Enabling AMD SEV in Xen

Xen Summit, 2024

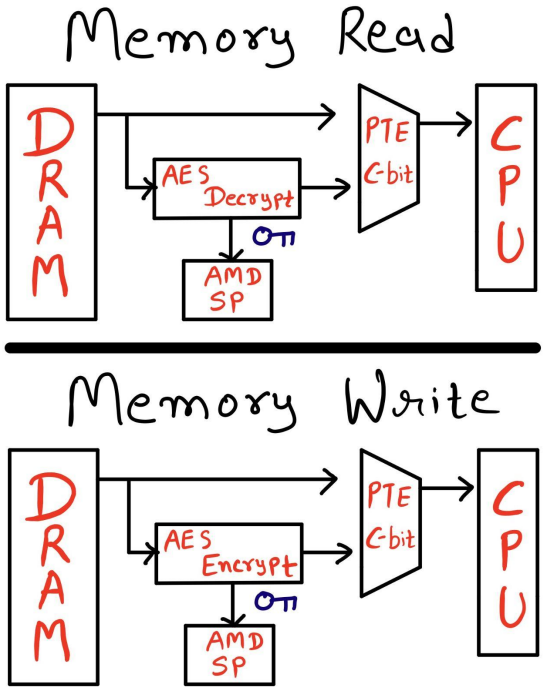
Vaishali Thakkar(she/her)
(Mastadon:@vaishali@hachyderm.io)
(vaishali.thakkar@vates.tech)

Agenda

- Overview of AMD Memory Encryption Technologies
- How AMD SEV works?
- AMD SEV and Xen
- Conclusion

AMD Memory Encryption Technologies

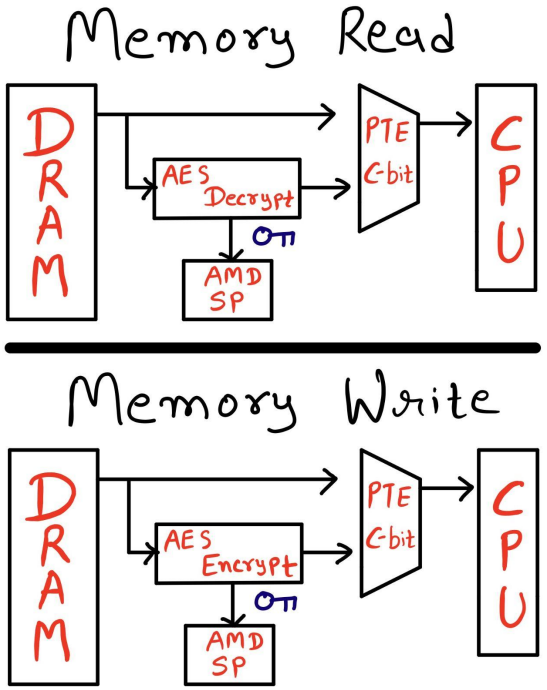
- **AMD Secure Memory Encryption [SME]**
  - Hardware AES engine located in the memory controller



AMD Memory Encryption Technologies

❖ AMD Secure Memory Encryption [SME]

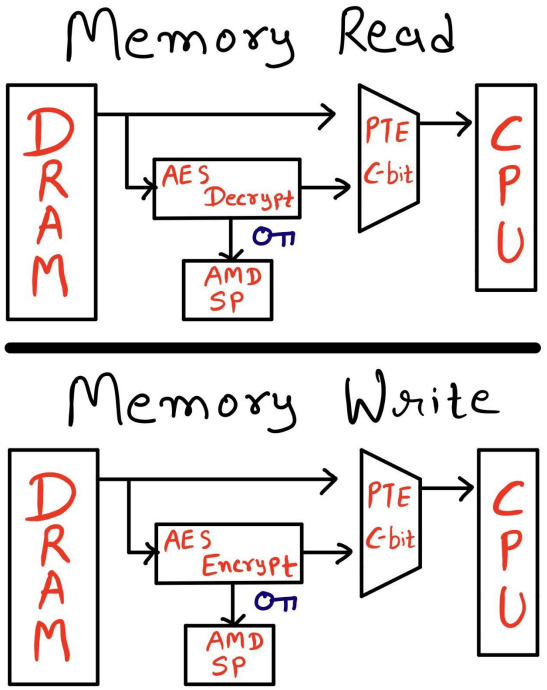
- ➢ Hardware AES engine located in the memory controller
- ➢ 128-bit encryption key, managed by AMD - SP



