29TH USENIX SECURITY SYMPOSIUM

An Off-Chip Attack on Hardware Enclaves via the Memory Bus

Dayeol Lee[1], Dongha Jung[3], Ian T. Fang[1], Chia-Che Tsai[1,2], Raluca Ada Popa[1]

[1] UC Berkeley

[2] Texas A&M University

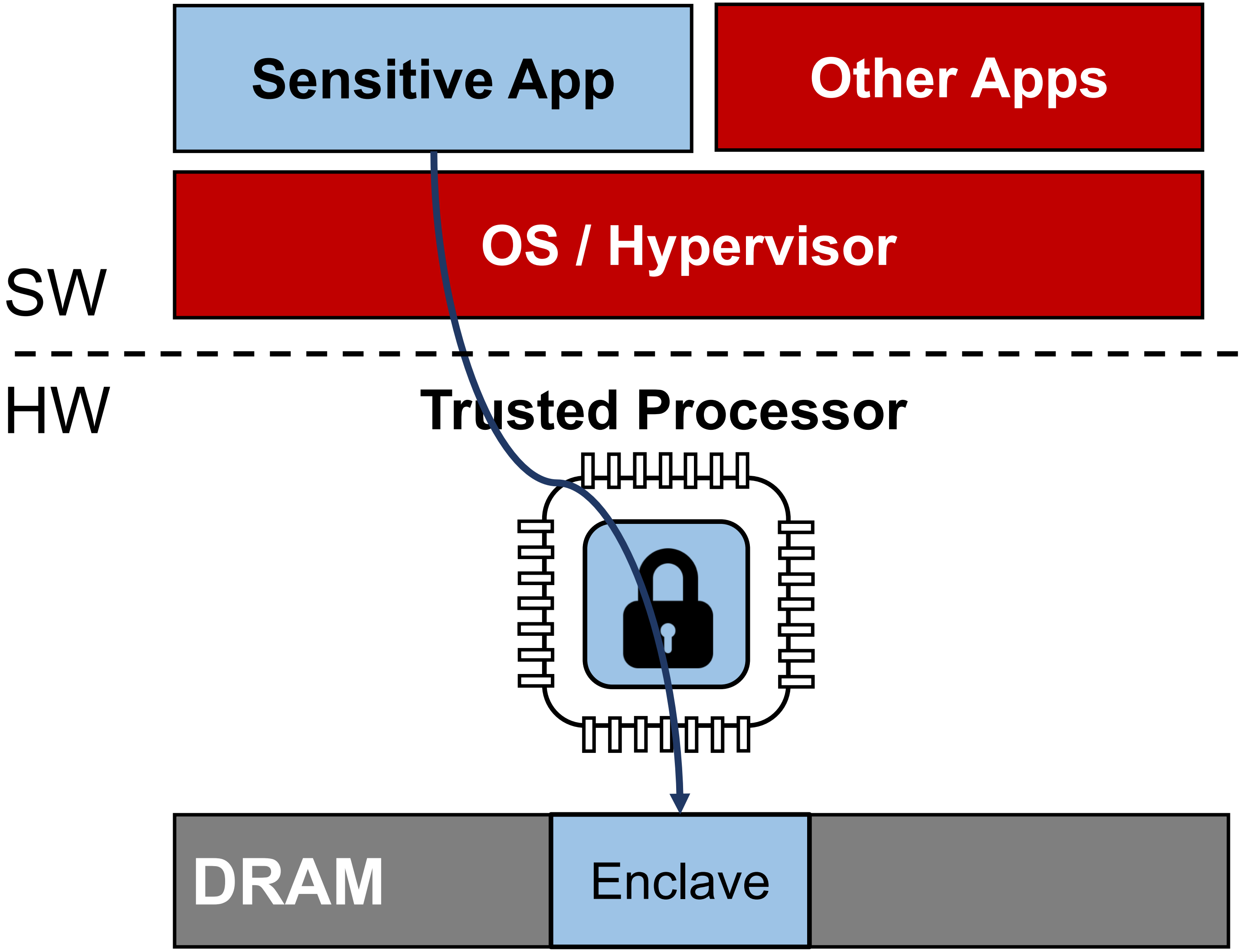
[3] SK Hynix Inc.

Berkeley | EECS
Electrical Engineering and Computer Sciences

TEXAS A&M UNIVERSITY
Department of Computer Science & Engineering

SK hynix

Trusted Execution Environments (TEEs)

