SUSE

13th March 2022

Confidential Computing mit AMD SEV-ES

Jörg Rödel <jroedel@suse.com>
@joergroedel

Was ist Confidential Computing

Daten vor unbefugtem Zugriff schützen

Während der Übertragung

→ Netzwerkverschlüsselung (TLS, …)

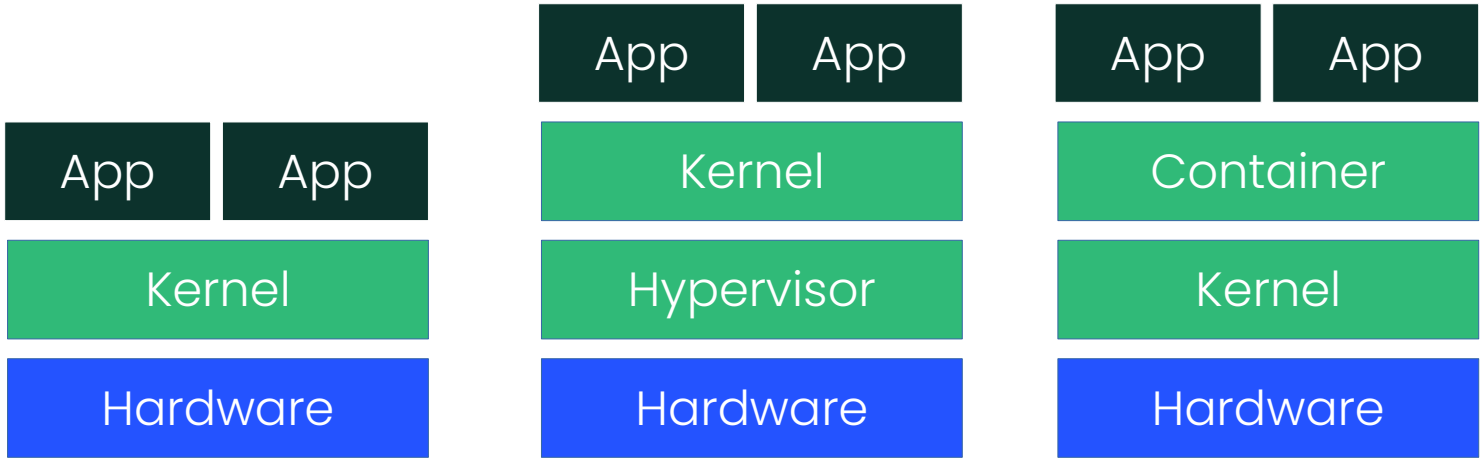
Auf dem Datenträger

→ Festplattenverschlüsselung (DM_Crypt + LUKS)

