Destruction de données sur supports de stockage locaux internes et externes

Par Adrien Ferron / lacapsule.org / Fédération régionale des reconditionneurs bretons OGO 2024

1.0.0 - Les différents types de supports de stockage

1.1.0 - Le disque dur mécanique HDD (hard disk drive)

1.1.1 - Introduction

Dans l'ensemble, le processus d'écriture et de lecture sur un disque dur repose sur la manipulation du champ magnétique pour représenter et extraire des données. Ce mécanisme est à la base des disques durs magnétiques traditionnels.

En général, les disques durs d'ordinateur classiques n'utilisent pas la spintronique de manière prédominante. Les disques durs traditionnels se basent sur la technologie magnétique pour stocker et récupérer des données, utilisant des têtes de lecture/écriture magnétiques pour manipuler les aimants présents sur le disque.

La spintronique, en revanche, est une branche de la physique qui exploite les propriétés de spin des électrons en plus de leur charge électrique. Bien que la spintronique soit utilisée dans certains dispositifs électroniques avancés, tels que les dispositifs à magnétorésistance géante (GMR) présents dans certains types de capteurs et de mémoires, elle n'est pas la technologie dominante dans les disques durs standard.

L’électron a de nombreuses propriétés dont la charge et le spin. L’électricité puis l’électronique utilisent la charge de l’électron pour transporter une information, alimenter des appareils ou encore effectuer des opérations logiques.

Les premières applications spintroniques ont vu le jour au XXe siècle, bien que les études théoriques aient débutées dès le XIXe siècle avec les équations de Maxwell dans les milieux magnétiques. Le premier grand succès de la spintronique est néanmoins la création du disque dur.

1.1.2 - Principes

Les disques durs d'ordinateur utilisent le stockage magnétique pour lire et écrire des données. Voici un aperçu des principes physiques impliqués dans ces opérations :

Média magnétique

Le cœur du disque dur est son média magnétique, généralement constitué de plusieurs plateaux circulaires revêtus d'un matériau magnétique. Ces plateaux tournent à grande vitesse (typiquement à quelques milliers de tours par minute).

Tête de lecture/écriture

Chaque plateau possède une tête de lecture/écriture, qui est montée sur un bras mobile. Cette tête flotte très près de la surface du plateau sans la toucher, grâce à l'effet de lévitation magnétique ou à l'utilisation de paliers d'air.

Magnétisme

Les surfaces des plateaux sont magnétisées. Chaque bit d'information est représenté par l'orientation magnétique des particules sur le disque. Dans un état magnétique particulier, le bit peut être interprété comme 0 ou 1.

- **Écriture :** Lorsqu'on écrit des données, un courant électrique est appliqué à la tête de lecture/écriture, générant un champ magnétique. Ce champ magnétique modifie l'orientation des particules magnétiques sur le disque, enregistrant ainsi les données.
- **Lecture :** Lors de la lecture, la tête de lecture/écriture détecte les variations du champ magnétique en survolant la surface du disque. Ces variations sont interprétées comme des bits 0 ou 1, formant ainsi les données stockées.

Précision positionnelle

La précision de la position de la tête de lecture/écriture est essentielle. Les disques durs utilisent des systèmes de suivi précis pour déplacer les têtes rapidement et avec précision afin de lire ou d'écrire des données sur les différentes pistes concentriques du disque.

Gestion de la tête

Un actuateur contrôle la position du bras sur lequel est montée la tête de lecture/écriture. Ce mécanisme permet de déplacer la tête rapidement et précisément vers la piste souhaitée.

1.1.3 - Composition d'un disque HDD

Les plateaux circulaires coaxiaux

Les plateaux d'un disque dur sont des disques minces et rigides qui tournent autour d'un axe central. Chaque plateau est recouvert de deux couches de matériau magnétique, une sur chaque face. Les deux faces d'un plateau sont utilisées pour stocker des données. Les disques durs utilisent plusieurs plateaux, ce qui leur permet d'obtenir une grande capacité de stockage.

Les moteurs rotatifs

Il permet le mouvement des plateaux et des têtes de lecture/écriture. Il y a deux types de moteurs dans un disque dur : un pour faire tourner les plateaux et un autre pour déplacer les têtes de lecture-écriture.

Les têtes de lecture

Les têtes de lecture sont constituées de deux parties principales : la partie supérieure, appelée "head", et la partie inférieure, appelée "tail". La tête est l'élément qui vient en contact avec le plateau pour lire ou écrire des données. La queue sert à guider la tête dans son mouvement.

Lors de la lecture, la tête de lecture déplace légèrement la surface du plateau pour créer un champ magnétique, ce qui induit un courant dans la tête de lecture. Ce courant est ensuite transformé en signal électrique par un convertisseur analogique numérique (CAN), qui peut être interprété par l'ordinateur.

Lors de l'écriture, les têtes de lecture génèrent un champ magnétique qui change la direction du champ magnétique sur la surface du plateau, permettant ainsi d'écrire des données.

En plus des têtes inductives, qui sont les plus couramment utilisées dans les disques durs traditionnels, il existe d'autres types de têtes de lecture qui peuvent être utilisées dans certains types de disques durs. Par exemple, les disques durs Shingled Magnetic Recording (SMR) utilisent des têtes à effet Hall, qui sont capables de lire et d'écrire des données sur les pistes d'un disque dur.

Les têtes à effet Hall sont conçues pour minimiser la friction avec les pistes de disque, ce qui permet d'augmenter la durée de vie du disque. Elles utilisent un champ magnétique pour générer un champ électromagnétique qui attire les particules de fer dans les pistes de disque, permettant ainsi la lecture et l'écriture des données.

