FROM RESEARCH TO INDUSTRY

cea tech

Towads an Implementation of a Blind Hypervisor

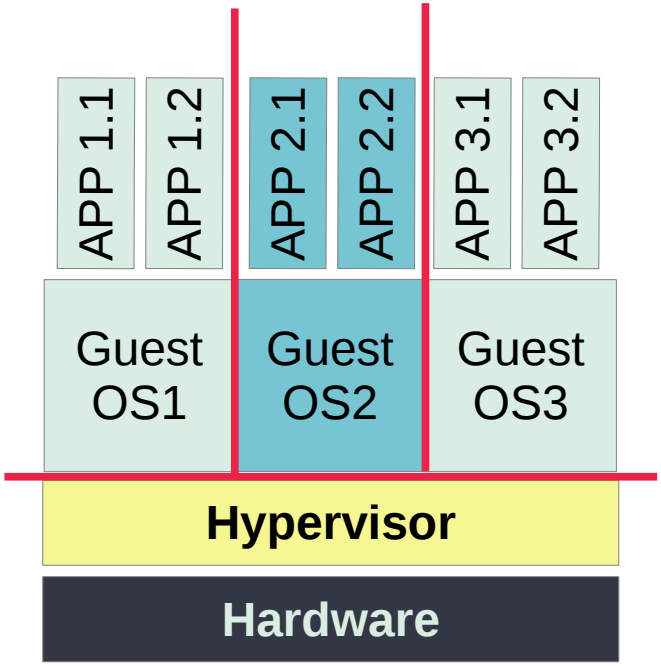
Mehdi Aichouch
CEA List
Laboratoire L3S

www.cea.fr

leti & list

Context

- Isolation guaranteed through **hypervision**
- Hypervisor is in **Trusted Computing Base**
- What if a hypervisor is **compromised**?
  - e.g. through an escalation of privilege attacks
- **Problem**
  - **Secret data** in a virtual machine might be accessed



