CROSSCON: Interoperable IoT Security Stack for Embedded Connected Devices

Tiago Gomes
Centro ALGORITMI, UMinho
Guimarães, Portugal
mr.gomes@dei.uminho.pt

Sandro Pinto
Centro ALGORITMI, UMinho
Guimarães, Portugal
sandro.pinto@dei.uminho.pt

Abstract - **The number of Internet of Things (IoT) embedded devices is estimated to reach 30 billion by 2030, leading to a highly dynamic landscape where distinct devices have to coexist. The rapid proliferation of different architectures and platforms requires a unified solution that can be supported by different devices, while providing a wide range of services to cope with the ongoing challenges of connecting devices to the Internet. CROSSCON, a 3-year Research and Innovation Action funded under Horizon Europe, aims to address these challenges by designing a new open, modular, highly portable, and vendor-independent IoT security stack that can run on various devices using heterogeneous embedded hardware architectures, such as ARM and RISC-V. At this stage of development, CROSSCON already specifies a unified level of abstraction, encompassing several components across multiple heterogeneous hardware platforms. It currently supports a bare-metal TEE for constrained devices, and novel security features provided by the CROSSCON hypervisor, such as per-VM TEE and Dynamic VM creation.**

Keywords—Internet of Things (IoT); Security Stack; CROSSCON; Interoperability; RISC-V; Arm.

I. INTRODUCTION

The Internet of Things (IoT) landscape is composed of billions of heterogeneous devices [1], ranging from bare-metal embedded systems with a few kilobytes of RAM and limited or inexistent security capabilities, to devices equipped with built-in hardware to implement the Root of Trust (RoT) and Trusted Execution Environments (TEEs) [2,3]. Such reality is the zeitgeist in the IoT, and it is still an open challenge to guarantee an acceptable level of security across the whole IoT spectrum [4,5]. A typical IoT stack infrastructure can be quite complex, involving several layers, such as hardware, firmware, hypervisor, operating system (OS), applications, and much more, each one enlarging the attack surface and opening many breaches to traditional and new attacks [5]. In addition to these challenges, the deployment of a security solution for the already broad IoT landscape is not straightforward, as it becomes harder to understand the security features and mechanisms underneath the different architectures currently being used.

The CROSSCON security stack aims at addressing various challenges in the design and deployment of a trusted and secure solution across heterogeneous IoT devices, requiring TEE abstraction and isolation features, new hypervisor mechanisms to handle heterogeneous guests, a bare-metal TEE implementation, novel trusted services, and a robust toolchain for facilitating its development, configuration, and full deployment. This approach facilitates and promotes interoperability across different devices and architectures, while supporting different isolated environments to securely run trusted applications. The novel hypervisor features include a per-VM TEE mechanism that distributes multiple TEE through VMs, and a dynamic VM creation. Finally, at the bottom of the stack, lies several security primitives that will guarantee the deployment of novel security features to assist a wide broad of present-day use cases.

In this paper, we present an overview of the CROSSCON project, highlighting the motivations that triggered its realization, as well as the use cases that will pioneer the deployment of the CROSSCON stack and supported services. Focusing with more detail on work package WP3, which is led by the University of Minho, we provide an overview of the security stack and how it can serve both RISC-V and ARM-based embedded devices. Finally, we present the project roadmap and short-term steps.

II. CROSSCON IN A NUTSHELL

A. Project Overview & Motivation

Lack of Open-Source Hardware Solutions: Most IoT solutions rely on proprietary hardware with closed-source licenses, limiting innovation and collaboration. CROSSCON aims to address this challenge by designing an open, modular, and highly portable IoT security stack that can run on a wide range of devices with heterogeneous hardware architectures. By providing open specifications and an open-source reference implementation, CROSSCON fosters collaboration and innovation in the development of IoT solutions.

Lack of Root- and Chain-of-Trust: CROSSCON focuses on establishing a robust security foundation for IoT ecosystems by incorporating strong RoT and CoT mechanisms into its security stack. By ensuring the integrity and authenticity of device identities and communications, CROSSCON enhances trustworthiness among users and stakeholders in IoT environments.

Lack of Interoperability Between IoT Devices: CROSSCON addresses this challenge by providing a unified set of APIs for accessing TEE functionalities and trusted services across different hardware platforms. By promoting interoperability, CROSSCON enables seamless connectivity and communication among diverse IoT devices, enhancing the overall efficiency and effectiveness of IoT ecosystems.

