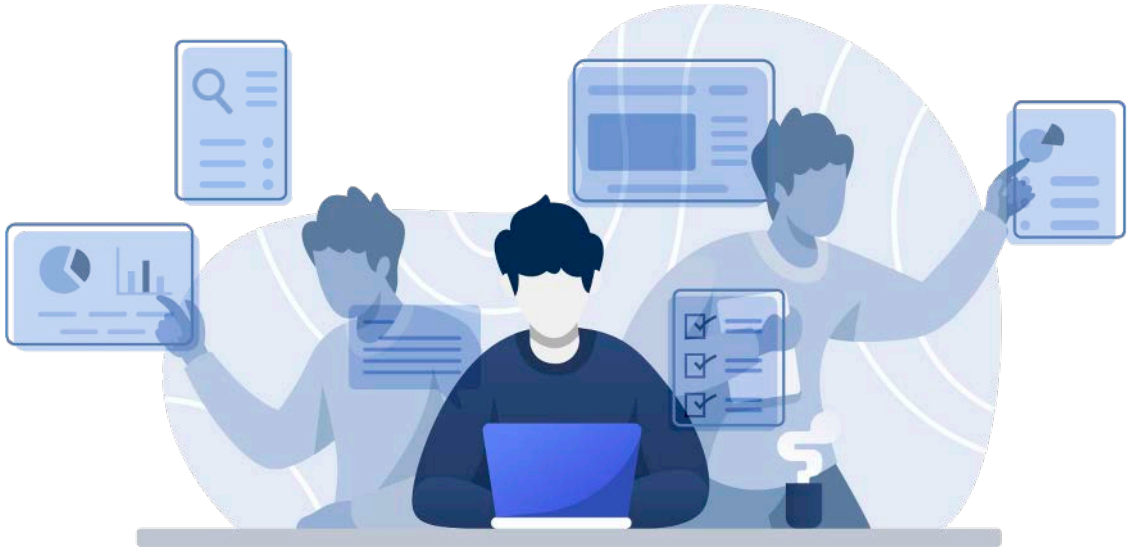
NEWSLETTER #2



CONTENTS:

- Scientific Leader Notes 1

DISSEMINATION UPDATES

- News & Events 2
- External Synergies 5
- Blog Posts 6

PROJECT UPDATES

- Use Cases 4 & 5 7
- Current Results 9
- Scientific Publications 10

As the CROSSCON project enters its second year, it continues to focus on developing an open IoT security stack designed to run seamlessly across various edge devices and multiple hardware platforms.

- Bruno Crispo

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

Scientific Leader Notes

We have released the initial version of the open specifications for the CROSSCON secure stack. Our approach is not to suggest a clean slate, which we find unrealistic, but rather to provide a solution that can enhance the security of existing systems and address gaps where security is currently lacking.

Dear Readers,

Welcome to the second newsletter of CROSSCON! The project started more than a year ago, and we are generating the first results, some of which are illustrated in this newsletter. We released the first version of the open specifications of the CROSSCON secure stack. CROSSCON proposes a modular architecture to support several classes of devices and platforms. The approach was not to propose a clean state, that we consider unrealistic, but rather a solution that could strengthen the security of what already exists and cover some gaps where actually no security is provided. Interoperability is the main driver of the CROSSCON approach; thus, the secure stack supports the Global Platform APIs to guarantee interoperability with existing trusted applications (TAs) as well as interactions with existing Trusted Execution Environments (TEEs).

One of the most important components of the CROSSCON stack is its hypervisor. The current version is a very lightweight standalone hypervisor implementing a static partitioning architecture that assigns resources to each VM at instantiation time. Differently from other existing solutions, it does not rely on any external dependency, and it can run on several platforms such as ARMv8 and RISC-V.

