undeSErVed trust

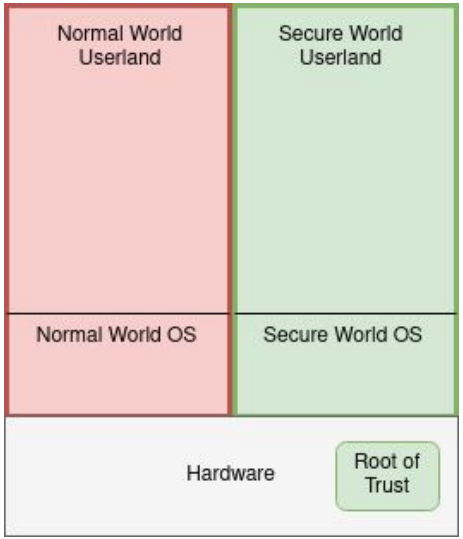
Luca Wilke, Jan Wichelmann, Florian Sieck and Thomas Eisenbarth
University of Lübeck

Exploiting Permutation-Agnostic Remote Attestation

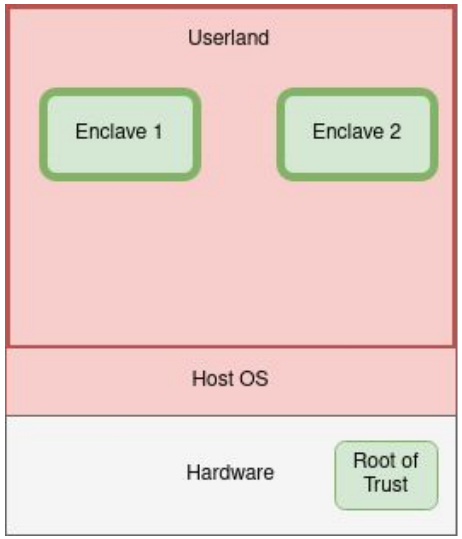
Trusted Execution Environments

