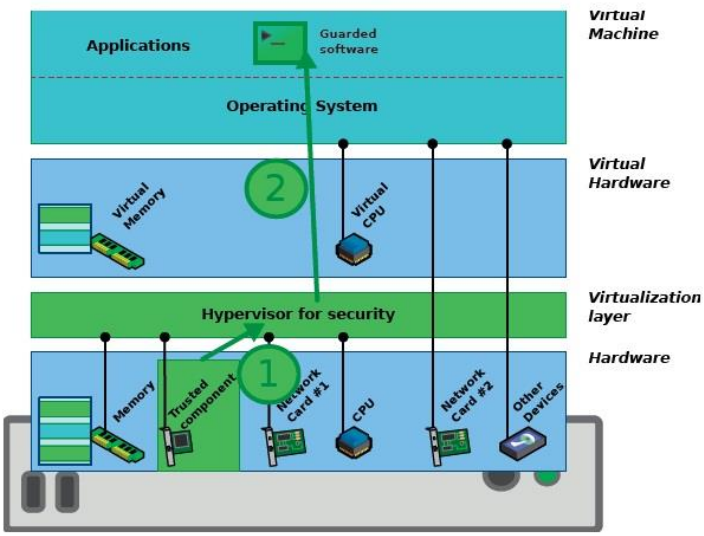
DIGITAL RISK & SECURITY

CMID: securely execute integrity checks of highly-critical software

Subtle attacks are able to successfully exploit vulnerabilities in low-level software, e.g. through compromised peripherals, even when running in the most privileged mode of a CPU providing built-in security features (e.g. Intel).

DESCRIPTION*

- CMID is a hybrid software-hardware trusted architecture for software integrity monitoring (security hypervisor and Trusted Hardware FPGA based component)
- Provide a highly secured environment for running a “guarded software”
- Risk of successfully corrupting the Trusted Hardware Component is extremely low
- Phase1: Trusted Hardware Component checks the integrity of the Security Hypervisor through challenges and environment checks
- Phase2: Security Hypervisor checks the integrity of the Guarded Software through an integrity function f provided by the developer of the guarded software



TECHNICAL SPECIFICATIONS

CPU	Intel (others possible)
Trusted HW Component	PCI Express
CPU Overhead	0-1%

*Technology recquiring license rights.

TOULOUSE TECH TRANSFER

COMPETITIVE ADVANTAGES

- Detect attacks linked to hardware vulnerabilities or misconfigurations
- Insignificant CPU overhead

APPLICATIONS

- Data centers
- Secured IT infrastructures
- Embedded Systems

INTELLECTUAL PROPERTY

- Software - Copyright

DEVELOPMENT STAGE

- Technology validated in relevant environment

1 2 3 4 **5** 6 7 8 9

LABORATORY

- TSF team

LAAS CNRS

CONTACT

T. +33 (0)5 62 25 50 60
numerique@toulouse-tech-transfer.com
www.toulouse-tech-transfer.com