Latest Implementation of AMD SEV-SNP in OVMF

r1chard-lyu
SUSE Labs Developer for EFI
FOSDEM 2025

Whoami

Richard Lyu

Taipei, Taiwan

Work at SUSE

SUSE Labs Developer for EFI

Maintain **OVMF** in SLES and openSUSE

Overview

- **Background**
  - Confidential Computing
  - AMD SEV-SNP
  - OVMF
- **Upstream Status**
  - AMD SEV-SNP in Open Source
  - Commits
- **Integration in Virtualization**
  - Integration
  - SEV Driver

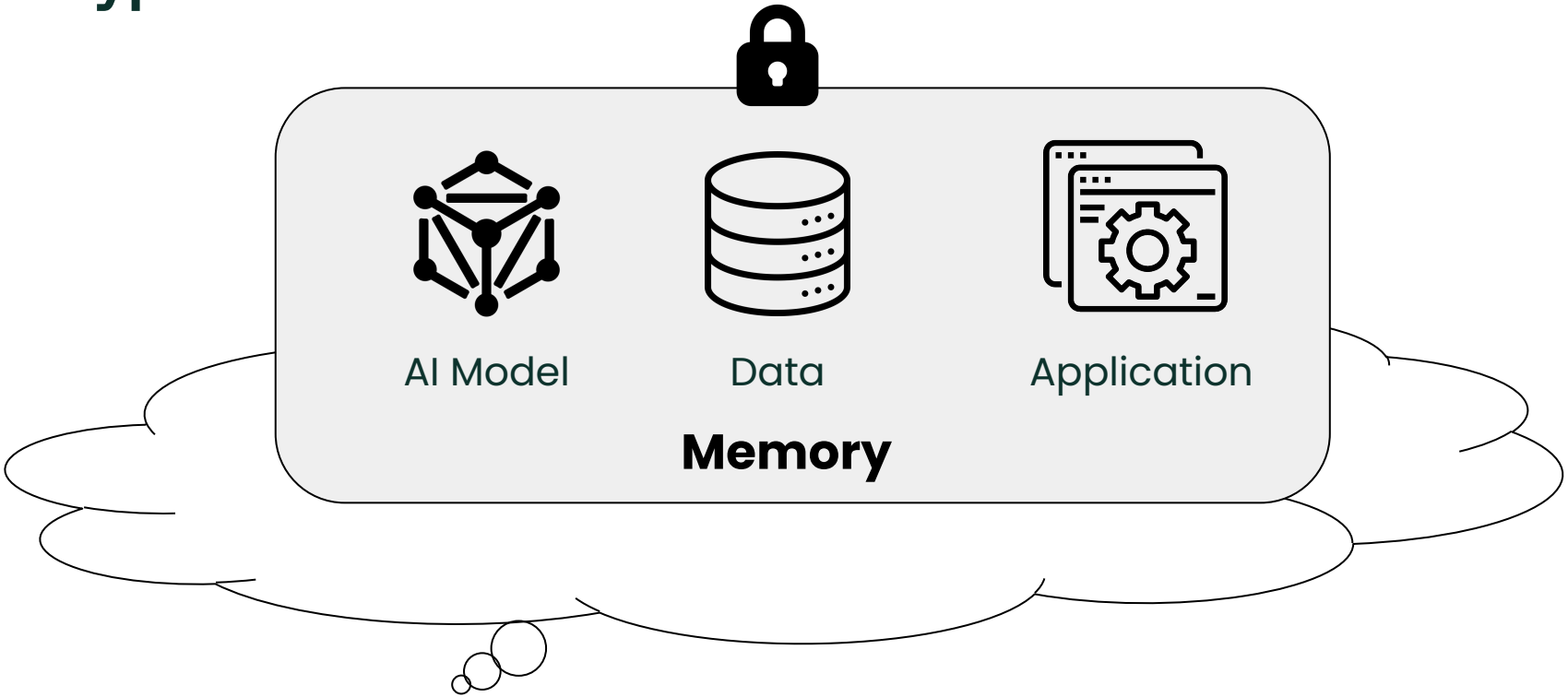
SUSE

SUSE

Background

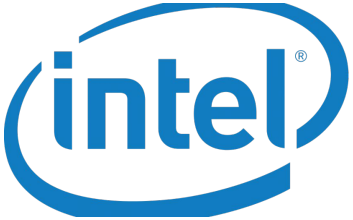
Confidential Computing

Encryption



Providers

- Require a combination of hardware and software



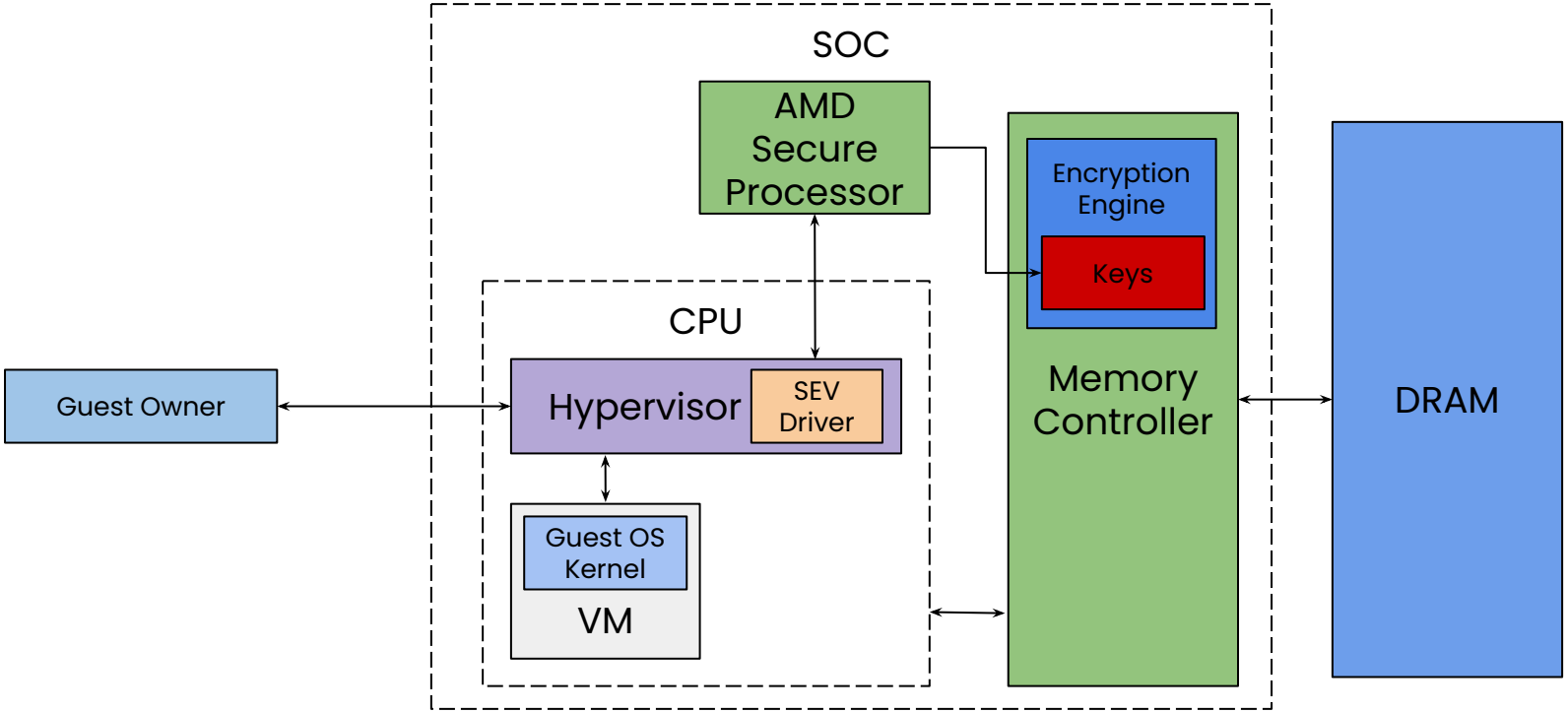
- Delivered with cloud providers or server manufacturers

AMD SEV-SNP

Key Features

- Memory Encryption
- Nested Paging
- Integrity Protection
- Key Management and Attestation

SEV Architecture



OVMF

What is OVMF?

