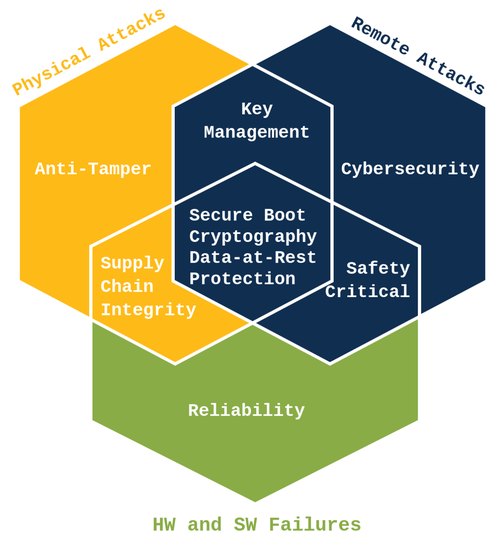
Advancing Confidential Computing on RISC-V with the Memory Protection Table

Stefano Mercogliano, Valerio Di Domenico, Alessandro Cilardo
Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione

Confidential Computing

Confidential Computing is a (hardware) security paradigm that guarantees **Confidentiality**, **Integrity** and **Authenticity** to

- Data at Rest
- Data in Transit
- Data in Use



A Look on Confidential Computing Technologies

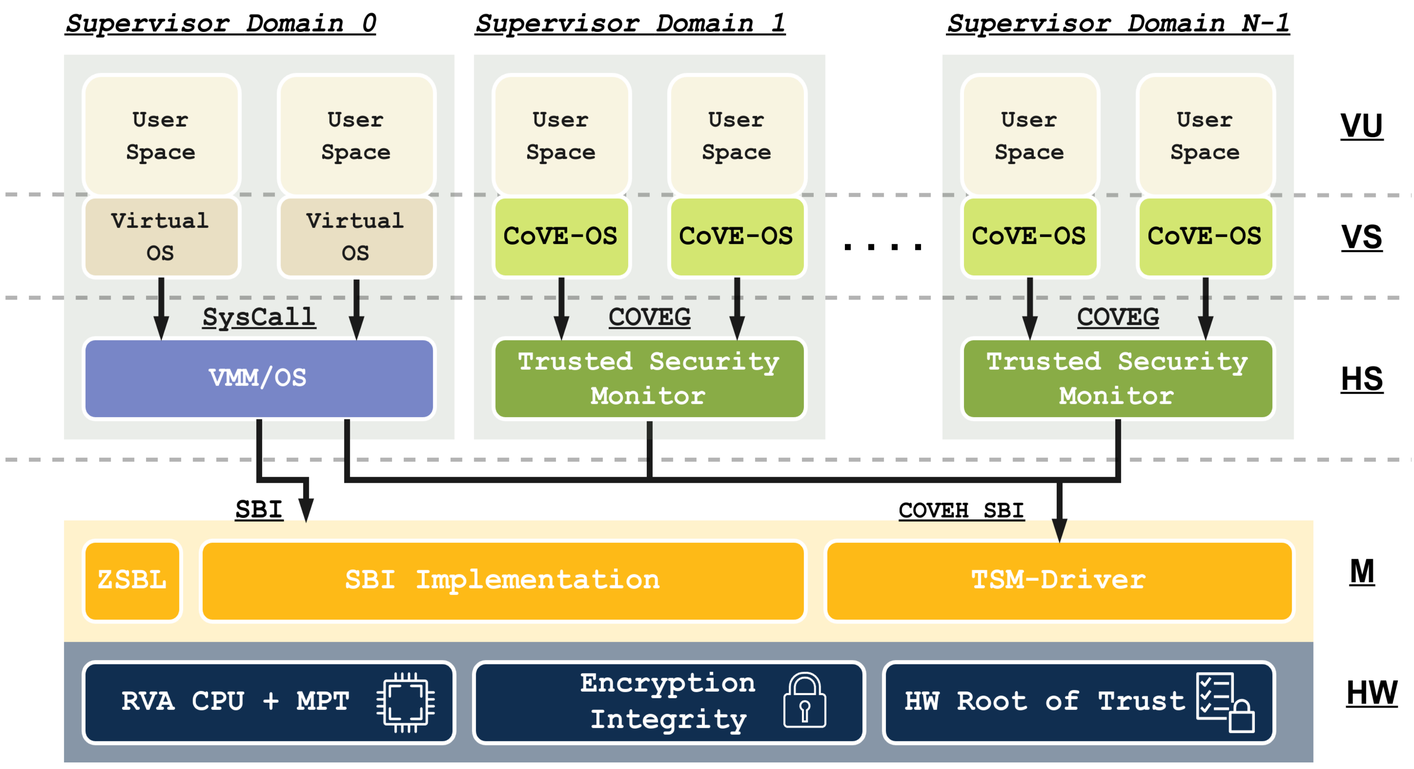
Confidential **V**irtual **M**achines (CVMs) technologies

