SEV-SNP-strengthening-vm-isolation-with-integrity-protection-and-more-1e2d0f1f63c9168a575bd487c8c8698b

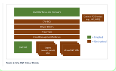
- Secure Encrypted Virtualization (SEV)
  - minimize their exposure to bugs in the cloud provider's infrastructure
  - keep their data confidential
  - isolate VMs at a hardware level
    - individual VMs could be assigned a unique AES encryption key
- SEV-ES (Encrypted State)
  - protection for CPU register state
- SEV-SNP (Secure Nested Paging)
  - memory integrity protection
    - data replay
    - corruption
    - memory re-mapping
    - aliasing based attacks
    - if a VM is able to read a private (encrypted) page of memory, it must always read the value it last wrote
  - stronger protection around interrupt behavior
  - increased protection against recently disclosed side channel attacks
  - requires a combination of new CPU hardware and firmware
  - Threat Model
    - 

      Figure 2: SEV-SNP Threat Model
      - fully trusted
        - AMD Secure Processor (AMD-SP)
        - VM
      - fully untrusted
        - all other CPU software components
          - BIOS on the host system
          - hypervisor
          - device drivers
          - other VMs
        - PCI devices
    - SEV technologies only protect data in-use
    - 

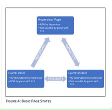
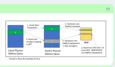
  - Reverse Map Table
    - single data structure shared across the system
    - one entry for every 4k page of DRAM that may be used by VMs
    - tracks the owner for each page of memory
    - in conjunction with standard x86 page tables
    - New CPU instructions exist to enable manipulation of RMP entries
      - PVALIDATE
        - sets the Validated bit
      - RMPUPDATE
        - assigns the page to the guest
      - 

        Figure 4: Basic Page States
      - RMPADJUST
        - allows a given VMPL to modify permissions for a less privileged VMPL
        - restricted so one level cannot grant more permissions than it currently has
    - AMD-V 2-level paging1
      - translate a Guest Virtual Address (GVA) to a Guest Physical Address (GPA)
        - to a System Physical Address (SPA).
      - every SPA can only be mapped to a single GPA at one time.
      - each RMP entry is a Validated bit
      - 

  - Virtual Machine Privilege Levels
    - provide hardware isolated abstraction layers within a VM for additional security controls
    - assistance with managing communication with the hypervisor
    - RMPADJUST
    - allows a guest VM to divide its address space into four levels
    - primarily used to set additional page permission checks and are otherwise orthogonal to other x86 security features
    - VMPL0 is the highest privilege
      - handle #VC events
      - configure which guest memory in another vCPU is private (C=1) versus shared (C=0)
      - intermediary for guest to hypervisor communications
    - VMPL3 is the least privileged
  - Interrupt/Exception Protection
    - restrictive interface between the VM and hypervisor regarding interrupts and exceptions
    - optional modes
      - Restricted Injection
      - Alternate Injection
  - Trusted Platform Information
    - Platform features and capabilities
    - malicious hypervisor can only cause denial-of-service on a guest by lying about CPUID features
    - AMD-SP will verify that the CPUID results that the hypervisor is reporting are no greater than the capabilities of the platform and that security sensitive information
  - TCB Versioning
    - upgradeable firmware components
      - considered trusted
    - AMD-SP version number
      - SEV-SNP

        Versioned Chip Endorsement Key (VCEK)

        unique to each AMD chip
  - VM Launch & Attestation
    - launch digest captures the layout of initial guest memory, as well as its contents
    - guest owner

      signed Identity Block (IDB) to associate with the VM
      - uniquely identify the VM
      - can only be associated with VMs which match the expected launch digest
      - included as part of the attestation report
      - supports more flexible attestation
        - Attestation reports can be requested through a protected path from the AMD-SP by the guest VM at any time
  - VM Migration
    - Migration Agent (MA)
      - MA is itself an SEV-SNP VM
      - single MA can manage migration for an arbitrary number of VMs
      - not required that both the source and destination machines be online at the same time
  - Side Channels
    - hardware capabilities4
    - protection from speculative side channel attacks and SMT
    - not able to protect against all possible side channel attacks
      - PRIME+PROBE
      - it is the responsibility of VM owners to follow standard security practices
      - Modern cryptographic libraries take special care
- shared (unencrypted) memory

