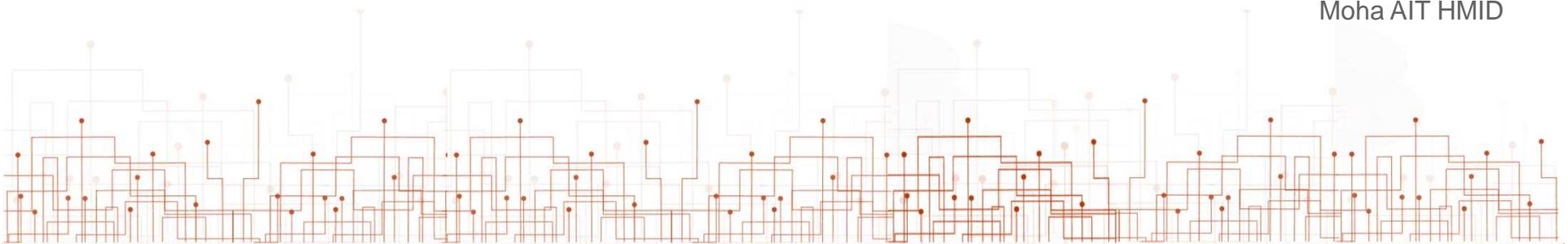


EMC2 3rd conference
Paris, September 28th 2016

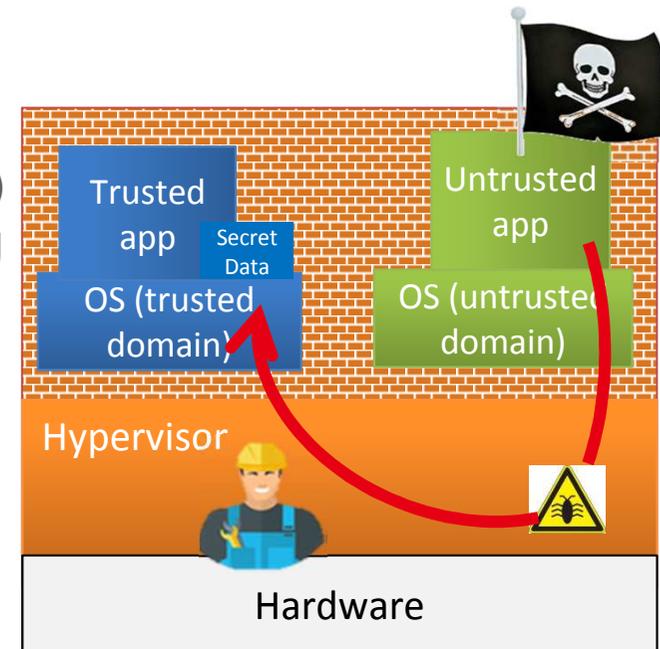
BLIND HYPERVISION TO PROTECT VIRTUAL MACHINES DEMONSTRATION

Moha AIT HMID



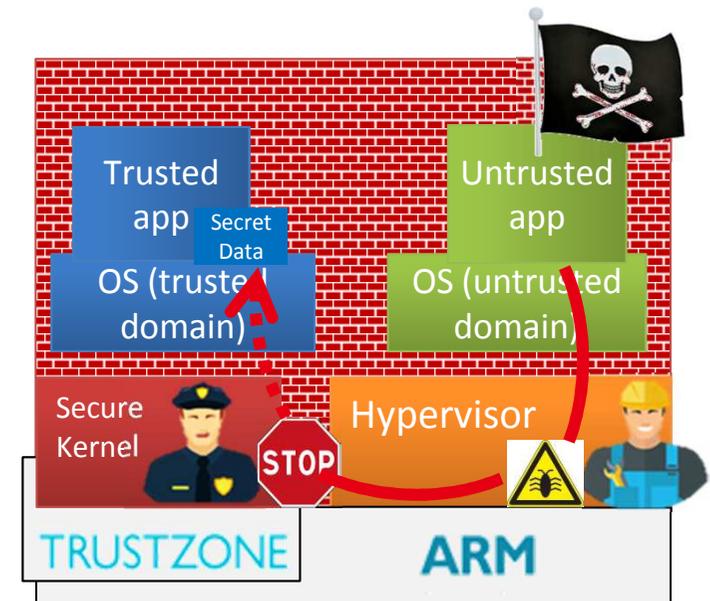
MULTI-DOMAIN SOFTWARE ATTACK

- 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)



