BadRAM

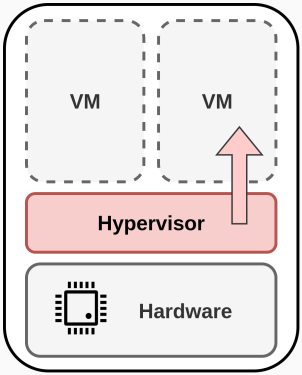
Practical Memory Aliasing Attacks on Trusted Execution Environments

Jesse De Meulemeester* Luca Wilke* David Oswald
Thomas Eisenbarth Ingrid Verbauwhede Jo Van Bulck
* Equal Contribution

2025-05-14, S&P25

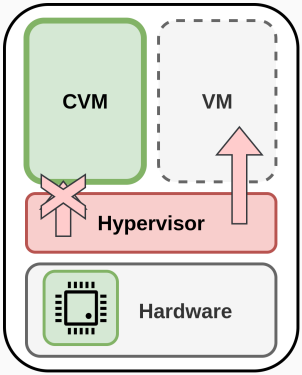
KU LEUVEN COSIC UNIVERSITAS LUBERCENSIS UNIVERSITY OF BIRMINGHAM DistriNet

Why Trusted Execution Environments?



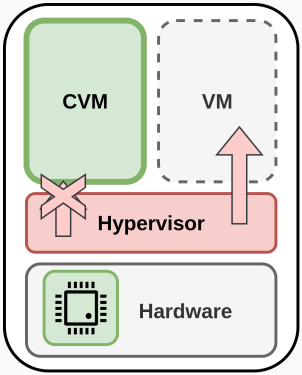
- Without TEEs cloud provider has full access to VMs
- Pitch: TEEs lock out the cloud provider
- Enable computing on private data in the cloud

Why Trusted Execution Environments?



- Without TEEs cloud provider has full access to VMs
- Pitch: TEEs lock out the cloud provider
- Enable computing on private data in the cloud

Why Trusted Execution Environments?

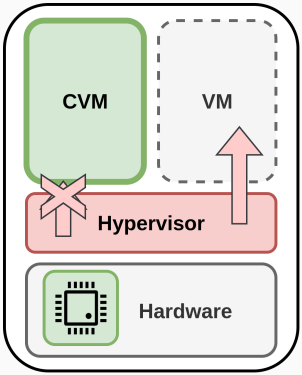


- Without TEEs cloud provider has full access to VMs
- Pitch: TEEs lock out the cloud provider
- Enable computing on private data in the cloud

AMD SEV-SNP

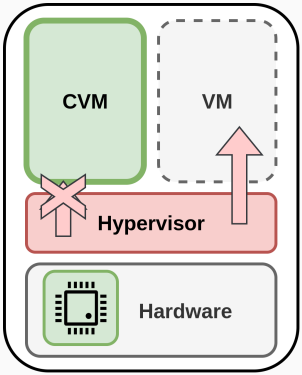
- Root-of-trust: Secure Processor (SP)
- Supported by wide range of cloud providers

Why Trusted Execution Environments?



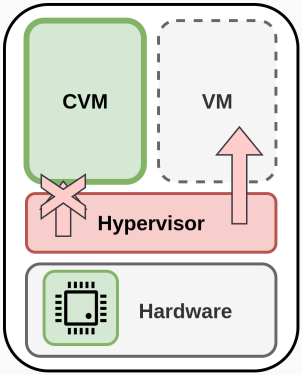
- Without TEEs cloud provider has full access to VMs
- Pitch: TEEs lock out the cloud provider
- Enable computing on private data in the cloud
- **However** strong attacker model enables a vast amount of attacks

Why Trusted Execution Environments?



- Without TEEs cloud provider has full access to VMs
- Pitch: TEEs lock out the cloud provider
- Enable computing on private data in the cloud
- **However** strong attacker model enables a vast amount of attacks
  - Software-level adversaries

Why Trusted Execution Environments?



- Without TEEs cloud provider has full access to VMs
- Pitch: TEEs lock out the cloud provider
- Enable computing on private data in the cloud
- **However** strong attacker model enables a vast amount of attacks
  - Software-level adversaries
  - Hardware-level adversaries

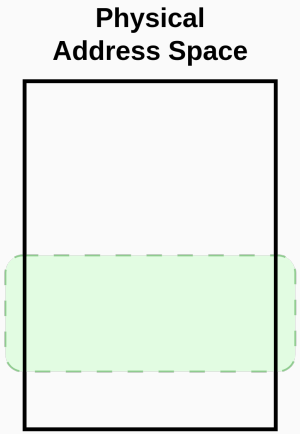
Memory Encryption in TEEs

			Guarantees		
TEE	**Encryption**	Scalable	*Confidentiality*	*Integrity*	*Freshness*
Intel Classic SGX	AES-CTR	✗	✓	✓	✓
Intel Scalable SGX	AES-XTS	✓	✓	✗	✗
Intel TDX	AES-XTS	✓	✓	✓	✗
AMD SEV-SNP	AES-XEX	✓	✓	✗	✗
Arm CCA	AES-XEX/QARMA	✓	✓	✗	✗

Memory Encryption in TEEs

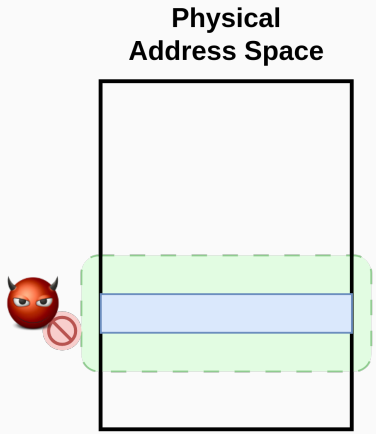
TEE	Encryption	Scalable	Guarantees		
			Confidentiality	*Integrity*	*Freshness*
Intel Classic SGX	AES-CTR	✗	✓	✓	✓
Intel Scalable SGX	AES-XTS	✓	✓	✗	✗
Intel TDX	AES-XTS	✓	✓	✓	✗
AMD SEV-SNP	AES-XEX	✓	✓	✗	✗
Arm CCA	AES-XEX/QARMA	✓	✓	✗	✗

Memory Isolation in TEEs



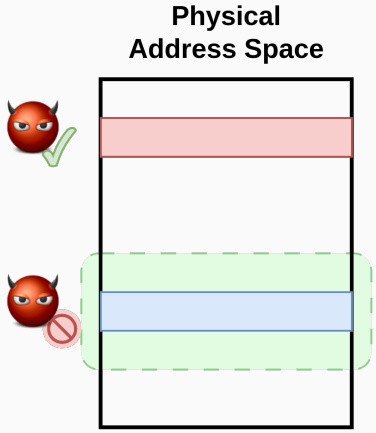
- Prevent access to TEE memory
  - SEV: *Ciphertext hiding*
  - SGX/TDX: Return fixed value & poison on write

Memory Isolation in TEEs



- Prevent access to TEE memory
  - SEV: *Ciphertext hiding*
  - SGX/TDX: Return fixed value & poison on write

