NEWSLETTER #1

CONTENTS:

CROSSCON designs an open, highly portable, and vendor-independent IoT security stack, and offers the necessary low-layer security primitives and trusted services to enable essential services and security properties at the higher layers, to the operating systems and applications running on IoT devices.

- Hristo Koshutanski

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

Project Coordinator Notes

> CROSSCON designs an open, highly portable, and vendor-independent IoT security stack, and offers the necessary low-layer security primitives and trusted services to enable essential services and security properties at the higher layers, to the operating systems and applications running on IoT devices.

Hristo Koshutanski
Project Coordinator, ATOS

Dear Readers of the 1st CROSSCON Newsletter:

I am very excited to introduce my notes to this first edition of the newsletter. First, I would like to say a big "thank you" to the consortium team, composed of very knowledgeable and experienced SMEs, universities, and a large industry, for their effort and dedication to materialize the idea into a successful project which the EC selected to fund its implementation.

I would like to start with what CROSSCON stands for – **a Cross-Platform Open Security Stack for Connected Devices** – a very representative goal to provide an interoperable security layer at the lowest level of IoT devices between the software and hardware – where we believe lies the challenge, ambition, and above all, the impact the project can generate from successful realization.

We all have witnessed the proliferation and impact the IoT paradigm has brought to us over the years, and we all have also seen the long and never-ending list of threats, vulnerabilities and attacks on IoT ecosystems. It is just enough to go through ENISA's Threat Landscape reports over the years to understand the more-than-ever growing concern about the security of IoT devices. A major part of the challenge comes from the fragmented IoT devices' landscape where different devices coexist, having different hardware platforms with different security guarantees, or no guarantees, or often with proprietary implementations of Root of Trust (RoT) and Trusted Execution Environment (TEE). This fragmentation makes it very difficult for applications and security services to interoperate.

CROSSCON aims at a bottom-up security solution. It designs an open, highly portable, and vendor-independent IoT security stack, and offers the necessary low-layer security primitives and trusted services to enable essential services and security properties at the higher layers, to the operating systems and applications running on IoT devices.

The solution will be, by-design interoperable across a wide range of devices and heterogeneous hardware architectures, offering a unified set of trusted APIs to the layers above. It will feature a high-level of modularity, allowing the configuration of only those security primitives necessary depending on the underlying hardware and firmware. In case security features are missing, like in bare metal devices, the stack will offer an entire TEE implementation suitable for such devices. The project will also provide a methodology and tools to formally verify the security properties and guarantees offered by the stack.

As devices are getting more powerful and more security mechanisms are incorporated directly into the hardware, CROSSCON will extend its primitives to leverage such advanced security features and open its scope to domain-specific hardware architectures. Importantly, several ambitious use cases have been defined to demonstrate CROSSCON's suitability to support essential IoT security services ranging from device multi-factor authentication, secure firmware updates, to IoT device commissioning and decommissioning, but also other novel domains of Intellectual Property protection through secure FPGA provisioning, and remote attestation of a fleet of drones in the field of smart agriculture.

Finally, I encourage you to stay tuned for this 3-year adventure of CROSSCON. We'll be glad to share results with you and collaborate throughout the project's lifetime and beyond.

CROSSCON - OBJECTIVES

Objective 1

Support IoT stakeholders with the design and implementation of an innovative IoT open-source security stack.

Expected Results

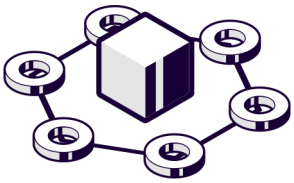
The achievement of this objective simplifies the development of trusted services and applications for IoT systems, thus reducing the time to market. It also the implementation of security in devices that lack protection, thus reducing the security threats in open source hardware.

Objective 2

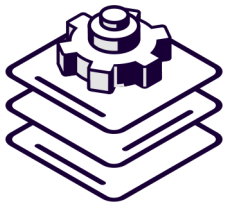
Strengthen memory protection and isolation in new and existing TEEs, mitigating the impact of side-channel attacks.