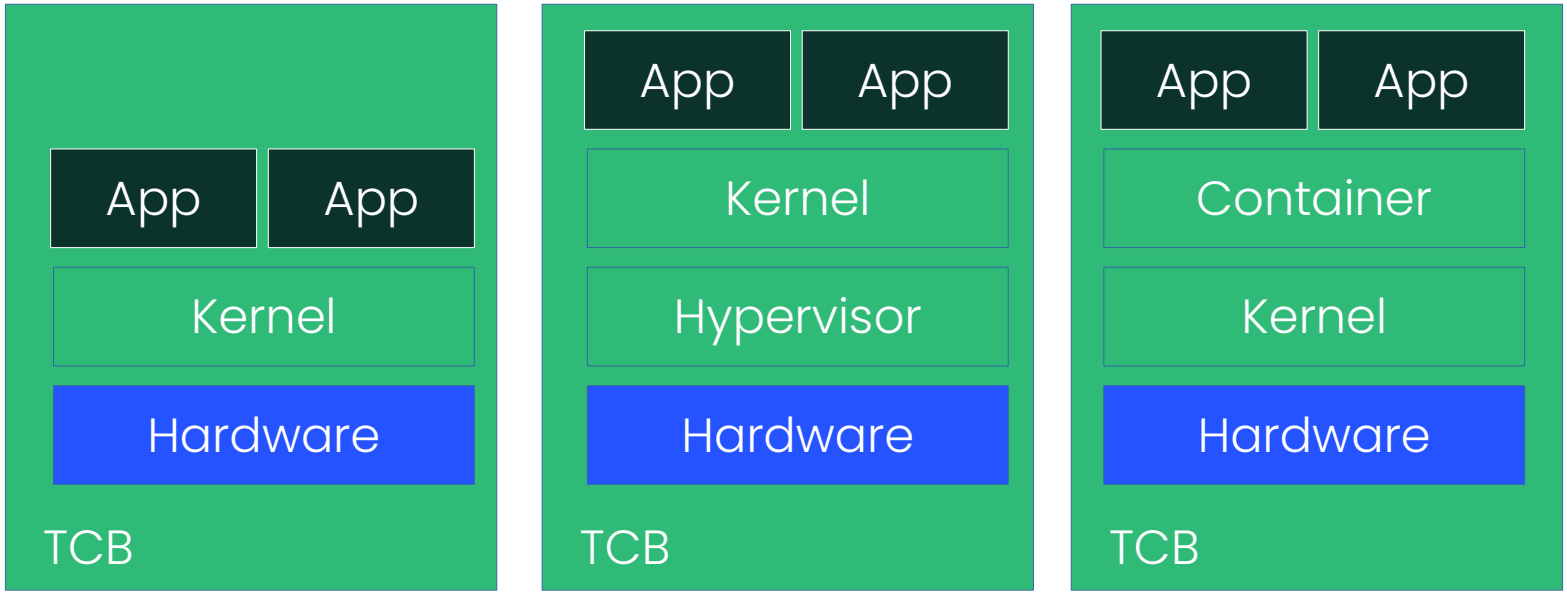
Während der Verarbeitung

→ Confidential Computing

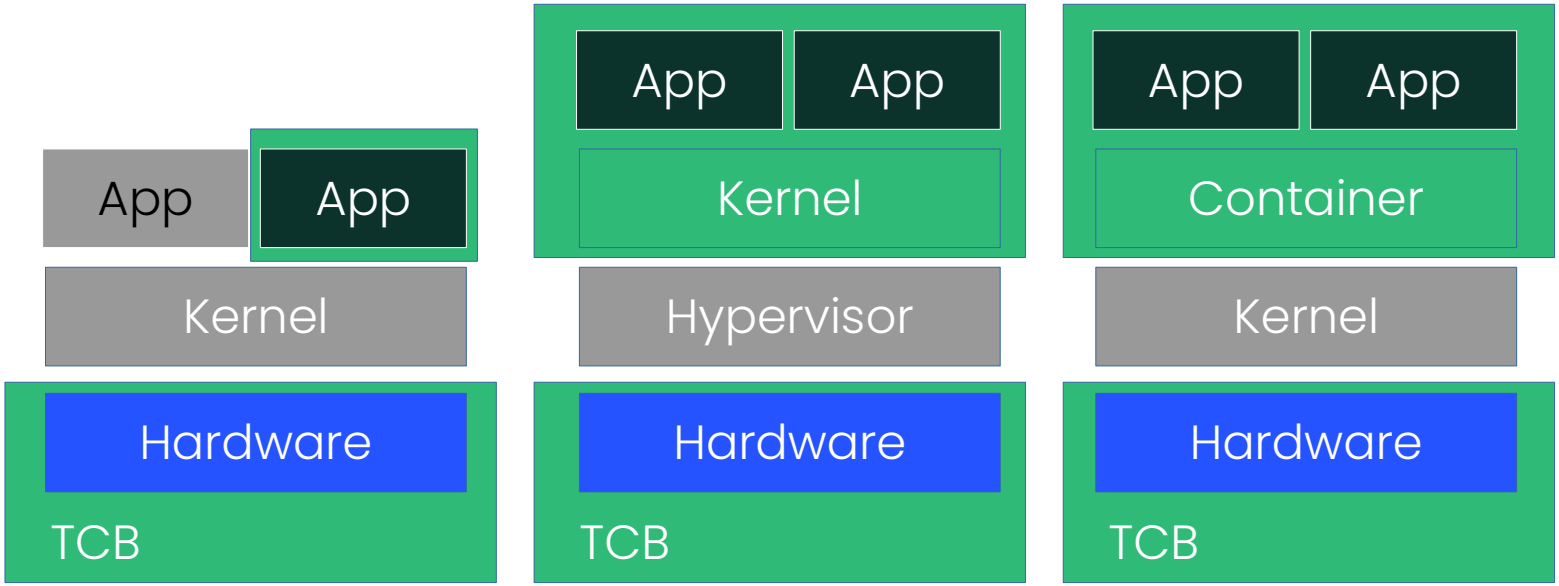
Computing Base



(Trusted?) Computing Base



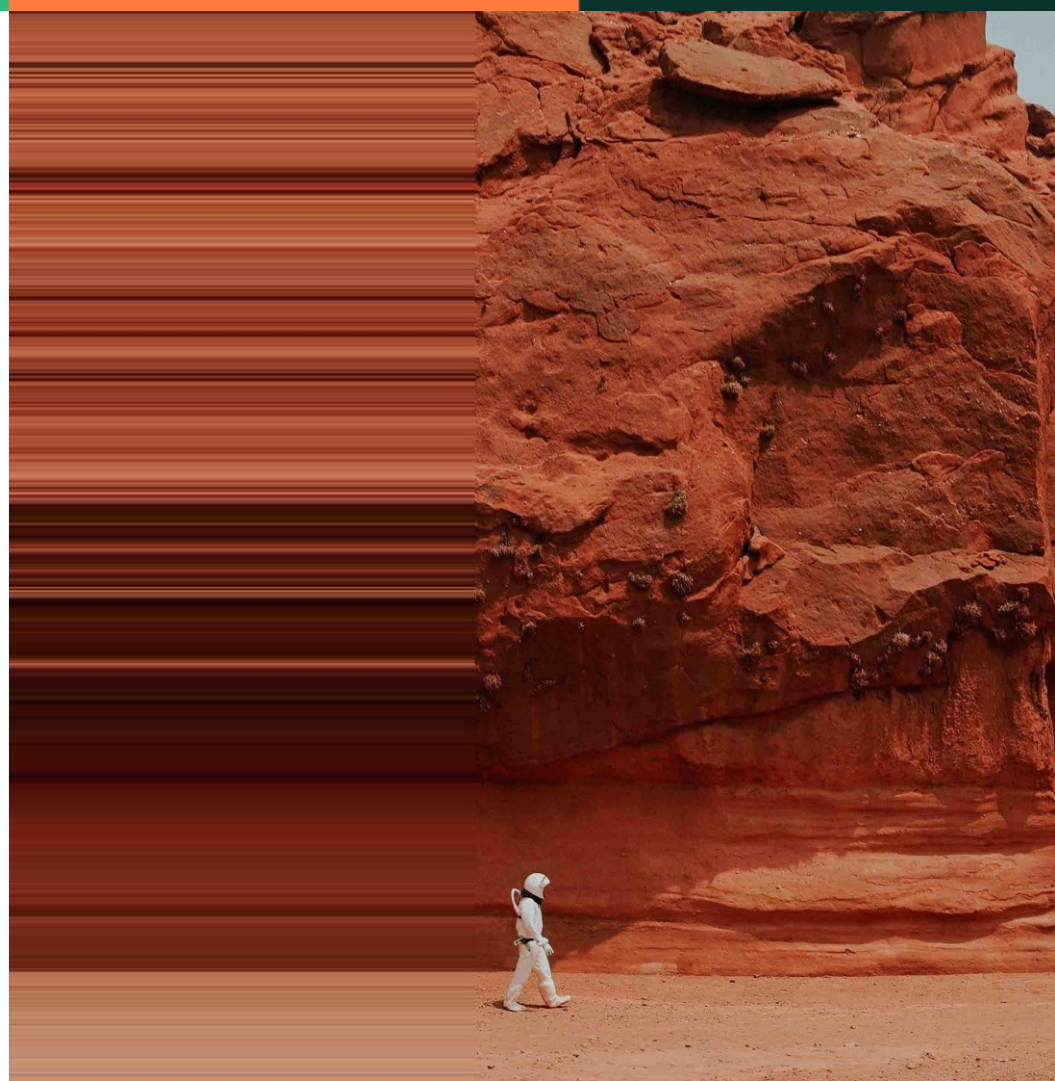
Trusted Computing Base



Trusted Computing Base

- Hardware immer Teil der TCB
- Herstellerspezifische ISA Erweiterungen