Another novel component of the CROSSCON stack is the software-based TEE designed specifically for bare-metal devices. This allows CROSSCON to cover the low-end of the IoT device's spectrum. Such specialized TEE can run on devices that have no security protection at all, and on those supported with only the memory protection unit (MPU). In terms of trusted services supported by CROSSCON, initial work has been done to design an advanced multi-factor authentication (MFA) scheme suitable for device authentication.

Bruno Crispo
Scientific Leader, Uni. Trento

During this year, the CROSSCON team also continued to explore and study novel threats, attacks, and discover new vulnerabilities on the microarchitectures that are the target of the project. On this end, a remarkable scientific result has been achieved by the University of Minho, that discovered a new microarchitectural side-channel attack in the micro-controller bus interconnect. Result that has been presented at Black Hat community as well as in one of the most prominent cybersecurity scientific conferences: the IEEE Security & Privacy conference. On the side of capacity building, CROSSCON provided the first workshop on the Bao hypervisor, one of the core components of the CROSSCON security stack.

For more details on the above results, please refer to the pages of this newsletter. And, if you're interested in using these outcomes, we recommend exploring the public deliverables of the project and staying updated through our project's website and social media channels.

Bruno Crispo

DISSEMINATION UPDATES

Events

During M6-M12, CROSSCON organized and participated in several events. Here is the summary of what hapenned!

RISC-V Summit Europe

05-09 Jun 2023 | Barcelona, Spain

https://crosscon.eu/events/risc-v-summit-europe-2023

CROSSCON participated and presented at the RISC-V Summit Europe 2023 that took place in Barcelona, Spain. Our poster presentation entitled "Interoperable IoT Security Stack: The RISC-V Opportunity" was a great opportunity to disseminate our main project ideas and goals for the upcoming months.

Encrypt: Clustering Workshop

01 Jun 2023 | Procida, Italy

https://encrypt-project.eu/communication/news/2nd-plenary-meeting-clustering-event/

CROSSCON had the privilege of taking part in the Cluster Workshop hosted by the EU project Encrypt, where we made a significant online presentation. This event provided an invaluable platform for fostering collaboration and synergy among various EU projects by facilitating the exchange of comprehensive scientific and technical insights related to the CROSSCON project.

ERATOSTHENES: Trust and Identity Management for IoT

16 Jun 2023 | Online

https://eratosthenes-project.eu/2nd-workhop-trust-and-identity-management-for-iot-friday-june-16-online/

The CROSSCON Project had the honor of being a participant in the ERATOSTHENES workshop. The primary objective of this workshop was to spotlight emerging innovations and project outcomes while also fostering the identification of collaborative synergies among the participating initiatives.

Events

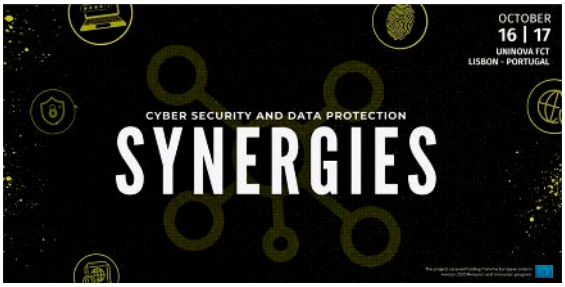
During M6-M12, CROSSCON organized and participated in several events. Here is the summary of what hapenned!

OERN: Segurança em Dispositivos e Aplicações IoT

09 Oct 2023 | Online

https://haengenharia.pt/noticias/video-houve-sessao-tecnica-sobre-seguranca-e-aplicacoes-iot/

During an IoT security and privacy webinar, the CROSSCON project highlighted its role in enhancing security and emphasized its collaborative efforts with academic and industry partners to create a versatile security stack for diverse devices.



Cyber Security and Data Protection

16-17 Oct 2023 | Lisbon, Portugal

https://youtu.be/2oOVyQmb8nw

CROSSCON Project was physically present in the Cyber Security and Data Protection Cluster meeting hosted by the SENTINEL EU project. The workshop aimed to encourage collaboration and synergies among the projects involved in EU cybersecurity. EU project representatives shared project status, results, resources, and expertise.

