SECURE PLATFORM FOR ICT SYSTEMS ROOTED AT THE SILICON MANUFACTURING PROCESS (SPIRS)

Blog 4: WP5 Outcomes

This blog post summarizes the key accomplishments of WP5, detailing the development of the SPIRS platform through its three major versions and presenting a methodology for automating the generation of this platform.

The SPIRS platform is a secure, FPGA-based System-on-Chip (SoC) designed to integrate advanced security features. The platform has undergone several iterations, each improving upon the previous in terms of security, performance, and power efficiency. Central to the platform is the integration of the CVA6 RISC-V processor and the Root-of-Trust (RoT) developed in WP2.

The initial version of the SPIRS platform, representing the first deliverable of WP5, was developed by integrating key hardware components, including the Spritz processor, a secure CVA6, and a first version of RoT modules such as AES, PUF, SHA2, and RSA. This platform was deployed on the Genesys 2 FPGA board. However, the first release encountered challenges related to power consumption and footprint, particularly with the integration of RSA2048.

The second version of the platform focused on refining the hardware design by removing the RSA module and introducing additional cryptographic components like SHA3 and EdDSA. This version also optimized resource usage, significantly reducing power consumption and improving the overall area efficiency on the FPGA. Moreover, the integration of a second PUF module allowed for enhanced secure boot processes and true random number generation.

The final version of the SPIRS platform resolved key issues identified during testing, such as application freezes on the Spritz processor caused by instruction incompatibility. To address this, the processor was upgraded to a newer version of the CVA6. This final version of SPIRS platform also integrates the secure boot ROM developed in WP3 of the project. The final design maintained the high security standards of the platform while optimizing resource efficiency, resulting in a power consumption of only 2.578W and using 58.21% of the available area.

The final SPIRS platform was rigorously tested and validated, ensuring that all components functioned correctly. The platform securely booted using the boot ROM from WP3, followed by loading a Linux operating system, establishing an Ethernet connection, and running multiple RoT software applications.

An automated generation methodology for the platform has been also developed in WP5. This methodology streamlines the creation process of the platform, reducing development time and increasing reproducibility. By using configuration files and templates, the platform generation tool produces SystemVerilog top-level files and a Device Tree Source (DTS) file of the platform. FuseSoc, an open-source package manager and build tool designed for FPGA and ASIC development, has been leveraged in the methodology. FuseSoc significantly simplified the integration process by automating the build tasks and managing dependencies between the various components of the platform.

Lead partner of WP5: CEA-LIST

Author: Caaliph Andriamisaina (CEA-LIST)

Submission date: 03/09/2024

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952622