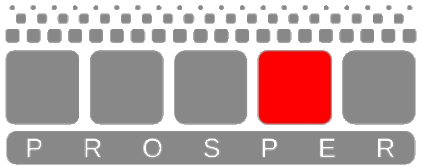
Roberto Guanciale
Mads Dam
Hamed Nemati
Christoph Baumann

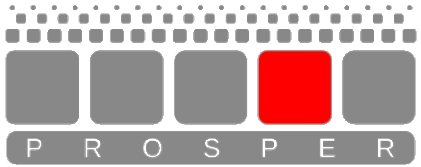
Cache Storage Channels **Alias-driven Attacks**

Formally Verified Platforms

Formally Verified Platforms



Formally Verified Platforms



Caches Excluded from the analysis

Formally Verified Platforms

seL4
Security. Performance. Proof.

Microsoft
Hyper-V

INTEGRITY

PROSPER

Caches Excluded from the analysis

Formally Verified Platforms

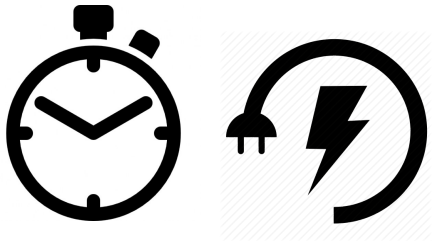
seL4
Security. Performance. Proof.

Microsoft Hyper-V

INTEGRITY

PROSPER

Caches Excluded from the analysis



Formally Verified Platforms

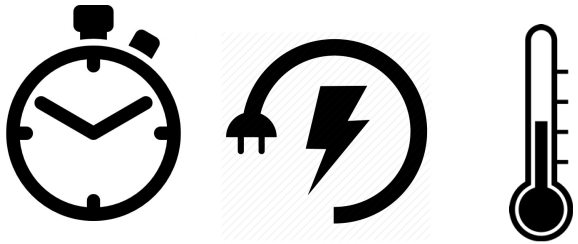
seL4
Security. Performance. Proof.

Microsoft Hyper-V

INTEGRITY

PROSPER

Caches Excluded from the analysis



Formally Verified Platforms

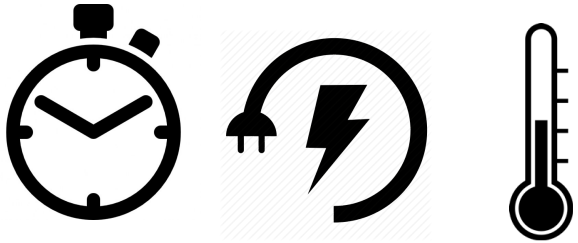
seL4
Security. Performance. Proof.

Microsoft Hyper-V

INTEGRITY

PROSPER

Caches Excluded from the analysis



Models should be Sound

Formally Verified Platforms

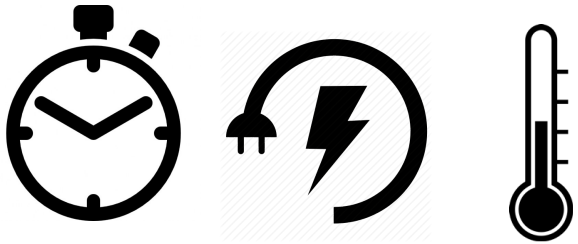
seL4
Security. Performance. Proof.

Microsoft Hyper-V

INTEGRITY

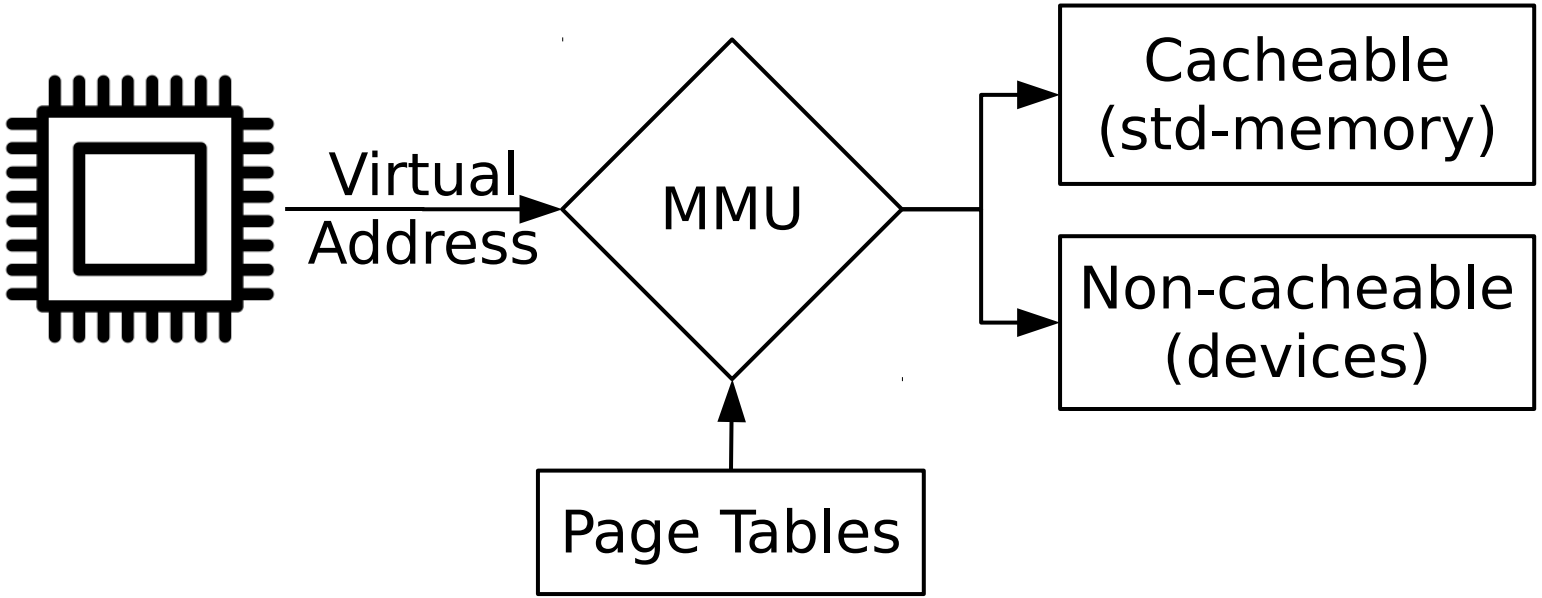
PROSPER

Caches Excluded from the analysis



Models should be Sound

Storage Channels can invalidate results



Incoherent Cache Behaviors

Mismatched cacheability attributes

Mismatched cacheability attributes

do not do this

Mismatched cacheability attributes

Please, do not do this

Mismatched cacheability attributes

Please, do not do this

Incoherent Cache Behaviors

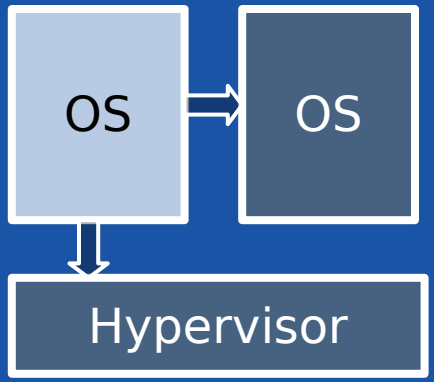
Mismatched cacheability attributes

Please, do not do this

Incoherent Cache Behaviors

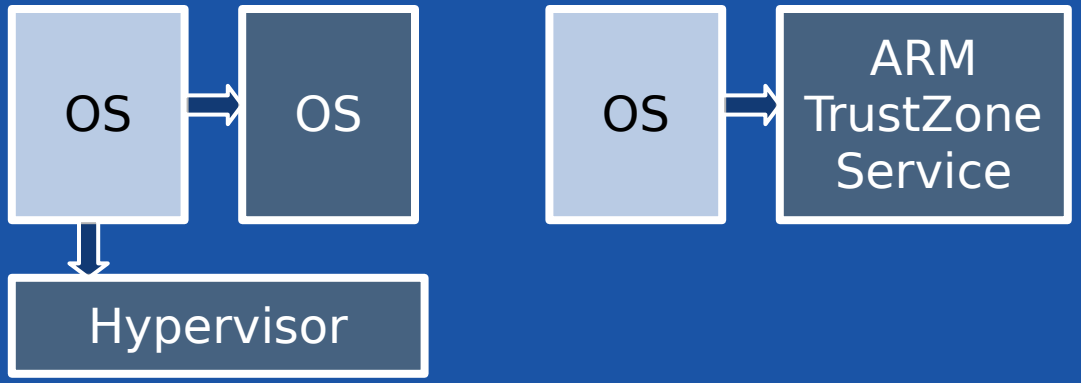
ARM-terminology: **unexpected cache hit**

if the data cache reports a hit on a memory location that is marked as non-cacheable, the cache might access the memory disregarding such hit.