Bao - Virtual Worshop

15 Nov 2023 | Online

Time: 11am - 1pm (CET)

https://github.com/bao-project

CROSSCON co-organized with BAO Project a virtual workshop about the Bao hypervisor, one of the core components of the CROSSCON security stack!

Nearly 100 participants joined live. In case you missed it, the workshop recording is available here:

https://www.youtube.com/watch?v=6c8_MG-OHYo

Next Events

NECS – PhD Winter School 2024

8-12 Jan 2024 | Cortina d'Ampezzo (Italy)

Program and Registration: https://necs-winterschool.disi.unitn.it/a-

The NeCS PhD School is a good opportunity to present young researchers advances in both attacks and defenses in the realm of cybersecurity. This year, the School is supported by the Horizon Europe project: CROSSCON, and by the Marie Skłodowska-Curie Action: DUCA. Confirmed speakers include Dr. Alexandra Dmitrienko (Universität Würzburg), Dr. Ahmad-Reza Sadeghi (TU Darmstadt), and Jurij Mihelic (Beyond Semiconductor) from CROSSCON.

CROSSCON Workshop - Security Services for Connected Devices

12 Jan 2024 | Cortina d'Ampezzo (Italy)

This workshop addresses challenges in the IoT security stack across diverse devices and platforms. It covers security approaches, their development, and technology adoption. The focus includes fundamental building blocks in connected devices, along with applications and use cases from various EU projects emphasizing security across heterogeneous connected devices.

CROSSCON course on TEEs

17Jan 2024 | 08:00 – 16:00 (WET) | Online

Attend here: https://t.ly/3DXgw

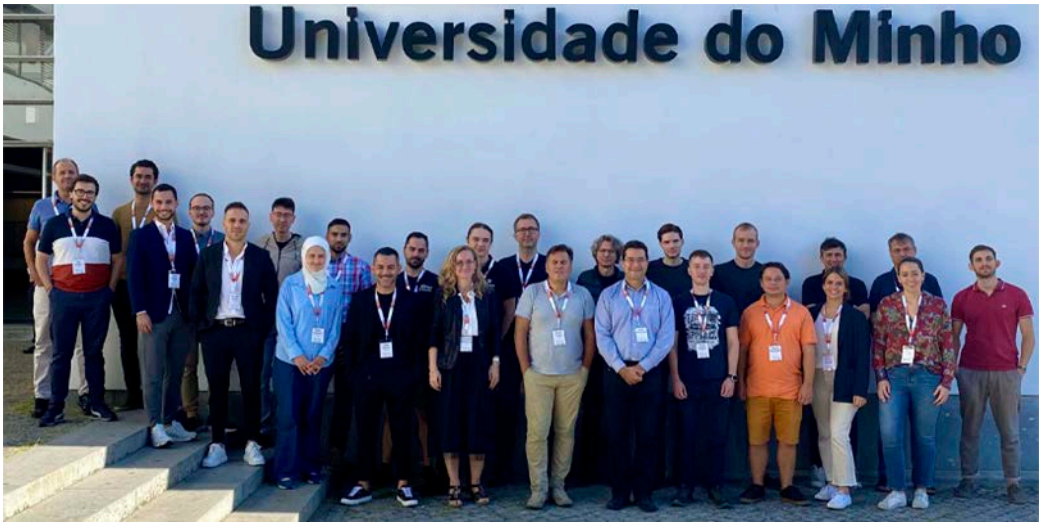
SEARCH-LAB
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY

Our partner, Search-Lab, based in Budapest (Hungary), specializes in security testing and evaluation of ICT products, with a particular focus on the security of embedded systems like mobile devices. They will be delivering an online course about Trusted Execution Environments (TEEs), open to everyone. Search-Lab, through its Secure Coding Academy, regularly conducts software security courses tailored for large software development companies.

Stay tuned for additional details!