- SEV-SNP-strengthening-vm-isolation-with-integrity-protection-and-more-1e2d0f1f63c9168a575bd487c8c8698b
  - Secure Encrypted Virtualization (SEV) ③
    - minimize their exposure to bugs in the cloud provider’s infrastructure ③
    - keep their data confidential ③
    - isolate VMs at a hardware level ③
      - individual VMs could be assigned a unique AES encryption key ③
  - SEV-ES (Encrypted State) ③
    - protection for CPU register state ③
  - SEV-SNP (Secure Nested Paging) ③
    - memory integrity protection ③
      - data replay ③
      - corruption ⑥
      - memory re-mapping ③
      - aliasing based attacks ⑥
      - if a VM is able to read a private (encrypted) page of memory, it must always read the value it last wrote ④
    - stronger protection around interrupt behavior ③
    - increased protection against recently disclosed side channel attacks ③
    - requires a combination of new CPU hardware and firmware ④
    - Threat Model ⑤
      - ⑤

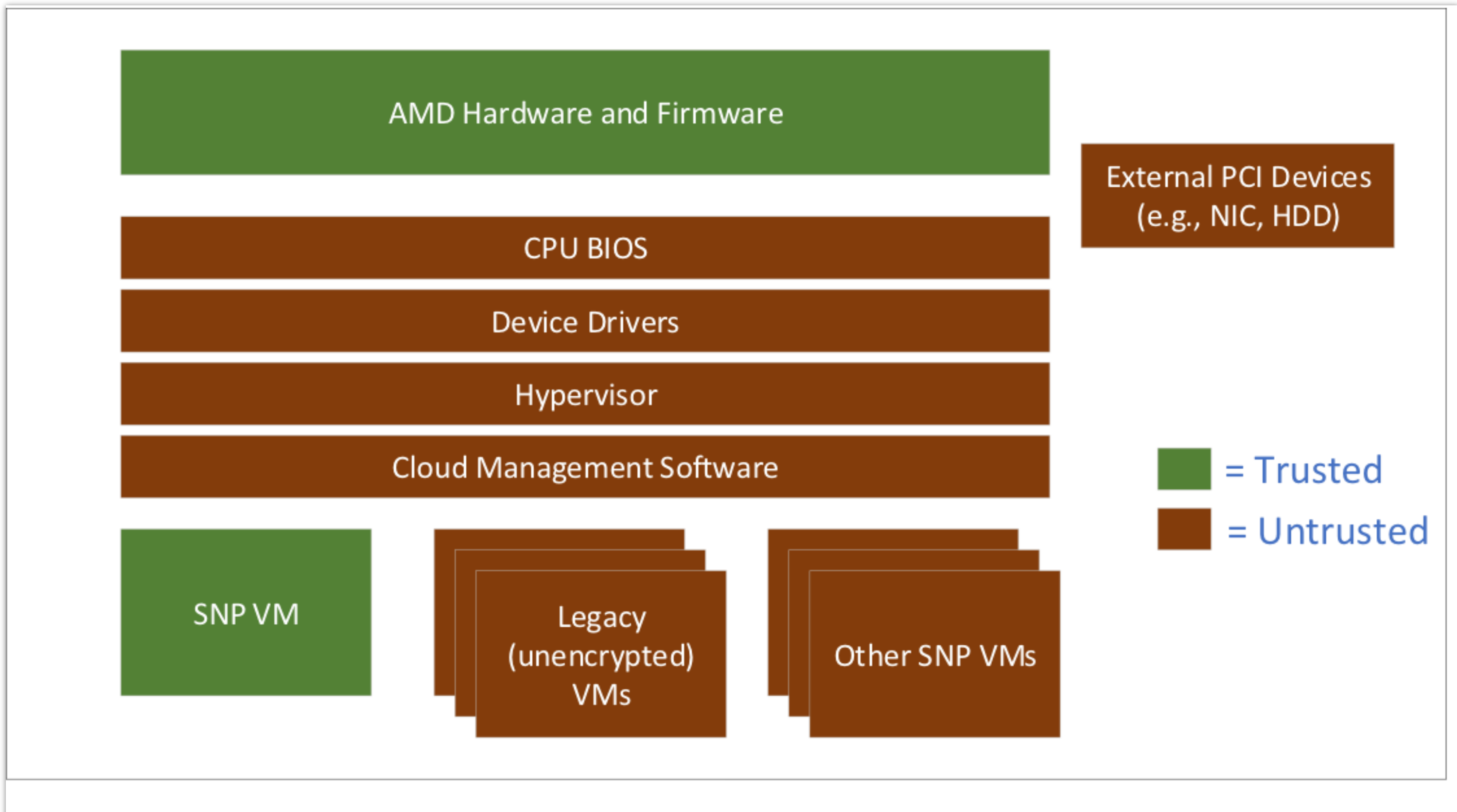


Figure 2: SEV-SNP Threat Model

  - fully trusted ⑤
    - AMD Secure Processor (AMD-SP) ⑤
    - VM ⑤
  - fully untrusted ⑤
    - all other CPU software components ⑤
      - BIOS on the host system ⑤
      - hypervisor ⑤
      - device drivers ⑤
      - other VMs ⑤
    - PCI devices ⑤
- SEV technologies only protect data in-use ⑤
- ⑦

✓ = Mitigated ★ = Optionally Mitigated ⊘ = Not Mitigated

Potential Threats	*SEV*	*SEV-ES*	*SEV-SNP*
Confidentiality			
VM Memory *Example attack: Hypervisor reads private VM memory*	✓	✓	✓
VM Register State *Example attack: Read VM register state after VMEXIT*	⊘	✓	✓
DMA Protection *Example attack: Device attempts to read VM memory*	✓	✓	✓
Integrity			
Replay Protection *Example attack: Replace VM memory with an old copy*	⊘	⊘	✓