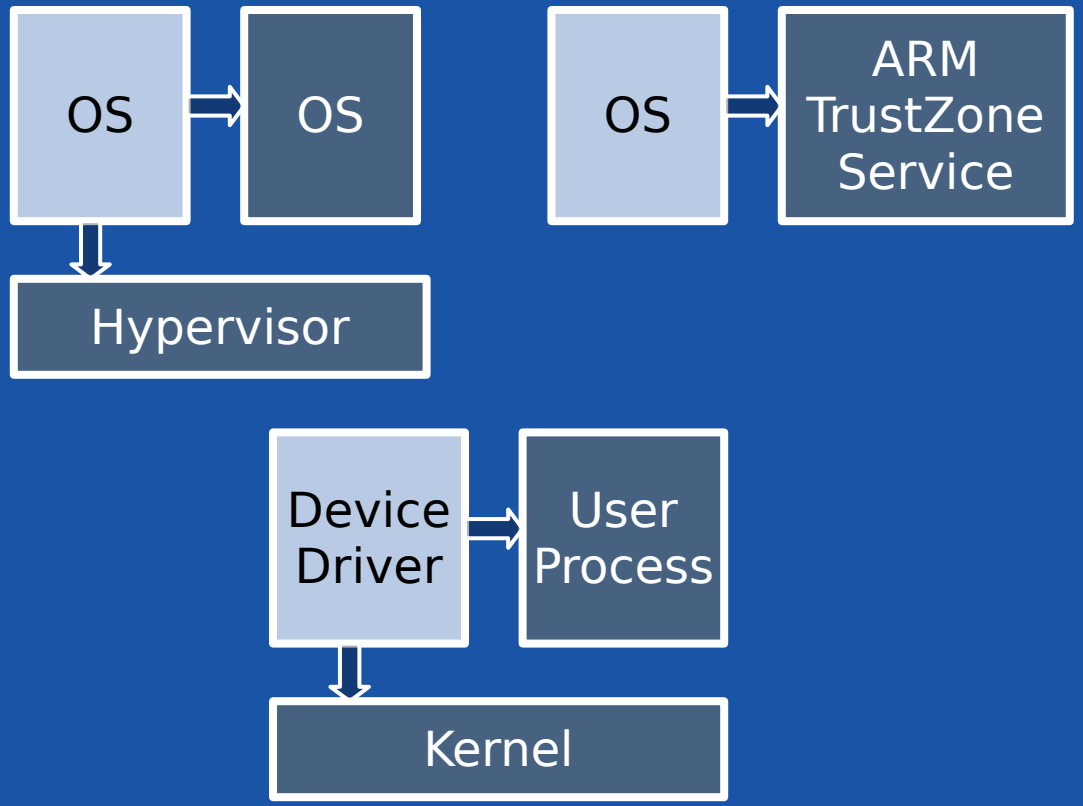


Scenarios

Scenarios



Scenarios

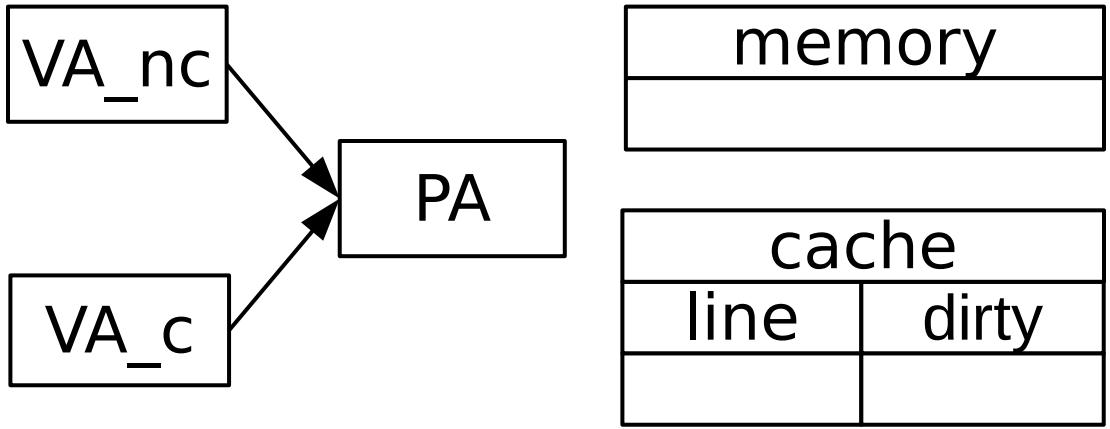

OS
OS
Hypervisor
OS
ARM TrustZone Service
Device Driver
User Process
Kernel

Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

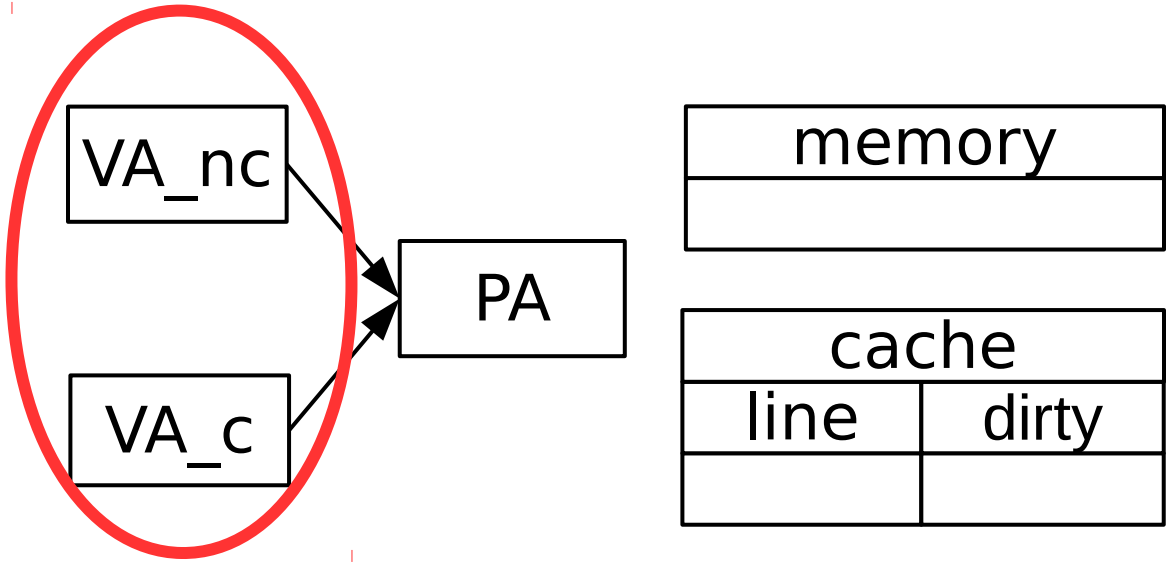


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

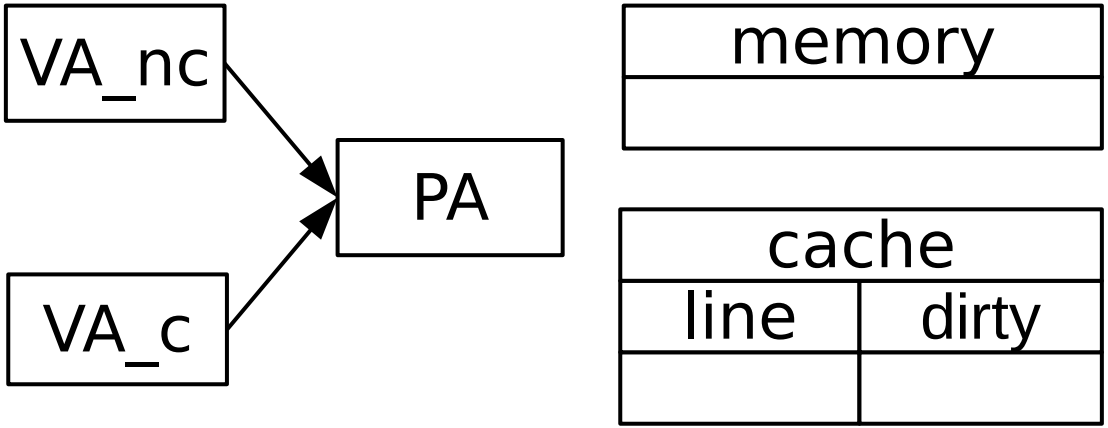


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

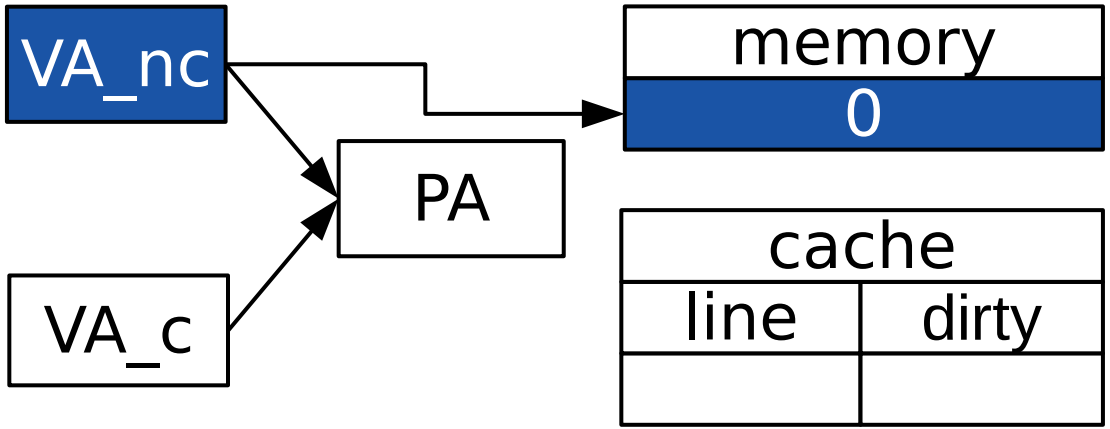


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

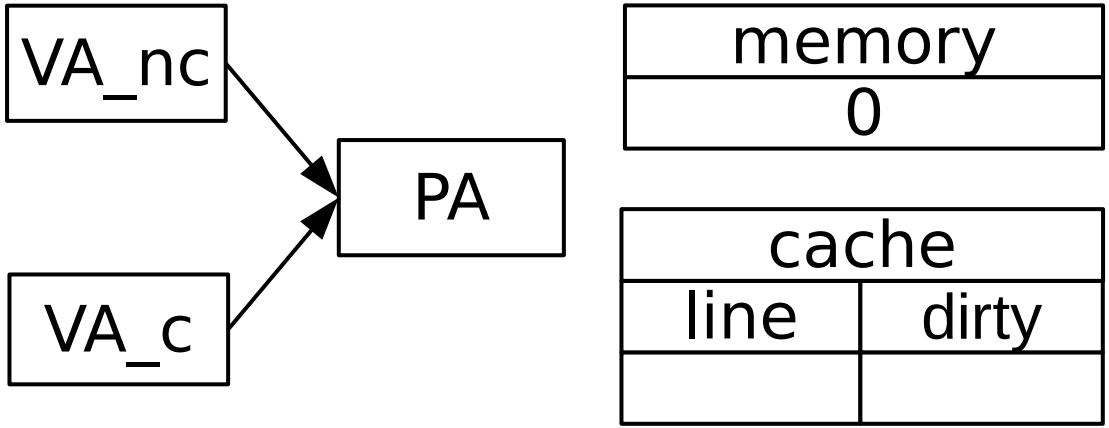


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

