NEWSLETTER #5

CONTENTS:

With the project now concluded and the final evaluation approaching, this issue provides a moment to reflect on the journey we have shared over the past three years and to highlight the mature outcomes that CROSSCON has delivered.

- Alexandra Dmitrienko, University of Würzburg

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

CROSSCON Closing Notes

With the project now concluded and the final evaluation approaching, this issue provides a moment to reflect on the journey we have shared over the past three years and to highlight the mature outcomes that CROSSCON has delivered.

Alexandra Dmitrienko

Head of Secure Software Systems Research Group, University of Würzburg

Dear Readers,

Welcome to the fifth and final issue of the CROSSCON newsletter. With the project now concluded and the final evaluation approaching, this issue provides a moment to reflect on the journey we have shared over the past three years and to highlight the mature outcomes that CROSSCON has delivered.

CROSSCON has brought together a diverse and vibrant community of researchers, engineers, and practitioners, all united by the common goal of advancing trustworthy and secure computing across heterogeneous hardware and software environments. In particular, our innovations target typical IoT and connected device systems, which often include devices from multiple manufacturers, each equipped with different security features and mechanisms. Ensuring reliable, interoperable, and secure operation in such heterogeneous ecosystems has been a core challenge of the project.

We are especially proud to announce that the CROSSCON stack has now reached a mature state. Key components, including the CROSSCON SoC, CROSSCON Hypervisor, CROSSCON Trusted Services, and CROSSCON Toolchain, are fully operational. Together with the pilots conducted during the project, these components have demonstrated their practical viability and paved the way for realworld deployment scenarios. The pilots have allowed us to test, validate and refine the stack in representative environments - bringing our work out of the lab and into connected device ecosystems.

For those who have followed our previous newsletters, this final issue captures the culmination of years of collaborative effort and innovation. It is a testament to the dedication, expertise, and creativity of the entire consortium. As we prepare for the project's final evaluation, we hope that the achievements documented here illustrate both the scientific and practical value that CROSSCON has created in the context of connected devices and heterogeneous IoT ecosystems.

Thank you to everyone who contributed to this journey — from the consortium partners to the broader community of readers and collaborators. It has been an honor to be part of this endeavor, and we look forward to seeing how the tools, methods, and services developed through CROSSCON will continue to influence secure computing research and applications in the years to come.