Expected Results

The achievement of this objective mitigates hardware-related security vulnerabilities. Also, it extends the availability of security primitives to implement Chains of Trust.



Objective 3



Provide methodology, techniques, and related tools to formally verify "correct by design" secure open-source software and firmware for connected

Expected Results

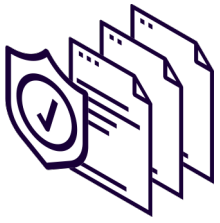
The achievement of this objective generates novel formal verification techniques and a methodology for open specification hardware and software.

Objective 4

Offer IoT stakeholders with a set of novel and high assurance trusted services.

Expected Results

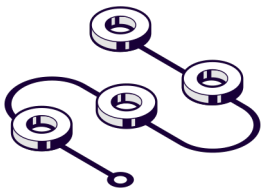
The achievement of this objective mitigates hardware-related security vulnerabilities. Also, it extends the availability of security primitives to domain-specific hardware architectures.



CROSSCON - OBJECTIVES

Objective 5

Provide a toolchain that integrates and validates lightweight techniques for security assurance.

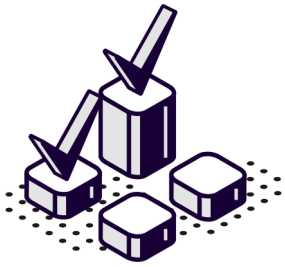


Expected Results

The achievement of this objective makes IoT security management and security service deployment simpler, more automated, easier to understand, and more trusted.

Objective 6

Provide IoT stakeholders with a validation and testing methodology, a replicable testbed, and testing and validation results for CROSSCON innovations.

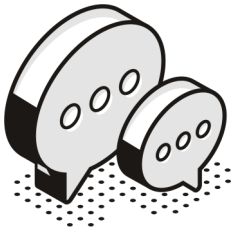


Expected Results

The achievement of this objective demonstrates and tests the effectiveness of the innovative security techniques and methods introduced by CROSSCON. It also validates our support to implement secure provisioning, inventory management, device authentication, remote attestation, and the secure management of security patches and updates.

Objective 7

Enable the valorisation and adoption of CROSSCON flagship results.



Expected Results

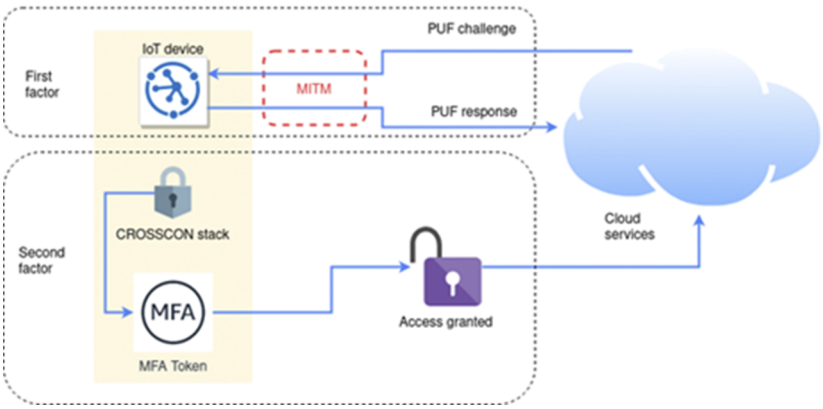
The achievement of this objective contributes to building European trustworthy platforms and opening the market of TEE applications development. It contributes to creating know- how on the general topic of trusted hardware platforms and trusted firmware. Engage security researchers, security engineers, IoT stakeholders, and open source and open hardware communities.

CROSSCON - USE CASES

UC1: Device Multi-Factor Authentication

The Internet of Things (IoT) has revolutionized the way we live and work by connecting devices and allowing them to communicate with each other. However, this increased connectivity also introduces new challenges in terms of security. One of the main challenges is ensuring that only authorized devices can access the network, or other specific resources.

