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**

- Normal World Userland
- Secure World Userland
- Normal World OS
- Secure World OS
- Hardware
- Root of Trust

**Intel SGX**

- Userland
- Enclave 1
- Enclave 2
- Host OS
- Hardware
- Root of Trust

**AMD SEV**

- Userland
- Userland
- Usersland
- Guest OS
- Guest OS
- Host OS
- Hypervisor
- Hardware
- Root of Trust
SEV Scenario
SEV Scenario
SEV Scenario
Creating SEV VMs: Boot Sequence

1. Initialization of VM
2. vCPU jumps to Reset Vector
3. UEFI configures CPU
4. Bootloader
5. OS
Creating SEV VMs: Load initial code image

Hash State = A

Measurement = HMAC(..., Finalize(Hash State); Key)
Creating SEV VMs: Load initial code image

Run 1

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

Run 2

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

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