Confidential Computing Demystified

An in-depth look into CVMs

Dimple Kuriakose

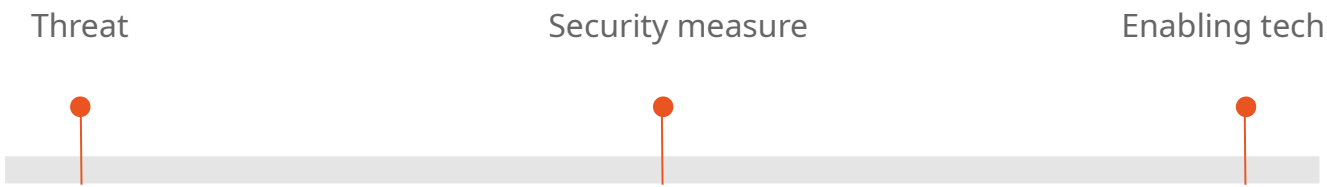
30th August 2025

Agenda

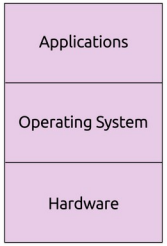
What is Confidential Computing?

Why do we need it?

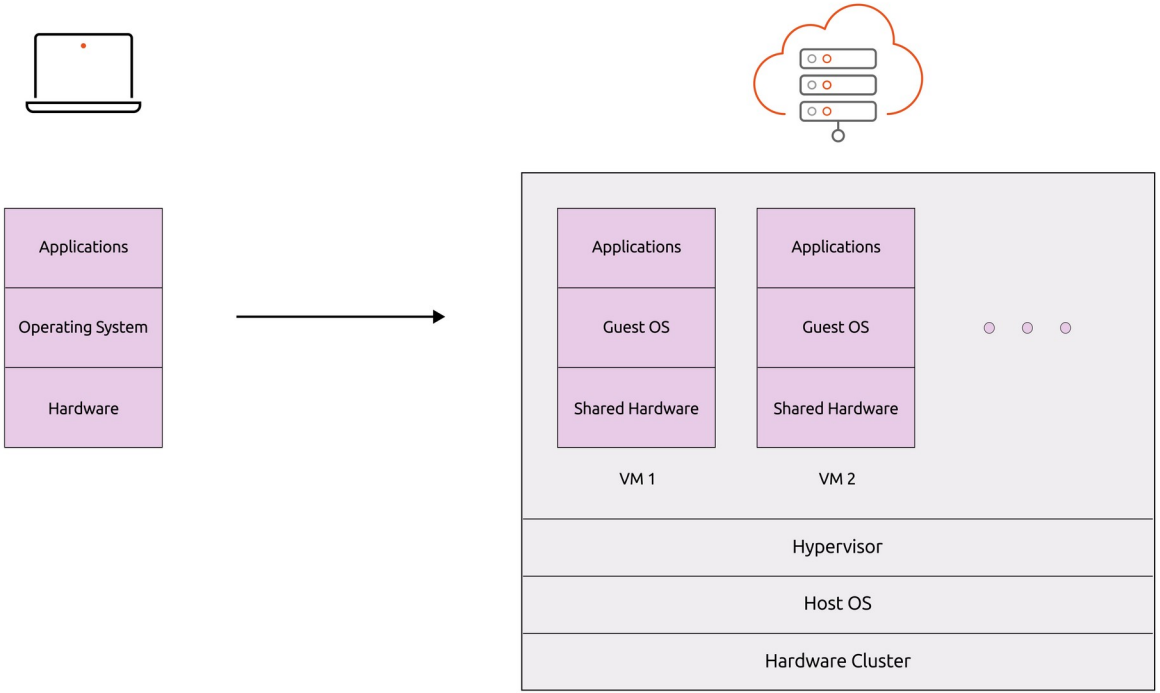
How is it implemented?



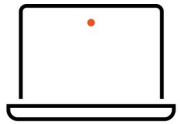
Problem: What do we trust?

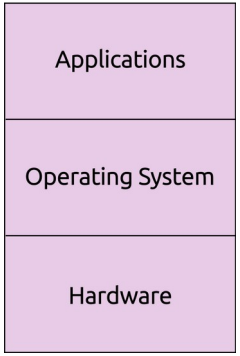


Problem: What do we trust?



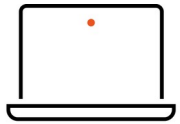
Trusting a Physical Machine

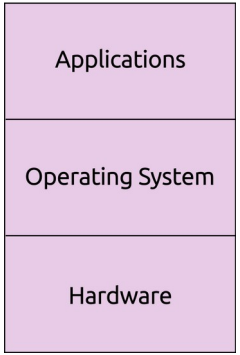




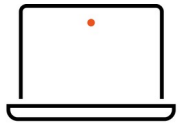
Trusting a Physical Machine

Hardware – We need to trust something!



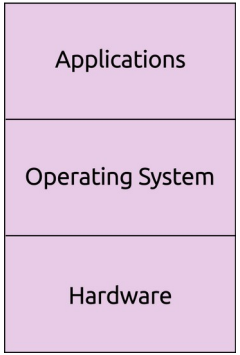


Trusting a Physical Machine

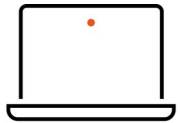


Hardware – We need to trust something!

Firmware – Trust it if it is authentic and uncompromised



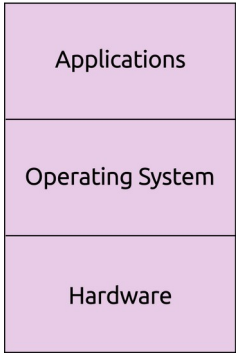
Trusting a Physical Machine



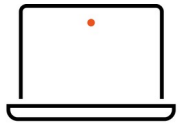
Hardware – We need to trust something!

Firmware – Trust it if it is authentic and uncompromised

OS – We need to take considerable effort to trust it



Trusting a Physical Machine

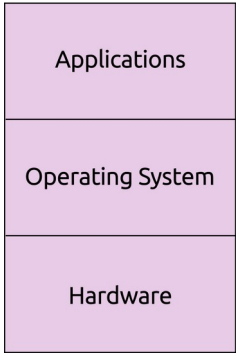


Hardware – We need to trust something!

Firmware – Trust it if it is authentic and uncompromised

OS – We need to take considerable effort to trust it

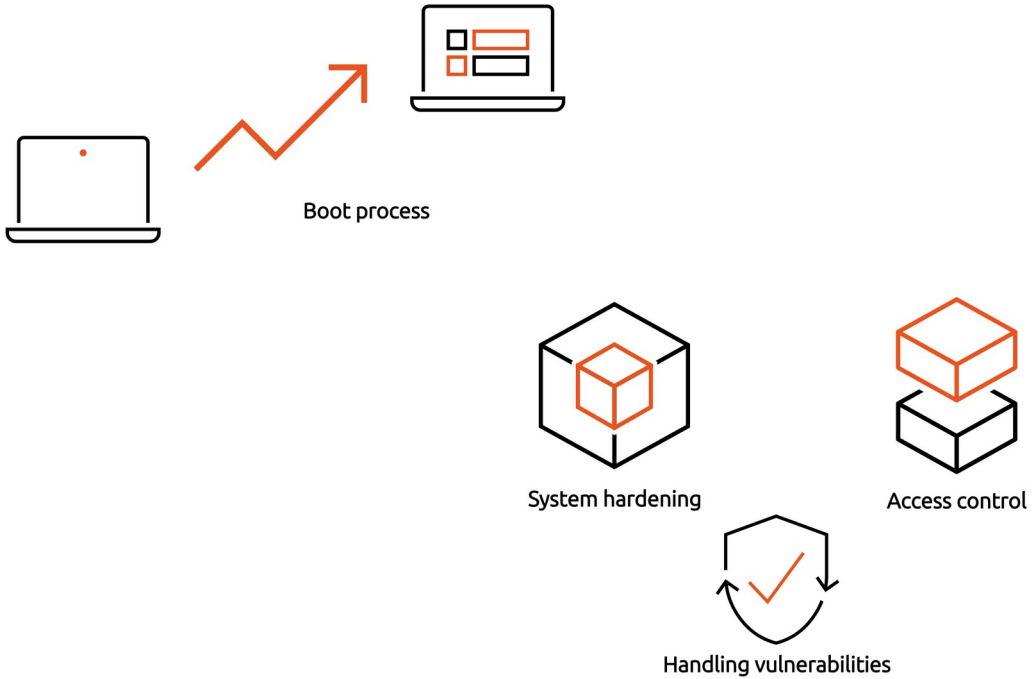
Apps – Can’t trust them
But you are the creator, so do your best!



Trusting the Operating System

Trusting the Operating System

Trusting the Operating System



OS Security Measures

System Hardening

Remove unnecessary components

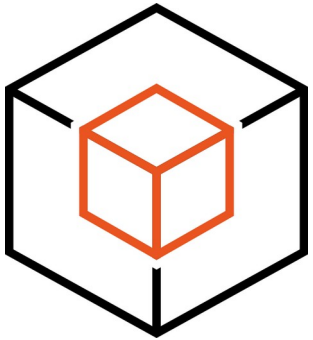
Disable unused hardware ports

Configuring strict file permissions

Secure network services

Configure remote logging and integrity checks

Enforce encryption



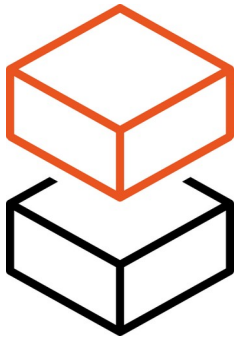
OS Security Measures

Access control

Protection against unknown vulnerabilities

Principle of least privilege

Apps can only access resources they legitimately need



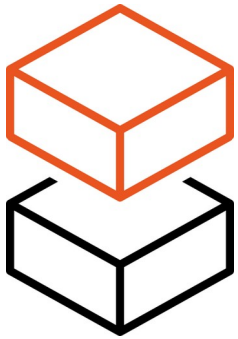
OS Security Measures

Access control

Protection against unknown vulnerabilities

Principle of least privilege

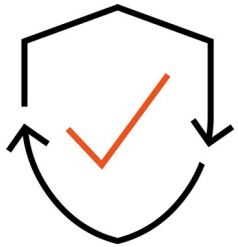
Apps can only access resources they legitimately need



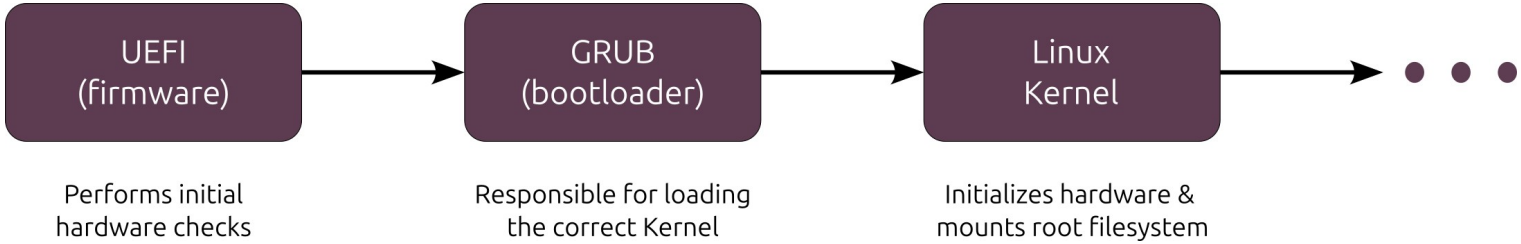
Handling Known Vulnerabilities

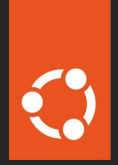
Monitor Common Vulnerabilities and Exposures (CVEs)

Patch them with security updates



Trusting the boot process



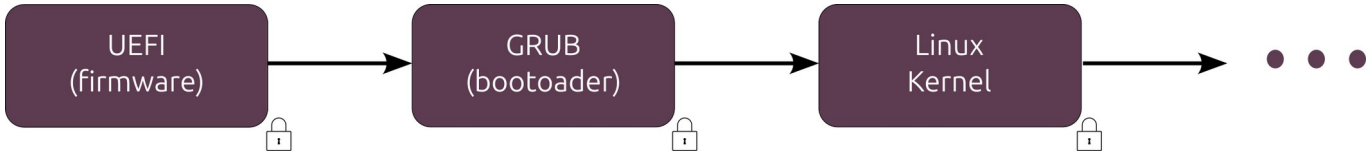


Have the modules been tampered with?

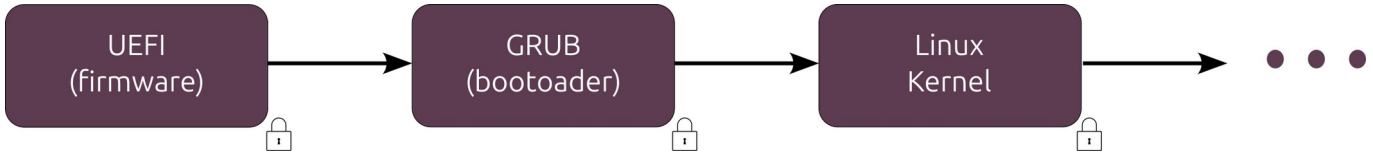
Are they the correct expected versions?