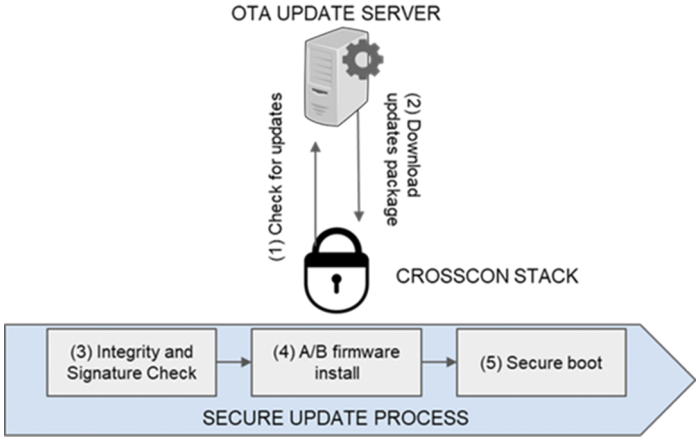
However, PUF-based authentication has proven to be difficult to implement in practice and is vulnerable to a variety of attacks. By combining multiple factors, we aim to overcome the limitations of existing PUF-based solutions and provide a more robust defense against MITM (Man-in-the-Middle).



As a final goal of this use case, we aim to propose a multi-factor authentication (MFA) solution for IoT devices to improve their security, as shown in Figure 1.

While the initial idea emerged based on the devices that leverage PUFs and other device-specific factors, we may extend it further, to provide general-purpose MFA solution. In the initial version of the use case description, we have not decided for the specific second factors yet.

UC2: Firmware Updates of IoT Devices.



Firmware update is a critical process for IoT device security. Not being able to update IoT device firmware is one of the most common sources of vulnerability during the device lifecycle. Furthermore, an insecure update process also presents a major issue as it allows an attacker to upload malicious logic on the device.

Typically, firmware updates are installed Over-The-Air (OTA). Updates and security patches can be digitally signed, such that their integrity and authenticity can be verified. However, despite digital signatures, the problem of secure updates still persists, since: i) updates often come as a bundle of libraries developed by different parties, ii) the signatures are not always issued by a mutually trusted certification authority, iii) digital signatures do not give any guarantee on the logic of the update.

This use case, considers two types of updates:

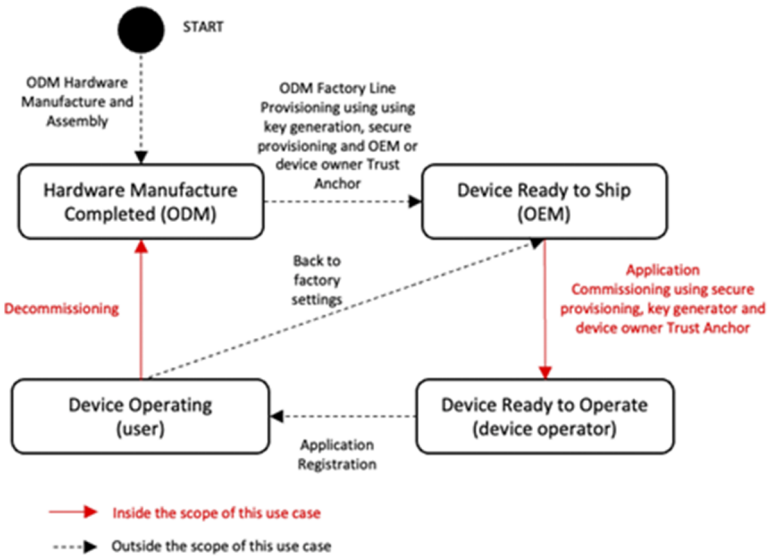
- **Full update:** the package contains the full replacement of the old package to be installed regardless of what the previous firmware installed was.