Blind Hypervisor

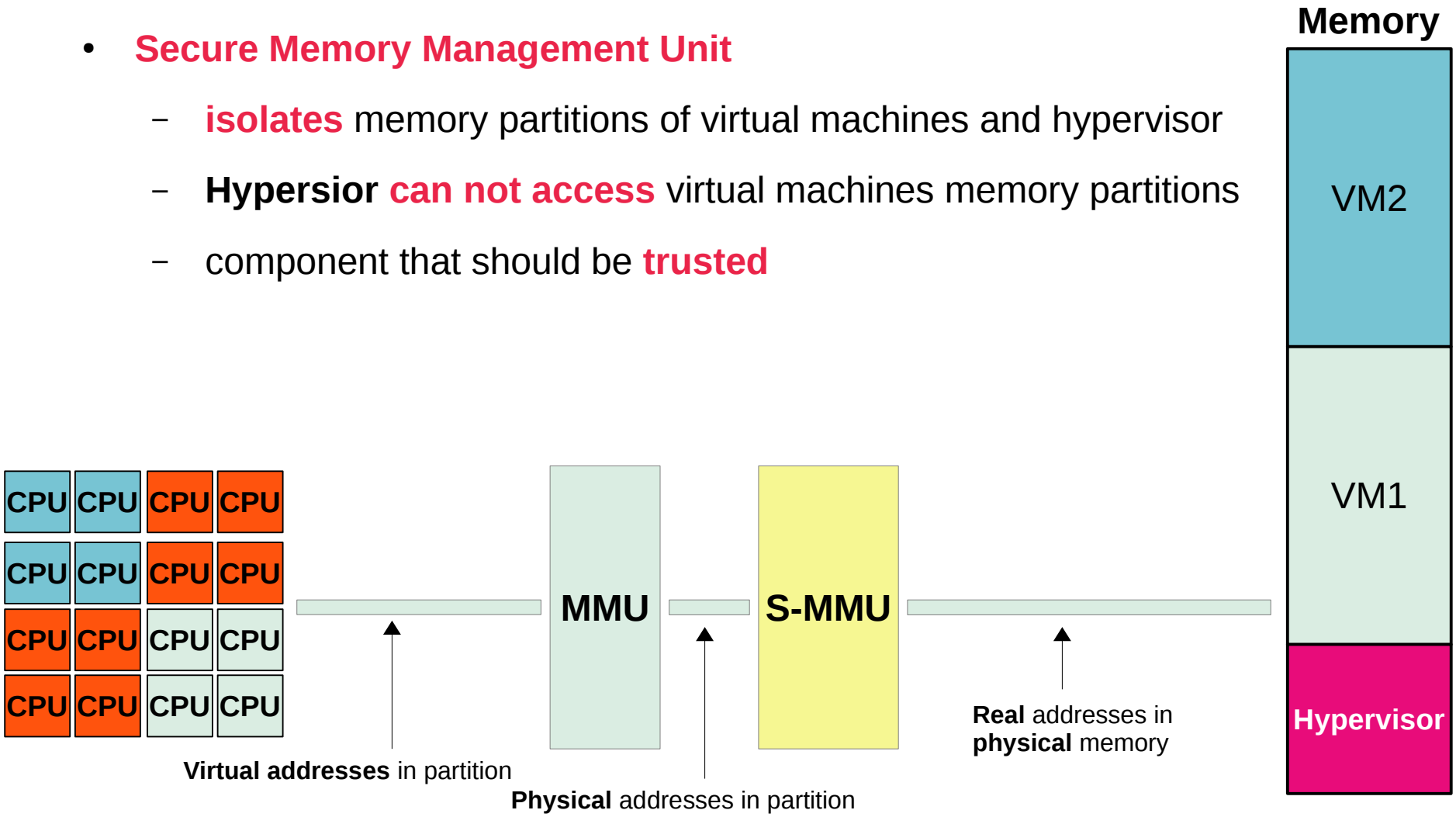
- **Goal**
  - Guarantee the **confidentiality** and **integrity** of virtual machines **even if the hypervisor is not trusted**
    - **Confidentiality** means no **read** access permission
    - **Integrity** means no **write** access permission
- **Protection scope**
  - Software attacks from virtual machines and hypervisor are prevented
  - Do not address hardware attacks

Blind Hypervisor

- **Design**
  - **Prevent** hypervisor from accessing virtual machine **memory partition**
  - Virtual machine **content** should be **encrypted** when stored on an external storage
  - Without impacting runtime performance
    - Both code and data are stored in clear text
    - No on-the-fly encryption required
    - Cyphering takes places during VM load into memory or migration only
  - Rely on hardware assisted techniques