Data Corruption *Example attack: Replace VM memory with junk data*	⊘	⊘	✓
Memory Aliasing *Example attack: Map two guest pages to same DRAM page*	⊘	⊘	✓
Memory Re-Mapping *Example attack: Switch DRAM page mapped to a guest page*	⊘	⊘	✓
Availability			
Denial of Service on Hypervisor *Example attack: Malicious guest refuses to yield/exit*	✓	✓	✓
Denial of Service on Guest *Example attack: Malicious hypervisor refuses to run guest*	⊘	⊘	⊘
Physical Access Attacks			
Offline DRAM analysis *Example attack: Cold boot*	✓	✓	✓
Active DRAM corruption *Example attack: Manipulate DDR bus while VM is running*	⊘	⊘	⊘
Misc.			
TCB Rollback *Example attack: Revert AMD-SP firmware to old version*	⊘	⊘	✓
Malicious Interrupt/Exception Injection *Example attack: Inject interrupt while RFLAGS.IF=0*	⊘	⊘	★
Indirect Branch Predictor Poisoning *Example attack: Poison BTB from hypervisor*	⊘	⊘	★
Secure Hardware Debug Registers *Example attack: Change breakpoints during debug*	⊘	⊘	★
Trusted CPUID Information *Example attack: Hypervisors lies about platform capabilities*	⊘	⊘	★
Architectural Side Channels *Example attack: PRIME+PROBE to track VM accesses*	⊘	⊘	⊘
Page-level Side Channels *Example attack: Track VM access patterns through page tables*	⊘	⊘	⊘
Performance Counter Tracking *Example attack: Fingerprint VM apps by performance data*	⊘	⊘	⊘

TABLE 1: THREAT MODEL

- Reverse Map Table 8
  - single data structure shared across the system 8
  - one entry for every 4k page of DRAM that may be used by VMs 8
  - tracks the owner for each page of memory 8
  - in conjunction with standard x86 page tables 8
  - New CPU instructions exist to enable manipulation of RMP entries 9
    - PVALIDATE 10
      - sets the Validated bit 10
    - RMPUPDATE 10
      - assigns the page to the guest 10
    - 10