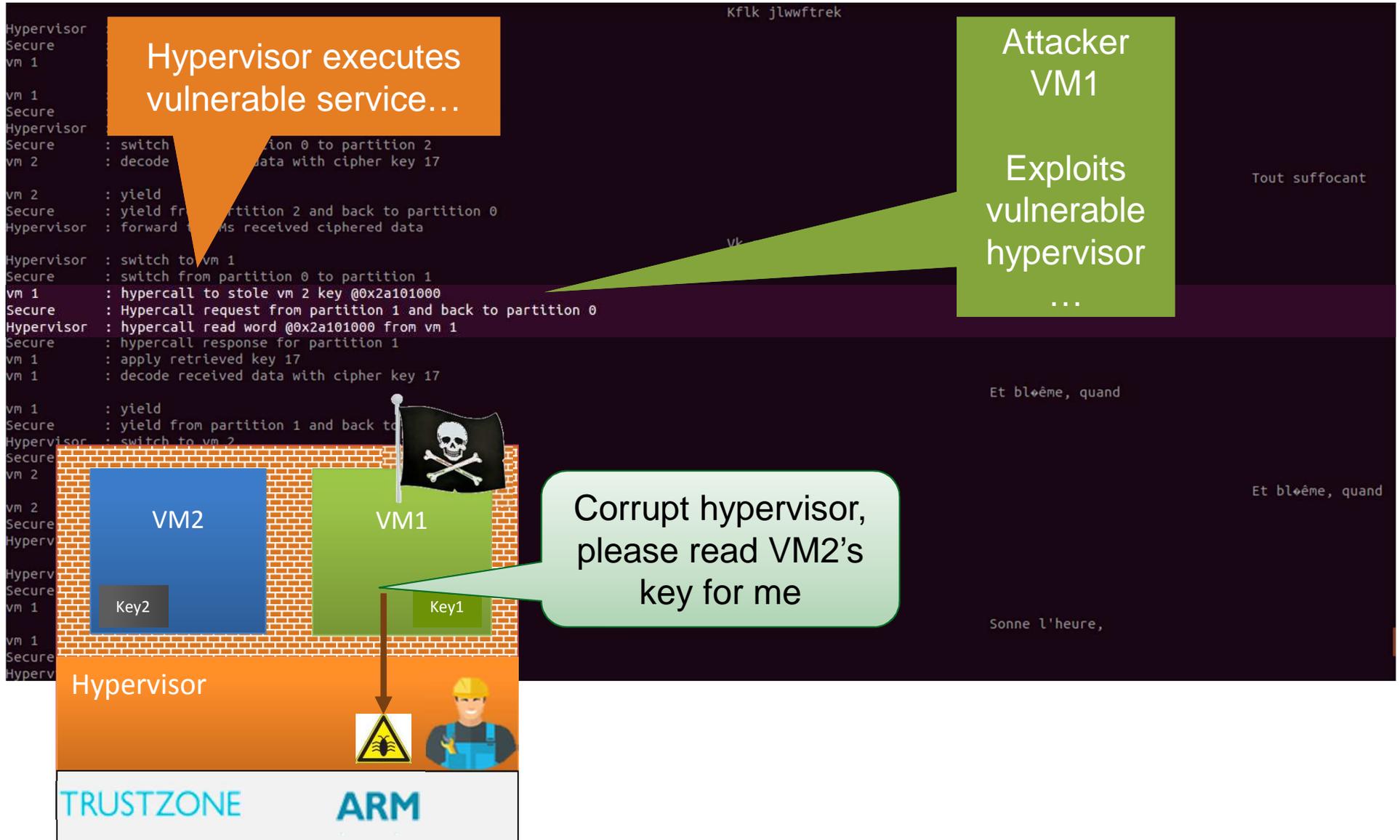
CEA SECURED HYPERVISOR SOLUTION

- 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)