Solution: Secure boot

Solution: Secure boot



Solution: Secure boot



Only allows trusted modules to be loaded

Each module verifies the authenticity and integrity of the next one

Creates a chain of trust

If any one fails the test, the boot process is halted

Trusted modules & their verification

Trusted modules & their verification

Trusted modules:

(1) Digitally signed by an authorized vendor or

(2) Ones developed by yourself

Trusted modules & their verification

Trusted modules:

(1) Digitally signed by an authorized vendor or

(2) Ones developed by yourself

Verification:

(1) Verify the vendor & the module content

(2) Verify the module content

Asymmetric Cryptography

Asymmetric Cryptography

Mathematically linked pair of keys

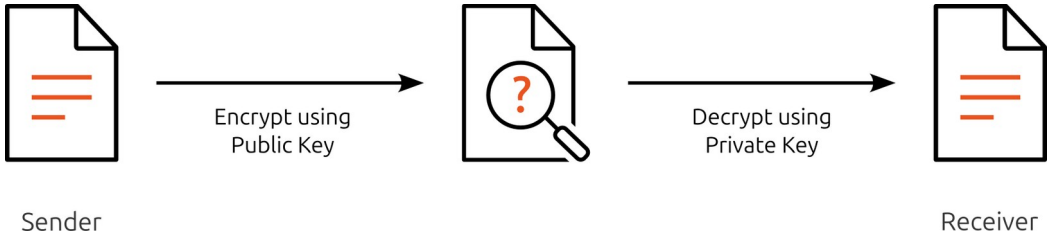
Public key (shared) and Private key (secret)

Asymmetric Cryptography

Mathematically linked pair of keys

Public key (shared) and Private key (secret)

Encryption achieves ‘Confidentiality’

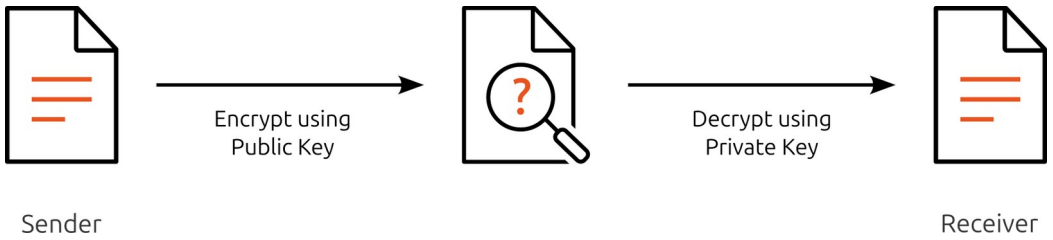


Asymmetric Cryptography

Mathematically linked pair of keys

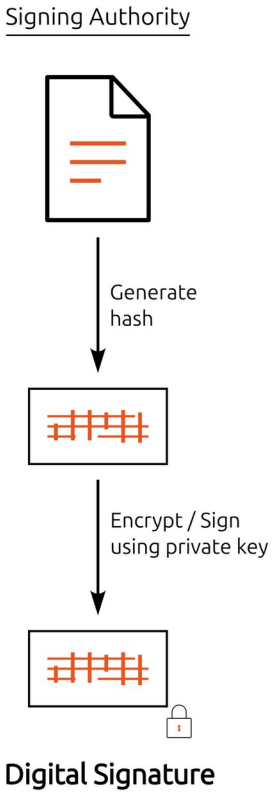
Public key (shared) and Private key (secret)

Encryption achieves ‘Confidentiality’

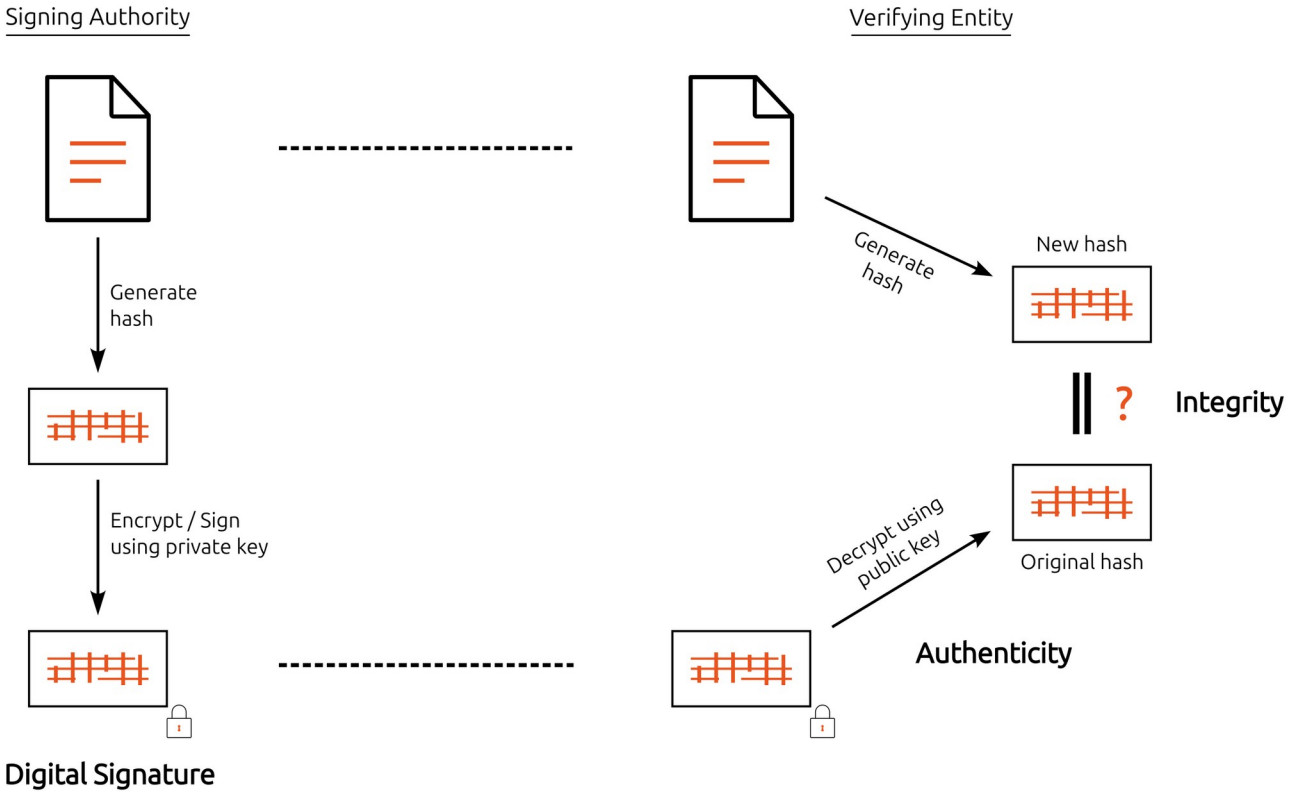


Digital signatures provide a means for ‘Authentication and Integrity’ check

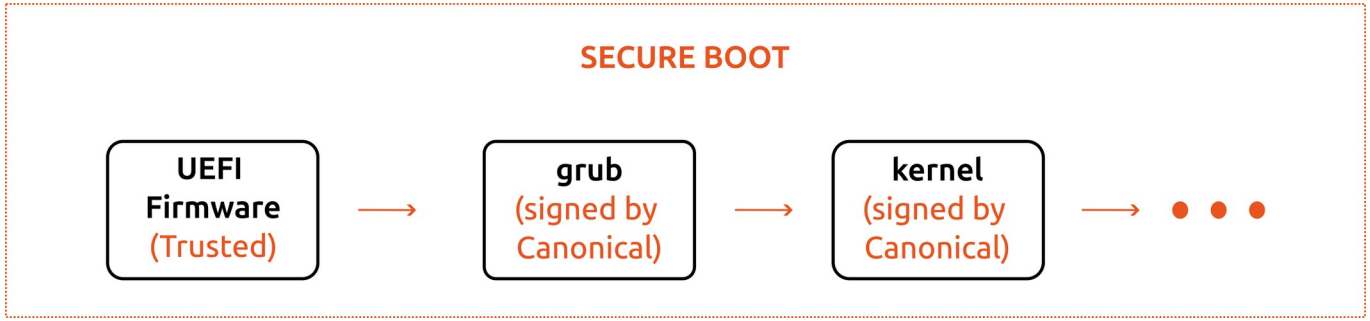
Authenticity and Integrity



Authenticity and Integrity

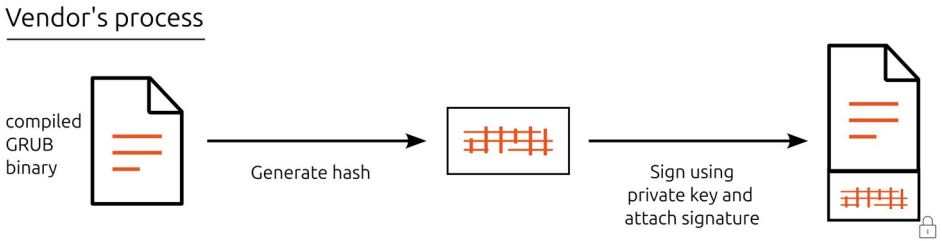


Solution: Secure boot

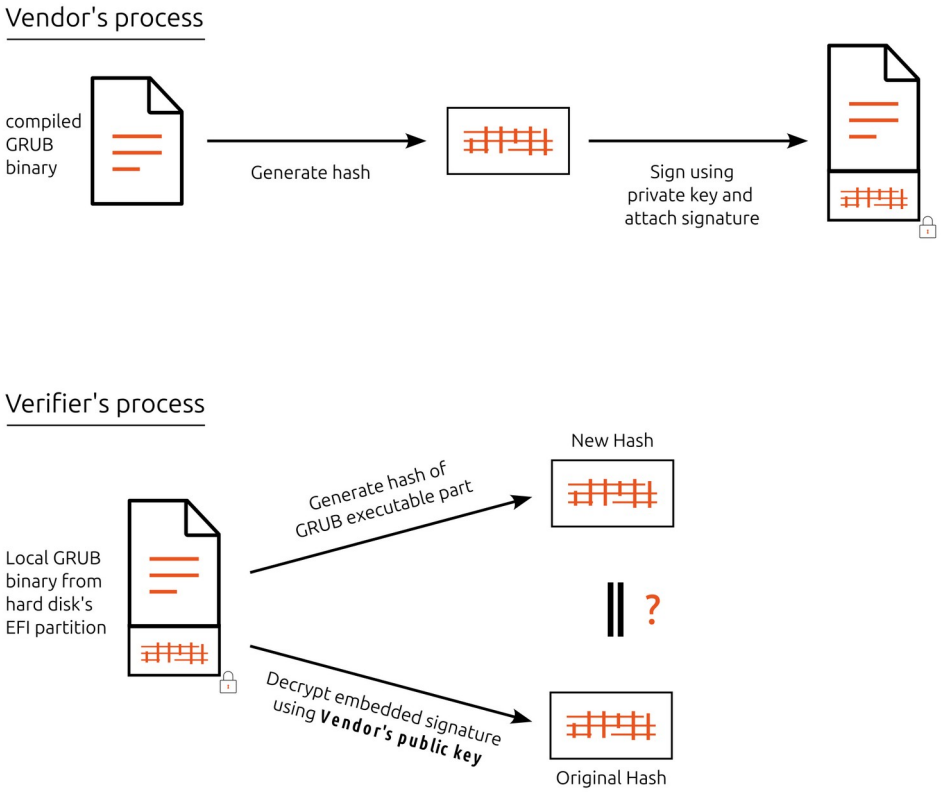


How is the verification of each module done?