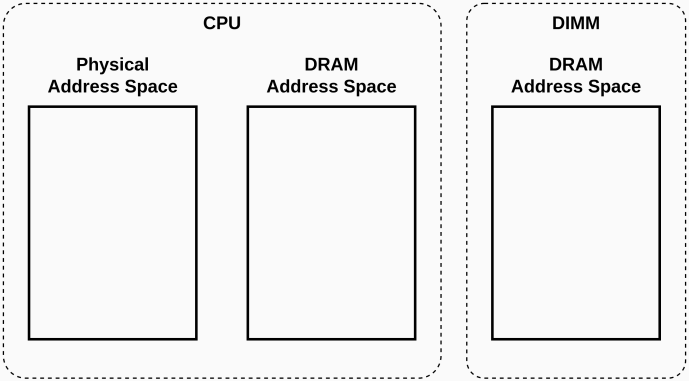
Memory Isolation in TEEs



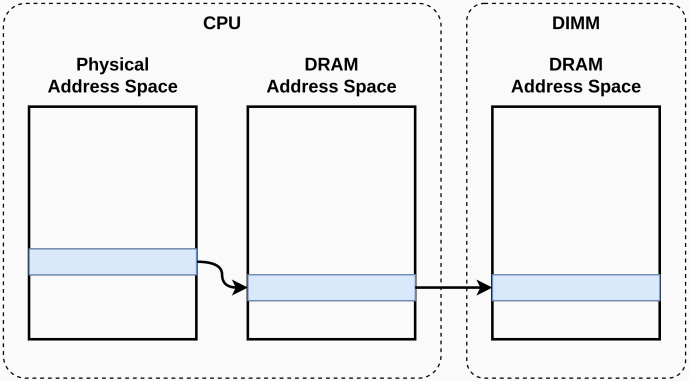
- Prevent access to TEE memory
  - SEV: *Ciphertext hiding*
  - SGX/TDX: Return fixed value & poison on write

Can DIMMs be manipulated to break integrity protections in scalable TEE designs?