- **Partial update:** the package contains just the binary difference between the new firmware version and the old firmware version. In this case, the device has to reassemble the firmware package using the binary difference (diff) and the old package.

UC3: Commissioning and Decommissioning of IoT devices.

IoT Device Commissioning is the process by which connected devices acquire the necessary information and configuration parameters for their intended use or application: this can include security certificates, credentials, application configuration such as URLs, and others.

Commissioning is a critical step in the IoT device lifecycle, and it needs to happen before the device starts to perform its regular operation.
As opposed, IoT Device Decommissioning is the process by which the commissioned information is removed from the device. This way the device gets back to its original state when it will no longer be used or used for a different purpose or customer. This is important, especially in the case of industrial devices that may contain sensitive information. Figure shows a typical state diagram of an IoT device lifecycle around the commissioning and decommissioning processes in a multi-stakeholder case, marking in red those processes which are part of the use case addressed by CROSSCON in this project.



In addition to 3 use cases defined in the project description, Partners are considering additional use cases that will be described later.

We are open, but formal

Aljosa Pasic
Exploitation Coordinator, ATOS

Marco Roveri
WP2 Leader, Uni. Trento

A manifesto is a name usually given to a public declaration of beliefs, principles, and intentions, often issued by a group or individual, proposing specific actions or policies. The most famous and influential manifestos in history are probably the Communist Manifesto by Karl Marx and Friedrich Engels and the Declaration of Independence by Thomas Jefferson, both being embraced by two very different political and ideological systems.

Less frequently, manifestos are also associated with software components and specifications, created by groups of software developers or professionals less known than those mentioned above. Examples include the Agile Manifesto, which emphasizes flexibility in development, the DevOps Manifesto, which focuses on collaboration between previously separated teams, and the Serverless Manifesto, which promotes the use of serverless computing architectures.

Within the CROSSCON Internet of Things (IoT) security stack, each component should be modular, reusable, interoperable, and well-documented. We also believe that they should come with a "Formal Certification Manifest" so that these components can be easily re-verified after being shared, reused, or integrated. Although Open-Source Software (OSS) communities have existed for many years, Open-Source Hardware (OSH) is much less known. Among many OSH ecosystems, RISC-V is the most relevant one for CROSSCON. It revolves around an instruction set architecture for microprocessor cores, originally developed at the University of California at Berkeley and released under an open-source license. RISC-V processors are used in a wide range of contexts, including IoT, general purpose operating systems like Linux, supercomputing, and automotive technologies. Currently, there are over 100 RISC-V cores available in various semiconductor types, and they are supported by different RTOS.

While this ecosystem and CROSSCON positioning will be discussed in more in detail in the exploitation activities of the project, they also face challenges on their own. Verification, for example, is costly and sometimes represents a bottleneck in the RISC-V design cycle.

One of the core tasks in CROSSCON is to openly design a security stack for connected devices and IoT, considering the requirements for enabling formal verification of security properties such as memory isolation and secure storage, as well as the life-time operations, including bug fixing, cross-compilation, and updates/patches.

This CROSSCON specification will be presented in a "Formal Certification Manifesto" associated with each element of the stack, including access policies, assumptions, used resources, and behaviors, among other information, formulated with suitable formalisms such as first-order formulas complemented with temporal logic formulas. This manifesto will then be the primary enabler for other activities, such as the formal verification of different components, continuous verification of patches, and security updates, among others.

This work leverages existing specifications, e.g., the RISC-V formal verification framework, complementing these with suitable extensions. Therefore, we will explain the importance of RISC-V and its relevance to the CROSSCON project.

Events

During M1-M6, CROSSCON partners and researchers have been already organizing and participating in several events. Here is the summary of what we have ben doing so far!

PHD WINTER SCHOOL 2023

6-10 Feb 2023 | Trento, Italy

https://crosscon.eu/events/phd-winter-school-2023

CROSSCON Project was present in the The European Network for Cybersecurity (NeCS) PhD Winter School 2023. The NeCS PhD School was launched in 2017 in response to the increase need of highly qualified experts in cyber-security.