Alexandra Dmitrienko

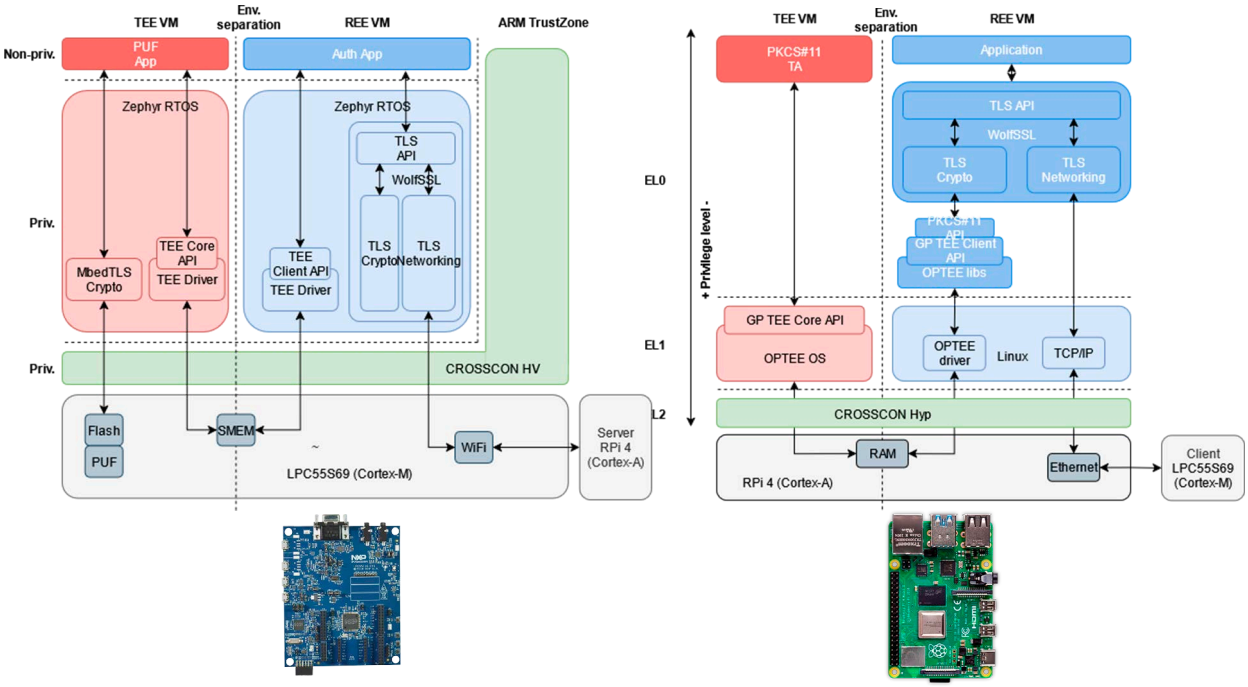
Project Updates

UC1 - Device Multi-Factor Authentication

This Use-Case demonstrates trusted second-factor authentication for IoT devices with varying capabilities. Two scenarios were implemented: a PUF-based factor for verifying low-end to high-end devices and Context-Based Authentication (CBA) for high-end ones. Both highlight the adaptability of CROSSCON's multi-factor authentication mechanisms.

UC1.1 - A PUF-based factor for verifying low-end to high-end devices

Use Case 1.1 focuses on launching the PUF Trusted Service in a real-life use case - second-factor authentication between low-end IoT devices and high-end edge devices. The picture below outlines the current software architecture of the IoT device.



Over the last few months, we have been focused on launching the novel CROSSCON Hypervisor for one of the low-end devices used in the CROSSCON project, specifically the LPCXpresso55S69. This device is a development kit that represents commonly used IoT devices on the Cortex-M architecture, with low to no security feature support. The hypervisor adds virtualization to the device, which initially lacks hardware virtualization, and utilizes ARM TrustZone to separate itself from the Virtual Machines. The final configuration enhances device security through virtualization-based separation. We have launched a setup with two Virtual Machines, both running Zephyr RTOSes. These Virtual Machines serve as the base for the Use Case 1.1. The first virtual machine, which serves as the source for first-factor TLS authentication, operates under the hypervisor and is capable of establishing a handshake with the edge device. The second Virtual Machine with PUF Trusted Service is operational and is responsible for the second-factor authentication. The high-end edge device is represented by Raspberry Pi 4 B board that runs CROSSCON Hypervisor with two VM's: a Linux VM for handling both first and second -factors, and the TEE VM with OPTEE OS for storing secrets for the first-factor authentication in secure storage

Put your hands on CROSSCON PUF-based authentication here:
https://github.com/crosscon/crosscon_puf_authentication
Demonstration:
https://crosscon.eu/blog/authentisafe-milestone-crosscon-project-iot-authentication