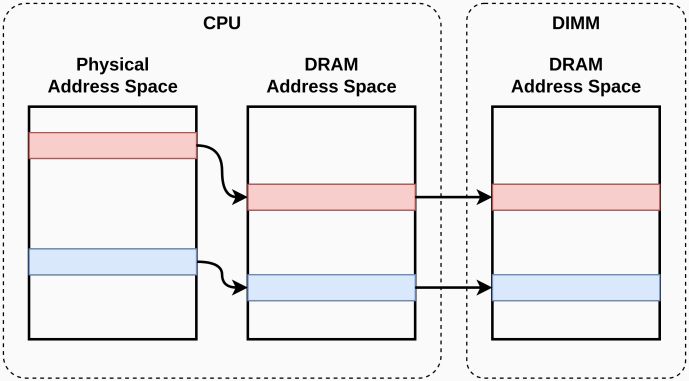
DRAM Addressing



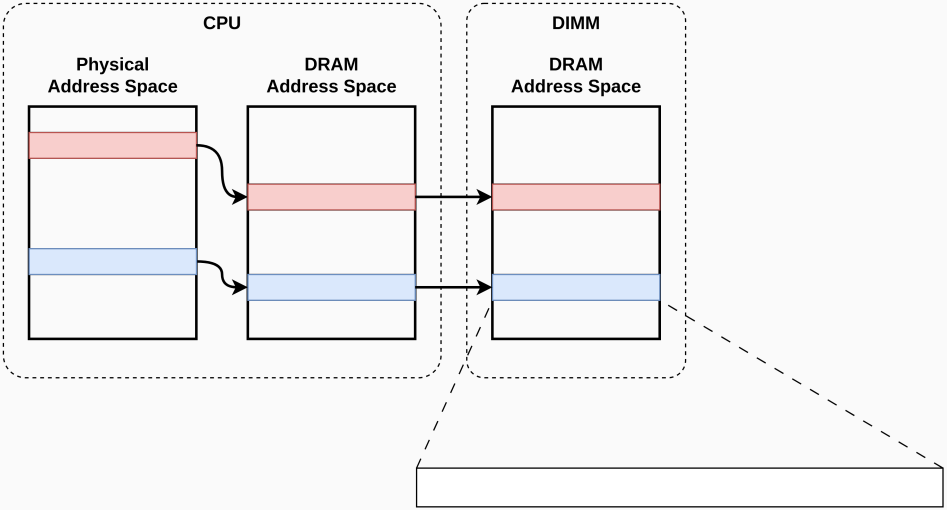
DRAM Addressing



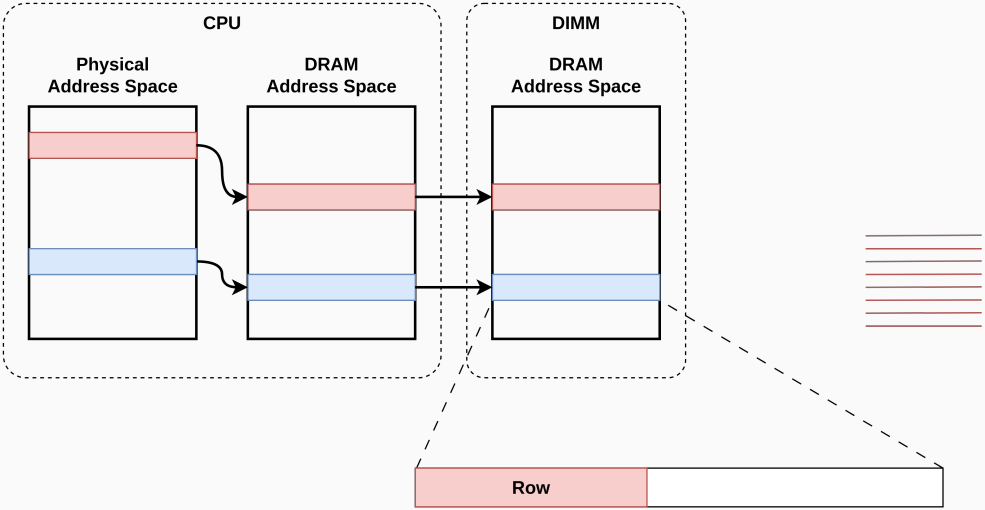
DRAM Addressing



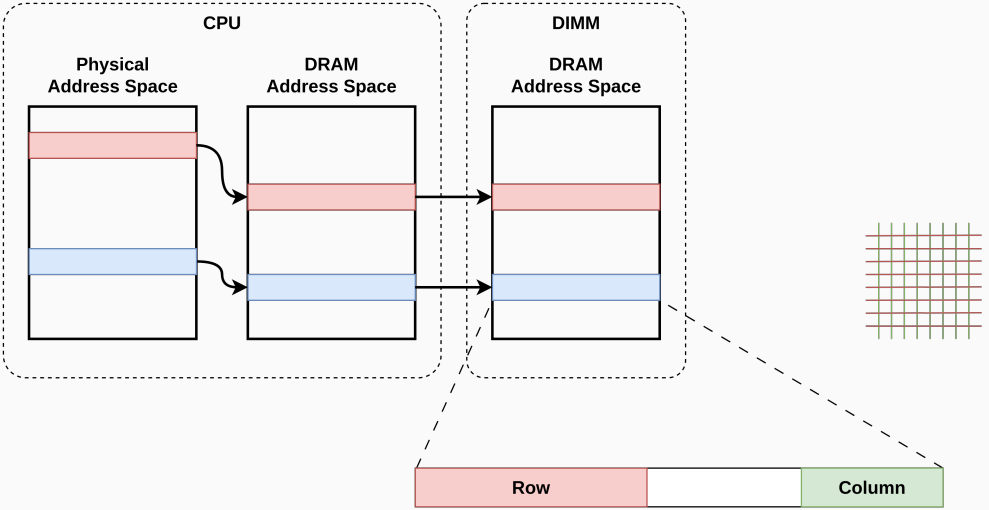
DRAM Addressing



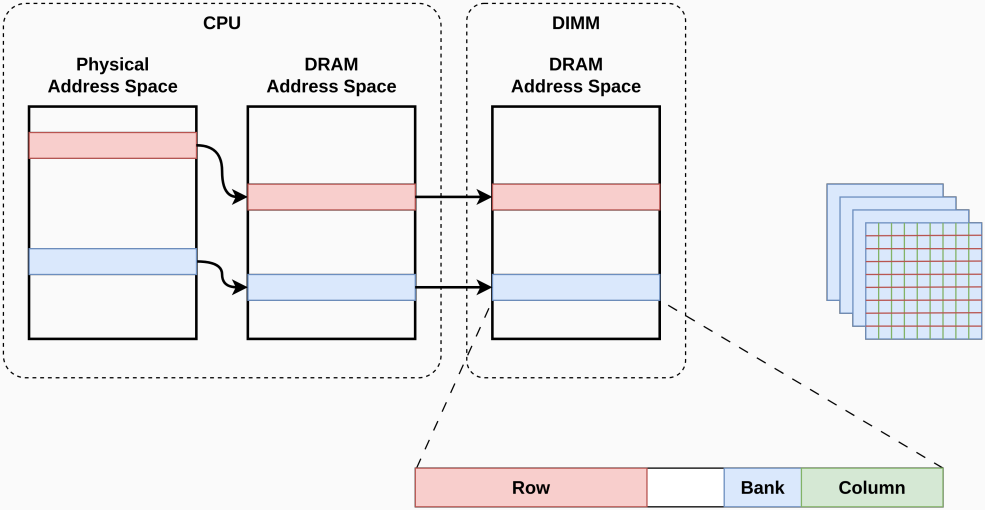
DRAM Addressing



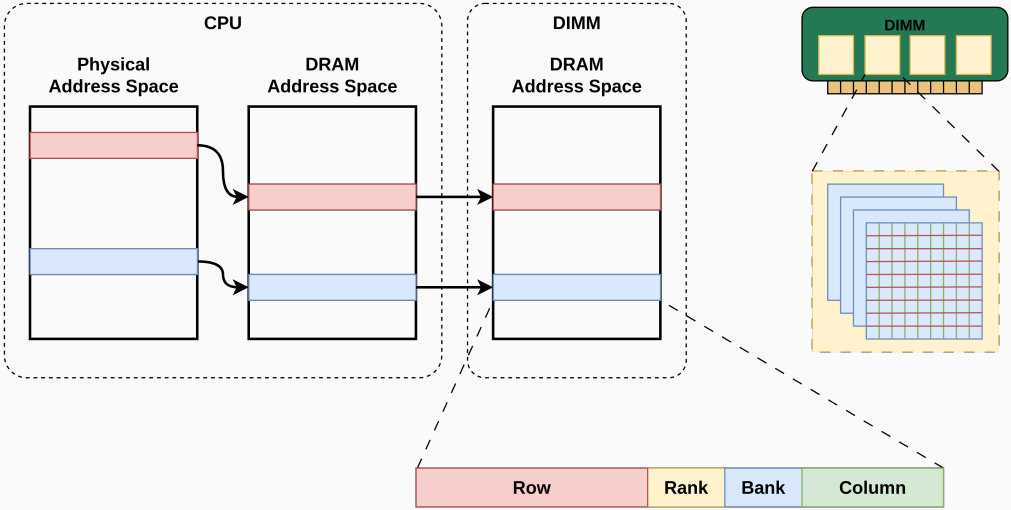
DRAM Addressing



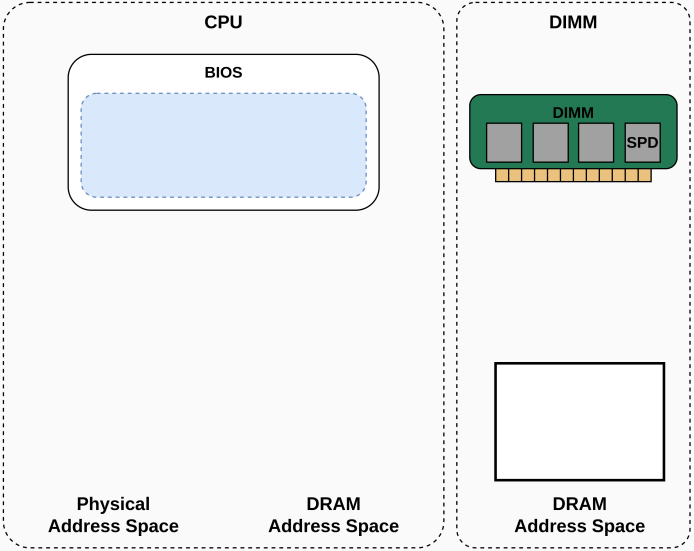
