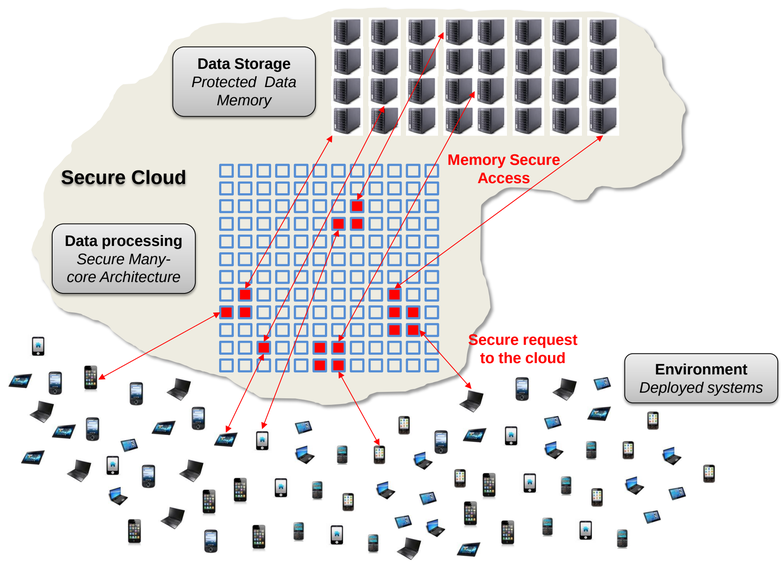
Applications security in many-core platform, from operating system to hypervisor: how to build a chain of trust

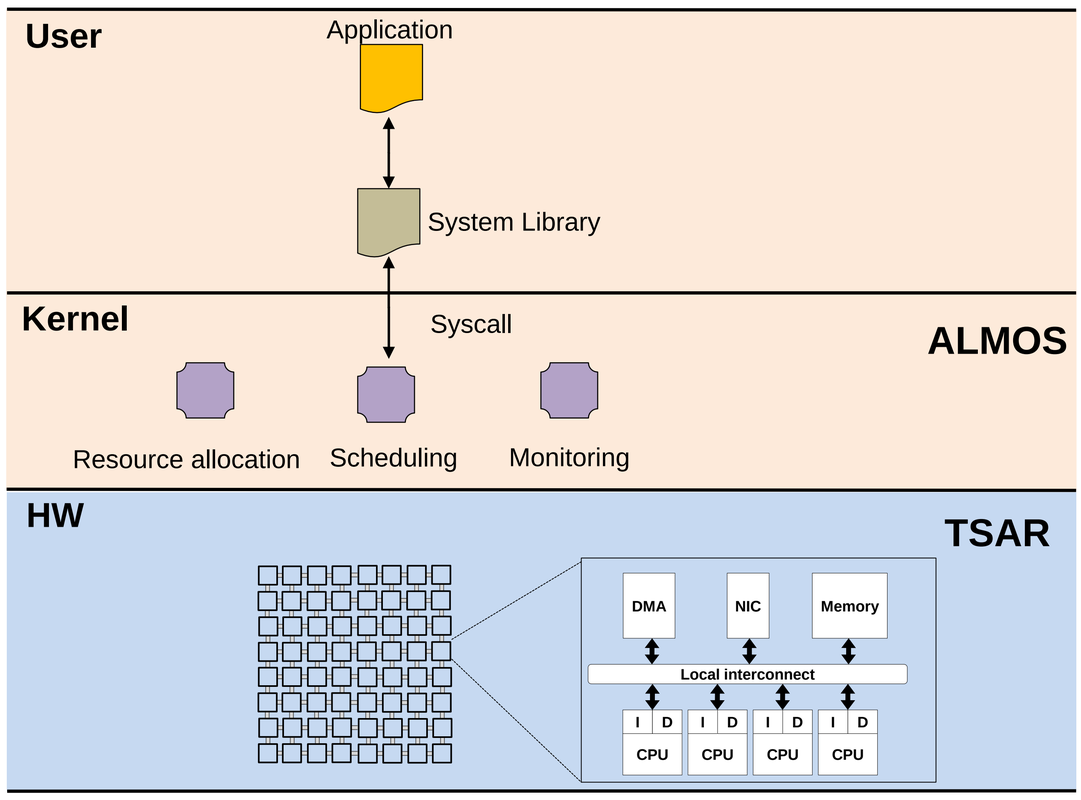
Maria Méndez Real*, Clément Dévigne¤, Cuauhtémoc Mancillas López¥, Mehdi Aichouch#, Vianney Lapotre*, Quentin Meunier¤, Lilian Bossuet¥, Moha Ait Hmid#, Guy Gogniat*, Franck Wajsbürt¤

*Univ. Bretagne Sud, Lab-STICC, firstname.lastname@univ-ubs.fr
¤UPMC Univ Paris Laboratoire LIP6, firstname.lastname@univ-ubs.fr
¥ Université de Lyon, Laboratoire Hubert Curien, firstname.lastname@univ-st-etienne.fr
CEA, List, Software Modules for System Security and Dependability Laboratory, Gif-sur-Yvette, FRANCE

TSUNAMY ANR project (2013-2017)



Many-core architecture (up to 1024 cores)



Threats model

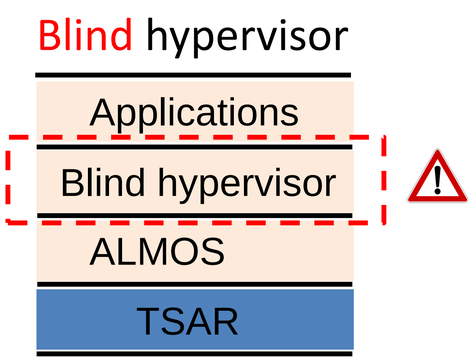
- Denial of Services
- Confidentiality
- Integrity
- Leakage of Information (Cache SCA) *

