



探索 AMD SEV-SNP: 下一代虛擬化記憶體加密與安全保護

Exploring AMD SEV-SNP:

Next-Generation Virtualized Memory Encryption and Security Protection

richard-lyu

SUSE Labs Developer for EFI

CYBERSEC 2025

Whoami



Richard Lyu

Taipei, Taiwan

Work at SUSE

SUSE Labs Developer for EFI

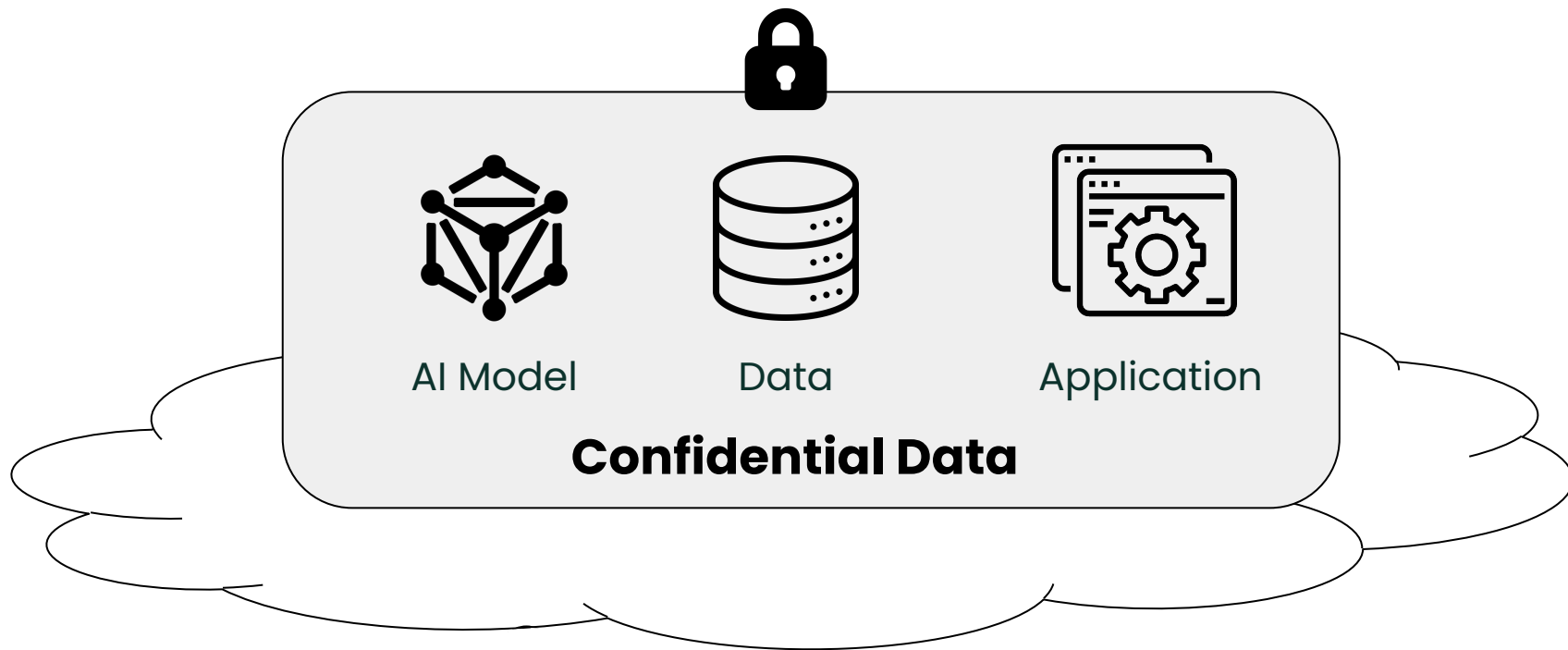
