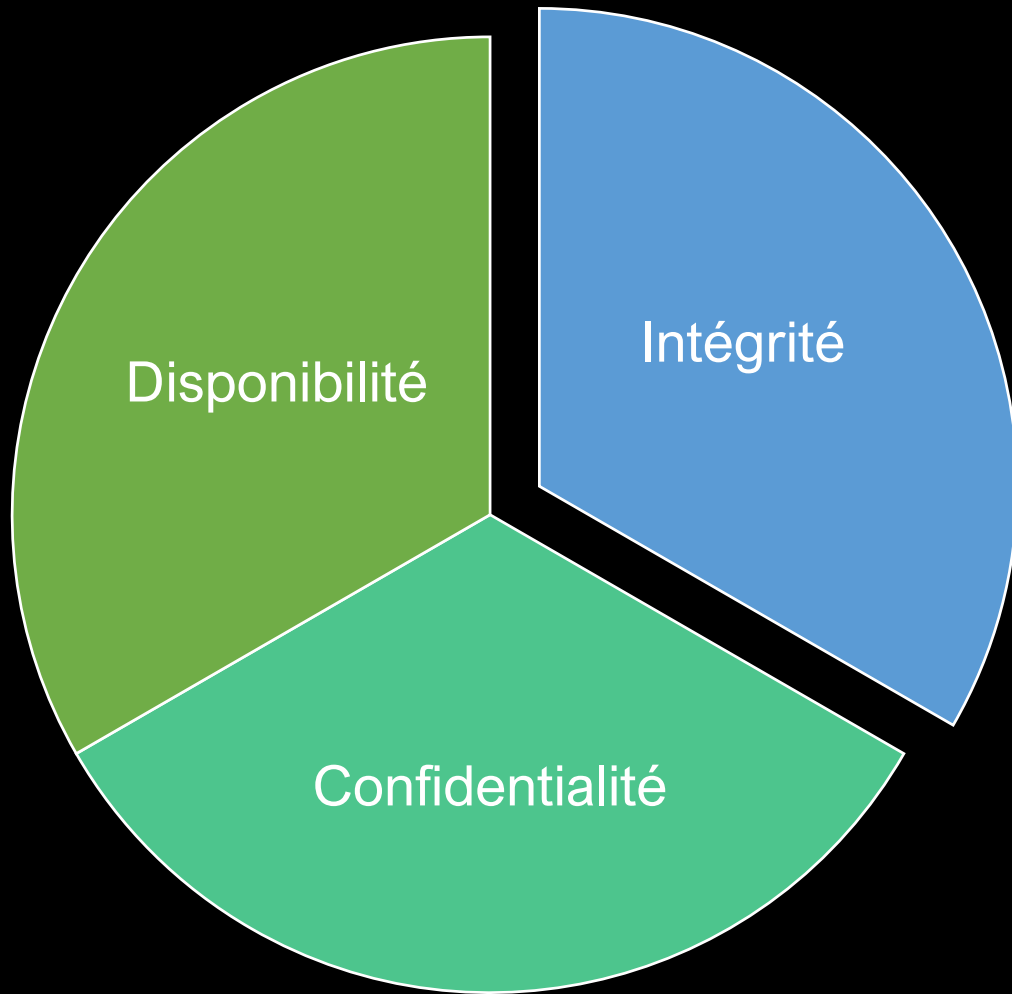


Environnement d'exécution sécurisé (TEE)

