SECURE PLATFORM FOR ICT SYSTEMS ROOTED AT THE SILICON MANUFACTURING PROCESS

Caaliph Andriamisaina *[1], Farhat Thabet [1], Jean-Roch Coulon[2], Guillaume Chauvon[2], Alejandro Cabrera Aldaya[3], Nicola Tuveri[3], Macarena C. Martínez-Rodríguez [4], Piedad Brox[4]

[1]Université Paris-Saclay, CEA, List, Palaiseau, France
[2]Thales Secure Silicon, Meyreuil, France
[3]Tampere University, Tampere, Finland
[4]Microelectronics Institute of Seville (CSIC/ University of Seville), Seville, Spain

Abstract

The digital transformation is accelerating and requires the design of secure and privacy-enhancing technologies to guarantee trust on electronic devices that support it. In this context, it is designed a platform that integrates a hardware dedicated Root-of-Trust and a RISC-V processor core with the capability of offering a full suite of security services. The platform will be able to leverage this capability to support cryptographic protocols, privacy respectful attestation mechanisms, and enable trusted communication channels across 5G network infrastructures.

Introduction

The evolution of our interconnected society brings multiple layers of cloud, edge computing, and Internet of Things (IoT) platforms that continuously interact with each other. The boom of digitalization demands infrastructures to develop functional engineering solutions in a short time. However, security issues were not studied in deep.

The "Secure Platform for ICT Systems Rooted at the Silicon Manufacturing Process" (SPIRS) EU-funded project addresses innovative approaches to provide security and data privacy to future Information and Communications Technology (ICT) elements [1]. This project encompasses the complete design of a SPIRS platform, which integrates a dedicated hardware Root of Trust (RoT) and a RISC-V processor core.

The hardware RoT in SPIRS is the source of trust for the entire system that is built over it. The security of software components (execution environment, boot process, applications) relies on identifiers, random numbers, and cryptographic functions that are provided by the RoT. In SPIRS, the RoT can be composed of several modules. This flexibility to add or remove components allows to generate ad-hoc RoTs that guarantee efficient implementations for particular applications. Moreover, the RoT is conceived as an evolving element, that can be updated over time.

The RISC-V core used in SPIRS is SPRITZ, provided by Thales in the framework of the OpenHW group. To build a complete solution, the SPIRS project also features a Trusted Execution Environment (TEE).

This contribution presents the first prototype of the SPIRS platform that integrates the SPRITZ core and a preliminary version of the hardware RoT, running a demo that shows the communication from both the RISC-V processor and the RoT to the High-Level Operating System (HLOS) through the TEE.

SPIRS Platform

The SPIRS platform (Figure 1) called also Common Programmable Platform (CPP) consists of a RISC-V core called SPRITZ, RoT components, some peripherals (Ethernet, UART, SPI, JTAG, Boot ROM, PLIC and CLINT), and a DDR3 memory. All these components are connected through an AXI4 interconnect.

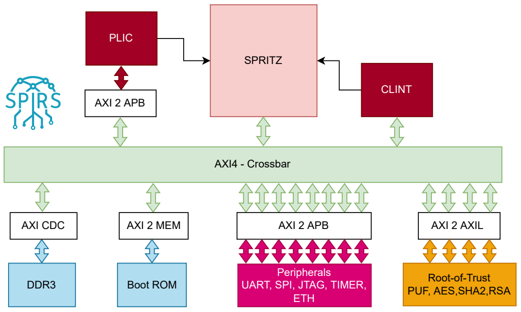

Figure 1: *Platform*

Hardware

SPRITZ The OpenHW Group runs a project overseeing the design of CORE-V CVA6, an open-source RISC-V application core which originated from the Ariane design by the Pulp team. During the SPIRS project, we confronted CVA6 with the security threats listed in the PP84 protection profile of the Common criteria, and addressed the detected vulnerabilities

*Corresponding author: `caaliph.andriamisaina@cea.fr` with a set of security countermeasures to produce a safe and secure version of CVA6, called SPRITZ.

One major threat is fault injection attacks [2], and we identified a list of countermeasures to detect or even correct such faults. To improve the countermeasure efficiency, and avoid waiting for the silicon to validate it, a flow was set-up to simulate the fault injection before tape out. The flow allows to reduce simulation times and corroborates that SPRITZ security is improved by implementing integrity in memory, bus, and core, as shown in Table 1.

