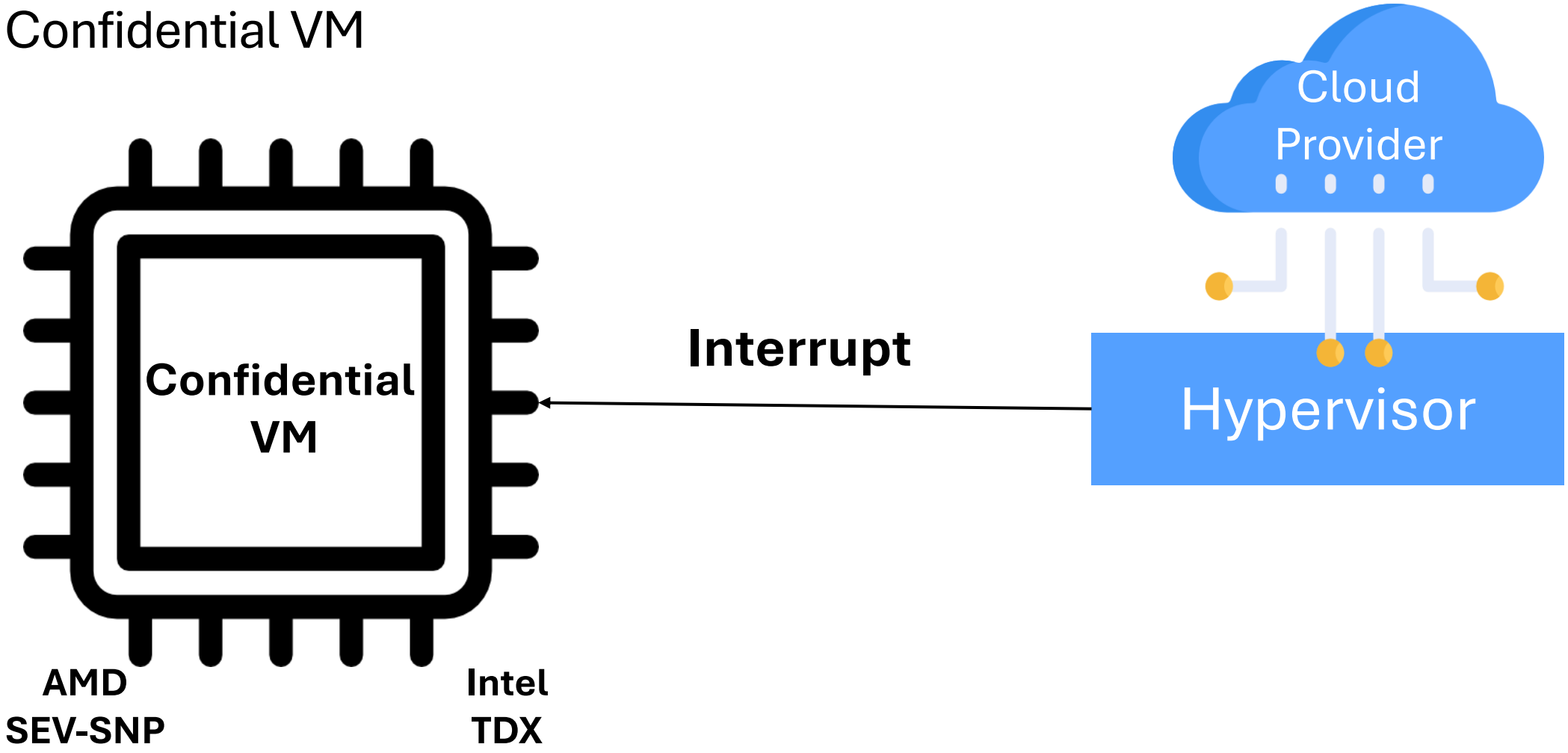
Heckler: Breaking Confidential VMs with Malicious Interrupts