Le bras électro-magnétique

Le bras électromagnétique d'un disque dur est un mécanisme crucial qui transporte les têtes de lecture/écriture au-dessus des plateaux du disque. Il est actionné par un moteur électromagnétique qui utilise un bobinage placé dans un champ magnétique créé par un aimant. Lorsque le courant est alimenté au bobinage, il génère un champ magnétique qui attire l'aimant, provoquant le mouvement du bras.

Le bras se déplace en injectant du courant mais le contrôle de ce mouvement est assez complexe. Par exemple, quand la tête doit aller lire une donnée à un endroit précis sur le disque, le courant injecté dans le bobinage du bras est contrôlé de manière précise pour déplacer la tête vers la position correcte.

La carte interface

La carte interface d'un disque dur est la partie du disque dur qui gère la communication entre le disque dur lui-même et le reste du système informatique. Elle est responsable de la transmission des données entre le disque dur et le contrôleur de disque dur, qui est une partie de la carte mère de l'ordinateur.

La carte interface comprend plusieurs composants clés :

Le contrôleur de disque dur

C'est le cerveau du disque dur. Il interagit avec le disque dur pour lire et écrire des données, contrôler les têtes de lecture/écriture et communiquer avec le reste du système informatique.

Les connecteurs de données

Ces connecteurs permettent à la carte interface de se connecter au reste du système informatique. Les types de connecteurs varient en fonction de l'interface du disque dur (par exemple, SATA, IDE, etc.).

Le circuit de commande

Ce circuit interprète les commandes envoyées par le contrôleur de disque dur et les traduit en mouvements appropriés pour les têtes de lecture/écriture.

Le circuit de données

Ce circuit gère la transmission des données entre le disque dur et le reste du système informatique.

Il existe plusieurs types d'interfaces pour les disques durs, parmi lesquels Serial ATA (SATA), IDE (PATA), SCSI, SAS, et Fibre Channel. Chacune de ces interfaces a ses propres avantages et inconvénients en termes de vitesse de transfert, de coût, et de compatibilité avec différents types de disques durs.

1.1.4 - Formats des disques durs magnétiques

Dimension

Les disques durs magnétiques peuvent venir en deux formats principaux : 2,5 pouces et 3,5 pouces. Ces tailles font référence à la largeur du disque dur, et elles sont nommées en fonction de l'inconvénient de l'industrie.

Disques durs 2,5 pouces

Ces disques sont généralement plus petits et plus légers que les disques 3,5 pouces. Ils sont souvent utilisés dans les ordinateurs portables et les ordinateurs de bureau compacts, car ils occupent moins d'espace. De plus, ils ont généralement une vitesse de rotation plus élevée, ce qui peut entraîner une meilleure performance en termes de vitesse de lecture et d'écriture.

Disques durs 3,5 pouces

Ces disques sont plus grands et plus lourds que les disques 2,5 pouces. Ils sont souvent utilisés dans les ordinateurs de bureau et les serveurs, car ils peuvent contenir des plateaux de disque plus grands, ce qui leur permet de stocker plus de données. De plus, ils ont généralement une vitesse de rotation plus basse que les disques 2,5 pouces, ce qui peut entraîner une meilleure durabilité.

Une autre différence entre les disques durs 2,5 pouces et 3,5 pouces concerne la taille du cache. Le cache est une petite quantité de mémoire rapide qui stocke temporairement les données pour une accélération des opérations de lecture et d'écriture. Les disques durs 3,5 pouces ont généralement une taille de cache plus grande que les disques 2,5 pouces pour le même prix.

Catégories

Il faut distinguer 2 catégories de disque dur :

Les disques durs grands publics

Ils peuvent ne pas être aussi robustes que les modèles professionnels et peuvent avoir une durée de vie plus courte.

Ils ont généralement des garanties plus courtes, souvent de deux à trois ans.

Ils peuvent avoir des fonctionnalités de gestion de l'énergie, mais celles-ci peuvent ne pas être aussi avancées que celles des modèles professionnels.

Les disques durs grand public sont souvent disponibles dans des capacités plus petites à moyennes, adaptées aux besoins des utilisateurs domestiques.

Les disques SATA : serial ATA

Il existe trois générations de disque SATA, la dernière (le SATA3) offrant évidemment les meilleures performances.

Sur un disque dur SATA, il y a un connecteur pour les données et un connecteur pour l'alimentation.

Concernant les performances, **ces disques ne permettent d'envoyer qu'une commande à la fois** : une écriture ou une lecture, on parle alors de technologie « half duplex ».

Comparé aux disques SAS et SSD, le disque SATA est le plus économique.

Utilisation des disques SATA

Les disques durs SATA sont la plupart du temps utilisés sur des PC et assez rarement sur des serveurs. Ces derniers demandant souvent des performances élevées en entrée-sortie disque, les disques SATA ne sont généralement pas suffisants.

Caractéristiques des disques SATA

Débit Max théorique : 6 Gbits/s
Tour/minutes Max : 7200 tr/min (voir dans de rare cas 10 000)
Formats disponibles : 2.5'' et 3.5''

Les disques durs à vocation professionnelle

Ils sont souvent optimisés pour des performances plus élevées. Cela peut inclure des vitesses de rotation plus rapides, des taux de transfert de données plus élevés et une meilleure gestion des charges de travail intensives.

Ils visent à offrir une plus grande fiabilité et durabilité. Ils peuvent inclure des fonctionnalités telles que des technologies de correction d'erreurs avancées, une meilleure gestion thermique et des composants de qualité supérieure.