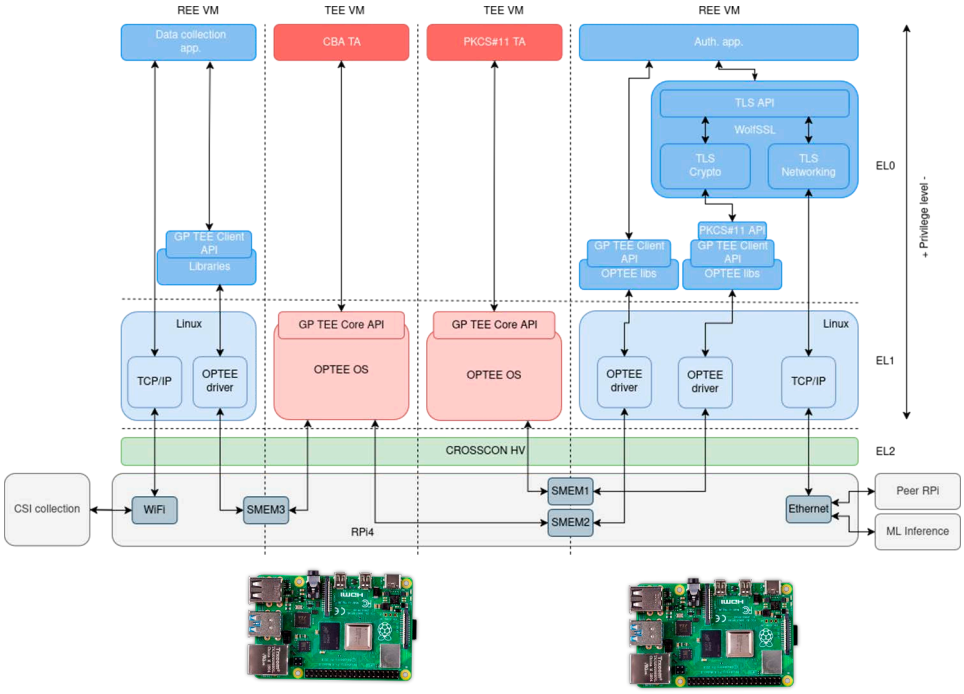
Project Updates

UC1 - Device Multi-Factor Authentication

This Use-Case demonstrates trusted second-factor authentication for IoT devices with varying capabilities. Two scenarios were implemented: a PUF-based factor for verifying low-end to high-end devices and Context-Based Authentication (CBA) for high-end ones. Both highlight the adaptability of CROSSCON's multi-factor authentication mechanisms.

UC1.2 - Context-Based Authentication (CBA) for high-end devices

Use Case 1.2 leverages the performance and architectural features of edge computing devices to provide an additional type of second-factor authentication - Context-Based Authentication. The goal here is to showcase the two-factor authentication between two edge computing or high-end devices.



The CROSSCON Hypervisor supports the ARMv8-A architecture, enabling it to run on popular Raspberry Pi 4 B boards. The Use Case will utilize the capability of CROSSCON Hypervisor to create multiple TEEs for running OP-TEE OSes and OP-TEE TAs. The TEEs will be responsible for storing and
manipulating both factor's secret data, ensuring its integrity. There are two Linux operating systems, mostly responsible for network connections with Context-Based Authentication-specific server and the peer for handshakes. We have now completed the development and testing of both the first-factor and the second-factor authentication, which utilizes the CROSSCON Hypervisor TEE with OPTEE OS and PKCS#11 Trusted Application as the cryptography engine for TLS operations for the first-factor and a CROSSCON Context-Based Authentication Trusted Service for the second-factor. Both factors was integrated and are now available for testing.

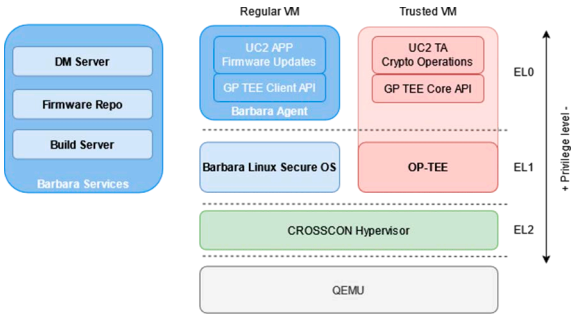
Put your hands on CROSSCON context-based authentication here:
https://github.com/crosscon/crosscon_puf_authentication
Demonstration:
https://github.com/crosscon/uc1-2-integration

Project Updates

UC2 – Firmware Updates of IoT Devices

This Use Case showcase authenticated and tamper-proof firmware delivery in heterogeneous environments. A dual-environment design separates update logic from cryptographic operations, ensuring both integrity and confidentiality throughout the device lifecycle.

UC2 demonstrates a secure and integrity-verified firmware update process for IoT devices. The use case showcases how firmware packages are downloaded, validated, decrypted, and installed within a protected environment. It leverages key CROSSCON components, including the CROSSCON Hypervisor for isolation between execution domains and an open-source TEE (the OP-TEE) for cryptographic validation and secure storage of sensitive assets.

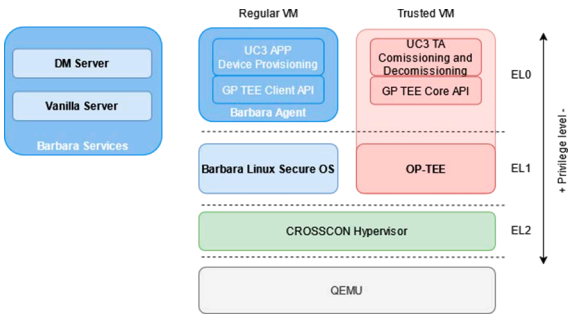


The architecture diagram illustrates the interaction between the Regular VM (running Barbara Linux Secure OS) and the Trusted VM (running OP-TEE). The implementation is deployed on a QEMU virtualized platform, emulating the environment to demonstrate the CROSSCON stack, isolation features, and secure update workflow.

