EMC2 3rd conference
Paris, September 28th 2016

BLIND HYPERVISION TO PROTECT VIRTUAL MACHINES DEMONSTRATION

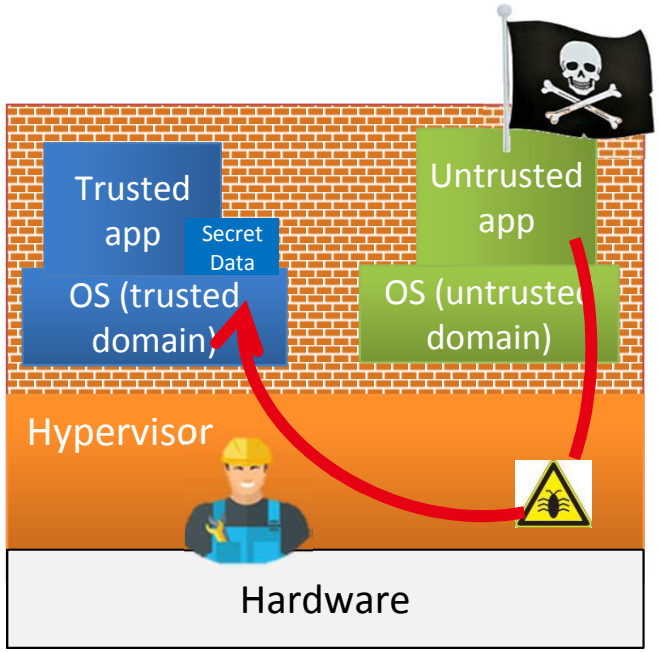
Moha AIT HMID

MULTI-DOMAIN SOFTWARE ATTACK

- **Objective : protect trusted domain privacy against software attacks from co-located untrusted domain**

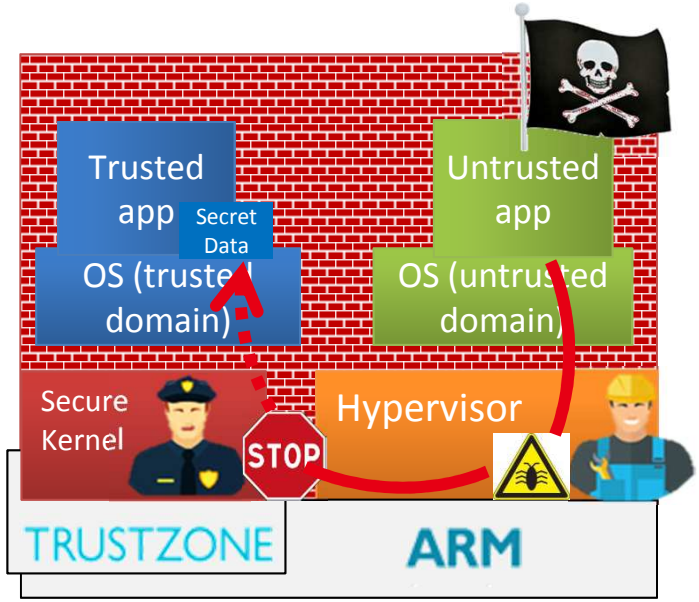
- **Traditional OS/hypervisor**
  - Ensure domain isolation
  - Is root of trust (TCB, Trusted Computing Base)
  - Has complete control of hardware features (eg MMU) that isolates domains

- **Weakness of existing solutions**
  - OS/Hypervisor are often too big/complex for complete/formal verification (=> possible vulnerably that may jeopardize domain isolation)



CEA SECURED HYPERVISOR SOLUTION

- Provides domain isolation (confidentiality and integrity) against software attacks including from hypervisor and equipment interfaces
- Domain isolation ensured by a small Secure Kernel (< 3kLoC) protected by ARM TrustZone hardware feature
- Untrusted hypervisor manage domains without accessing them
- High level assurance (small TCB => formal verification feasible)