SRIO

Djob Mvondo

Principes de sécurité



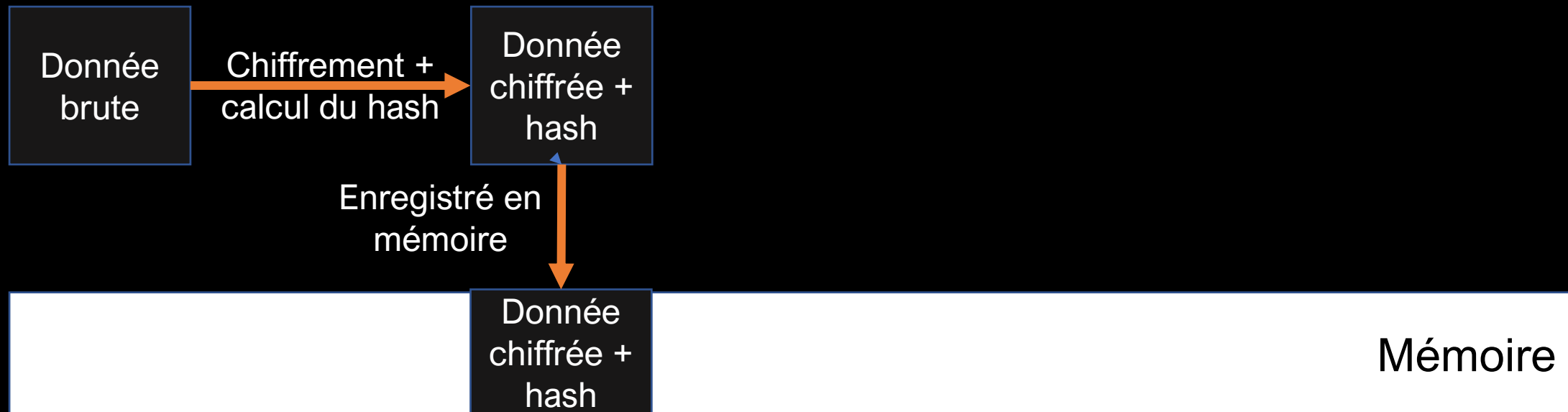
Ces trois éléments sont d'une importance capitale.

Néanmoins il y'a un qui semble être plus complexe que les autres

Quelles sont les techniques pour assurer l'intégrité d'un système ?

Donc c'est parfait?

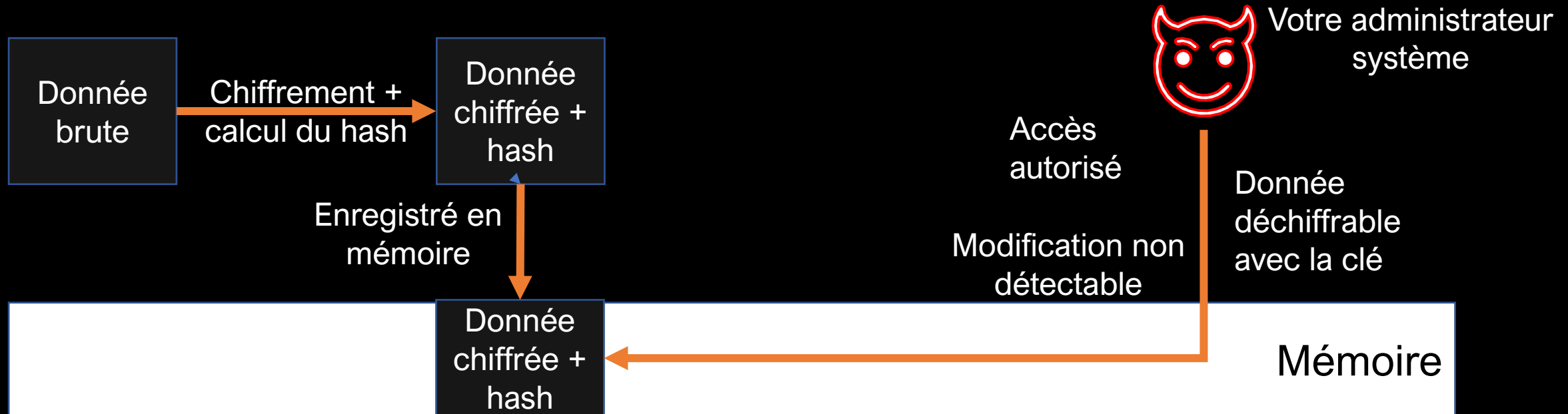
Hashing + Chiffrement etc...



Quelles sont les techniques pour assurer l'intégrité d'un système ?

Hashing + Chiffrement etc...