UC3 – Commissioning and Decommissioning of IoT Devices

This Use Case focuses on secure device identity provisioning and lifecycle management, ensuring that each device is uniquely identified, securely onboarded, and properly decommissioned at the end of its lifecycle.

UC3 demonstrates the CROSSCON Hypervisor and CROSSCON TEE implementation, which provide hardware-enforced isolation, secure key generation, credential management, and tamper-resistant storage within the Trusted VM.



The architecture diagram details the interactions between the Regular VM (running Barbara Linux Secure OS) and the Trusted VM (running OP-TEE) during both commissioning and decommissioning phases. The system is implemented and executed on a QEMU virtualized platform, enabling realistic testing and validation of secure provisioning, certificate handling, and identity lifecycle operations within a controlled emulated environment.

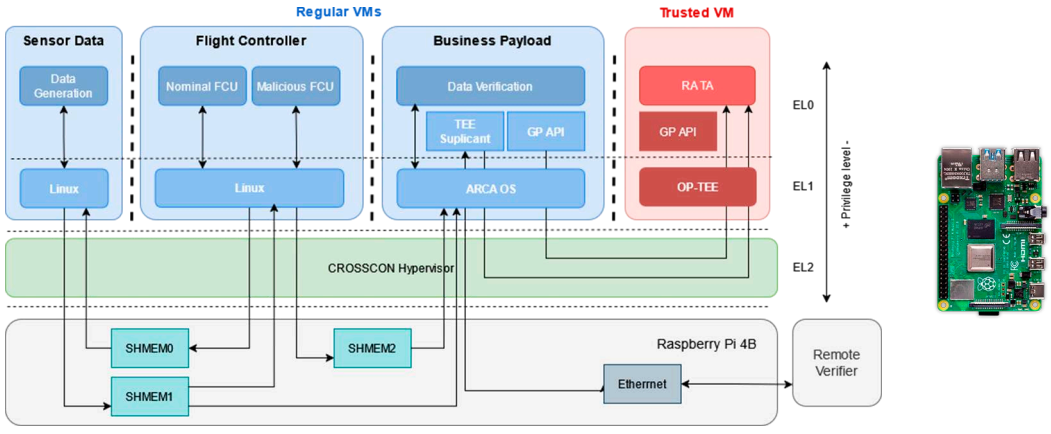
Project Updates

UC4- Remote Attestation for Identification and Integrity Validation of Agricultural UAVs

In Unmanned Aerial Vehicles (UAVs), the Flight Control Unit (FCU) manages all drone movements, executing pilot commands or autonomous flight plans. It is also the main entry point for sensor data (e.g., GPS, airspeed) and the sole communication path to flight controllers, making it essential for safe operation. However, the FCU is typically a separate hardware or software module not developed by the UAV owner, meaning it cannot be inherently trusted. It also operates alongside the business payload running commercial applications, which depend on flight-related data shared by the FCU; thus, any tampering with the FCU directly affects UAV operations. To address these risks, UC4 aims to secure UAV operation by ensuring the FCU behaves correctly, using Remote Attestation (RA) to validate its integrity and operational state.

The UC4 demonstrates how the CROSSCON Stack can enhance the safety and integrity of UAVs through RA mechanisms. The goal is to ensure that critical UAV components, especially the Flight Controller Unit (FCU), operate in a trusted state. The final implementation introduces a virtualized UAV environment running over the CROSSCON Hypervisor, with multiple isolated Virtual Machines (VMs) representing UAV components:

- Sensor Data VM: Collects and distributes emulated sensor data securely to other VMs, ensuring trust and isolation from potentially compromised components.
- Flight Controller VM: Simulates both nominal and malicious FCU behaviour to test integrity validation mechanisms.
- Business Payload VM: Runs CYSEC's ARCA Trusted OS and includes a validation module that monitors sensor and control data. If anomalies are detected, it triggers remote attestation.
- Trusted OP-TEE VM: Hosts the RA Trusted Application (RA TA), which measures FCU memory integrity and communicates securely with a Remote Verifier over TLS.



Its demonstration relies on the CROSSCON Hypervisor, OP-TEE for hosting the Remote Attestation services, CYSEC's ARCA Trusted OS, and multiple virtualized VMs representing UAV subsystems. The UC4 scenario has been deployed and validated on a Raspberry Pi platform, demonstrating the feasibility of running trusted virtualized environments on low-cost, resource-constrained hardware. This setup establishes the foundation for future multi-FCU architectures aimed at improving redundancy and fault detection.

