BadRAM: Practical Memory Aliasing Attacks on Trusted Execution Environments

Jesse De Meulemeester*[1], Luca Wilke*[2], David Oswald[3], Thomas Eisenbarth[2], Ingrid Verbauwhede[1], and Jo Van Bulck[1]

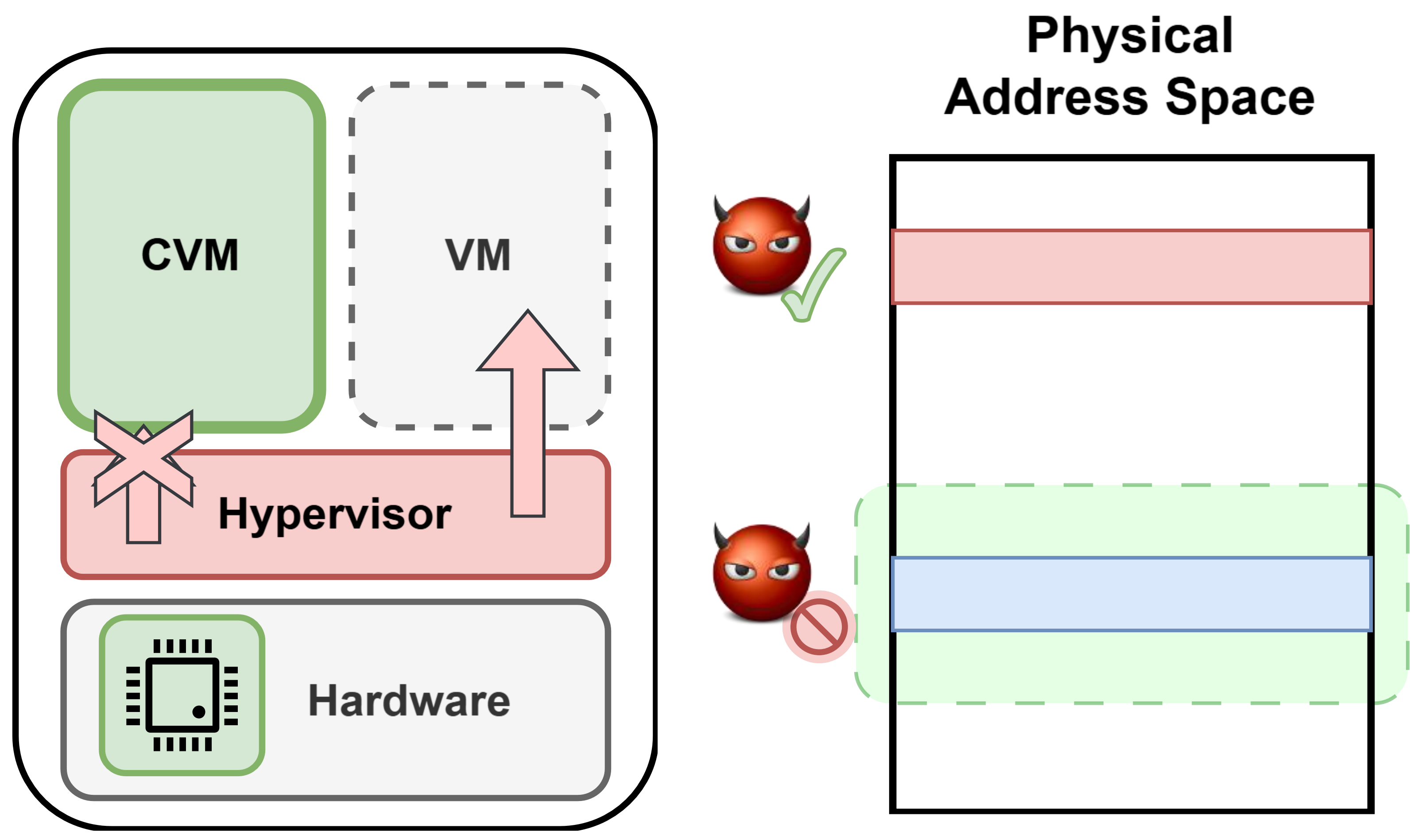
[1] KU LEUVEN

[2] UNIVERSITÄT ZU LÜBECK

[3] UNIVERSITY OF BIRMINGHAM

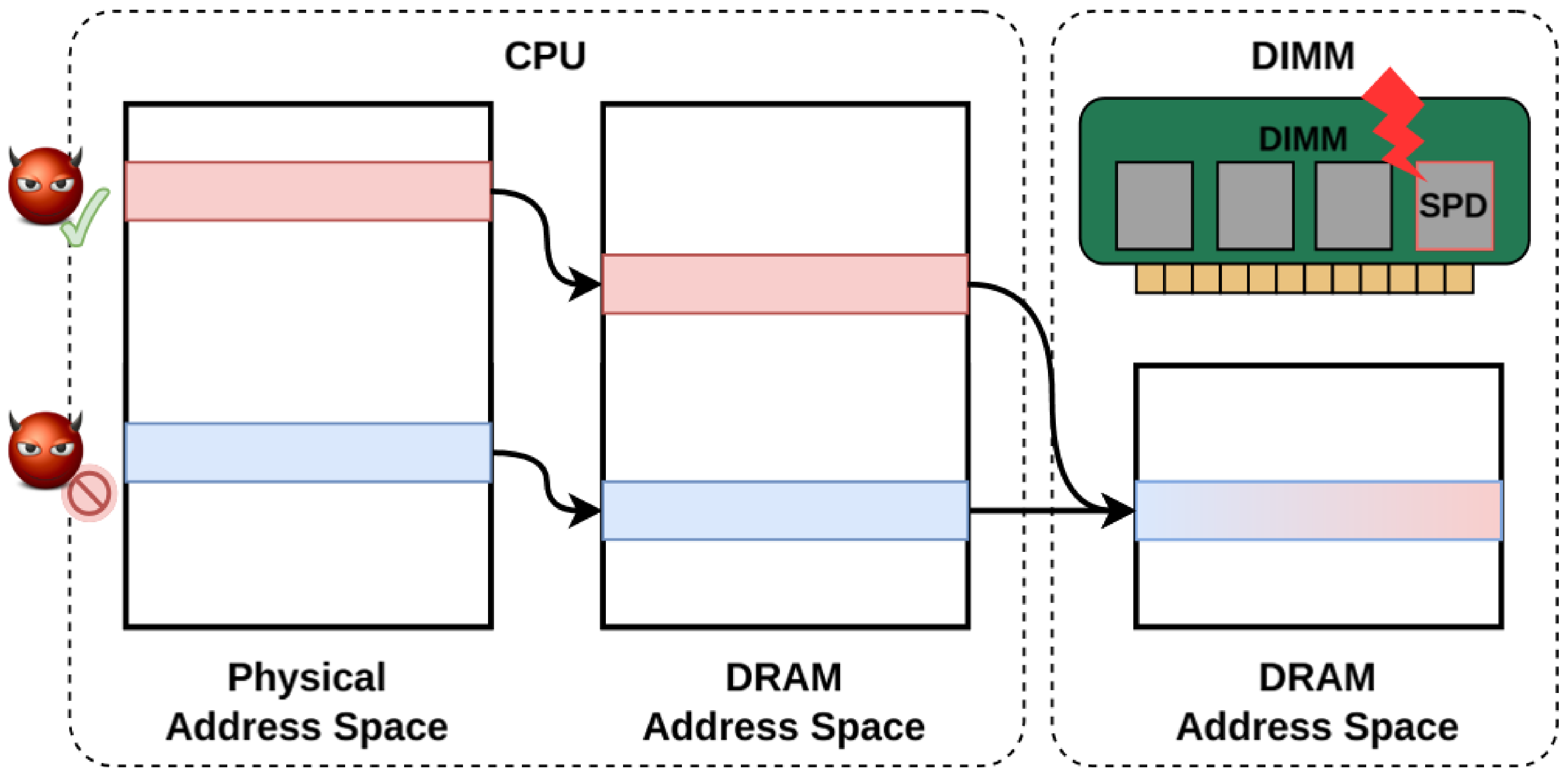