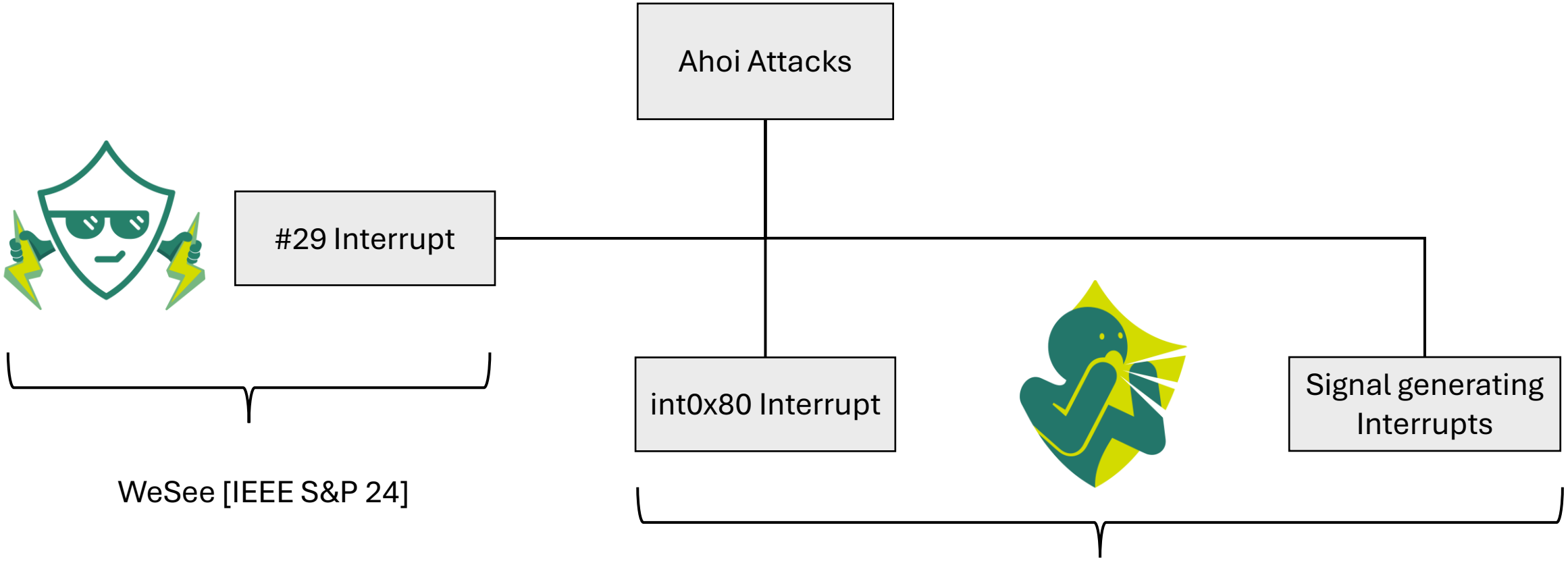
Benedict Schlüter, Supraja Sridhara, Mark Kuhne, Andrin Bertschi, Shweta Shinde