- Transparente Datenverschlüsselung (RAM + Register)
- Zwei Arten: Virtualisierung und Enclaves
- Software-Teil der TCB ist “Trusted Execution Environment” (TEE)

AMD SEV-ES



AMD SEV in a Nutshell

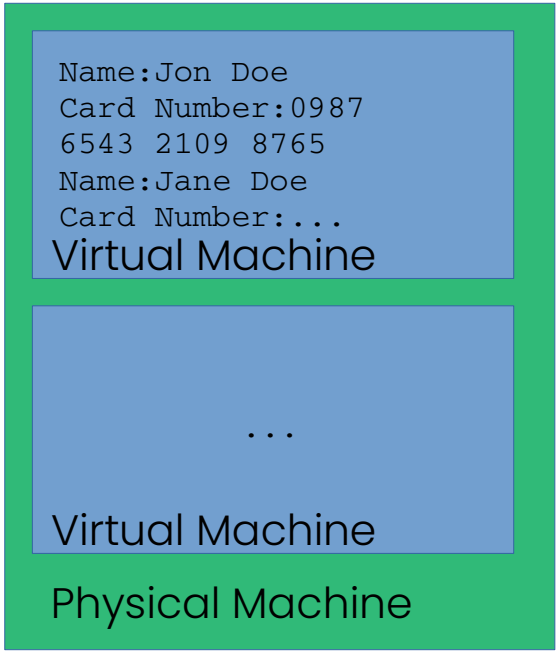
1. **Secure Encrypted Virtualization (SEV)**
   Verschlüsselung des RAM der virtuellen Maschine