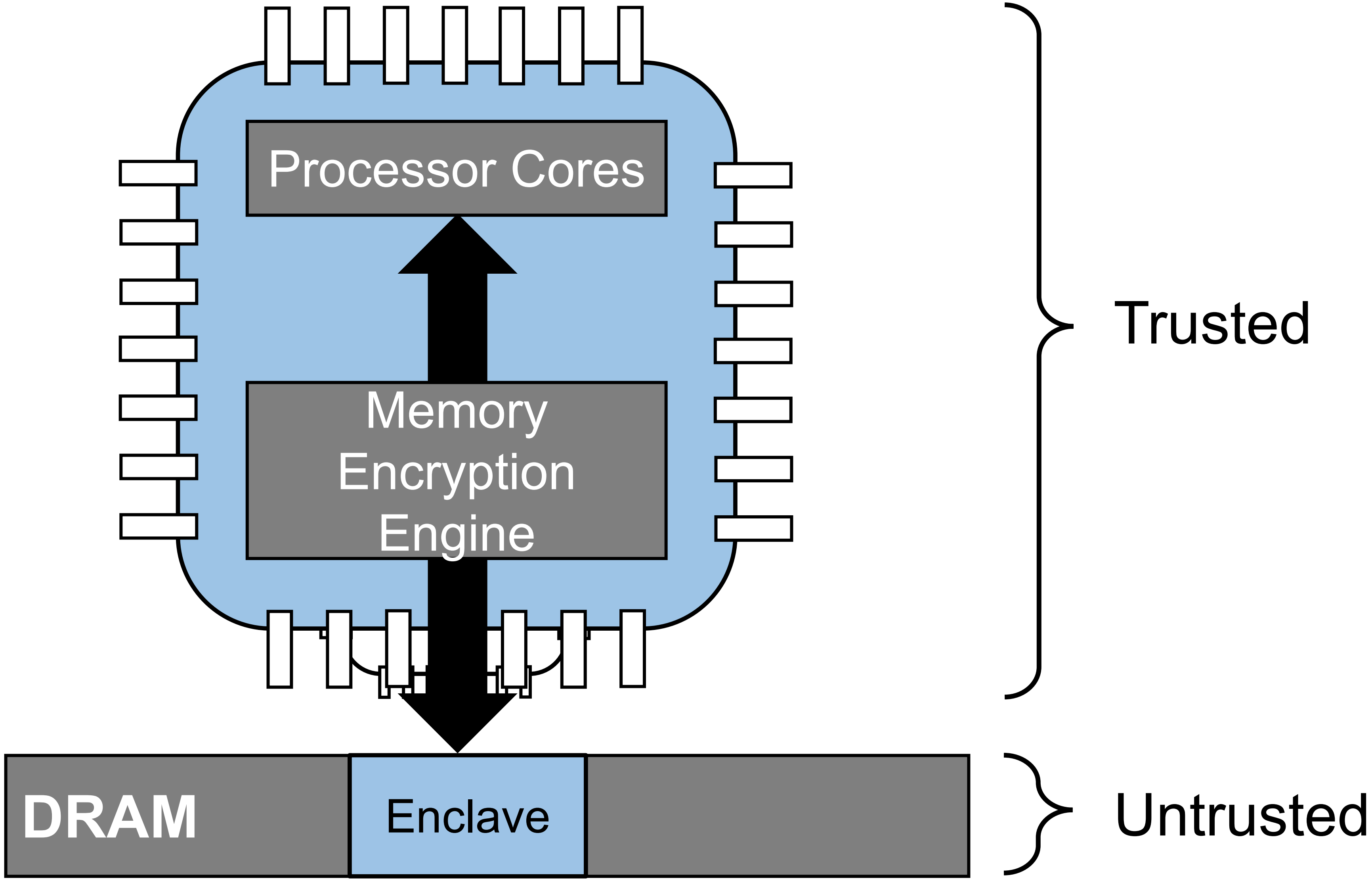


Integrity

Confidentiality

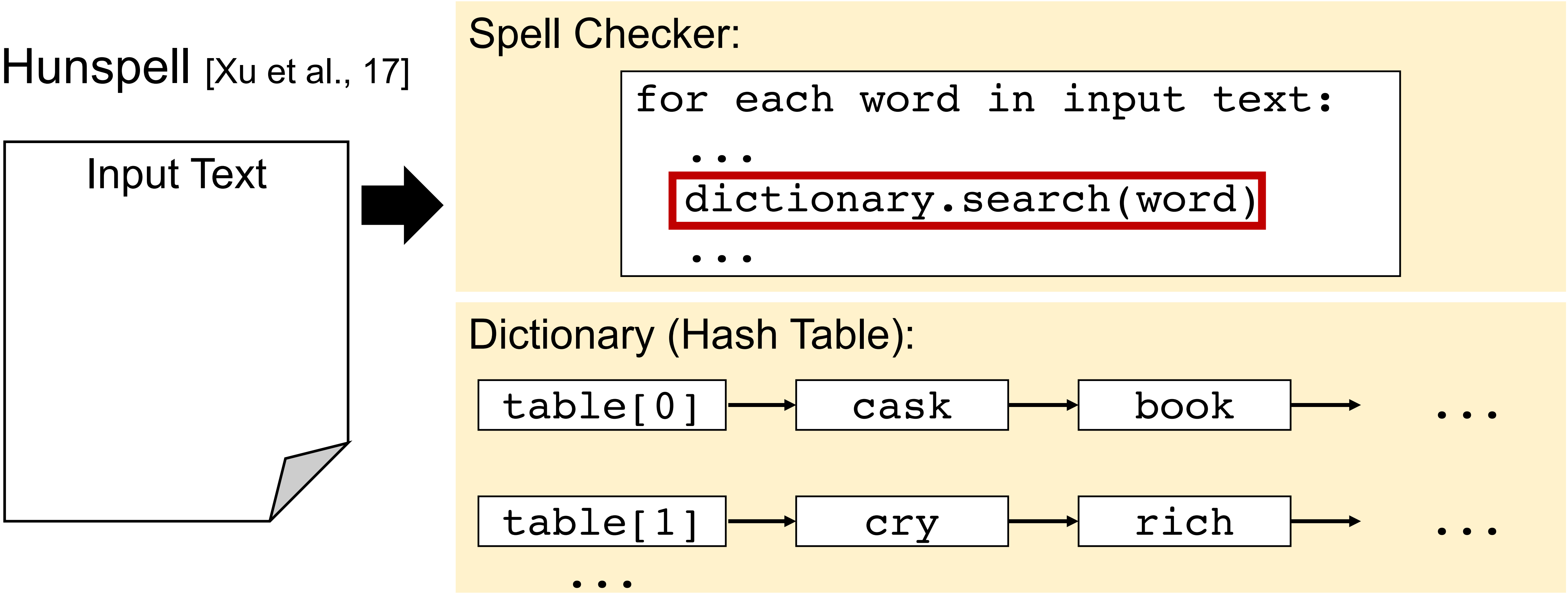
Remote Attestation

Memory Encryption of Intel SGX



Access Pattern Leakage via Side Channel

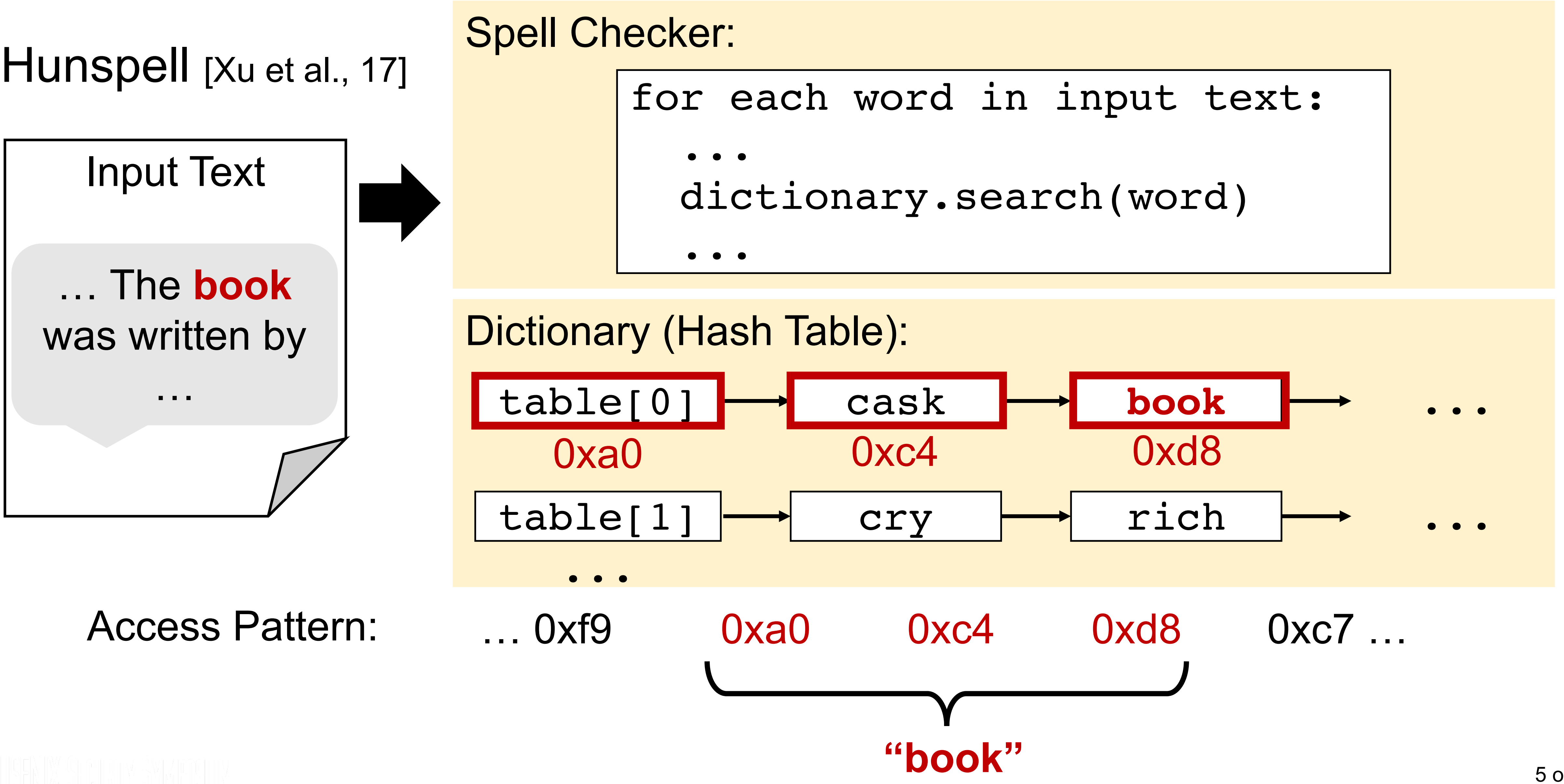
Hunspell [Xu et al., 17]



```
for each word in input text:
  ...
  dictionary.search(word)
  ...
```

Access Pattern Leakage via Side Channel

Hunspell [Xu et al., 17]



Input Text

… The **book** was written by …

Spell Checker:

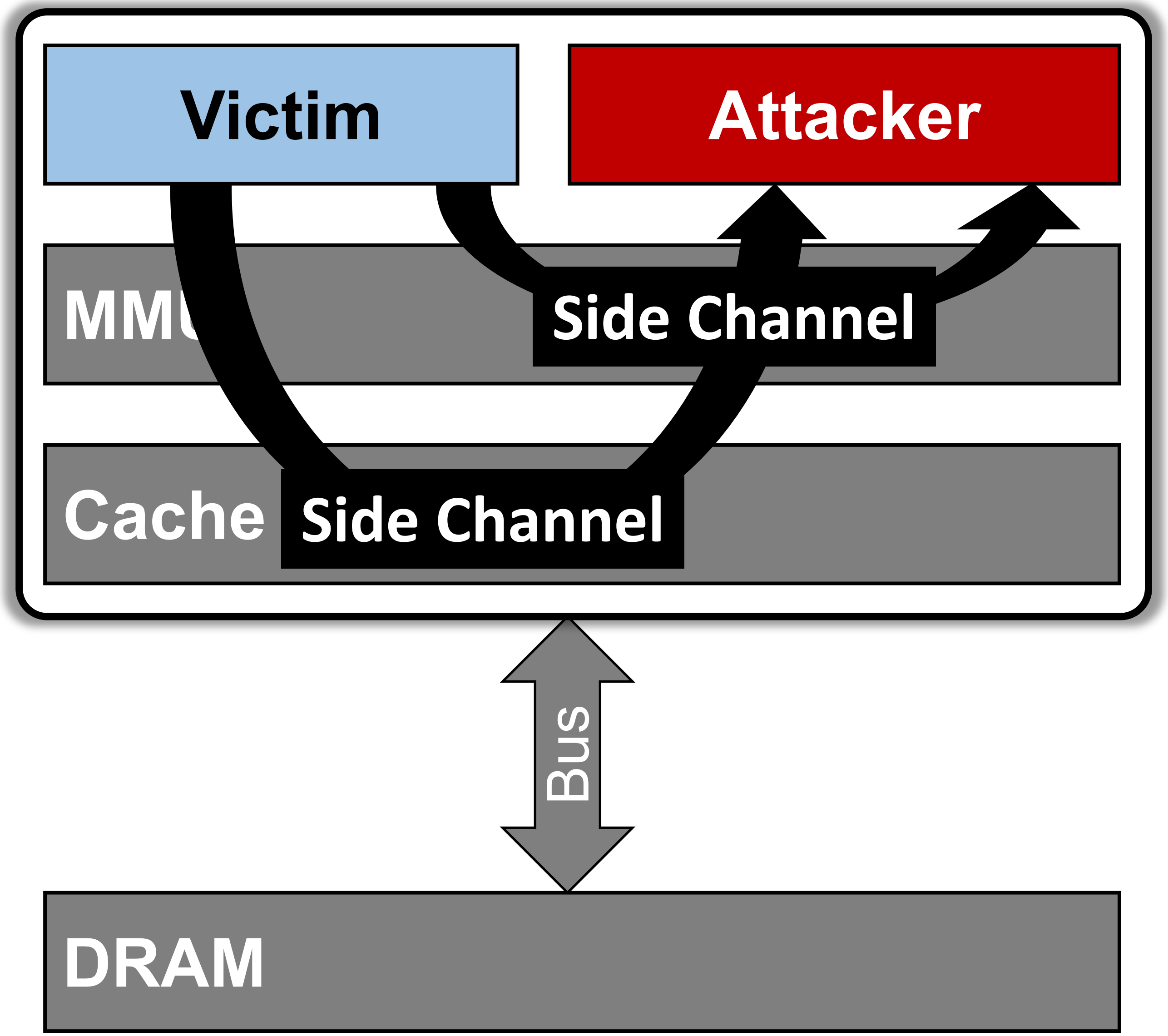
```
for each word in input text:
   ...
   dictionary.search(word)
   ...
```

Dictionary (Hash Table):

Access Pattern: … 0xf9 0xa0 0xc4 0xd8 0xc7 …

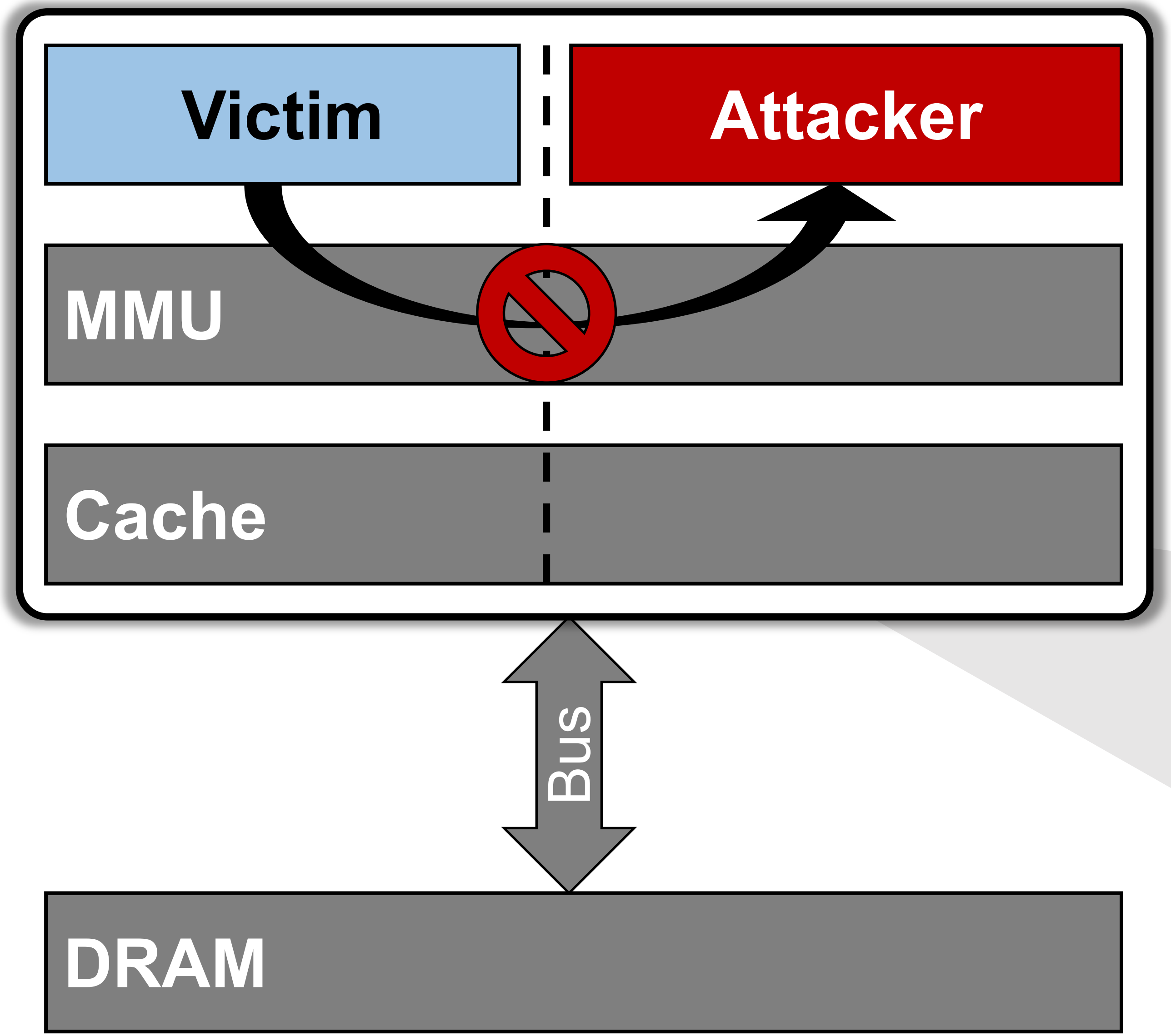
“book”

Side-Channel Attacks on SGX Enclaves



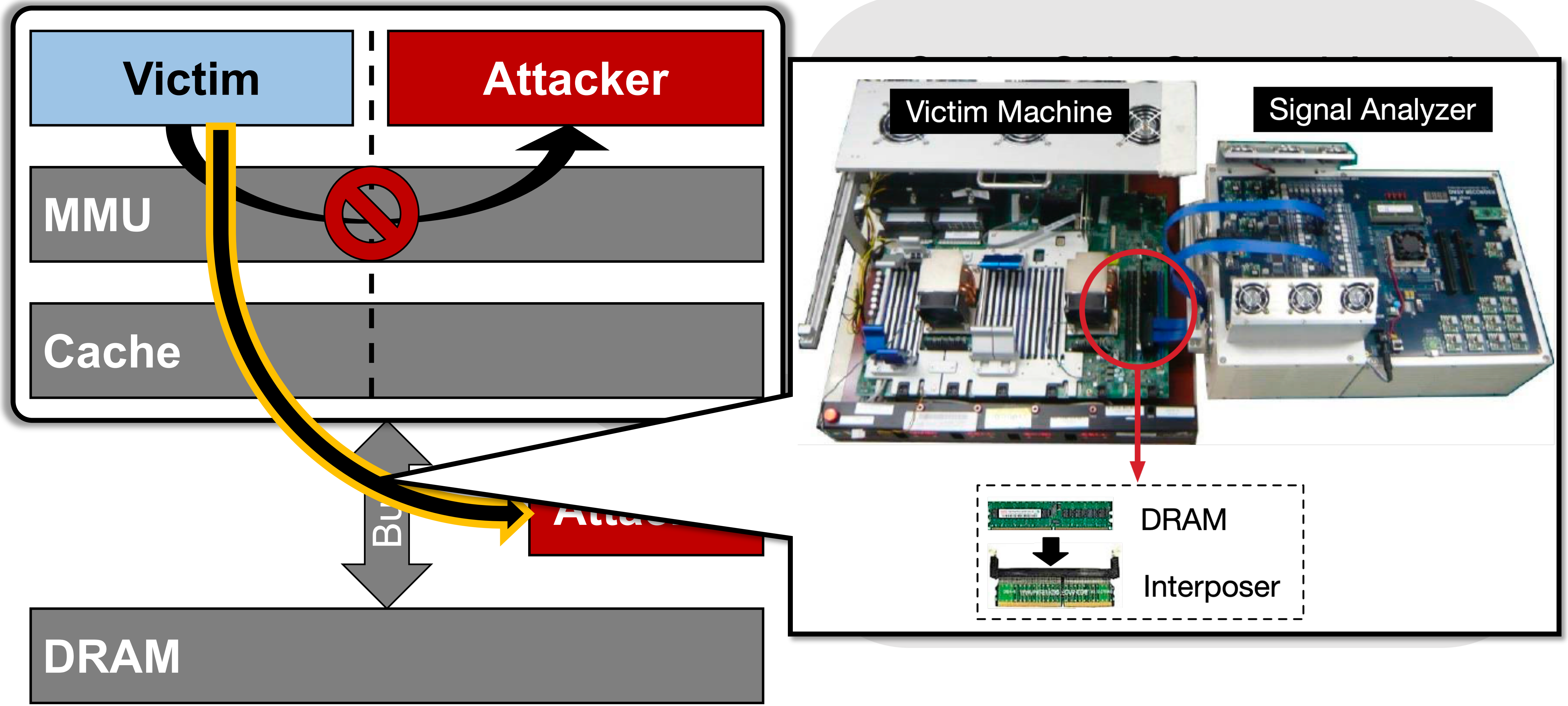
- Cache Side-Channel Attacks
  - Brasser’17, Schwarz’17, Moghimi’17, VanBulck’18
- Page Table-Based Attacks
  - Controlled-Channel'15, VanBulck’17