SECURE KERNEL PARTITION ISOLATION DISABLED

Hypervisor forwards encrypted messages and schedules VMs

Attacker VM1

Attempts at decyphering

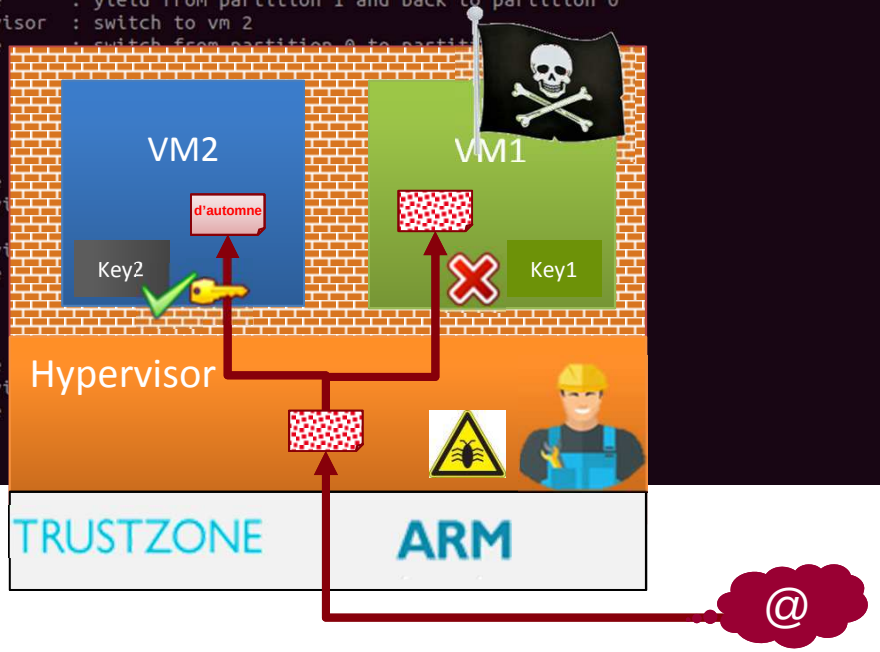
Victim VM2

Decyphers messages

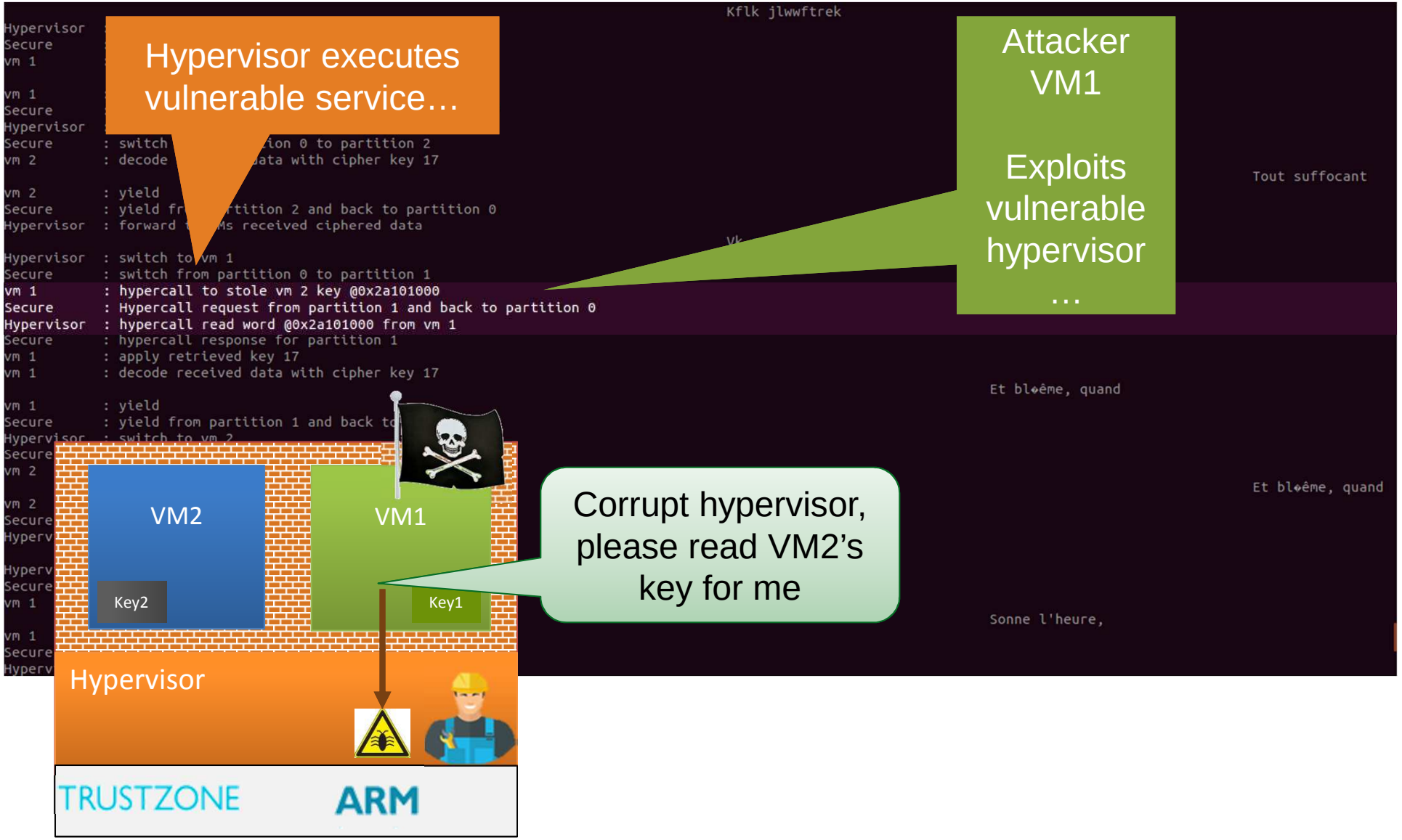
```
BOOTP broadcast 12
BOOTP broadcast 13
BOOTP broadcast 14
Secure      : reset and switch to Hypervisor (partition 0)
Hypervisor  : start

Hypervisor  : reset of vm 1
Secure      : reset partition 1
Hypervisor  : reset of vm 2
Secure      : reset partition 2
Hypervisor  : forward to VMs received ciphered data

Hypervisor  : switch to vm 1
Secure      : switch from partition 0 to partition 1
vm 1        : start with cipher key 0 stored at @29101000

vm 1        : decode received data with cipher key 0

vm 1        : yield
Secure      : yield from partition 1 and back to partition 0
Hypervisor  : switch to vm 2
Secure      : switch from partition 0 to partiti
vm 2

vm 2

vm 2
Secure
Hypervi

Hypervi
Secure
vm 1

vm 1
Secure
Hypervi
Secure
vm 2

vm 2
```

```
Hypervisor

Tyrejfe u'rlkfdev

Cvj jrexcfkj cfexj
```