DISSEMINATION UPDATES

News



3rd GA Meeting

03-04 Oct 2023
Guimarães, Portugal

The CROSSCON consortium just gathered at the Universidade do Minho in Guimarães (Portugal) for a productive meeting filled with insightful discussions and valuable outcomes.

https://crosscon.eu/news/crosscon-3rd-ga-meeting

Media Hits Digital

SAPOTEK | AICEP | PC-GUIA | BUSINESS.IT | PME | MAGAZINE | ALGORITMI | EXAME INFORMÁTICA
https://crosscon.eu/news/media-hits-digital

External Synergies

SecOPERA

https://secopera.eu/

SecOPERA aims to provide a one-stop hub for complex OSS/OSH solutions delivering to a connected device designer, implementer and operator as well as any open-source software/hardware developer, the means to analyse, assess, secure/harden and share open-source solutions as those are integrated in an overall complex product developed for a networked connected environment.

ARCADIAN-IoT aims to develop and make available an innovative, advanced, solid framework for trust, security and privacy management for IoT systems. The ARCADIAN-IoT framework will accelerate the development of IoT systems towards decentralized, transparent and user controllable privacy in three real use cases.

ARCADIAN-IoT

https://www.arcadian-iot.eu/

ENTRUST

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

ENTRUST sits at the forefront of digital transformation for the Healthcare domain as it moves into the next generation of Connected Medical Devices, where the expansion of connectivity and data processing capabilities and resources at the edge have revolutionized the health sector by improving outcomes, lowering healthcare costs, and enhancing patient safety.

Blog Posts

TEEs are not Silver Bullets

Trusted Execution Environments (TEEs) are secure execution environments that provide hardware-based isolation and protection for Trusted Applications (TAs) and data on a device. They are designed to offer a secure computing environment that is isolated from the main operating system and other applications on the device, i.e., the Rich Execution Environment (REE).

Read more: https://crosscon.eu/blog/tees-are-not-silver-bullets

David Cerdeira
R&D Engineer
University of Minho

Enhancing Security in Agricultural UAVs: The Power of Remote Attestation

In today's modern agricultural landscape, Unmanned Aerial Vehicles (UAVs), commonly known as agricultural drones, are revolutionizing the way farmers operate. Equipped with advanced sensors and cameras, these UAVs provide invaluable data on crops and soil, enabling farmers to make informed decisions regarding planting, fertilization, irrigation, and pest control.

Read more: https://crosscon.eu/blog/enhancing-security-agricultural-uavs

Malvina Catalano
R&D Scientist
CYSEC

Cybersecurity is a Community Effort

Undoubtedly, deploying Internet of Things (IoT)-connected devices, whether they are sensors, edge gateways, or large equipment, presents significant challenges in terms of usability and security. Contrary to what might be assumed, achieving seamless usability and robust security for connected devices proves exceedingly complex.

Read more: https://crosscon.eu/blog/cybersecurity-community-effort

David Purón
CEO
Barbara IoT

Enhancing IoT Security through Device-to-Device Authentication

In the contemporary digital realm, the principle of multi-factor authentication (MFA) has become a cornerstone, especially in sectors like banking. Traditionally, authentication is the act of proving an assertion, such as the identity of a computer system user.

Read more: https://crosscon.eu/blog/enhancing-iot-security-through-device-device-authentication

Rafał Kochanowski
Senior Project Manager
3MDEB

Information Flow Tracking: Enhancing Data Security and Privacy

Information flow tracking is an area of computer security that focuses on studying methods and techniques used to monitor and control the movement of data within an information processing system as well as the movement of data across the system's boundaries, where communication with the world external to the system takes place.

Read more:
https://crosscon.eu/blog/information-flow-tracking-enhancing-data-security-and-privacy

Jure Mihelič
Senior Project Manager
Beyond Semiconductor

PROJECT UPDATES

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

Agricultural UAVs (Unmanned Aerial Vehicles), also known as agricultural drones, are becoming an increasingly important tool in modern agriculture. These UAVs are equipped with sensors and cameras that can gather data on crops and soil, allowing farmers to make more informed decisions about planting, fertilization, irrigation, and pest control.

