TrustSoC-V : An heterogeneous SoC architecture for RISC-V, Secure-by-Design

Raphaële Milan[1], Lilian Bossuet[1], Loïc Lagadec[2], Carlos Andres Lara Nino[3]

Context

SoC design security "a posteriori"

All too often, the security of the SoC is not properly considered during the design stage [1] leading to potentially introducing vulnerabilities.

Third-party components

Untrusted third-party hardware or software modules are introduced during design process.

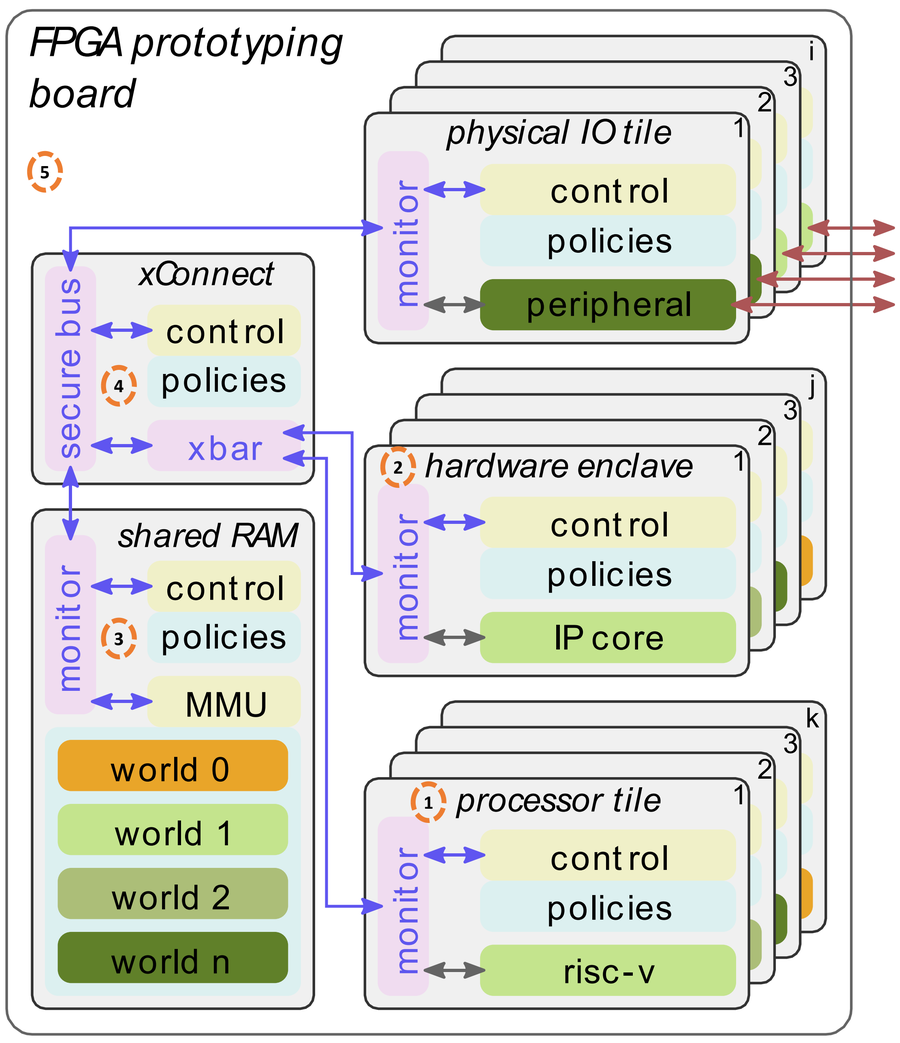
Threat model

We consider threats from **remote software and hardware attacks.**

The untrusted third-party components can perform attacks:

- illegitimate bus requests,
- modifications of the memory contents,
- modifications of the bus contents.

TrustSoC-V



Main features of TrustSoC-V

1. **Processor tiles**
   Open-source, RISC-V tiles but possible on other cores [2] .

2. **Hardware enclaves**
   Inside the FPGA, encapsulate hardware accelerators. Monitor the operations, provide a generic interface to communicate.

3. **Shared memory**
   Divided in multiple enclaves with a memory protection unit.

4. **Secure bus**
   Open-source. Links the different components of the SoC and enforces access controls.

5. **Segregation in multiple levels of privilege and monitoring**
   Organizes the architecture in varying degrees of privilege, "worlds". Monitors operations with the help of added hardware-coded blocks.

Implementation costs

On a AMD-Xilinx Zynq SoC-FPGA (XC7Z020-CLG484), on a small system.

IPs	LUTs			FFs			F_{max} (MHz)		
	Base	Protected	%	Base	Protected	%	Base	Protected	%
Edge Sobel	2,785	2,792	+0.25	4,355	4,357	+0.05	223	215	-3.59
Montgomery	4,863	4,901	+0.78	1,625	1,627	+0.15	100	104	+4.0
CV32A6	8,538	Future work	--	4,063	Future work	--	180	Future work	--

References

[1] EM Benhani, Lilian Bossuet, and Alain Aubert, "The security of ARM TrustZone in a FPGA-based SoC". In: IEEE Transactions on Computers, 68.8. (2019).

[2] Raphaële Milan, Lilian Bossuet, Loïc Lagadec *et al.*, "TrustSoC: Light and Efficient Heterogeneous SoC Architecture, Secure-by-design". In: 2023 Asian Hardware Oriented Security and Trust Symposium IEEE, 2023.

[1] author.name@univ-st-etienne.fr, [2] author.name@ensta-bretagne.fr, [3]carlos.lara@fundacio.urv.cat

Laboratoire Hubert Curien
UMR ▪ CNRS ▪ 5516 ▪ Saint-Étienne

Université Jean Monnet Saint-Étienne

AGENCE INNOVATION DÉFENSE

RISC-V®