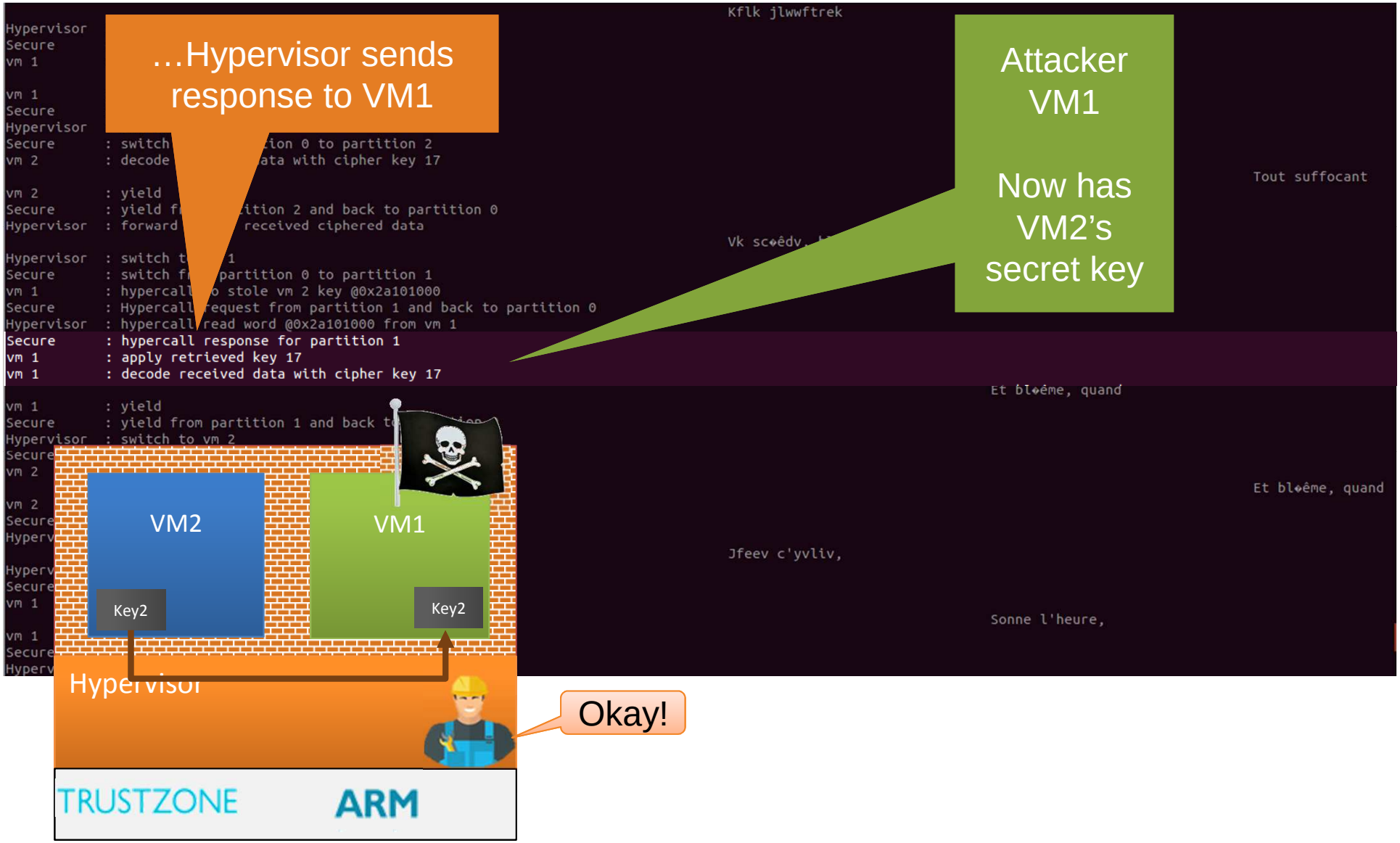
```
VM 1

Tyrejfe u'rlkfdev

VM 2

Chanson d'automne

Cvj jrexcfkj cfexj

Les sanglots long
```