Some of the benefits of using agricultural UAVs include:

Improved efficiency: UAVs can cover large areas of farmland quickly and accurately, reducing the time and cost of traditional methods such as manual labor or satellite imaging.

Precision agriculture: UAVs can provide detailed, high-resolution data on soil moisture, nutrient levels, and plant health, enabling farmers to apply fertilizers, pesticides, and water precisely where they are needed, reducing waste and increasing yields.

Reduced environmental impact: By providing farmers with precise data, agricultural UAVs can help reduce the amount of pesticides and fertilizers that are applied to crops, minimizing their impact on the environment.

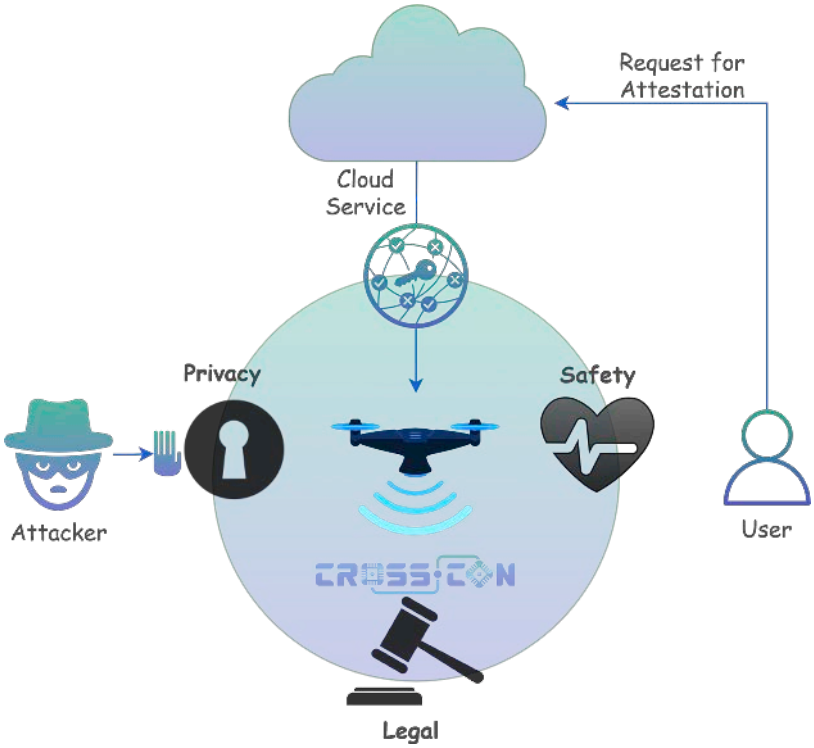
Increased safety: UAVs can be used to monitor crops and livestock without putting farmers at risk of injury or exposure to hazardous chemicals.

While agricultural UAVs offer many advantages, they also pose some security-related challenges that need to be addressed such as:

Privacy concerns: Agricultural UAVs can gather a large amount of data on crops, soil, and other aspects of farmland, raising concerns about privacy and data security.

Unauthorized access: Agricultural UAVs can be stolen, hacked or used for malicious purposes if they fall into the wrong hands, potentially causing damage to crops, property, or even human life.

Legal and regulatory compliance: Agricultural UAVs are subject to a range of regulations and restrictions, such as registration requirements, flight restrictions, and privacy laws, which can be complex and difficult to navigate.