AMD Memory Encryption Technologies

❖ AMD Secure Memory Encryption [SME]

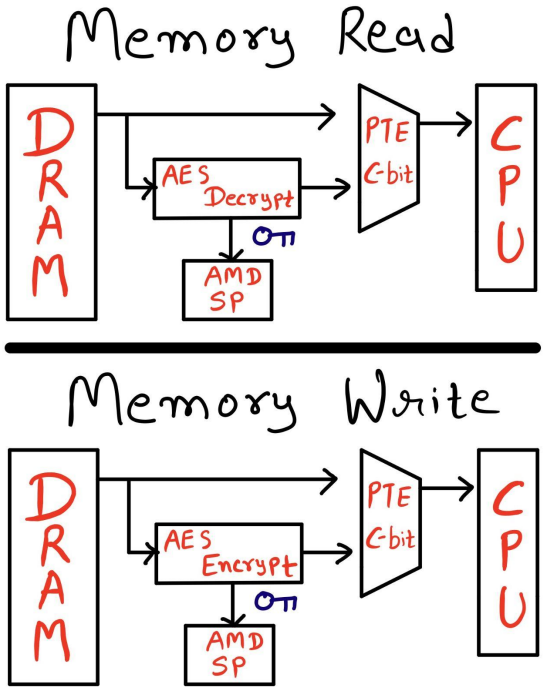
- ➢ Hardware AES engine located in the memory controller
- ➢ 128-bit encryption key, managed by AMD - SP
- ➢ C-bit to mark the encryption of pages



AMD Memory Encryption Technologies

❖ AMD Secure Memory Encryption [SME]

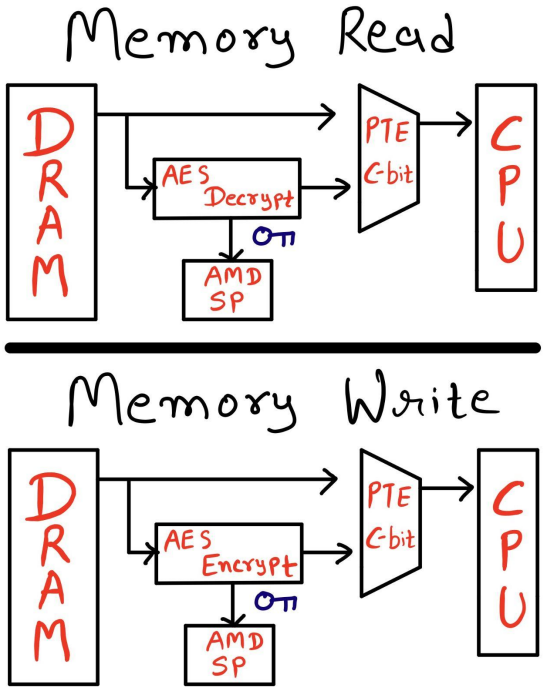
- ➢ Hardware AES engine located in the memory controller
- ➢ 128-bit encryption key, managed by AMD - SP
- ➢ C-bit to mark the encryption of pages
- ➢ Useful for full or partial(guest VMs) memory encryption



AMD Memory Encryption Technologies

❖ AMD Secure Memory Encryption [SME]