Maintain **OVMF** in SLES and openSUSE

Member of **UEFI Forum**

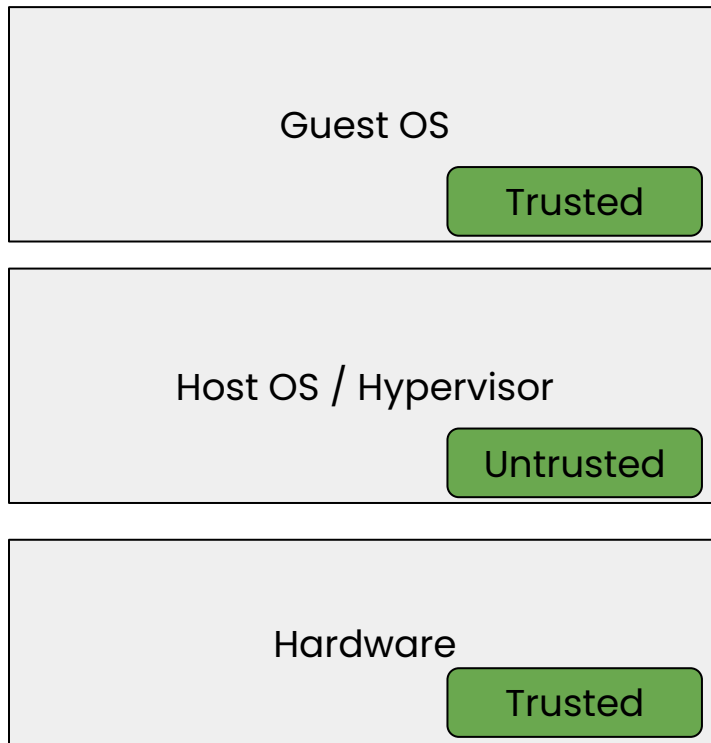
Confidential Computing



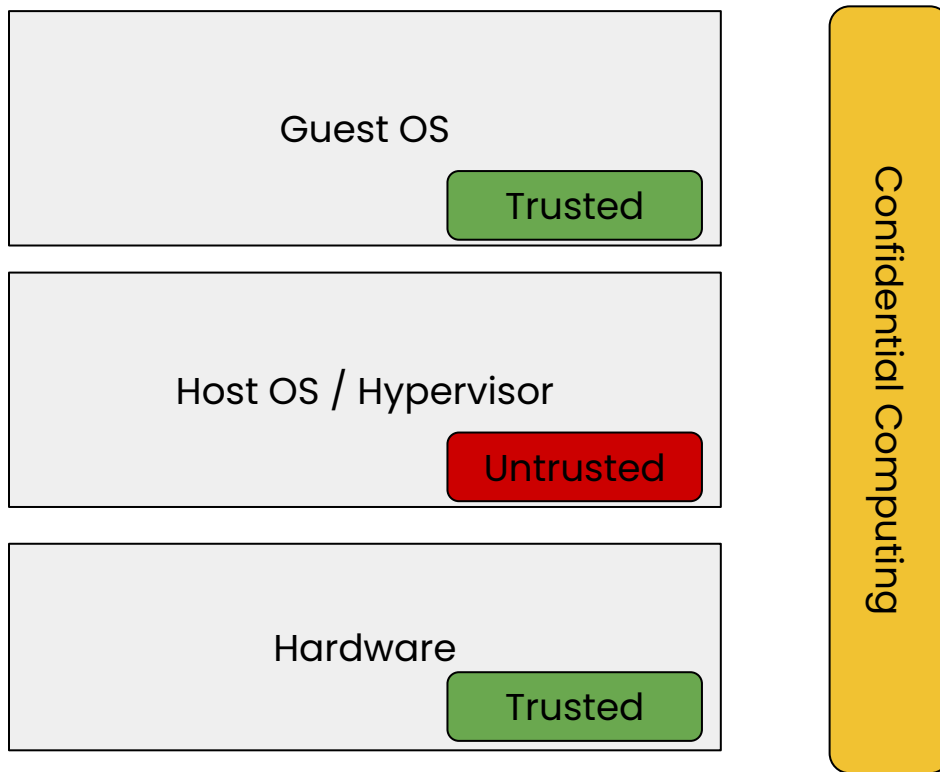
Encryption Confidential Data



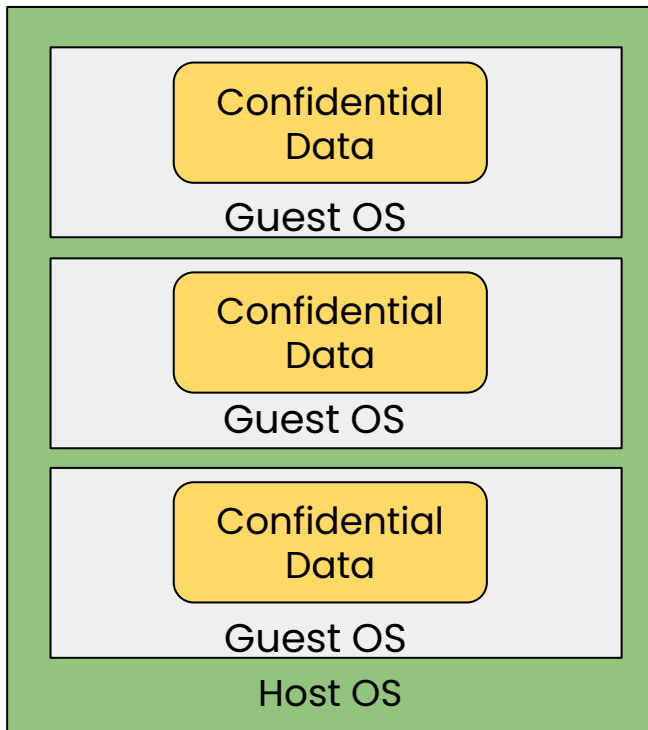
Trusted Execution Base (TEB)



