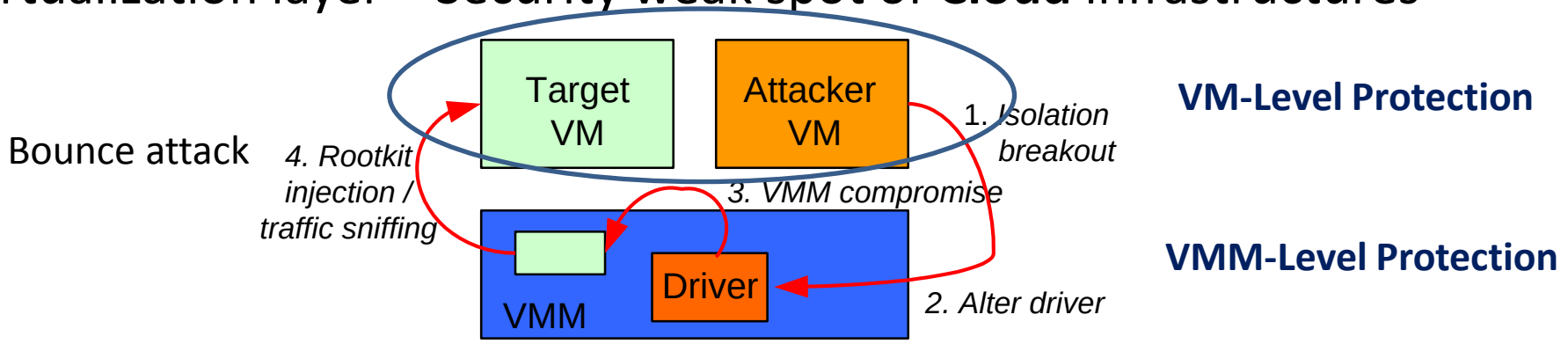
KungFuVisor: Enabling Hypervisor Self-Defense

EuroDW 2012

Aurélien Wailly (Orange Labs)
aurelien.wailly@orange.com
Marc Lacoste (Orange Labs)
marc.lacoste@orange.com
Hervé Debar (Télécom SudParis)
herve.debar@it-sudparis.net

Challenge

Virtualization layer = Security weak spot of **Cloud** infrastructures



Focus: Protecting the hypervisor

- Resource sharing
- Hypervisor breakout
- Poorly confined **device drivers** are the ones to blame!

Existing techniques are not enough!

Driver virtualization, Driver sandboxing, Trusted computing, …

No protection for the VMM layer

Approach: Self-Protecting Hypervisor

Design principles

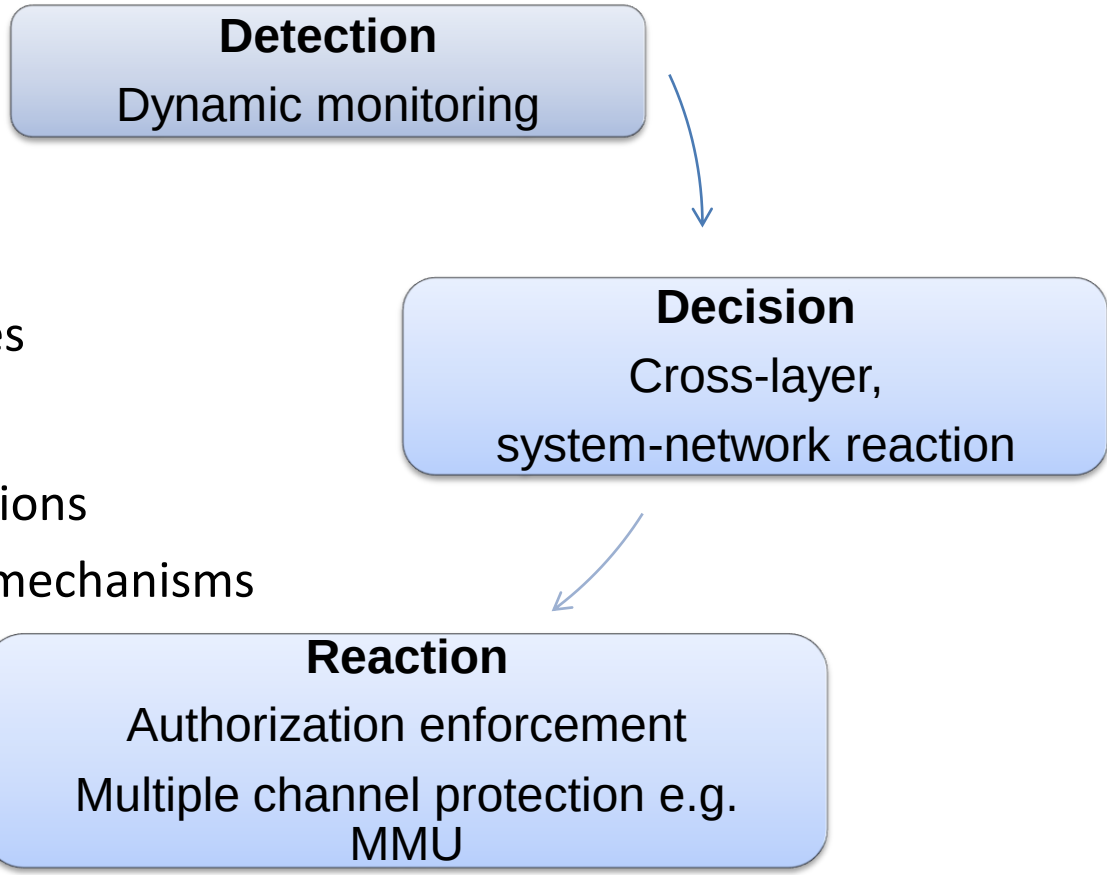
- **Autonomic** architecture
- Multiple **security loops**