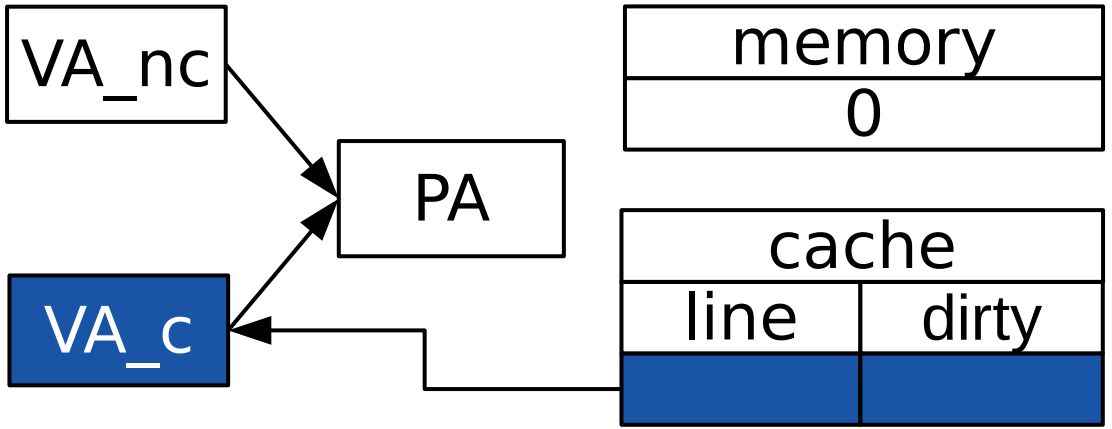


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

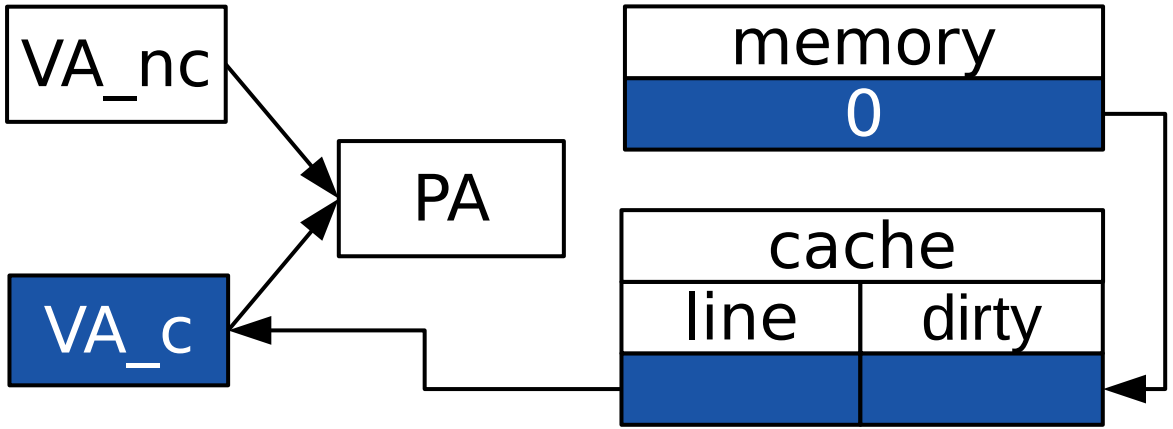


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

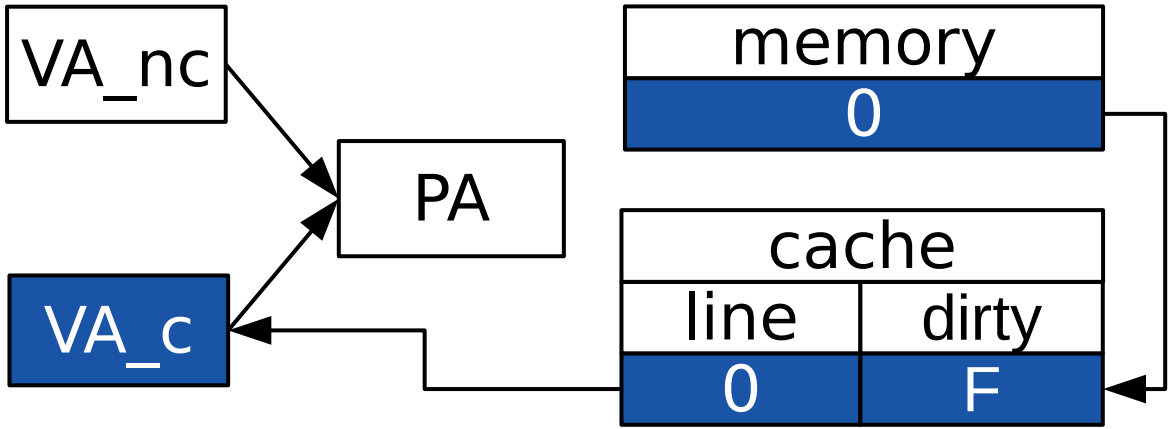


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

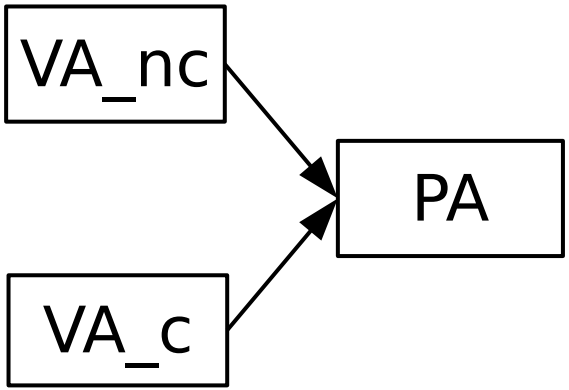


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```



memory
0

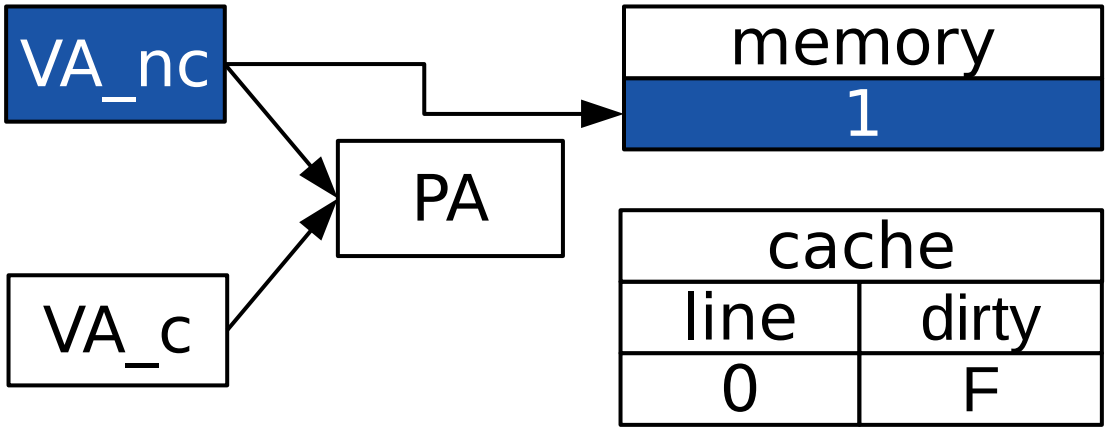
cache	
line	dirty
0	F

Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

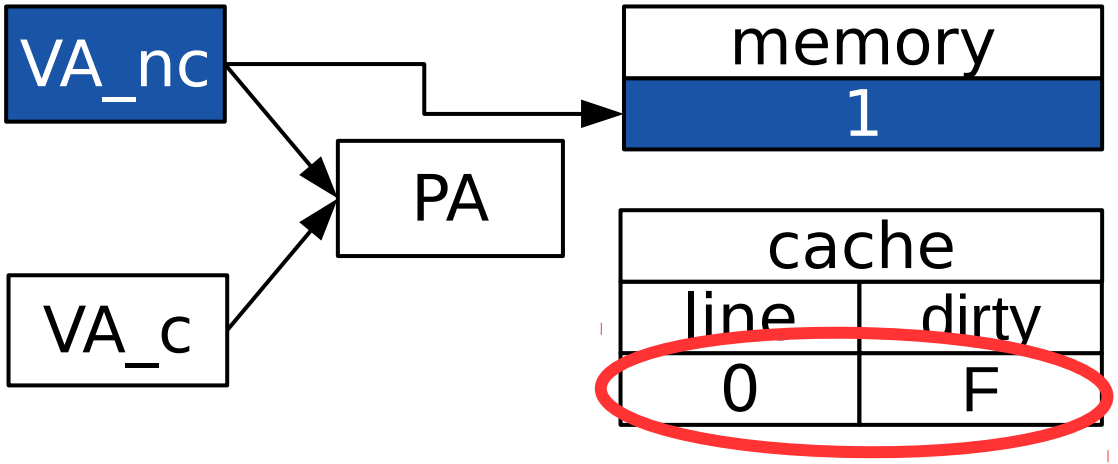


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

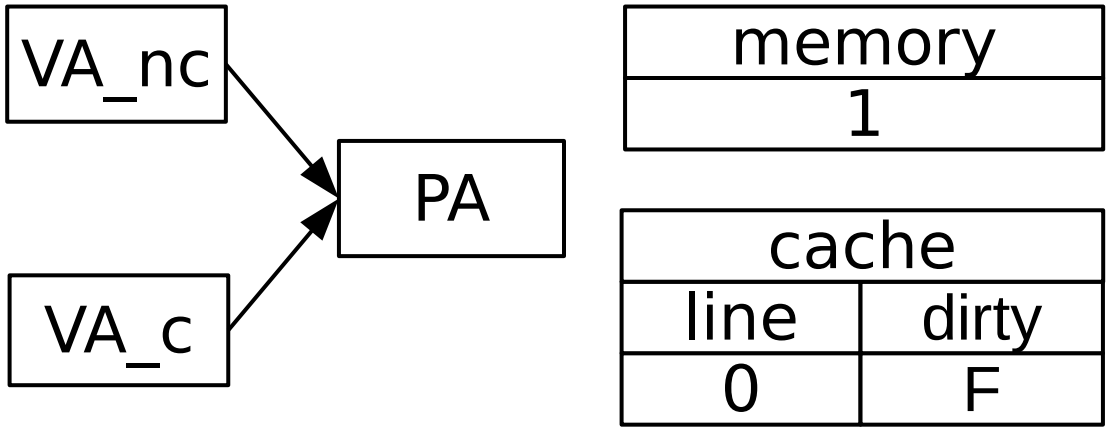