Ils offrent souvent des garanties plus longues, parfois de trois à cinq ans, voire plus. Cela témoigne de la confiance des fabricants dans la durabilité et la fiabilité de leurs produits.

Ils peuvent être conçus avec une gestion de l'énergie plus sophistiquée pour répondre aux besoins des environnements d'entreprise.

Ils peuvent être disponibles dans des capacités plus importantes pour répondre aux besoins de stockage massif des entreprises.

Les disques SAS : serial attached SCSI

A la différence des disques SATA, les disques SAS possèdent un connecteur qui inclut à la fois l'alimentation et le transfert des données.

Ces disques peuvent envoyer deux commandes simultanément, cela améliore donc leur temps de réponse. On parle alors de technologie « full duplex ».

Utilisation des disques durs SAS

Ces disques sont utilisés la plupart du temps sur des serveurs pour supporter des applications de virtualisation, des bases de données etc... Ils peuvent également être installés sur des PC dans le cas d'exécution d'applications « gourmandes », typiquement sur une workstation.

Les usages typiques sont donc : les serveurs de base de données, les serveurs de virtualisation, les serveurs applicatifs métiers, ...

Caractéristiques des disques SAS

Débit Max théorique : 12 Gbits/s
Tour / minutes Max : 15 000 tr/min
Formats disponibles : 2.5'' et 3.5''

TL;DR : Les éléments qui permettent de les distinguer sont leur vitesse de rotation, le format physique et l'interface. L'interface connue pour un usage professionnel est SATA et SAS. La vitesse de rotation du disque dur (RPM ou TPM) offre des débits plus élevés, un temps d'accès plus court. Mais en contre partie elle engendre une consommation d'énergie plus importante, des températures plus élevées et des nuisances sonores plus importantes.

Technologies

Les disques durs magnétiques utilisent principalement deux technologies pour stocker les données : PMR (Perpendicular Magnetic Recording) et VMR (Vertical Magnetic Recording).

PMR (Perpendicular Magnetic Recording)

Dans cette technologie, les données sont stockées en utilisant des domaines magnétiques horizontaux sur les plateaux du disque dur. Chaque domaine magnétique peut stocker un bit de données, soit 0 ou 1. Les plateaux tournent à une vitesse élevée pour permettre un accès rapide aux données.

VMR (Vertical Magnetic Recording)

Cette technologie est similaire à PMR, mais elle utilise des domaines magnétiques verticaux au lieu de horizontaux. Cela permet de stocker plus de données par cellule, augmentant ainsi la densité de stockage. Cependant, cette technologie est généralement plus lente que PMR en raison de la nécessité de déplacer la tête de lecture vers le haut et vers le bas pour lire et écrire les données

1.2.0 - Le disque dur électronique SSD (solid state drive)

1.2.1 - Introduction

Les disques SSD utilisent principalement la technologie NAND pour stocker les données. Cette technologie repose sur la propriété des transistors de changer d'état (passer de l'état "0" à l'état "1") en fonction de la présence ou de l'absence d'un champ électrique. Cette propriété est utilisée pour lire et écrire des données sur les cellules de mémoire.

Cependant, la technologie NAND n'est pas la seule technologie utilisée dans les disques SSD. Les disques SSD 3D NAND, par exemple, combinent plusieurs couches de cellules de mémoire au-dessus d'une seule couche de substrate, ce qui permet d'augmenter la densité de stockage. Les disques SSD SLC (Single-Level Cell) et MLC (Multi-Level Cell) stockent un nombre variable de bits de données par cellule, permettant de stocker plus d'informations et d'augmenter la capacité de stockage.

En comparaison, la spintronique utilise les propriétés magnétiques des électrons, appelées spin, pour stocker et traiter des informations. Cette technologie est encore en phase de recherche et développement et n'est pas largement utilisée dans les disques SSD actuels.

1.2.2 - Principes

Stockage de données persistantes

Contrairement aux disques durs traditionnels qui utilisent des disques tournants pour stocker des données, les SSD utilisent des circuits intégrés pour stocker des données de manière permanente. Ils fonctionnent généralement en utilisant de la mémoire flash, qui peut contenir entre 1 et 4 bits de données par cellule.

Résistance aux chocs physiques

Les SSD sont généralement plus résistants aux chocs physiques que les disques durs traditionnels. Ils fonctionnent sans pièces mobiles, ce qui les rend plus robustes et leur permet de continuer à fonctionner même après avoir subi un impact.

Haute vitesse d'entrée/sortie

Les SSD ont des taux d'entrée/sortie plus élevés et une latence plus faible que les disques durs traditionnels. Cela signifie qu'ils peuvent lire et écrire des données plus rapidement, ce qui les rend idéaux pour les applications qui nécessitent un accès rapide aux données.

Capacité élevée

Les SSD peuvent avoir une capacité allant jusqu'à 100 To, ce qui est beaucoup plus grand que celle des disques durs traditionnels. Cela signifie que vous pouvez stocker beaucoup plus de données sur un SSD que sur un disque dur.

Interface variée

Les SSD peuvent être connectés à un ordinateur via différentes interfaces, y compris SATA, PCIe et M.2. Ces interfaces permettent aux SSD de communiquer efficacement avec l'ordinateur et de transférer des données rapidement.

1.2.3 - Composition d'un disque SSD

La composition d'un disque SSD diffère de celle d'un disque dur traditionnel.