Goal: Perform sensitive computation on an untrusted system

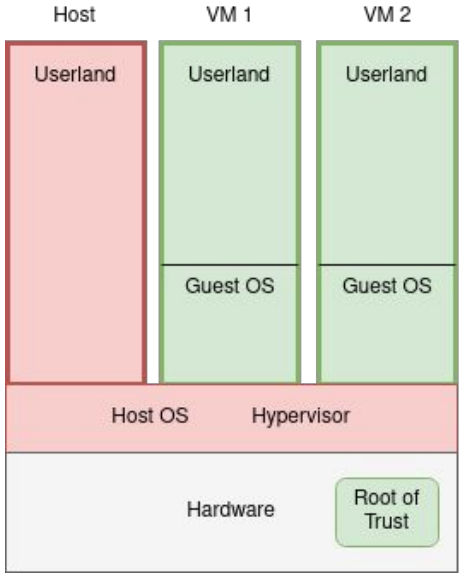
ARM Trustzone



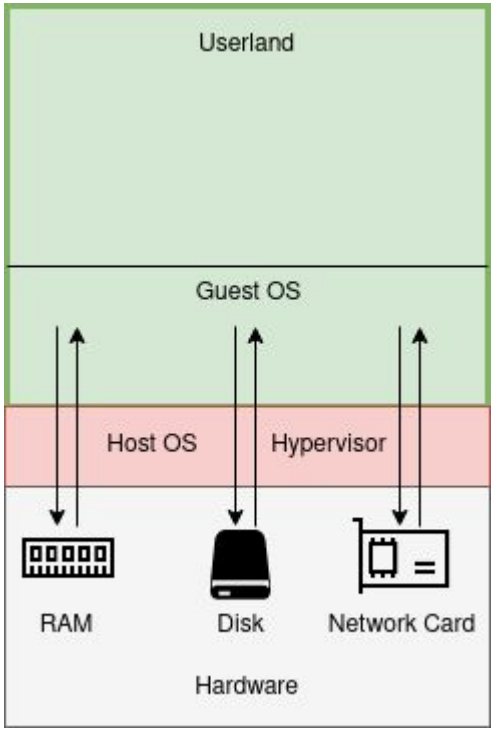
Intel SGX



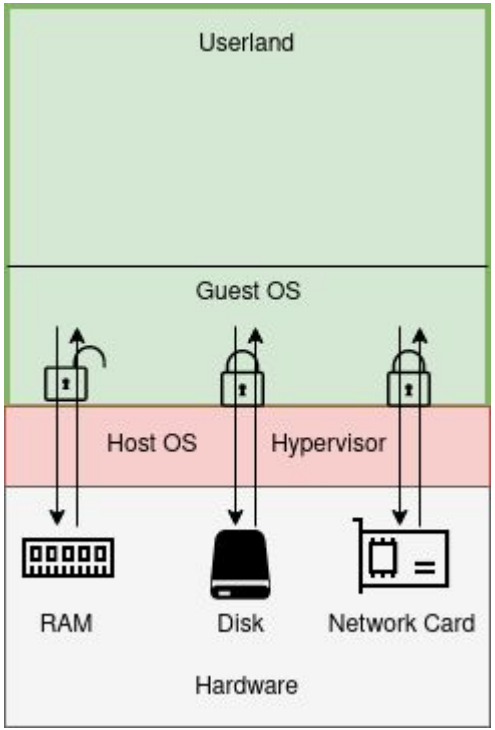
AMD SEV



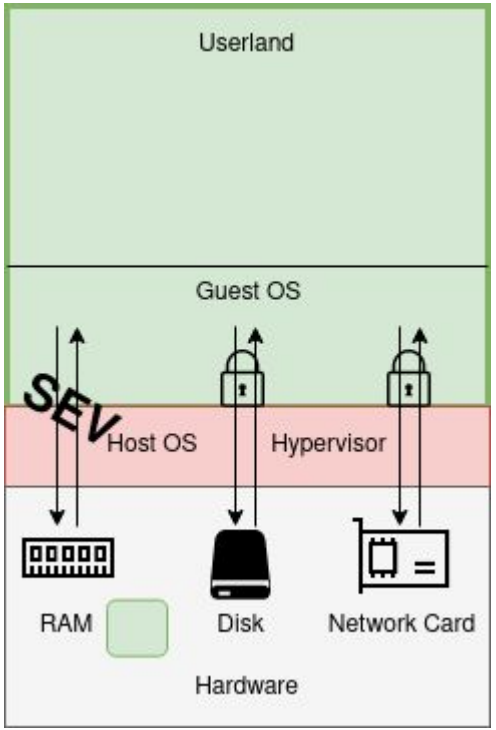
SEV Scenario



SEV Scenario

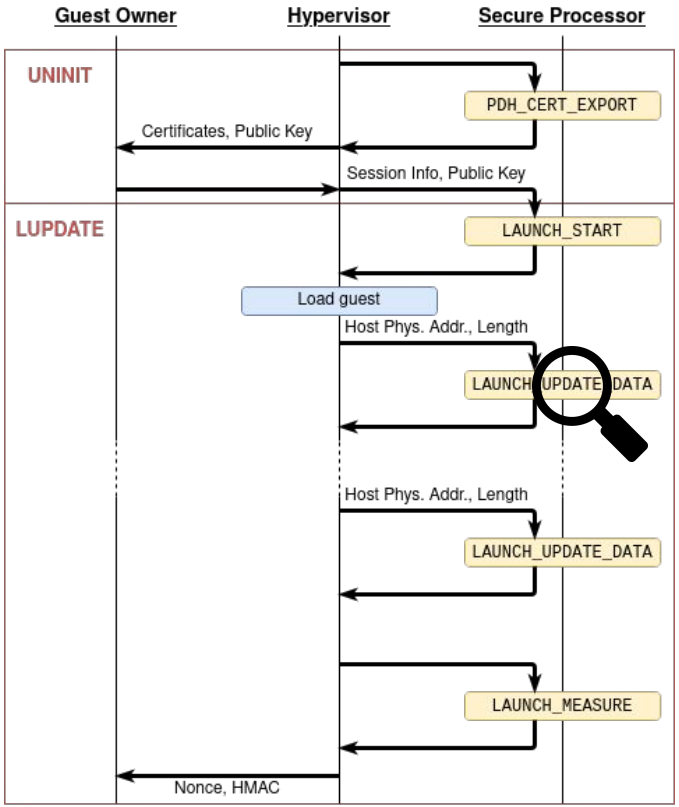