ETH Zurich

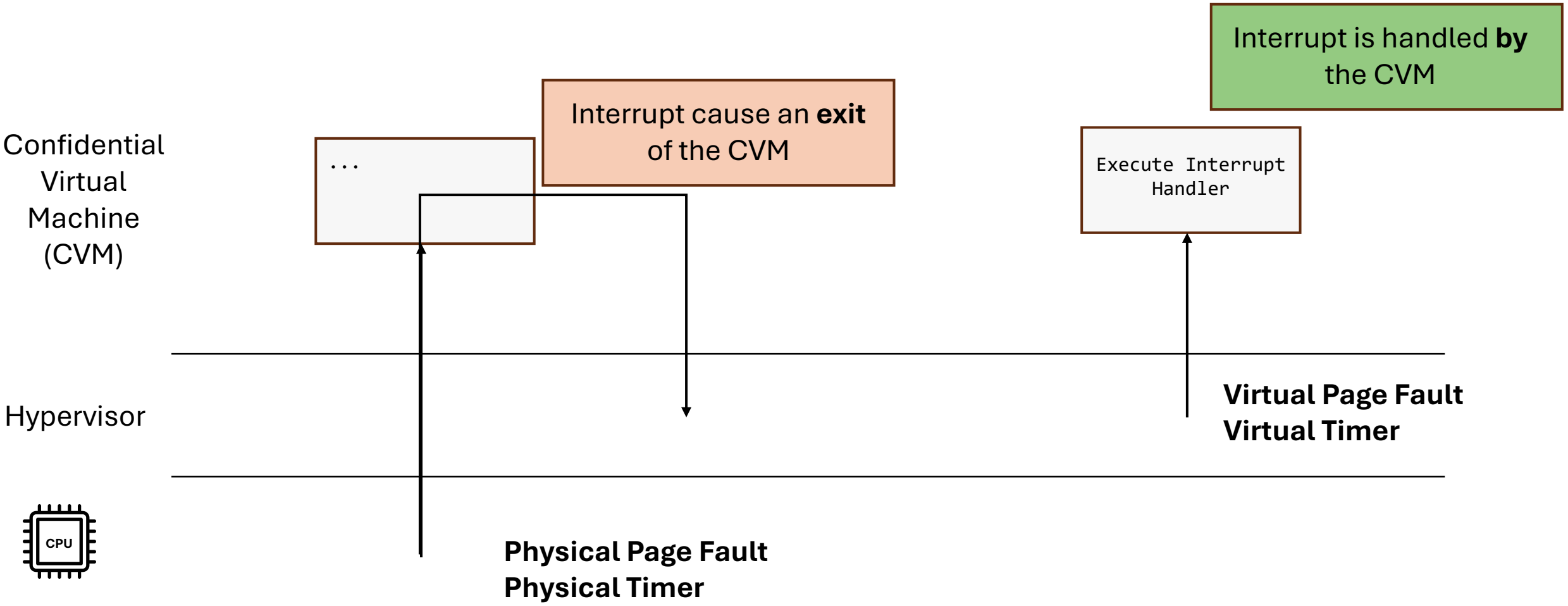
Confidential VM



Overview


Ahoi Attacks
#29 Interrupt
int0x80 Interrupt
Signal generating Interrupts
WeSee [IEEE S&P 24]
Heckler
Breaking Confidential VMs with Malicious Interrupts