La mémoire flash

Contrairement à un disque dur, qui utilise des plateaux magnétiques pour stocker les données, un SSD utilise une mémoire flash pour stocker les informations. Cette mémoire est constituée de nombreuses cellules qui peuvent être activées ou désactivées individuellement, permettant ainsi le stockage et la récupération de données.

Les contrôleurs

Les contrôleurs gèrent la communication entre la mémoire flash et le reste du système informatique. Ils sont responsables de l'interprétation des commandes provenant de l'ordinateur et de la transmission des données vers et depuis la mémoire flash.

Les circuits logiques

Ces composants, qui comprennent des circuits intégrés (IC), gèrent divers aspects du fonctionnement du SSD, comme le traitement des commandes, le contrôle de l'accès à la mémoire flash, et la gestion de l'état du SSD.

La carte de connexion

Comme pour un disque dur, un SSD nécessite une carte pour se connecter à l'ordinateur. Cependant, contrairement à un disque dur, cette carte n'a pas besoin de moteurs pour tourner. Au lieu de cela, elle utilise l'électricité pour lire et écrire des données sur la mémoire flash.

1.2.4 - Formats des disques SSD

Types

SSD SATA

À propos des types de SSD, le SSD SATA est le plus courant. En tant que type d'interface de connexion, SATA (Serial ATA) est utilisé par le SSD pour communiquer des données avec le système. Si vous possédez un SSD SATA, vous pouvez pratiquement garantir qu'il peut être utilisé avec n'importe quel ordinateur de bureau ou portable en votre possession actuellement, même si cet ordinateur a dix ans.

Le SATA lui-même a un degré de vitesse, et vous verrez le SATA 2 et le SATA 3 dans tout SSD considéré pour l'utilisation, appelé respectivement « SATA II »/ »SATA 3Gbps » ou « SATA III »/ »SATA 6Gbps ». Ceux-ci indiquent le taux de transfert de données maximal possible du lecteur, à condition que le lecteur soit installé dans un PC doté d'une interface SATA prenant en charge la même norme.

Aujourd'hui, le SATA 3.0 est le format de SSD le plus polyvalent, avec une vitesse de transfert théorique de 6 Go/s (750 Mo/s). Cependant, comme une certaine surcharge physique se produit lors de l'encodage des données à transférer, sa vitesse de transfert réelle est de 4,8 Go/s (600 Mo/s).

SSD PCIe

Le SSD PCIe est l'un des types de disques durs SSD. Le SSD PCIe désigne un SSD connecté à un système informatique à l'aide d'une interface PCIe. Le SSD PCIe est devenu une nouvelle méthode pour augmenter la vitesse des SSD (solid-state drive) vers les serveurs et les périphériques de stockage.

PCI Express, formellement abrégé en PCIe ou PCI-e, est l'abréviation de Peripheral Component Interconnect Express. En tant que norme de bus d'extension informatique à haut débit, PCIe peut remplacer les anciennes normes de bus PCI, PCI-X et AGP. De plus, PCIe est une interface de carte mère commune pour les cartes graphiques d'ordinateur, le disque dur, le SSD, le Wi-Fi et la connexion matérielle Ethernet.

SSD M.2

Le SSD M.2 appartient également à l'un des types de SSD. Il était auparavant connu sous le nom de NGFF (Next Generation Form Factor). Les SSD M.2 sont de petits circuits imprimés contenant de la mémoire flash et des puces de contrôleur, plutôt que des périphériques sous forme de dalles contenant ces puces.

La forme du SSD M.2 est similaire à celle de la RAM, mais elle est beaucoup plus petite et est devenue une configuration standard dans les ordinateurs portables ultra-fins, mais vous les trouverez également sur de nombreuses cartes mères d'ordinateurs de bureau. De nombreuses cartes mères haut de gamme disposent même de deux ou plusieurs emplacements M.2, ce qui vous permet de faire fonctionner le SSD M.2 en RAID.

La taille du SSD M.2 varie, généralement 80 mm, 60 mm ou 42 mm de long, 22 mm de large, avec des puces NAND sur un ou deux côtés. Il se distingue par les quatre ou cinq chiffres de son nom. Les deux premiers chiffres représentent la largeur et les deux autres la longueur.

La taille la plus courante est marquée comme M.2 Type-2280. Bien que les ordinateurs portables ne soient généralement disponibles que dans une seule taille, de nombreuses cartes mères d'ordinateurs de bureau ont des points de fixation pouvant être utilisés pour des lecteurs plus longs ou plus courts.

SSD U.2

Concernant les types de SSD, il convient de mentionner les SSD U.2. Un SSD U.2 a une interface U.2. U.2 (anciennement connu sous le nom de SFF-8639) est une norme d'interface définie par le SSD Form Factor Working Group (SFFWG). L'U.2 est développé pour le marché des entreprises et vise à être compatible avec les normes d'interface PCI-E, SATA, SATA-E et SAS.

Les SSD U.2 ressemblent aux disques durs SATA traditionnels, mais ils utilisent un connecteur différent et envoient les données via l'interface PCIe rapide, et ils sont généralement plus épais que les disques durs et SSD de 2,5 pouces.

De manière triviale, nous pourrons dire que le U.2 est au SSD, ce que le SAS est au HDD.

SSD NVME

Les différents types de SSD possèdent des interfaces variées. Un SSD NVMe est un SSD doté d'une interface NVMe. NVM Express (NVMe) est l'abréviation de Non-Volatile Memory Host Controller Interface Specification (NVMHCIS). Il s'agit d'une spécification d'interface de périphérique logique ouverte permettant d'accéder à des supports de stockage non volatils connectés via le bus PCI Express (PCIe).