High Costs of Developing Trusted Services: Developing secure IoT services requires specialized hardware, security expertise, and extensive testing processes. CROSSCON offers an open, modular, and cost-effective IoT security solution, making trusted service development accessible to a broader audience.

Vulnerabilities in Core Trust Components: Security flaws in crucial trusted components can undermine the reliability of IoT systems. CROSSCON focuses on strengthening key trusted components within its security stack through formal verification of its security stack design and implementation. This ensures the integrity and reliability of the CROSSCON IoT security stack, mitigating vulnerabilities and enhancing the overall security posture of IoT systems.

B. Use Cases

UC1 - Device Multi-Factor Authentication: One of the main challenges of IoT devices is the access and authorization to the network or other specific resources. In recent years, Physically Unclonable Functions (PUFs) have been proposed as a solution for device authentication in constrained devices, mainly due to the scarcity of resources that hamper the utilization of regular cryptographic operations. However, PUF-based authentication has proven to be challenging to implement in practice and is vulnerable to a variety of attacks. CROSSCON proposes a multi-factor authentication (MFA) solution for IoT devices to improve their security and overcome the limitations of PUF-based authentication, providing a more robust defense against MITM (Man-in-the-Middle) attacks. The new authentication features are based on context and behavioral authentication, which may include both traditional authentication methods (PUF, private/public key scheme, and other credentials), and novel PUF-based authentication combined with environmental factors such as the network where the device is connected.

UC2 - Firmware Updates of IoT Devices: It is very common to find IoT devices in the field without a secure firmware update system [6,7]. Even those devices having firmware update mechanisms are in many cases not updated. An analysis performed over a total of 1.061.284 IoT devices shows the average age of the installed firmware is 19.2 months [8], leading to many vulnerabilities uncovered during large periods of time. 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. Updates and security patches can be digitally signed, so 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; and (iii) digital signatures do not give any guarantee on the logic of the update. CROSSCON aims at addressing the device's firmware update problem by providing a secure partial and full firmware update solution.

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, which can include security certificates, credentials, application configuration, and more. 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. The current solutions in the market, especially for resource-constrained devices, do not allow in many cases to generate unique random keys per device in a multi-stakeholder environment. This ends up in many cases with devices shipping with default and hard-coded credentials that can be exposed to attackers, which by stealing device secrets, can gain extra privileges within the device. CROSSCON is committed to implementing robust commissioning and decommissioning, ensuring the highest levels of security and reliability in IoT device operations.

UC4: Remote Attestation for Identification and Integrity Validation of Agricultural Unmanned Aerial Vehicles (UAVs): Agricultural UAVs are essential for helping farmers in several tasks, e.g., seeding, fertilizing, irrigating, and pest controlling. Nevertheless, they also bring several privacy- and safety-related challenges. With a remote attestation feature, a method by which a client authenticates its hardware and software configuration to a remote host, we can ensure that a UAV runs a trusted software and hardware stack that meets the privacy, safety, and legal requirements.

UC5: Intellectual Property Protection for Secure Multi-Tenancy on FPGA: Reconfigurable technology can be used for deploying compute-intensive tasks. To optimize its resource utilization, multiple tenants can share the reconfigurable platform. However, considering the security requirements of the CROSSCON stack, these resources must be temporal and/or spatially isolated. While the former ensures that one tenant has access to resources at a time, the latter provides access to different resources according to the tenant, supporting simultaneous tenants accessing the FPGA. This use case aims at providing secure multi-tenancy, ensuring that the workload of one tenant cannot interact with others nor affect the hardware resources, and that no data can be leaked by any means.

C. Main Work Packages

WP2 - Design Specification and Assurance for IoT: This work package focuses on establishing the foundational specifications and design framework for the CROSSCON architecture. This involves defining an open specification for the CROSSCON security stack, establishing a formal design framework for IoT safety and assurance, and specifying a uniform security stack deployable across different TEEs. The goal is to create a flexible and adaptable architecture that ensures the secure execution of sensitive tasks across diverse IoT devices. The specifications developed in WP2 serve as the basis for WP3 and WP4.

WP3 - Development of CROSSCON Security Stack. This WP aims to strengthen the CROSSCON architecture's functionality and security. These objectives include defining new trusted services, establishing a robust toolchain for the development and deployment of the stack, creating a comprehensive security manifest, and developing specifications to abstract different TEE models and architectures. Additionally, WP3 aims to enhance TEE isolation capabilities, address hypervisor limitations, and develop CROSSCON TEE for bare metal devices. These efforts collectively contribute to fortifying the security infrastructure of CROSSCON across various IoT environments.

