performance across constrained platforms, achieving authentication times as low as 0.01s.

We've open-sourced our proof-of-concept on GitHub, with three reference implementations, ZK-PUF, PAVOC and PAWOS, conducted and tested on the LPC55S69-EVK development board from NXP.

Put your hands on CROSSCON PUF-based authentication here:
https://github.com/crosscon/crosscon_puf_authentication

[1]https://crosscon.eu/blog/authentisafe-milestone-crosscon-project-iot-authentication

CROSSCON Baremetal TEE

As mentioned in the previous newsletter version, for resource-constrained devices that can't run the CROSSCON Hypervisor we've developed a software-based bare-metal TEE delivering memory isolation, privilege separation and secure cross-domain communication. Two variants cover all profiles:

- BareTEE-noMPU for MCUs without a Memory Protection Unit
- BareTEE-MPU for MCUs equipped with an MPU

Currrent Status:
Over the past few months, UMINHO and UNITN have developed a new bare-metal TEE prototype, following an approach similar to our ARMv7-M MPU-based design but now targeting RISC-V (M-mode + U-mode) on the Arty100T board and leveraging its Physical Memory Protection (PMP) unit. To demonstrate true interoperability across architectures, TEE implementations and device classes, we deployed an unmodified BitcoinWallet Trusted Application on this RISC-V TEE, fully compliant with GlobalPlatform standards. CROSSCON will present these results at RISC-V Summit Europe 2025 in Paris.

Put your hands on CROSSCON Baremetal TEE here:
https://github.com/crosscon/baremetal-tee

DISSEMINATION UPDATES

Past Events

During M24-M31, CROSSCON organized and participated in several events. Here is the summary of what hapenned!

The IoT Security Foundation Conference

23 Oct 2024 | IET, London

https://iotsecurityfoundation.org/conference/

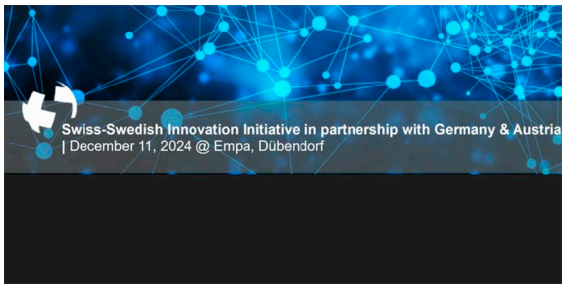
CROSSCON was present at IoTSF conference, represented by UNITN. With the theme "IoT Security: Past, Present, and Future," the event explored advancements in AI, quantum computing, and zero trust. UNITN shared CROSSCON insights and engaged with global experts to strengthen future IoT security through innovation and collaboration.

WB3C: New Technologies & Cybersecurity

5-8 Nov 2024 | Podgorica, Montenegro

https://wb3c.org/event/16

CROSSCON was represented by BEYOND at a cybersecurity workshop in Slovenia, organized with URSIV and CEP. The event addressed key topics like quantum technologies, post-quantum cryptography, AI in cybersecurity, and threat intelligence. BEYOND presented "Cybersecurity in an era of quantum technologies," highlighting CROSSCON's commitment to European cyber resilience and collaboration.



SWII 2024 I Transformational Technologies for Net-Zero Societies

11 Dec 2024 | Dübendorf, Switzerland

https://www.swii.org/index.php/transformational-technologies-for-net-zero-societies

CROSSCON was represented by CYSEC at the Transformational Technologies event held in Dübendorf, Switzerland. Focused on AI, ML, robotics, and automation for net-zero industries, the event attracted top innovators, SMEs, and research institutes. CROSSCON's presence highlighted its commitment to secure, next-generation technologies within Europe.

NECS – PhD Winter School 2025

20-24 Jan 2025 | Cortina d'Ampezzo, Italy

https://necs-winterschool.disi.unitn.it/

CROSSCON co-organized the NeCS PhD School alongside the Marie Skłodowska-Curie DUCA project, aiming to train junior researchers in cybersecurity through lectures and hands-on sessions. UMINHO participated in a presentation entitled "Virtualization-based TEE: from MCU to APU, and vice versa," highlighting the project's advancements in trusted execution technologies across several architectures and project platforms.