Side-Channel Attacks on SGX Enclaves

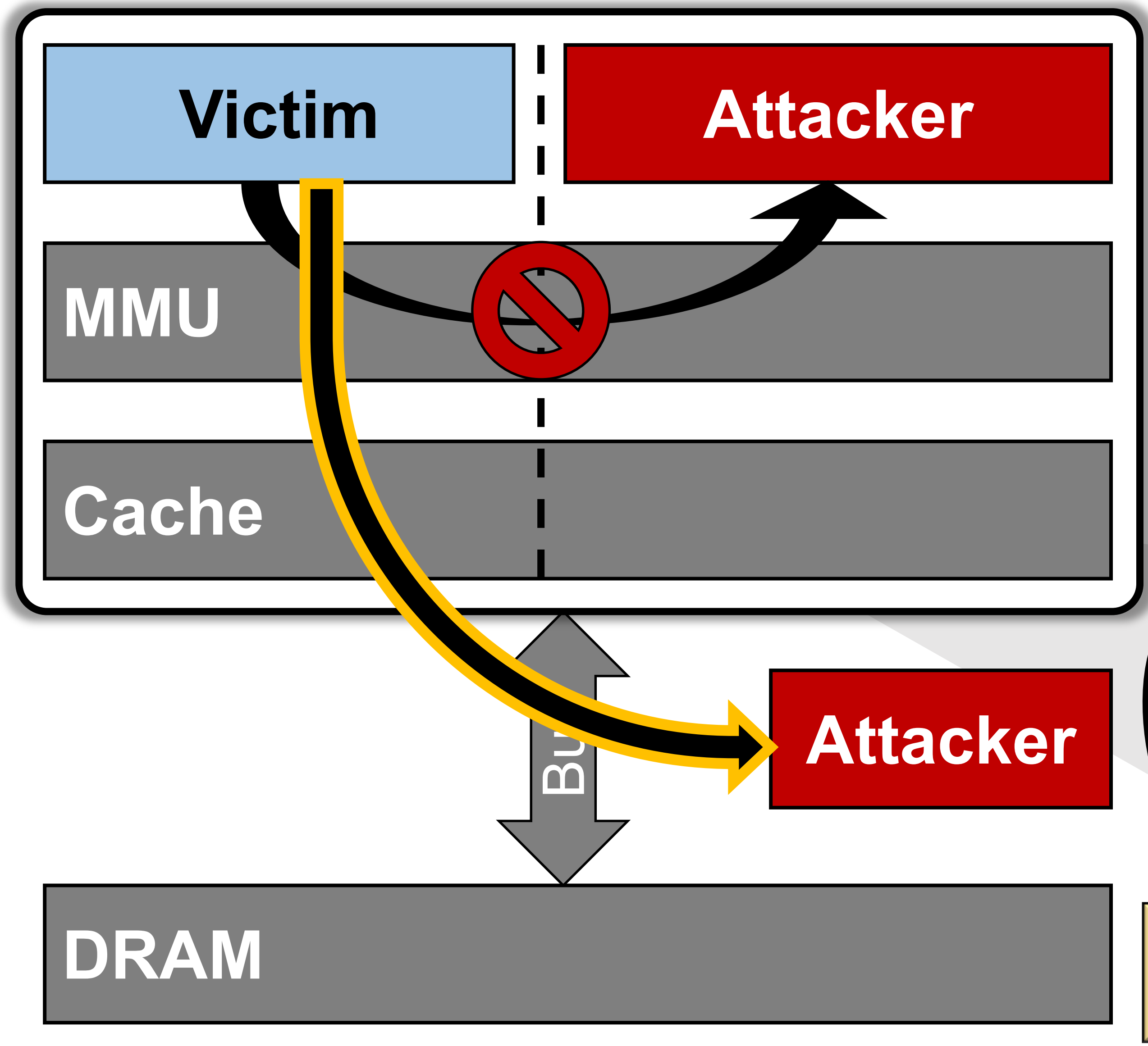


- Cache Side-Channel Attacks
  - Brasser’17, Schwarz’17, Moghimi’17, VanBulck’18
- Page Table-Based Attacks
  - Controlled-Channel'15, VanBulck’17
- Mitigations
  - Varys ’18, Chen et al.’18, Gruss et al. ’17, T-SGX’17, DéJà Vu ’17
- TEEs from Academia
  - Keystone’20, Sanctum’16

MEMBUSTER: Demonstrating "Off-Chip Attack"



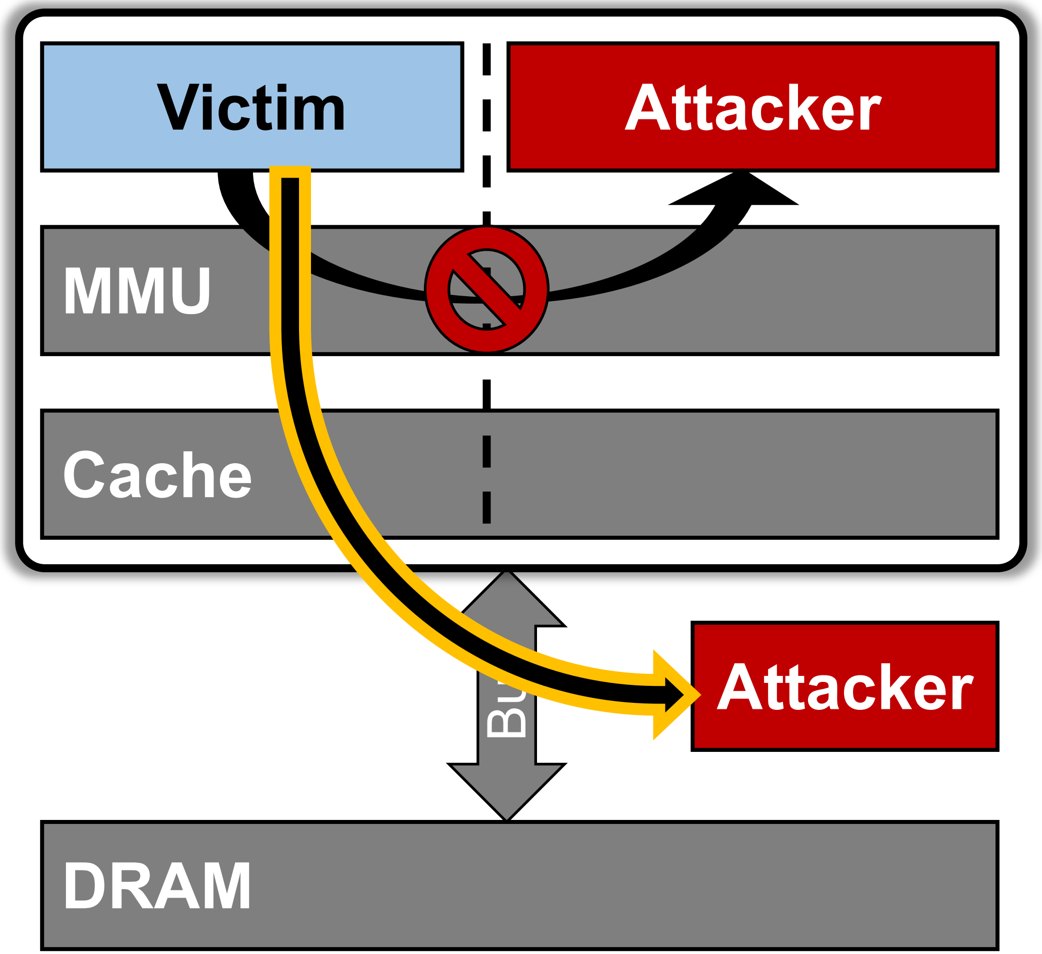
MEMBUSTER: Demonstrating “Off-Chip Attack”