NVM Express permet au matériel et au logiciel hôte de tirer pleinement parti du parallélisme possible dans les SSD modernes. Par conséquent, par rapport à l'interface de périphérique logique précédente, NVM Express réduit la surcharge d'E/S et apporte diverses améliorations des performances, notamment de longues files d'attente de commandes multiples et une latence réduite.

Formats

2.5''

C'est le format « classique » et le plus répandu. Mais **il tend à disparaître au profit du format M.2** interfacé en SATA via le protocole AHCI car cela permet de se passer de câble de données et d'alimentation.

mSATA (Mini-SATA)

Appelé aussi Mini-SATA et destiné aux **PC portables très fins et aux ultrabooks.** Ils permettent de profiter d'un taux de transfert maximal atteignant les 550 Mo/s en lecture et 520 Mo/s en écriture. Ils tendent eux aussi à disparaitre au profit du format M.2.

M.2

Afin de répondre à la demande croissante en systèmes de plus en plus minces et rapides, les constructeurs proposent des SSD sans boitier au format M.2 et **compatible avec le protocole NVMe** offrant un taux de transfert optimal.

U2

Moins connu, le connecteur U2 n’est pourtant pas aussi neuf que son nom : il s’agit en effet de la nouvelle version du SFF-8639 qui équipait alors principalement les installations professionnelles. Comme le M.2, il a pour objectif d’améliorer les débits (4 Go/s en théorique). Si les 2 peuvent être confondus, ils n’ont pourtant ni la même forme ni le même câblage et restent dans tous les cas extrêmement confidentiels.

Interfaces

SATA

En termes de performance, l'interface SATA est généralement suffisante pour la plupart des applications. Cependant, pour les applications gourmandes en ressources, comme les jeux vidéo ou les logiciels de montage vidéo, une interface plus rapide comme NVMe peut être préférée.

Il convient de noter que la vitesse de transfert d'un disque SSD SATA peut varier en fonction de la version de SATA qu'il utilise. Par exemple, SATA III offre des vitesses de transfert théoriques allant jusqu'à 6 Gbit/s, tandis que SATA II offre des vitesses de transfert allant jusqu'à 3 Gbit/s.

PCI-Express

PCIe est souvent utilisé en combinaison avec NVMe (Non-Volatile Memory Express), un protocole de contrôle conçu spécifiquement pour les SSD. NVMe a remplacé AHCI (Advanced Host Controller Interface), le schéma de contrôle utilisé par les disques durs et les SSD SATA pour le flux de données sur le bus SATA. NVMe a été conçu dès le départ pour gouverner la mémoire à l'état solide et est optimisé pour le stockage basé sur la technologie flash.

Les SSD PCIe sont généralement connectés via des emplacements M.2, qui peuvent prendre différentes formes et tailles. Les SSD PCIe existent en plusieurs générations, y compris PCIe 3.0, 4.0 et 5.0, chacune offrant des vitesses de transfert de données différentes. Par exemple, un SSD PCIe Gen3 peut atteindre des vitesses de lecture et d'écriture de jusqu'à 20 Gbit/s, tandis qu'un SSD PCIe Gen4 peut atteindre des vitesses encore plus élevées

M.2

L'interface M.2 est une norme pour les cartes d'extension de stockage internes. Elle a été introduite pour remplacer la norme mSATA et offre une plus grande flexibilité en termes de largeur et de longueur des modules. L'interface M.2 permet d'intégrer différents types de fonctions, y compris les disques durs (HDD) et les disques SSD (Solid State Drive).

1.2.5 - Technologies

Types de mémoires Flash

Les mémoires NOR Flash

NOR correspondant à NON-OU.

Les mémoires NOR sont un type de mémoire flash utilisée dans les dispositifs d'entrée/sortie (E/S) et les circuits intégrés (CI). Elles sont souvent utilisées dans les applications où la rapidité est importante, car elles peuvent lire et écrire des données plus rapidement que d'autres types de mémoires flash.

Les mémoires NOR sont très compactes et peuvent être intégrées directement dans les circuits intégrés, ce qui les rend idéales pour les applications embarquées où l'espace est limité. Cependant, elles ont une durée de vie limitée, car chaque cellule de mémoire peut seulement être écrite un certain nombre de fois avant de devenir obsolète.

Les mémoires NAND Flash

NAND correspond à la table logique NON-ET pour laquelle la sortie est NON seulement si toutes ses entrées sont OUI.

C'est la technologie la plus courante utilisée dans les disques SSD. Elle est connue pour sa grande densité de stockage, ce qui permet aux disques SSD de stocker une grande quantité de données sur une petite surface. Les disques SSD utilisant la technologie NAND Flash ont généralement une capacité de stockage beaucoup plus grande que les disques durs traditionnels.

3D XPoint (3D NAND)

Cette technologie est une forme de mémoire flash qui utilise une structure de cellule plus complexe que celle utilisée par la technologie NAND. Cela permet d'améliorer la densité de stockage et la vitesse d'accès aux données. Les disques SSD utilisant la technologie 3D XPoint sont généralement plus rapides et offrent une meilleure performance que ceux utilisant la technologie NAND.

Niveaux de charge

SLC (Single-Level Cell)

Ces disques SSD utilisent une mémoire flash NAND pour stocker les données. Ils stockent un seul bit de données dans chaque cellule de mémoire, ce qui permet de stocker plus d'informations par cellule et d'augmenter la capacité de stockage.

