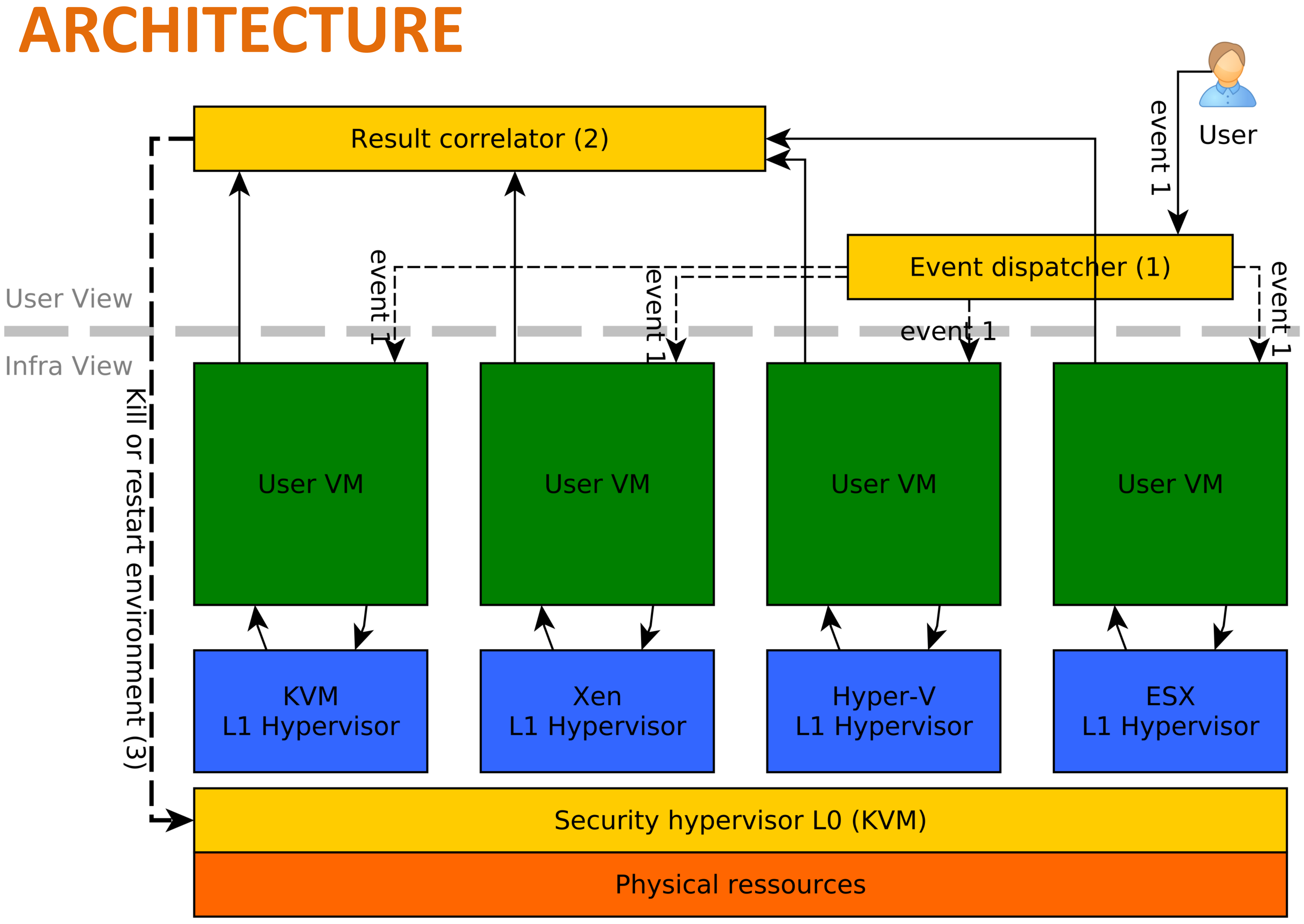
RetroVisor: Nested Virtualization for Multi-IaaS VM Availability

Aurélien Wailly[1], Marc Lacoste[1], Hervé Debar[2]

[1]Orange Labs, [2]Télécom SudParis

ARCHITECTURE



CONTEXT

Problem

Multi-IaaS platforms offer low protection against the failure of an hypervisor

- Is it possible to replicate execution of a single VM on different hypervisors ?

Solution: RetroVisor

Security architecture to seamlessly run a virtual machine on multiple hypervisors simultaneously.

Benefits

- High-availability
- Strong execution guarantees

IMPLEMENTING THE DISPATCHER

Option 1: User-based synchronization

- User handles multiple connections to the hypervisor.
- Sends mouse moves / keystrokes to each hypervisor.

\+ VNC clients are available in Python.
\- **Increased size** of client display program.
\- User has to **perform entire security administration**.

Option 2: Router-based synchronization

- Packets received on router VNC port are replicated.

\+ **Transparent security management**.
\- Network protocols and management components need to be modified (porting RFB or using UDP tunnel).

Option 3: L0 Hypervisor-based synchronization

- **Facade to L1 hypervisors** to notify user events to VMs.

\+ User uses normalized interfaces, **increasing security**.
\- **Error-prone:** each bug in L0 hypervisor severely threatens infrastructure security.

We selected the user-based approach as a first implementation of RetroVisor

EVALUATION (higher is better)

Approach	Easiness	Fault tolerance	Genericity	Security
User	High	High	High	Low
Router	High	Medium	Medium	High
Hypervisor	Low	Low	Low	High

Summary

- **Strong guarantees** of VM execution.
- **High availability**.
- Leverage nested virtualization.
- **Detect** failures and **recover** to a safe state.

NEXT STEPS

- More investigation of reaction mechanisms.
- Advanced threat detection through the **VESPA** framework [ICAC12].

REFERENCES

[CCS12] S. BUTT et al. Self-Service Cloud Computing. CCS 2012.

[VESPA] A. WAILLY, M. LACOSTE, and H. DEBAR. VESPA: Multi-Layered Self-Protection forCloud Resources. ICAC'12.

[RFB] T. RICHARDSON and J. LEVINE. The Remote Framebuffer Protocol. IETF RFC 6143, 2011.

[OSDI10] M. BEN-YEHUDA et al. The Turtles project: Design and Implementation of Nested Virtualization. OSDI'10.

[XenB12] D. WILLIAMS et al.. The Xen-Blanket: Virtualize Once, Run Everywhere. EUROSYS'12.