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

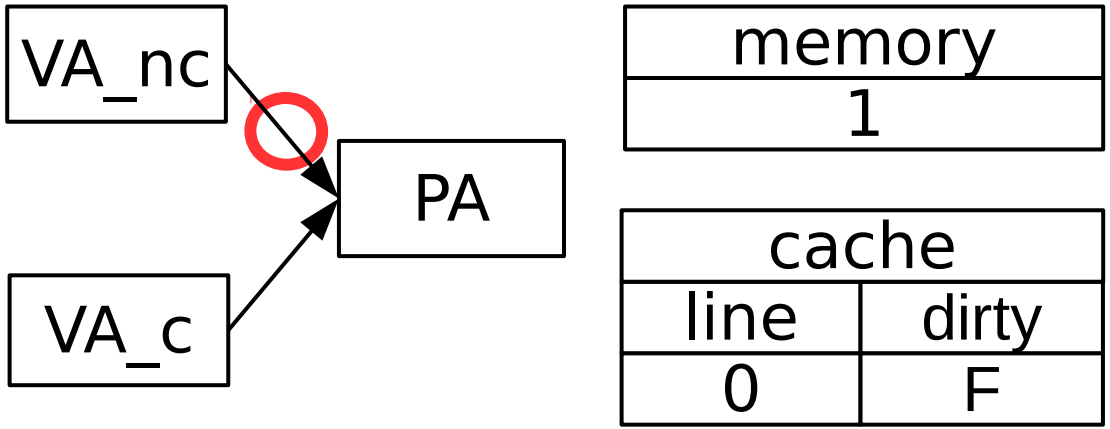


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

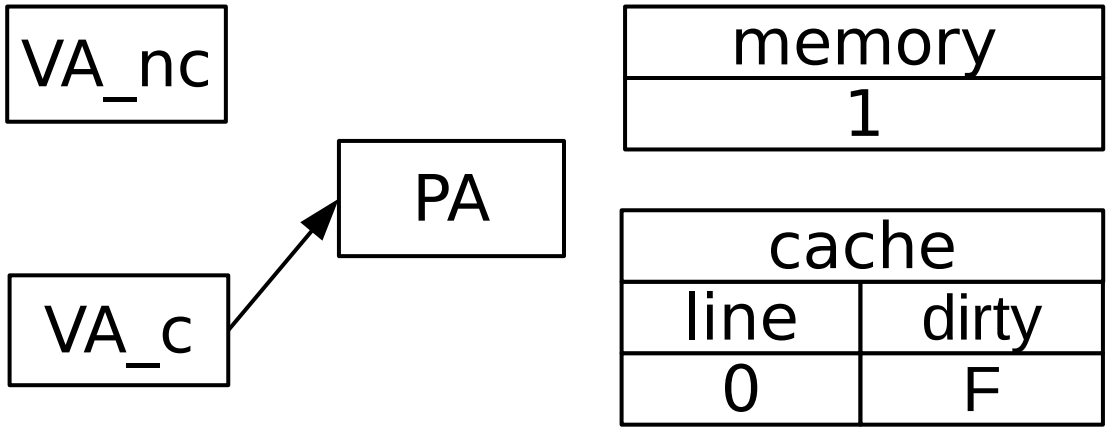


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

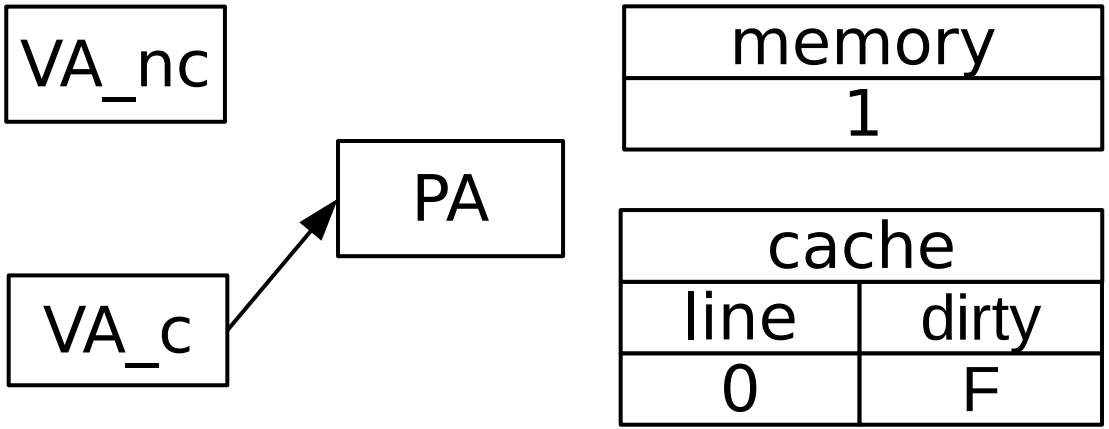


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

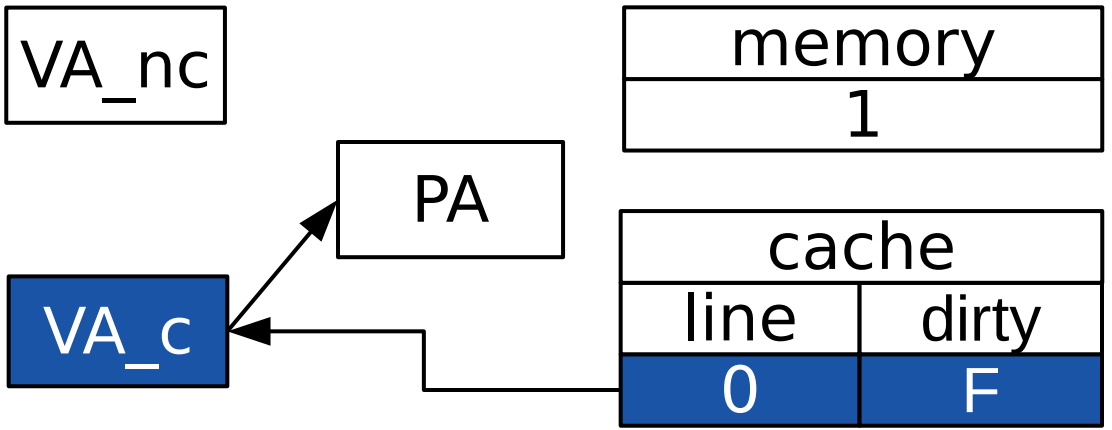


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

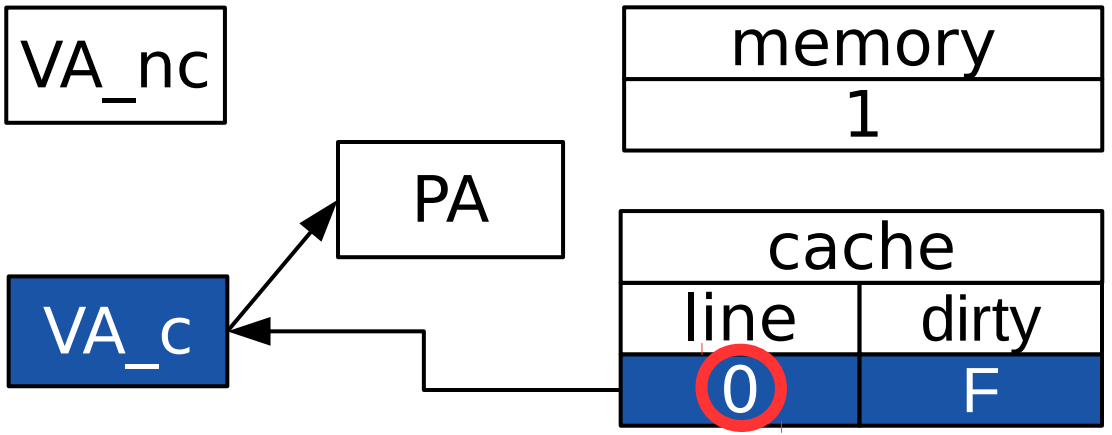


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

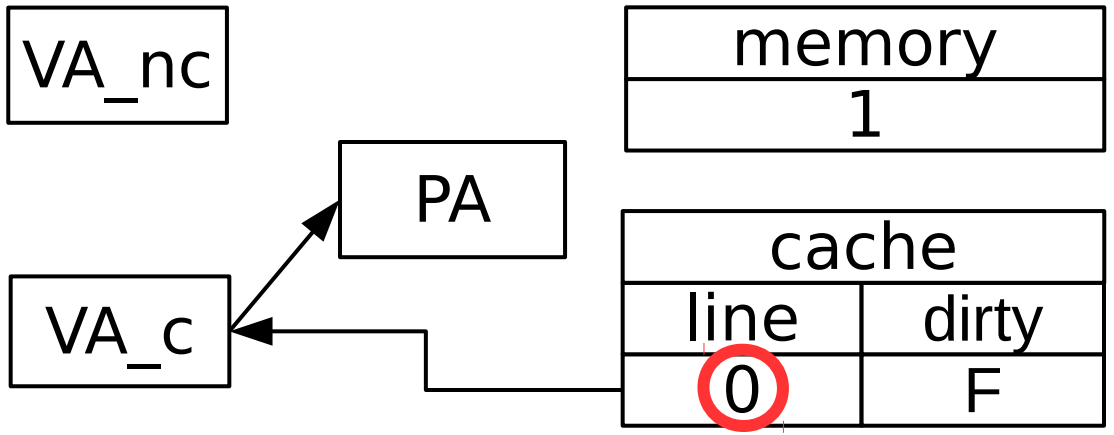


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

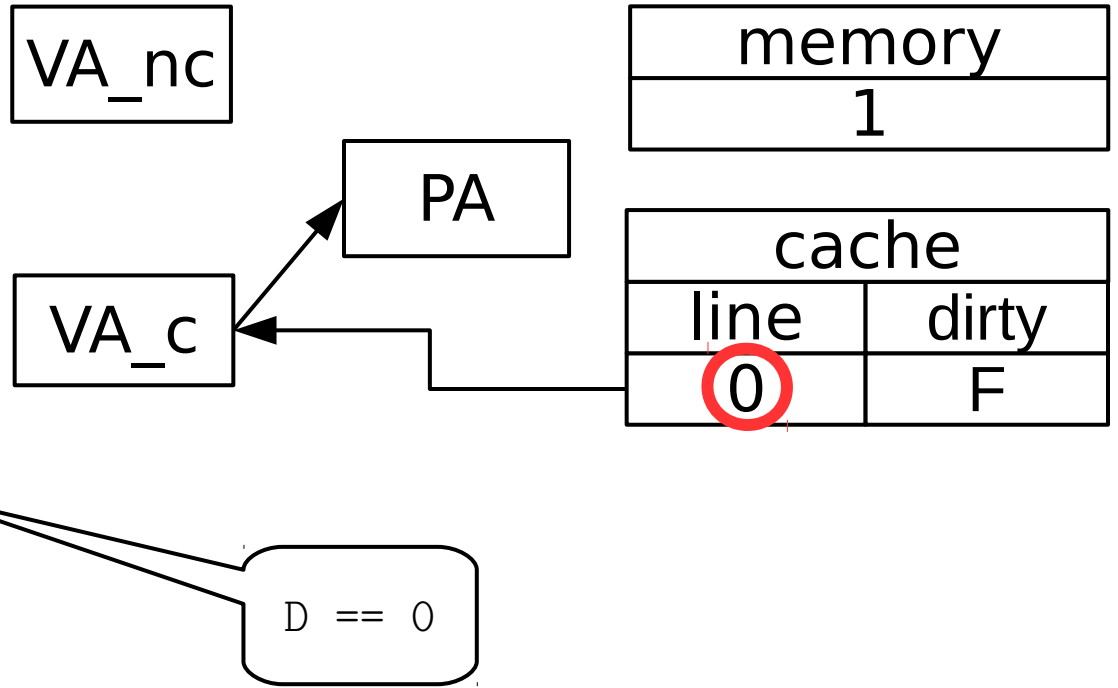