DRAM Addressing



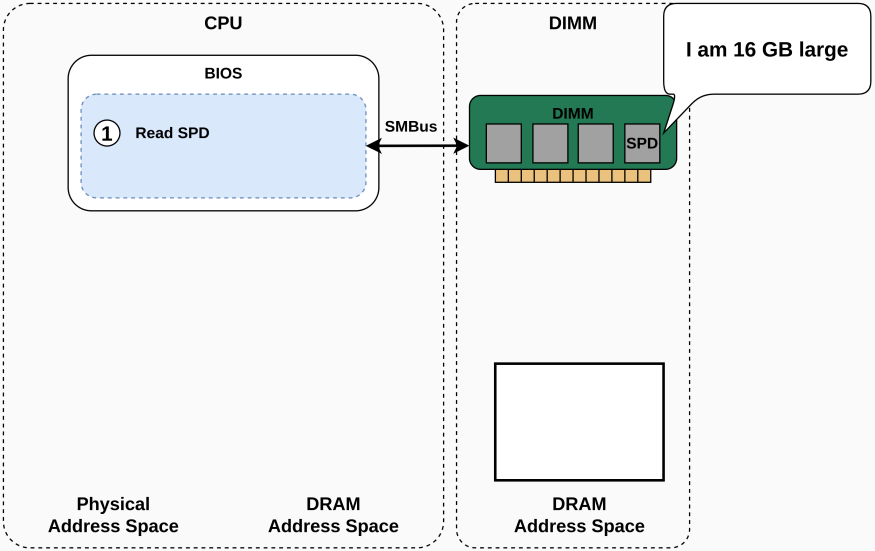
DRAM Addressing



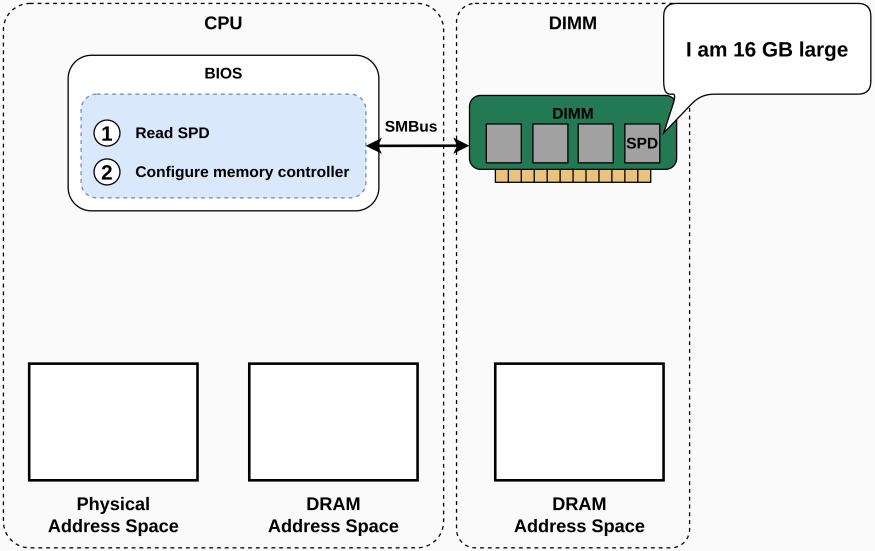
Introducing Aliases



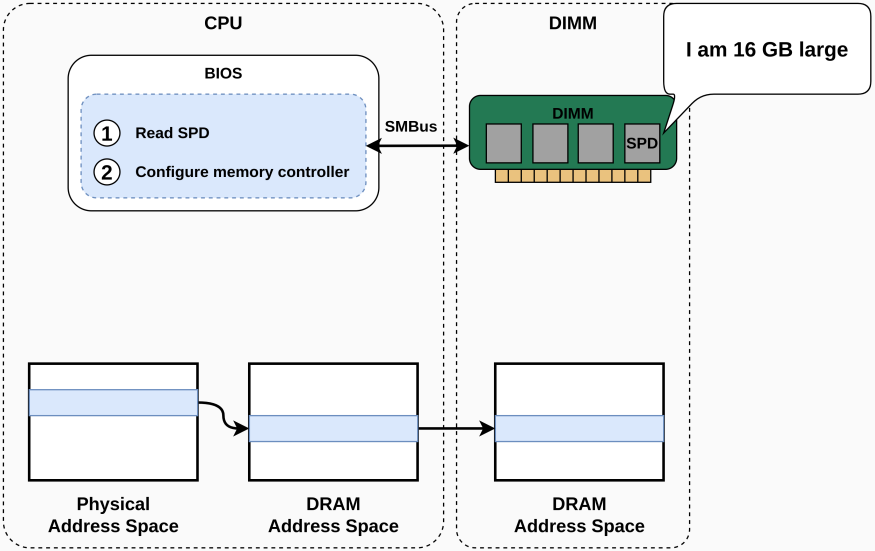
Introducing Aliases



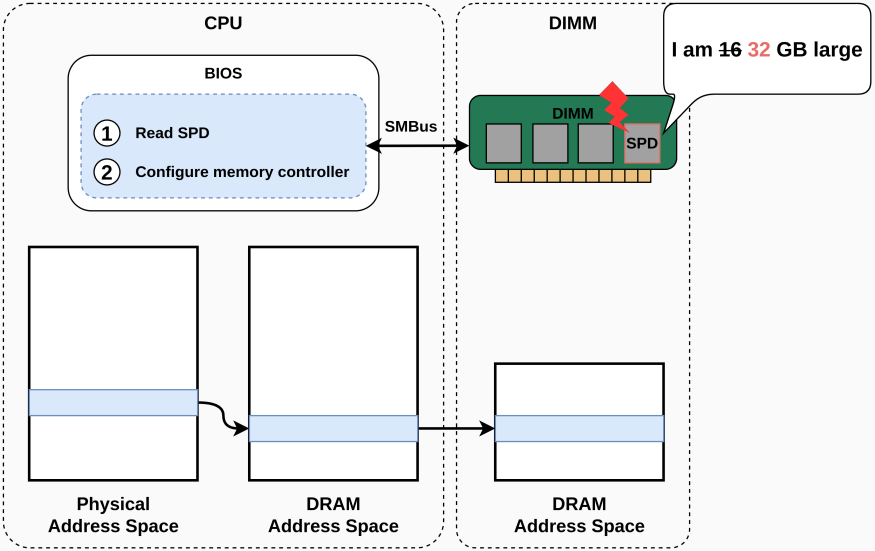
Introducing Aliases



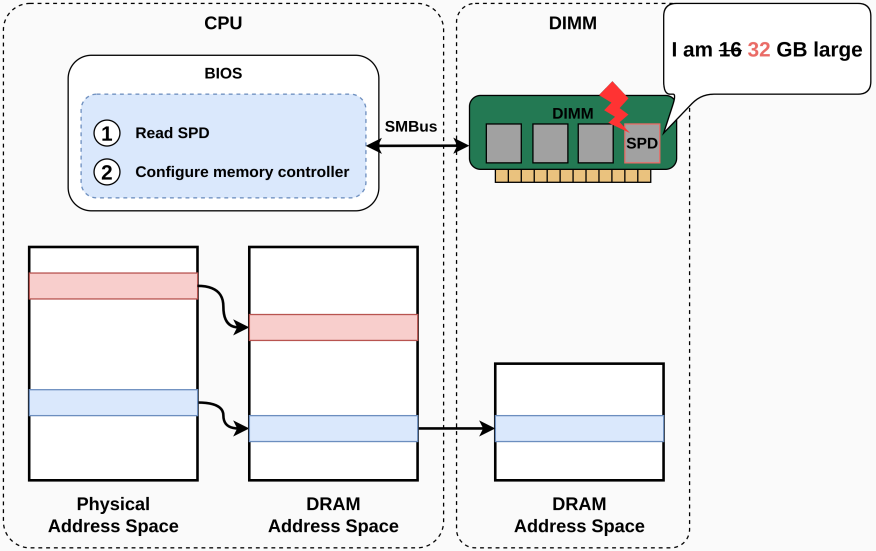
Introducing Aliases



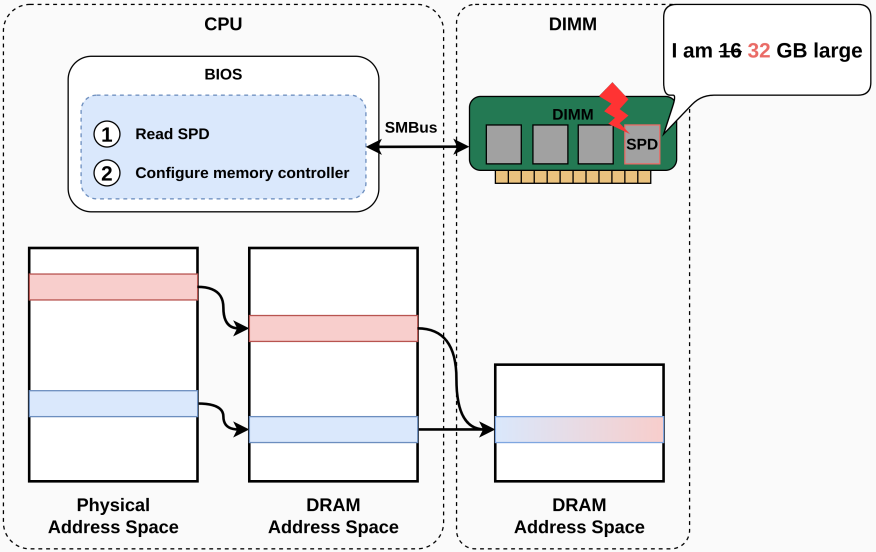
Introducing Aliases