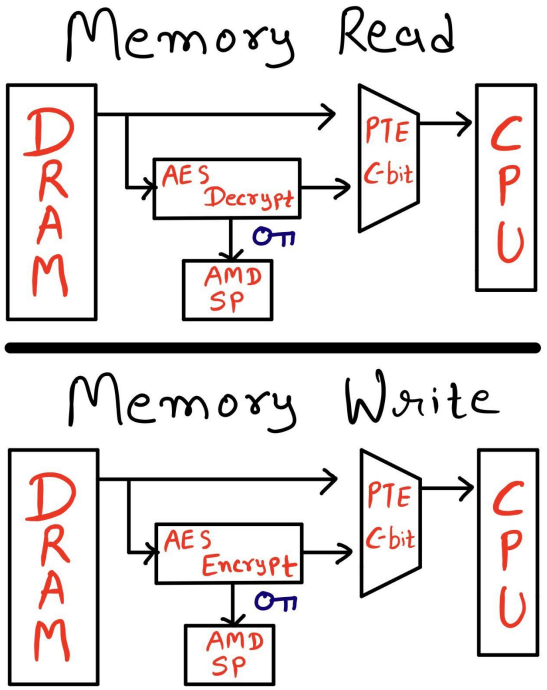
- ➢ Hardware AES engine located in the memory controller
- ➢ 128-bit encryption key, managed by AMD - SP
- ➢ C-bit to mark the encryption of pages
- ➢ Useful for full or partial(guest VMs) memory encryption
- ➢ Transparent SME (TSME)



AMD Memory Encryption Technologies

❖ AMD Secure Memory Encryption [SME]

- ➢ Hardware AES engine located in the memory controller
- ➢ 128-bit encryption key, managed by AMD - SP
- ➢ C-bit to mark the encryption of pages
- ➢ Useful for full or partial(guest VMs) memory encryption
- ➢ Transparent SME (TSME)
- ➢ AMD SME Demo



AMD Memory Encryption Technologies

- **AMD Secure Encrypted Virtualization[SEV]**
  - Integrates memory encryption with AMD-V

AMD Memory Encryption Technologies

- **AMD Secure Encrypted Virtualization[SEV]**
  - Integrates memory encryption with AMD-V
  - Built around the idea of secure sandbox environments

AMD Memory Encryption Technologies

- **AMD Secure Encrypted Virtualization[SEV]**
  - Integrates memory encryption with AMD-V
  - Built around the idea of secure sandbox environments
  - Tags all the code and data with VM ASID

AMD Memory Encryption Technologies

- **AMD Secure Encrypted Virtualization[SEV]**
  - Integrates memory encryption with AMD-V
  - Built around the idea of secure sandbox environments
  - Tags all the code and data with VM ASID
  - Single key per VM, different key for hypervisor

AMD Memory Encryption Technologies

- **AMD Secure Encrypted Virtualization[SEV]**
  - Integrates memory encryption with AMD-V
  - Built around the idea of secure sandbox environments
  - Tags all the code and data with VM ASID
  - Single key per VM, different key for hypervisor
  - Same encryption engine as SME & C-bit to mark encrypted pages

AMD Memory Encryption Technologies

- **AMD Secure Encrypted Virtualization[SEV]**
  - Integrates memory encryption with AMD-V
  - Built around the idea of secure sandbox environments
  - Tags all the code and data with VM ASID
  - Single key per VM, different key for hypervisor
  - Same encryption engine as SME & C-bit to mark encrypted pages
  - Some restrictions on data in shared pages

AMD Memory Encryption Technologies

- **AMD SEV - Encrypted State (SEV-ES)**
  - To protect guest VM from attacks on it’s register state

AMD Memory Encryption Technologies

- **AMD SEV - Encrypted State (SEV-ES)**
  - To protect guest VM from attacks on it’s register state
  - Register state protected with guest encryption key

AMD Memory Encryption Technologies

- **AMD SEV - Encrypted State (SEV-ES)**
  - To protect guest VM from attacks on it’s register state
  - Register state protected with guest encryption key
  - Guest must explicitly share register state with the hypervisor

AMD Memory Encryption Technologies

- **AMD SEV - Encrypted State (SEV-ES)**
  - To protect guest VM from attacks on it’s register state
  - Register state protected with guest encryption key
  - Guest must explicitly share register state with the hypervisor
  - Integrity check on the saved register state

AMD Memory Encryption Technologies

- **AMD SEV - Encrypted State (SEV-ES)**
  - To protect guest VM from attacks on it's register state
  - Register state protected with guest encryption key
  - Guest must explicitly share register state with the hypervisor
  - Integrity check on the saved register state
  - White paper on AMD SEV-ES