Put your hands on UC4 components here:

- https://github.com/crosscon/remote-attestation-trusted-application
- https://github.com/crosscon/remote-attestation-optee-os
- https://github.com/crosscon/remote-attestation-remote-verifier

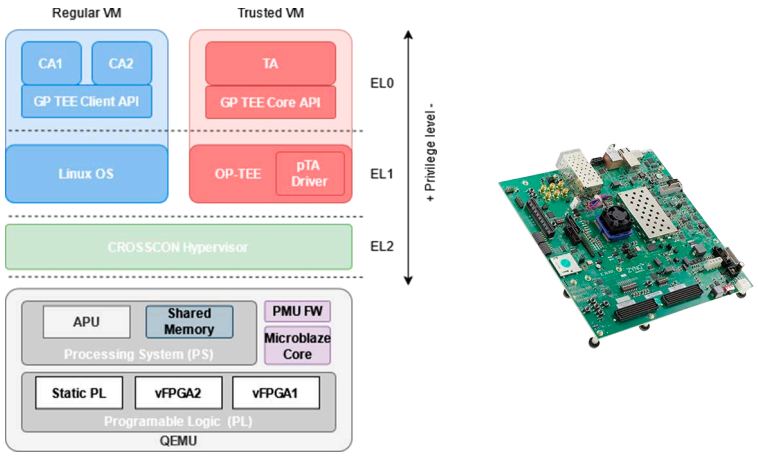
CYSEC

Project Updates

UC 5 – Intellectual Property Protection for Secure Multi-Tenancy on FPGA

Field Programmable Gate Arrays (FPGAs) have become integral components in modern computing environments due to their adaptability and versatility. Partial Reconfiguration (PR) introduces the capability for dynamic reconfiguration of regions of the FPGA while the remainder of the logic continues to function seamlessly. This approach involves partitioning the FPGA into a static region and one or more partially reconfigurable regions that can be configured at runtime.

The UC5 provide a technology demonstrator to enable Secure FPGA Provisioning for clients by extending a trusted execution environment to FPGAs via the CROSSCON Hypervisor within a multi-tenant deployment model. To achieve this, we aim to enable secure sharing of FPGA resources among multiple users and applications, facilitating true multi-tenancy. This involves supporting secure configuration and deployment of intellectual property (IP) hardware designs on shared and virtualized FPGAs and enforcing access control to IP designs on the FPGA and their data. By doing so, we ensure that FPGA resources are utilized efficiently, providing robust security measures to protect each user's data and IP, and maintaining the integrity and confidentiality of all operations conducted on the FPGA platform.



The UC5 architecture consists of Linux-based client applications (CA1 and CA2) that act as tenants of a shared FPGA and send encrypted, signed partial bitstreams to a Trusted Application (TA) running inside an OP-TEE-based Trusted VM. The TA authenticates and decrypts these packages, then hands the bitstreams to a pseudo-TA (pTA) driver, which cleans caches and issues a Secure Monitor Call (SMC) to trigger FPGA reconfiguration. A Regular VM hosts the CAs without access to secure memory, while the Trusted VM owns the secure DRAM region and exposes GlobalPlatform APIs. The CROSSCON Hypervisor at EL2 enforces isolation between Linux and OP-TEE, manages second-stage page tables, and forwards reconfiguration SMCs to ARM Trusted Firmware (ATF). ATF, running at EL3, validates buffer bounds and passes the bitstreams to the Platform Management Unit firmware. On the Zynq Ultrascale+ MPSoC ZCU102 board, the Processing System (PS) handles APU cores, DDR, and the PCAP interface, while the Programmable Logic (PL) contains a static region for data flow management and two dynamically reconfigurable partitions (vFPGA1 and vFPGA2). A Microblaze core running PMU-FW ultimately drives the PCAP to load the partial bitstreams into the FPGA fabric.

Put your hands on UC5 components here:

- https://github.com/crosscon/UC5-IP_Protection_for_Secure_Multi-Tenancy_on_FPGA

DISSEMINATION UPDATES

During M30-M36, CROSSCON organized and participated in several events. Here is the summary of what hapenned!

Zarhus Developers meetup #1

6 May 2025 | Online

https://cfp.3mdeb.com/zarhus-developers-meetup-0x1-2025

CROSSCON partner 3mdeb hosted this workshop that bring open-source enthusiasts to explore CROSSCON's components and technologies. The session offered both general and specialized audiences valuable insights into trusted execution and secure virtualization, fostering knowledge exchange within the open-source and research communities.