2. **Encrypted State (SEV-ES)**
   Zusätzliche Verschlüsselung der CPU Register

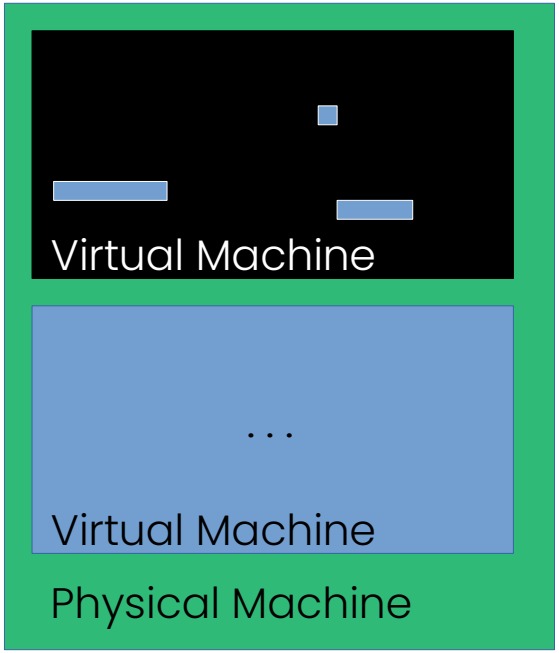
3. **Secure Nested Paging (SEV-SNP)**
   Erweitert den Schutz gegen Attacken auf das Gast Speicherlayout. Der Hypervisor kann nicht mehr unbemerkt auf privaten Gastspeicher zugreifen.

Secure Encrypted Virtualization (SEV)

Legacy Virtualization



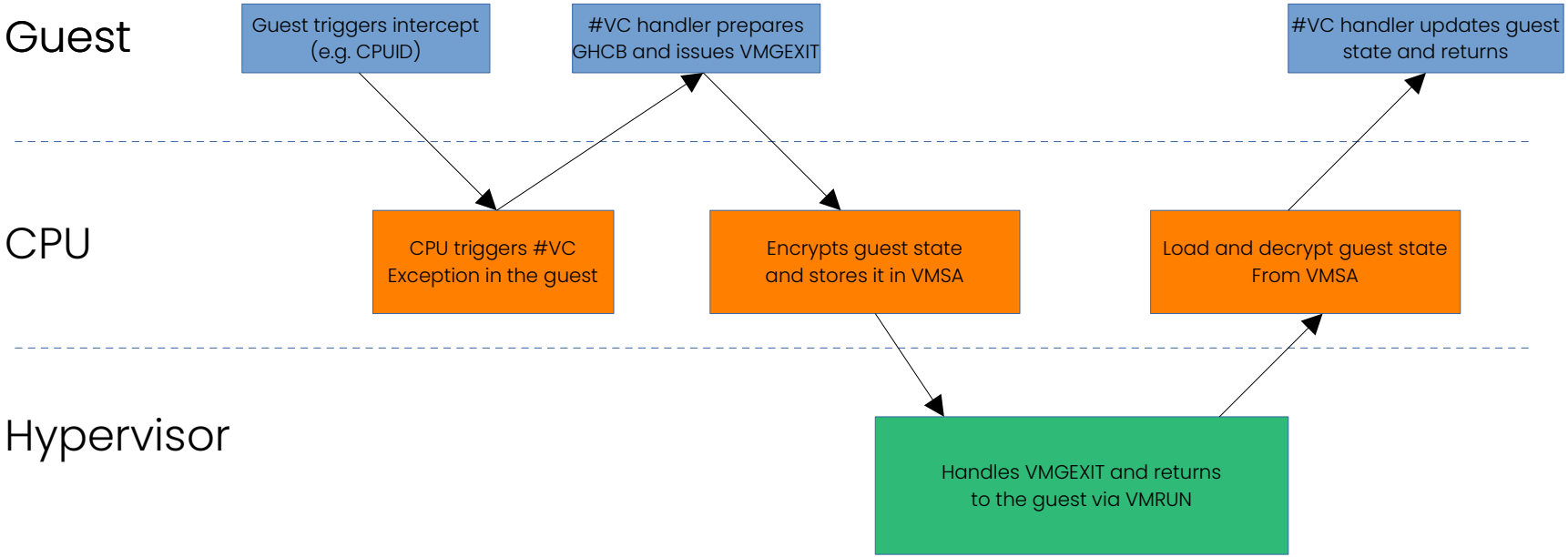
Secure Encrypted Virtualization



Encrypted State (SEV-ES)

- CPU Register der VM werden verschlüsselt
- Hypervisor kann Register weder lesen noch verändern
- Viele Intercepts werden zu Exceptions in der VM
- Exception Vektor: #VC (Vektor 29)
- Paravirtualisiertes Protokoll zur Kommunikation Guest-Hypervisor-Control-Block (GHCB)
- GHCB enthält nur notwendige Informationen

Encrypted State (SEV-ES)