SEV Scenario



Creating SEV VMs : Boot Sequence

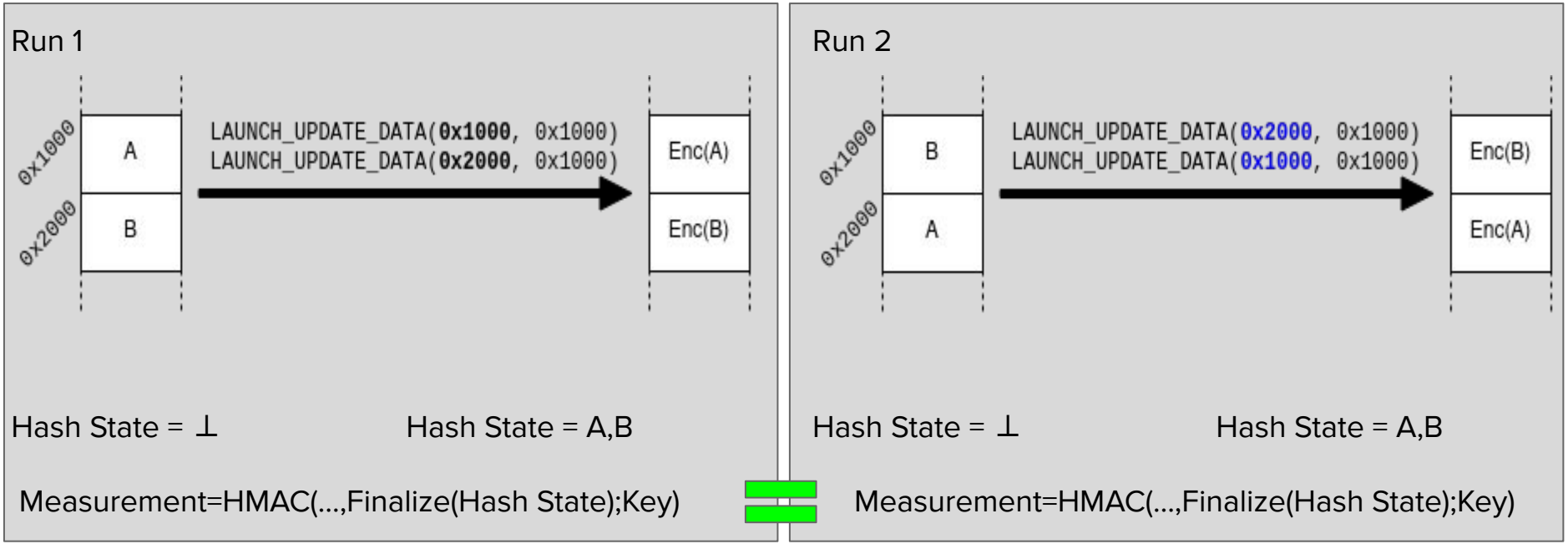
Creating SEV VMs : Load initial code image



Hash State = $\perp$ $\xrightarrow{1}$ Hash State = A $\xrightarrow{2}$ Has State = A,B

Measurement=HMAC(...,Finalize(Hash State);Key)