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

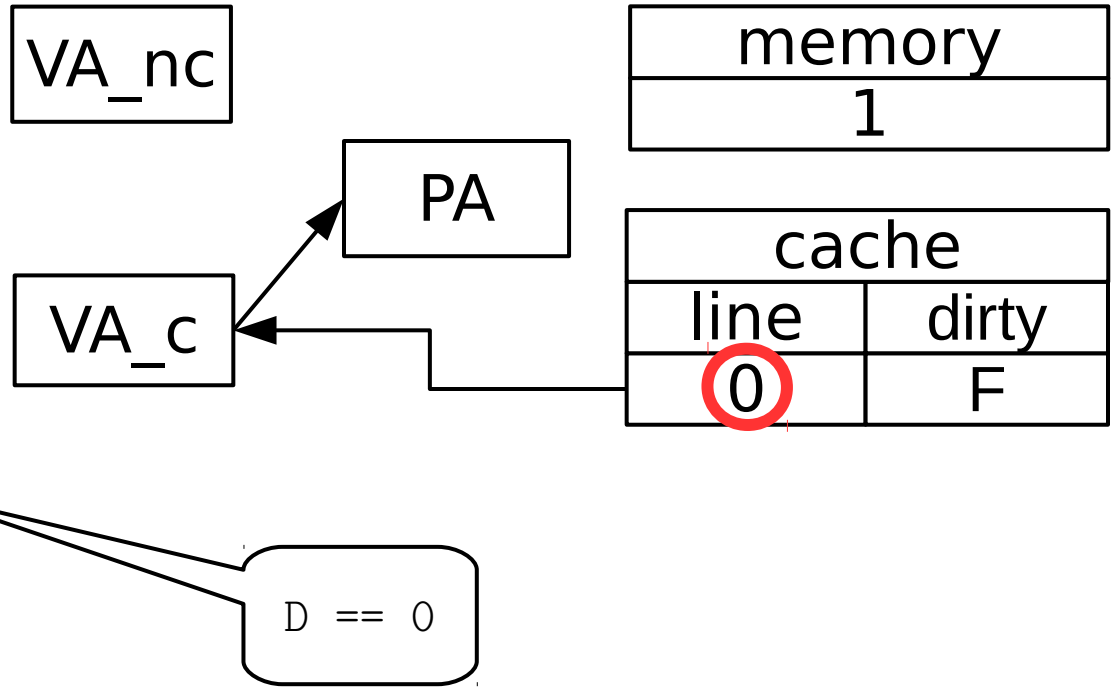


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

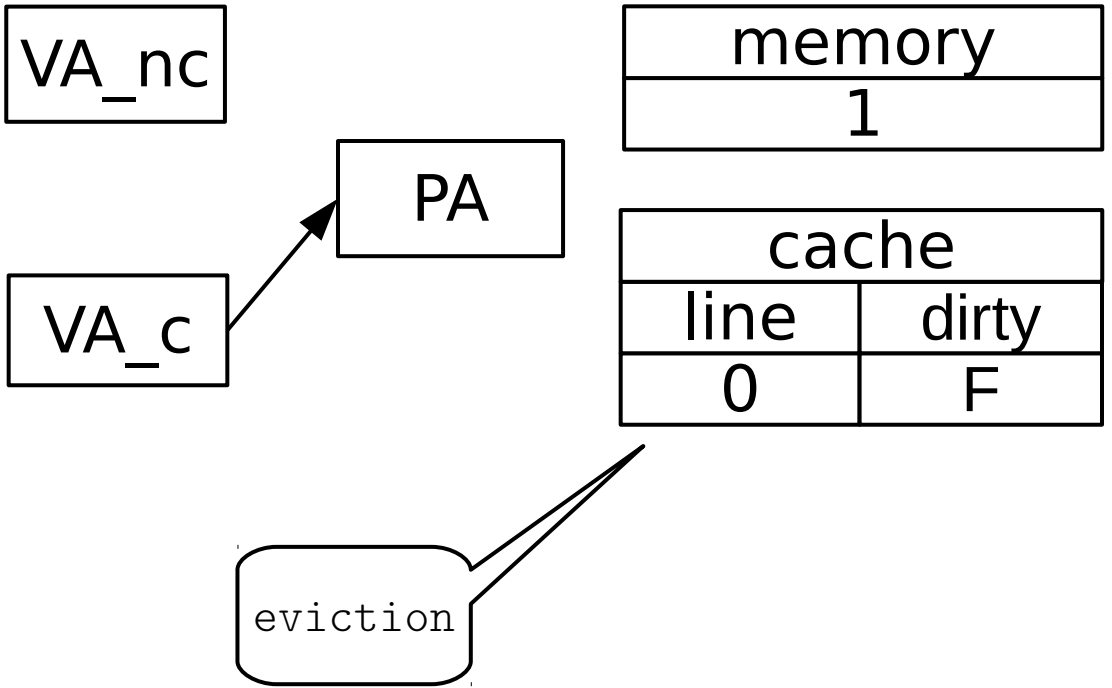


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

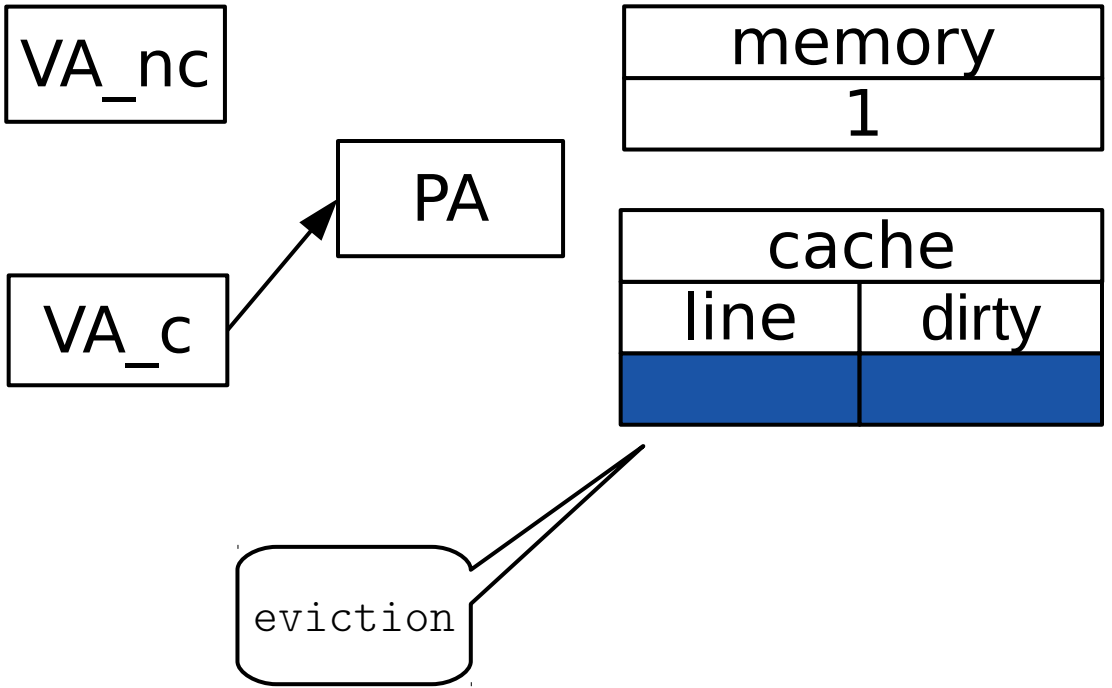


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

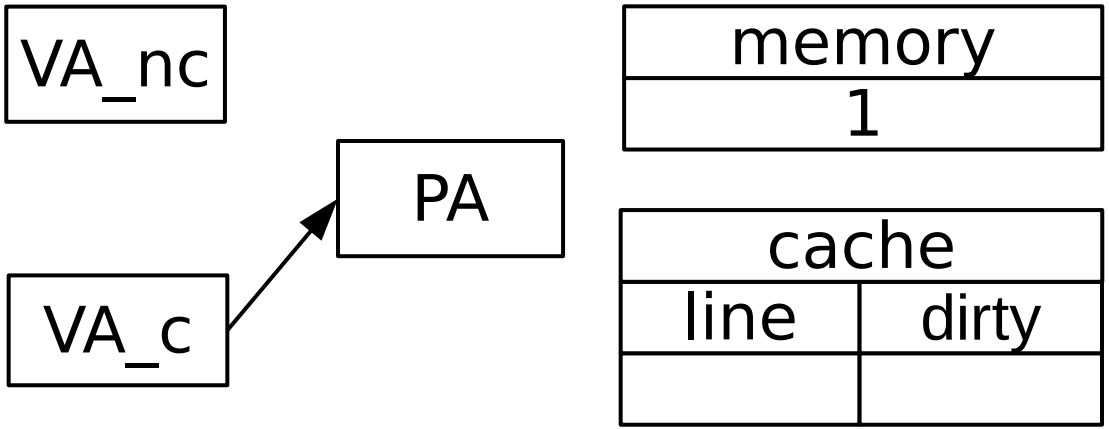


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

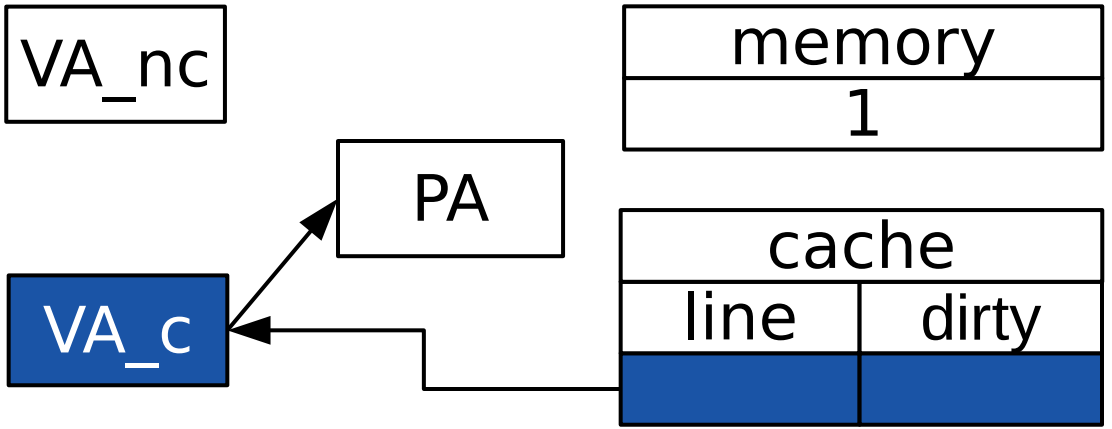


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

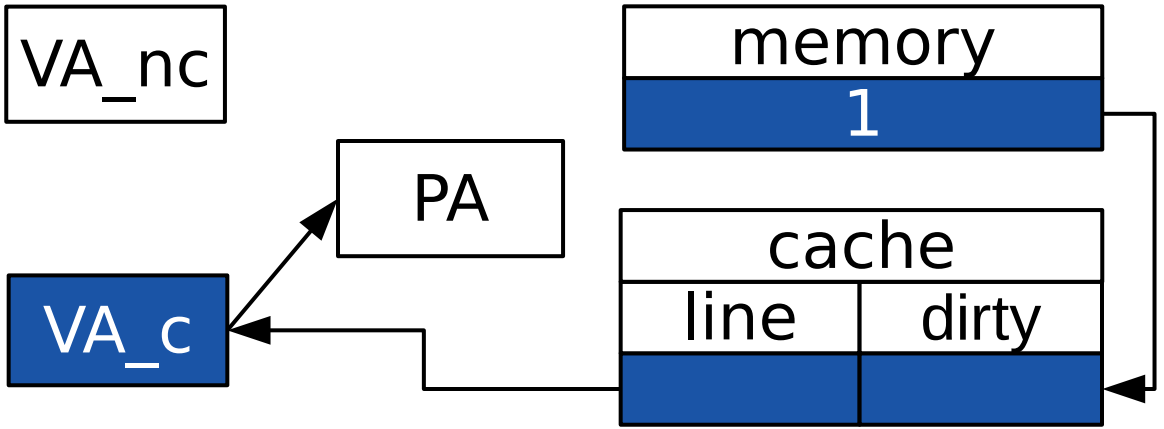


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