Destination of Interrupts



`int 0x80`: Legacy Systemcall Flow

Userspace Register State

```
rax = #write_sys
int 0x80
...
```

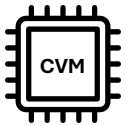
```
rax : 4
```

userspace

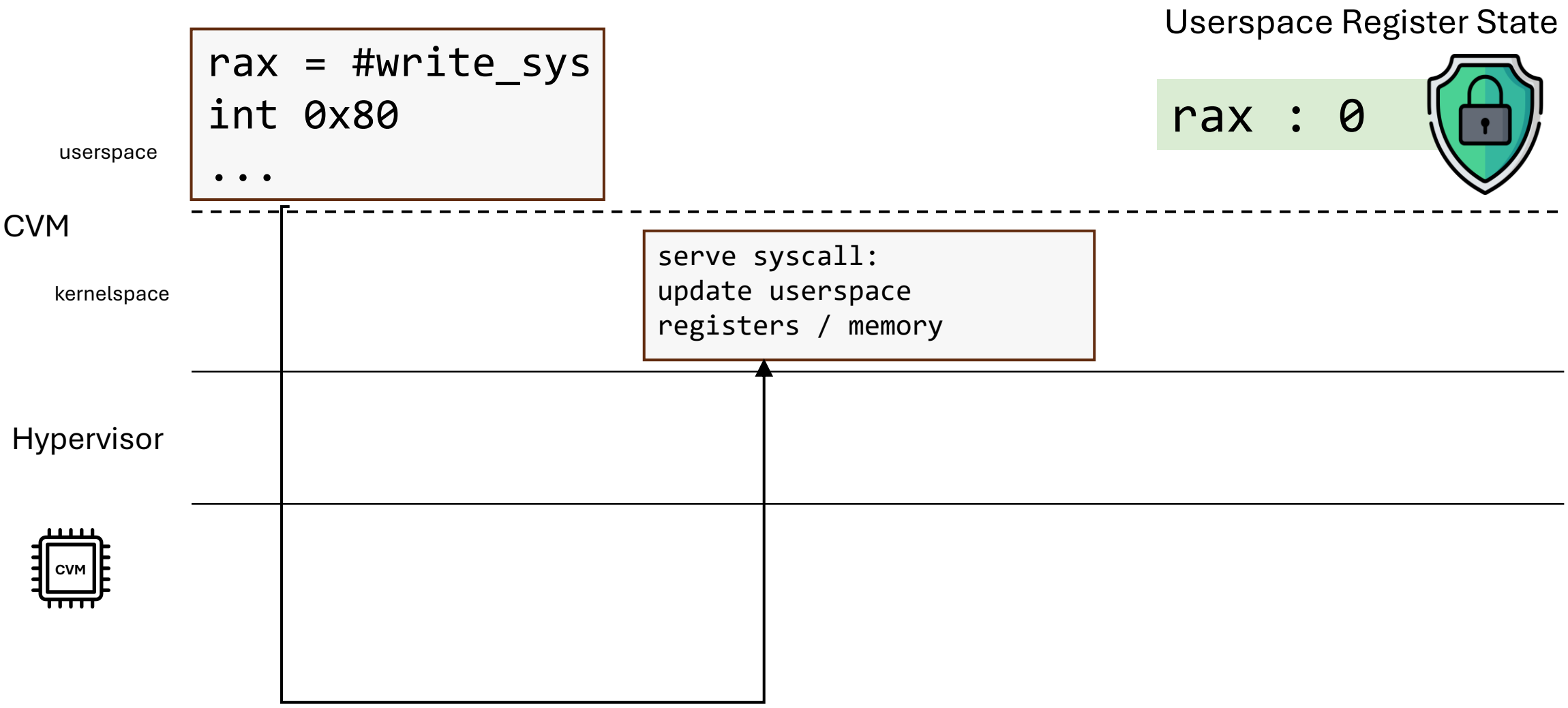