SECURE KERNEL PARTITION ISOLATION DISABLED



SECURE KERNEL PARTITION ISOLATION DISABLED



SECURE KERNEL PARTITION ISOLATION DISABLED

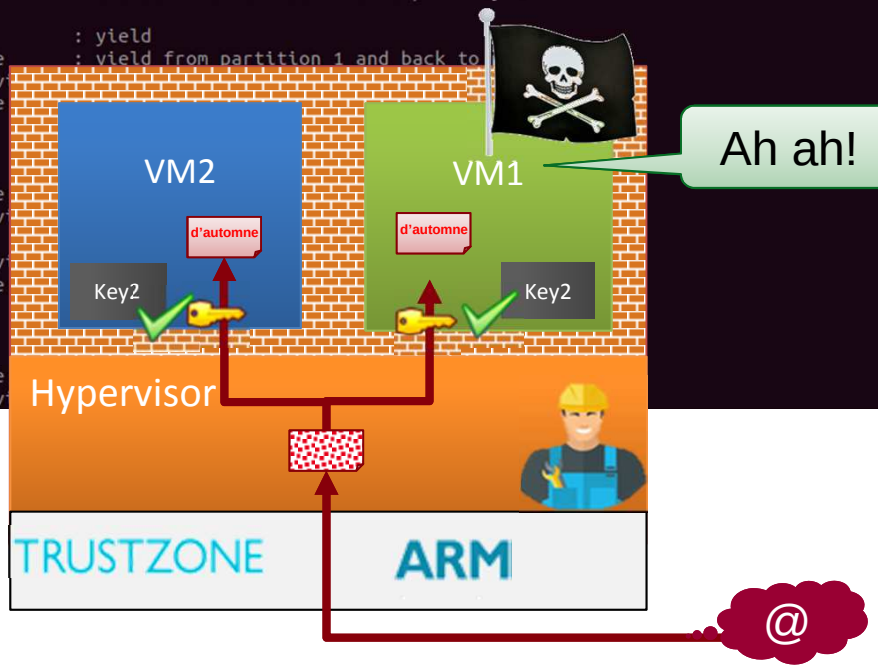
```
Hypervisor  : switch to vm 1
Secure      : switch from partition 0 to partition 1
vm 1        : decode received data with cipher key 0

vm 1        : yield
Secure      : yield from partition 1 and back to partition 0
Hypervisor  : switch to vm 2
Secure      : switch from partition 0 to partition 2
vm 2        : decode received data with cipher key 17

vm 2        : yield
Secure      : yield from partition 2 and back to partition 0
Hypervisor  : forward to VMs received ciphered data

Hypervisor  : switch to vm 1
Secure      : switch from partition 0 to partition 1
vm 1        : hypercall to stole vm 2 key @0x2a101000
Secure      : Hypercall request from partition 1 and back to partition 0
Hypervisor  : hypercall read word @0x2a101000 from vm 1
Secure      : hypercall response for partition 1
vm 1        : apply retrieved key 17
vm 1        : decode received data with cipher key 17

vm 1        : yield
Secure      : yield from partition 1 and back to
Hyperv
Secure
vm 2

vm 2
Secure
Hyperv

Hyperv
Secure
vm 1

vm 1
Secure
Hyperv
```

```
Kflk jlwwftrek

Vk sc◆êdv, hlreu

Jfeev c'yvliv,
```