MLC (Multi-Level Cell)

Ces disques SSD utilisent également une mémoire flash NAND pour stocker les données. Ils stockent plusieurs bits de données dans chaque cellule de mémoire, ce qui permet de stocker plus d'informations par cellule et d'augmenter la capacité de stockage. Cependant, ils ont besoin de plus de cycles de programmation/effacement (P/E) que les disques SSD SLC.

TLC (Triple-Level Cell)

Ces disques SSD utilisent également une mémoire flash NAND pour stocker les données. Ils stockent trois bits de données dans chaque cellule de mémoire, ce qui permet de stocker encore plus d'informations par cellule et d'augmenter la capacité de stockage. Cependant, ils ont besoin de plus de cycles de programmation/effacement (P/E) que les disques SSD MLC.

QLC (Quad-Level Cell)

Ces disques SSD utilisent également une mémoire flash NAND pour stocker les données. Ils stockent quatre bits de données dans chaque cellule de mémoire, ce qui permet de stocker encore plus d'informations par cellule et d'augmenter la capacité de stockage. Cependant, ils ont besoin de plus de cycles de programmation/effacement (P/E) que les disques SSD TLC.

Le firmware

À la différence d'autres composants, ce micrologiciel (jeu d'instructions intégré) joue un rôle majeur dans un SSD. Il intervient dans l'utilisation des cellules, le traitement des fichiers à écrire, le support du TRIM et la gestion du ou des caches. **Le TRIM est une commande informant en temps réel le SSD sur les fichiers toujours présents** : sans cette commande le contrôleur ne sait pas qu'un secteur a été effacé, et doit donc lire la cellule, éventuellement la copier ailleurs pour ensuite réécrire la nouvelle donnée.

Pour limiter le nombre de lecture écriture la commande TRIM indique donc au contrôleur chaque secteur précédemment utilisé par le fichier supprimé. Cette fonction améliore les performances et évite une usure « prématurée » des cellules mémoires. Le firmware est toujours important sur un SSD, contrairement aux cartes mères ; si nouvelle version il y a il faut l'installer.

1.3.0 - Le disque dur hybride SSHD (fusion drive)

1.3.1 - Introduction

Un disque dur hybride (SSHD) est une nouvelle catégorie de stockage de données qui combine les caractéristiques des disques durs (HDD) et des disques SSD (Solid State Drive). Il s'agit d'un type de stockage de données qui offre à la fois les avantages des disques durs traditionnels et ceux des SSD modernes.

Un SSHD se présente sous la forme d'un disque dur normal, mais il dispose d'un cache SSD intégré. Ce cache sert de tampon entre le processeur et le reste du disque dur. Lorsque le processeur demande des données, le SSHD vérifie d'abord si ces données sont dans le cache SSD. Si c'est le cas, les données sont lues directement depuis le cache, ce qui est beaucoup plus rapide que de les lire depuis le reste du disque dur. Si les données ne sont pas dans le cache, elles sont lues depuis le reste du disque dur, puis mises en cache pour une utilisation future.

Cela permet aux SSHD de bénéficier des vitesses de lecture et d'écriture rapides des SSD pour les opérations de lecture et d'écriture fréquentes, tout en conservant la grande capacité de stockage des disques durs traditionnels pour stocker des données à long terme. De plus, car le cache SSD est intégré au disque dur, il n'y a pas besoin de connexions supplémentaires pour le cache, ce qui simplifie l'installation et la configuration du SSHD.

Il est important de noter que, bien que les SSHD offrent une combinaison unique de vitesse et de capacité, ils peuvent ne pas être aussi fiables que les disques durs traditionnels ou les SSD. En effet, le cache SSD a une durée de vie limitée, et une fois que toutes ses cellules de stockage sont épuisées, le SSHD devra commencer à utiliser le reste du disque dur pour le cache. Cela peut entraîner une diminution des performances et une augmentation de l'usure du disque dur.

1.3.2 - Principes

Mémoire cache

Les disques SSHD utilisent une petite quantité de mémoire cache (généralement 6 Go ou plus) pour améliorer les performances de lecture et d'écriture. Cette mémoire cache est utilisée pour stocker temporairement les données fréquemment consultées ou modifiées, réduisant ainsi le temps nécessaire pour lire ou écrire ces données.

Capacité d'entrelacement

Les disques SSHD ont une capacité de stockage beaucoup plus grande que celle des SSD traditionnels. Par exemple, un disque SSHD peut avoir une capacité allant jusqu'à 1 To, tandis qu'un SSD de la même gamme n'atteint généralement que 128 Go. Cela permet de conserver une grande quantité de données sans avoir besoin d'un SSD plus grand et coûteux.

Technologie NAND Flash

Les disques SSHD utilisent la technologie NAND Flash pour stocker les données. Cette technologie offre des vitesses de lecture et d'écriture rapides, ce qui permet d'accélérer le processus de chargement des applications et de transférer rapidement les données.

Tests SMART

Les disques SSHD peuvent effectuer des tests SMART (Self-Monitoring, Analysis and Reporting Technology) pour surveiller leur état de santé. Ces tests peuvent être exécutés en parallèle avec d'autres opérations, comme les instantanés et les scrubs, sans perturber leurs performances.

Instantanés

Les disques SSHD peuvent créer des instantanés de leurs données, ce qui permet de restaurer l'état d'une machine à un moment donné. Ces instantanés sont stockés dans la mémoire cache, ce qui permet d'accélérer le processus de restauration.

1.3.3 - Composition d'un disque SSHD

Disque dur mécanique (HDD)

Le cœur du disque SSHD est constitué d'un disque dur mécanique traditionnel. Ce disque dur stocke les données de manière permanente sur des plates tournantes magnétiques. Il offre une grande capacité de stockage à un coût relativement bas.