Embedded World 2025

11-13 Mar 2025 | Nuremberg, Germany

https://events.linuxfoundation.org/riscv-at-embedded-world/

CROSSCON was present at Embedded World Exhibition & Conference 2025 in Nuremberg, Germany—one of the largest global events for embedded systems. UMINHO represented the project with the talk "CVA6 MMU-less Virtualization – From Hardware to Software, and Vice Versa!", showcasing CROSSCON's innovative contributions to embedded virtualization technologies.

DISSEMINATION UPDATES

Past Events

During M24-M31, CROSSCON organized and participated in several events. Here is the summary of what hapenned!

Crypto-Chipset Security

28 April 2025 | Online

https://crosscon.eu/events/workshop-trusted-execution-environments-tees

CROSSCON organized a webinar with SLAB as main coordinator, focusing on key security protocols, recent cryptographic attacks, practical cryptography concepts, and secure coding fundamentals. Open to all and held online, the session promoted awareness and secure development practices

Zarhus Developers Meetup 0x1

6 May 2025 | Online

https://vpub.dasharo.com/e/22/zarhus-developers-meetup-0x1

CROSSCON was at Zarhus Developers Meetup, a virtual event uniting Zarhus users and developers to exchange ideas, explore upcoming features, and strengthen the Zarhus and embedded security community. CROSSCON presented two security-focused talks highlighting key features of the CROSSCON Hypervisor.

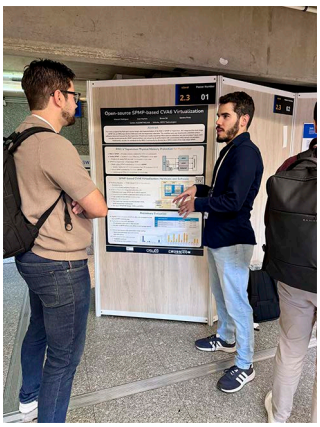
RISC-V Summit Europe

12–15 May 2025 | Paris, France

https://riscv-europe.org/summit/2025/

CROSSCON participated in the RISC-V Summit Europe 2025, held in Paris, a key event for RISC-V innovation in industry, academia, and research.
University of Minho (UMINHO) showcased two posters:

"An Open-Source Trusted Execution Environment for Resource-Constrained RISC-V MCUs"
Showcasing CROSSCON's efforts to deliver secure and open-source solutions for low-end RISC-V devices.



"Open-Source SPMP-Based CVA6 Virtualization"
Showcasing how SPMP (Simplified Physical Memory Protection) enables secure and lightweight virtualization on RISC-V.

Next Events

During next months CROSSCON will organize and participate in several events. Here is the summary of what events are scheduled!

SecRIot 2025

9 June 2025 | Tuscany, Italy

https://sites.google.com/view/secriot2025/home

CROSSCON will be represented by UNITN at SecRIoT, a key event addressing the urgent need for secure IoT systems. As billions of devices become interconnected, vulnerabilities in hardware, software, and supply chains persist. UNITN will present CROSSCON's advancements in trusted execution and secure design, contributing to a safer and more resilient IoT ecosystem.

DISSEMINATION UPDATES

News

Over the past few months, we have organized various meetings with our partners to share updates, review the progress of each task, and discuss the next steps of ongoing WPs.

5th GA Meeting

8–9 Oct 2024 Ljubljana, Slovenia

https://crosscon.eu/news/crosscon-4th-ga-meeting

The CROSSCON consortium recently assembled at the University of Ljubljana in Slovenia for a productive meeting with focus on Use-Case implementation plan.

6th GA Meeting

6–7 Mar 2025 Madrid, Spain

https://crosscon.eu/news/crosscon-4th-ga-meeting

The CROSSCON consortium meet at EVIDEN in Spain for a technical meeting focused on reviewing the progress of ongoing work package tasks. Particular attention was given to security challenges in low-end devices, fostering in-depth discussions and coordination among partners to ensure alignment and advance the project's technical objectives.