- Cache Side-Channel Attacks
  - Brasser’17, Schwarz’17, Moghimi’17, VanBulck’18
- Page Table-Based Attacks
  - Controlled-Channel'15, VanBulck’17
- Mitigations
  - Varys ’18, Chen et al.’18, Gruss et al. ’17, T-SGX’17, DéJà Vu ’17
- TEEs from Academia
  - Keystone’20, Sanctum’16

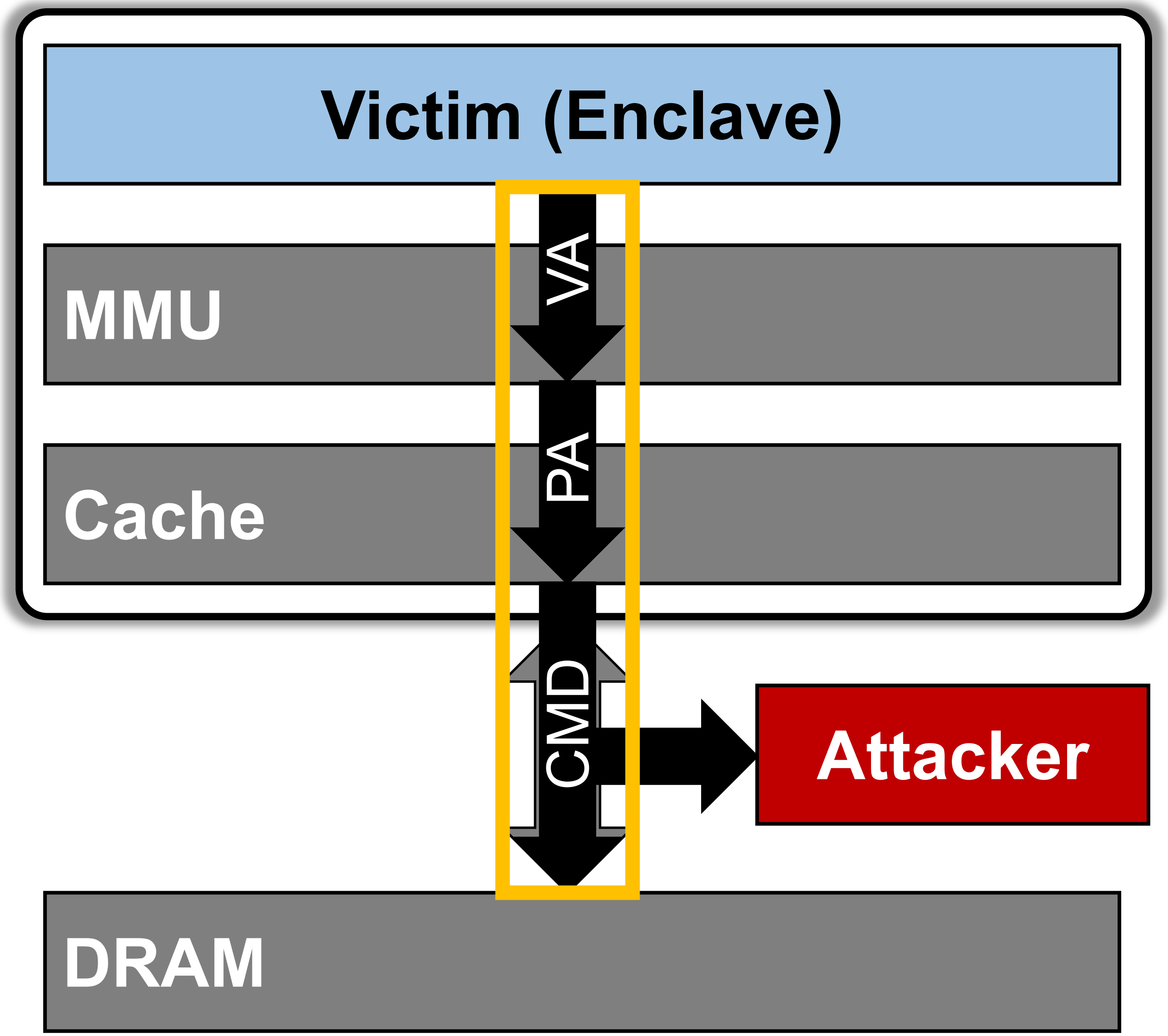
None of these can mitigate

MEMBUSTER: Demonstrating "Off-Chip Attack"



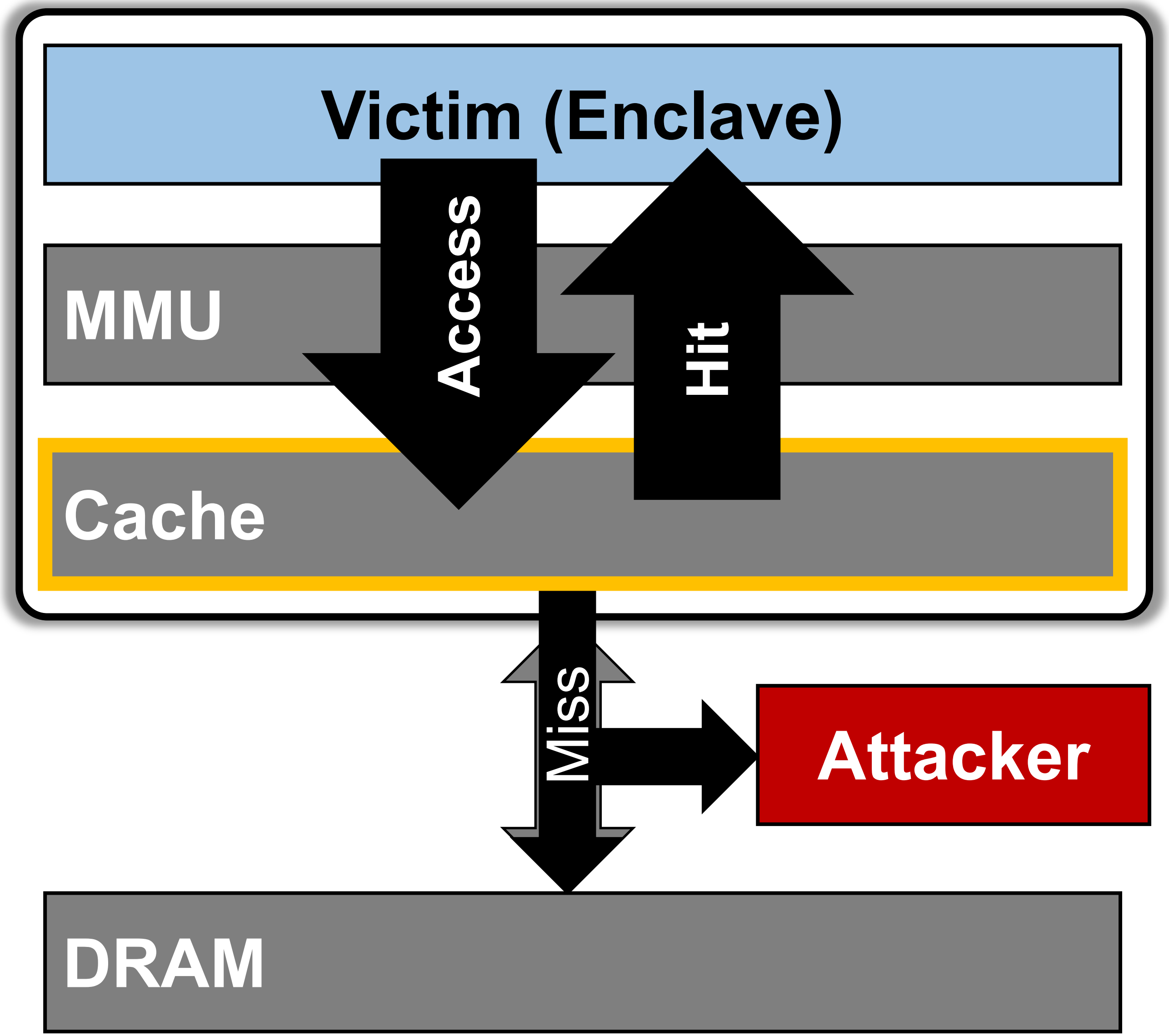
- Hard to detect or mitigate on chip
  - No interference with SW
  - Resource partitioning does not work
- Oblivious memory access
  - Performance impact
- Address bus encryption
  - Infeasible in commodity DRAM