Trusted Execution Base



Trusted Execution Base



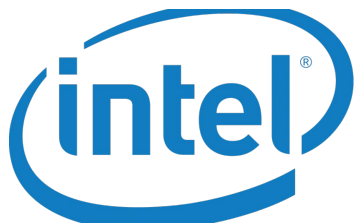
Without Confidential Computing



Confidential Computing

Providers

- Require a combination of hardware and software



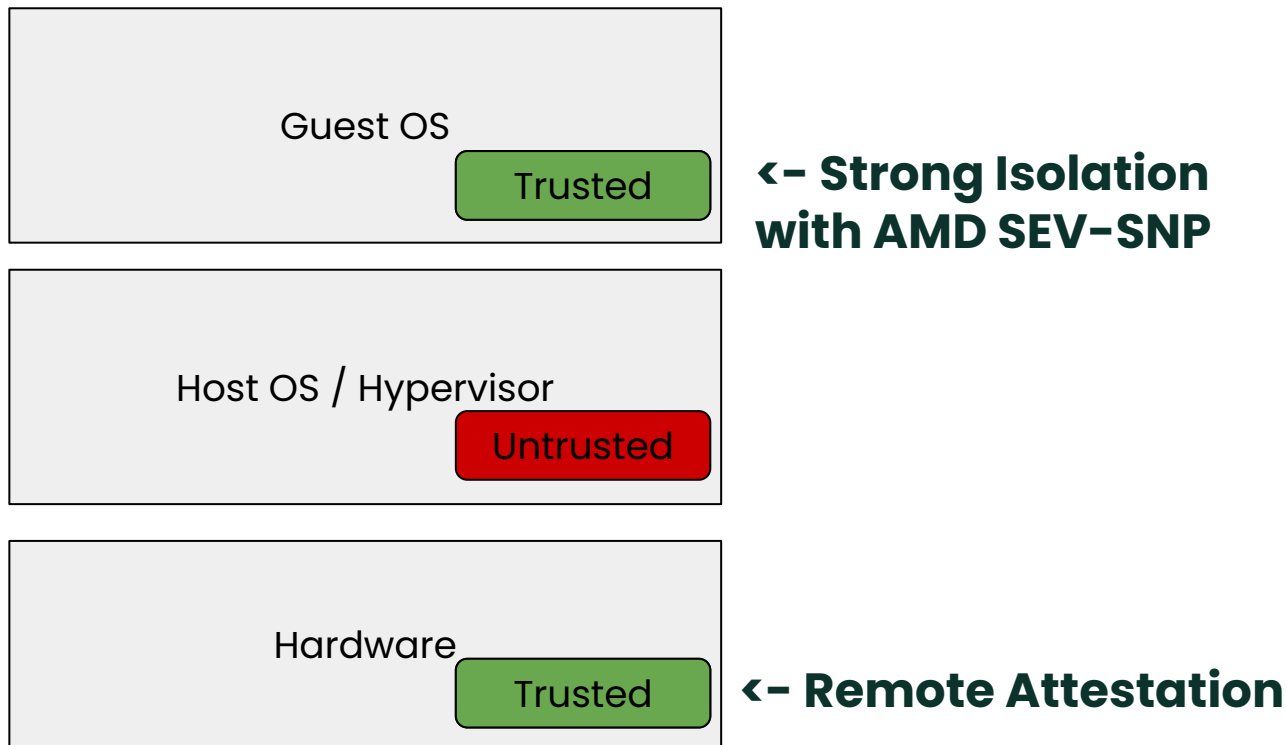
- Delivered with cloud providers or server manufacturers



