# Executing Secured Virtual Machines within a Manycore Architecture

Clément Dévigne, Jean-Baptiste Bréjon, Quentin Meunier and Franck Wajsburt
Sorbonne Universités, UPMC Univ. Paris 06,
CNRS, UMR 7606, LIP6, Paris, France

www: http://www-soc.lip6.fr/ E-mail: clement.devigne@lip6.fr, quentin.meunier@lip6.fr, franck.wajsburt@lip6.fr

## Context and Motivations

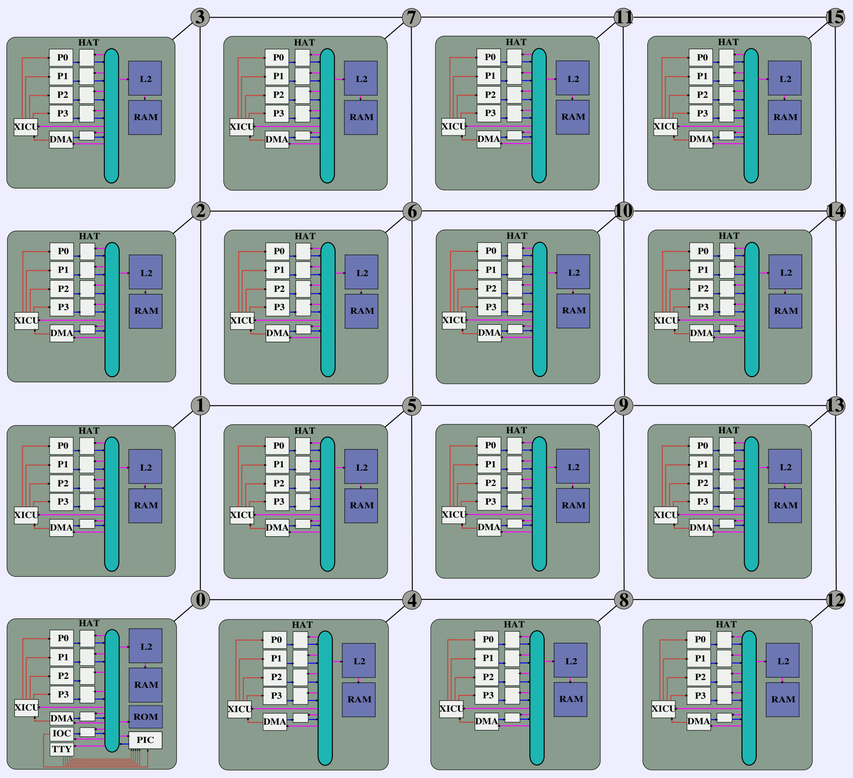
- The computer world is facing an explosion of digital data. The information contained in these data are valuable in several domains (economic, commercial, health-related). Clearly, the access to these information needs to be secure.
- Manycore processors are able to process a large data stream. However, they must guarantee security properties.

The TSUNAMY ANR project [1] aims at proposing a mixed hardware/software solution allowing to execute numerous independent applications, while providing an isolated execution environment as a response to the confidentiality and integrity problematics.

## Hypothesis and Threat Model

- Physical attacks are not handled.
- Operating Systems running on the platform are untrusted.
- The hypervisor manages all the Virtual Machines (VM).
- The hypervisor is blind (i.e. it is not able to access VM ressources after their configuration).
- VMs do not share any core or memory bank.
- Three address spaces: virtual, physical and machine.