RISC-V Summit Europe

12 May 2025 | Paris, France

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

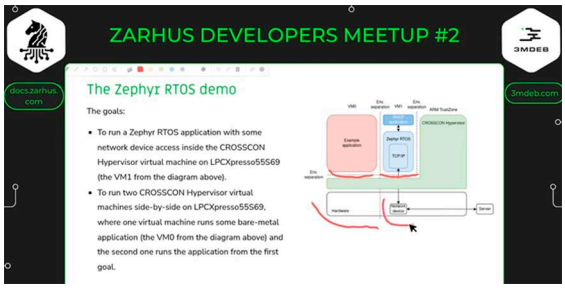
CROSSCON participated in the RISC-V Europe 2025 event, joining industry leaders and researchers to showcase advancements in secure virtualization and trusted execution. The project's presence highlighted its contribution to strengthening RISC-V security ecosystems and promoting collaboration within Europe's open hardware and software community.

SecRIot 2025

9 Jun 2025 | Tuscany, Italy

https://sites.google.com/view/secriot2025/home - co-located with DCOSS-IoT 2025

CROSSCON was presented at the SecRIoT conference, where UNITN showcased CROSSCON Baremetal TEE component. The presentation also highlighted CROSSCON's role in enhancing IoT security and resilience, fostering collaboration between academia and industry within the European research landscape.



Zarhus Developers Meetup #2

5 Aug 2025 | Online

https://cfp.3mdeb.com/zarhus-developers-meetup-2-2025/

CROSSCON partner 3mdeb hosted the second edition of the Zarhus Developers Workshop, bringing together open-source enthusiasts to disseminate CROSSCON's components and technologies. During the event, 3mdeb demonstrated a real-world use case, integrating CROSSCON components such as newly developed trusted services and the CROSSCON Hypervisor.

Cyber Security Workshop: Empowering NREN Institution

25 Jul 2025 | AIT, Thailand

https://ait.ac.th/2025/07/ait-ai-center-hosts-empowering-nren-institutions-generative-ai-training-for-network-monitoring-cyber-security-workshop/

CROSSCON was also presented outside Europe in this event. The project's core concept and vision were disseminated to a global audience, highlighting CROSSCON's commitment to advancing secure and trustworthy computing worldwide.

DISSEMINATION UPDATES

News

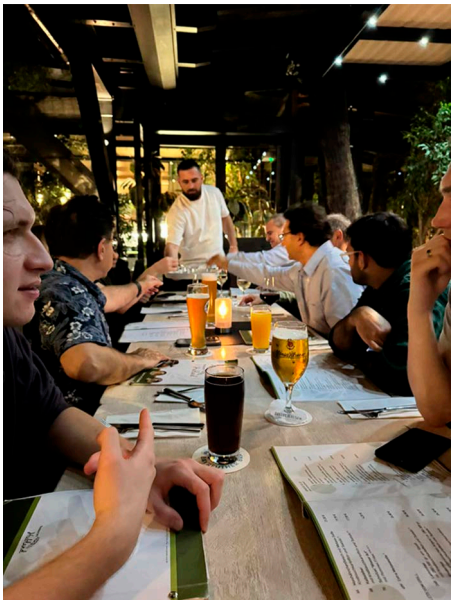
Over the past few months, we have organized various meetings with our partners to share updates, review the progress of each task, and discuss the next steps of ongoing WPs.

8th GA Meeting

7–8 Oct 2025 Würzburg, Germany

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

The CROSSCON consortium recently gathered in Wurzburg, Germany for a productive General Assembly meeting. The partners discussed the remaining action points to successfully close the project, defined the demonstrations for the final review, and presented the current status of all Use Cases, ensuring alignment on deliverables and outcomes.



Blog Posts

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

Secure Authentication Using Context

Traditional IoT authentication methods remain vulnerable to attacks like spoofing and brute force. The CROSSCON Context-Based Authentication (CBA) leverages Wi-Fi Channel State Information (CSI) to create digital fingerprints of devices and their environment, enabling secure, location-aware authentication. Lightweight and efficient, CBA strengthens IoT security by combining device- and environment-specific features, making it extremely hard for attackers to replicate, while aligning with CROSSCON's vision of robust protection for heterogeneous IoT systems.

Read more: https://crosscon.eu/blog/secure-authentication-using-context

Hamid Dashtbani
Ph. D. Student
UWU

DISSEMINATION UPDATES

Blog Posts

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.