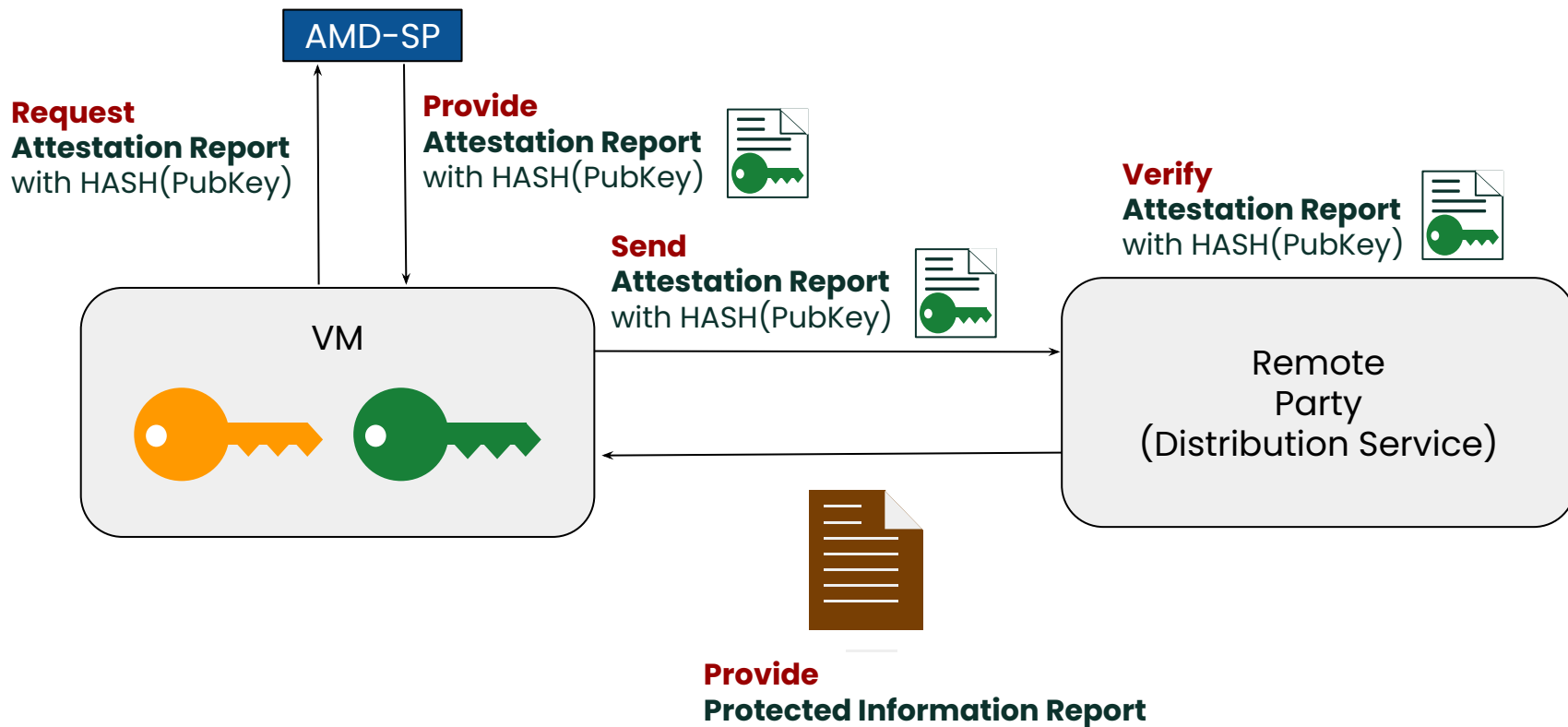
AMD SEV-SNP

Secure Encrypted Virtualization – Secure Nested Paging

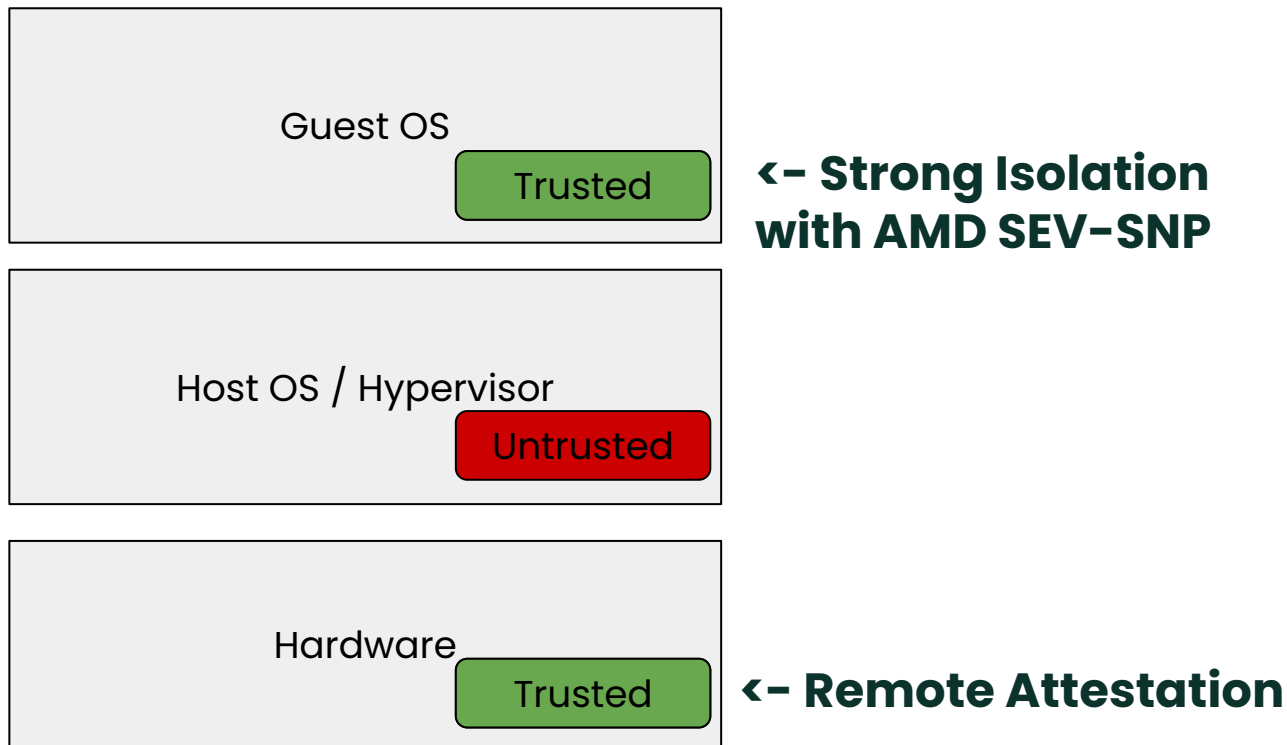
Trusted Execution Base



Remote Attestation



Trusted Execution Base