Mémoire cache NAND Flash

Une partie du disque SSHD est équipée d'une mémoire cache NAND Flash. Cette mémoire cache est utilisée pour stocker temporairement les données fréquemment consultées ou modifiées, permettant ainsi d'accélérer les opérations de lecture et d'écriture.

Logiciel de gestion

Un logiciel spécifique gère l'interaction entre le disque dur mécanique et la mémoire cache. Ce logiciel décide quand les données doivent être déplacées vers ou depuis la mémoire cache, afin d'optimiser les performances globales du disque SSHD.

Connecteurs

Enfin, le disque SSHD dispose de connecteurs SATA ou USB pour se connecter au reste du système informatique. Ces connecteurs permettent la communication entre le disque SSHD et le reste du système, y compris le processeur, la carte mère et le système d'exploitation.

1.4.0 - Caractéristiques techniques des zones cachées, inaccessibles ou méconnues

Ces mécanismes et zones sont conçus pour optimiser la performance, la sécurité et la fiabilité des disques durs, mais ils peuvent également compliquer la gestion des données et la récupération de données en cas de problème.

Garbage Collection

La Garbage Collection est un mécanisme utilisé dans les systèmes de fichiers SSD (Solid State Drives) pour gérer l'élimination des blocs de données obsolètes ou inutilisés. Elle permet de maintenir l'efficacité du SSD en libérant de l'espace occupé par des données qui n'y sont plus nécessaires. Ce processus est automatique et se produit en arrière-plan, rendant difficile son contrôle direct par l'utilisateur.

HPA (Host Protected Area)

Le HPA est une zone réservée sur un disque dur qui peut être utilisée par le système d'exploitation ou par des applications pour stocker des informations importantes. Cette zone est protégée contre les opérations de clonage ou de copie du disque dur, ce qui signifie qu'elle ne sera pas incluse lorsque vous clonez ou copiez votre disque dur. Le but principal du HPA est de préserver la sécurité des données sensibles stockées dans cette zone.

DCO (Device Configuration Overlay)

Le DCO est une fonctionnalité qui permet de modifier dynamiquement les paramètres de configuration d'un disque dur après sa fabrication. Cela peut inclure des ajustements tels que la modification de la taille des partitions ou la mise à jour des informations de firmware. Le DCO est souvent utilisé pour améliorer la compatibilité du disque dur avec différents systèmes d'exploitation ou pour corriger des bugs de firmware.

AMA (Access Method Area) et AMAC (Access Method Area Control)

L'AMA et l'AMAC sont des termes utilisés dans le domaine des systèmes de fichiers pour désigner des zones spécifiques du disque dur qui sont utilisées pour stocker des métadonnées ou des informations de configuration. L'AMA est la zone elle-même où ces informations sont stockées, tandis que l'AMAC contrôle l'accès à cette zone, déterminant qui peut lire ou écrire dans l'AMA. Ces zones sont essentielles pour le bon fonctionnement du système de fichiers et peuvent contenir des informations critiques pour la gestion des données sur le disque dur.

2.0.0 - Les différentes unités

2.1.0 - Introduction

En informatique, un **octet** est un multiplet de 8 bits codant une information. Dans ce système de codage s'appuyant sur le système binaire, un octet permet de représenter 28 nombres, soit 256 valeurs différentes. Un octet permet de coder des valeurs numériques ou jusqu'à 256 caractères différents.

La distinction entre les bytes et les octets n'est pas aussi claire qu'il pourrait sembler, surtout en raison des différences linguistiques et historiques.

2.2.0 - Les différences entre Bit, Byte et octet

2.2.1 - Byte et Bits

Un byte est égal à 8 bits. Donc, si vous avez une quantité de données mesurée en bits, vous pouvez obtenir la quantité équivalente en bytes en divisant le nombre total de bits par 8.

2.2.2 - Byte et Octet

Un byte est une unité de mesure de l'information informatique qui est généralement utilisée en anglais. Un byte est défini comme étant égal à 8 bits. Cependant, en français, le terme "byte" est rarement utilisé et est généralement remplacé par "octet", qui est également défini comme étant égal à 8 bits. Ainsi, en pratique, un byte est équivalent à un octet.

2.2.3 - Usage du Byte et de l'Octet

En anglais, si vous voulez exprimer explicitement une quantité de huit bits, vous utilisez le mot "octet". Cependant, si vous voulez exprimer l'unité d'adressage indépendamment du nombre de bits, vous utilisez le mot "byte". En français, le mot "octet" est utilisé de manière similaire.

2.3.0 - Le bit

Un bit, qui vient du terme "binary digit", est la plus petite unité d'information en informatique. Il est utilisé pour représenter une information binaire, c'est-à-dire une donnée qui peut prendre l'une de deux valeurs possibles : 0 ou 1.

Représentation de l'information

Un bit peut représenter une information simple, comme l'état d'une lumière (allumée ou éteinte) ou l'état d'un interrupteur (activé ou désactivé). C'est pourquoi un bit est parfois appelé "le plus petit élément d'information".

Base de l'informatique

Les bits sont la base de toute l'informatique. Ils sont utilisés pour construire des groupes plus complexes de données, comme des octets (8 bits), des mots (32, 64 ou plus bits selon la machine), des nombres entiers, des nombres à virgule flottante, et plus encore. Tous les calculs effectués par une machine informatique sont basés sur des bits.

Traitement de l'information

Un ordinateur traite l'information en séquence de bits. Par exemple, un ordinateur 32 bits traite 32 bits de données à la fois.