Table 1: *Results of fault injection attacks on CVA6 and SPRITZ*

CVA6	Detected	Succeeded	Not propagated
System Memory	20%	55%	25%
Register	26%	64%	10%
SPRITZ	Detected	Succeeded	Not propagated
System Memory	100%	0%	0%
Register	98%	0%	2%

Root-of-trust components The initial version of the HW RoT in SPIRS encompasses: (i) A Physical Unclonable Function (PUF) based on a Ring Oscillator architecture capable of retrieving identifiers and generating random numbers; (ii) AES-256 as a symmetric cipher for data encryption and decryption; (iii) SHA-256 as hashing function; (iv) A HW implementation of the modular exponentiation used for RSA digital signatures.

FPGA implementation results The platform has been implemented on a Genesys 2 board based on Kintex-7™ XC7K325T-2FFG900C. The system clock constraint was kept at 20ns, identical to the original platform [3]. Table 2 contains the platform performance in terms of power (W) and area occupation per component in terms of LUTs, FFs, and RAMB36s. The majority of power is consumed by "Others" (DDR controller, AXI4 crossbar, peripherals, and so on.).

Software

TEE on RISC-V The basic software stack described in Figure 2, modeled after the Keystone framework [4], depicts the different software components that interact in the SPIRS TEE design. At the core of the separation between trusted and untrusted partitions is the trusted *Security Monitor* (SM), which has the highest execution privileges on the platform, manages access rights to memory and devices, leverages the capabilities of the HW RoT, and provides communication means between the two partitions.

Table 2: *SPIRS platform performance*

Components	Power (W)	LUT	FF	RAMB36
SPRITZ	0.22 (9.27%)	59969	33317	120
AES	0.071 (2.99%)	1818	1059	0
PUF	0.15 (6.32%)	2487	628	1
SHA2	0.026 (1.1%)	2432	1677	0
RSA	0.001 (0.04%)	21318	10728	0
Others	1.844 (77.71%)	30982	24900	12
Total	2.311 (100%)	119006 (58.39%)	72309 (17.74%)	133 (29.89%)

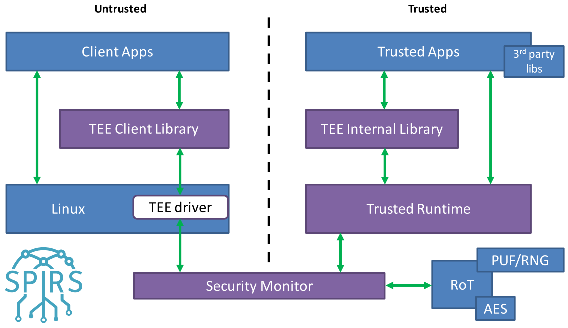

Figure 2: *Basic SPIRS TEE software stack*

On the untrusted side, userspace *Client Apps* can leverage the rich capabilities of the HLOS (i.e., *Linux*), and establish a client/server relation with *Trusted Apps* (TAs) via a *TEE Client Library*, which implements the GlobalPlatform "*TEE Client API Specification v1.0*" [5] as the communication interface. All interactions between Linux (and its userspace) and the SM are mediated through a dedicated *TEE driver*. On the trusted side, TAs are simple applications, designed aiming to minimize the surface of the *Trusted Computing Base*, that encapsulate the functionalities requiring the features of the TEE. TAs rely on the SPIRS *Trusted Runtime* to mediate access to the SM, and for basic functionalities like dynamic memory management. The *TEE Internal Library* provides TA developers with an interface to communicate with *Client Apps*, based on a subset of the GlobalPlatform "*TEE Internal Core API Specification v1.1.2*" [6]. The adoption of well established GlobalPlatform TEE specifications [5, 6] helps reducing development fragmentation and bridging the gap between ARM and RISC-V software ecosystems.

Acknowledgements

This research was supported in part by the SPIRS Project with Grant Agreement No. 952622 under the EU H2020 research and innovation programme. M.C.M.R. holds a postdoc fellowship from the Andalusia Government with support from PO FSE EU.

References

[1] *SPIRS web page*. https://www.spirs-project.eu.

[2] Jean-Roch Coulon. *Fault attacks on RISC-V processor*. URL: https://jaif.io/2022/media/JAIF2022_Coulon.pdf.

[3] *OpenHW Group*. https://github.com/openhwgroup/cva6.

[4] Dayeol Lee et al. "Keystone: an open framework for architecting trusted execution environments". In: *EuroSys*. ACM, 2020. DOI: 10.1145/3342195.3387532.

[5] GlobalPlatform Inc. *TEE Client API Specification v1.0*. Tech. rep. GPD_SPE_007. GlobalPlatform Inc., July 2010.

[6] GlobalPlatform Inc. *TEE Internal Core API Specification v1.1.2*. Tech. rep. GPD_SPE_010. GlobalPlatform Inc., Nov. 2016.