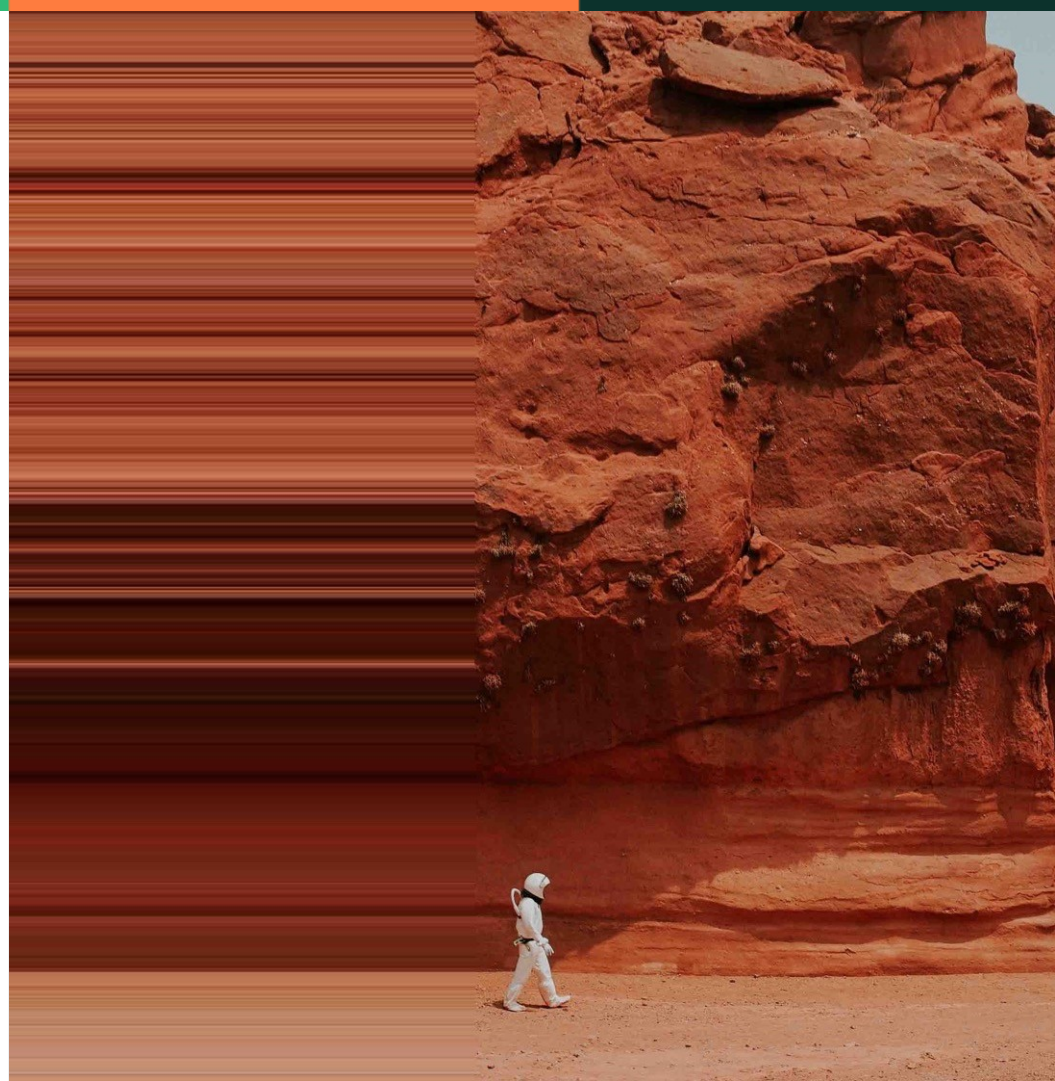
SEV-ES in Linux – Support Status

- Code für SEV-ES ist Upstream:
  - QEMU (seit Version 6.0)
  - OVMF (seit November 2020)
  - Linux Kernel Guest Support (Seit Linux 5.10)
  - Linux Kernel KVM Support (Seit Linux 5.11)
- OpenSUSE Tumbleweed hat vollständigen Support seit Mai 2021
- SUSE Linux Enterprise Server 15 SP3 und OpenSUSE Leap 15.3 können in einer SEV-ES VM laufen