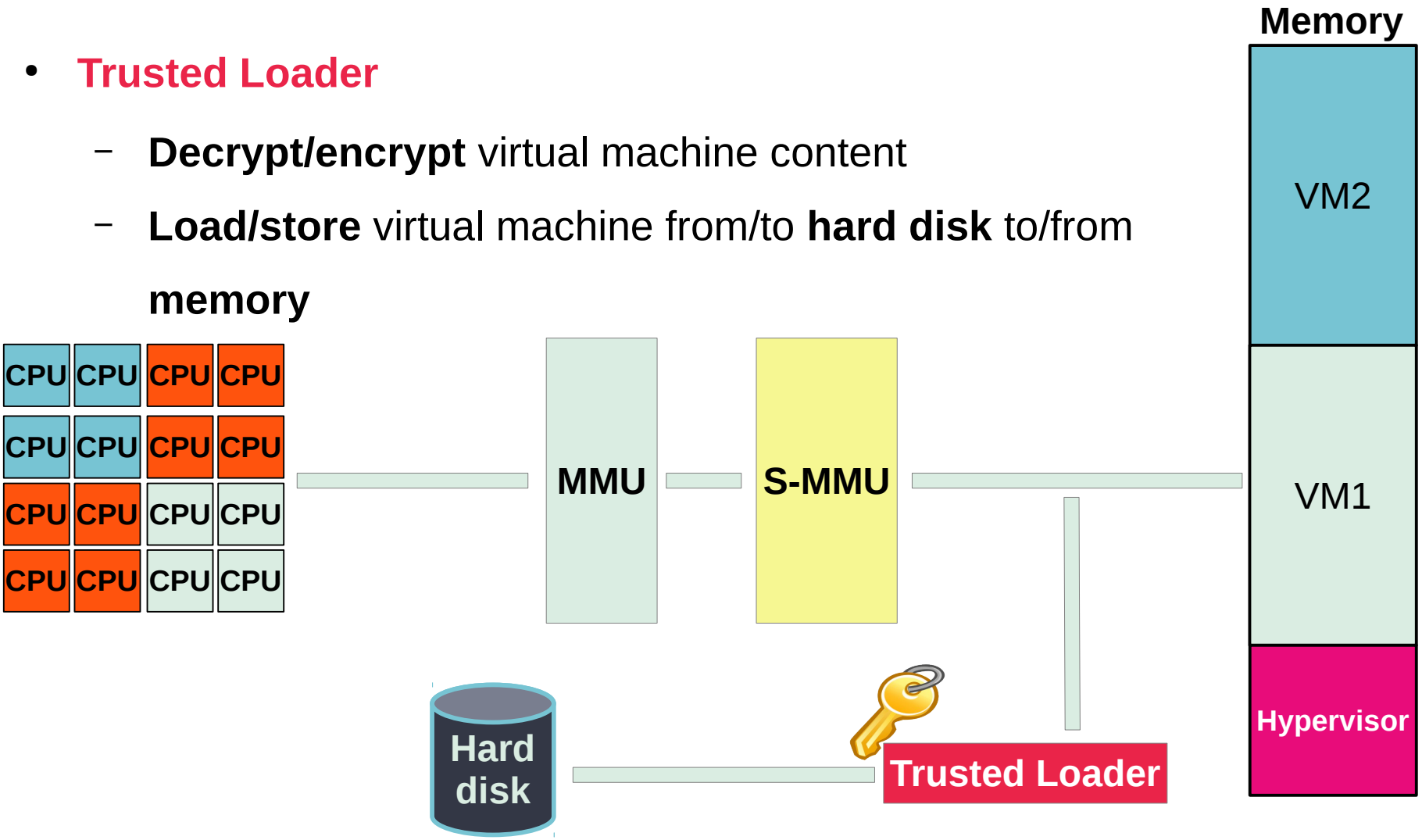
Hardware Extension

- **Secure Memory Management Unit**
  - **isolates** memory partitions of virtual machines and hypervisor
  - **Hypersior can not access** virtual machines memory partitions
  - component that should be **trusted**