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

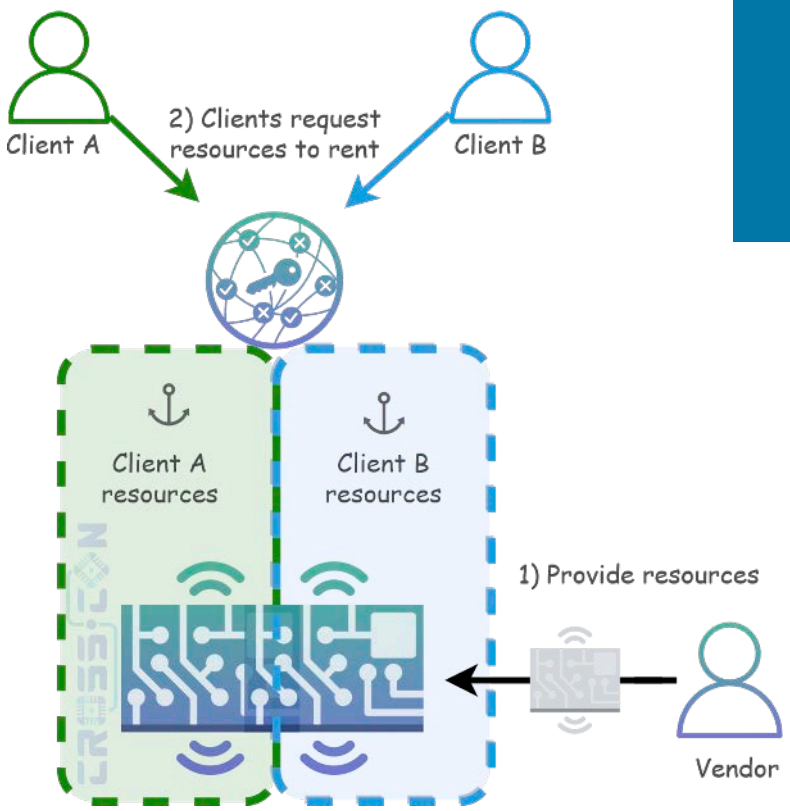
Due to limitations in computational and memory capacity, many IoT nodes are limited in what kind of workloads can be executed on them. Especially compute-intensive tasks related to, e.g., training and inference of AI algorithms can be too heavy operations for IoT devices to handle themselves.

There is therefore a need to offload compute-intensive tasks to accelerator nodes that are accessible over the network. In particular, FPGA-based accelerators offered by Cloud Service providers are here of interest, as they offer the possibility for highly efficient computations of compute tasks optimised for the the task at hand.

To reduce the cost of such "FPGA as a service" offerings, it is highly desirable for the cloud service providers to be able to provision the compute workloads of several different clients onto the same FPGA fabric, thereby enabling multi-tenancy on the FPGA. A key question here is, how secure multi-tenancy can be assured so that workloads of one tenant can not have adverse effects on the workloads of other tenants or the FPGA fabric itself and does not lead to unintended leakage of private information processed on the FPGA.