- Open-source UEFI firmware for virtual machines.
- Part of Tianocore's EDK II project.

Key Features:

- UEFI-compliant boot environment.
- Works with QEMU/KVM.
- Simplifies UEFI app development.

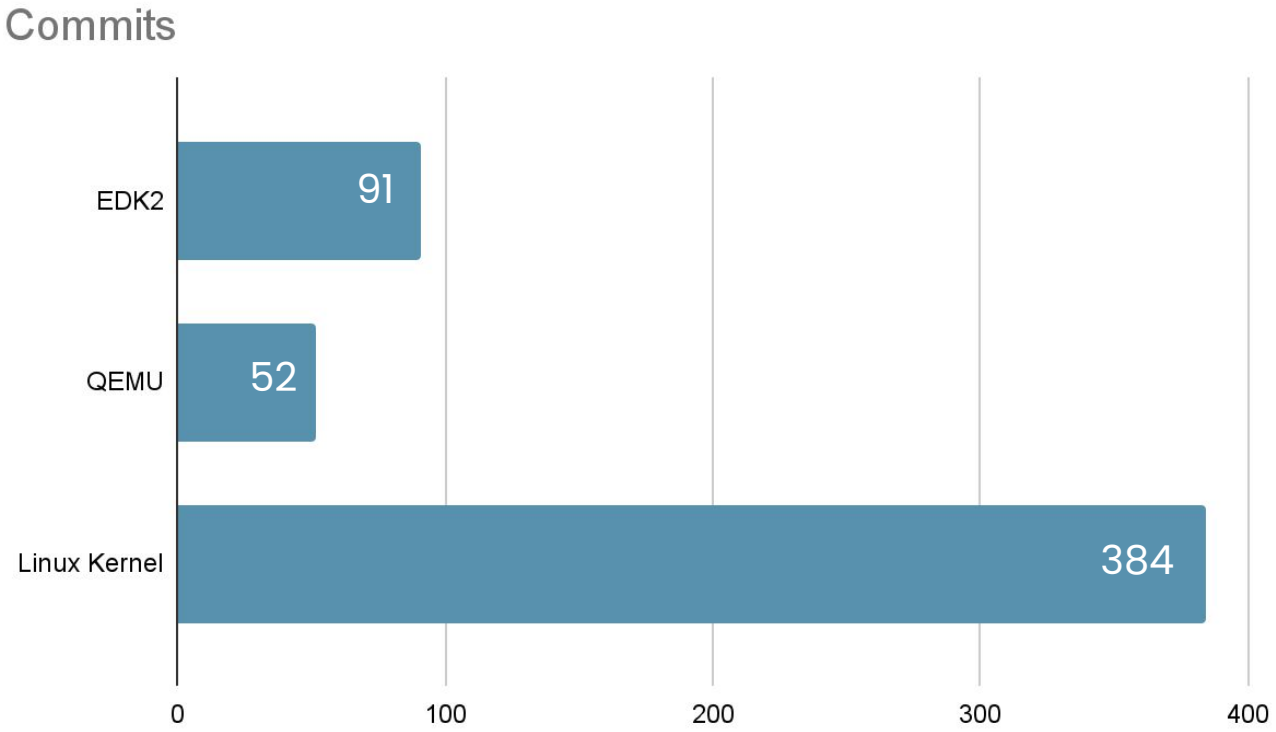
SUSE

Upstream Status

AMD SEV-SNP in Open Source

Technology	Features	EDK2	QEMU	Linux
SEV	Memory encryption	>= edk2-stable201808	>= 2.12	>= 4.15
SEV-ES	Memory encryption + CPU state encryption	>= edk2-stable202008	>= 6.0	>= 5.10
SEV-SNP	Memory encryption + CPU state encryption + Memory integrity protection	>= edk2-stable202405	>= 9.10	>= 6.11