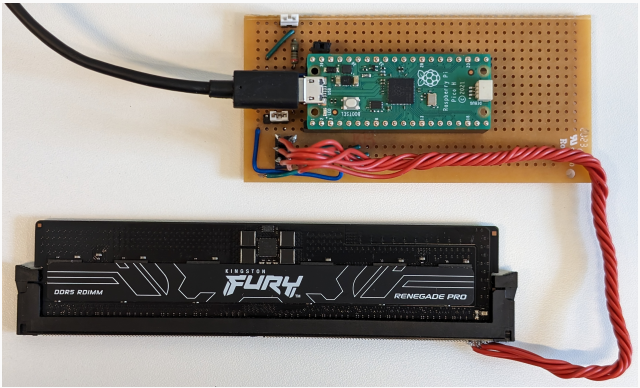
Introducing Aliases



Introducing Aliases

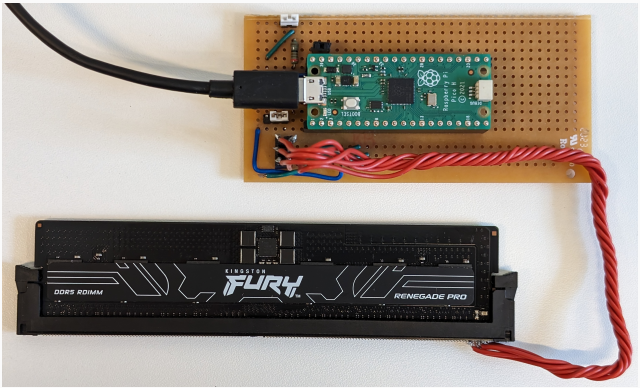


Modifying SPD



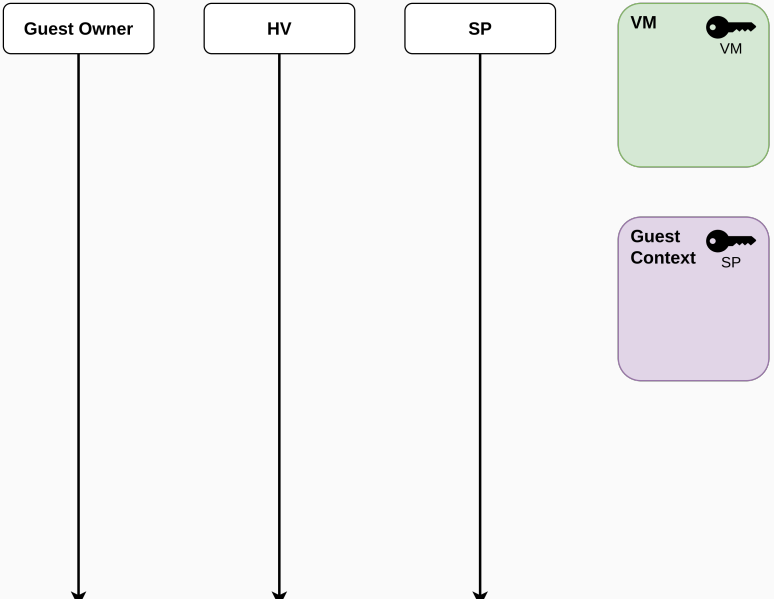
- I^2C pins exposed on DIMM
- Trivial to unlock and overwrite

Modifying SPD

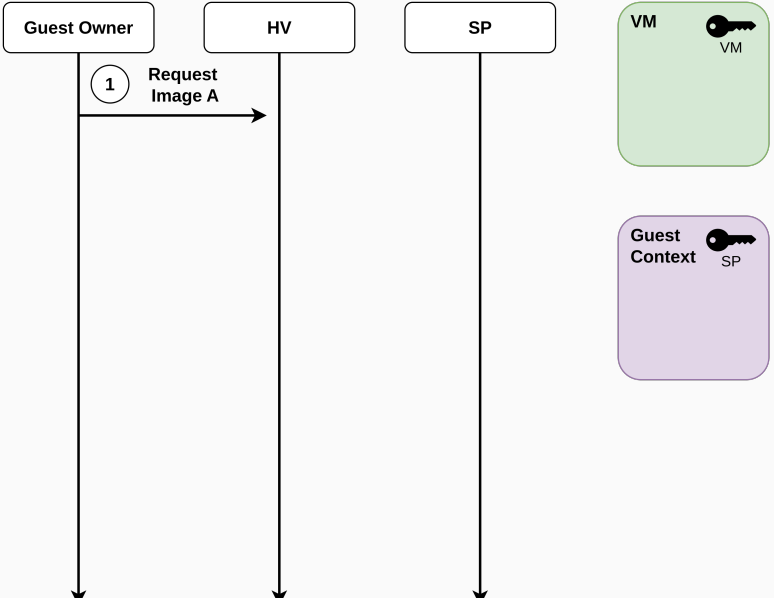


- I^2C pins exposed on DIMM
- Trivial to unlock and overwrite
- Total cost: ~**10$**