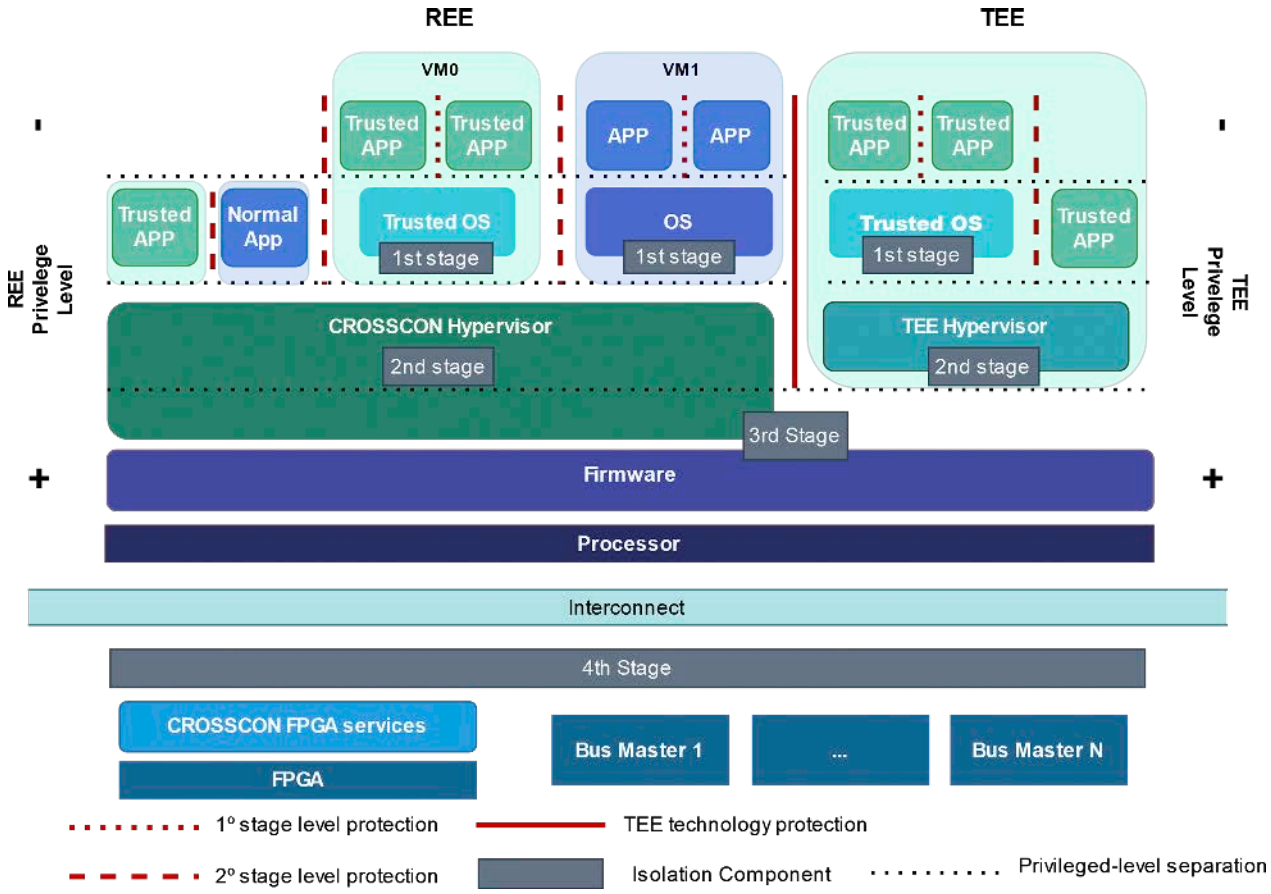
One can distinguish between temporal and spatial multi tenancy. In temporal multi-tenancy, only one client has access to the entire FPGA fabric at a time. Multi-tenancy is thus achieved through alternation of the entire FPGA resource to different clients at different times.

The goal of this use case is therefore to demonstrate secure spatial multi-tenancy on an FPGA fabric offered as a cloud-based service. The particular challenge to be solved here is related to the confidentiality of the proprietary IP to be provisioned on the FPGA: How can the cloud service provider verify that the IP does not contain any malicious payloads potentially having adverse effects on the FPGA or leading to data leakage of other tenants, while at the same time preserving the confidentiality of the IP in order to protect the client's intellectual property?



CROSSCON HYPERVISOR

Community efforts have underscored the potential of hypervisor components in overseeing trusted applications (TA) in connected devices. In the CROSSCON abstract model hypervisor component is situated immediately above the firmware and its objective is to create and support distinct and isolated virtual machines (VMs), ensuring they run as if they were operating independently on separate hardware. For effective resource isolation, including shared architectural resources like last-level caches, interconnects, and memory controllers, the hypervisor may adapt its security features according to the underlying hardware. Its design varies based on the specific ISA it operates on. For example, in APU processors, the hypervisor leverages virtualization extensions, including 2nd stage translation and other virtualization techniques, to establish isolation between virtual machines. In contrast, in simple MCU processors, the hypervisor employs components that restrict access to physical memory for each guest without the need for hardware mechanisms.