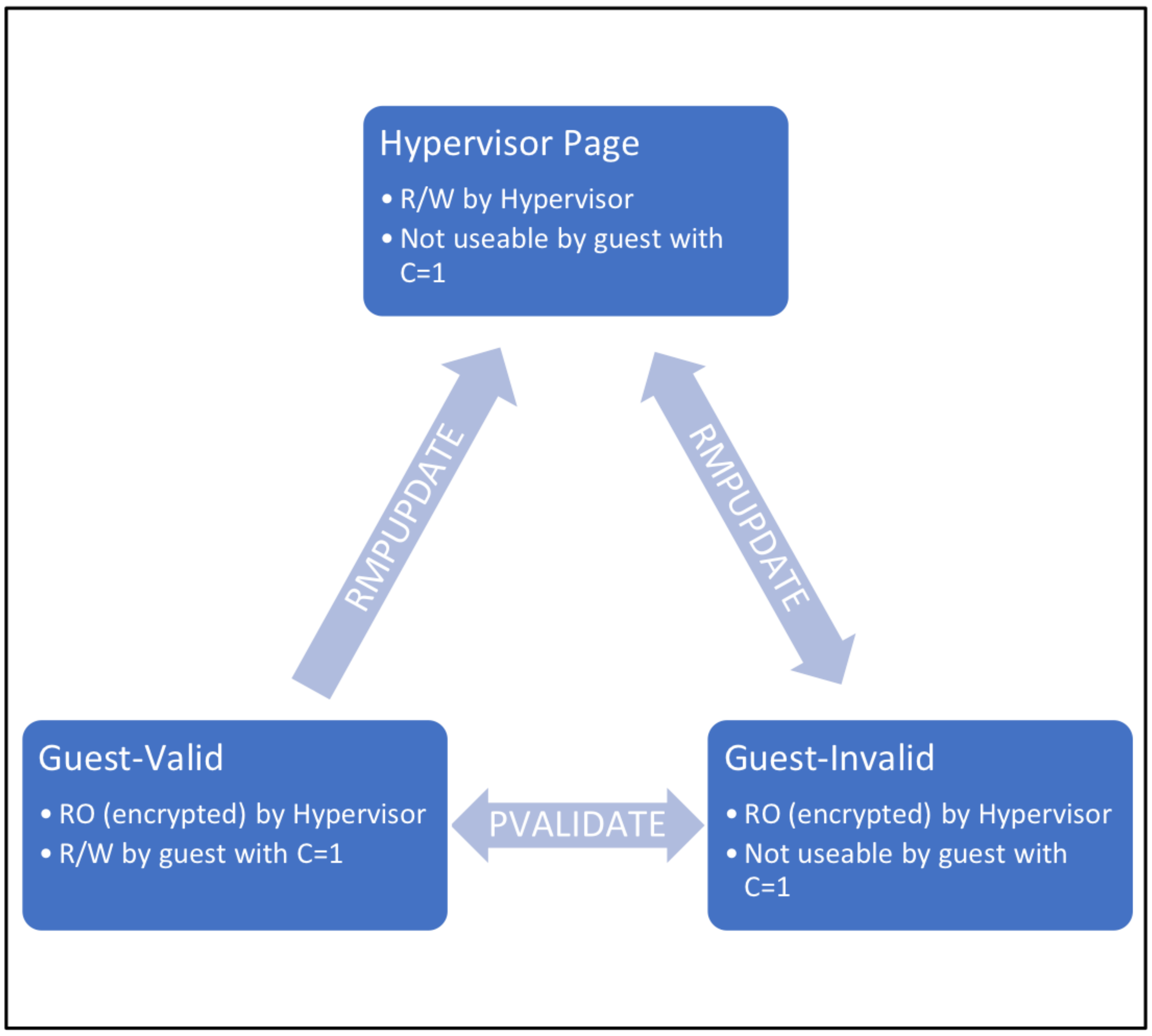
      

      FIGURE 4: BASIC PAGE STATES
    - RMPADJUST 13
      - allows a given VMPL to modify permissions for a less privileged VMPL 13
      - restricted so one level cannot grant more permissions than it currently has 13
  - AMD-V 2-level paging1 9