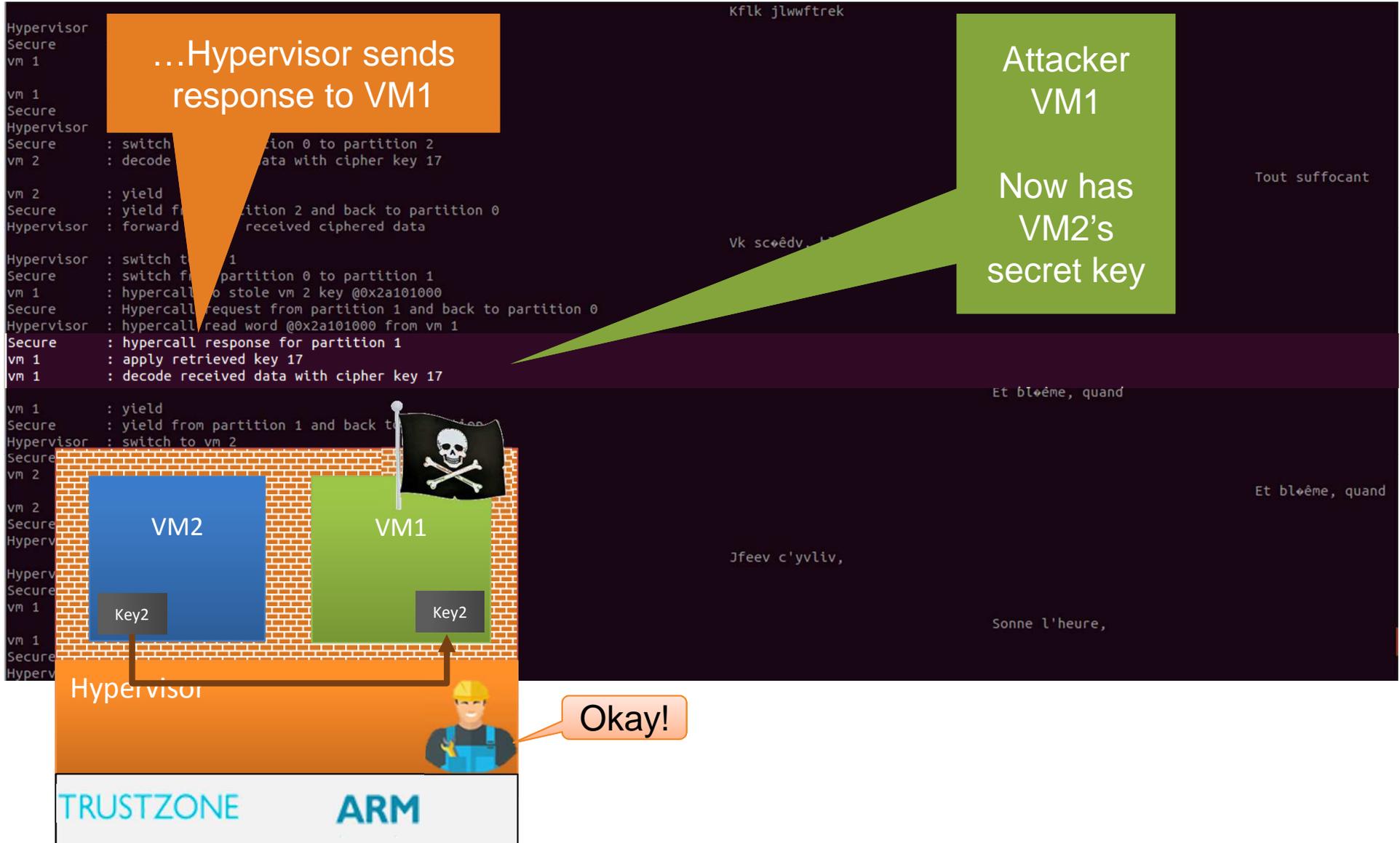




SECURE KERNEL PARTITION ISOLATION DISABLED



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 jlwftrek

Attacker VM2

Can decrypt messages!