AMD Memory Encryption Technologies

- **AMD SEV - Secure Nested Paging (SEV-SNP)**
  - Designed to prevent software-based integrity attacks

AMD Memory Encryption Technologies

- **AMD SEV - Secure Nested Paging (SEV-SNP)**
  - Designed to prevent software-based integrity attacks
  - Integrity guarantees offered through RMP

AMD Memory Encryption Technologies

- **AMD SEV - Secure Nested Paging (SEV-SNP)**
  - Designed to prevent software-based integrity attacks
  - Integrity guarantees offered through RMP
  - RMP tracks the owner of each page

AMD Memory Encryption Technologies

- **AMD SEV - Secure Nested Paging (SEV-SNP)**
  - Designed to prevent software-based integrity attacks
  - Integrity guarantees offered through RMP
  - RMP tracks the owner of each page
  - Virtual machine Privilege Levels

AMD Memory Encryption Technologies

- **AMD SEV - Secure Nested Paging (SEV-SNP)**
  - Designed to prevent software-based integrity attacks
  - Integrity guarantees offered through RMP
  - RMP tracks the owner of each page
  - Virtual machine Privilege Levels
  - Supported starting in 3rd generation AMD EPYC

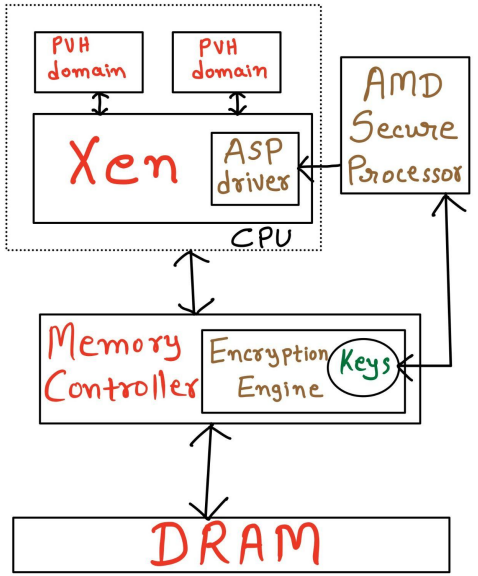
AMD Memory Encryption Technologies

- **AMD SEV - Secure Nested Paging (SEV-SNP)**
  - Designed to prevent software-based integrity attacks
  - Integrity guarantees offered through RMP
  - RMP tracks the owner of each page
  - Virtual machine Privilege Levels
  - Supported starting in 3rd generation AMD EPYC
  - AMD SEV/SEV-ES/SEV-SNP Enablement Plan

How AMD SEV works?

❖ AMD SEV Architecture

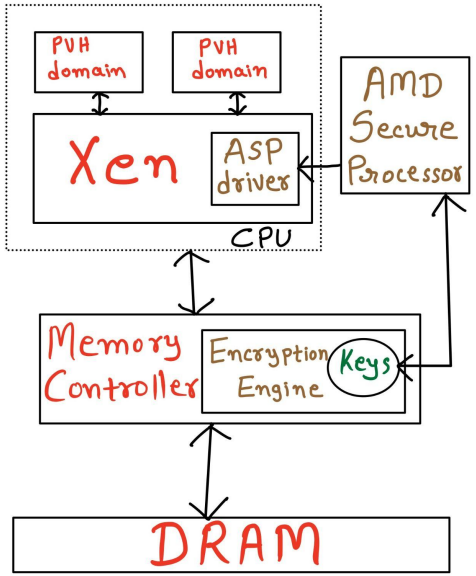
- ➢ AMD Secure Processor



How AMD SEV works?