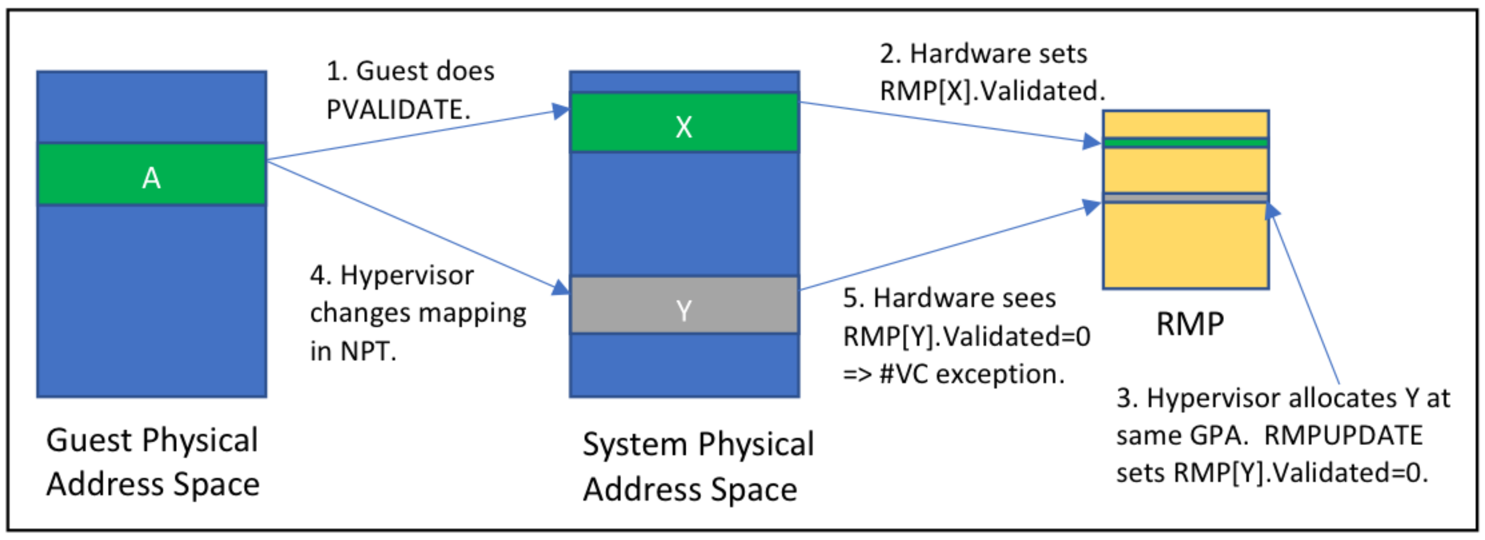
    - translate a Guest Virtual Address (GVA) to a Guest Physical Address (GPA) ⑨
      - to a System Physical Address (SPA). ⑨
    - every SPA can only be mapped to a single GPA at one time. ⑩
    - each RMP entry is a Validated bit ⑩
    - 

      FIGURE 5: PAGE RE-MAPPING ATTACK ⑪
- Virtual Machine Privilege Levels ⑬
  - provide hardware isolated abstraction layers within a VM for additional security controls ⑬
  - assistance with managing communication with the hypervisor ⑬
  - RMPADJUST ⑬
  - allows a guest VM to divide its address space into four levels ⑬
  - primarily used to set additional page permission checks and are otherwise orthogonal to other x86 security features ⑬
  - VMPL0 is the highest privilege ⑬
    - handle #VC events ⑭
    - configure which guest memory in another vCPU is private (C=1) versus shared (C=0) ⑭
    - intermediary for guest to hypervisor communications ⑭
  - VMPL3 is the least privileged ⑬
- Interrupt/Exception Protection ⑮
  - restrictive interface between the VM and hypervisor regarding interrupts and exceptions ⑮
  - optional modes ⑮
    - Restricted Injection ⑮

    - Alternate Injection ⑮
- Trusted Platform Information ⑯
  - Platform features and capabilities ⑯
  - malicious hypervisor can only cause denial-of-service on a guest by lying about CPUID features ⑯
  - AMD-SP will verify that the CPUID results that the hypervisor is reporting are no greater than the capabilities of the platform and that security sensitive information ⑯
- TCB Versioning ⑯
  - upgradeable firmware components ⑯
    - considered trusted ⑯
  - AMD-SP version number ⑯
    - SEV-SNP ⑯

      Versioned Chip Endorsement Key (VCEK)

      unique to each AMD chip
- VM Launch & Attestation ⑰
  - launch digest captures the layout of initial guest memory, as well as its contents ⑰
  - guest owner ⑰

    signed Identity Block (IDB) to associate with the VM
    - uniquely identify the VM ⑰
    - can only be associated with VMs which match the expected launch digest ⑰
    - included as part of the attestation report ⑰
    - supports more flexible attestation ⑰
      - Attestation reports can be requested through a protected path from the AMD-SP by the guest VM at any time ⑰
- VM Migration ⑱
  - Migration Agent (MA) ⑱
    - MA is itself an SEV-SNP VM ⑱
    - single MA can manage migration for an arbitrary number of VMs ⑱

      - not required that both the source and destination machines be online at the same time ⑱
  - Side Channels ⑲
    - hardware capabilities4 ⑲
    - protection from speculative side channel attacks and SMT ⑲
    - not able to protect against all possible side channel attacks ⑲
      - PRIME+PROBE ⑲
      - it is the responsibility of VM owners to follow standard security practices ⑳
      - Modern cryptographic libraries take special care ⑲
- shared (unencrypted) memory ④