Blog Posts

Over the past few months, we have published six new blog posts where our partners share updates and insights on the project content they are responsible for.

Improving the resilience of trusted applications with control flow integrity

One of the targets of the CROSSCON project is the development of foundational trusted services whose goal is to support the various security-relevant activities to be performed on IoT devices. In this blog post we analyze in detail one of these services, implementing a control flow integrity facility for applications running on the CROSSCON bare-metal Trusted Execution Environment.
Read more: https://crosscon.eu/blog/improving-resilience-trusted-applications-control-flow-integrity

Alberto Tacchella
Post-doctoral researcher
UNITN

DISSEMINATION UPDATES

Blog Posts

Over the past few months, we have published six new blog posts where our partners share updates and insights on the project content they are responsible for.

Ensuring Memory Safety for Trusted Applications through Secure Compilation

A Trusted Application (TA) is an application running in a Trusted Execution Environment (TEE) that implements a security-critical functionality. Especially on low-end IoT devices, TAs are typically written in unsafe languages like C or C++, and are thus prone to all the pitfalls of manual memory management. Moreover, TEEs typically do not provide isolation guarantees inside the address space of single TAs, but only between different TAs...
Read more: https://crosscon.eu/blog/ensuring-memory-safety-trusted-applications-through-secure-compilation

Alberto Tacchella
Post-doctoral researcher
UNITN

Ensuring Secure IoT Systems: CROSSCON's Approach to Security Testing

At CROSSCON, robust security evaluation is the cornerstone of releasing secure implementations. This process is guided by security requirements defined in WP1 and implemented through the MEFORMA methodology, which ensures comprehensive security testing across the stack.
Read more: https://crosscon.eu/blog/ensuring-secure-iot-systems-crosscons-approach-security-testing

Ákos Milánkovich
Security Analyst
SEARCH-LAB

AuthentiSafe: A Milestone in the CROSSCON Project for IoT Authentication

AuthentiSafe is a pivotal result of the CROSSCON project, which was created to enhance security and efficiency in Internet of Things (IoT) communication. Recognizing the demands of resource-constrained devices, AuthentiSafe provides a practical way for them to verify one another. It aligns with CROSSCON's commitment to offering modular, reusable, and formally verified trusted services.
Read more: https://crosscon.eu/blog/authentisafe-milestone-crosscon-project-iot-authentication

Christoph Sendner
Chair of Software Engineering
UWU

Fuzzing the Future: How AI is Transforming Hardware Security Evaluation

The first half of the CROSSCON project targets validating research into practical techniques for complex IoT systems. CROSSCON aims to develop a versatile secure stack, leveraging diverse hardware and security mechanisms to ensure trust across multiple layers and devices, overcoming the limitations of tightly coupled, hardware-specific security solutions.
Read more: https://crosscon.eu/blog/fuzzing-future-how-ai-transforming-hardware-security-evaluation

Nikhilesh Singh
Postdoc
Huimin Li
Postdoc
Lichao Wu
Postdoc
Mohamadreza
PhD Student
Ahmad Sadeghi
Professor
TUD

Many TEEs, One Hypervisor: Enhancing Cross-Platform Security and Interoperability

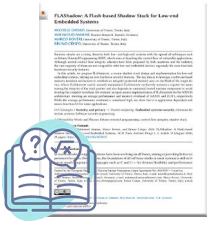
In many IoT systems, various devices coexist, presenting an ongoing challenge to ensure they all provide the essential security to establish a security baseline across the whole system. As technology advances, system complexity increases, and the integration of functionalities with different criticality levels within the same device ...
Read more: https://crosscon.eu/blog/many-tees-one-hypervisor-enhancing-cross-platform-security-and-interoperability