Strong Isolation with AMD SEV-SNP

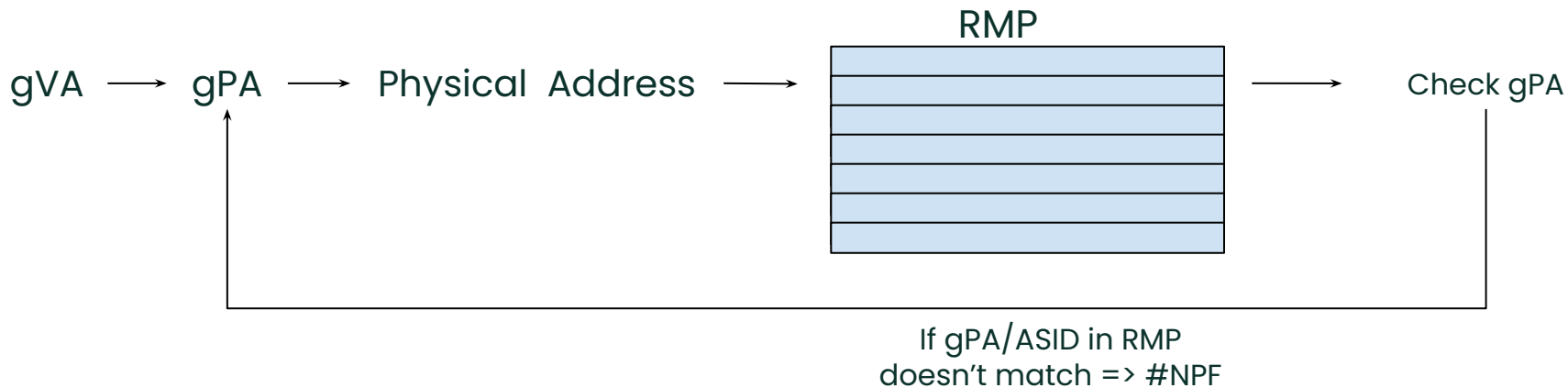
- VM Memory Encryption
- VM Register Encryption
- Reverse Map Table
- Page Validation
- Virtual Machine Privilege Levels (VMPLs)