Challenges of the Off-Chip Attack



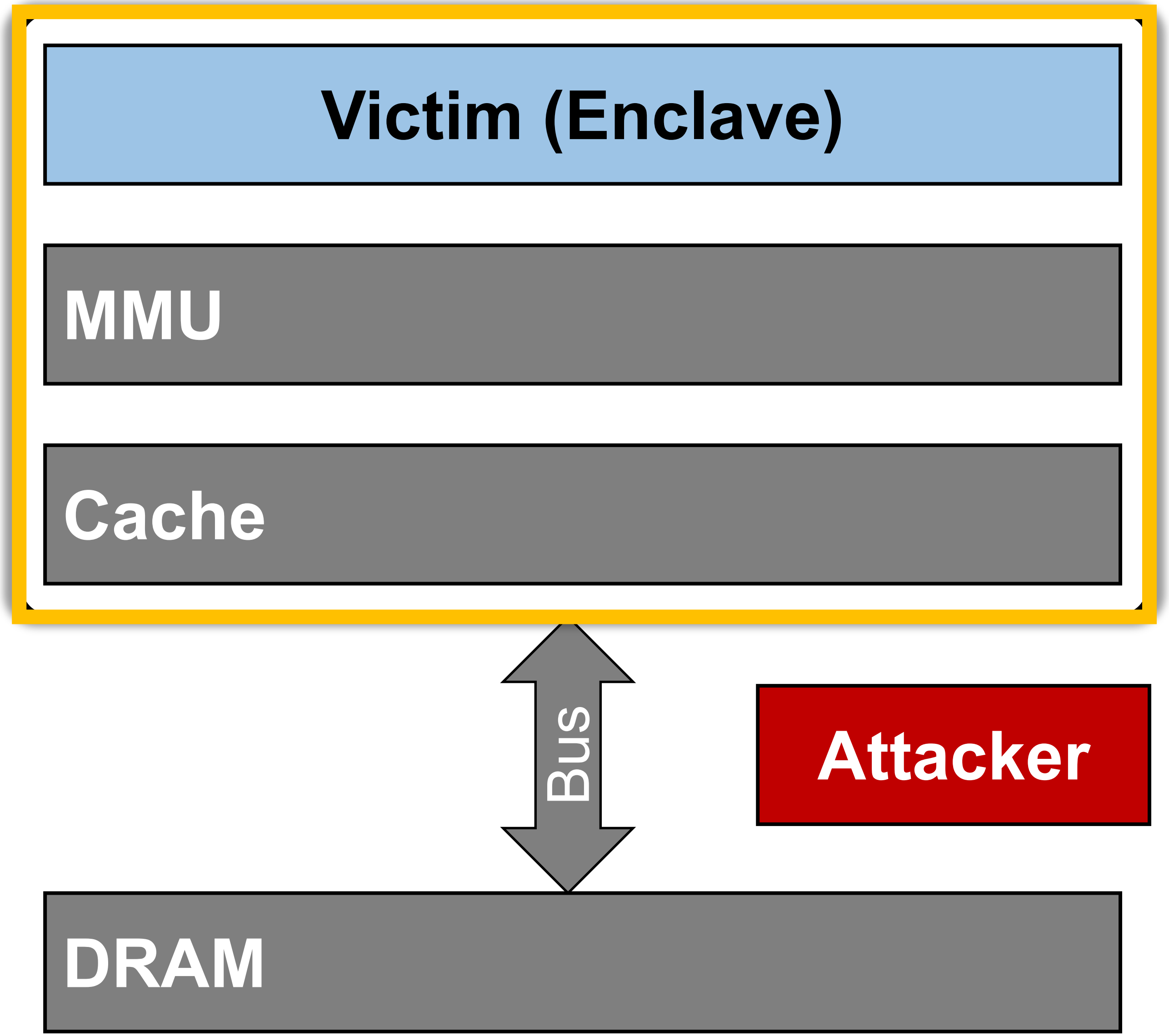
- Address Translation and Synchronization

Challenges of the Off-Chip Attack



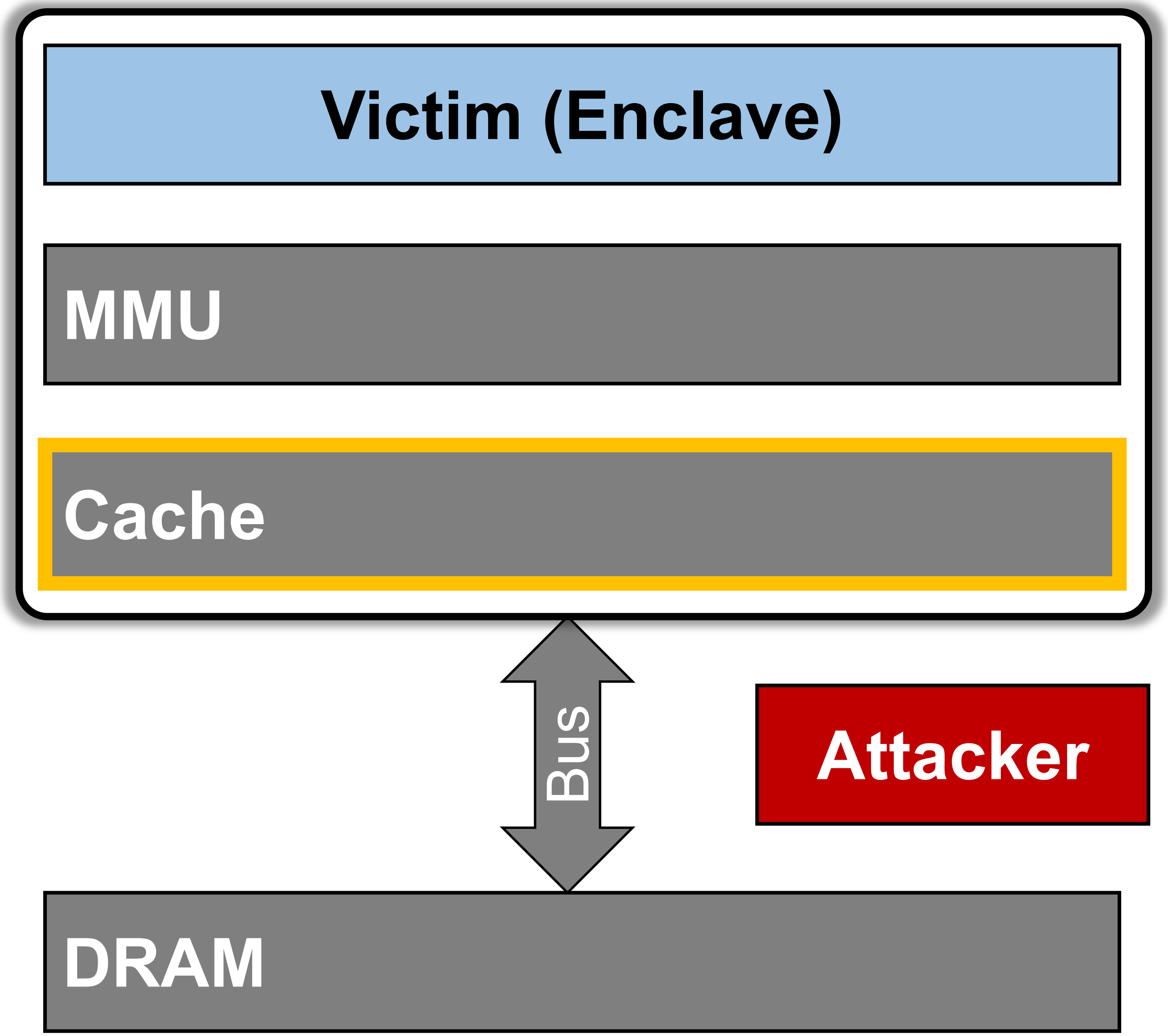
- Address Translation and Synchronization
- Lossy Channel due to Cache Hierarchy

