Detection of virtual machine monitor corruptions

Benoît Morgan, Eric Alata, Vincent Nicomette

LAAS-CNRS - Dependable Computing and Fault Tolerance (TSF) Team

Journée SEC 2 - June 30th, 2015

Outline

Context

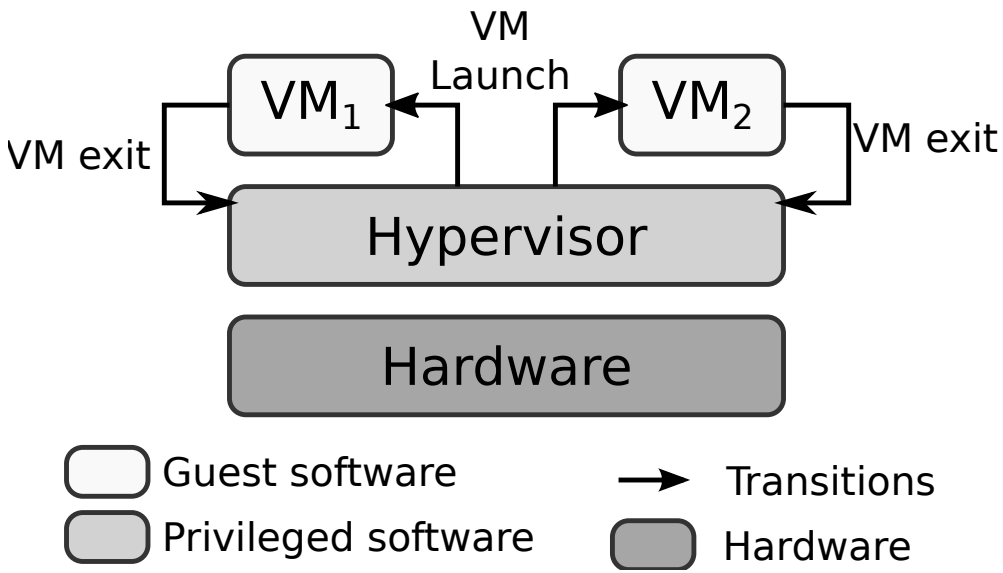
Project SVC – *Secured Virtual Cloud*

- Project Investissement d'Avenir
  Itrust, *Bull*, *Eneed*, *Secludit*, *Eurogiciel*, *Val Informatique*, *Blue Mind*, *LAAS-CNRS*, *IRIT*
- Project Coordinator : Bull

LAAS Contributions – 3 PhDs, 2 focusing on security

- Evaluation of intrusion detection mechanisms in *clouds*
- **Detection of virtual machine monitor corruptions**

Virtual machine monitors



- Privileged entity
- Ensures space and time isolation between virtual machines
- Control model similar to operating system control over userland applications

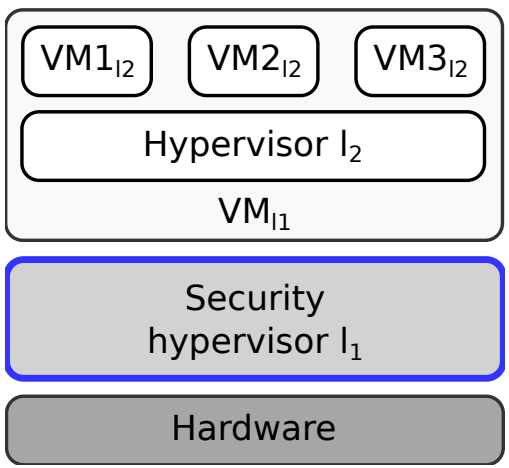
Motivations

- More and more complex VMM
  - Xen, KVM, VMware ESXi
  - Peripherals virtualisation
  - Mass storage virtualisation
  - Remote administration
- Vulnerabilities regularly discovered
- Large attack surface
- Necessity to detect the compromission of the hypervisor

Outline

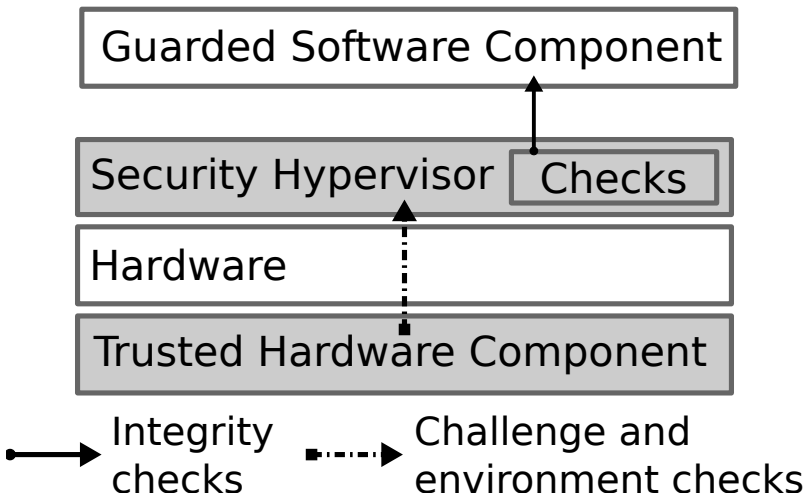
Trusted architecture proposed

- A tiny security hypervisor (l_1) in charge of detecting corruption of virtualised hypervisor (l_2)