WP4 CROSSCON for Domain-Specific Hardware Architectures. The WP4 focuses on enhancing the security and flexibility of IoT devices. It emphasizes the development of a custom System-on-Chip (SoC) to overcome the limitations of off-the-shelf options, aiming for greater control and security. WP4 is responsible for defining hardware primitives for trusted services, ensuring seamless enforcement of dynamic data properties across CPUs and hardware accelerators, enabling TEEs on FPGA, integrating dynamic data properties enforcement into the SoC interconnect and hardware accelerator IP blocks, and assessing the performance implications of these security measures.

III. Development of the CROSSCON Security Stack

A. Bao Hypervisor

Bao [9] is a static partitioning hypervisor that serves as the foundation of the CROSSCON hypervisor. It provides strong isolation between different partitions, not just limited to the architectural level, isolating VMs from each other, but extends to the microarchitectural level as well. CROSSCON achieves this isolation by implementing built-in mechanisms like cache coloring, which ensures isolation for shared resources such as last-level caches. Bao, which initially targeted Armv8-A, includes now support for RISC-V [10,11] and with Armv7-A and Armv8-R ports as work in progress. Bao is maintained by the Bao Project, and is open source under the Apache 2.0 license, allowing free use for commercial applications.

B. CROSSCON Security Stack

The CROSSCON system stack is highly configurable. It may comprise a combination of several components, leading to a wide range of instantiation options. A CROSSCON system stack can go from a bare metal environment running in a microcontroller (MCU) platform with one privilege level, to a complex system stack in an Accelerated Processing Unit (APU) platform featuring multiple environments around four privilege levels. Figure 1 depicts a high-level representation of the CROSSCON architecture, encompassing all instantiation possibilities. CROSSCON strives to achieve a similar level of protection across various instantiation options, offering a unified level of abstraction across multiple hardware platforms.

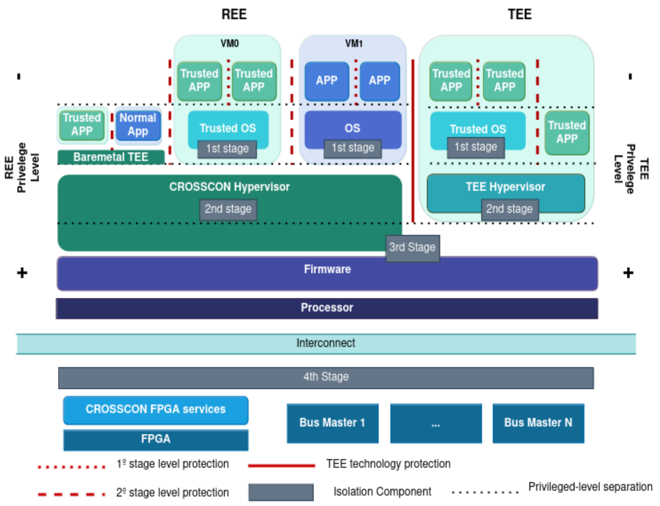

Figure 1 - CROSSCON Security Stack Model.

There are two high-level scenarios for the CROSSCON stack. The first is the support for a software-only TEE in platforms not featuring hardware isolation mechanisms, and the second one is where the isolation mechanisms present in the platform are used to create isolated environments, including TEEs. The CROSSCON instantiated TEEs can be either stand alone, useful for platforms not featuring TEE mechanisms, or complement built-in TEE solutions, for example, to decompose the trusted services hosted in a single TEE environment into multiple mutually isolated environments.

C. CROSSCON Hypervisor

CROSSCON hypervisor builds upon Bao. The use of a thin static partitioning hypervisor layer helps in maintaining a minimal TCB, which is crucial for upholding high-security guarantees. Existing technologies often rely on a large general-purpose OS or hypervisor, preventing widespread adoption. CROSSCON's approach can be applied to a broad range of devices by reducing the platform resource requirements. However, leveraging a static partition hypervisor comes with its own set of challenges, such as the lack of flexibility to dynamically create and manage new VMs and services. These challenges are addressed by enhancing the static partitioning design of the Bao hypervisor [12].