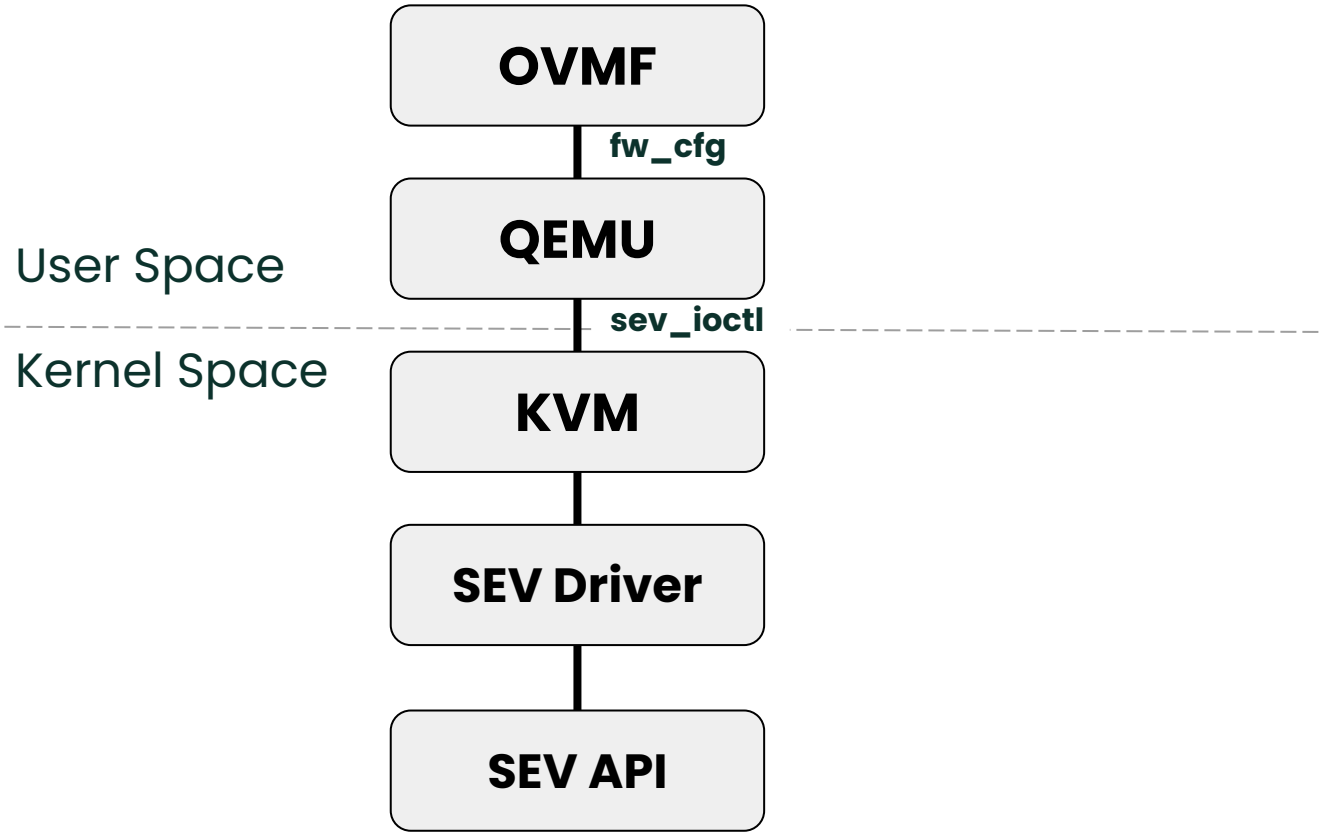
Commits



SUSE

Integration in Virtualization

Integration



SEV Driver

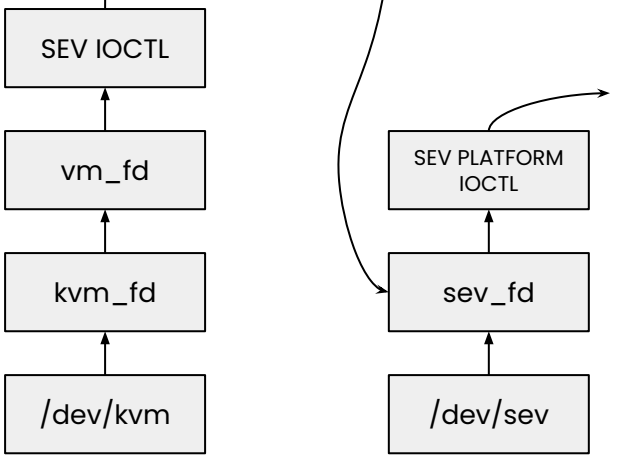
```
struct kvm_sev_cmd {
        __u32 id;
        __u32 pad0;
        __u64 data;
        __u32 error;
        __u32 sev_fd;
};
```

```
/* Secure Encrypted Virtualization command */
enum sev_cmd_id {
        /* Guest initialization commands */
        KVM_SEV_INIT = 0,
        KVM_SEV_ES_INIT,
        /* Guest launch commands */
        KVM_SEV_LAUNCH_START,
        KVM_SEV_LAUNCH_UPDATE_DATA,
        KVM_SEV_LAUNCH_UPDATE_VMSA,
    …
        KVM_SEV_NR_MAX,
};
```

```
struct sev_issue_cmd {
        __u32 cmd;              /* In */
        __u64 data;             /* In */
        __u32 error;            /* Out */
} __packed;
```