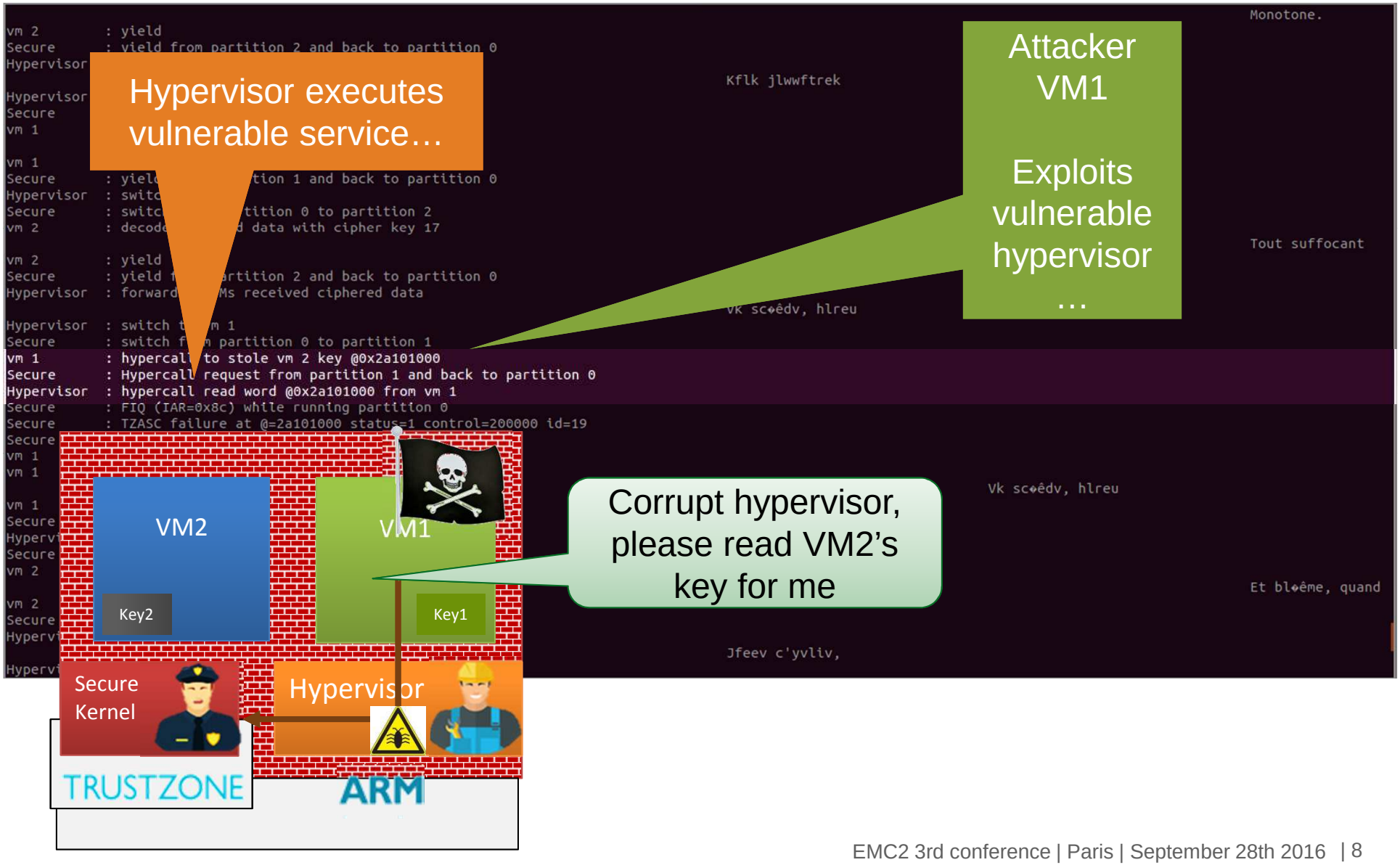
Attacker VM2

Can decrypt messages!

```
Tout suffocant

Et bl◆ême, quand

Et bl◆ême, quand

Sonne l'heure,
```