Reverse Page Table

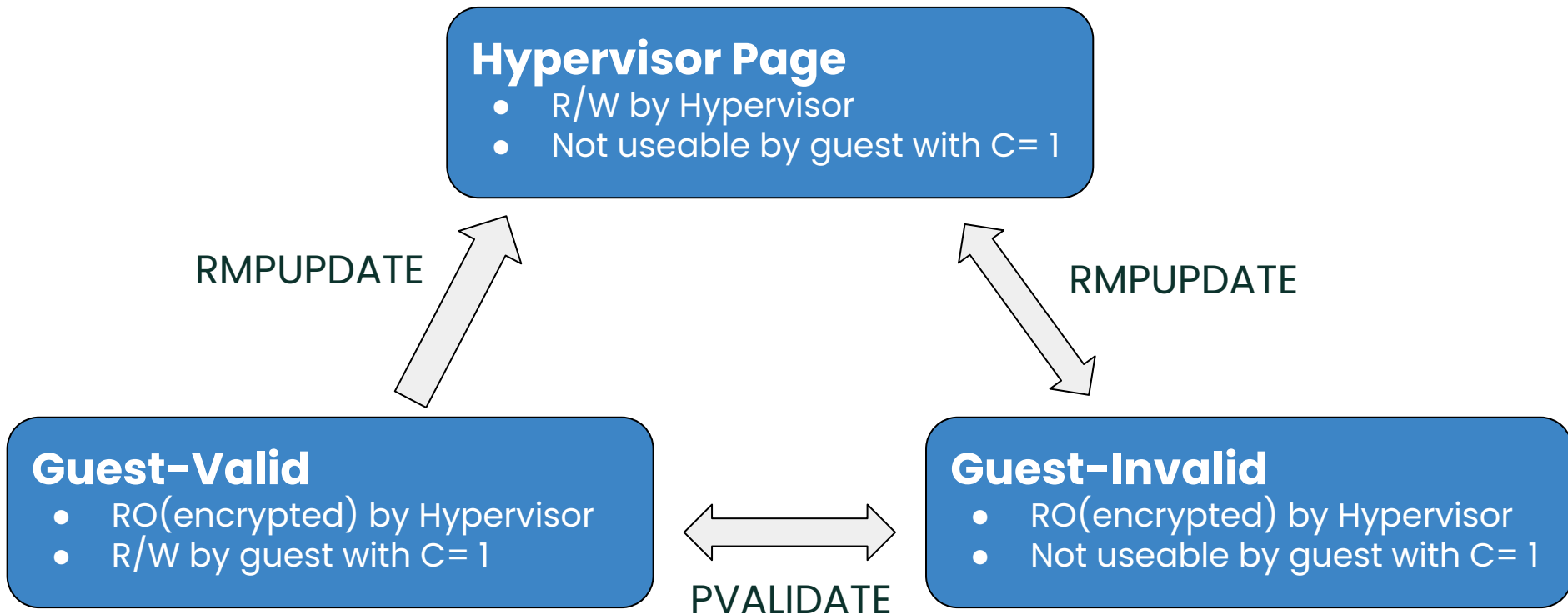
Native tablewalk



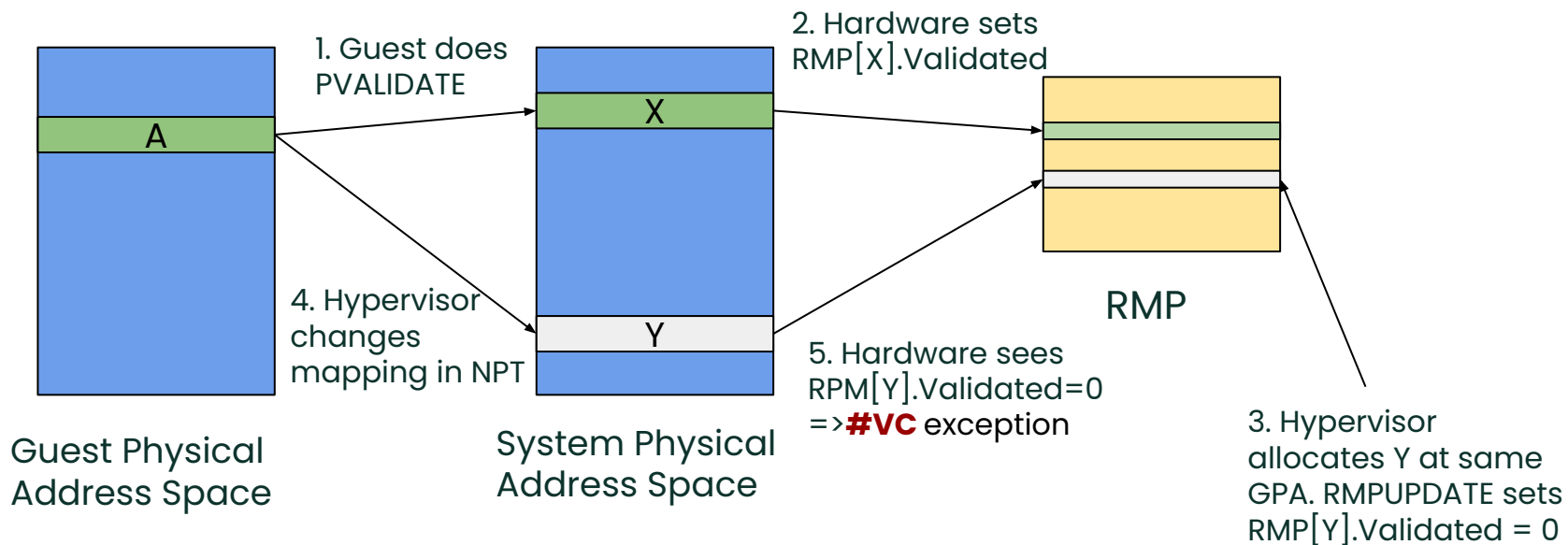
Nested tablewalk



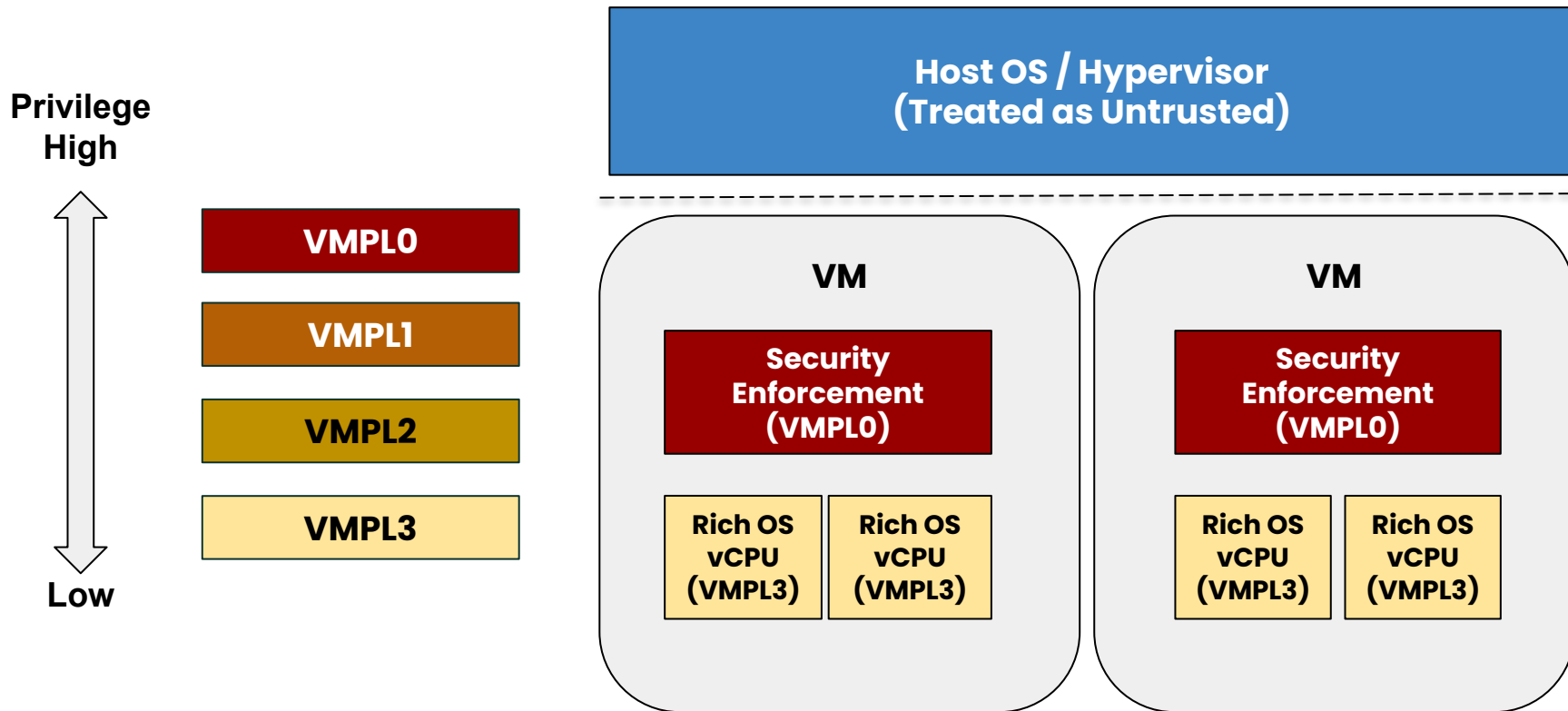
Page Validation



Page Re-Mapping Attack



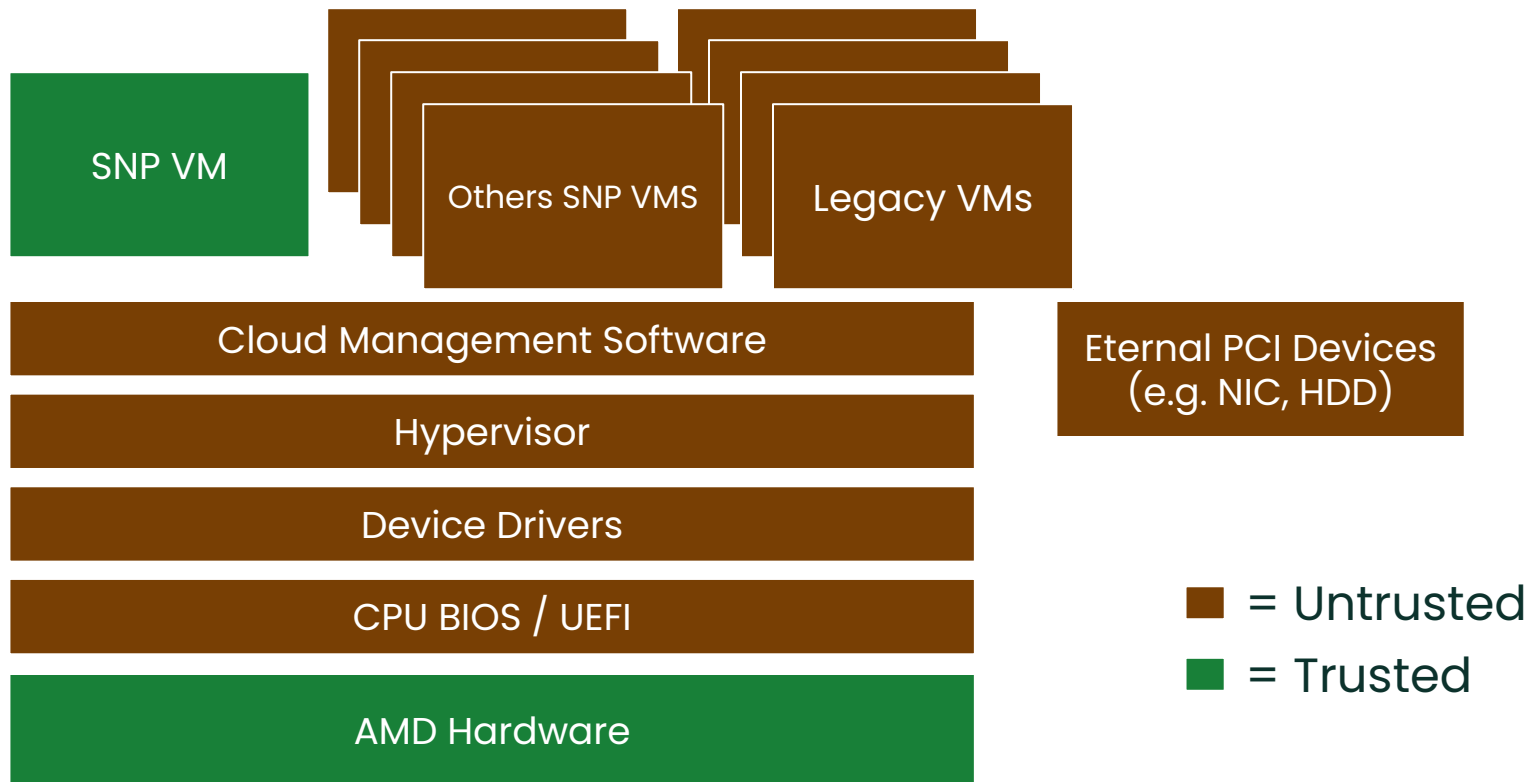
Virtual Machine Privilege Levels (VMPLs)



Security



Threat Model



Threat Model

Hardware-based trusted execution

- Remote attestation <- Initial state security guarantees
- Strong isolation <- Runtime security guarantees

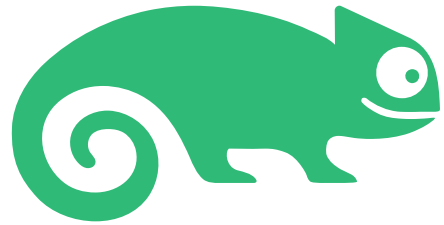


Potential Threats

Category	Attack Vector	With SEV-SNP	Without SEV-SNP
Confidentiality	VM Memory	✓ Memory Encryption	✗
	VM Register State	✓ Register Encryption	✗
	DMA Protection	✓ IOMMU + RMP	✗
Integrity	Relay Protection	✓ RMP	✗