- BUT, the security hypervisor (l_1) may be also attacked and compromised
  - Hardware bugs
  - Malicious peripherals
- Necessity to control the integrity of the security hypervisor itself through a trusted autonomous hardware component

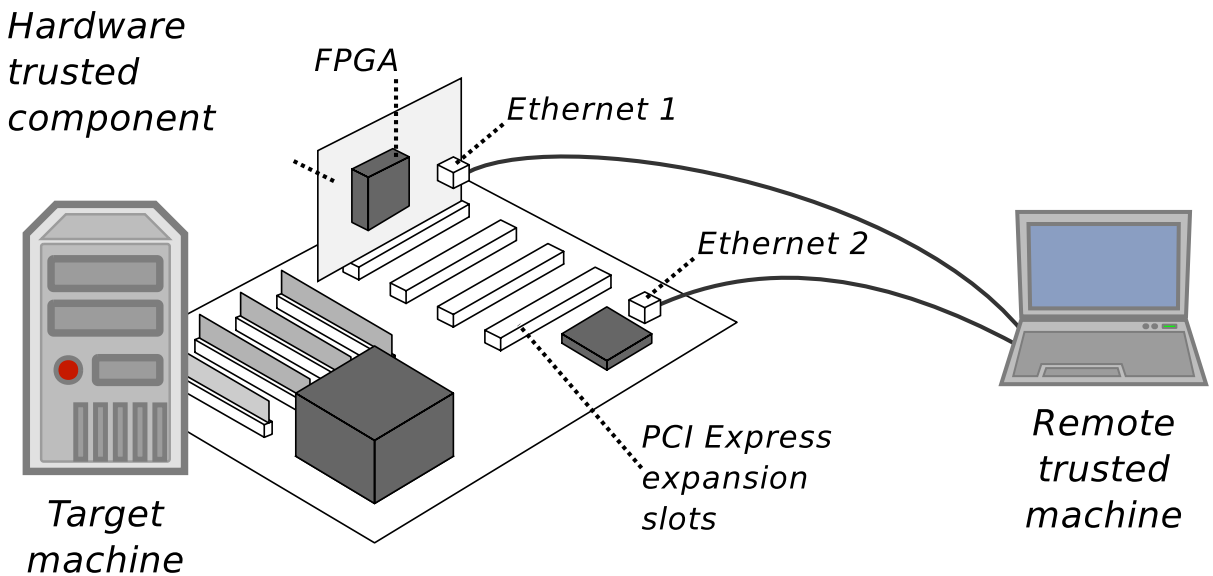
An execution enclave of integrity checks



1. The integrity of the security hypervisor is regularly checked by the trusted hardware component through 1) challenges and 2) environment checks
2. The integrity of the guarded software component is checked by the security hypervisor
3. Alarms are raised when challenges or integrity checks fail

Prototype

- PC with Intel processor (VT-x, VT-d), PCI Express bus
- Trusted hardware component based on FPGA technology
- Bare metal security hypervisor using nested virtualisation technology
- Experimentation with Linux and a corrupted driver in the kernel as the Guarded Software Component



- Publications : SSTIC 2014[2]

Outline

Perspectives

- Current virtualisation of KVM ou VMware ESXi
- Improving the challenges and environment checks

- First prototype of recursive hypervisor (allowing to implement several security mechanisms at different privilege levels)
- Publications : SSTIC 2015[3]

Detection of virtual machine monitor corruptions

Benoît Morgan, Eric Alata, Vincent Nicomette

LAAS-CNRS - Dependable Computing and Fault Tolerance (TSF) Team

Journée SEC 2 - June 30th, 2015

Références

[1] http://sarssi2013.univ-pau.fr/index.php/programme

[2] https://www.sstic.org/2014/presentation/tests_dintegrite_dhyperviseurs/

[3] https://www.sstic.org/2015/presentation/abyme__un_voyage_au_coeur_des_hyperviseurs_recursifs/

- Démo 1 : https://youtu.be/Nax0SHUx9GQ
- Démo 2 : https://youtu.be/1yz_ZUA2KGM