- **ARM R**ealm **M**anagement **E**xtension (RME)
- **Intel T**rusted **D**omain **E**xtension (TDX)
- **AMD S**ecure **E**ncrypted **V**irtualization (SEV)

What About

RISC-V

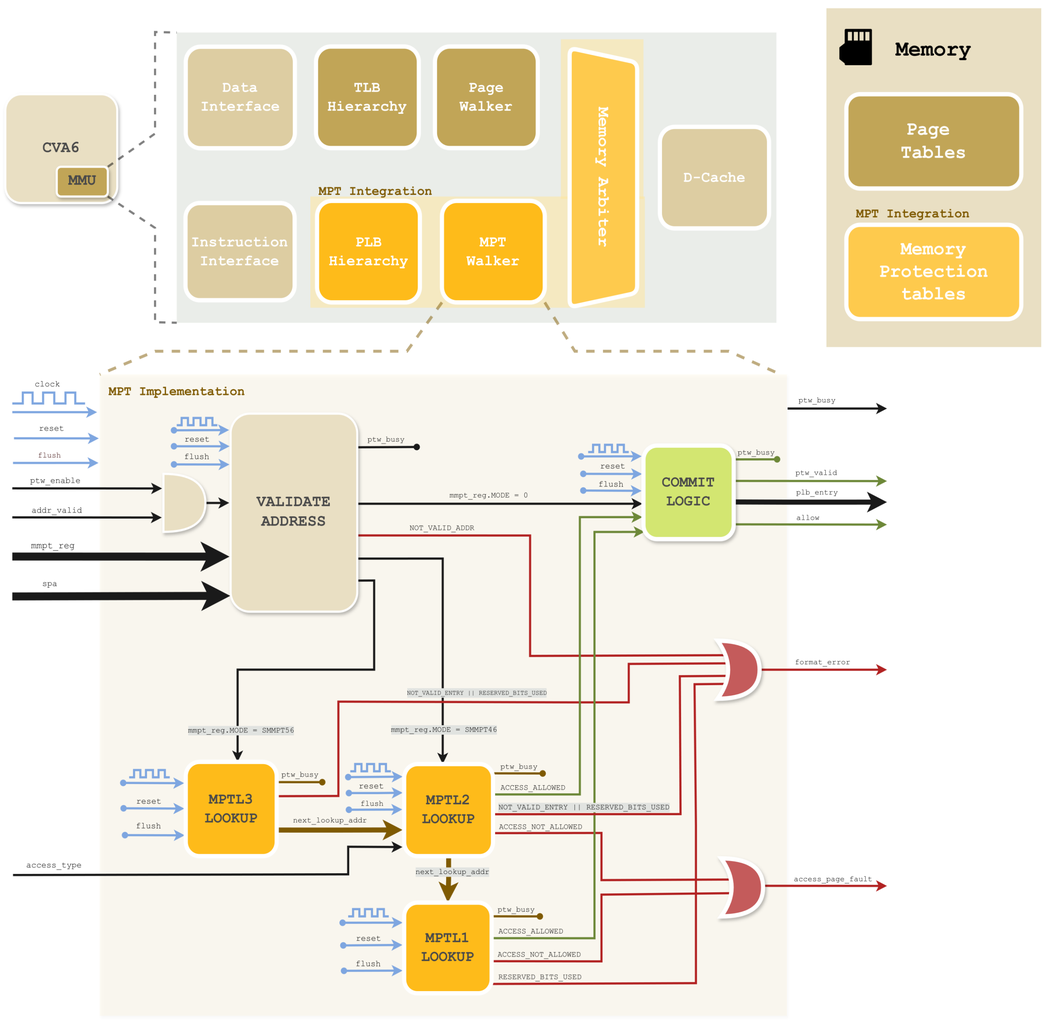
RISC-V Confidential Virtualization Extension (CoVE)