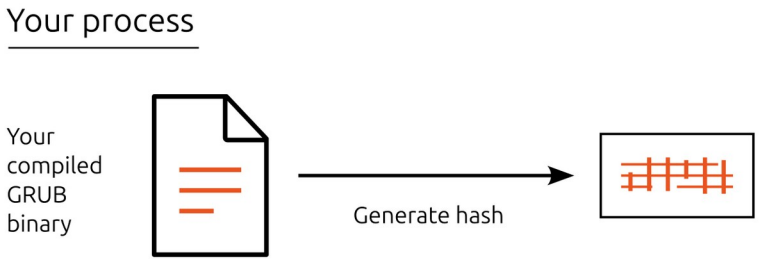
Verification of vendor-signed module



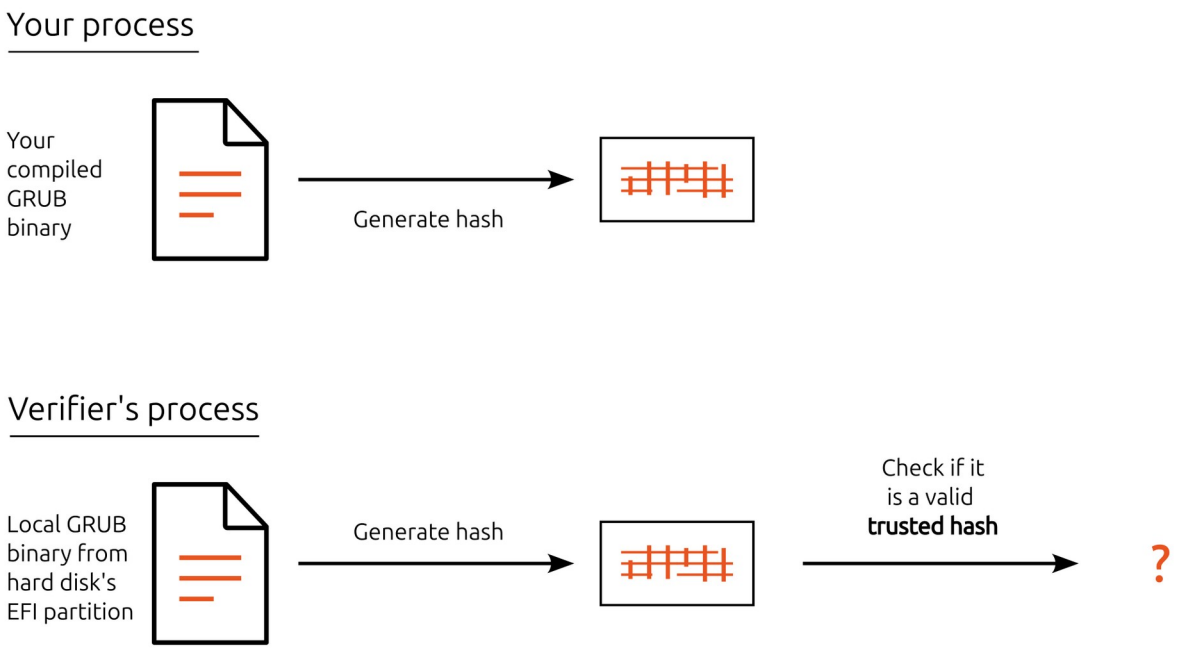
Verification of vendor-signed module



Verification of an unsigned module



Verification of an unsigned module



Enabling Tech: UEFI

Enabling Tech: UEFI

Unified Extensible Firmware Interface (UEFI)

Defines the firmware architecture

Defines the secure boot process

Enabling Tech: UEFI

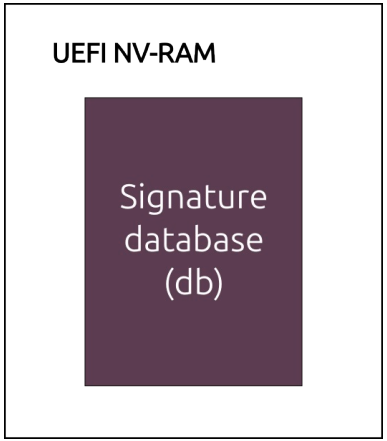
Unified Extensible Firmware Interface (UEFI)

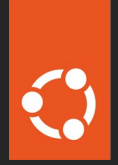
Defines the firmware architecture

Defines the secure boot process

Signature database (db):

- “allowed list”
- digital certificates of trusted vendors
- hashes of trusted modules





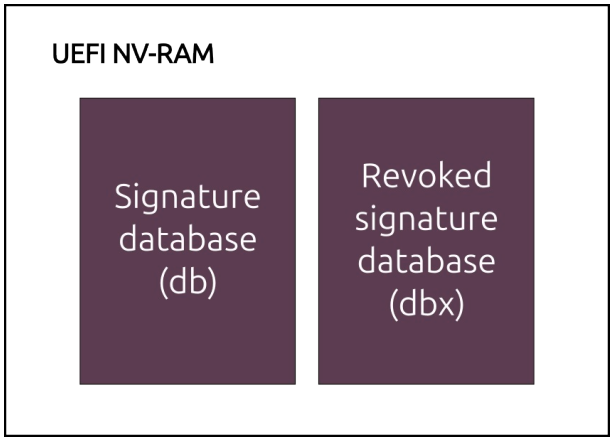
What if private keys are stolen?

What if trusted modules have vulnerabilities?

Enabling Tech: UEFI

Signature database (db):

- “allowed list”
- digital certificates of trusted vendors
- hashes of trusted modules



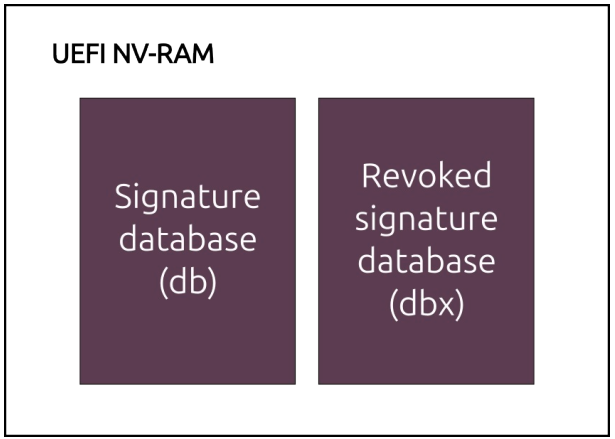
Enabling Tech: UEFI

Signature database (db):

- “allowed list”
- digital certificates of trusted vendors
- hashes of trusted modules

Revoked signature database (dbx):

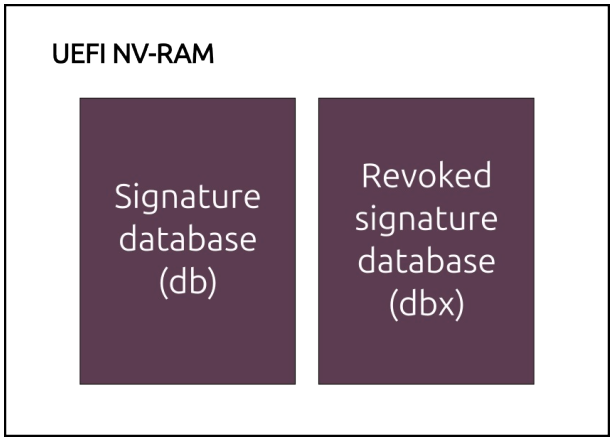
- “banned list”
- Revoked digital certificates (stolen keys)
- Hashes of known malwares (signed or unsigned)
- Signatures of vulnerable modules (older versions)



Enabling Tech: UEFI

Signature database (db):

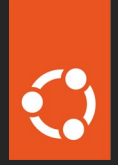
- “allowed list”
- digital certificates of trusted vendors
- hashes of trusted modules



Revoked signature database (dbx):

- “banned list”
- Revoked digital certificates (stolen keys)
- Hashes of known malwares (signed or unsigned)
- Signatures of vulnerable modules (older versions)

UEFI loads a module only if it is **not in dbx** and it **is in db**



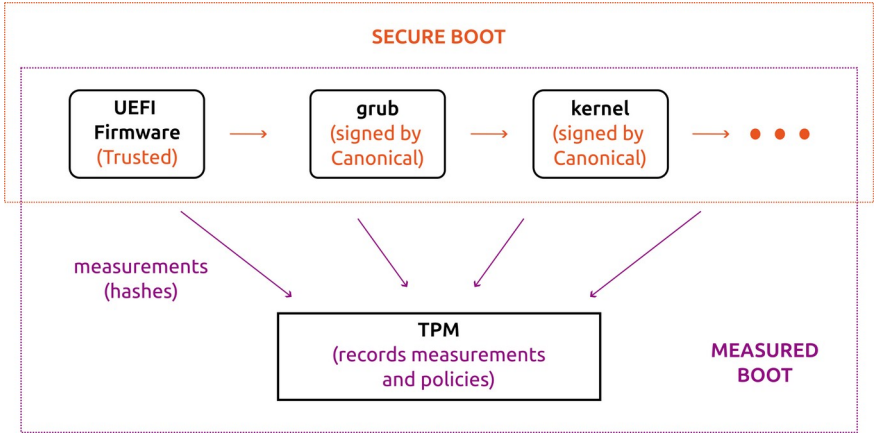
The modules may be trusted, but are they the expected ones?

What if a new, unknown threat manages to get a valid signature?

Solution: Measured Boot + Attestation

Measured Boot:

- Part of the UEFI spec
- Generates and records hashes
- Creates a verifiable audit trail



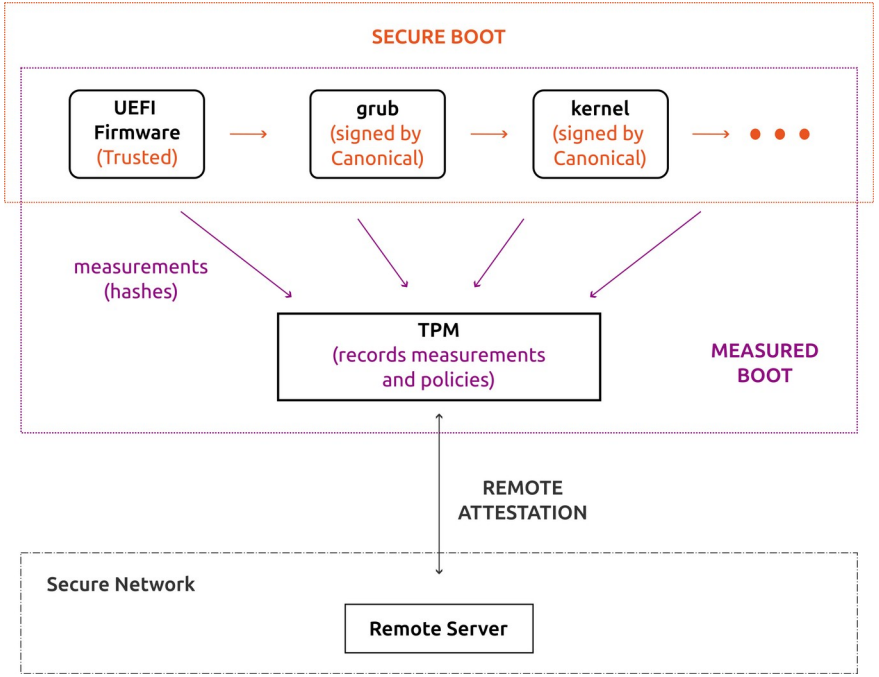
Solution: Measured Boot + Attestation

Measured Boot:

- Part of the UEFI spec
- Generates and records hashes
- Creates a verifiable audit trail

Remote Attestation:

- Remote server verifies the log
- Grants access only if the machine state matches expected policy



Enabling Tech: TPM

Enabling Tech: TPM

Trusted Platform Module (TPM)

- a specialized tamper-resistant security chip
- stores sensitive data like encryption keys and digital certificates
- performs cryptographic operations safely, away from the main CPU

Enabling Tech: TPM

Trusted Platform Module (TPM)

- a specialized tamper-resistant security chip
- stores sensitive data like encryption keys and digital certificates
- performs cryptographic operations safely, away from the main CPU

Hash values are recorded in the TPM's Platform Configuration Registers (PCRs)

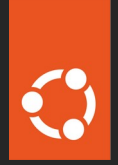
Enabling Tech: TPM

Trusted Platform Module (TPM)

- a specialized tamper-resistant security chip
- stores sensitive data like encryption keys and digital certificates
- performs cryptographic operations safely, away from the main CPU

Hash values are recorded in the TPM's Platform Configuration Registers (PCRs)

Creates the audit trail log and signs it



Boot process modules are trusted, but what about the root file system?

Someone with physical access could easily remove the hard-disk and tamper it!