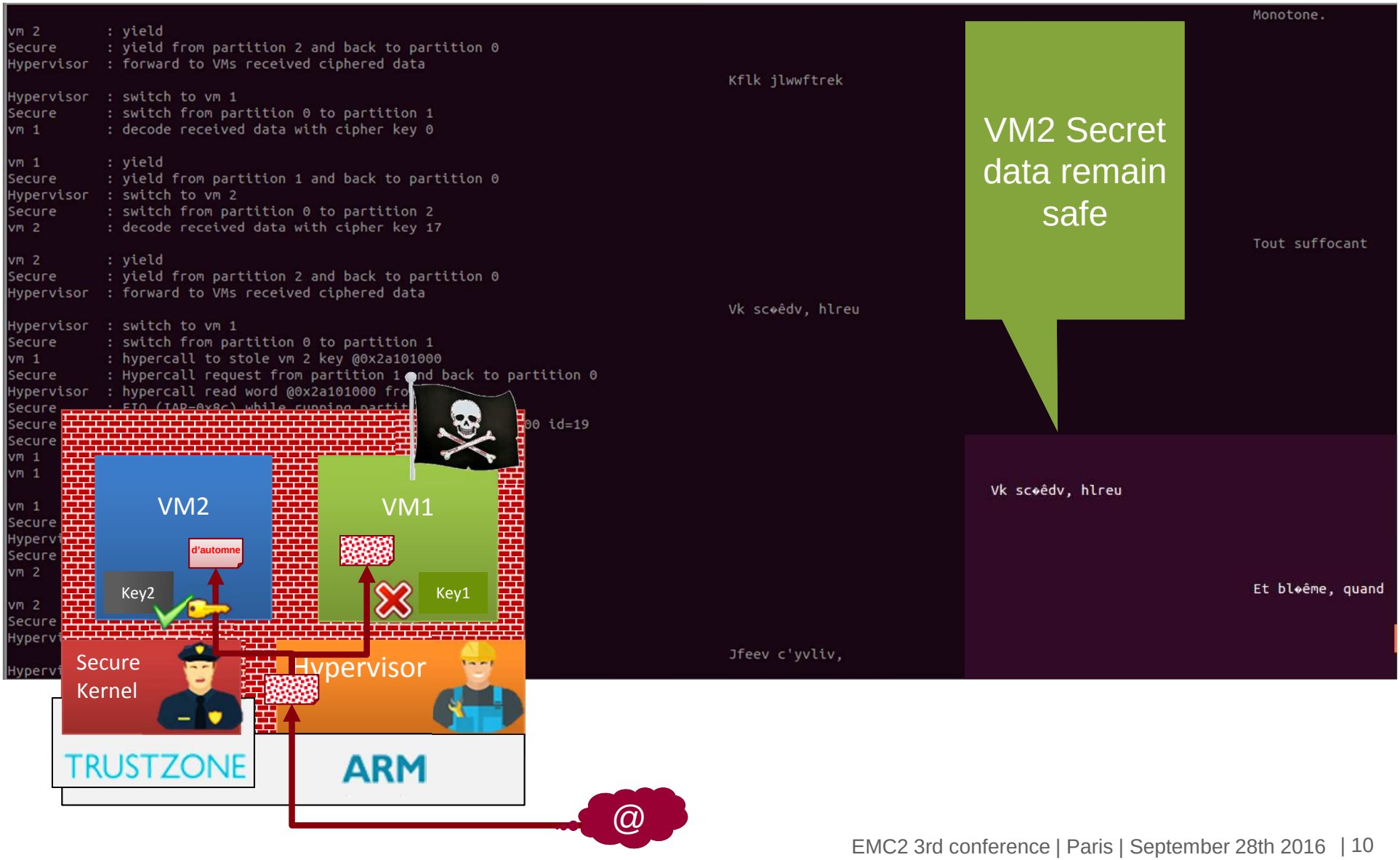


SECURE KERNEL PARTITION ISOLATION ENABLED



SECURE KERNEL PARTITION ISOLATION ENABLED

SECURE KERNEL PARTITION ISOLATION ENABLED



Centre de Saclay
Nano-Innov PC 172 - 91191 Gif sur Yvette Cedex

INSTITUT CARNOT CEA LIST