Challenges of the Off-Chip Attack



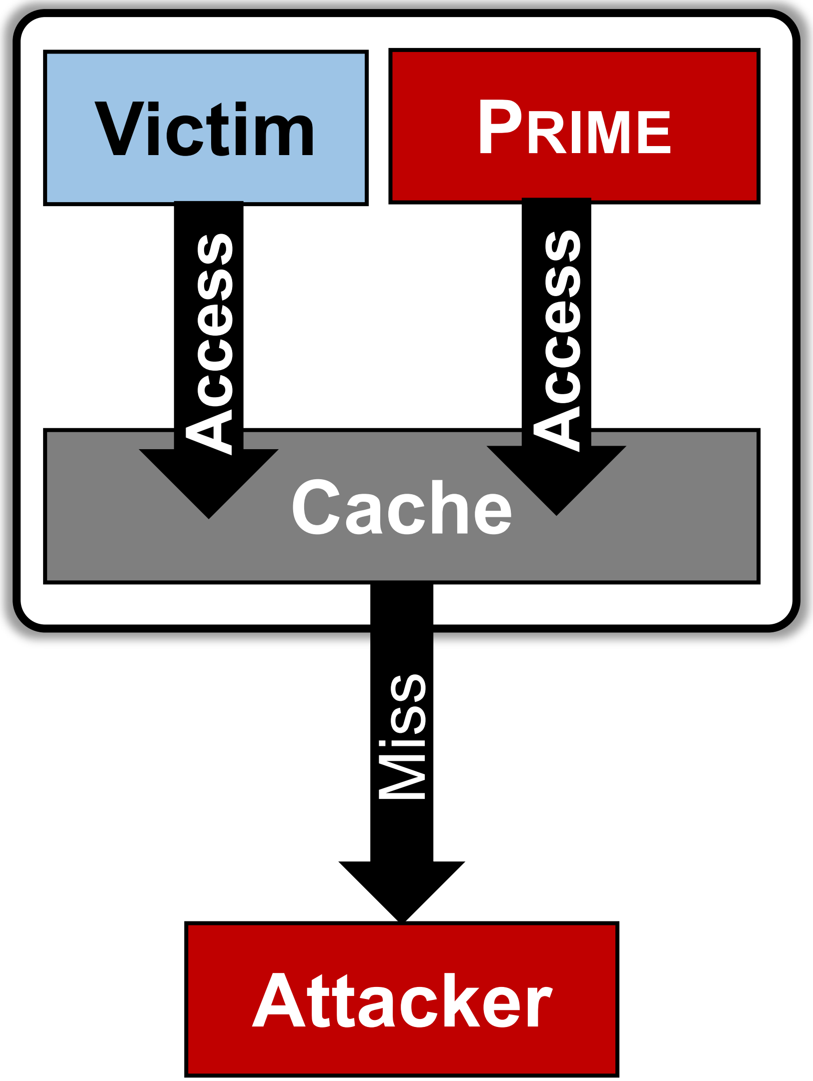
- Address Translation and Synchronization
- Lossy Channel due to Cache Hierarchy
- Unusual Behavior in SGX

Challenges of the Off-Chip Attack



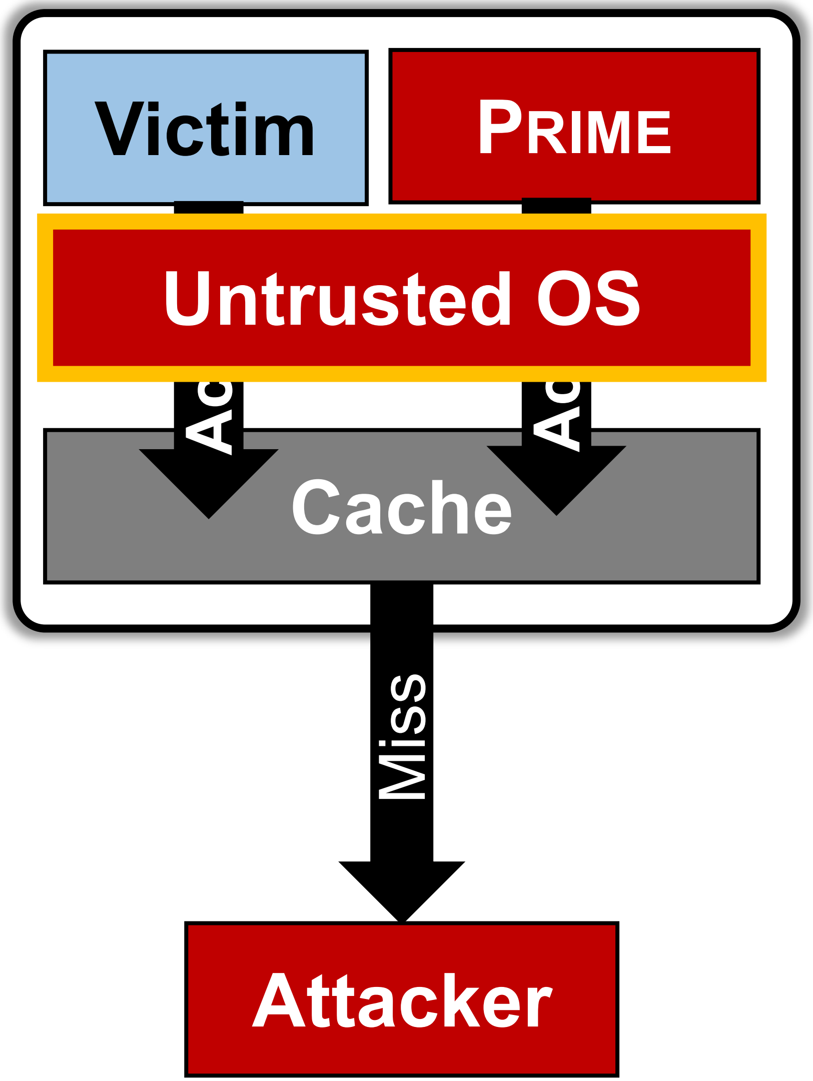
- Address Translation and Synchronization
- Lossy Channel due to Cache Hierarchy
- Unusual Behavior in SGX

Maximizing Side-Channel Information



- Goal:
  - Increase cache misses
  - Avoid detectable interference
- Cross-core cache priming
  - Cache eviction in PRIME+PROBE Attack
- Problems
  - Insufficient memory access bandwidth
  - Large last-level cache
  - Hundreds of milliseconds to evict all