CVM

kernelspace

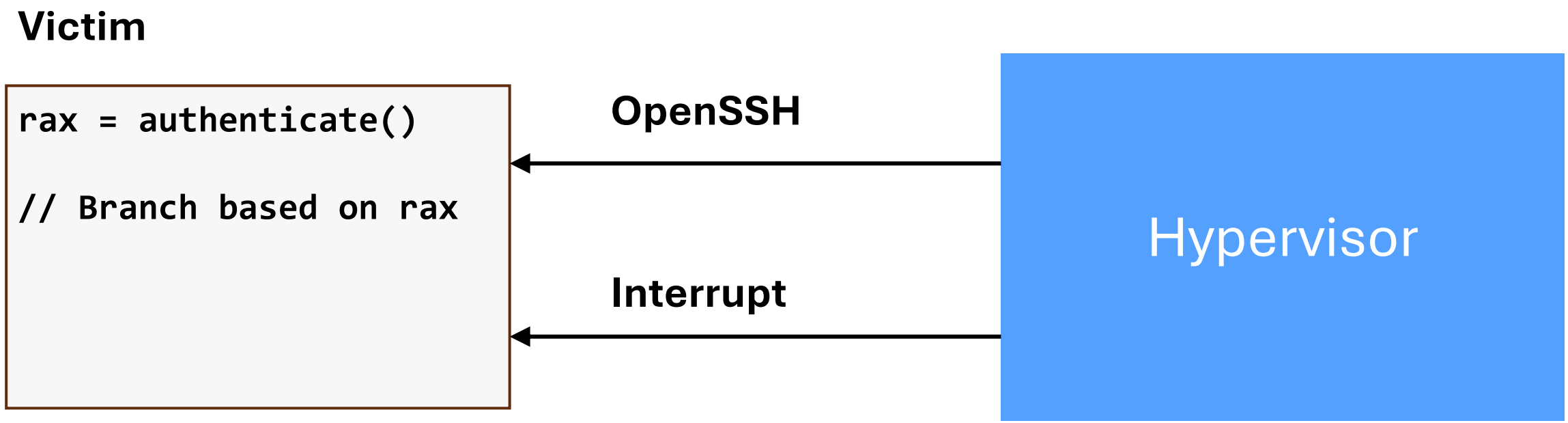
Hypervisor



`int 0x80`: Legacy Systemcall Flow



Remote Authentication



Heckler Attack (Intel TDX and AMD SEV-SNP)

```
rax = authenticate()
if (rax): goto auth
...
```