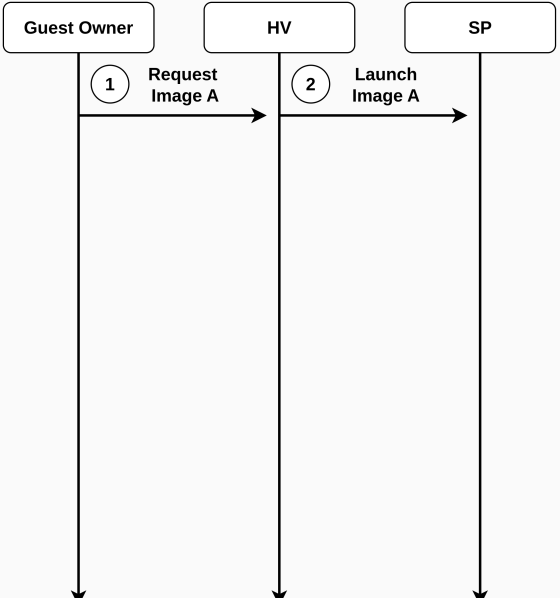
SEV-SNP Attestation Attack: Phase 1

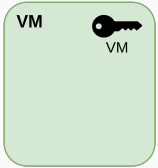


SEV-SNP Attestation Attack: Phase 1

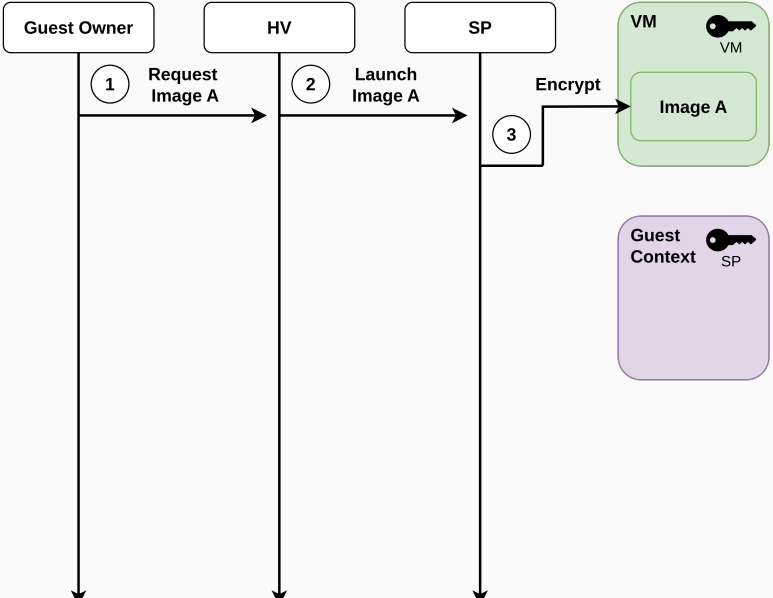


SEV-SNP Attestation Attack: Phase 1

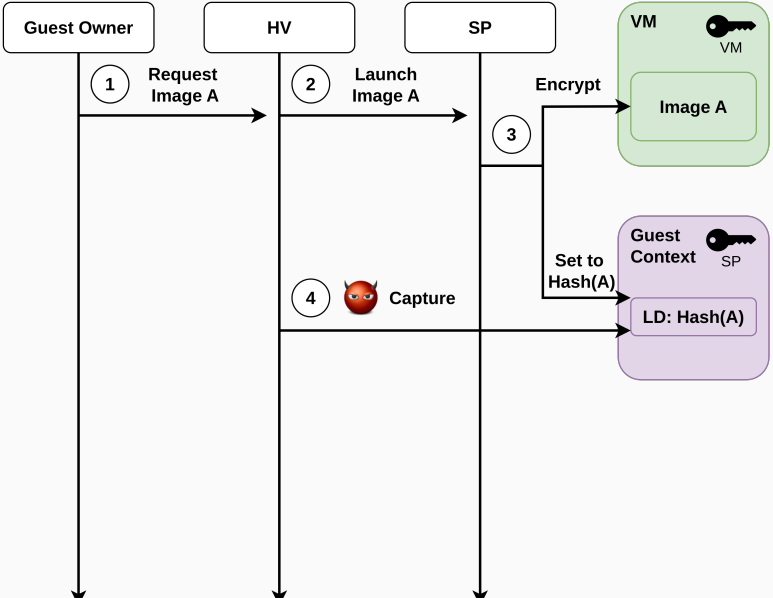




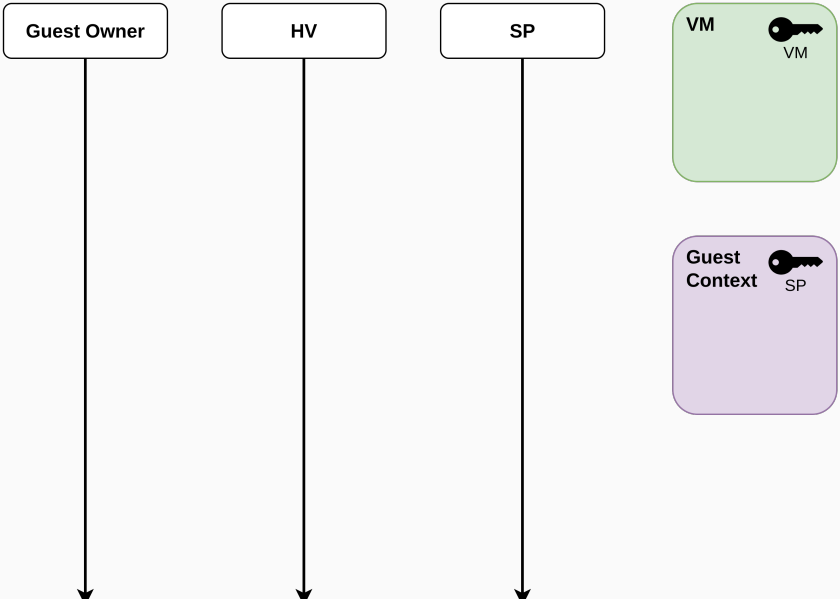
SEV-SNP Attestation Attack: Phase 1



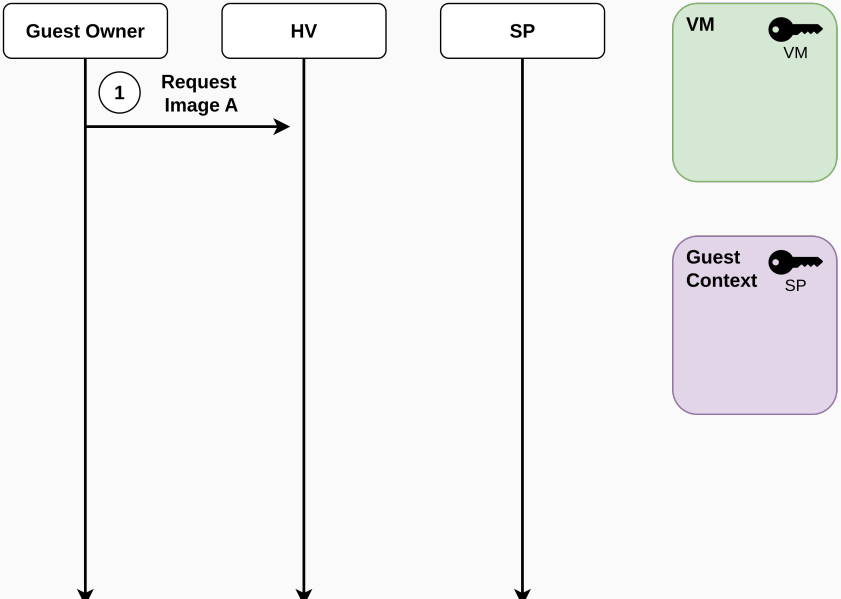
SEV-SNP Attestation Attack: Phase 1



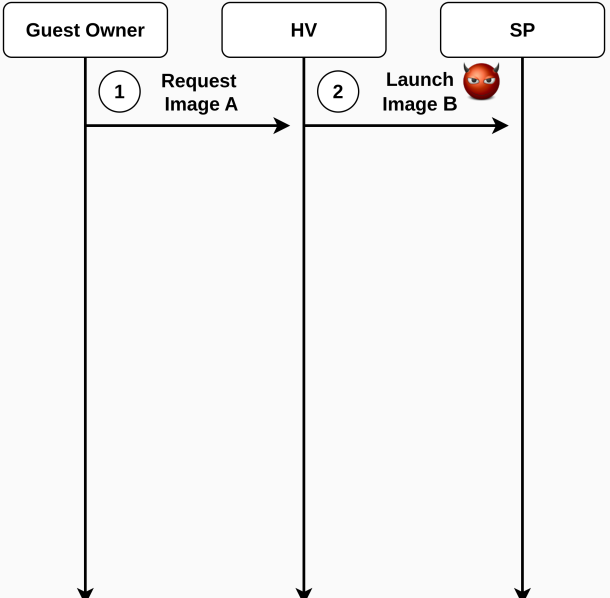
SEV-SNP Attestation Attack: Phase 2

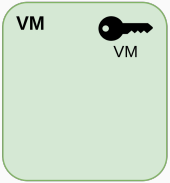


SEV-SNP Attestation Attack: Phase 2

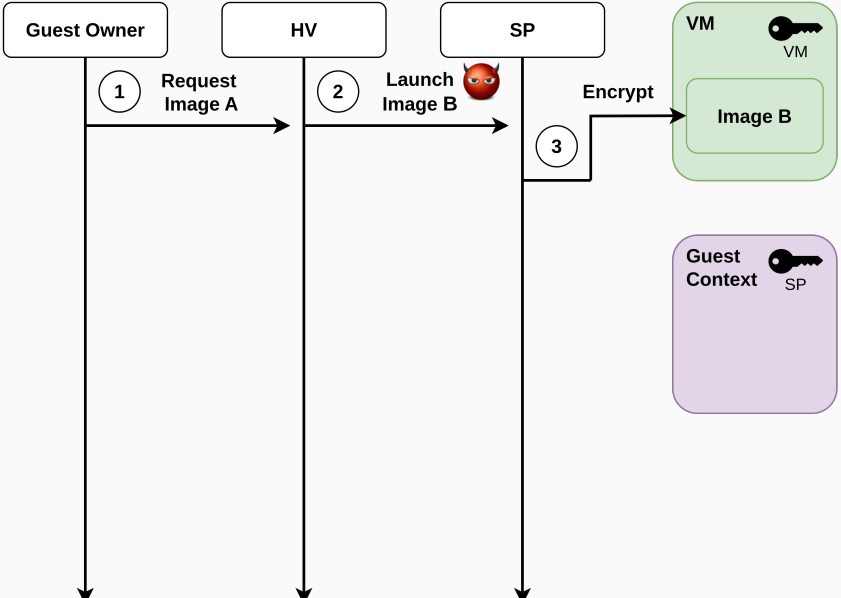


SEV-SNP Attestation Attack: Phase 2

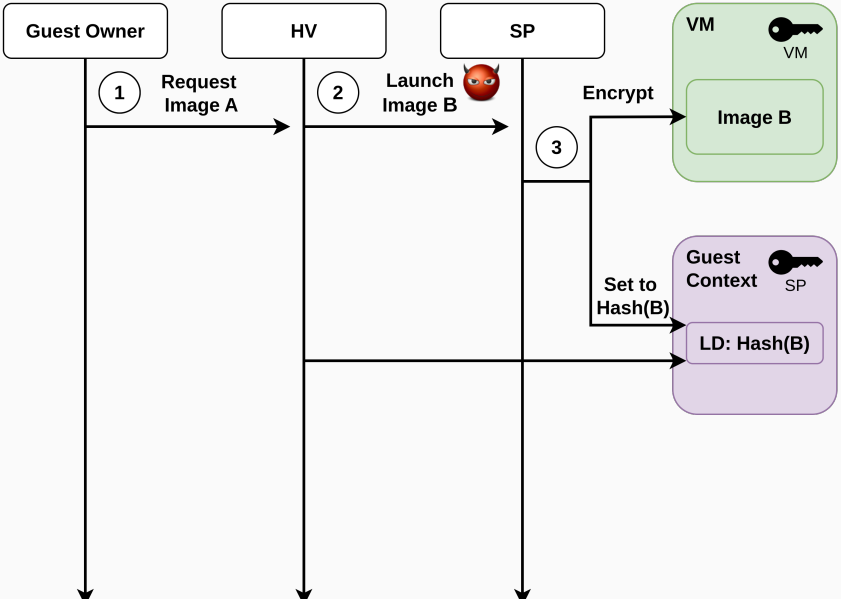




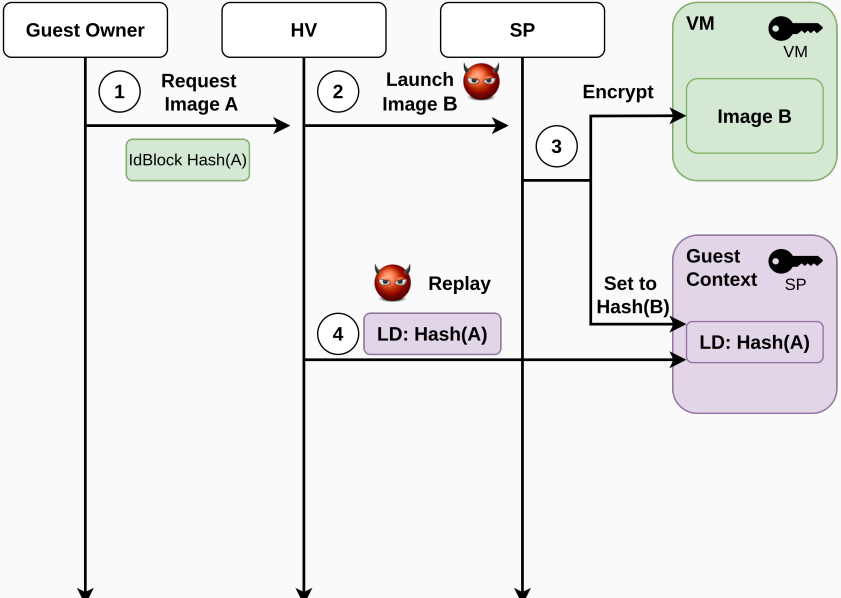
SEV-SNP Attestation Attack: Phase 2



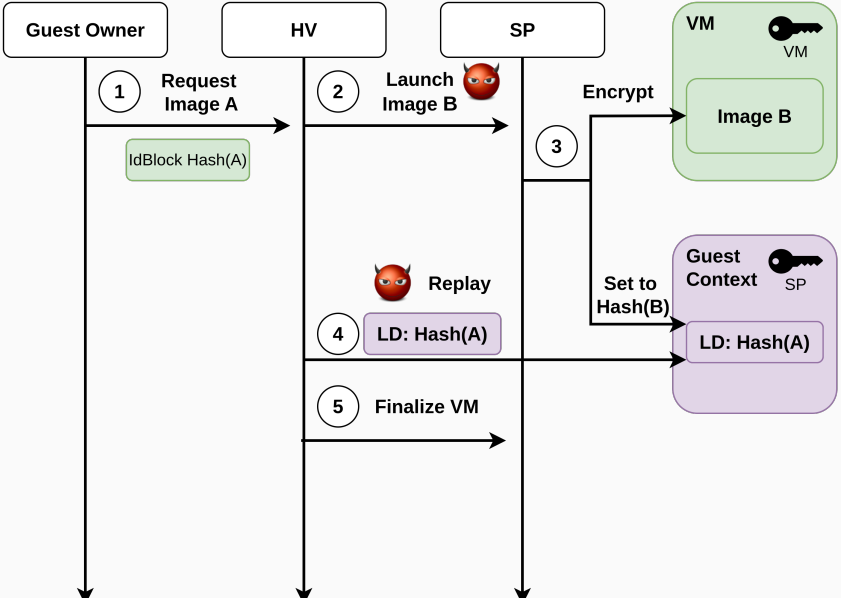
SEV-SNP Attestation Attack: Phase 2



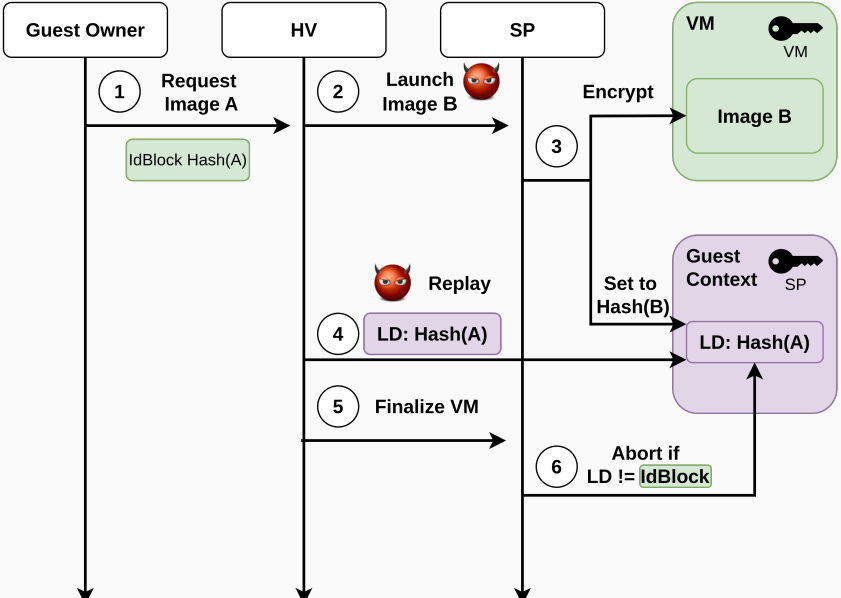
SEV-SNP Attestation Attack: Phase 2



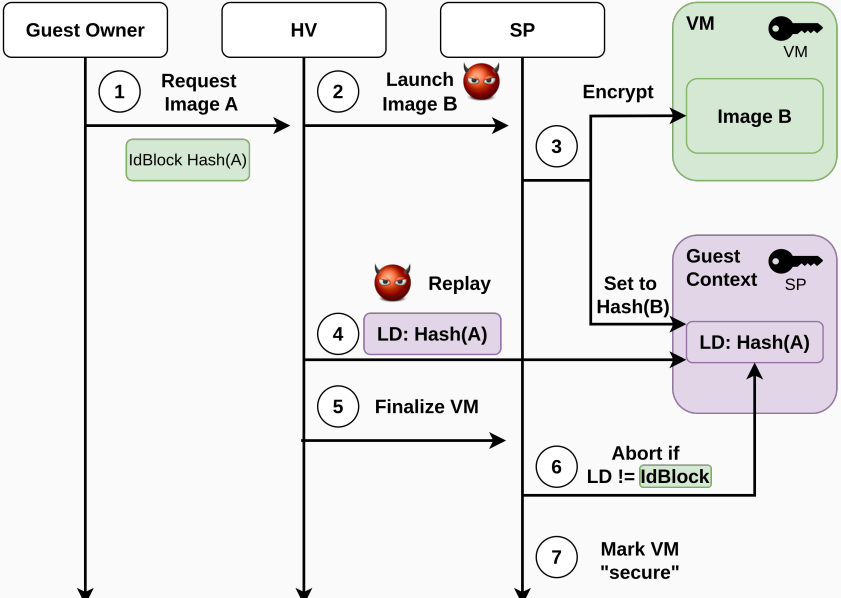
SEV-SNP Attestation Attack: Phase 2



SEV-SNP Attestation Attack: Phase 2



SEV-SNP Attestation Attack: Phase 2