❖ AMD SEV Architecture

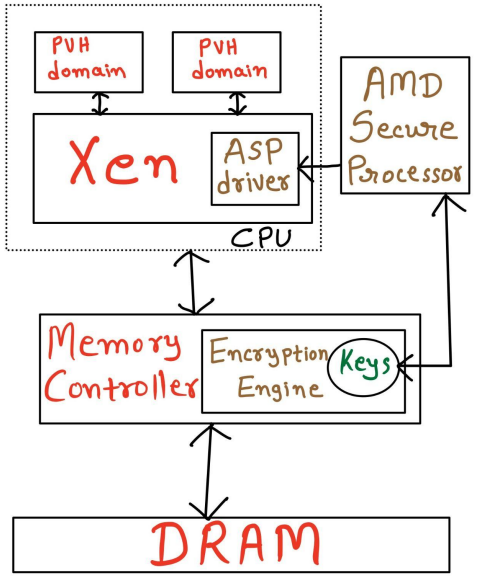
- ➢ AMD Secure Processor
- ➢ Min supported keys: CPUID Fn8000_001F[EDX]
- ➢ Max supported keys: CPUID Fn8000_001F[ECX]



How AMD SEV works?

❖ AMD SEV Architecture

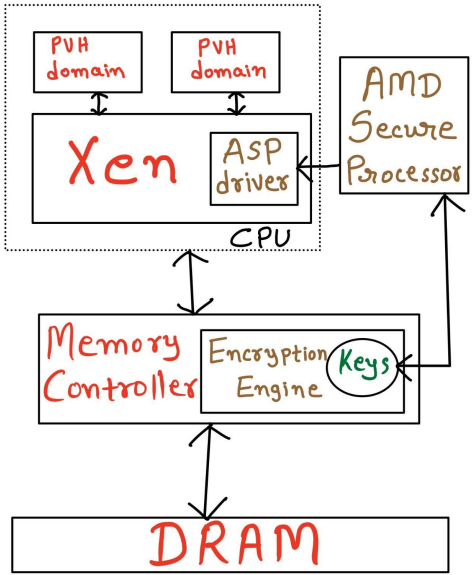
- ➢ AMD Secure Processor
- ➢ Min supported keys: CPUID Fn8000_001F[EDX]
- ➢ Max supported keys: CPUID Fn8000_001F[ECX]
- ➢ Instruction code pages & guest page tables always private



How AMD SEV works?

❖ AMD SEV Architecture

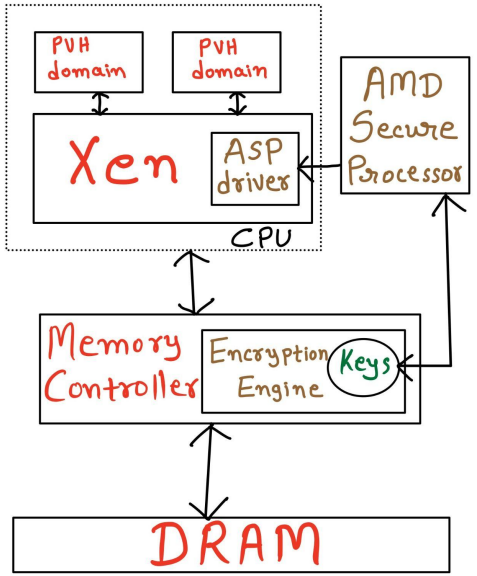
- ➢ AMD Secure Processor
- ➢ Min supported keys: CPUID Fn8000_001F[EDX]
- ➢ Max supported keys: CPUID Fn8000_001F[ECX]
- ➢ Instruction code pages & guest page tables always private
- ➢ Data pages can be private or shared



How AMD SEV works?

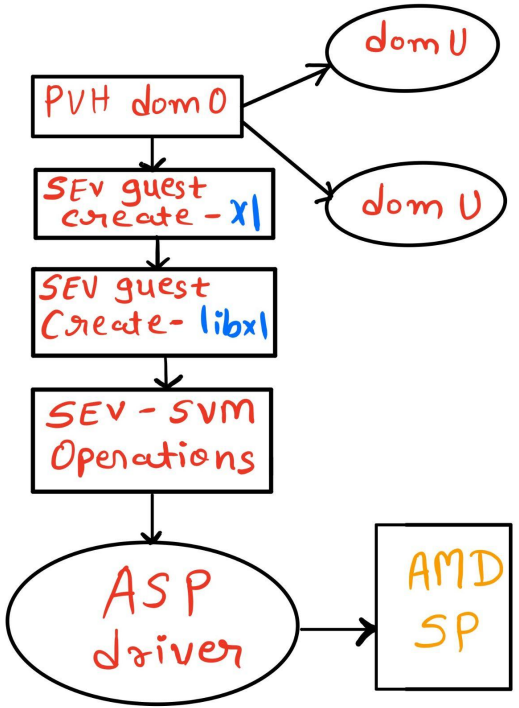
❖ AMD SEV Architecture

- ➢ AMD Secure Processor
- ➢ Min supported keys: CPUID Fn8000_001F[EDX]
- ➢ Max supported keys: CPUID Fn8000_001F[ECX]
- ➢ Instruction code pages & guest page tables always private
- ➢ Data pages can be private or shared
- ➢ All DMA must occur to shared pages