Userspace Register State

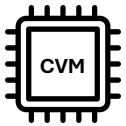
```
rax : 0
```

userspace

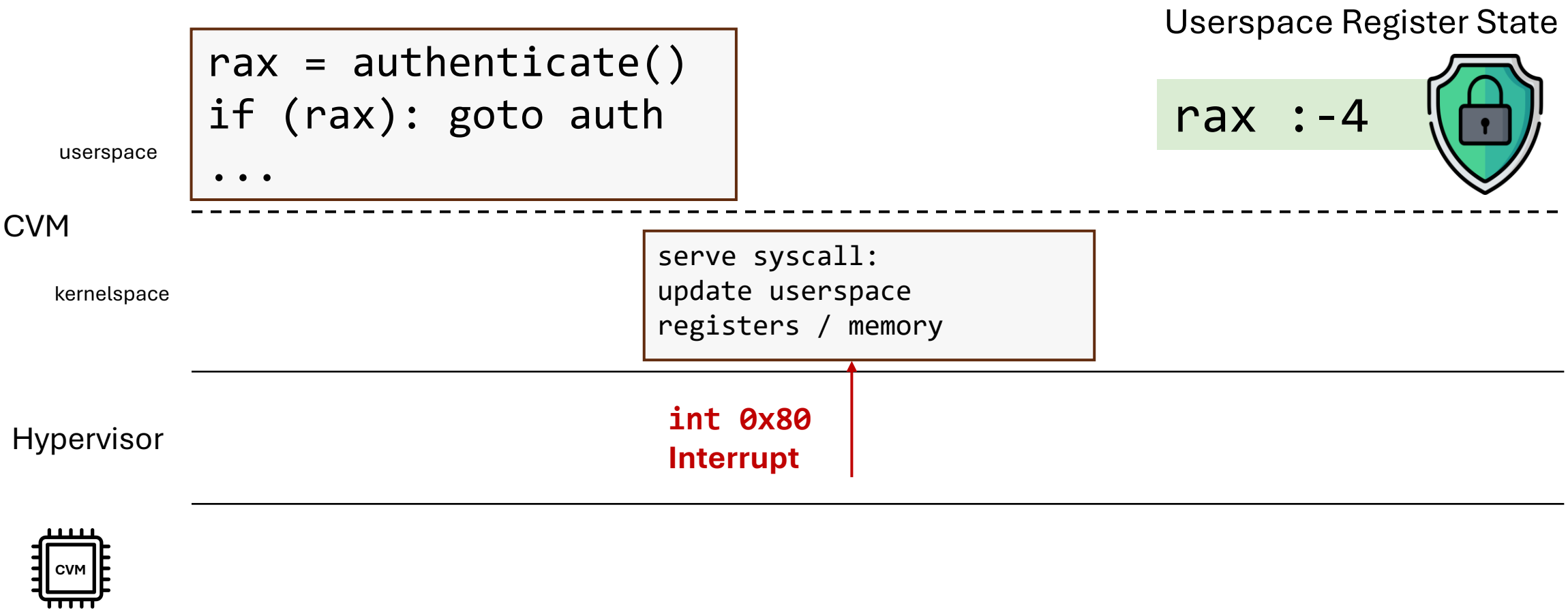
CVM

kernelspace

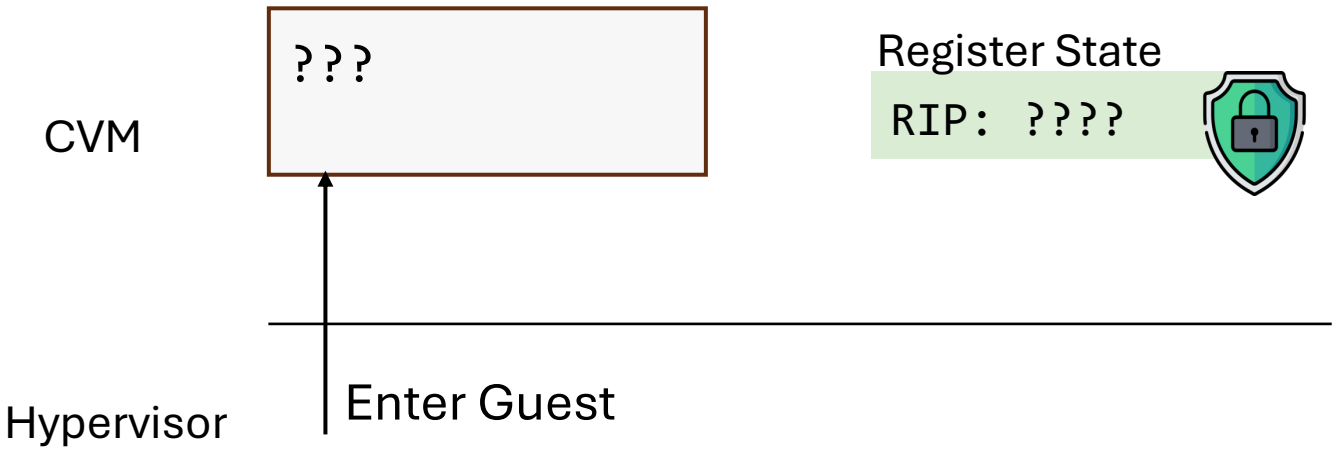
Hypervisor



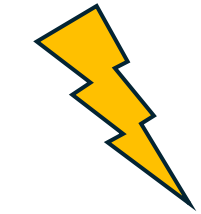
Heckler Attack (Intel TDX and AMD SEV-SNP)



Hypervisor View on CVM Execution State




```
rax = authenticate()
if (rax): goto auth
...
```



Tracking the page-level execution state of CVMs

```
rax = authenticate()
if (rax): goto auth
...
```

Page A

```
call authenticate
test eax,eax
je auth
...
```

Page B

```
do authentication
...
ret
```

Hypervisor observes page faults

Page A

Page B

Page A

Inject interrupt before marking Page A as executable

Finding Gadget Pages

Offline Phase

0xF00, 0x100, 0x200,
0x700, 0x900, 0x500,
0xB00, 0xC00, 0x900

Page A: 0xF00
Page B: 0x900

f(...)