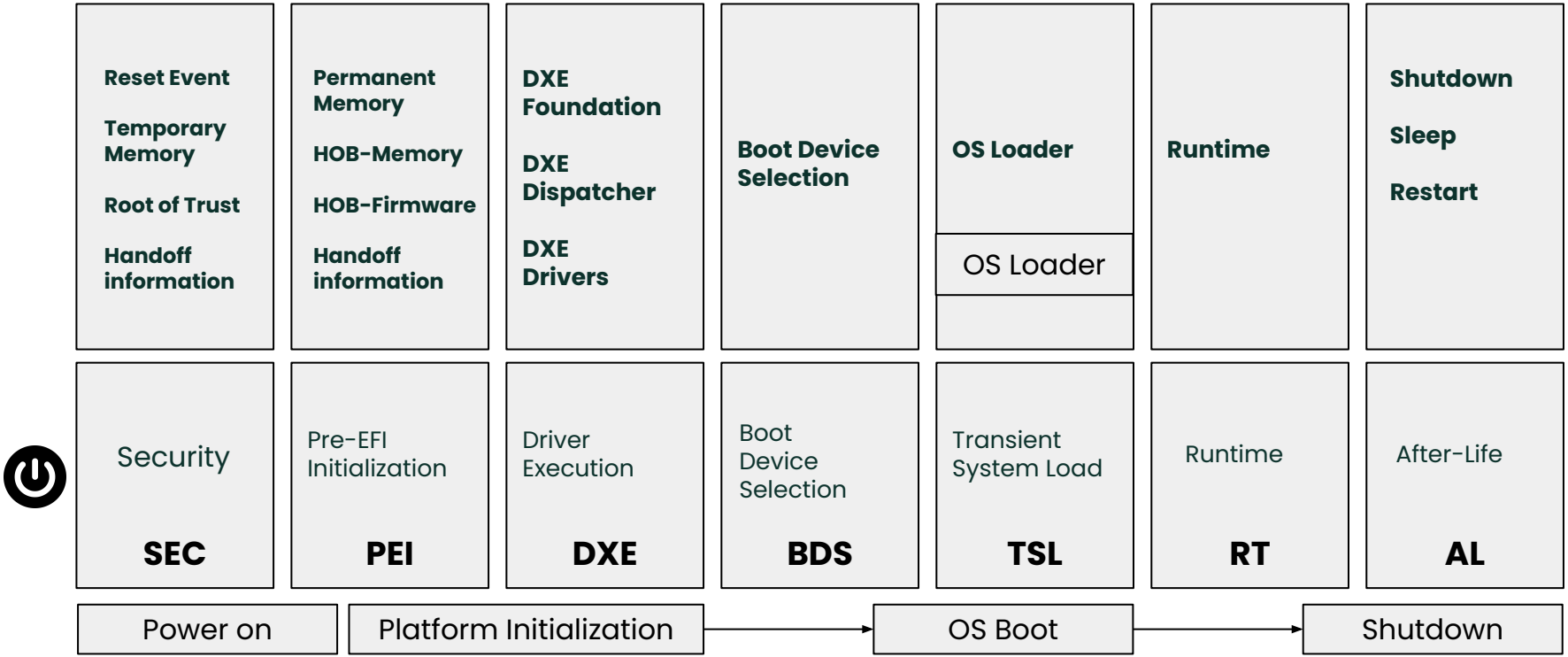
```
/**
 * SEV platform commands
 */
enum {
        SEV_FACTORY_RESET = 0,
        SEV_PLATFORM_STATUS,
        SEV_PEK_GEN,
        SEV_PEK_CSR,
        SEV_PDH_GEN,
        SEV_PDH_CERT_EXPORT,
        SEV_PEK_CERT_IMPORT,
        SEV_GET_ID,     /* This command is
deprecated, use SEV_GET_ID2 */
        SEV_GET_ID2,
        SNP_PLATFORM_STATUS,
        SNP_COMMIT,
        SNP_SET_CONFIG,
        SNP_VLEK_LOAD,

        SEV_MAX,
};
```