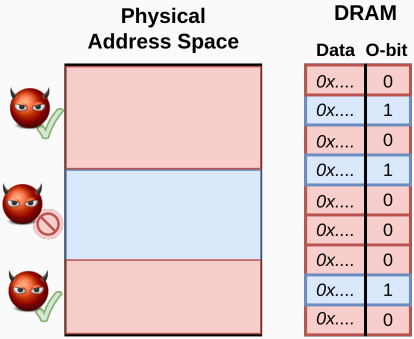
Intel's Countermeasures

1. Alias Checking[1,2]
   - Idea: Search for aliases at boot time
   - TOCTOU?
2. ECC-based MAC/Owner bit[1]
   - Idea: Store metadata in ECC bits
   - **Owner bit** Mark TDX/SGX pages
   - **MAC** integrity protection

[1] S. Johnson et al. *Supporting Intel SGX on Multi-Socket Platforms.* Intel tech rep. 784473, August 2023.
[2] AMD. *Undermining Integrity Features of SEV-SNP with Memory Aliasing.* AMD SB-3015, December 2024.

Intel's Countermeasures

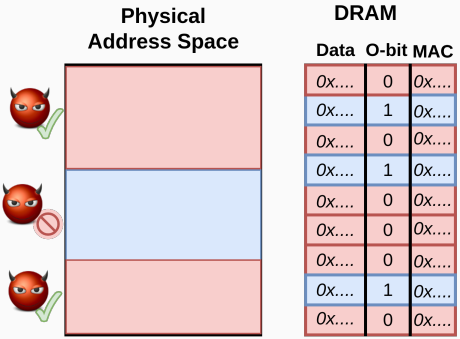
1. Alias Checking[1,2]
   - Idea: Search for aliases at boot time
   - TOCTOU?
2. ECC-based MAC/Owner bit[1]
   - Idea: Store metadata in ECC bits
   - **Owner bit** Mark TDX/SGX pages
   - **MAC** integrity protection



[1] S. Johnson et al. *Supporting Intel SGX on Multi-Socket Platforms.* Intel tech rep. 784473, August 2023.
[2] AMD. *Undermining Integrity Features of SEV-SNP with Memory Aliasing.* AMD SB-3015, December 2024.

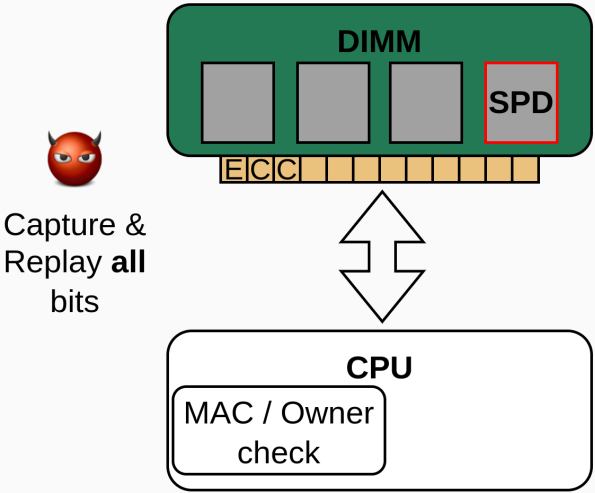
Intel's Countermeasures

1. Alias Checking[1,2]
   - Idea: Search for aliases at boot time
   - TOCTOU?