High-Tech Women (HTW'23)

30 Mar 2023 | Darmstadt, Germany

https://crosscon.eu/events/high-tech-women-htw23

The System Security Lab and CROSSING organizED the third Darmstadt Women in Tech event on March 30, 2023. The conference will feature talks by internationally renowned female speakers from all over the world.

Embedded World 2023

14-16 Mar 2023 | Nuremberg, Germany

https://crosscon.eu/events/embedded-world-2023

CROSSCON Project was present at the Embedded World Exhibition & Conference 2023, which takes place annually in Nuremberg, Germany. Embedded World is one of the largest international events for embedded system technologies and applications, bringing together experts and professionals from around the world to discuss the latest trends and innovations in the field.

CYSAT 2023

26-27 Apr 2023 | Paris, France

https://crosscon.eu/events/cysat-2023

Our partner CYSEC is organising the 3rd edition of CYSAT, the biggest European event on space cybersecurity that brings together academics, industrial players, and agencies to explore the latest innovations in the field.

CROSSCON - NEWS & EVENTS

News

CROSSCON also shared exciting news that happened during the first 6 months. Follow our social channels and CROSSCON's website to stay tuned!

CROSSCON Kick-off Meeting

22-23 Nov 2022 | Madrid, Spain

https://crosscon.eu/news/crosscon-kick-meeting

The kick-off meeting for the Horizon Europe project CROSSCON (grant agreement ID 101070537) took place on November 22nd and 23rd at the ATOS facilities in Madrid, Spain.

External Synergies

ERATOSTHENES

https://eratosthenes-project.eu/

ERATOSTHENES aims to solve critical obstacles considering "Security of Things" as core to the future IoT success. The project envisions to develop a decentralized and contextual Trust and Identity Management Framework for resource-restricted IoT environments following a self-sovereign approach.

ORSHIN

https://horizon-orshin.eu/

Open-source ReSilient Hardware and software for Internet of thiNgs. How to design embedded and connected devices taking advantage of open source hardware (and software)

REWIRE

https://www.rewire-he.eu/

REWIRE envisions a holistic framework for continuous security assessment and management of open-source and open-specification hardware and software for IoT devices, throughout their entire lifecycle, under the zero-trust concept, adhering to the security-by-design principle and providing cybersecurity certification.

CERTIFY

CERTIFY defines a methodological, technological, and organizational approach towards IoT security lifecycle management.

https://certify-project.eu/

IoT-NGIN

IoT-NGIIN introduces novel research and innovation concepts, acting as the "IoT Engine" which will fuel the next Generation of IoT as a part of the European Next Generation Internet.

https://iot-ngin.eu/

Consortium

The CROSSCON consortium is made up of 11 partners from 8 European countries: **Spain, Italy, Portugal, Slovenia, Hungary, Germany, Poland, and Switzerland**. It is formed by a large industrial partner (**ATOS**), 4 academic institutions (**UNITN, UMINHO, UWU and TUD**), and 5 SMEs (**BEYOND, CYSEC, 3MDEB, SLAB, BIOT**) combining technological and scientific know-how, industrial and end user perspective, as well as business and market insight. The partners are well positioned to cooperate and collaborate to respond to the technological challenges of CROSSCON. They have been carefully selected not only for their abilities to perform the tasks described in this proposal, but also because of the experience and background that create a strong and solid basis for ensuring success of the project.

CROSSCON - MEET THE PARTNERS

ATOS

DESCRIPTION: Atos (ATOS) is a global leader in digital transformation with over 110,000 employees in 73 countries and annual revenue of over € 11 billion. Atos has portfolio of advanced digital security solutions with its network of over 6,500 dedicated experts and 16 next-generation Security Operation Centers (SOCs). Atos is involved in CROSSCON through Atos Research & Innovation (ARI), the R&D hub based in Spain with almost 30 years of experience in running Research, Development and Innovation projects.