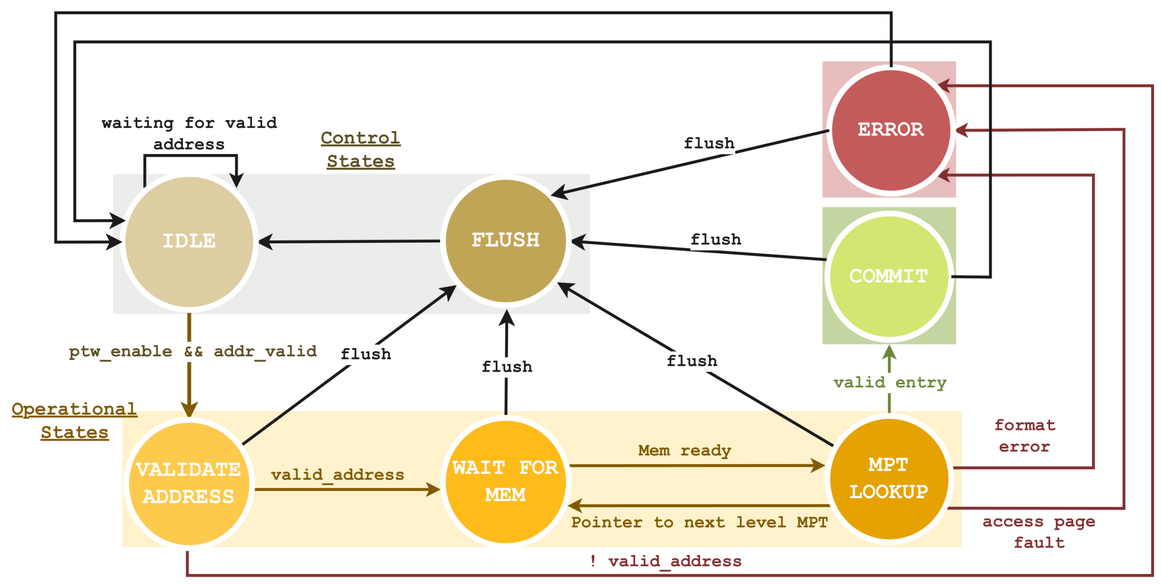


- Assumes multiple **Deployment Models**
  - Ranging from Embedded to Cloud
- Supports multiple **distrustful software stacks**
- Standardizes secure boot procedures and "secure calls"
- Phyisical resources are now selectively assigned to **Supervisor Domains**
- Access Permissions must be defined at a Page Level Granularity

PMP mechanism **is not enough**

The Fundation of Supervisor Domains: The Memory Protection Table (MPT)





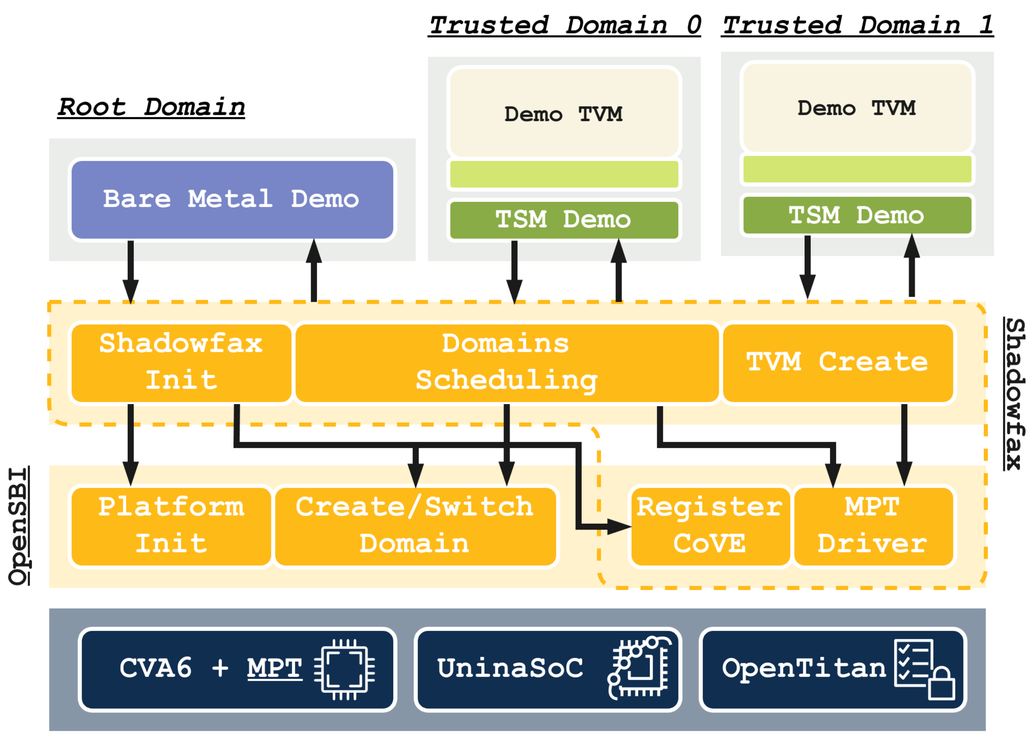
Hardware

- Implements latest *Smmpt specification*
- Integrated and Tested in the Open-Source *CVA6 CPU*
- Available SystemVerilog source code
  - ***https://github.com/Granp4sso/RISC-V-Memory-Protection-Table***

Software

- Patched *OpenSBI* to support MPT-Drivers
- Tested on our Open-Source rust-based *TSM-Driver* (**Shadowfax**)
  - ***https://github.com/Granp4sso/shadowfax***

The TSM-Driver: Shadowfax



{stefano.mercogliano, valer.didomenico, acilardo}@unina.it