Solution: Full-Disk Encryption (FDE)

Solution: Full-Disk Encryption (FDE)

Everything on the hard-disk is encrypted

Solution: Full-Disk Encryption (FDE)

Everything on the hard-disk is encrypted

CPU uses a symmetric key to encrypt/decrypt
- stored on the disk itself
- encrypted / “sealed” using another key

Solution: Full-Disk Encryption (FDE)

Everything on the hard-disk is encrypted

CPU uses a symmetric key to encrypt/decrypt
- stored on the disk itself
- encrypted / “sealed” using another key

TPM or user’s password provides this other key

Solution: Full-Disk Encryption (FDE)

Everything on the hard-disk is encrypted

CPU uses a symmetric key to encrypt/decrypt
- stored on the disk itself
- encrypted / “sealed” using another key

TPM or user’s password provides this other key

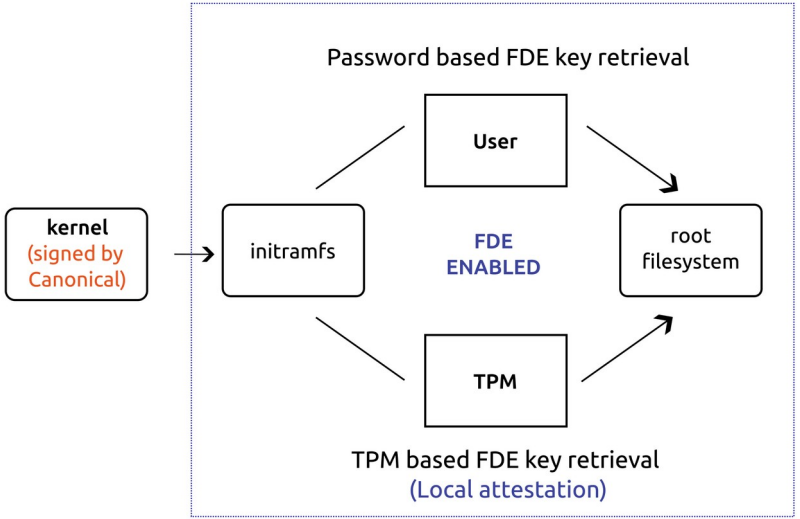
Hardware accelerator built into the CPU makes it fast

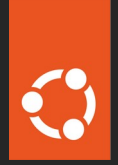
Added protection: Local Attestation

If TPM is used:

- Unseals the FDE key only if machine state matches expected policy

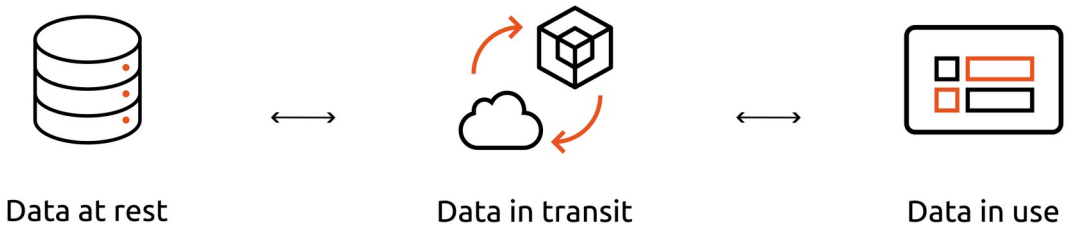
- Matches current PCR values with a specific pre-approved set



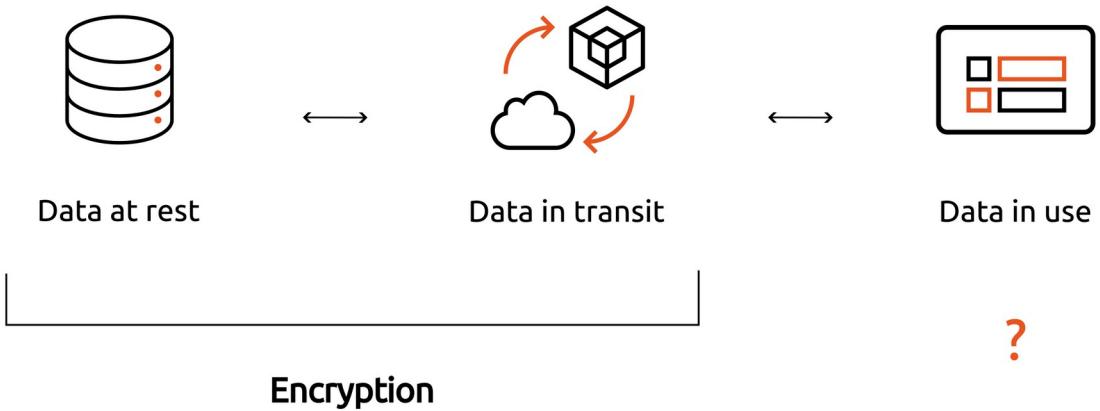


Can we trust anything in a cloud?

Converted problem: Protect data

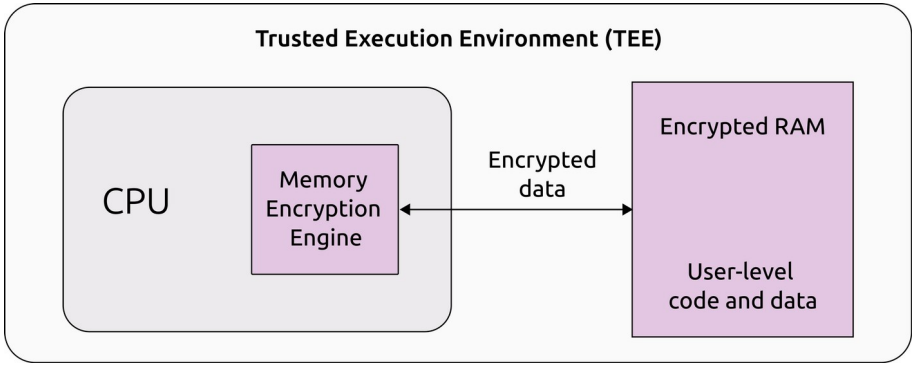


Converted problem: Protect data

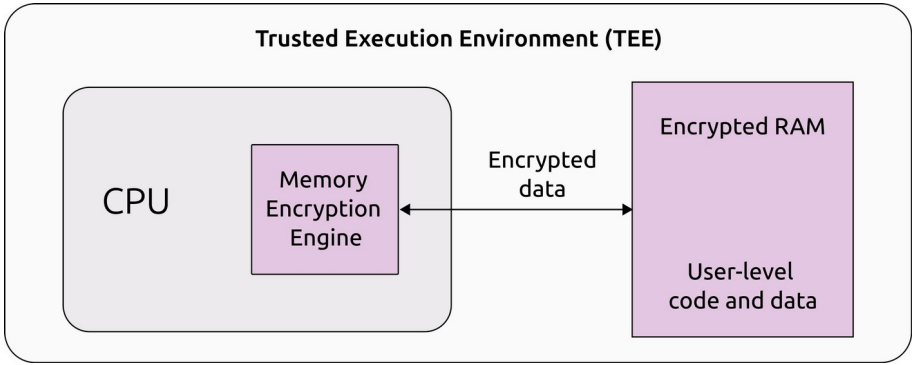


Solution: Confidential Computing

Solution: Confidential Computing



Solution: Confidential Computing



Trusted Execution Environment (TEE)

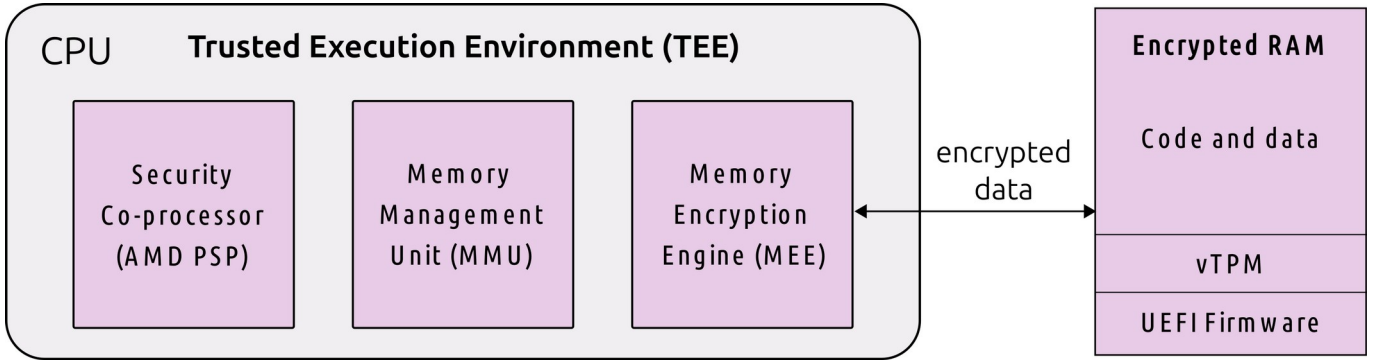
Isolation - No unauthorized access to code and data

Encryption - Data if accessed should be unreadable

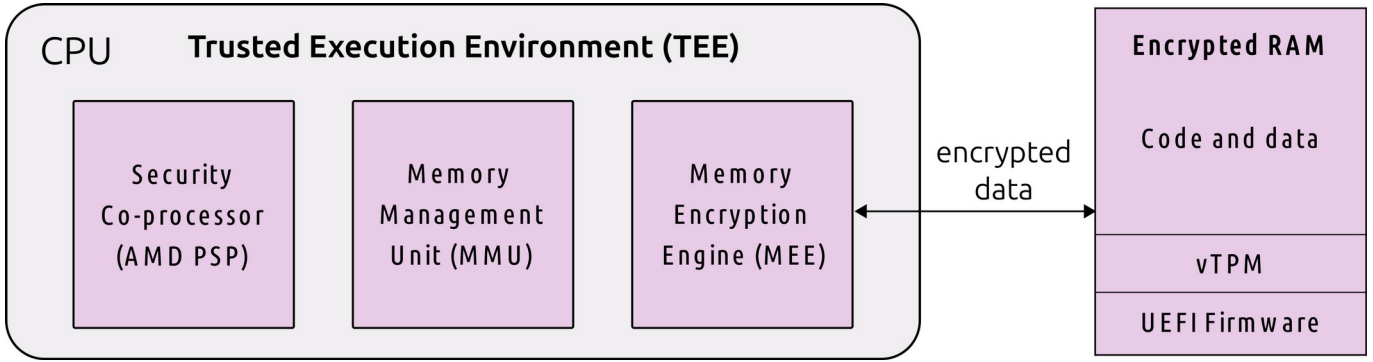
Attestation - Ability to prove its own identity and integrity

TEE Implementation

TEE Implementation

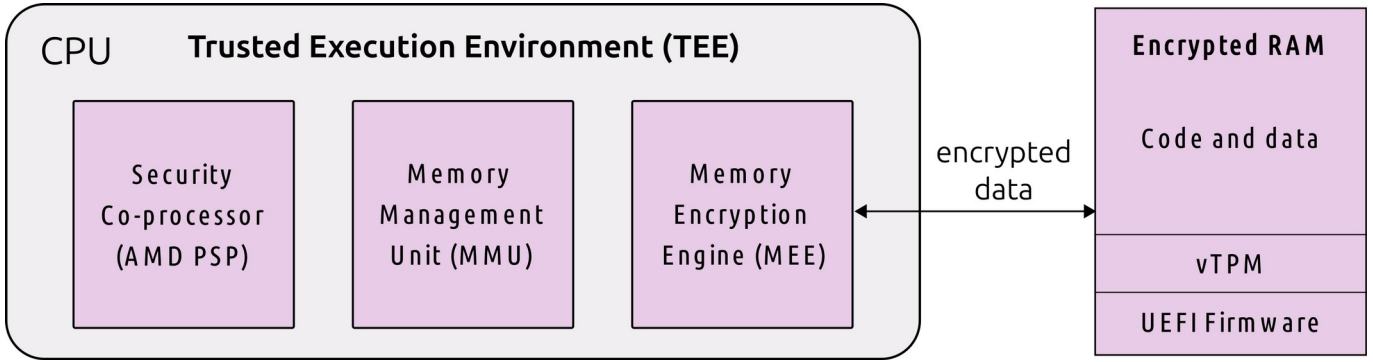


TEE Implementation



Isolation – Handled by Security Co-Processor and MMU using unique IDs for each CVM and their respective memory pages

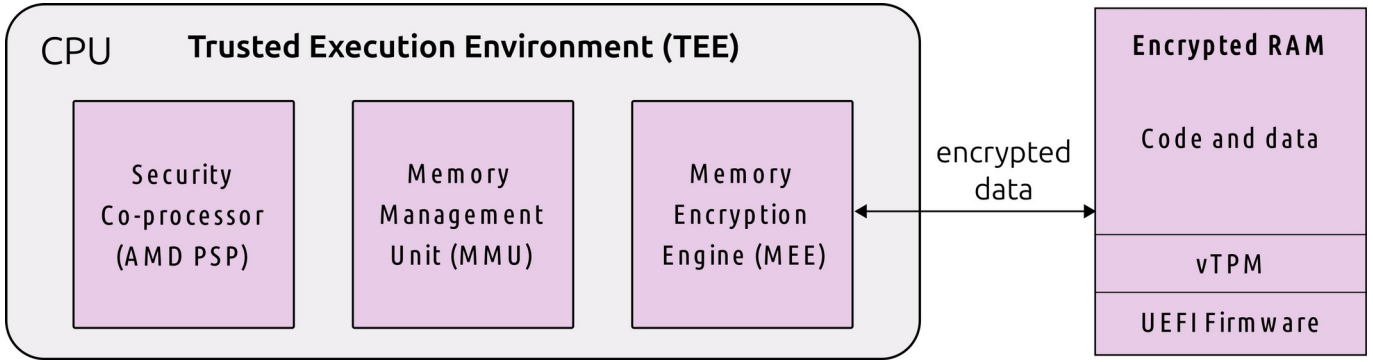
TEE Implementation



Isolation – Handled by Security Co-Processor and MMU using unique IDs for each CVM and their respective memory pages