Creating SEV VMs : Load initial code image

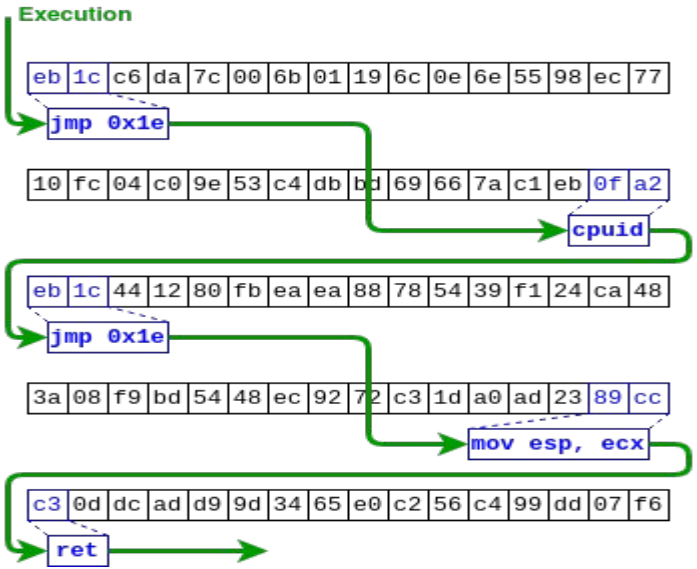


Different VM content, same measurement!
“Block” granularity is as low as 16 bytes

Exploit

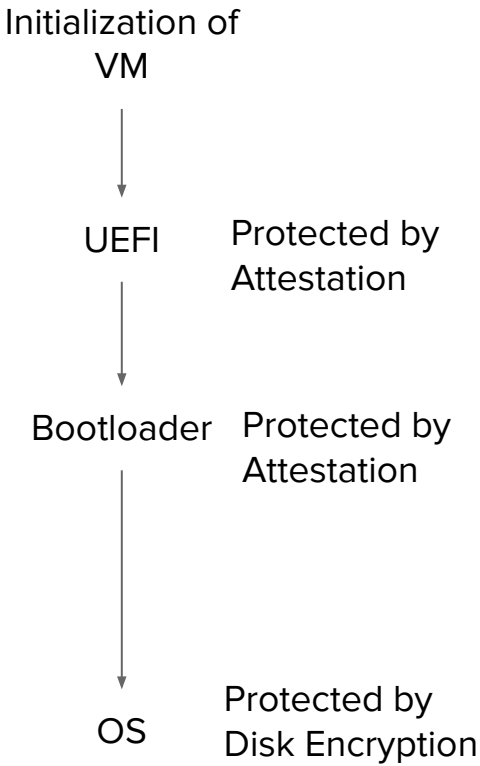
Exploiting Control Over Blocks

1. Reorder initial VM image to create a malicious code gadget
2. Measure and start VM; Owner cannot detect malicious gadget
3. Malicious Gadget maps VM's stack to an unencrypted page
4. Hypervisor writes ROP addresses and payload code onto VM's stack
5. ROP gadgets moves payload to private page and executes it



"Blockchain" produced by reordering the memory blocks

Case Study : Stealing Disk Encryption Keys



Scenario

- SEV only protects RAM; Disk Encryption is done in SW
- Secure Processor has API to securely load secrets into VM's RAM

Attack

Use ROP gadget to move secret from encrypted memory to unencrypted memory

Countermeasures

SEV(-ES)

- Increase minimal size limit for measured blocks during launch
  - Makes exploitation harder
  - Limited to 4096 byte blocks (one page) due to page remapping flaw
- Include addresses of blocks in measurement
  - Can ensure order inside a page but not beyond due to page remapping flaw

SEV(-SNP)

- Page remapping flaw is resolved
- Block size is increased to 4096 bytes (page)
- Addresses included in measurement

Summary

- Attacker Model: Malicious hypervisor
- Attestation of SEV(-ES) does not detect permutations of measured content
  - 16 byte granularity
- Reordering blocks can be used to construct malicious code gadgets
- Case Study: Steal Disk Encryption Keys
- Partial countermeasures for SEV(-ES) possible
- Full mitigation available in SEV-SNP (3rd Gen Epyc only)
- Disclosed to AMD on January 19th, embargo until May 11

CVE-2021-26311

UNIVERSITÄT ZU LÜBECK

uzl-its.github.io/undeserved-trust/

@lucawilkeUzL
@JanWichelmann
@tomcrypt