ROLE: Besides its role of project coordinator and the leader of quality management and exploitation activities, Atos is also responsible for the website. It also acts as task leader for use case definition and contributes to several other technical tasks.

University of Trento

DESCRIPTION: The University of Trento, with slightly more than 50 years since its foundation, ranks consistently among the top Italian universities. The Computer Science Department ranked 84 in the European QS World Ranking 2016 and 91 worldwide in the THE rankings 2019. In 2018 our department has been awarded a research excellence grant in the area of Industrial and Computer Engineering by the Ministry of Research and Education. The research team is internationally recognized in cybersecurity and has a significant experience in the security of networks and systems.

ROLE: UNITN is the scientific coordinator of CROSSCON and leader of the design, specifications, and assurance workpackage (WP2). It also leads the technical activities on the security of bare metal devices as well as building a trusted toolchain for TEEs (WP3). UNITN takes also part in the dissemination and exploitation activities with an active role in building a community around the topics covered by the project. case definition and contributes to several other technical tasks.

University of Minho

DESCRIPTION: The University of Minho is a public research university in Braga and Guimarães, Portugal. It was established in 1973 and is considered one of the country's youngest and most dynamic universities. The university is recognized for its research and innovation activities and has partnerships and collaborations with institutions and companies worldwide. The Embedded Systems Research Group (ESRG) lab, at the School of Engineering, specializes in designing, developing, and implementing embedded systems on different fields such as real-time systems, cyber-physical systems, networked embedded systems, and reconfigurable systems. The group has been actively developing cyber-security solutions for the next generation of IoT devices, including virtualization and hardware security.

ROLE: UMINHO is the leader of the WP3 - Development of the CROSSCON stack. Primary responsibilities within the WP3 are the development of the CROSSCON TEE Isolation and Abstraction, and the CROSSCON Hypervisor. It also provides support in technical activities for Domain-Specific Hardware Architectures (WP4). UMINHO also has an active role in the dissemination and exploitation activities, leading the dissemination and communication tasks covered by the project.

CROSSCON - MEET THE PARTNERS

SEARCH-LAB

DESCRIPTION: SEARCH-LAB Ltd is a spin-off company established in 2002 at the Budapest University of Technology and Economics with a focus on security research and development. The laboratory is specialized in security testing and evaluation of various ICT products, with a special expertise in security of embedded systems. Through its Secure Coding Academy it runs software security courses specifically tailored for large software development companies. Since its establishment, the laboratory has carried out several R&D projects with topics covering security issues in various fields.

ROLE: SEARCH-LAB leads testbed creation (WP5) and will provide a physical testbed for the partners. SEARCH-LAB takes part in the creation of security requirements, validation activities, TEE toolchain (WP3) and will conduct security testing of the CROSSCON stack. SEARCH-LAB also develops interactive instructor-led online trainings with hardware-based hands-on exercises to showcase the capabilities of the CROSSCON stack.

Barbara

DESCRIPTION: Barbara helps industrial companies in their digitisation process by facilitating Edge IoT in a cyber-secure way. Barbara has developed a Secure Linux based Edge IoT Operating System to govern distributed intelligence, based on standard technology and interoperable with specific solutions for sectors such as energy, water, manufacturing and rail transport. Barbara has been developing technology for the Edge IoT for 5 years, creating, deploying and executing Artificial Intelligence algorithms from different authors, on distributed Edge IoT Nodes.

ROLE: As these Edge IoT Nodes are hardware equipment like the one developed in the CROSSCON project, Barbara focuses on the study of use cases and security guarantees that may be needed by some of the end users to support the CROSSCON stack design process. In addition, within the project Barbara will provide its operating system to use the CROSSCON stack and validate the capabilities and security guarantees it offers.