Tout suffocant

Vk scøêdv, hlreu

Et bløème, quand

Et bløème, quand

Jfeev c'yvliv,

Sonne l'heure,

The diagram illustrates a security breach in a virtualized environment. Two virtual machines, VM1 and VM2, are shown within a Hypervisor. VM1 is depicted with a skull and crossbones flag, indicating it is the attacker. A speech bubble from VM1 says "Ah ah!". Both VMs contain a box labeled "Key2" with a key icon, suggesting they share a common cryptographic key. The Hypervisor is connected to a TRUSTZONE and an ARM chip. A red arrow points from the ARM chip to the Hypervisor, representing the data path. The background of the diagram is a brick wall, symbolizing a security barrier that has been compromised.



SECURE KERNEL PARTITION ISOLATION ENABLED

vm 2 : yield
Secure : yield from partition 2 and back to partition 0
Hypervisor : ...
Kflk jlwwftrek

vm 1 : yield from partition 1 and back to partition 0
Secure : yield from partition 1 and back to partition 0
Hypervisor : switch from partition 0 to partition 1
Secure : switch from partition 0 to partition 2
vm 2 : decode ... data with cipher key 17
vm 2 : yield
Secure : yield from partition 2 and back to partition 0
Hypervisor : forward ... VMs received ciphered data
VK scœdv, hlreu

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 : FIQ (IAR=0x8c) while running partition 0
Secure : TZASC failure at @=2a101000 status=1 control=200000 id=19
Secure : ...
vm 1 : ...
vm 1 : ...
vm 1 : ...
vm 2 : ...
Secure : ...
Hypervisor : ...
Hypervisor : ...
Jfeev c'yvliv,

Monotone.
Tout suffocant
Et bløeme, quand

Hypervisor executes vulnerable service...

Attacker VM1
Exploits vulnerable hypervisor
...

Corrupt hypervisor, please read VM2's key for me



SECURE KERNEL PARTITION ISOLATION ENABLED

```

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

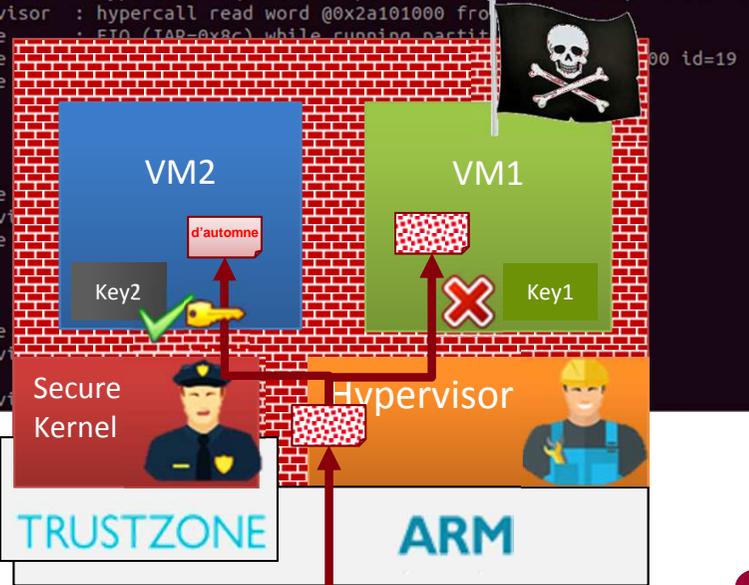
Hypervisor : switch to vm 1
Secure   : switch from partition 0 to partition 1
vm 1     : decode received data with cipher key 0

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
Secure   : FIQ (IAP=0x8c) while running partit
Secure   : 00 id=19
Secure
Secure
vm 1
vm 1
vm 1
Secure
Hyperv
Secure
vm 2
vm 2
Secure
Hyperv
Hyperv

```



VM2 Secret data remain safe

Kflk jlwftrek

Monotone.

Vk scœdv, hlreu

Tout suffocant

Vk scœdv, hlreu

Et blême, quand

Jfeev c'yvliv,



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