SEV-ES in Linux

DEMO

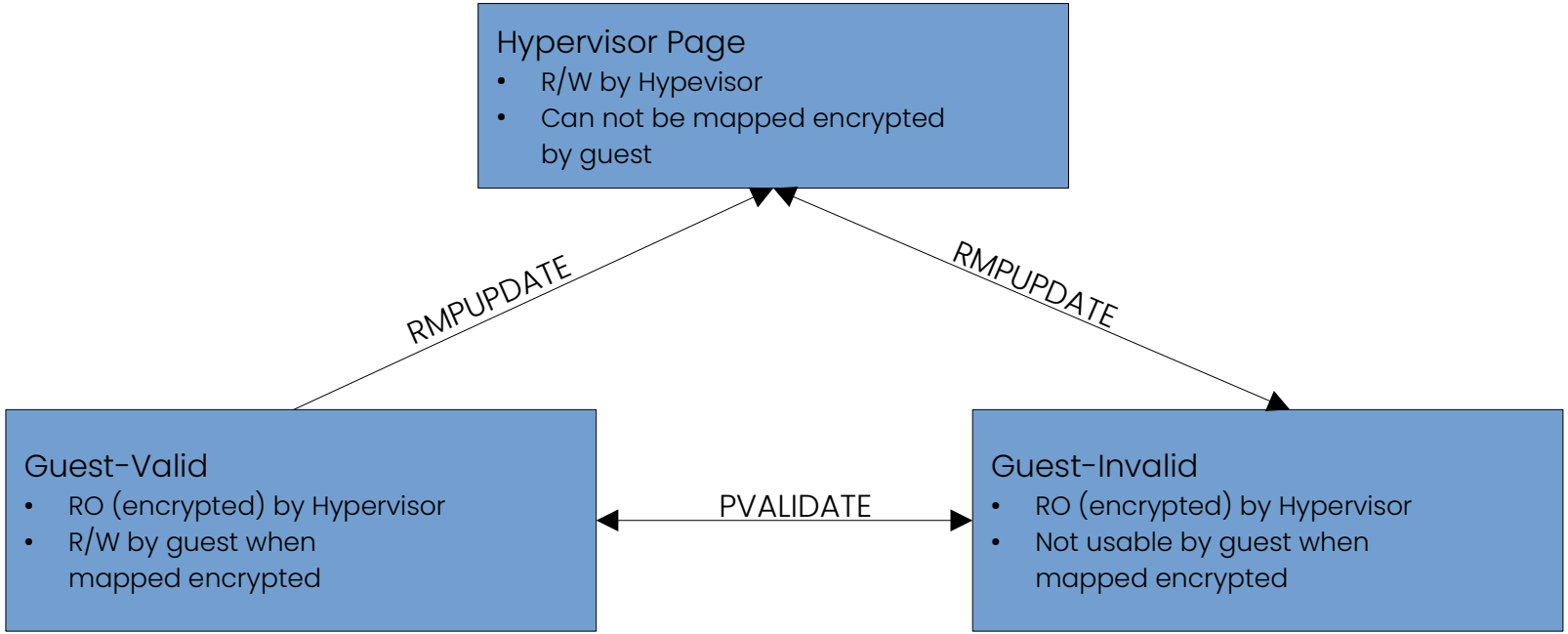
SEV-SNP



Secure Nested Paging (SEV-SNP)

- Schützt VM vor Memory Remapping und Replay Attacken
- SEV-SNP speichert einen State für jede Page welcher festlegt wer wie darauf zugreifen darf
- Page-State wird in der RMP-Table gespeichert
- RMP-Table kann nur durch spezielle Instruktionen verändert werden (RMPUPDATE, RMPADJUST, PVALIDATE)