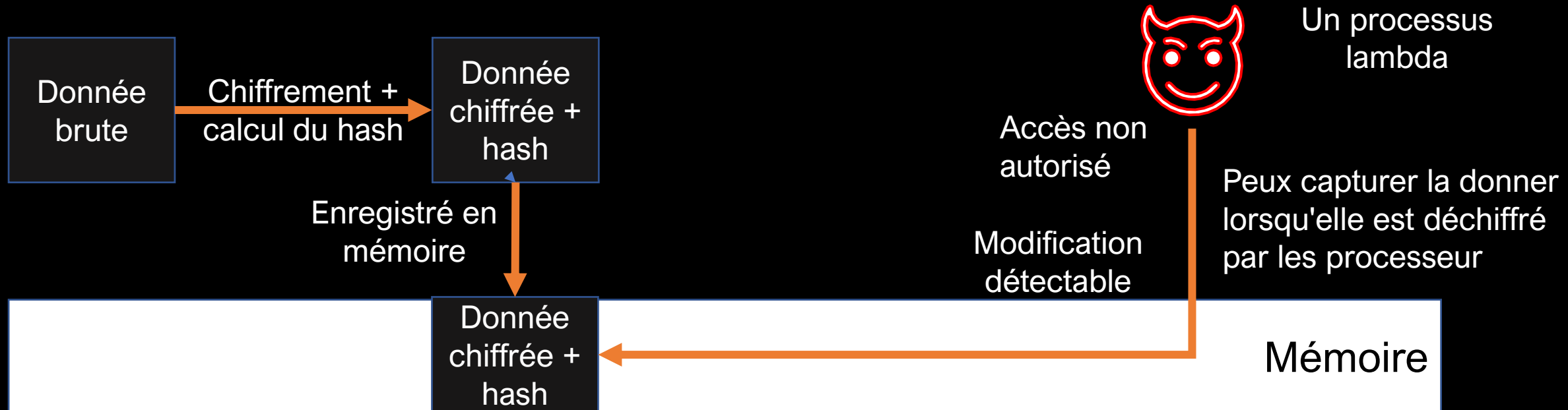
Malheureusement non



Quelles sont les techniques pour assurer l'intégrité d'un système ?

Hashing + Chiffrement etc...

Malheureusement non

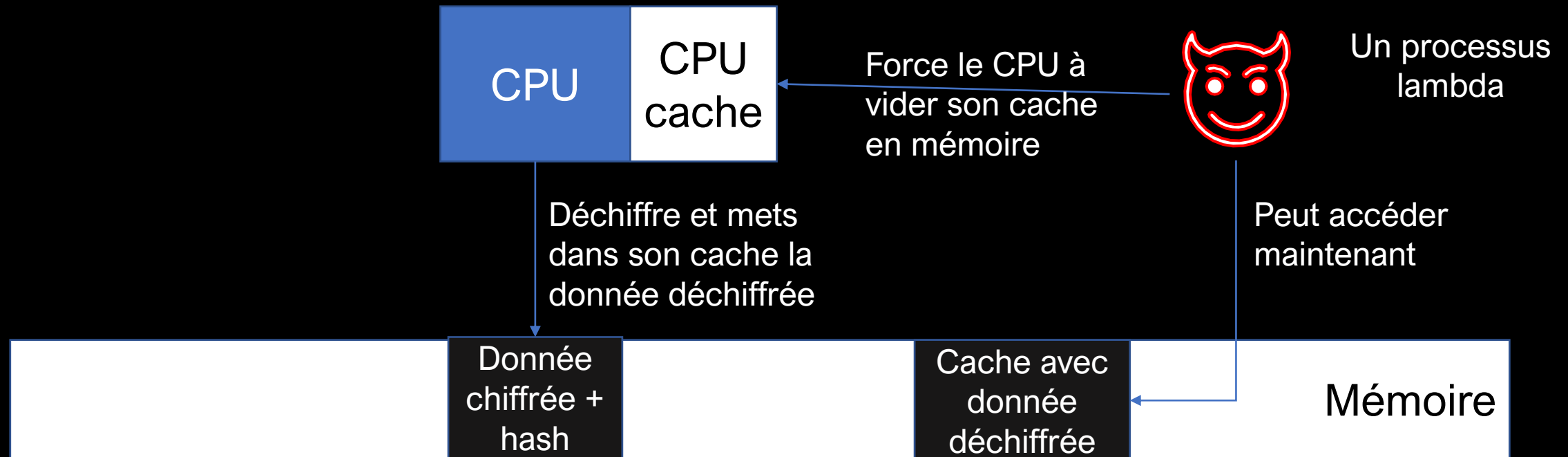


Quelles sont les techniques pour assurer l'intégrité d'un système ?