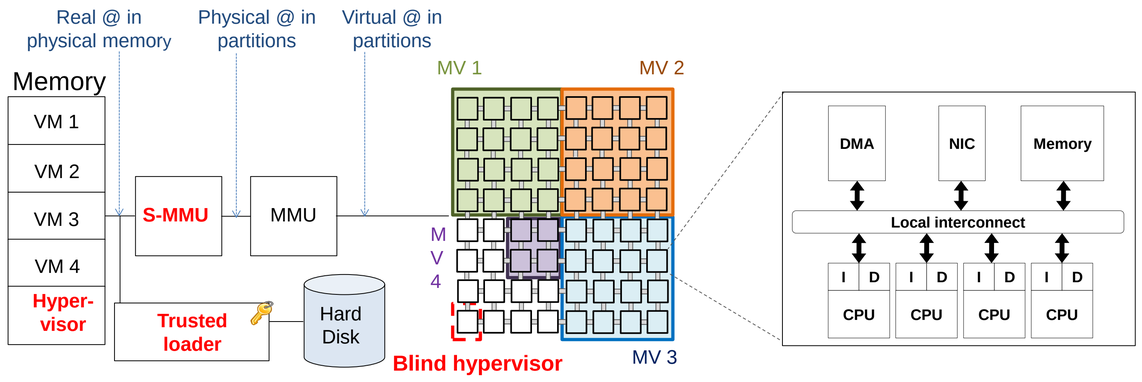
Building a chain of trust

Secure deployment and execution of Virtual Machines → **Secure applications deployment** → **Enhancing TSAR with crypto-processors**

1. Secure deployment and execution of Virtual Machines (VM)

Objective:
Deploying and protecting VMs from each other and from the hypervisor (Confidentiality & Integrity)

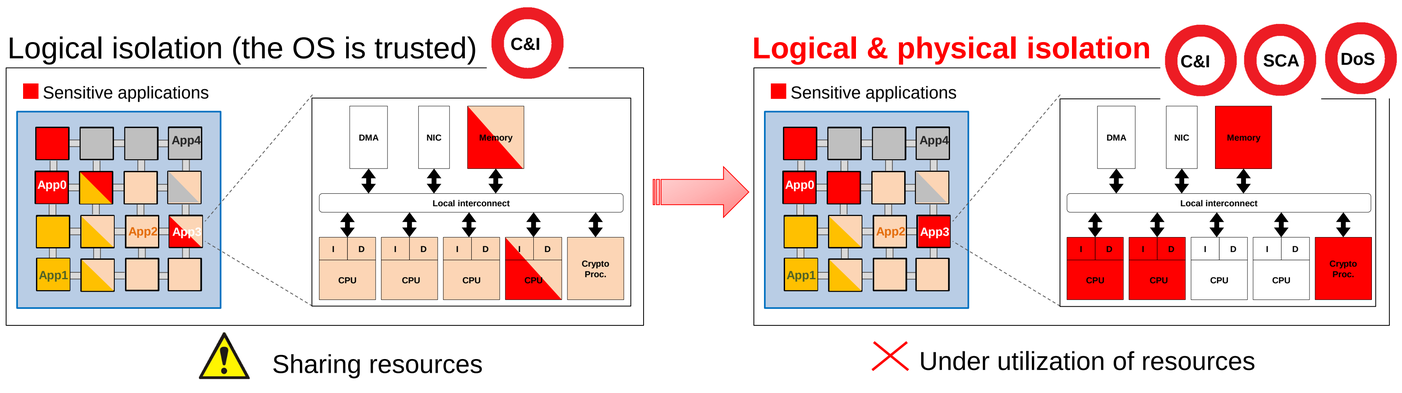




How:
- Once the VM is deployed, no more access to the VM partition (*Trusted S-MMU*)
- Content of VMs encrypted when stored on hard disk or retrieved from the network (*Trusted loader*)
- A Hardware Address Translator (*HAT*) translates addresses from physical to machine (real) addresses.

3. Secure applications deployment

Objective:
Securely deploying and protecting sensitive applications from other applications thanks to *Secure zones* (DoS, C&I, and Cache SCA)

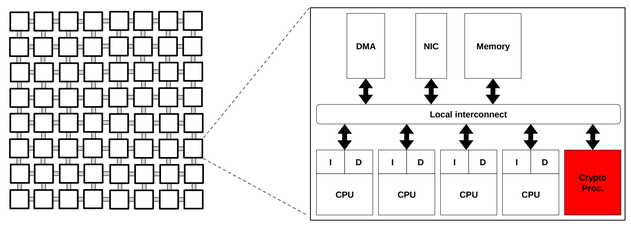


Tradeoff between security and performance

How:
Extension of the OS in order to integrate new secure aware services

1. Enhancing the TSAR architecture with crypto-processors

Objective:
Improving performance dedicating resources to encryption, using the crypto-processor as a co-processor



How:
- TSAR compatible VciHCrypt3
- Necessity of a secure sharing key mechanism

* J. Demme and S. Sethumadhavan. *Side-channel vulnerability metrics: Svf vs . csv*. In WDDD, 2014
Y. W. and G. E. Suh. *Efficient timing channel protection for onchip networks*. In NOCS 12 Proceedings of the 2012 IEEE/ACM Sixth International Symposium on Networks-on-Chip, pages 142–151, 2012