https://badram.eu

Memory isolation in TEEs



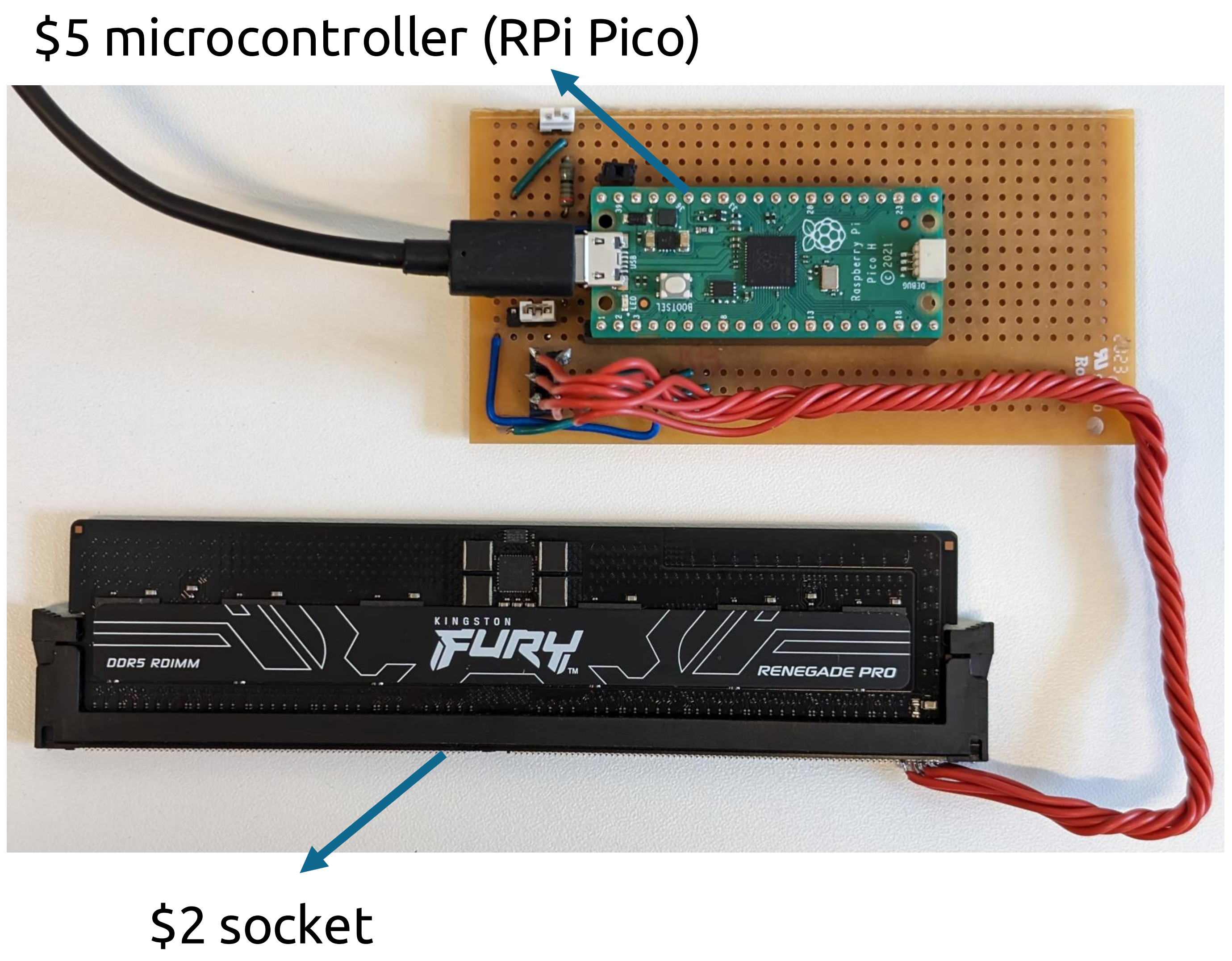
- TEEs ensure **isolation from hypervisor**
- Isolation requires **physical address checks**