2. ECC-based MAC/Owner bit[1]
   - Idea: Store metadata in ECC bits
   - **Owner bit** Mark TDX/SGX pages
   - **MAC** integrity protection



[1] S. Johnson et al. *Supporting Intel SGX on Multi-Socket Platforms.* Intel tech rep. 784473, August 2023.
[2] AMD. *Undermining Integrity Features of SEV-SNP with Memory Aliasing.* AMD SB-3015, December 2024.

Intel's Countermeasures: ECC-based MAC/Owner bit



Principled Countermeasures

- Strong Crypto
  - Abandoned by Intel, AMD, and Arm
- Highly Integrated Memory
  - Inflexible, size constraints

Summary

- **BadRAM creates aliases** in physical address space
  - One-time physical access to DIMM
  - Total cost: ~10$
- E2E attack: **Break SEV-SNP attestation**
- Deployed Countermeasures
  - Alias check: Scalable SGX, TDX, **SEV-SNP (new)**
  - ECC metadata: Scalable SGX, TDX
- Principled Countermeasures: strong crypto, highly integrated memory

BadRAM

Practical Memory Aliasing Attacks on Trusted Execution Environments

Jesse De Meulemeester* Luca Wilke*
David Oswald Thomas Eisenbarth
Ingrid Verbauwhede Jo Van Bulck
* Equal Contribution

KU LEUVEN COSIC UNIVERSITY OF BIRMINGHAM DistriNet