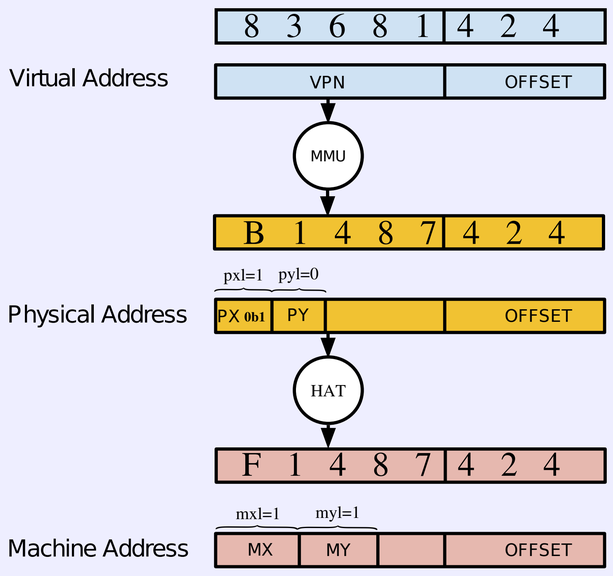
## Tsunamy Architecture




The TSUNAMY architecture is based on the TSAR architecture [2]. It is described in SystemC CABA with the SoCLib [3] library.

- All clusters contain:
  - ⇨ 4 MIPS cores with their first level caches. The L1 cache coherence is managed entirely in hardware.
  - ⇨ 1 second level (L2) cache, which is in charge of a segment of the physical memory address space.
  - ⇨ 2 internal peripherals: an interrupt controller including timer functions (XICU) and a DMA controller.
  - ⇨ A local crossbar.
  - ⇨ The Hardware Address Translator (HAT) behind all network initiators.
- The I/O cluster additionally contains:
  - ⇨ A terminal controller (TTY).
  - ⇨ A hard-drive disk controller (IOC).
  - ⇨ A Programmable Interrupt Controller (PIC), able to convert a hardware interrupt into a software one.

## HAT: Address Translation Mechanism

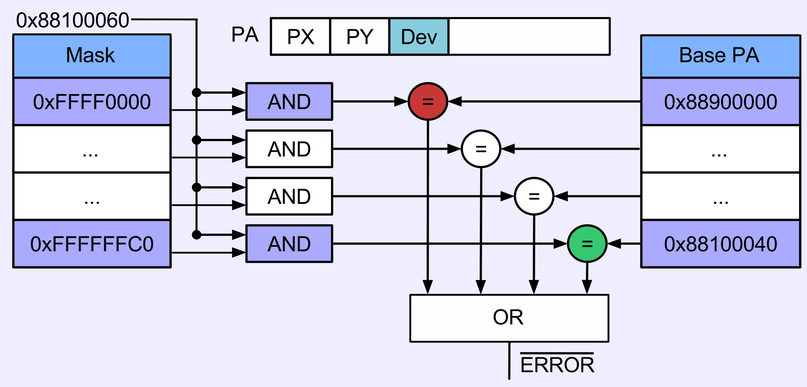



- Most significant bits (MSB) define the cluster coordinates (X; Y).
- The address translation consists only in changing the MSB.
- Pxl and Pyl define the number of bits needed to code X and Y sizes for the VM.
- Mxl and Myl define the number of bits needed to code X and Y sizes for the architecture.

In this example, one VM is executed on 2 clusters (cluster 1 and 3) and the Tsunamy platform contains 4 clusters. The parameters of this scenario are:

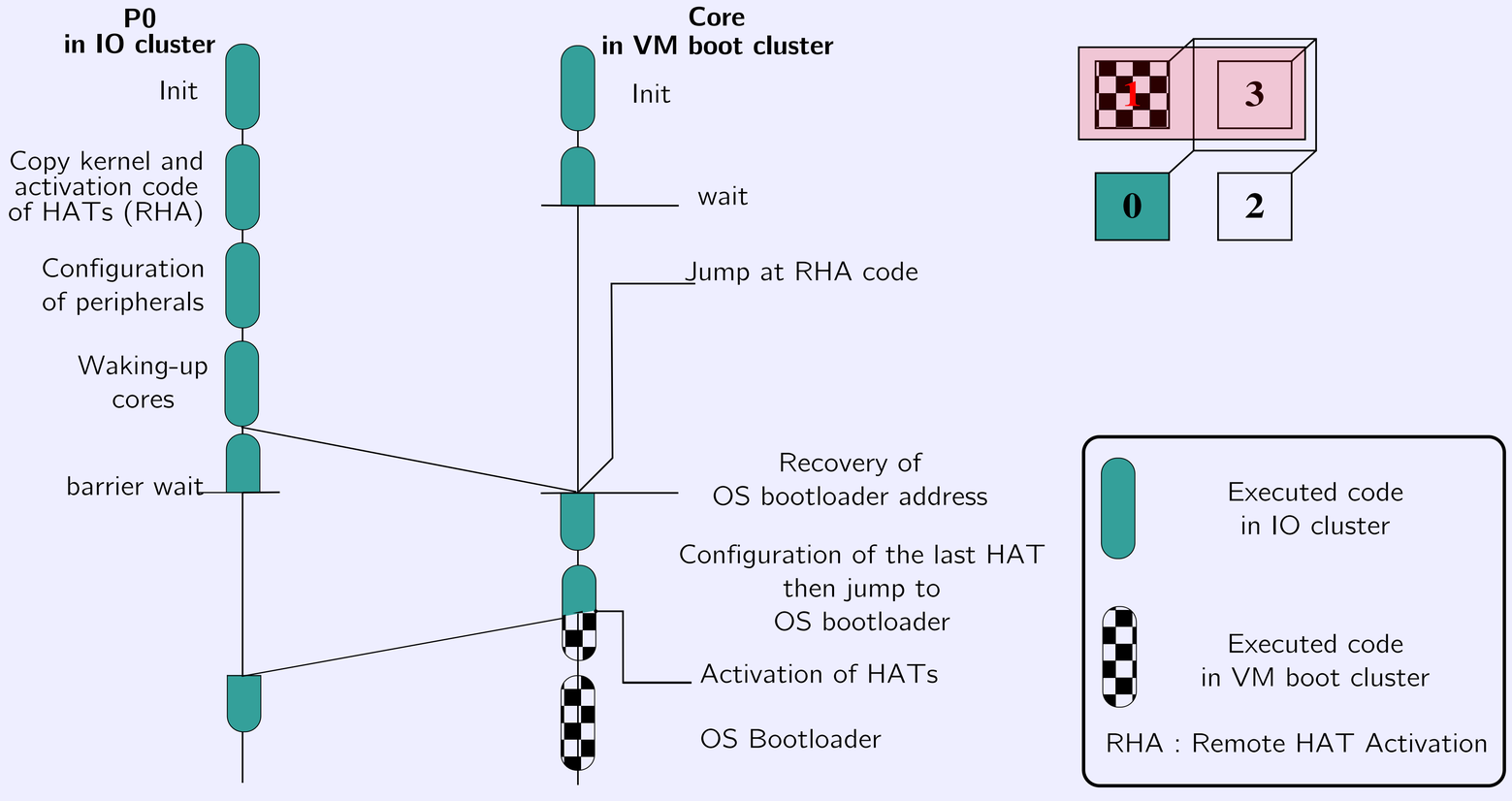
- mxl = 1 and myl = 1
- pxl = 1 and pyl = 0

## HAT: Peripheral Access Mechanism




- 1 bit in the physical address defines if the request targets a peripheral (DEV bit).
- 2 tables into the HAT handle peripheral accesses:
  - ⇨ Base Physical Address table contains all addresses of peripherals reachable by the VM.
  - ⇨ Mask table contains two's complement of the size of these peripherals.
- First the physical address is masked using the mask table entries.
- Secondly the masked address is compared with the base physical address table entries.

## Boot Procedure of a Virtual Machine







## References

[1] LIP6, Lab-STICC, LabHC and CEA-LIST, Hardware and software managemenT of data SecUrity iN A ManY-core platform, https://www.tsunamy.fr.

[2] LIP6 and BULL, TSAR (Tera-Scale Architecture), https://www-soc.lip6.fr/trac/tsar.

[3] LIP6, SoCLib : an open platform for virtual prototyping of MP-SoC, http://www.soclib.fr.

[4] ANR, Agence Nationale de la Recherche, http://www.agence-nationale-recherche.fr.

## Acknowlegments

This poster was realized in the frame of the TSUNAMY project number ANR-13-INSE-0002-02 supported by the French Agence Nationale de la Recherche [4].