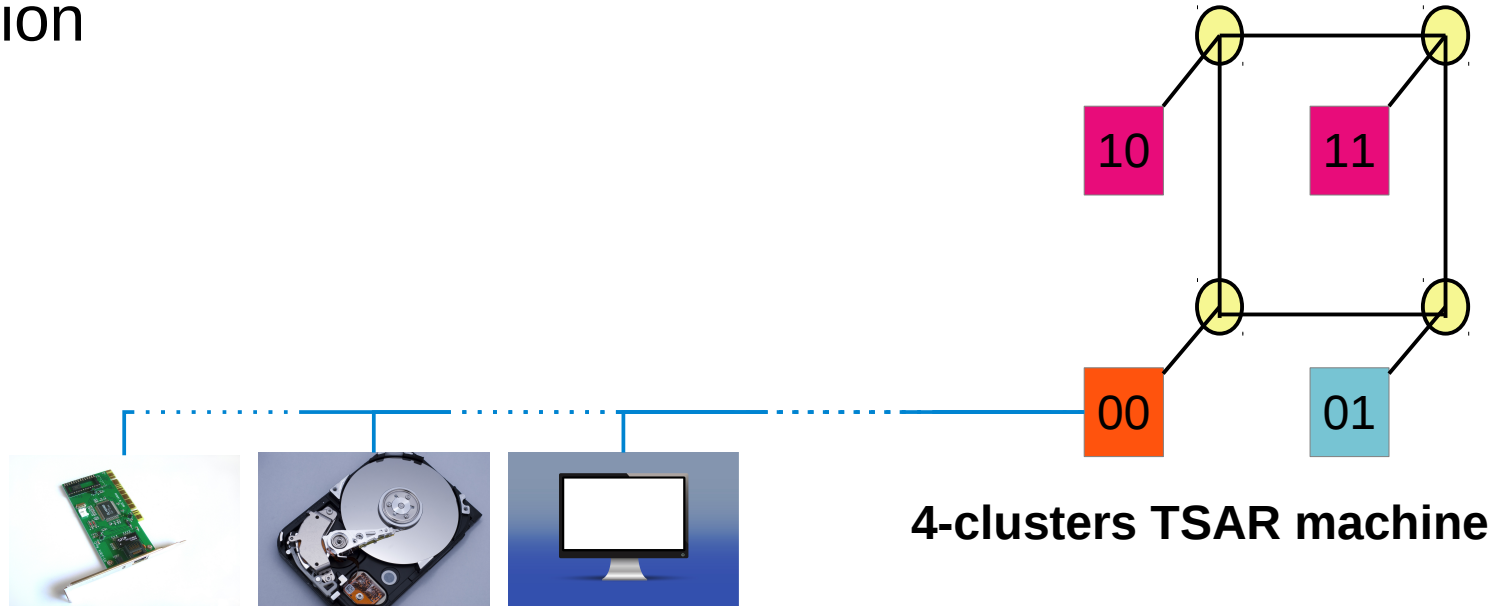
Hardware Extension

- **Trusted Loader**
  - **Decrypt/encrypt** virtual machine content
  - **Load/store** virtual machine from/to **hard disk** to/from **memory**



TSAR architecture

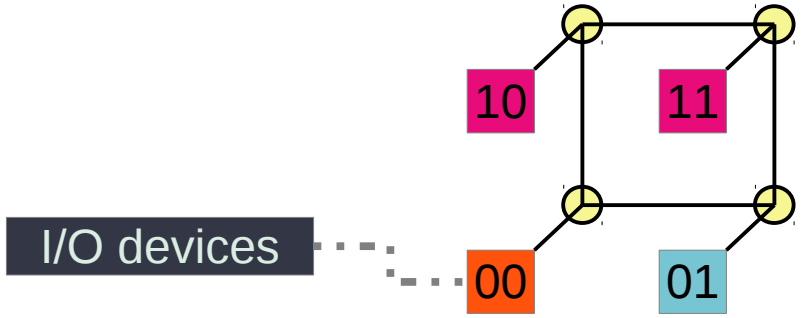
- **Manycore** *cache-coherent* **NUMA** architecture
- Clusters connected through a **Network-on-Chip**
- One **special cluster** for **I/O operations**
- All other **standard** clusters for virtual machines execution



4-clusters TSAR machine

Hypervisor Functionality

- Hypervisor is **executed** on the **I/O cluster**
- **Hypervisor configures** the **Secure Memory Management Unit**
  - To confine VM into a restricted clusters area
- Allocates **I/O devices channels** to allow virtual machines to access I/O devices



Summary

- Implementation of a **blind hypervisor** on a 16-clusters TSAR machine

- **Future work**
  - Integration on the TSAR architecture of a “trusted loader”
  - Evaluating different threats models and performance

Thank you!

Question are welcome