CROSSCON intends to provide a hypervisor that allows hardware resources to not be shared across VMs and provide a set of built-in mechanisms (e.g., cache coloring) to guarantee strong isolation not only at the architectural but also micro-architectural level. The idea is to complement a TEE architecture with a thin static partitioning hypervisor layer to achieve enhanced isolation and security guarantees through a micro-kernel-like design. The hypervisor will ensure the correct enforcement of the access control policies to guarantee that VMs can securely execute security-sensitive workloads, for example, running a Trusted OS and TAs. Addressing the lack of flexibility to dynamically create and manage new VMs and services on static partitioning hypervisors is the objective of task T2 of WP3.

PROJECT UPDATES

Latest Publications

Shedding Light on Static Partitioning Hypervisors for Arm-based Mixed-Criticality Systems

Martins, José, and Sandro Pinto. "Shedding Light on Static Partitioning Hypervisors for Arm-based Mixed-Criticality Systems." arXiv preprint arXiv:2303.11186 (2023).
https://arxiv.org/abs/2303.11186

Efficient and Safe I/O Operations for Intermittent Systems

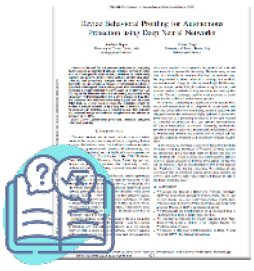
Eren Yildiz, Saad Ahmed, Bashima Islam, Josiah Hester, and Kasim Sinan Yildirim. 2023. Efficient and Safe I/O Operations for Intermittent Systems. In Proceedings of the Eighteenth European Conference on Computer Systems (EuroSys '23).
https://dl.acm.org/doi/abs/10.1145/3552326.3587435

Interoperable IoT Security Stack: The RISC-V Opportunity

Sandro Pinto, Matjaz Breskvar, Tiago Gomes, Hristo Koshutanski, Aljosa Pasic, et al., "CROSSCON: Interoperable IoT Security Stack The RISC-V Opportunity", In RISC-V Summit Summit Europe 2023, 5-9 June 2023, Barcelona, Spain.
https://crosscon.eu/sites/crosscon/files/public/content-files/2023-06/POSTER-RISCV-SUMMIT-2023.pdf

BUSted!!! Microarchitectural Side-Channel Attacks on the MCU Bus Interconnect

Cristiano Rodrigues, Daniel Oliveira, and Sandro Pinto, "BUSted!!! Microarchitectural Side-Channel Attacks on the MCU Bus Interconnect", 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2024.
https://bustedattack.com/resources/BUSted.pdf



Device behavioral profiling for autonomous protection using deep neural networks

S. Gupta and B. Crispo, "Device Behavioral Profiling for Autonomous Protection Using Deep Neural Networks," 2023 IEEE Symposium on Computers and Communications (ISCC), Gammarth, Tunisia, 2023.
https://ieeexplore.ieee.org/document/10218275

AppBox: A Black-Box Application Sandboxing Technique for Mobile App Management Solutions

M. Ahmad, F. Bergadano, V. Costamagna, B. Crispo and G. Russello, "AppBox: A Black-Box Application Sandboxing Technique for Mobile App Management Solutions," 2023 IEEE Symposium on Computers and Communications (ISCC), Gammarth, Tunisia, 2023, pp.
https://ieeexplore.ieee.org/abstract/document/10217861

µIPS: Software-Based Intrusion Prevention for Bare-metal Embedded Systems

Luca Degani, Majid Salehi, Fabio Martinelli, and Bruno Crispo, "µIPS: Software-Based Intrusion Prevention for Bare-metal Embedded Systems", 28th European Symposium on Research in Computer Security (ESORICS), The Hague, The Netherlands, September 25-29, 2023.
https://esorics2023.org/program/accepted_papers/

Next Release

NEWSLETTER #3

It will be released by the end of Q2 2024

Meanwhile, stay up-to-date with other important CROSSCON's News by subscribing and following our social media channels!

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

Subscribe the newsletter:
https://crosscon.eu/