Encryption – Handled by MEE on the fly

TEE Implementation

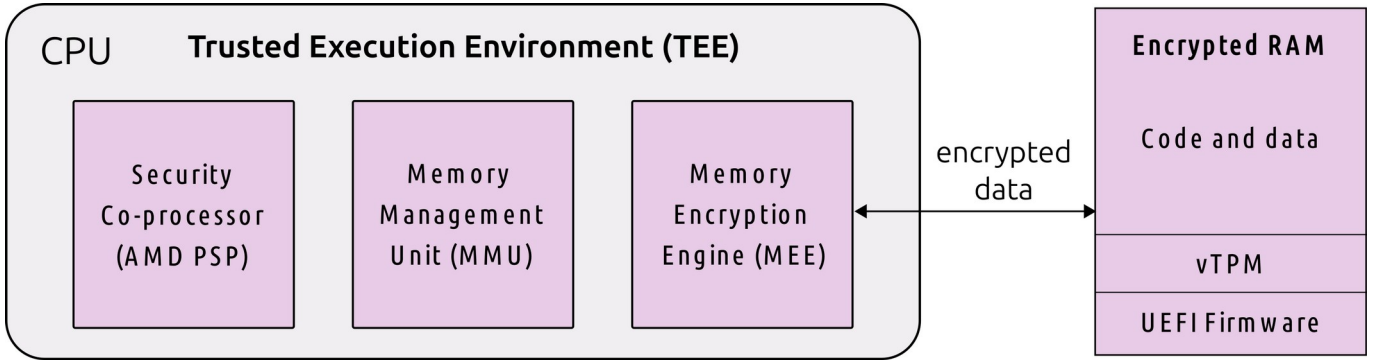


Isolation – Handled by Security Co-Processor and MMU using unique IDs for each CVM and their respective memory pages

Encryption – Handled by MEE on the fly

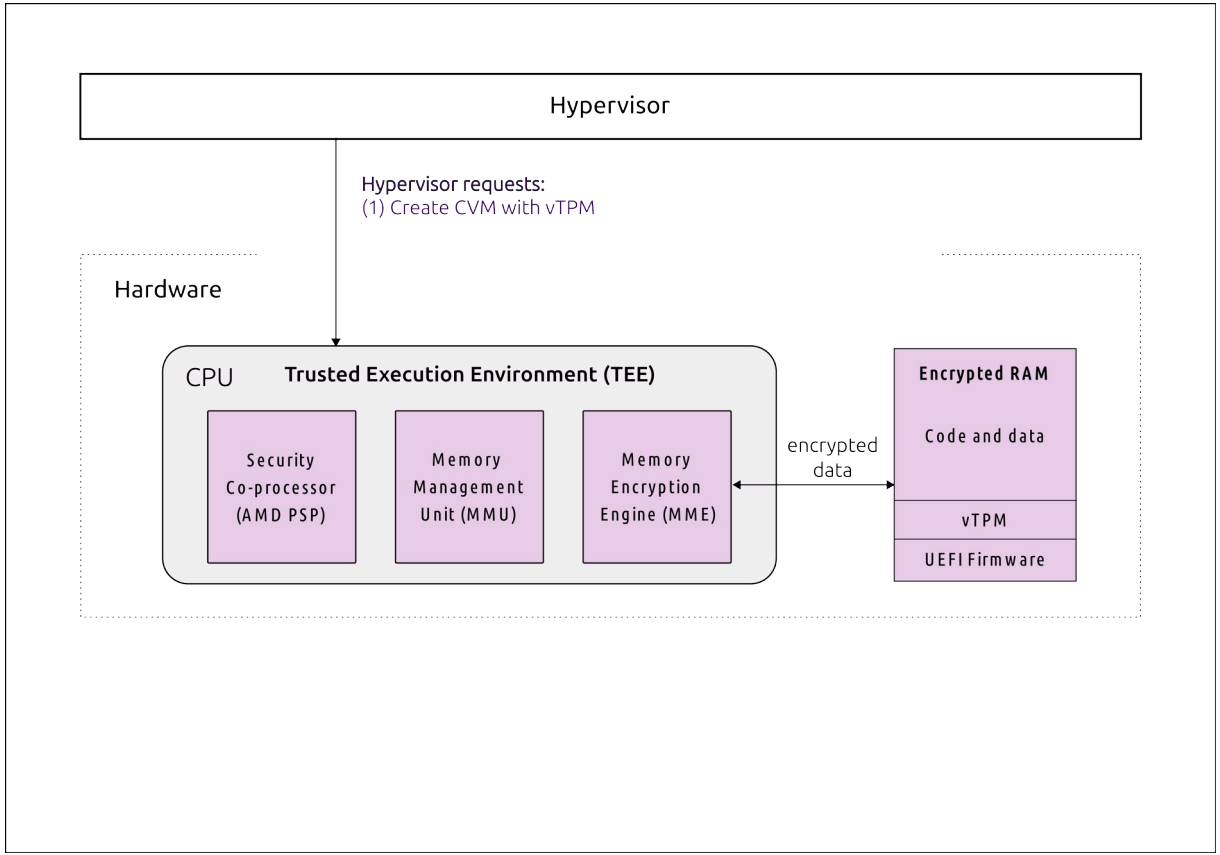
Attestation – Handled by vTPM and Security Co-Processor to generate an attestation report about the CVM and TEE state