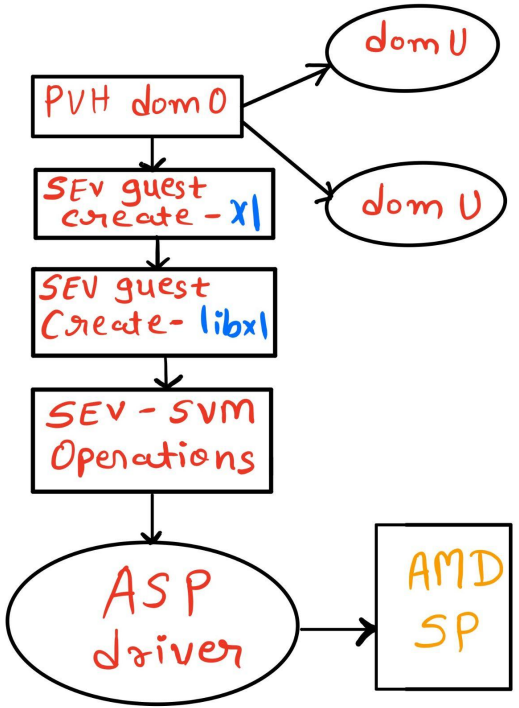
Enablement of SEV in Xen

- **AMD SEV Architecture and Xen:**
  - AMD Secure processor driver



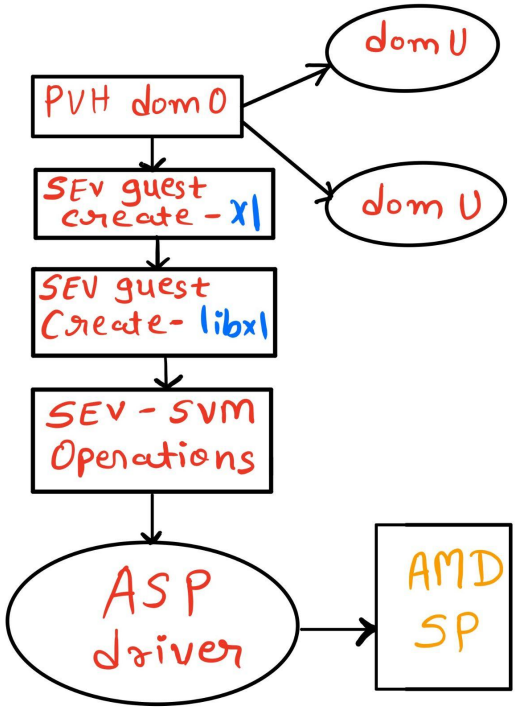
Enablement of SEV in Xen

- **AMD SEV Architecture and Xen:**
  - AMD Secure processor driver
    - Platform Management cycle