Aliasing via malicious DIMM configuration



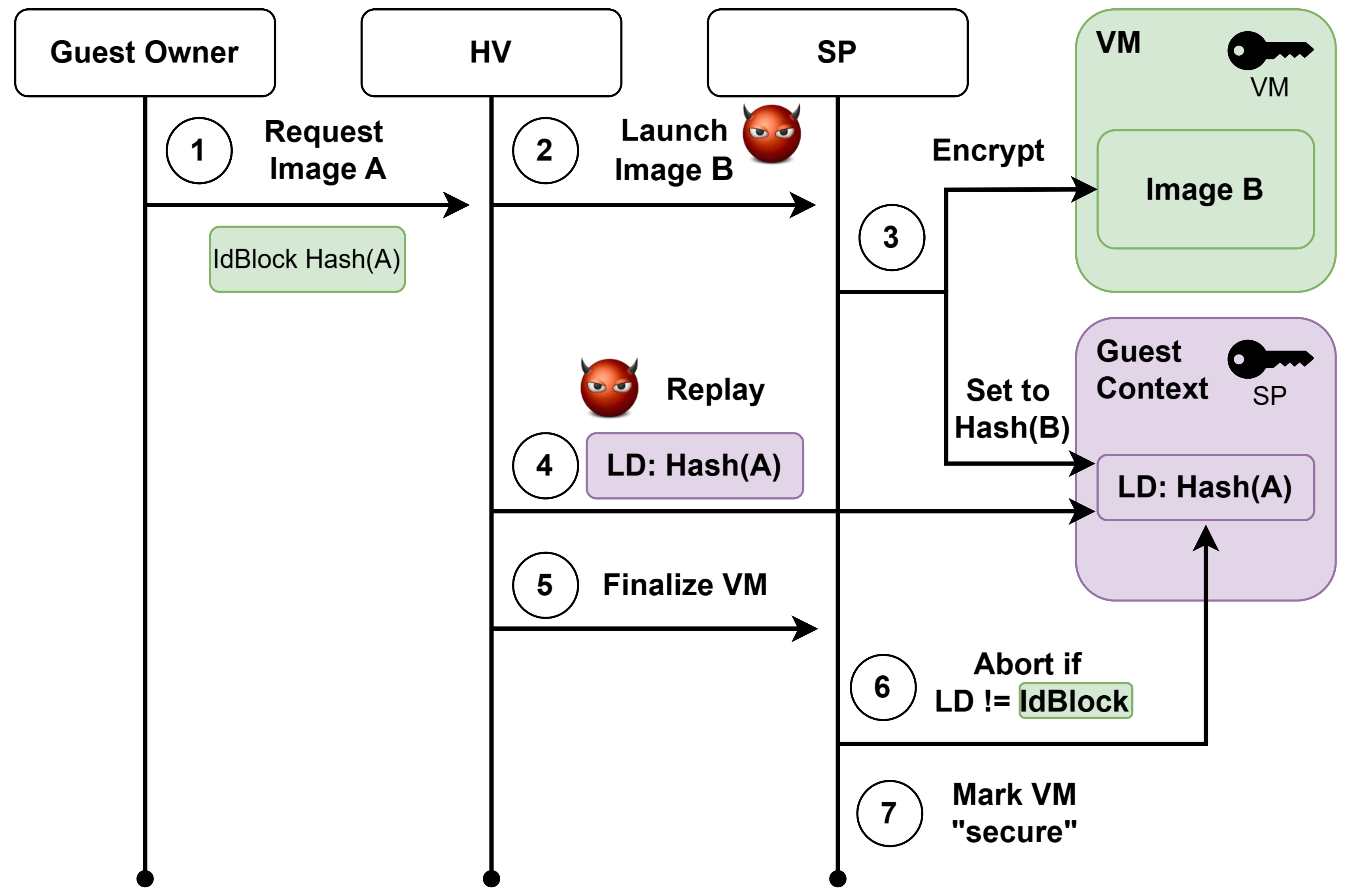
- BIOS configures memory controller
- **Malicious SPD contents** introduces aliases