Achieving persistent tagging for robust stack memory error protection

Memory safety remains a leading cause of software vulnerabilities, affecting platforms from browsers to embedded systems. This work explores memory tagging on RISC-V to detect invalid memory accesses, introducing a LLVM-based persistent tagging mechanism to ensure tag integrity and prevent pointer corruption.
Read more: https://crosscon.eu/blog/achieving-persistent-tagging-robust-stack-memory-error-protection

Carlo Ramponi
Ph. D. Student
UNITN

CROSSCON: from knowhow generation to technology development, maturation and impact creation - Mission accomplished!

CROSSCON successfully delivered innovative, interoperable IoT security technologies, including hypervisors, TEEs, trusted services, and a RISC-V SoC, supported by reproducible demonstrations and strong community impact. With 44 publications, extensive collaborations, and major event participation, the project advanced market-ready IoT security solutions and invites future partnerships.
Read more: https://crosscon.eu/blog/crosscon-knowhow-generation-technology-development-maturation-and-impact-creation-mission

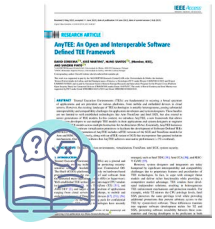
Hristo Koshutanski
Project Cooridinator
ATOS

Latest Publications

Over the past few months, we have published and presented several scientific works in journals and conferences related to the CROSSCON project. Please refer to the list below to see which publications were produced, by whom, and in which venues they were presented.

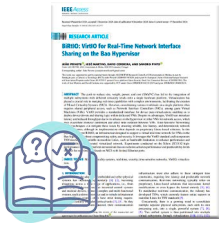
Firmware Secure Updates meet Formal Verification

Alberto Tacchella, Emanuele Beozzo, Bruno Crispo, and Marco Roveri. 2025. Firmware Secure Updates meet Formal Verification. ACM Trans. Cyber-Phys. Syst. Just Accepted (July 2025)
https://doi.org/10.1145/3754455



AnyTEE: An Open and Interoperable Software Defined TEE

D. Cerdeira, J. Martins, N. Santos and S. Pinto, "AnyTEE: An Open and Interoperable Software Defined TEE Framework," in IEEE Access, 2025
https://ieeexplore.ieee.org/document/11043152



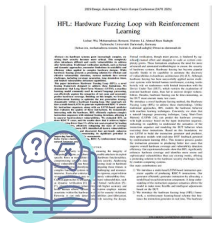
Bridging the Interoperability Gaps among Trusted Architectures in MCUs

Pinto, Sandro & Cunha, Luís & Oliveira, Daniel & Grisafi, Michele & Beozzo, Emanuele & Crispo, Bruno. (2025). “Bridging the Interoperability Gaps Among Trusted Architectures in MCUs.”
https://www.researchgate.net/publication/396706028_Bridging_the_Interoperability_Gaps_Among_Trusted_Architectures_in_MCUs

DISSEMINATION UPDATES

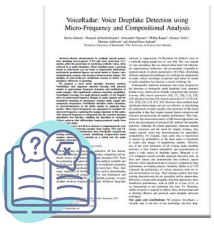
Latest Publications

Over the past few months, we have published and presented several scientific works in journals and conferences related to the CROSSCON project. Please refer to the list below to see which publications were produced, by whom, and in which venues they were presented.



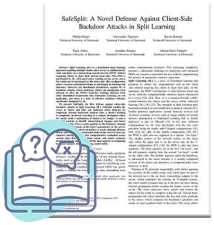
HFL: Hardware Fuzzing Loop with Reinforcement Learning

L. Wu, M. Rostami, H. Li and A. -R. Sadeghi, "HFL: Hardware Fuzzing Loop with Reinforcement Learning," 2025 Design, Automation & Test in Europe Conference (DATE), Lyon, France, 2025, pp. 1-7, doi: 10.23919/DATE64628.2025.10993080.
https://ieeexplore.ieee.org/document/10993080



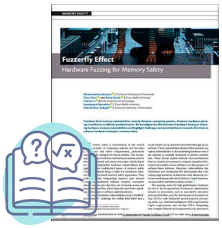
VoiceRadar: Voice Deepfake Detection using Micro-Frequency and Compositional Analysis