TEE Implementation

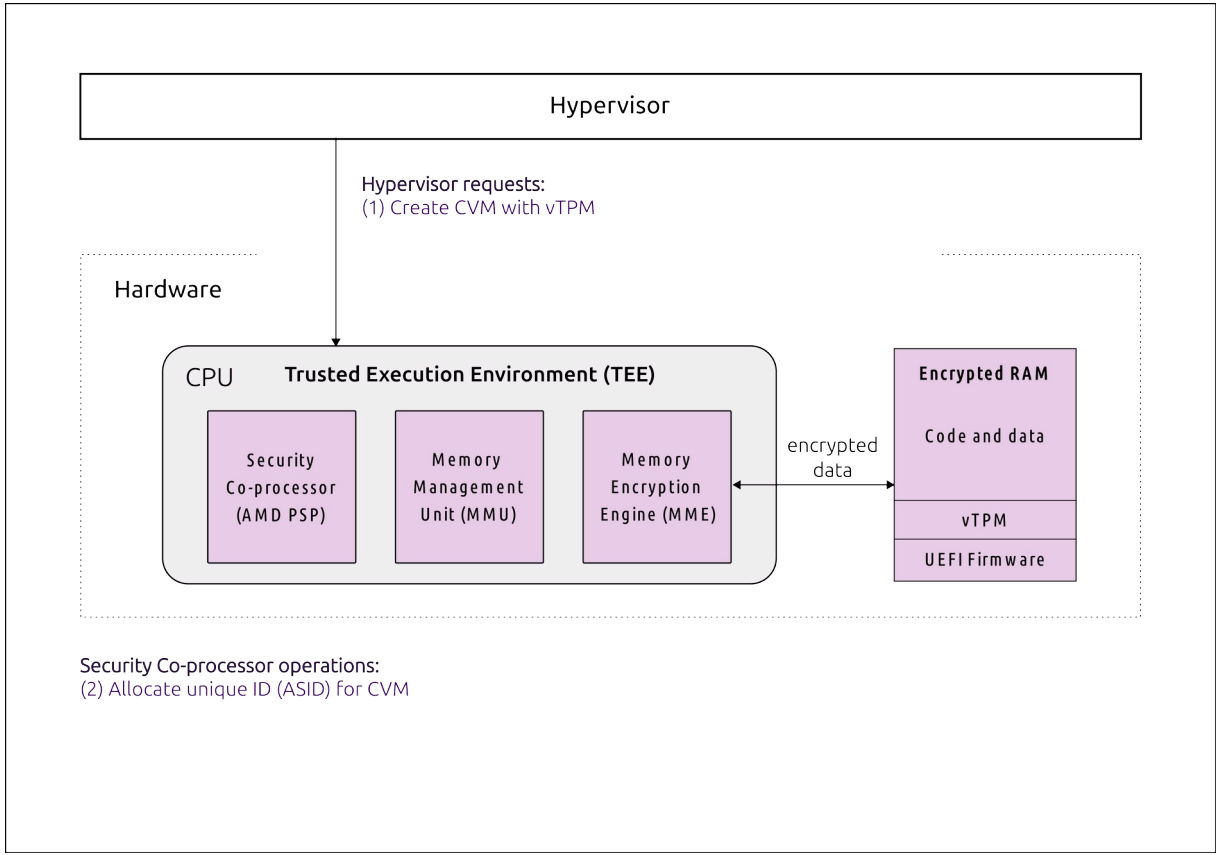


Enabling Tech: Intel TDX
AMD SEV-SNP
NVIDIA H100 GPUs

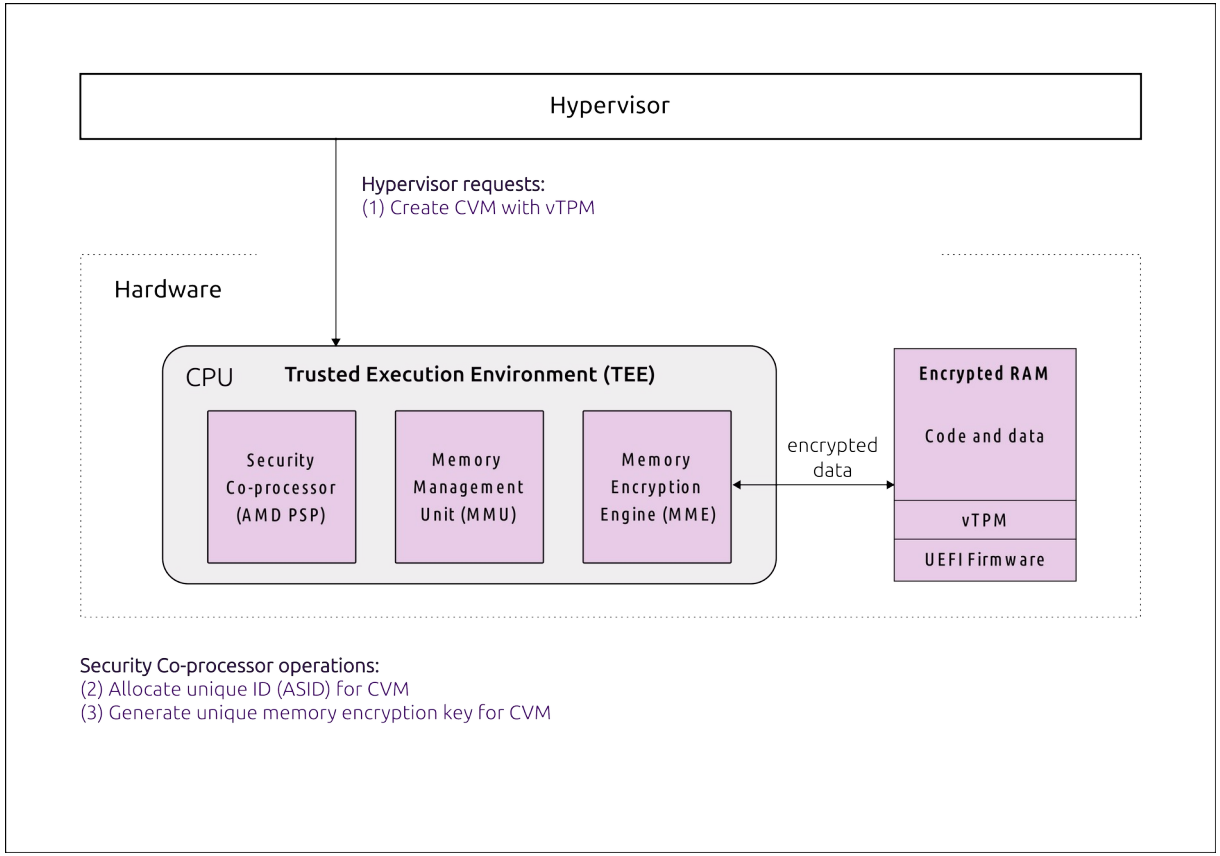
CVM launch process



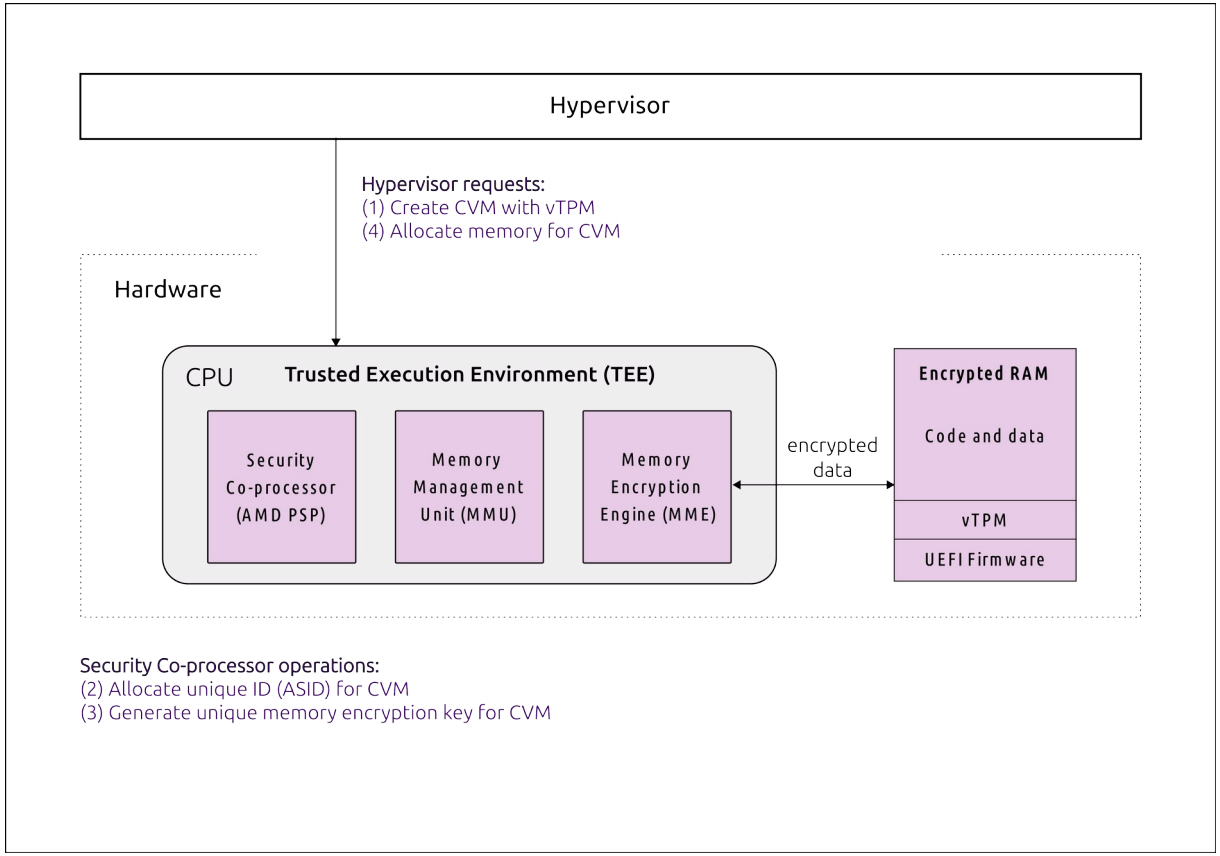
CVM launch process



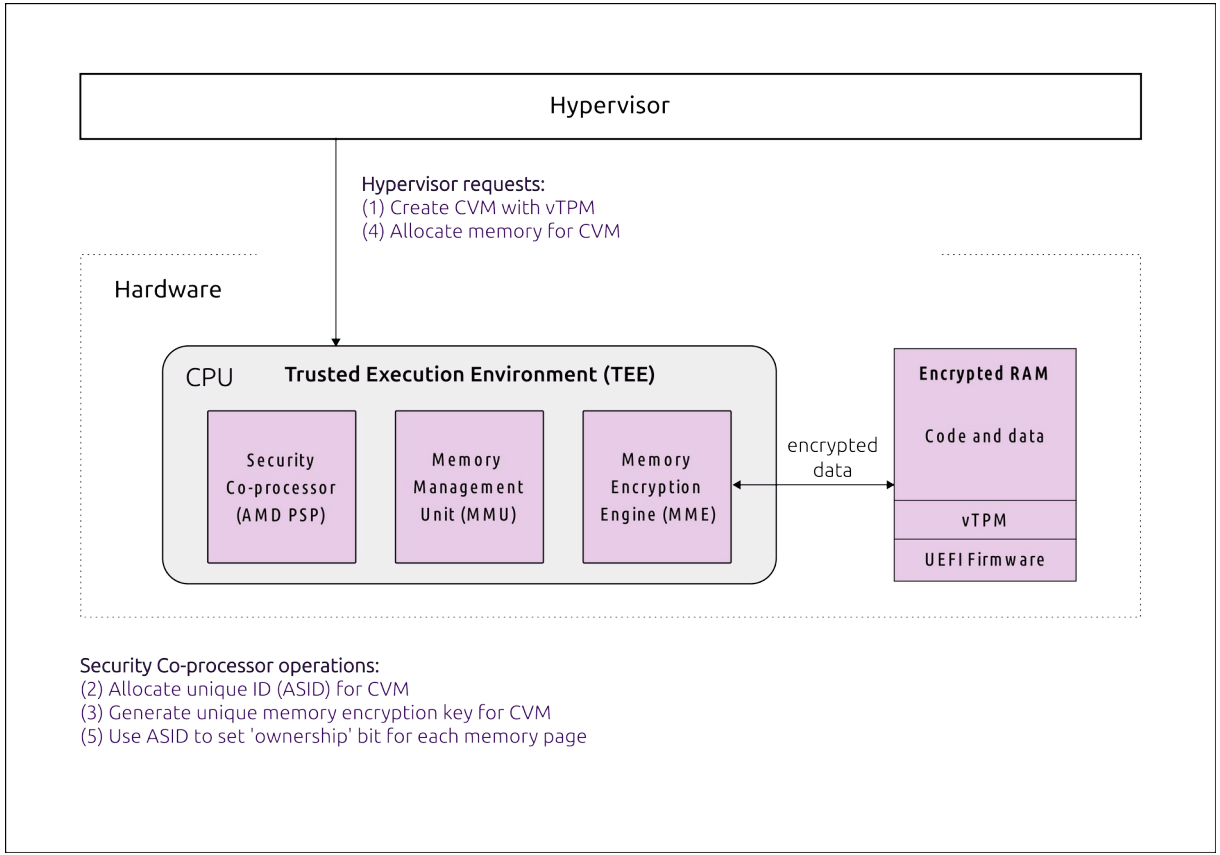
CVM launch process



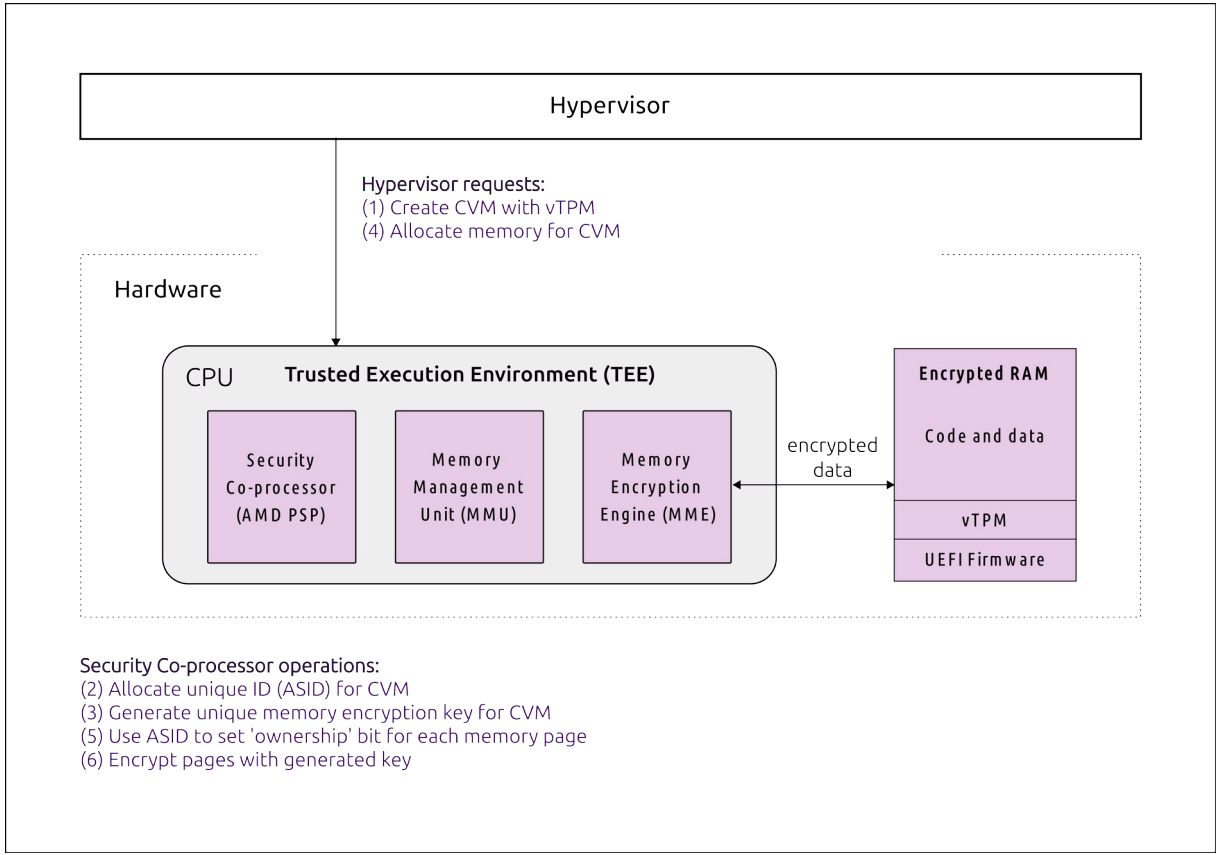
CVM launch process



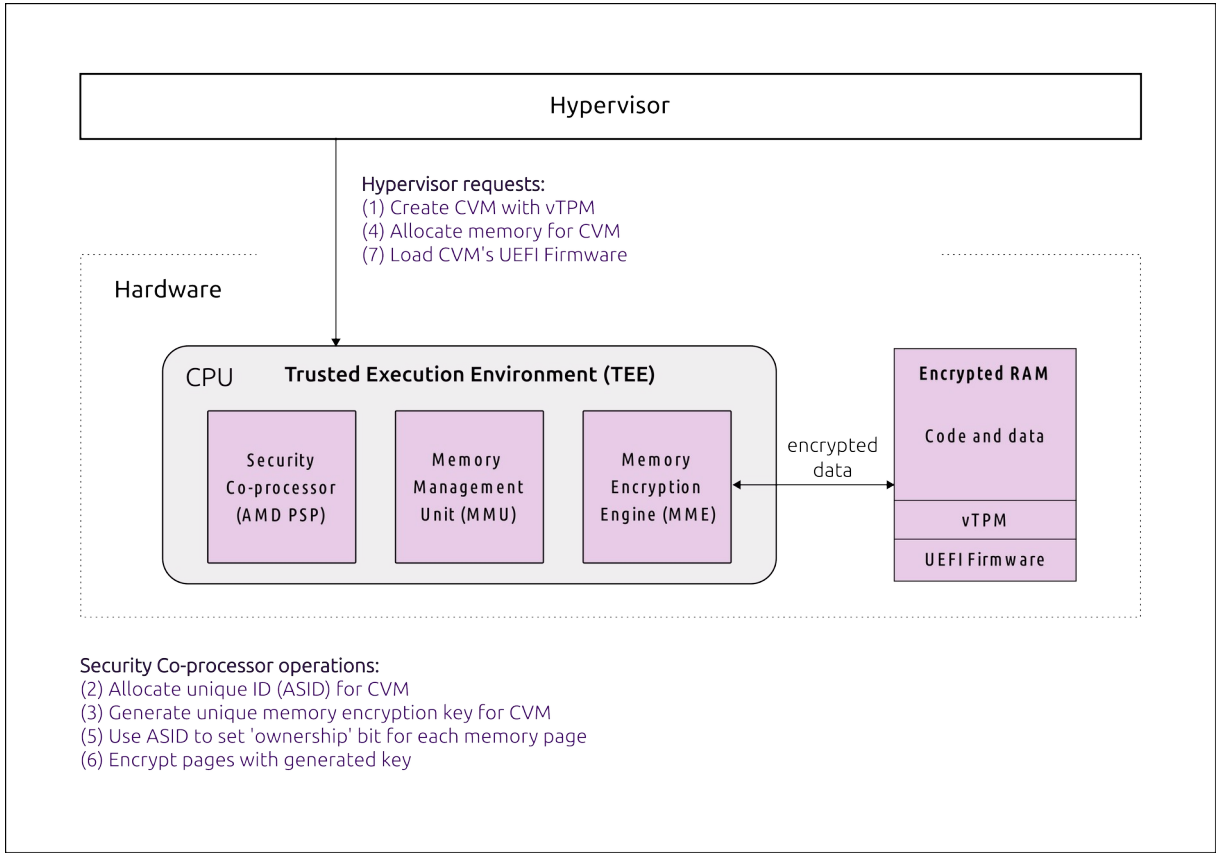
CVM launch process



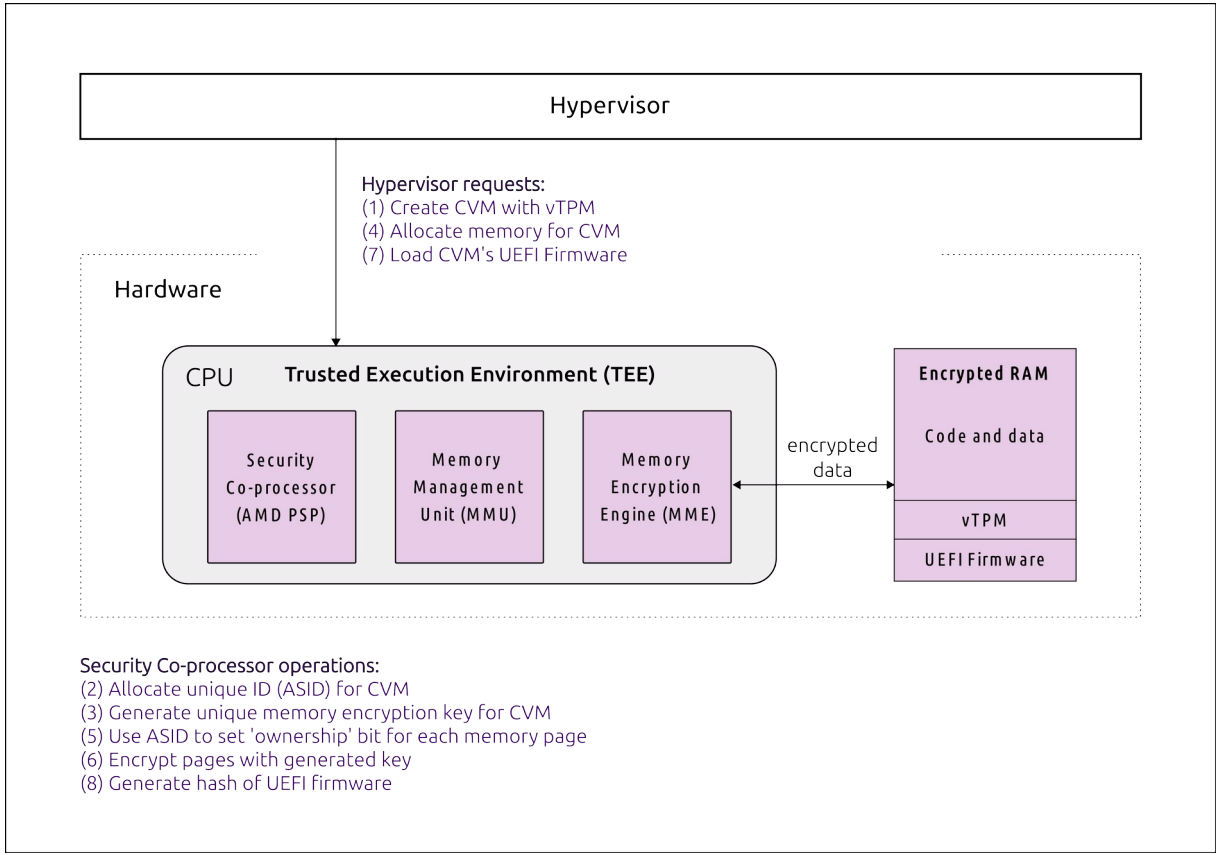
CVM launch process



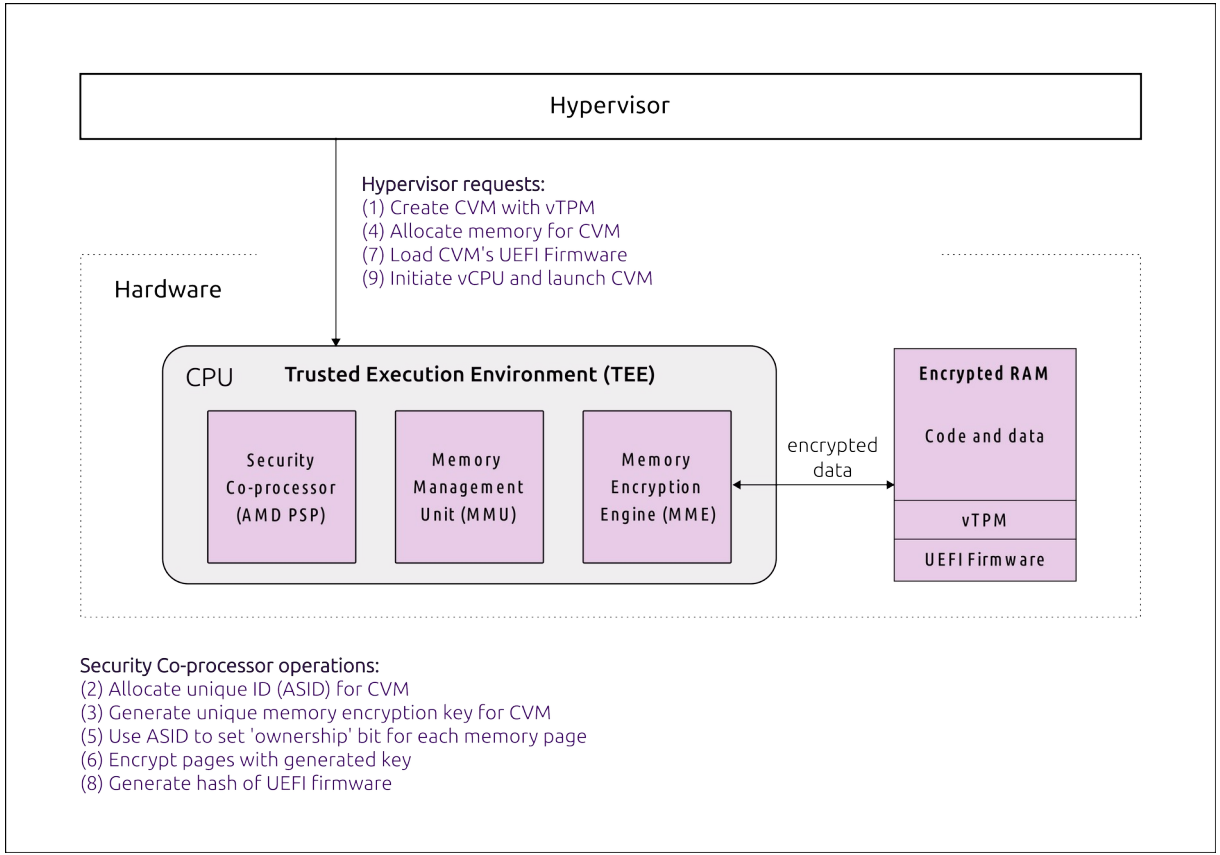