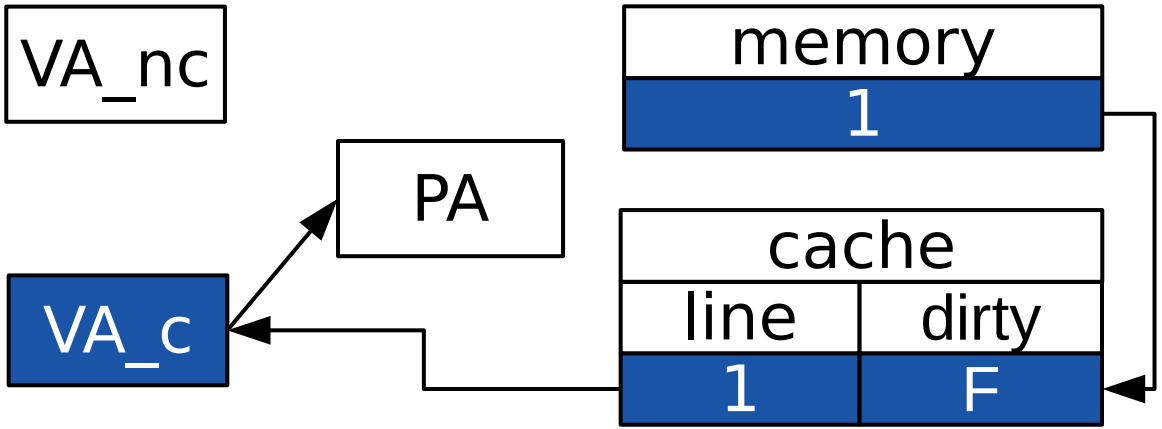


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```

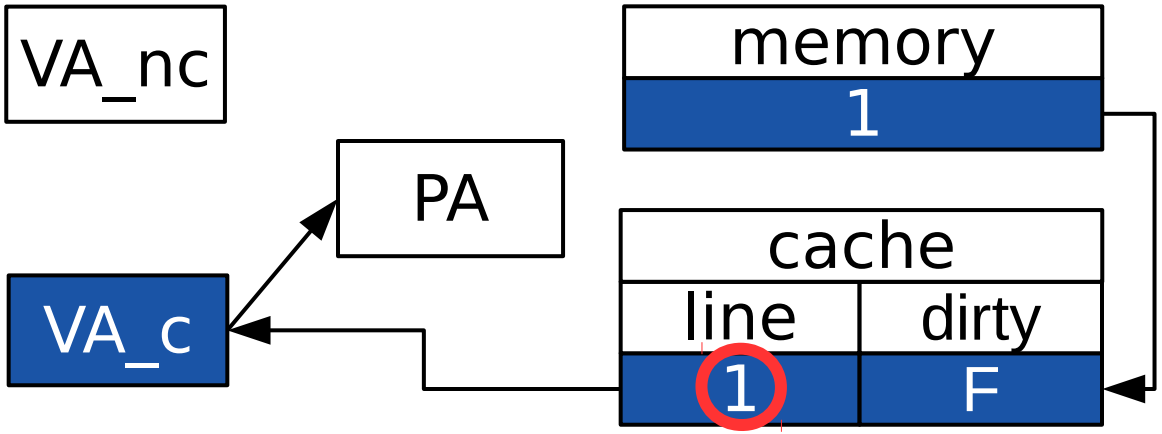


Attacker

```
write(VA_nc, 0)
…
write(VA_nc, 1)
free(VA_nc)
```

Victim

```
D = access(VA_c)
…
D = access(VA_c)
if not policy(D)
   Reject()
…
use(VA_c)
```



Storage channels

Integrity threat

- Transfer of memory ownership
- Time Of Check To Time Of Use attacks
- No need of
  - simultaneous double mapping
  - concurrency

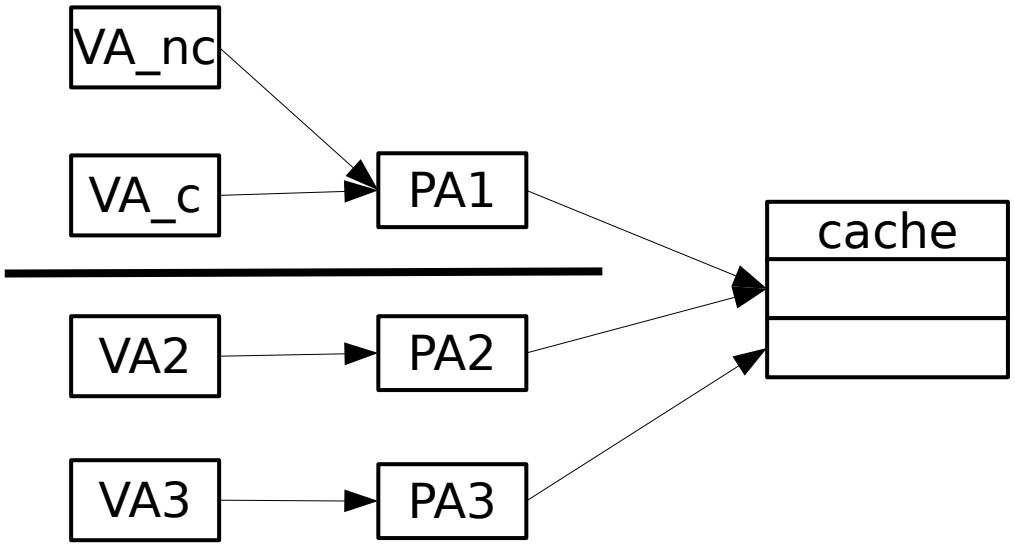
Natural preys: reference monitors

Attacker

```
invalidate(VA_c)
write(VA_nc, 0)
D = read(VA_c)
write(VA_nc, 1)
call victim
D = read(VA_c)
```