Kavita Kumari, Maryam Abbasihafshejani, Alessandro Pegoraro, Phillip Rieger, Kamyar Arshi, Murtuza Jadliwala, Ahmad-Reza Sadeghi. “VoiceRadar: Voice Deepfake Detection using Micro-Frequency and Compositional Analysis”, NDSS, 2025
https://www.ndss-symposium.org/ndss-paper/voiceradar-voice-deepfake-detection-using-micro-frequency-and-compositional-analysis/



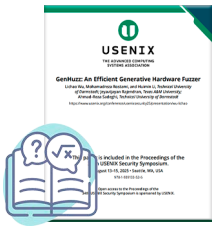
SafeSplit: A Novel Defense Against Client-Side Backdoor Attacks in Split Learning

Phillip Rieger, Alessandro Pegoraro, Kavita Kumari, Tigist Abera, Jonathan Knauer, Ahmad-Reza Sadeghi. “VoiceRadar: Voice Deepfake Detection using Micro-Frequency and Compositional Analysis”, NDSS, 2025
https://www.ndss-symposium.org/wp-content/uploads/2025-1698-paper.pdf



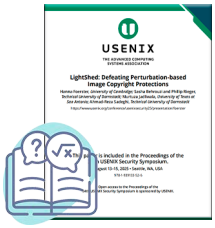
Fuzzerfly Effect: Hardware Fuzzing for Memory Safety.

M. Rostami, C. Chen, R. Kande, H. Li, J. Rajendran and A. -R. Sadeghi, "Fuzzerfly Effect: Hardware Fuzzing for Memory Safety," in IEEE Security & Privacy, 2024
https://ieeexplore.ieee.org/document/10462151



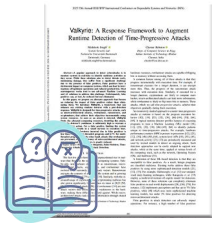
GenHuzz: An Efficient Generative Hardware Fuzzer

Lichao Wu, Mohamadreza Rostami, and Huimin Li, Technical University of Darmstadt; Jeyavijayan Rajendran, Texas A&M University; Ahmad-Reza Sadeghi, “GenHuzz: An Efficient Generative Hardware Fuzzer“, USENIX 2025
https://events.linuxfoundation.org/riscv-at-embedded-world/



LightShed: Defeating Perturbation-based Image Copyright Protections

Hanna Foerster, Sasha Behrouzi, Phillip Rieger, Murtuza Jadliwala, Ahmad-Reza Sadeghi, “LightShed: Defeating Perturbation-based Image Copyright Protections”, USENIX 25
https://www.usenix.org/system/files/usenixsecurity25-foerster.pdf



Valkyrie: A Response Framework to Augment Runtime Detection of Time-Progressive Attacks

Nikhilesh Singh, Chester Rebeiro, "Valkyrie: A Response Framework to Augment Runtime Detection of Time-Progressive Attacks," International Conference on Dependable Systems and Networks (DSN) 2025
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=11068882

DISSEMINATION UPDATES

Latest Publications

Over the past few months, we have published and presented several scientific works in journals and conferences related to the CROSSCON project. Please refer to the list below to see which publications were produced, by whom, and in which venues they were presented.

Gain insights into the latest empirical Cyber Security trends and results from Horizon Europe Funded Projects

CROSSCON White Paper
https://crosscon.eu/dissemination-material/white-paper-3-gain-insights-latest-empirical-cyber-security-trends-and

PROJECT RESULTS

Throughout the CROSSCON project, we achieved scientific, technical, and community results. The table on the right highlights our key performance indicators (KPIs), including publications, events, EU collaborations. Together, these outcomes demonstrate our commitment to advancing secure and interoperable IoT technologies.

KPI Description	KPI Value	
Scientific publications	**50+**	
Events attended/organized	Attended: **40+**	Organized:**10+**
Winter/Summer schools	**3**	
Liaison with projects	**15+**	
White papers	**3**	
Demonstrators/Repositories	**17**	
Press Releases	**3**	
Newsletters	**5**	
Blog Posts	**24**	
Use Cases	**5**	

All materials, including blog posts, publications, and software components are publicly available in our Website and GitHub page, and you can access them through the following links:

- **Blog Posts:** https://crosscon.eu/category/92
- **GitHub page:** https://github.com/crosscon
- **Scientific Publications:** https://crosscon.eu/publications

Thank you to everyone who contributed to this journey — from the consortium partners to the broader community of readers and collaborators.

- Alexandra Dmitrienko, University of Würzburg