Depending on the ISA and the class of the device, the hypervisor leverages a high privileged level. CROSSCON hypervisor supports both RISC-V and Arm architectures. This multi-architecture support contributes to the interoperability objectives of the project. Figure 2 represents the CROSSCON security stack instantiation for a RISC-V system with virtualization support. Each VM is isolated from the rest of the system via a second-stage memory protection mechanism, e.g., 2-stage MMU or 2-stage MPU. The hypervisor will then manage the physical resources, assigning them to the various VMs. On top of handling the physical resources, the hypervisor is entrusted with instantiating various VMs, including VMs loaded dynamically upon request. For instance, an untrusted VM can request the allocation of a trusted application, which will be bootstrapped on demand by the hypervisor and then destroyed when no longer needed. All communication between different VMs is enabled through the hypervisor, which securely establishes a shared memory region between VMs. The system TEE is supported for both ARM, i.e., TrustZone[13], and RISC-V, leveraging the PMP. The bare-metal TEE, which only leverages software techniques to isolate execution, is also not necessary in this CROSSCON instantiation, as the CROSSCON hypervisor leverages the platform's hardware isolation mechanisms.

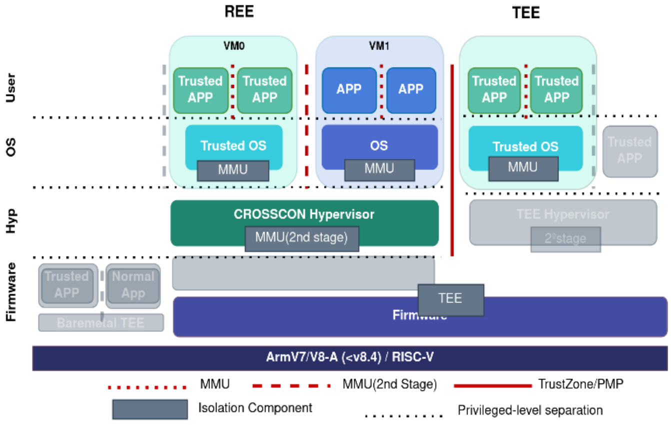

Figure 2- CROSSCON Stack Instantiation for ARM and RISC-V Architectures.

D. *CROSSCON Bare-metal TEE*

Bare-metal devices are widely employed in both industry and research due to their cost-effectiveness and power efficiency. However, the features offered by such devices are very limited, featuring minimal memory resources and forsaking security features often present on higher-end devices, e.g., memory management units and hardware TEEs. As a result, the security of bare-metal devices is usually dependent on the applications deployed on top of them. CROSSCON proposes a bare-metal TEE to allow bare-metal systems to interact securely with the rest of the CROSSCON stack. In the absence of the basic security hardware, e.g. the MPU, CROSSCON resorts to an extremely compact and stripped-down TEE with only the most basic security services. Memory isolation must be implemented purely in software through software instrumentation and instruction virtualization. However, if an MPU is present, the CROSSCON Bare-metal TEE uses it to isolate applications.

I. PROJECT STATUS & ROADMAP

A. *Project Status*

Integration with OP-TEE (Arm and RISC-V). OP-TEE has been integrated with CROSSCON hypervisor to execute within VMs, Figure 3, in both Arm and RISC-V. This feature enhances security by enabling per-VM TEE services and splitting a single TEE system into multiple isolated TEEs. To support OP-TEE in CROSSCON, two VMs are instantiated at boot time, booting the VM with the trusted OS (secure world) before the VM executes the normal world OS (normal world). The configuration file establishes the resources belonging to each VM. Naturally, CROSSCON hypervisor relies on secure integration into the platform's secure boot. A request for the Trusted OS typically originates from an application, which then interacts with the trusted OS driver that will perform firmware calls, SMC calls in Arm, and ECALLS in RISC-V. These calls are transparently intercepted by the hypervisor, which then performs a VM context switch to the trusted OS VM. The trusted OS VM currently only supports OP-TEE Trusted OS, other Trusted OSes require direct support. This system can further be configured to host several GPOS and trusted OS VMs depending on the system design and requirements.

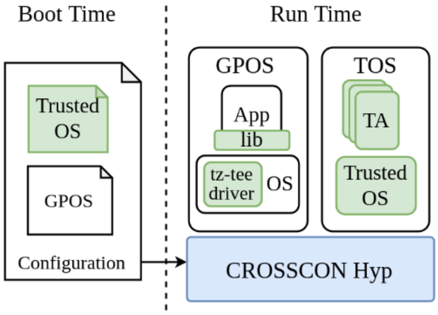

Figure 3 - Per-VM TEE Feature of CROSSCON Hypervisor.