Victim

```
if secret
   access(VA2)
else
   access(VA3)
```



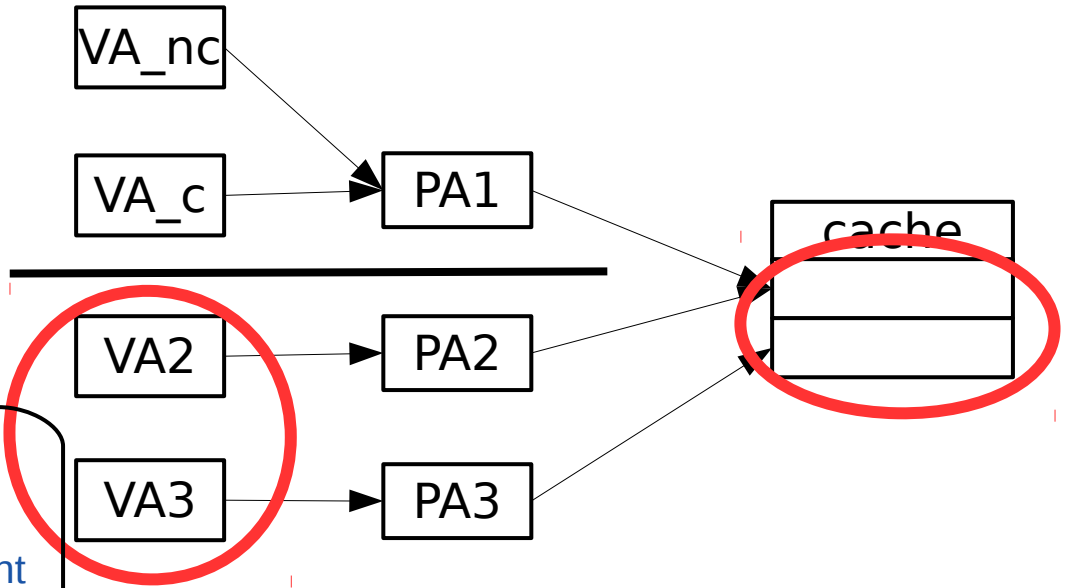
Attacker

```
invalidate(VA_c)
write(VA_nc, 0)
D = read(VA_c)
write(VA_nc, 1)
call victim
D = read(VA_c)
```

Victim

```
if secret
   access(VA2)
else
   access(VA3)
```

Accessed cache line is secret-dependent

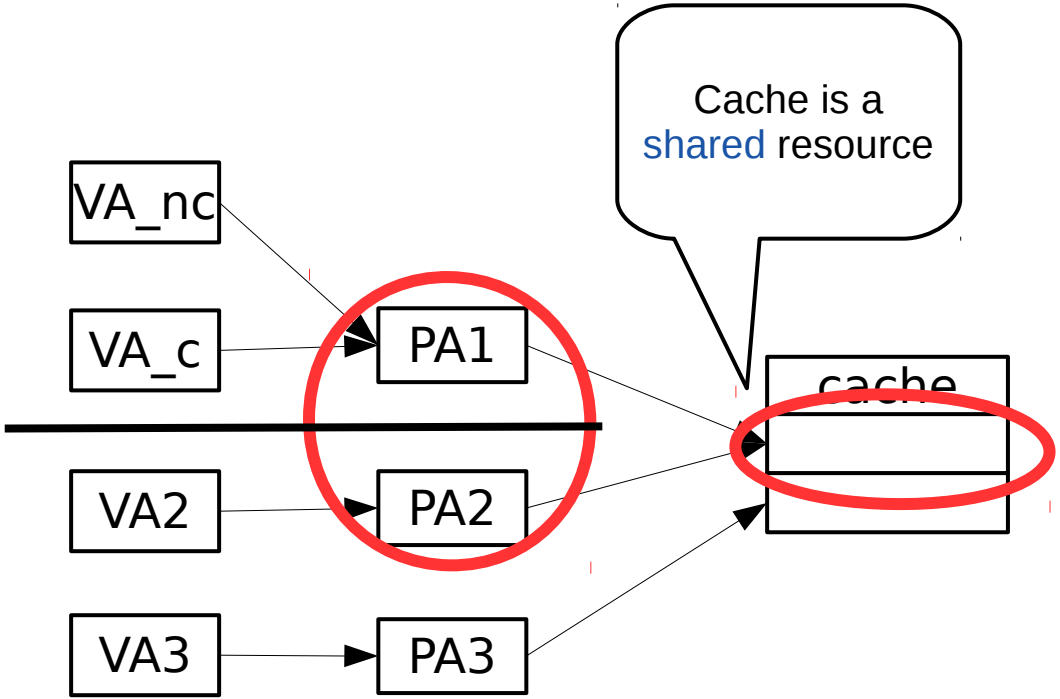


Attacker

```
invalidate(VA_c)
write(VA_nc, 0)
D = read(VA_c)
write(VA_nc, 1)
call victim
D = read(VA_c)
```

Victim

```
if secret
   access(VA2)
else
   access(VA3)
```

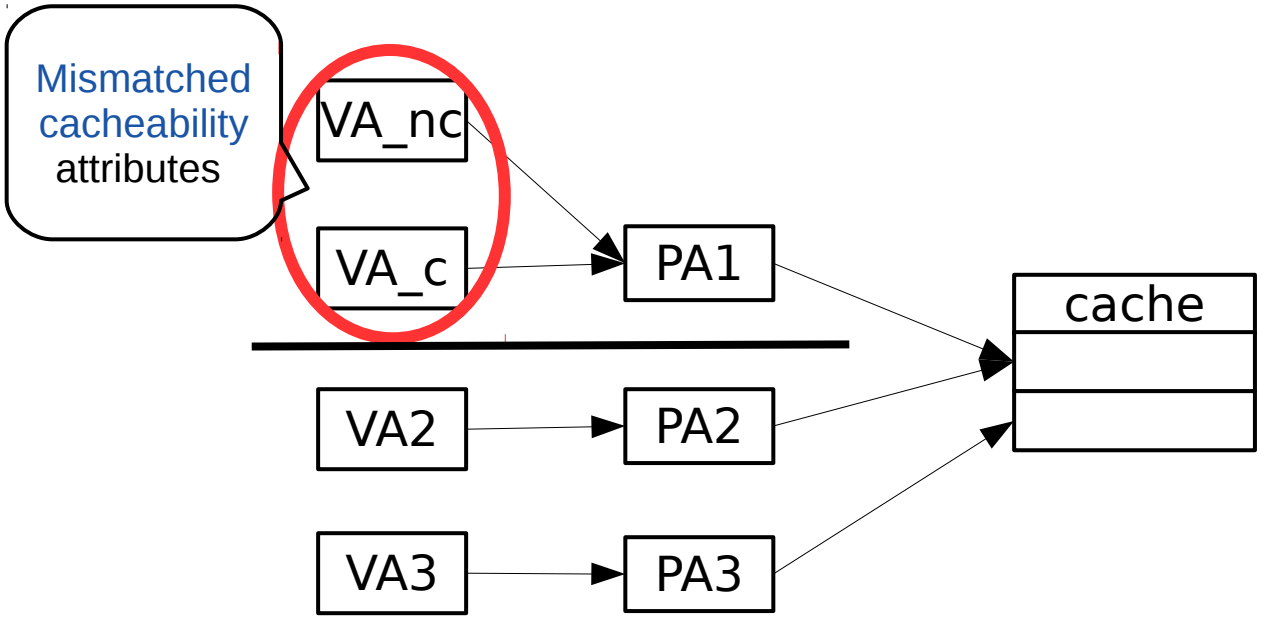


Attacker

```
invalidate(VA_c)
write(VA_nc, 0)
D = read(VA_c)
write(VA_nc, 1)
call victim
D = read(VA_c)
```

Victim

```
if secret
   access(VA2)
else
   access(VA3)
```



Storage channels

Integrity threat

- Transfer of memory ownership
- Time Of Check To Time Of Use
- No need of
  - simultaneous double mapping
  - concurrency

Natural preys: reference monitors

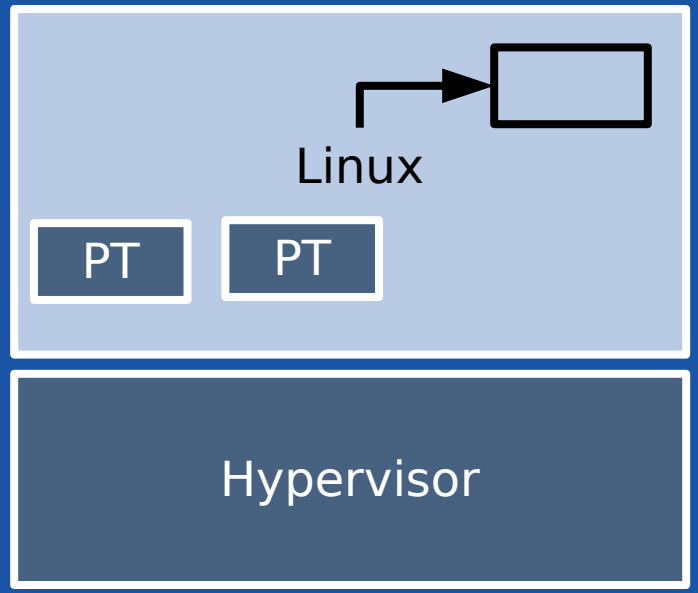
Confidentiality threat

- Access driven attacks
- No external measure needed
- Difficult to counter-measure at probing time