CVM launch process



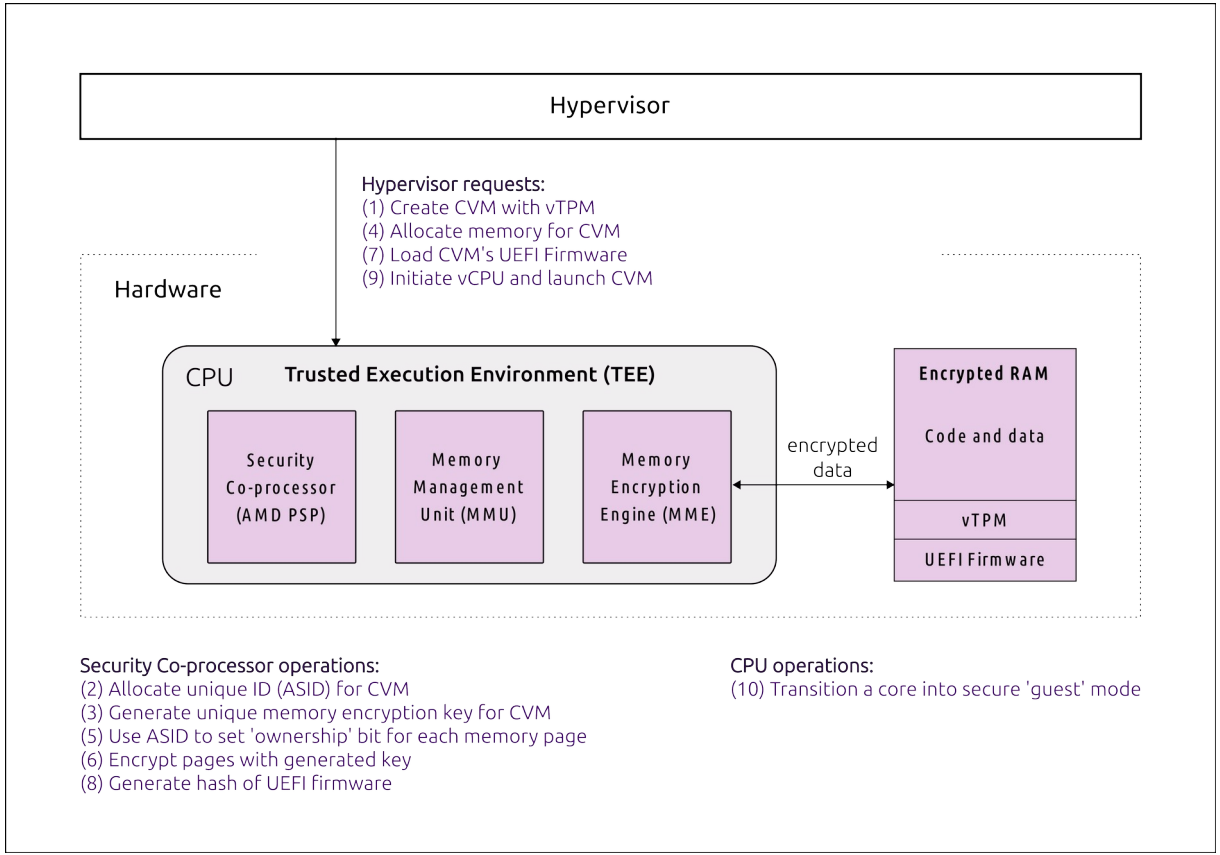
CVM launch process



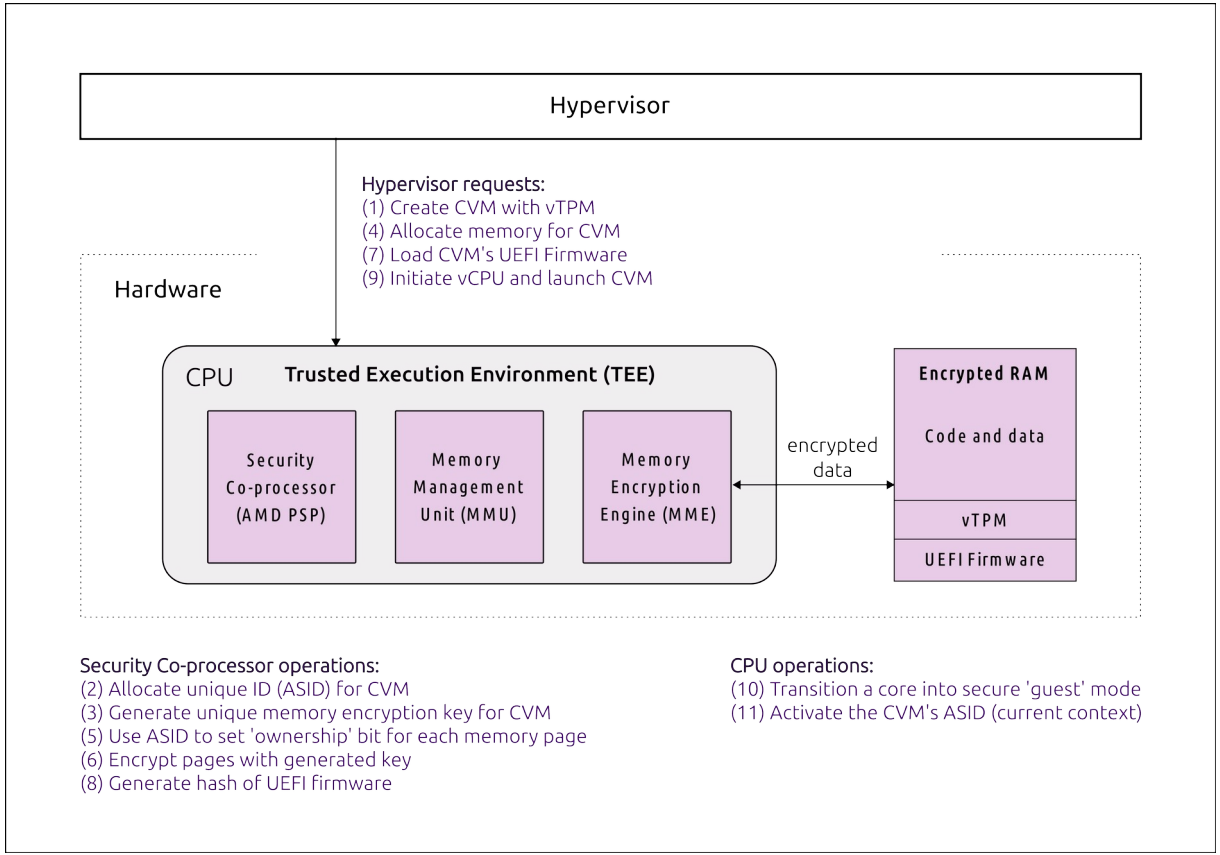
CVM launch process



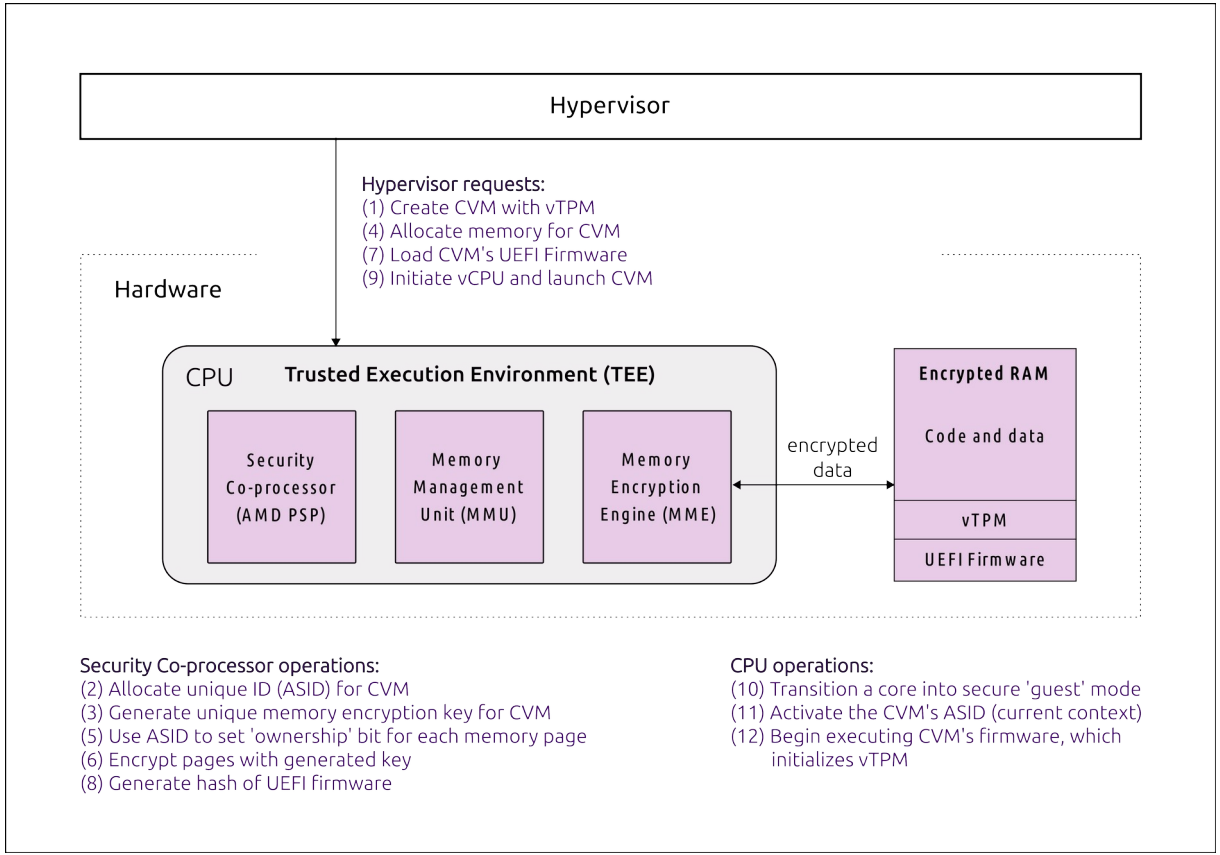
CVM launch process



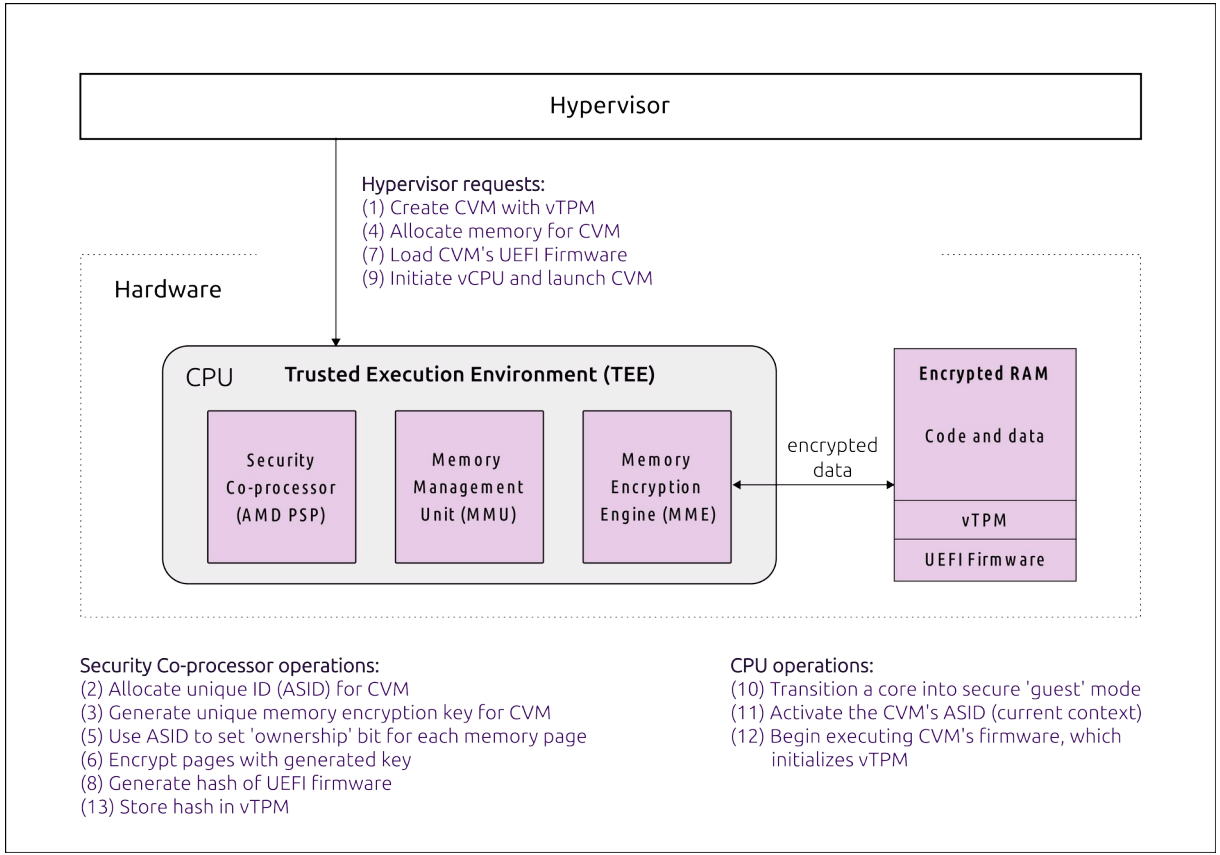
CVM launch process



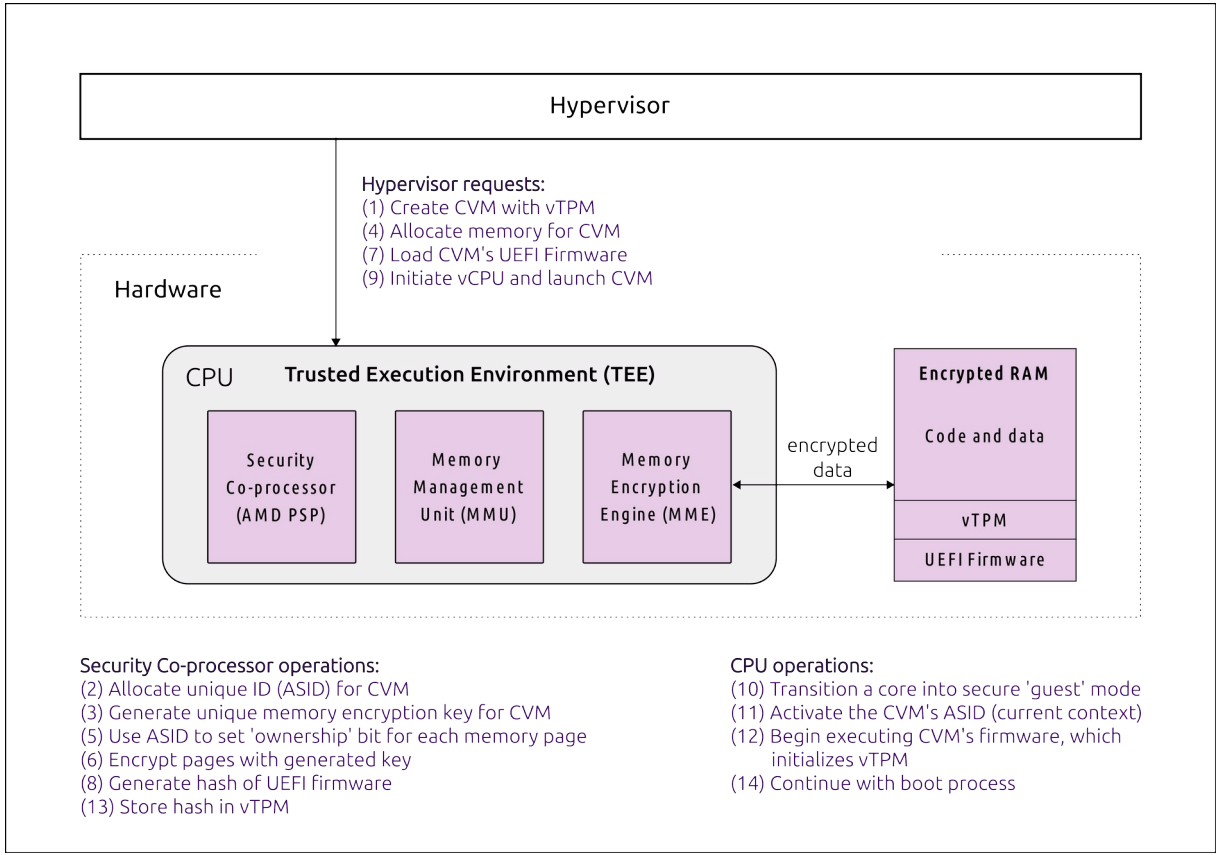
CVM launch process



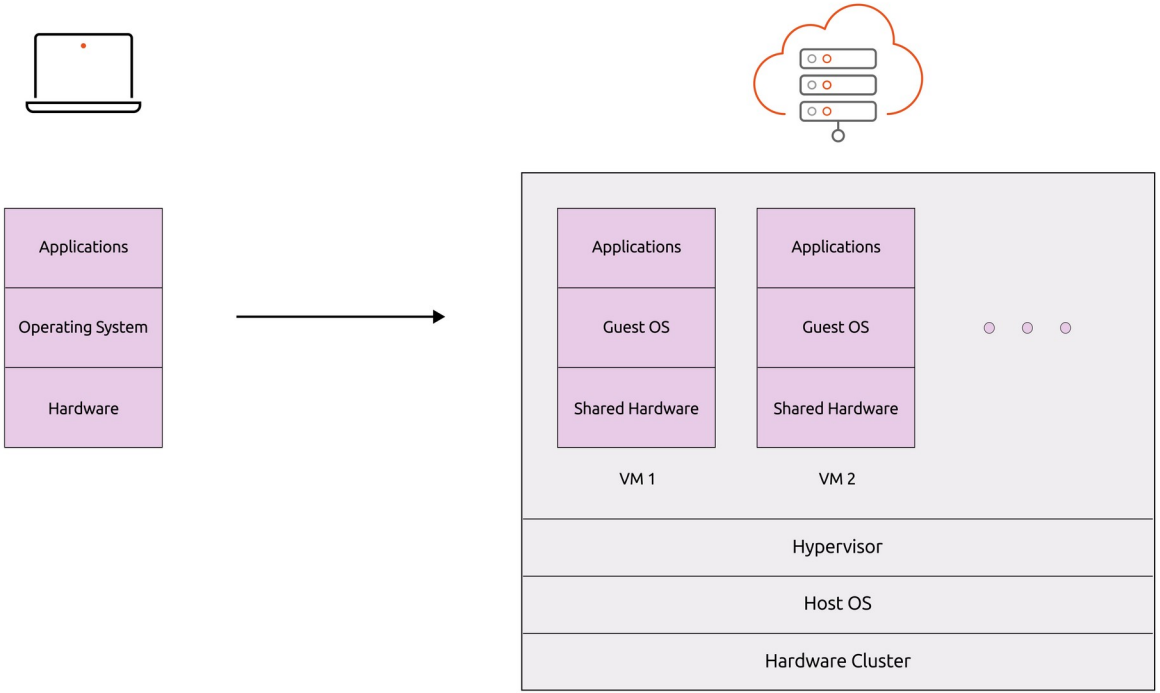
CVM launch process



CVM launch process



Confidential Computing



Security / CC at a glance ..

Threats	Security measures	Enabling technologies
Physical access Boot/Root kits	Secure Boot, Measured Boot Remote Attestation, FDE	UEFI firmware Trusted Platform Module (TPM)
Malicious software Bugs in software	System hardening, Access control Handling vulnerabilities	Ubuntu Security Guide AppArmor, Ubuntu Pro
Malicious host Malicious hypervisor Root user compromises Memory dump attack Untrusted cloud provider	Confidential Computing (TEE + Remote attestation)	Intel TDX AMD SEV-SNP NVIDIA H100

Availability of Confidential VMs

Available on most major public clouds:

Enabling technologies:

Thank you! Questions?