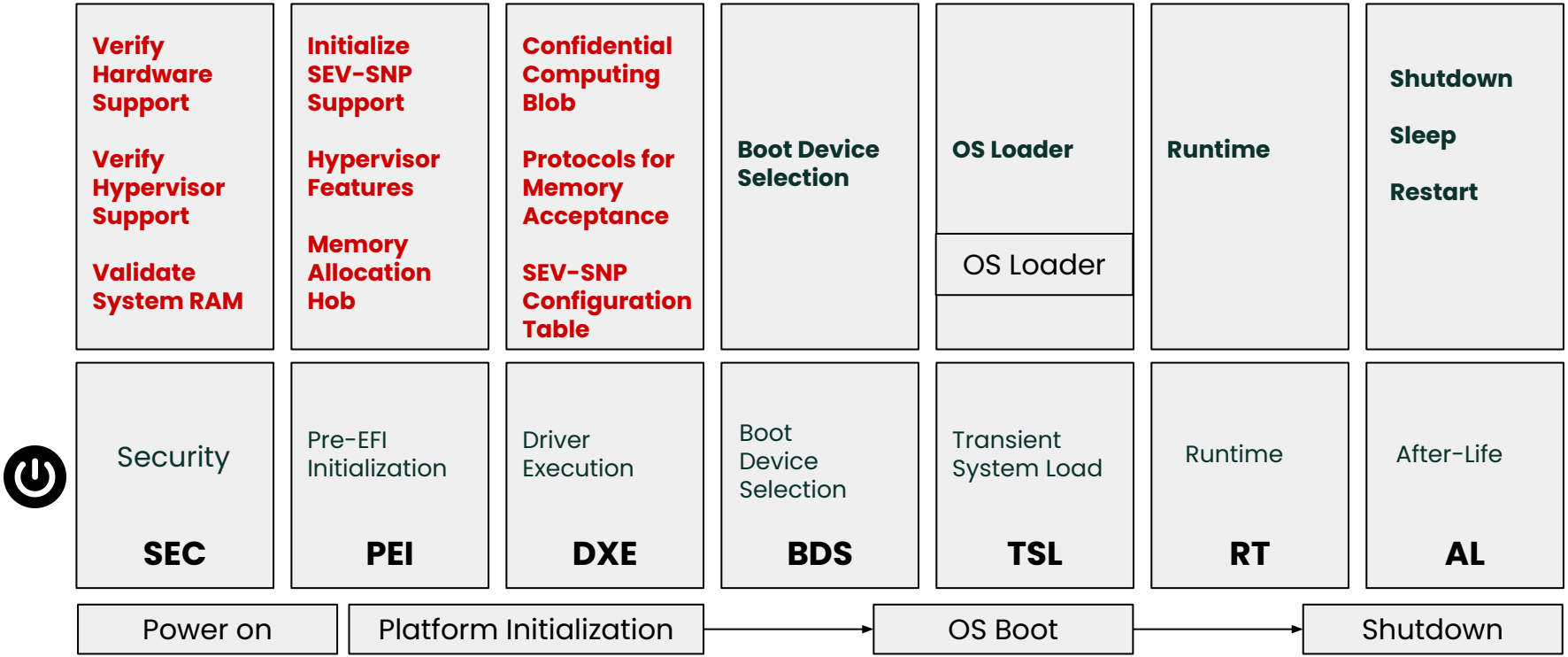


SUSE

PI Architecture Firmware Phases



PI Architecture Firmware Phases



SUSE

Thank You!

Q&A

Reference

[1] AMD64 Architecture Programmer's Manual Volume 2: System Programming
https://www.amd.com/content/dam/amd/en/documents/processor-tech-docs/programmer-references/24593.pdf
[2] AMD64 Architecture Programmer's Manual Volume 3: General-Purpose and System Instructions
https://www.amd.com/content/dam/amd/en/documents/processor-tech-docs/programmer-references/24594.pdf
[3] AMD-V™ Nested Paging
https://www.cse.iitd.ac.in/~sbansal/csl862-virt/2010/readings/NPT-WP-1%201-final-TM.pdf
[4] Accelerating Two-Dimensional Page Walks for Virtualized Systems
https://pages.cs.wisc.edu/~remzi/Classes/838/Spring2013/Papers/p26-bhargava.pdf
[5] Memory virtualization: shadow page & nest page
https://blog.csdn.net/hit_shaoqi/article/details/121887459
[6] AMD-SEV API
https://www.amd.com/content/dam/amd/en/documents/epyc-technical-docs/programmer-references/55766_SEV-KM_API_Specification.pdf

Reference

[7] AMD Memory Encryption
https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/white-papers/memory-encryption-white-paper.pdf
[8] QEMU - AMD SEV
https://www.qemu.org/docs/master/system/i386/amd-memory-encryption.html
[9] Linux - KVM
https://www.kernel.org/doc/html/v5.7/virt/kvm/index.html
[10] AMD SEV-SNP White Paper
https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/white-papers/SEV-SNP-strengthening-vm-isolation-with-integrity-protection-and-more.pdf
[11] AMD SEV in ThinkSystem
https://lenovopress.lenovo.com/lp1545-using-amd-secure-encrypted-virtualization-encrypted-state-sev-es
[12] AMD SEV-SNP Key Attestation
https://www.amd.com/content/dam/amd/en/documents/developer/lss-snp-attestation.pdf
[13] AMD Virtualization Memory Encryption Technology
https://www.linux-kvm.org/images/7/74/02x08A-Thomas_Lendacky-AMDs_Virtualizatoin_Memory_Encryption_Technology.pdf