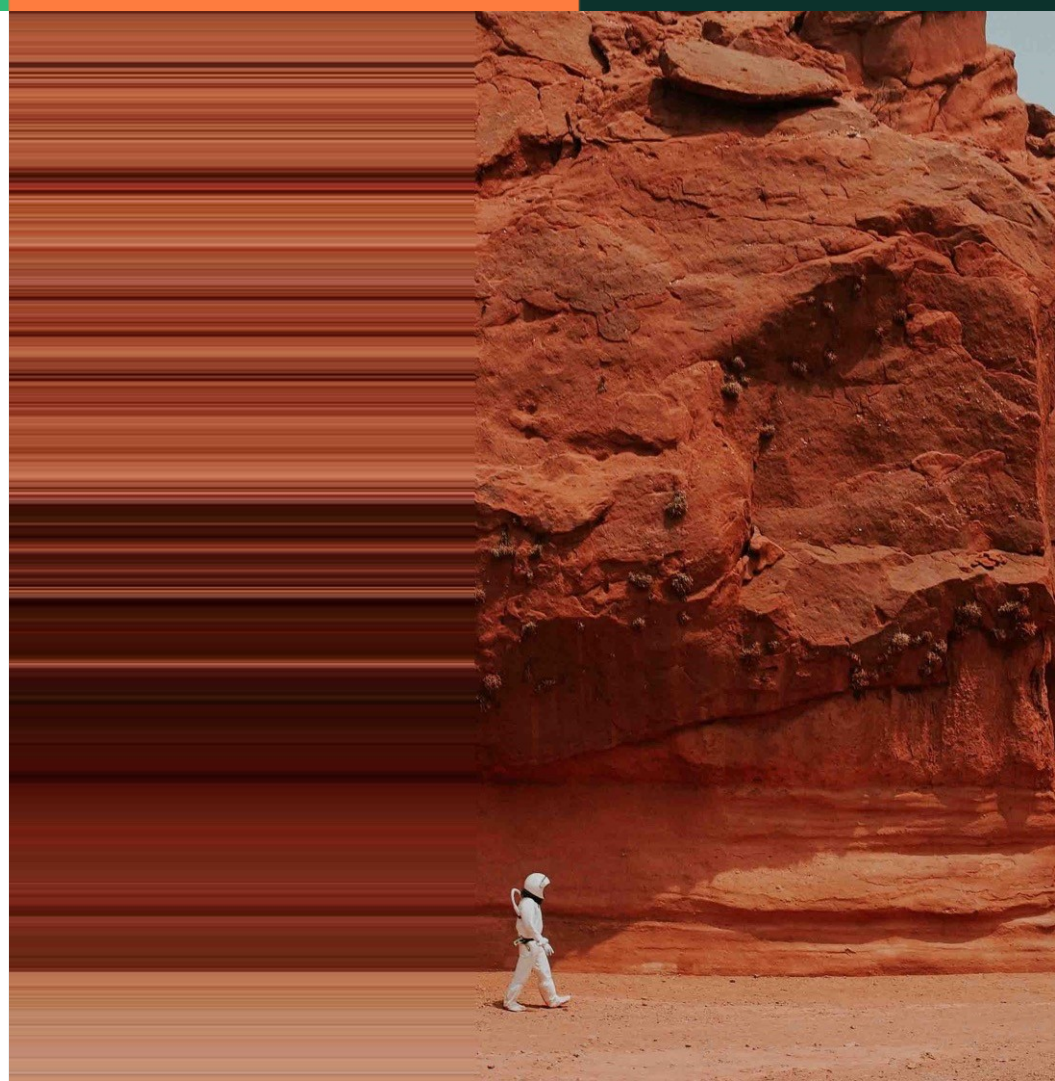
Secure Nested Paging – Page-States



Secure Nested Paging – Weitere Funktionen

- CPUID Security
- VM Priviledge Levels
- Reflect-VC
- Interrupt Security

Confidential VMs absichern



Hardware Provided Trust

- Hardware garantiert: Nur Software im TEE kann Daten sehen
- Hardware hilft Attacken gegen das TEE zu erkennen

1. Wie sichert man Ein- und Ausgabe von Daten?
2. Wie stellt man sicher, dass nur vertrauenswürdige Software im TEE läuft?

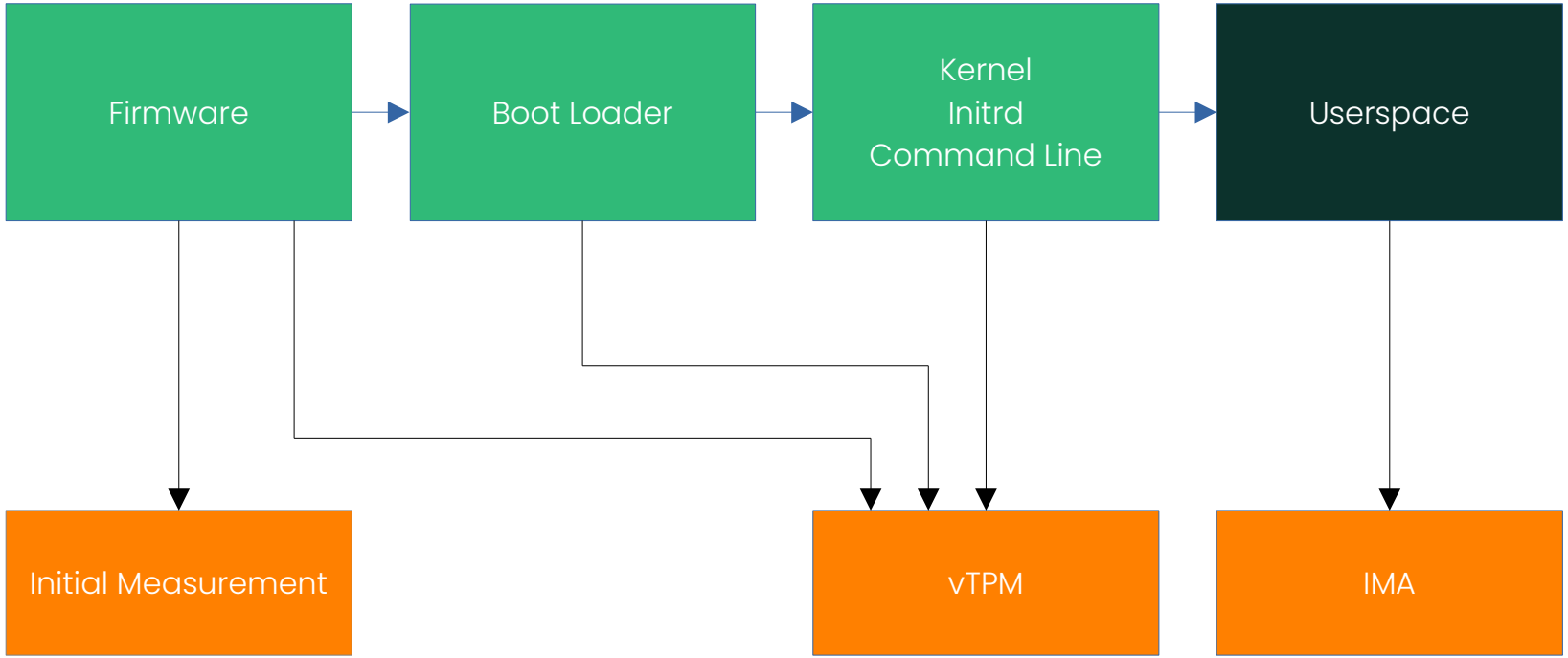
Encrypt Everything

- Alle Netzwerkverbindungen des TEE müssen verschlüsselt werden
- Festplatten müssen verschlüsselt sein
  - DM_Crypt und LUKS
  - DM_Integrity für Integrity-Protection

