RESSI 2022 submission

Overview

Nom	Amplificateurs de sécurité pour l'IoT à base de Processeur-In-Memory (PIM)
Acronym	TANDEM
Porteur	UPMEM - Massimiliano BARTOLI (Security Technical Lead)
Date	01/2019 - 07/2022
Consortium	**UPMEM**, bringing its innovative Process-In-Memory technology. **Orange**, bringing its knowledge of end to end security for IoT edge processing applications and infrastructures.
Financement	DGA RAPID (Régime d'APpui à l'Innovation Duale)
TRL	TRL4: Validation des fonctions clés du concept en laboratoire

Project description

The Tandem project is the result of a partnership between UPMEM and Orange with the goal to analyze the potential benefits of using the UPMEM Processor-In-Memory technology as a security amplificator with a very competitive cost.

State of the art

Confidential computing is an urgent challenge faced by IoT edge and cloud computing.
Typical solutions address this challenge by using processor-supported secure enclaves which virtually isolate security critical applications to prevent unauthorized access from any other software (including the untrusted OS) or co-processor. Unfortunately researchers have recently demonstrated that secure enclave architectures can be vulnerable to different kinds of side-channel attacks targeting the resources that the enclave shares with its host CPU (e.g cache).
Trusted Platform Modules (TPM) are alternative solutions to protect data "in use". TPMs have the benefit of being physically isolated from the rest of the system, but they have limited computation capabilities and cannot be programmed with arbitrary code.
Finally, IoT end-devices are usually poor in security and lack such secure enclave or security co-processor support. This exposes these devices, as well as the supporting infrastructure, to potential security threats.

UPMEM PIM for security

The UPMEM Processing In Memory is an unique acceleration solution that solves the data movement problem in servers by performing computation where the data resides. This results in a drastic reduction of the server energy consumption and in a boost of performance. The core of this technology is the integration of multiple co-processors, called DPUs (DRAM Processing Units), into DIMM DRAM chips used by the system "main" CPU to process data and

share the results. Typical server memory configurations (>128 GB) result in the addition of thousands of DPUs providing a huge parallelization opportunity.

From a security perspective DPUs can be seen as isolated programmable multi-thread CPUs owning an internal RAM and with privileged access to the system main RAM. This put the DPUs in an ideal position to play the role of secure co-processors offering some security benefits by design: being isolated DPUs are protected from secure-enclave typical side-channel attacks caused by resource sharing (e.g cache attacks) and data movement (e.g. attacks on memory bus); being programmable and scalable DPUs offer much more flexibility than standard TPMs; being embedded within fully compliant DIMM modules, DPUs can boost the security level of poor security devices with no hardware redesign needs (by replacing standard DIMMs with UPMEM DIMMs).

Methodological approach

A simplified UPMEM DIMM design (Proof of Concept) has been developed on an FPGA environment (Xilinx SOC Zynq® UltraScale+™) and used to validate the two following target cases:

- DPU running an authenticated user application. At this scope the user application has been signed with ECDSA P256 and verified by the DPU before being executed.
- DPU running an encrypted application with a key known by the DPU only (unknown by the main CPU). At this scope AES-256 has been used, the user application has been decrypted by the DPU before being executed.

Thanks to the prototyping and the use case analysis several areas of improvement have been identified to turn the original UPMEM PIM design to behave as a security co-processor. Example of such areas are:

- DPU boot process
- DPU internal memory isolation
- DRAM access control

Achievements

As result of this effort, an updated PIM HW architecture has been released including the following security achievements:

- DIMM-DRAMs support two modes of operation: non-secure and secure.
  When in non-secure mode the DPUs act as open co-processors whose internal memories are directly accessible by the main CPU.
  When in secure-mode the DPUs act as secure co-processors: the DPUs internal memories are never accessible by the main CPU; instead of being loaded in the DPU internal RAM, user applications are copied in the main RAM and validated (e.g. authenticated, decrypted) by the DPU before being executed.
- Boot process: a DPU root application is executed on each power cycle. This application performs the needed system initialization and validates the user applications before execution.
- A partition based access control has been enforced on the system main RAM, allowing the creation of partitions never accessible by the Host CPU. Those partitions can be used by the DPU to enlarge its available volatile memory.
- DPU critical data protection: a hardware stream cipher has been introduced to protect root key(s) during storage and transition state.