Benefits

- **Automated management**
- **Flexibility** of security policies

KungFuVisor overview

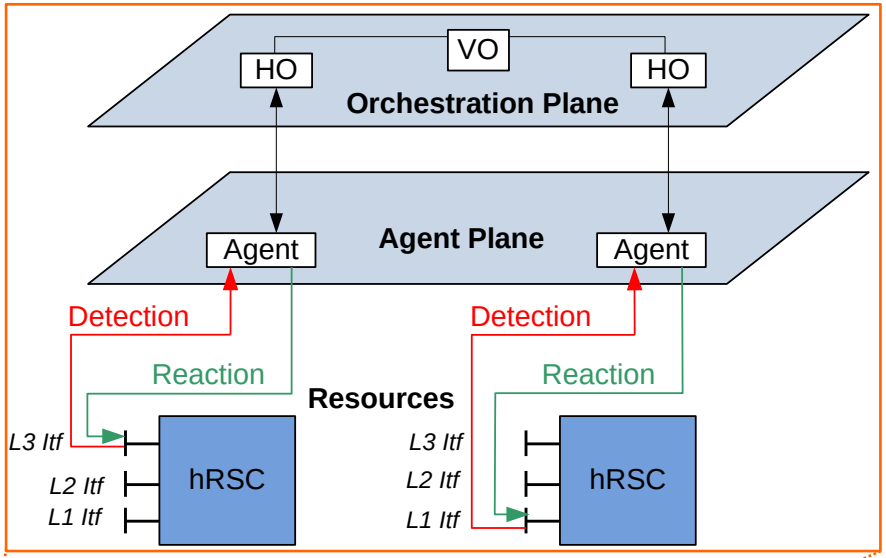
- Mediation of driver interactions
- Compatibility with existing mechanisms

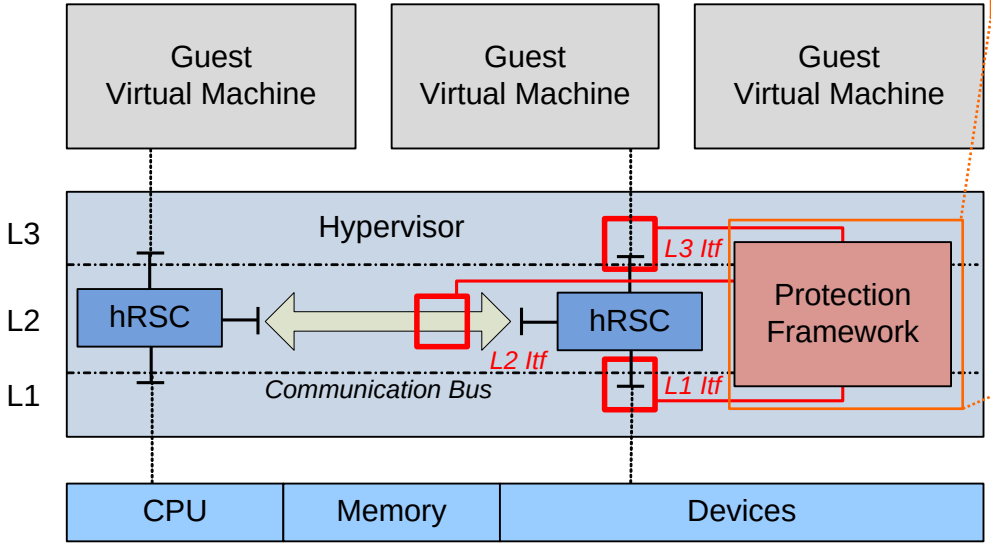


Solution: KungFuVisor

Orchestrators
HO: local threat response
VO: System-wide decisions

Agents
hRSC wrappers
Monitor and modify resources





Layer3
Hypercalls from VMs

Layer2
Hypervisor view of Layer1 resources

Layer1
HW compute/networking resources

Current Status

KungFuVisor brings self-defense to hypervisors

Ongoing work:

- First **specification/implementation** of the framework
- Added components in *kvm* parts containing drivers

Future work:

- **Mapping** framework to other VMMs
- **Protecting** framework components
- **Offloading** framework components in security VM