	Data Corruption	✓ RMP	✗
	Memory Aliasing	✓ RMP	✗
	Memory Re-Mapping	✓ Page Validation	✗
Availability	DOS from Guest	✓ VMPLs	✗
	DOS from Host	✗	✗

CVEs

ID / Name	Affected	Severity	Summary	Status
CVE-2024-56161	Zen 1–5	High	Weak hash in microcode signature → malicious code injection	✓ Patched
CVE-2023-31346	Milan, Genoa	Medium	Access to stale data, guest integrity risks	✓ Patched
CVE-2024-21978	Milan, Genoa	Med-High	Firmware flaws affecting SEV-SNP trust	✓ Patched
CVE-2024-25742 (WeSee)	SEV-SNP VMs	High	Malicious #VC interrupts → data leak/code injection	✓ Patched
CVE-2024-25744 (Heckler)	SEV-SNP VMs	High	Async interrupts → guest state manipulation	✓ Patched



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/Courses/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]AMD SEV基本原理

<https://blog.csdn.net/huang987246510/article/details/135487665>

[9]QEMU - AMD SEV

<https://www.qemu.org/docs/master/system/i386/amd-memory-encryption.html>

[10]Linux - KVM

<https://www.kernel.org/doc/html/v5.7/virt/kvm/index.html>

[11] 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>

[12] AMD SEV in ThinkSystem

<https://lenovopress.lenovo.com/lp1545-using-amd-secure-encrypted-virtualization-encrypted-state-sev-es>

[13] AMD SEV-SNP Key Attestation

<https://www.amd.com/content/dam/amd/en/documents/developer/lss-snp-attestation.pdf>

[14]AMD Virtualization Memory Encryption Technology

https://www.linux-kvm.org/images/7/74/02x08A-Thomas_Lendacky-AMDs_Virtualizatoin_Memory_Encryption_Technology.pdf