A $10 hack that erodes trust in the cloud



- **Low-cost setup** for DDR4 and DDR5 DIMMs
- **Open-source** practical SPD tools

Breaking AMD SEV-SNP



- **Static encryption** enables ciphertext replay
- **E2E attack** breaking SEV-SNP's attestation

DRAM trust in TEEs

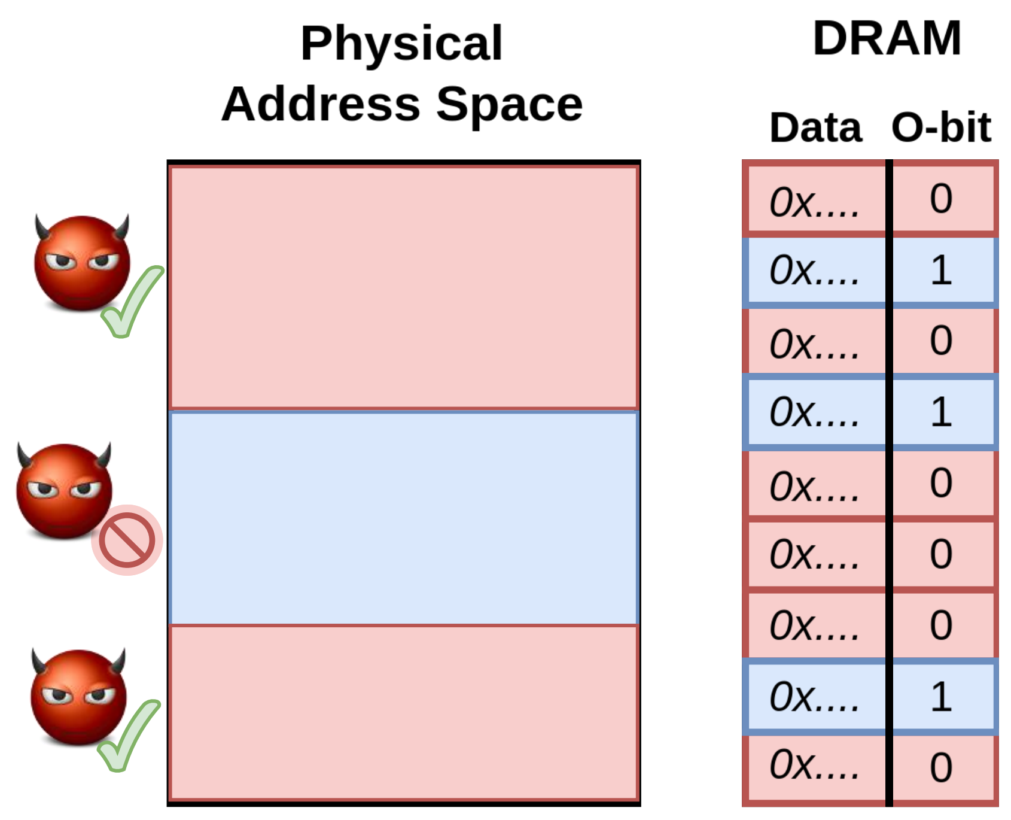
TEE	Encryption	Guarantees		
		Confidentiality	Integrity	Freshness
Classic SGX	AES-CTR	✓	✓	✓
Scalable SGX	AEX-XTS	✓	✗	✗
TDX	AES-XTS	✓	✓	✗
SEV-SNP	AES-XEC	✓	✗	✗
CCA	AES-XEX/ QARMA	✓	✗	✗

- Scalable TEEs **forgo strong crypto**
- Need for **additional aliasing mitigations**

Countermeasures

Deployed Countermeasures
- Boot-time alias check
- ECC-based metadata
  - Owner bit (SGX & TDX)
  - MAC (TDX)

Principled Countermeasures
- Strong Crypto
- Highly Integrated Memory



- **Limited protection** against physical attacks
- Principled mitigations **not deployed**

Published in 46th IEEE Symposium on Security and Privacy (S&P), 2025.

Cyber Security fwo Funded by the European Union erc European Research Council Bundesministerium für Bildung und Forschung