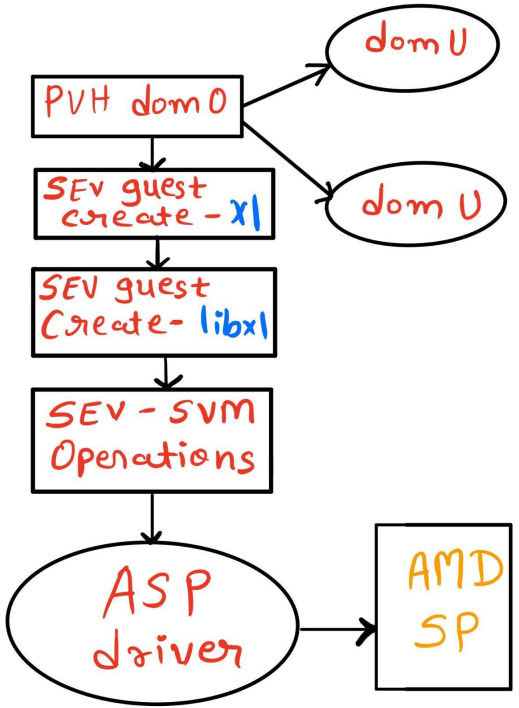
Enablement of SEV in Xen

- **AMD SEV Architecture and Xen:**
  - AMD Secure processor driver
    - Platform Management cycle
    - Guest management lifecycle



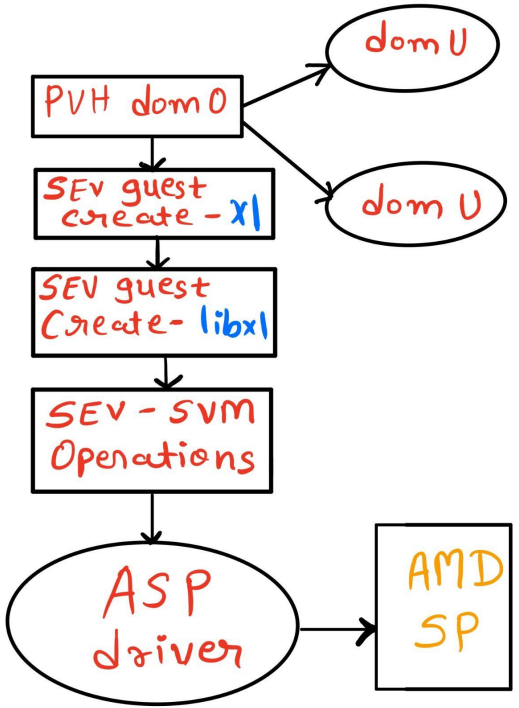
Enablement of SEV in Xen

- **AMD SEV Architecture and Xen:**
  - AMD Secure processor driver
  - SVM operations for SEV commands



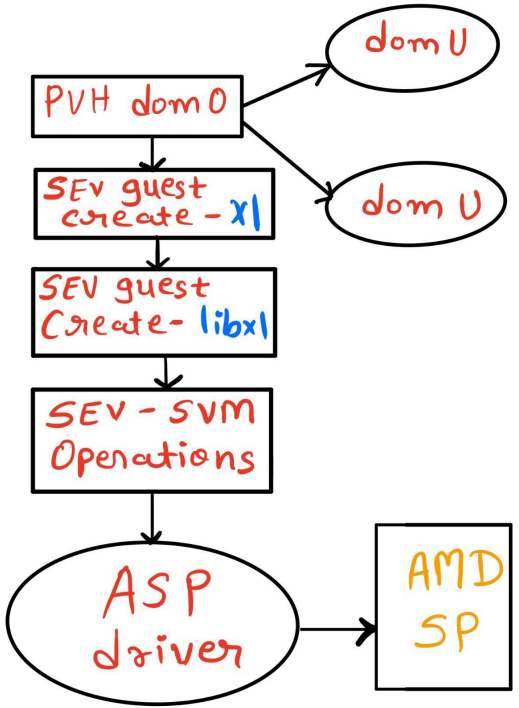
Enablement of SEV in Xen

- **AMD SEV Architecture and Xen:**
  - AMD Secure processor driver
  - SVM operations for SEV commands
  - Libxl



Enablement of SEV in Xen

- **AMD SEV Architecture and Xen:**
  - AMD Secure processor driver
  - SVM operations for SEV commands
  - Libxl
  - Xl



Upstream status

- RFC for implementing AMD Secure Processor (ASP) driver (Andrei)
  - Infrastructure improvements for AMD SEV and SVM leaves (Andrew)
- RFC for introducing the xen-wide ASID allocator (Vaishali)

Questions?

References

- AMD SME and SEV white paper
- Talk by Brijesh from AMD @ Xen Summit, 2016
- Blogpost on how ASID allocator works in Xen
- AMD architecture manual: Section 15.34
- AMD ASP Firmware code