CROSSCON-Hypervisor Dynamic VMs. For dynamic VM creation, the CROSSOCN hypervisor interface enables VMs to create new VMs via a *request creation* hypervisor call. The hypervisor then instantiates the child VM while donating all necessary resources, except physical CPUs, from the parent VM. The physical CPUs are not removed as they are shared between parent and child VMs. Figure 4 depicts a parent VM boot time setup and the dynamic creation of a child VM.

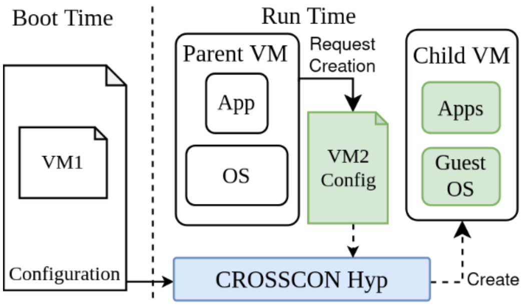

Figure 4 - Dynamic VMs Feature of CROSSCON Hypervisor.

B. Roadmap

The CROSSCON stack development also encompasses trusted services. Novel trusted services will complement existing services such as secure boot, remote attestation, cryptographic and secure storage. The plan is to design, implement, and validate the correctness of the novel trusted services, specifically: PUF- and context-based authentication, control flow integrity and secure firmware update. Further, CROSSCON will support a trusted service manifest that will be used to verify the composition of the CROSSCON stack.

IV. Conclusion

This paper presented the CROSSCON project, a security stack that targets the current heterogeneity of the IoT landscape. It shows the current development of the project, highlighting the security stack specification, components, and its security features including TEE abstraction and isolation, and novel hypervisor features, already tested and supported on different devices and architectures currently being deployed at the edge.

Acknowledgments

This work is supported by FCT – Fundação para a Ciência e Tecnologia within the R&D Units Project Scope UIDB/00319/2020; and European Union’s Horizon Europe research and innovation program under grant agreement No 101070537, project CROSSCON (Cross-platform Open Security Stack for Connected Devices).

References

[1] P. Sparks, “The route to a trillion devices - The outlook for IoT investment to 2035,” Arm White Paper, 2017.

[2] Michele Grisafi et al. “PISTIS: Trusted Computing Architecture for Low-end Embedded Systems”. In: USENIX Security. 2022.

[3] David Cerdeira et al. “ReZone: Disarming TrustZone with TEE Privilege Reduction”. In: USENIX Security. 2022.

[4] O. Alrawi, C. Lever, M. Antonakakis and F. Monrose, “SoK: Security Evaluation of Home-Based IoT Deployments." IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019.

[5] David Cerdeira, Nuno Santos, Pedro Fonseca, Sandro Pinto. "SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems." IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020.

[6] K. Zandberg, K. Schleiser, F. Acosta, H. Tschofenig and E. Baccelli, "Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check," in IEEE Access, vol. 7, 2019.

[7] A. Kolehmainen, "Secure Firmware Updates for IoT: A Survey," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 112-117.

[8] F. Ebbers, "A Large-Scale Analysis of IoT Firmware Version Distribution in the Wild," in IEEE Transactions on Software Engineering, 2022.

[9] J. Martins et al., “Bao: A Lightweight Static Partitioning Hypervisor for Modern Multi-Core Embedded Systems,” Workshop on NG-RES, 2020.

[10] Sá, Bruno, José Martins, and Sandro Pinto. "A first look at RISC-V virtualization from an embedded systems perspective." IEEE Transactions on Computers 71.9 (2021): 2177-2190. 19.

[11] B. Sa et al., “CVA6 RISC-V Virtualization: Architecture, Microarchitecture, and Design Space Exploration,” arXiv:2302.02969, 2023.

[12] Martins, José, and Sandro Pinto. "Shedding light on static partitioning hypervisors for Arm-based mixed-criticality systems." 2023 IEEE 29th Real-Time and Embedded Technology and Applications Symposium (RTAS). IEEE, 2023.

[13] S. Pinto and N. Santos, “Demystifying Arm TrustZone: A Comprehensive Survey,” ACM Comput. Surv., vol. 51, no. 6, pp. 1–36, 2018.