João Sousa
PhD student
UMINHO

Tiago Gomes
Assistant Prof.
UMINHO

DISSEMINATION UPDATES

Latest Publications

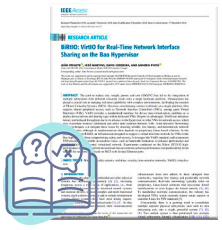


FLAShadow: A Flash-based Shadow Stack for Low-end Embedded Systems

Michele Grisafi, Mahmoud Ammar, Marco Roveri, and Bruno Crispo. 2024. “FLAShadow: A Flash-based Shadow Stack for Low-end Embedded Systems.” ACM Trans. Internet Things
https://dl.acm.org/doi/10.1145/3670413

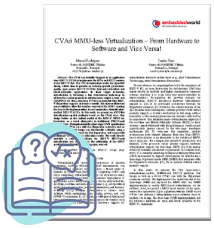
Gain Insights into the Latest Cybersecurity Trends from Horizon Europe Funded Projects

AI4CYBER, CERTIFY, CROSSCON, ENCRYPT, KINAITICS, REWIRE, TRUMPET and TRUSTEE, “Gain Insights into the Latest Cybersecurity Trends from Horizon Europe Funded Projects” in CROSSCON Website
https://crosscon.eu/publications



BiRtIO: VirtIO for Real-Time Network Interface Sharing on the Bao Hypervisor

J. Peixoto, J. Martins, D. Cerdeira and S. Pinto, "BiRtIO: VirtIO for Real-Time Network Interface Sharing on the Bao Hypervisor," in IEEE Access, vol. 12, pp. 185434-185447, 2024
https://ieeexplore.ieee.org/document/10781314

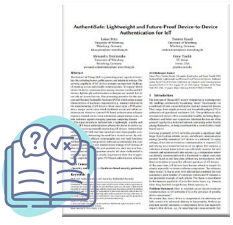


CVA6 MMU-less Virtualization – From Hardware to Software, and Vice Versa!

Manuel Rodrigues and Sandro Pinto. Embedded World 2025
https://events.linuxfoundation.org/riscv-at-embedded-world/

AuthentiSafe: Lightweight and Future-Proof Device-to-Device Authentication for IoT

Petzi, L., Krauß, T., Dmitrienko, A. & Tsudik, G. (2025). AuthentiSafe: Lightweight and Future-Proof Device-to-Device Authentication for IoT. to appear in the 20th ACM ASIA Conference on Computer and Communications Security.
https://www.bibsonomy.org/bibtex/2222ec11248ab6c589907dcd790f04b49/sssgroup



RLFuzz: Accelerating Hardware Fuzzing with Deep Reinforcement Learning

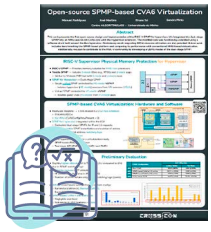
Raphael Götz, Christoph Sendner, Nico Ruck, Mohamadreza Rostami, Alexandra Dmitrienko, and Ahmad-Reza Sadeghi, “RLFuzz: Accelerating Hardware Fuzzing with Deep Reinforcement Learning”, in IEEE Host, 2025
http://www.hostsymposium.org/program-html.php

Certified IoT Security Updates

Alberto Tacchella, Emanuele Beozzo, Bruno Crispo, and Marco Roveri, “Certified Secure Updates for IoT Devices”, in IFIP SEC 2025
https://sec2025.um.si/ (Close-Source)

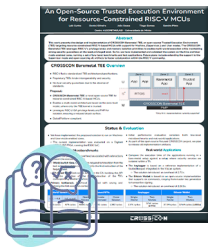
GET IN TOUCH!

Latest Publications



An open-source Trusted Execution Environment for Resource-Constrained RISC-V MCUs

Luis Cunha, Daniel Oliveira, João Sousa, Tiago Gomes, Sandro Pinto
https://crosscon.eu/publications



Open-source SPMP-based CVA6 Virtualization

Manuel Rodrigues, José Martins, Bruno Sá, Sandro Pinto
https://crosscon.eu/publications

Next Release

NEWSLETTER #5

It will be released by Q4 2025

Meanwhile, stay up-to-date with other important CROSSCON news by following our social media channels!

www.crosscon.eu contact@crosscon.eu @crosscon_eu in/crosscon

Subscribe:

https://crosscon.eu/
https://zenodo.org/communities/crosscon