University of Wuerzburg

DESCRIPTION: The University of Wuerzburg (JMU), located in the city of Wuerzburg, Bavaria, Germany, is a renowned public research university. It has a rich history, having been founded in 1402, and is widely respected for its academic excellence and research capabilities. The university is particularly well known for its strong commitment to computer science education and research, with a well-established department that maintains numerous partnerships with industry and government institutions. The Security of Software Systems Group led by Prof. Dr.-Ing. Alexandra Dmitrienko is actively engaged in various research areas of security, including software security and IoT security.

ROLE: JMU is taking the lead in driving the development of new, novel, trusted services, as well as specifying extension primitives that meet the specific requirements of Domain-Specific Hardware Architectures. In addition to its primary responsibility, JMU contributes its expertise in other areas of the project, such as designing the Open Specification of the CROSSCON Stack.

Technical University of Darmstadt

DESCRIPTION: The Technical University of Darmstadt is one of the leading universities in Germany and Europe in the field of cyber security research and artificial intelligence. As part of the Centre for Research in Security and Privacy, which is funded by the federal and state governments, Darmstadt is one of the central research locations in the field of IT security in Europe. The System Security department of Prof. Dr.-Ing. Ahmad-Reza Sadeghi is involved in the design and development of security architectures and trusted infrastructures with a special focus on hardware security architectures, IoT security and security of AI.

ROLE: The role of TUD within CROSSCON is in contributing its extensive expertise in the area of System Security for developing and Open Specification of the CROSSCON architecture encompassing both hardware and software components. TUD will also contribute in developing novel security services as part of the CROSSCON service stack, in particular in researching ways for trustworthy provisioning of IoT-related workloads on Cloud-based FGPA accelerators.

CROSSCON - MEET THE PARTNERS

Beyond

DESCRIPTION: Beyond Semiconductor is electronics research and development company that works in the field of semiconductor IP and hardware based security. Besides high assurance network encryptors the company's products include data diodes, security and cryptographic IP cores, image and video compression IP, highly efficient (including RISC-V) processors and digital signal processing IP. The company's intellectual property is implemented by some of the world's most renowned semiconductor corporations and shipped in billions of ASICs.

ROLE: As part of the CROSSCON project, Beyond Semiconductor will provide security and hardware related expertise to enable the development of the CROSSCON stack. The contribution includes development of a security enhanced RISC-V based SoC providing extended hardware security guarantees to the CROSSCON stack.

3MDEB

DESCRIPTION: 3mdeb team has been committed to providing innovative solutions for hardware OEMs and ODMs to achieve delivered products' full potential, security, and reliability. We accomplish this by using the Dasharo open-source firmware distributions, which combines coreboot, EDKII, LinuxBoot, U-Boot, and other open-source firmware projects to provide clean and simple code, long-term maintenance, transparent validation, superior documentation, privacy-respecting implementation, liberty for the owners, and trustworthiness for all.

ROLE: In the Crosscon project, we are responsible for creating security validation criteria for IoT devices, including defining their KPIs and ensuring that the security aspects built in the Crosscon stack have a practical dimension, not just a theoretical one.

CYSEC

DESCRIPTION: CYSEC is a Swiss cybersecurity company providing a Confidential Computing software solution which enables companies to secure workloads execution. We help companies to securely deploy their application with highly sensitive data in industries such as financial services, edge applications and space. Our core team has competences in offen sive and defensive IT security, software development, embedded hardware and cryptography.
Based at the EPFL Innovation Park in Lausanne Switzerland, CYSEC has managed since its inception to develop ARCA Trusted OS, a container-specific confidential computing environment, today commercialized with different deployment options from the cloud to the Edge.

ROLE: JMU is taking the lead in driving the development of new, novel, trusted services, as well as specifying extension primitives that meet the specific requirements of Domain-Specific Hardware Architectures. In addition to its primary responsibility, JMU contributes its expertise in other areas of the project, such as designing the Open Specification of the CROSSCON Stack.

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