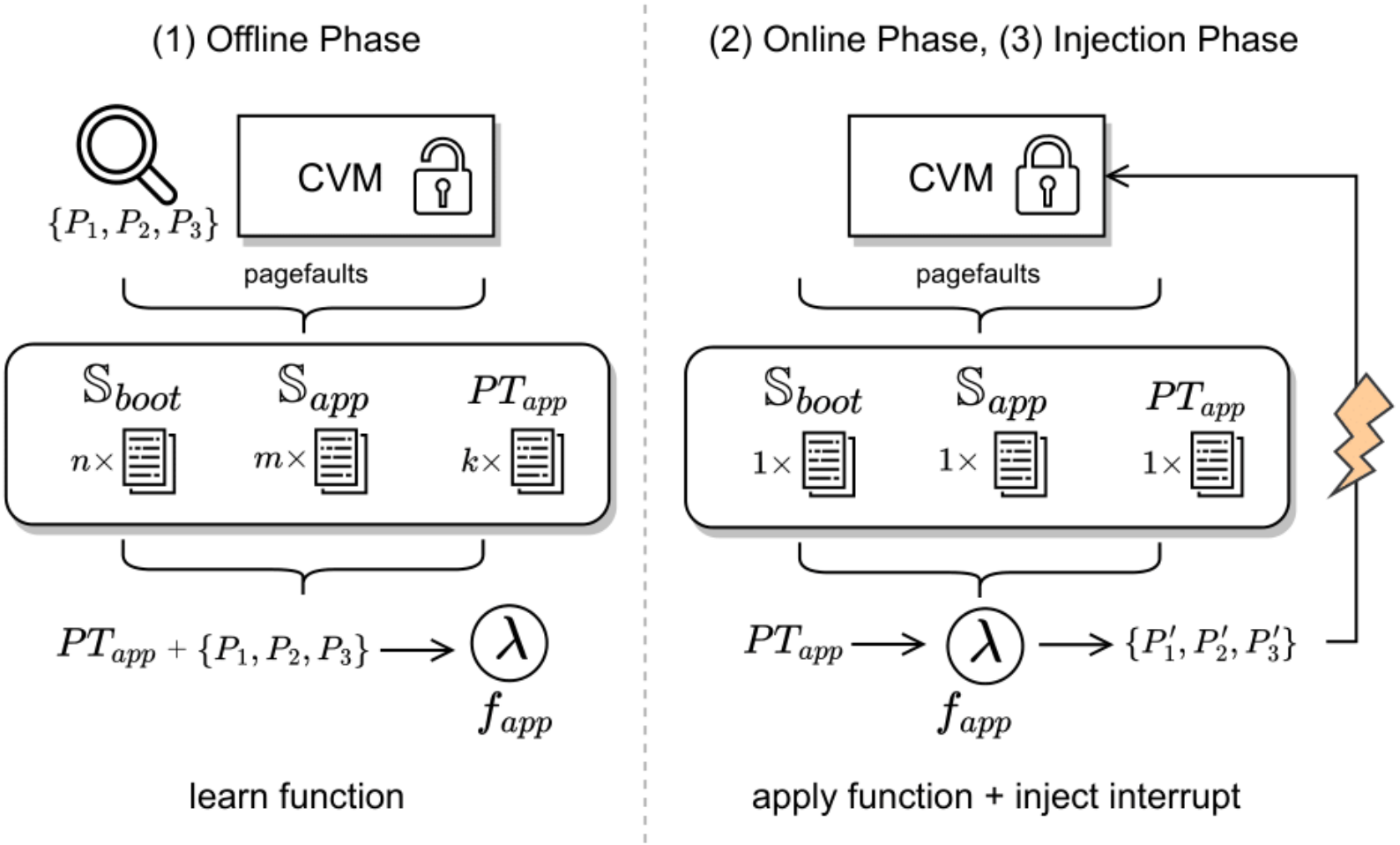
Attack Phase

0x800, 0x100, 0x200,
0x700, 0x900, 0x500,
0xB00, 0xC00, 0xA00

f(...)

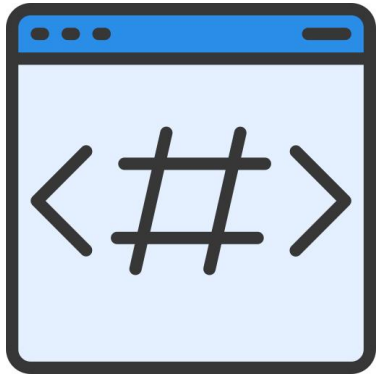
Page A: 0x800
Page B: 0xA00

Finding Gadget Pages



Case Studies

Bypass OpenSSH's password authentication



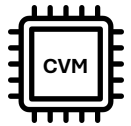
Bypass Sudo authentication (libPAM)

Signal Generating Interrupts (AMD SEV-SNP)

```
try {
    v = Covariance(...);
} catch(ArithmeticException ex) {
    v = 0;
}
```

CVM

Hypervisor



Signal Generating Interrupts (AMD SEV-SNP)

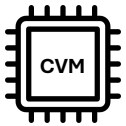
```
try {
    v = Covariance(...);
} catch(ArithmeticException ex) {
    v = 0;
}
```

CVM

```
serve interrupt:
Inject signal to
userspace
```

int 0x10
Interrupt

Hypervisor



Root Cause

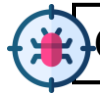
Hypervisor can inject interrupts that should never be generated by it

Hotfixes


CVE 2024-25743

Disable int0x80 syscall interrupt on CVMs (v6.7)

- Subsequent patch enables int0x80 **only** for TDX again and perform validation of interrupt source
- On SEV-SNP the VM cannot distinguish between interrupt sources


CVE 2024-25744

Signal generating interrupt sources remain unfixed until today (only SEV-SNP)

New class of attacks called Ahoi attacks:

- Malicious Interrupt Injection to trigger handlers
- This paper: int0x80 / signal generating Interrupts
- Our IEEE SP 2024 paper, WeSee: #VC

https://ahoi-attacks.github.io/

We demonstrate Heckler with case studies:

- OpenSSH password authentication bypass
- libPAM password authentication bypass (sudo, doas, …)

CVE 2024-25743 and 2024-25744