Natural preys: look-up tables

Paravirtualizing Hypervisor

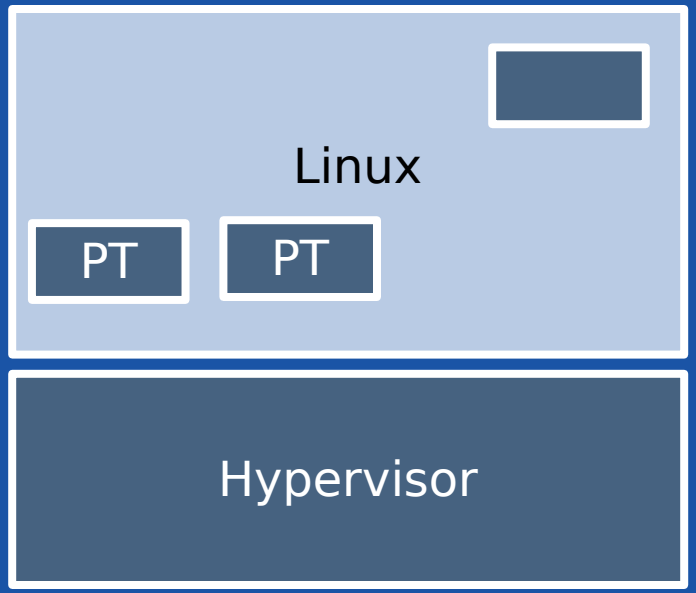
- Beagleboard



Linux prepares a PT

Paravirtualizing Hypervisor

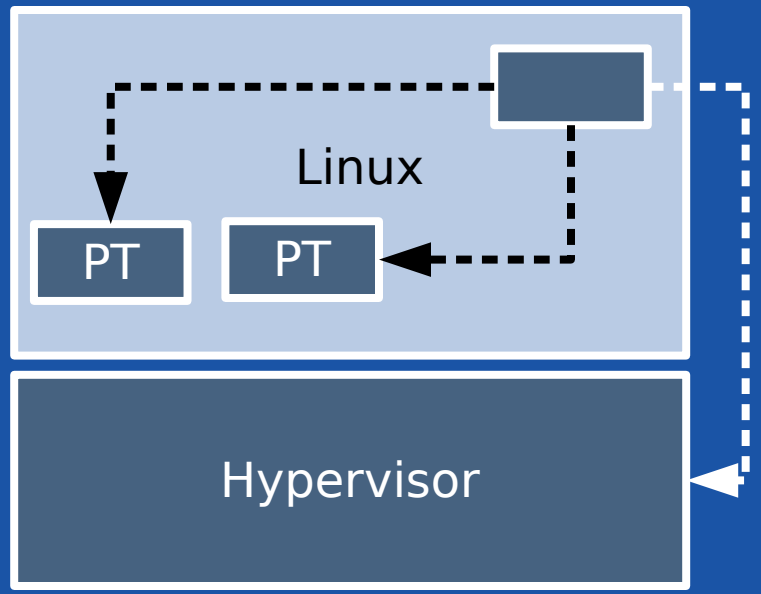
- Beagleboard



Hypervisor makes region read-only

Paravirtualizing Hypervisor

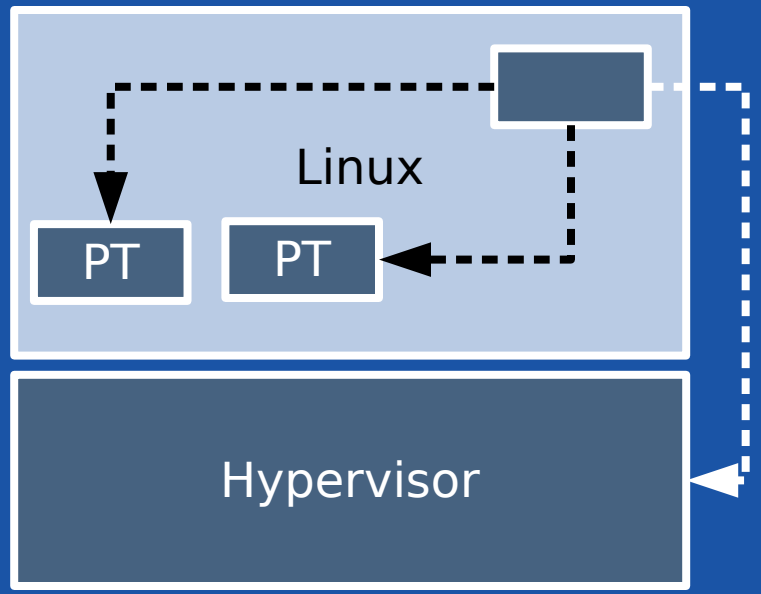
- Beagleboard



Hypervisor validates content

Paravirtualizing Hypervisor

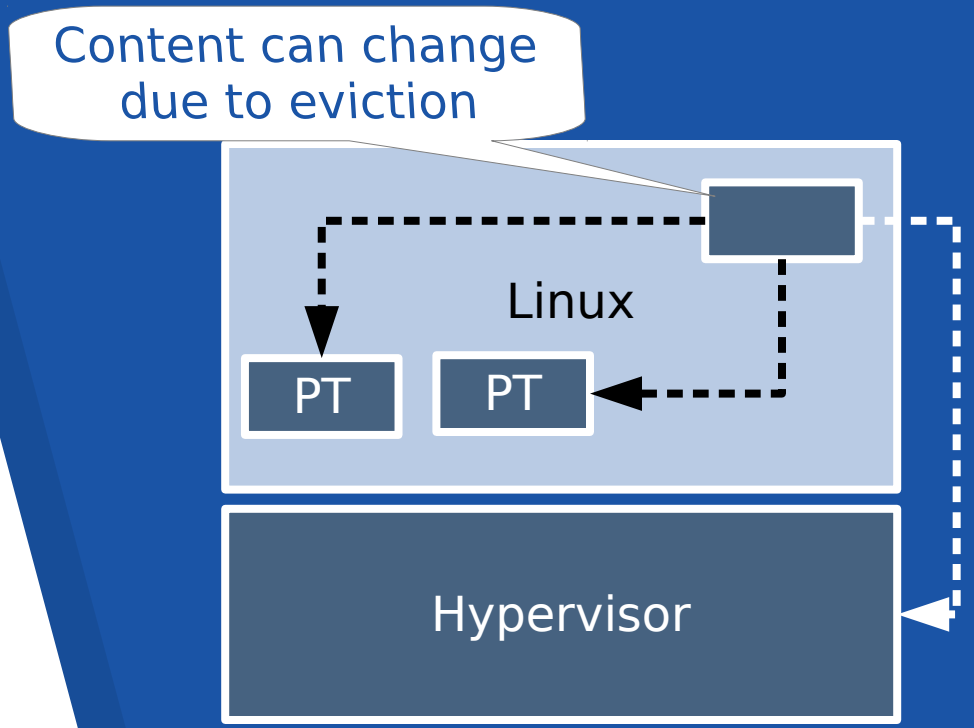
- Beagleboard



Hypervisor activates PT

Paravirtualizing Hypervisor

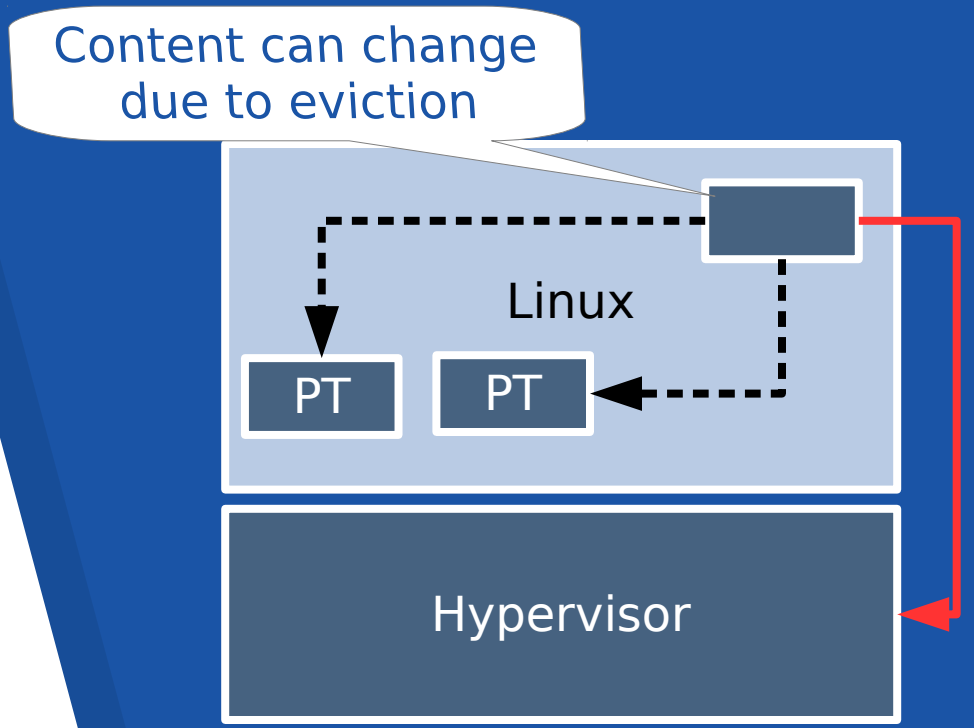
- Beagleboard



Hypervisor activates PT

Paravirtualizing Hypervisor

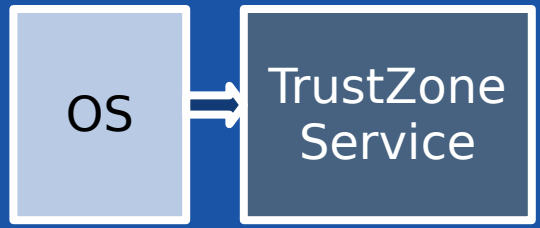
- Beagleboard
- Linux takes complete control



Hypervisor activates PT

AES Cryptoservice

- Raspberry PI 2
- 128-bit key extracted after 850 encryptions



Vulnerability:

c[j]=Kn[j] xor T4[s[j]]

Observable

Inferred

Countermeasures

Integrity threat
guarantee memory coherency

- cache flushes
  (8x overhead)
- selective eviction
  (0.2x overhead)

Countermeasures

Integrity threat
guarantee memory coherency

- cache flushes
  (8x overhead)
- selective eviction
  (0.2x overhead)

Confidentiality threat
standard timing approaches

- secret-independent accesses
  (5x overhead)
- no cache for secret accesses
  (6x overhead)

Countermeasures

Integrity threat
guarantee memory coherency

- cache flushes
  (8x overhead)
- selective eviction
  (0.2x overhead)

Vector specific

- avoid uncacheable aliases
  (0.15x overhead)

Confidentiality threat
standard timing approaches

- secret-independent accesses
  (5x overhead)
- no cache for secret accesses
  (6x overhead)

Countermeasures

Integrity threat
guarantee memory coherency

- cache flushes
  (8x overhead)
- selective eviction
  (0.2x overhead)

Vector specific

- avoid uncacheable aliases
  (0.15x overhead)

Confidentiality threat
standard timing approaches

- secret-independent accesses
  (5x overhead)
- no cache for secret accesses
  (6x overhead)

HW Countermeasures

- do not disregard
  unexpected cache hit

Concluding **remarks**

Confidentiality threat using **self-modifying code**

Ongoing work

- Repair **formal verification**
- TLBs / Branch prediction / …
- Experimentation in multi-core
- Evaluating HW countermeasures

THANKS!

Any questions?

You can find me at robertog@kth.se
http://prosper.sics.se/
http://haspoc.sics.se/