Peux capturer la donnée lorsqu'elle est déchiffrée par le processeur

Hashing + Chiffrement etc...

Malheureusement non



Quelles sont les techniques pour assurer l'intégrité d'un système ?

Hashing + Chiffrement etc... → **Insuffisant**

Administrateur

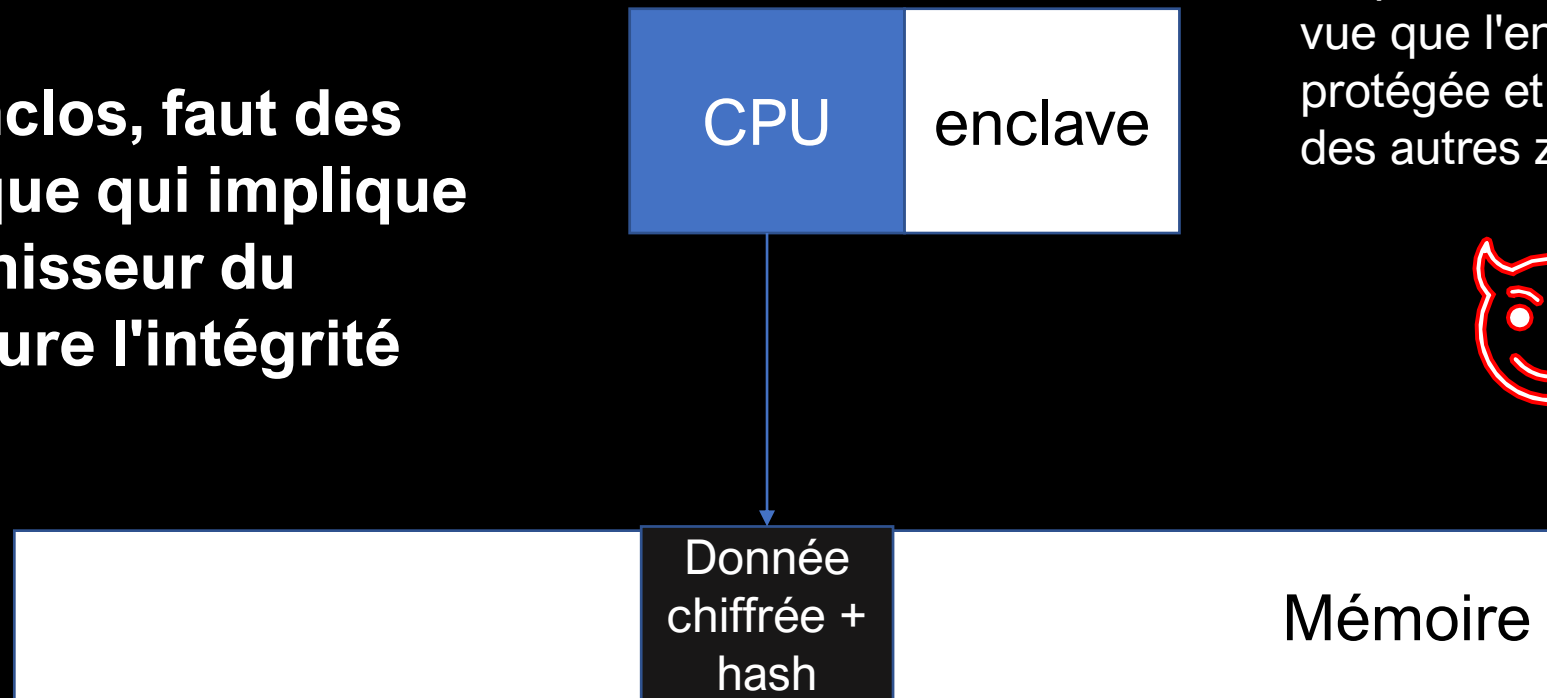
Utilisateur
lambda

Faut un support matériel

Environnement d'exécution sécurisé

Une zone appelée **enclos** dans le processeur qui n'est accessible que par le processus ayant la clé.