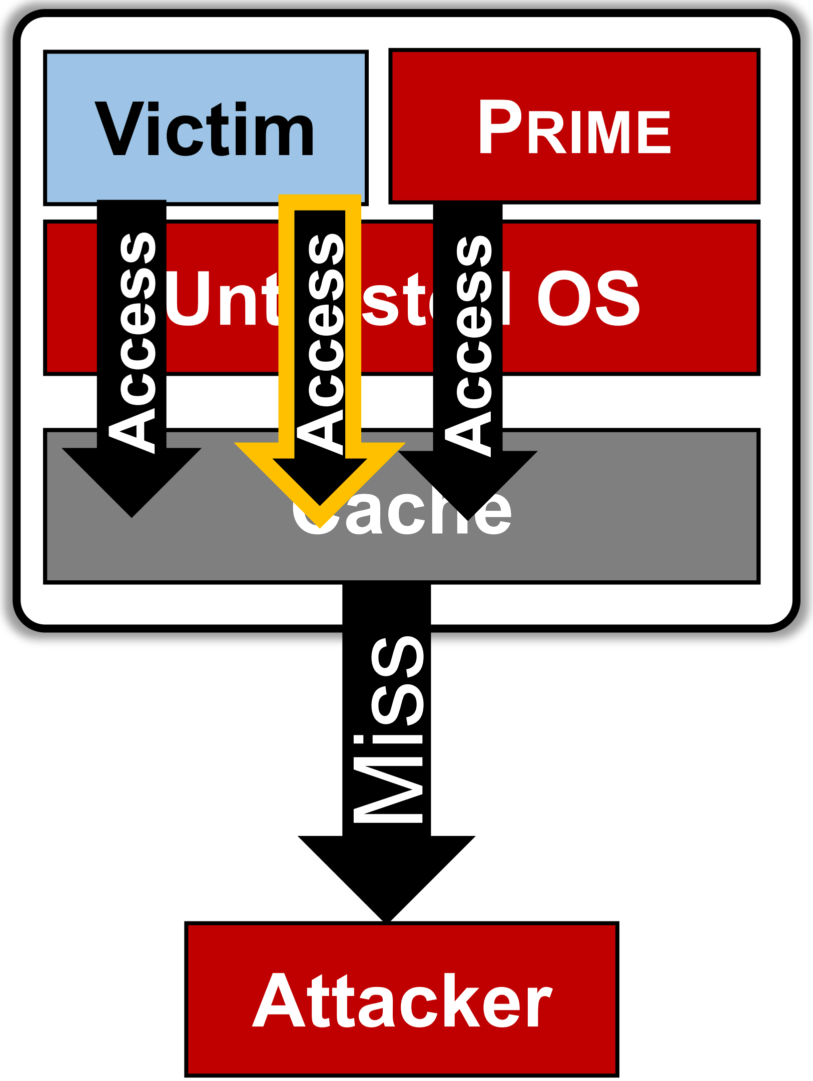
Maximizing Side-Channel Information



- **Observation 1**

  The address mapping is untrusted

Maximizing Side-Channel Information



- **Observation 1**

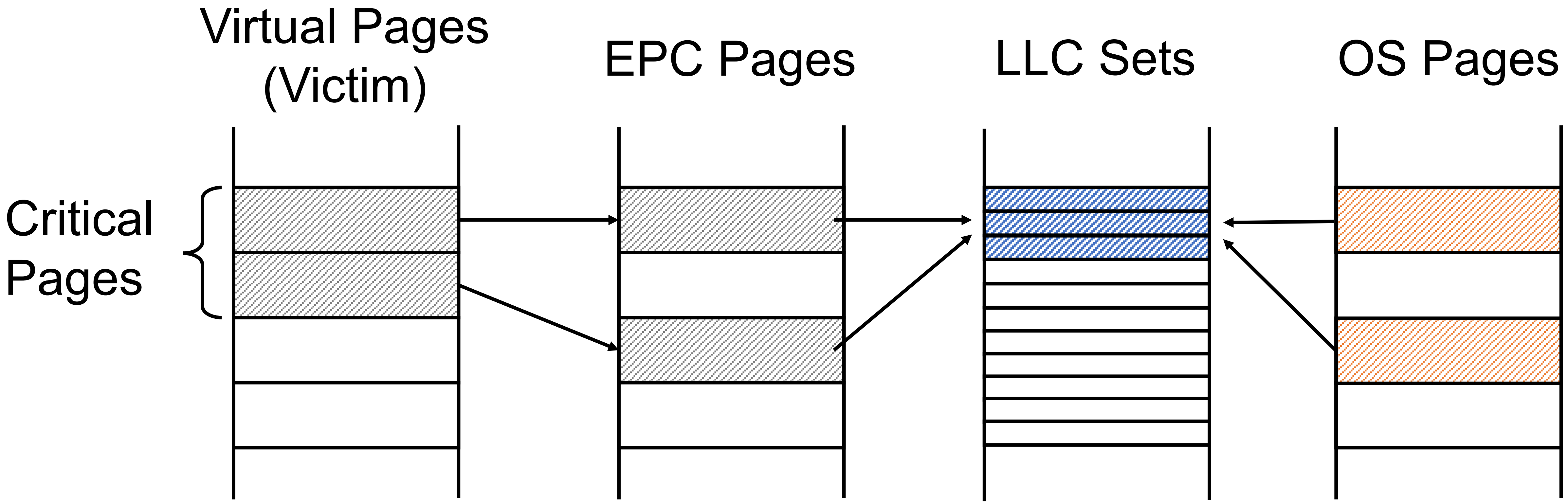
  The address mapping is untrusted

- **Observation 2**

  The attacker only needs to observe “critical” memory accesses

Idea: Squeeze the Cache!

Cache Squeezing in a Nutshell



Virtual Pages (Victim)

EPC Pages

LLC Sets

OS Pages

Critical Pages

No interrupt nor fault

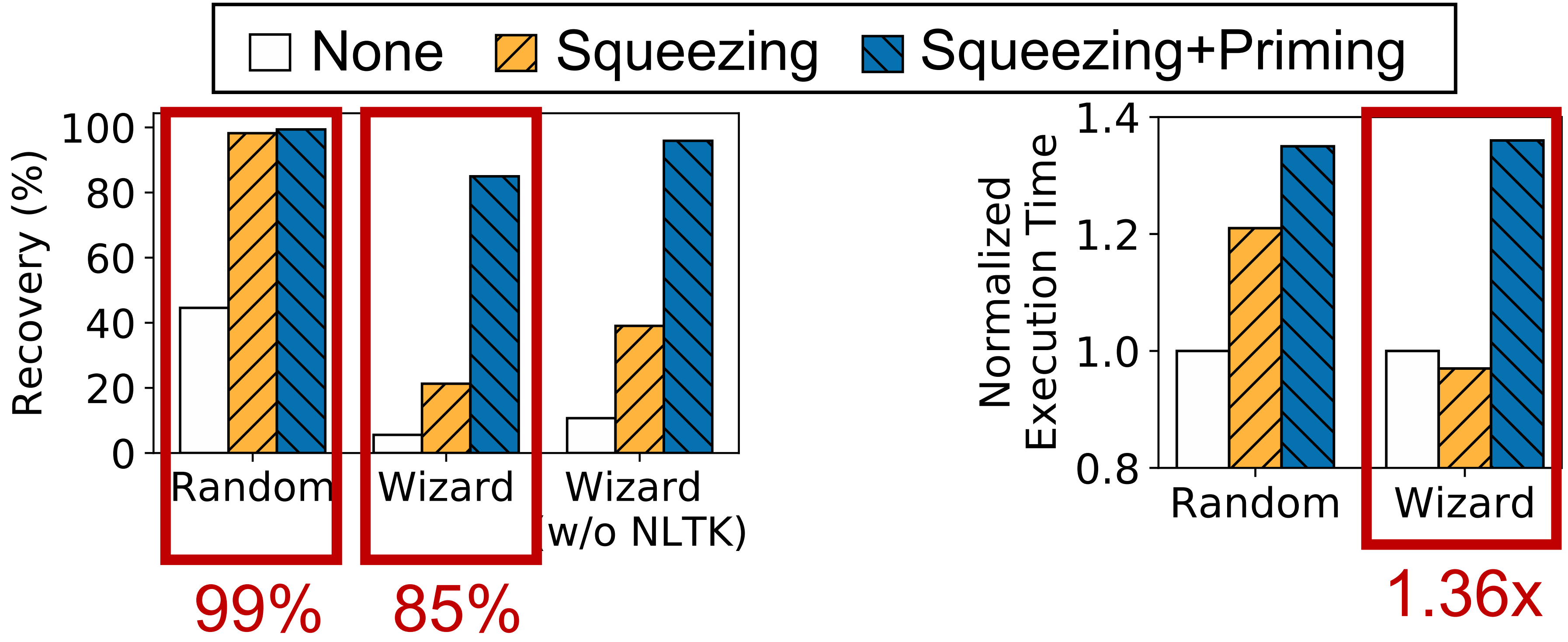
Small slowdown

Evaluation

- Hardware
  - Intel i5-8400 (Coffee Lake)
  - LLC: 9MB, 6-slice, 12-way set associative, 2048 sets
  - DRAM: Non-ECC DDR4-2400 UDIMM 8GB
  - Interposer/signal analyzer from SK Hynix
- Software
  - Two attack examples: Hunspell and Memcached
  - Graphene-SGX with unmodified victim application
  - Modified SGX driver for cache squeezing

Hunspell Attack Results

- Randomly-generated words (Random) and Wizard of Oz (Wizard)
- Squeezing+Priming recovers most of the data



99%

85%

1.36x

No interference: hard to detect with on-chip techniques

Conclusion

- Membuster: an **off-chip** attack via the memory bus
  - Performed on commodity CPU and DRAM
  - Non-interfering with victim application
  - Previous on-chip solutions or other TEEs do not defeat the attack
- Costly mitigation techniques
  - Oblivious memory access
  - Alternative TEE architecture (e.g., memory bus encryption)

Thank You!

Thank You!

Dayeol Lee (dayeol@berkeley.edu)
Chia-Che Tsai (chiache@tamu.edu)
Raluca Ada Popa (raluca.popa@berkeley.edu)