Vertauenswürdige Software

- Software wird attestiert (Remote Attestation)
- Alle Software Komponenten werden gehashed (measured)
- Hashes werden in sicherer Komponente gesichert (z. Bsp. vTPM)
- Linux Integrated Measurement Architecture (IMA) für Userspace

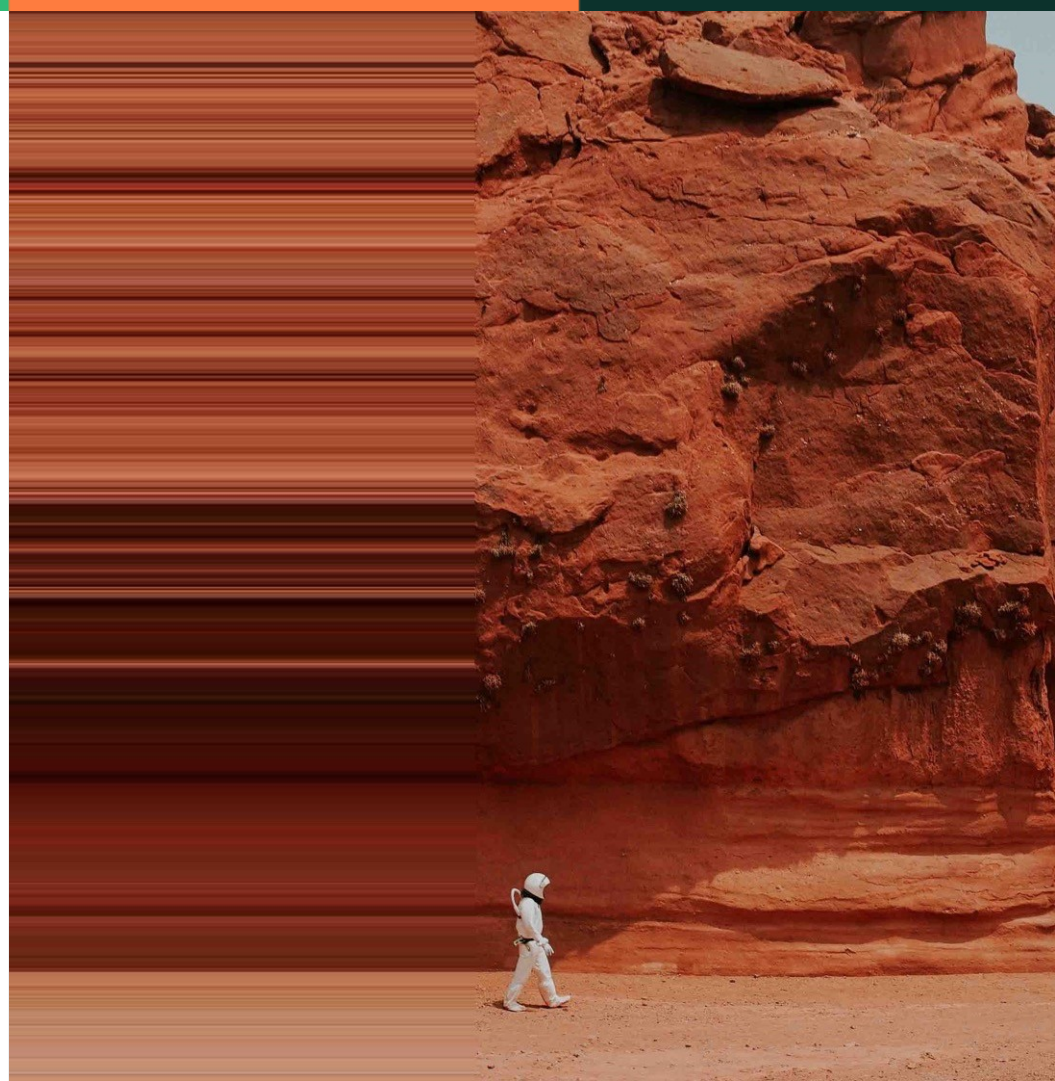
Measured Boot



Remote Attestation

- Boot Hashes werden an Verification Service (VS) gesendet
- VS vergleicht Hashes mit Referenzwerten
- Stimmen Hashes überein sendet der VS Secrets an die VM
- Secrets können z. Bsp. sein: Disk Keys, SSH keys, TLS Zertifikate, ...

Zusammenfassung



Zusammenfassung

- Mit Linux und AMD SEV-ES kann man Confidential VMs betreiben
- Weitere Unterstützung für SEV-SNP ist in Arbeit
- Confidential VMs müssen weiter abgesichert werden
- Vollständige Absicherung heute noch nicht möglich
  - Weitere Komponenten notwendig, z. Bsp. sicherer vTPM
  - Weiter SEV-SNP Funktionen müssen implementiert werden

Thank you

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

+49 (0)911-740 53-0 (Worldwide)

Maxfeldstrasse 5

90409 Nuremberg

www.suse.com