Pour accéder à l'enclos, faut des opérations spécifique qui implique l'agrément du fournisseur du processeur qui assure l'intégrité des clés.



Ne peut rien faire
vue que l'enclave est
protégée et séparé
des autres zones

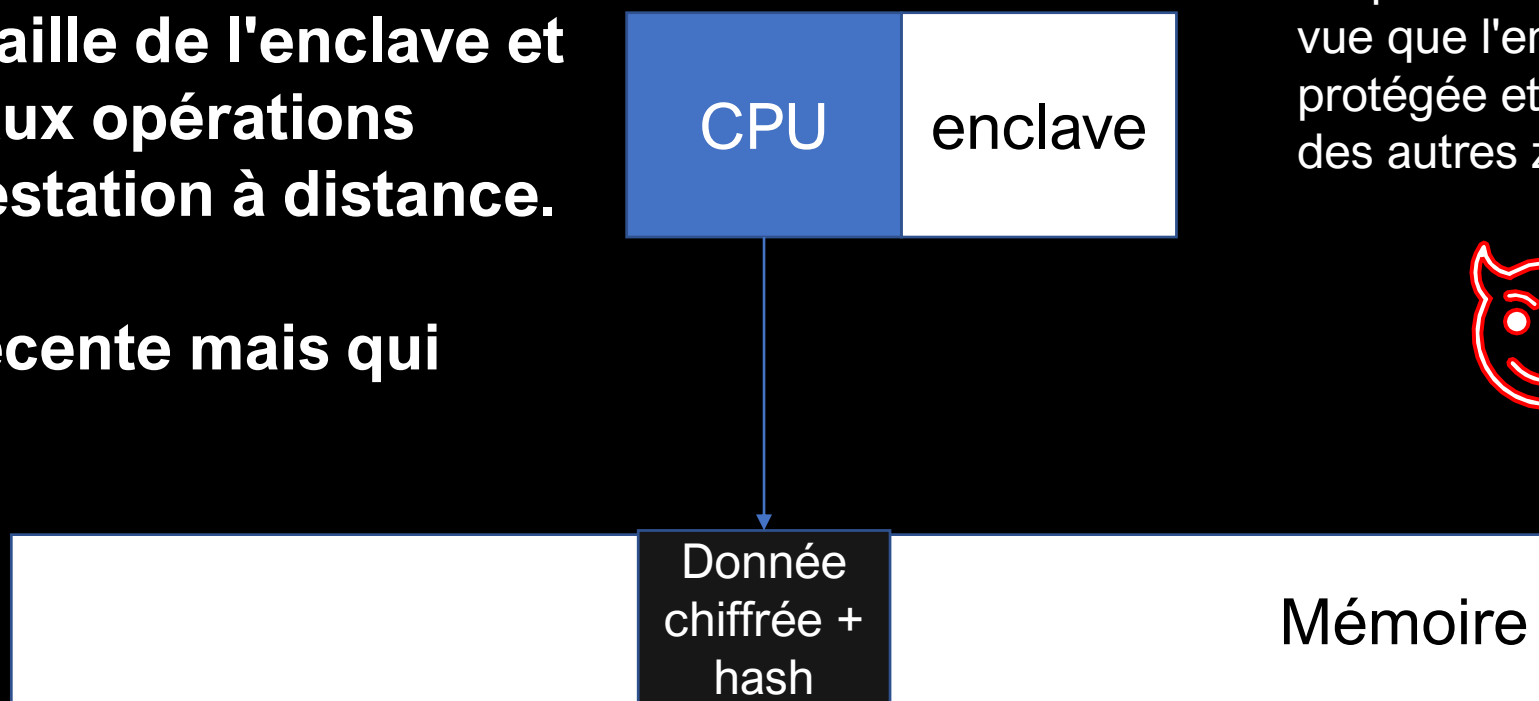


Environnement d'exécution sécurisé

Plusieurs constructeurs propose leur TEE: Intel SGX, AMD SEV, etc...

Des limitations, la taille de l'enclave et la dégradation du aux opérations spécifiques et l'attestation à distance.

Technologie très récente mais qui continue à évoluer.



Ne peut rien faire vue que l'enclave est protégée et séparé des autres zones