2.4.0 - Les Bytes

- **Byte (B)** : C'est l'unité de base de l'information en informatique. Un byte est égal à 8 bits, et peut prendre 2^8 valeurs différentes, soit de 0 à 255.
- **Kilobyte (KB)** : Un kilobyte est égal à 1024 bytes. Il est souvent utilisé pour mesurer la taille des fichiers sur un disque dur.
- **Megabyte (MB)** : Un megabyte est égal à 1024 kilobytes.
- **Gigabyte (GB)** : Un gigabyte est égal à 1024 megabytes. Cette unité est couramment utilisée pour mesurer la capacité des disques durs.
- **Terabyte (TB)** : Un terabyte est égal à 1024 gigabytes.

- **Petabyte (PB)** : Un petabyte est égal à 1024 terabytes.

2.5.0 - Les Octets

- **Kilo-octet (Ko)** : mille octets, soit une demi-page de texte
- **Méga-octet (Mo)** : 1 million d'octets, soit quelques petites photos compressées
- **Giga-octet (Go)** : 1 milliard d'octets, soit plus d'1 heure de vidéo
- **Tera-octet (To)** : 1000 milliards d'octets, soit 75 chaînes TV enregistrées pendant 24 h !
- **Peta-octet (Po)** : 1 million de milliards d'octets, soit 1/3 de la mémoire installée dans le monde en 2000
- **Exa-octet (Eo) :** 1 milliard de milliards d'octets, soit 1/3 de l'ensemble des informations, numériques ou non, produites dans le monde en 2000
- **Zetta-octet (Zo) :** mille milliards de milliards d'octets, soit 100 fois plus que l'ensemble de l'information produite depuis le début de l'humanité
- **Yotta-octet (Yo) :** un million de milliards de milliards d'octets ; le plus grand préfixe....

3.0.0 - Les différentes interfaces

3.1.0 - Introduction

Pour comprendre les différentes interfaces de stockage comme SATA (Serial ATA) et NVMe (Non-Volatile Memory Express), il est essentiel de se familiariser avec les concepts de base tels que les bus, les branchements, et les facteurs de forme. Ces éléments sont cruciaux pour appréhender comment les données sont transférées entre le matériel de stockage et le reste du système informatique.

3.2.0 - Les différents bus

Un **bus** est un chemin de communication qui permet aux différents composants d'un ordinateur de communiquer entre eux. Il existe plusieurs types de bus, dont les plus courants sont le bus ISA (Industry Standard Architecture), le bus PCI (Peripheral Component Interconnect), et le bus PCIe (Peripheral Component Interconnect Express).

3.2.1 - Bus Internes

- **Bus de données**: Transmet les données entre les composants. Sa taille en bits détermine le nombre d'informations qu'il peut transmettre en un seul cycle. Les tailles courantes sont 8, 16, 32, ou 64 bits, mais certaines cartes graphiques peuvent utiliser des bus de jusqu'à 1024 bits.
- **Lignes d'adresse**: Indiquent quel composant doit émettre ou recevoir l'information présente sur les bus de données. Le nombre de conducteurs d'adresse détermine l'espace adressable du bus.
- **Lignes de contrôle**: Indiquent quelle opération doit être effectuée, comme lecture ou écriture.
- **Bus AXI (Advanced eXtensible Interface)**: Un bus de communication interne pour les systèmes embarqués, utilisé principalement dans les processeurs ARM. Il est conçu pour offrir une haute performance et une faible latence.

3.2.2 - Bus Externes

- **Bus ISA** était le bus standard pour les ordinateurs personnels dans les années 1980 et 1990. Il a été remplacé par le bus PCI.
- **Bus SCSI (Small Computer System Interface)**: Utilisé pour connecter périphériques externes tels que les disques durs et les lecteurs CD-ROM à l'ordinateur via une interface parallèle.
- **Bus USB (Universal Serial Bus)**: Un bus standard pour connecter périphériques externes à un ordinateur. Il supporte une variété de types de périphériques et offre une connexion hot-plug, ce qui signifie que vous pouvez ajouter ou retirer des périphériques sans éteindre l'ordinateur.
- **Bus PCI** a été introduit dans les années 90 et a permis une meilleure intégration des périphériques externes dans les ordinateurs. Cependant, il souffrait de limitations en termes de vitesse et de capacité.
- **Bus PCI Express (Peripheral Component Interconnect Express)**: l'héritier du PCI, offre une vitesse de transmission de données beaucoup plus élevée et est capable de supporter une plus grande quantité de données. Il est largement utilisé aujourd'hui pour les cartes graphiques, les SSD, et d'autres périphériques de haute performance.

Les **branchements** se réfèrent à la manière dont ces buses sont configurés pour connecter différents composants. Par exemple, un ordinateur peut avoir plusieurs ports USB, chacun branché sur un bus différent pour gérer les communications avec les périphériques connectés.

3.3.0 - Facteurs de forme

Les **facteurs de forme** décrivent la taille et la disposition physique des dispositifs de stockage, comme les disques durs (HDD) et les SSD.

- **AIC (Add-In Card)** : Les SSD AIC sont des cartes d'extension qui s'insèrent dans les slots PCIe de la carte mère. Elles sont idéales pour les déploiements commerciaux, comme dans les centres de données, grâce à leur facilité de connexion via le bus PCIe. Certaines versions incluent des processeurs et des puces supplémentaires pour améliorer les performances.
- **U.2** : Les SSD U.2 peuvent s'adapter à l'emplacement existant de la carte mère destiné aux disques SSD SATA, mais ils peuvent également utiliser jusqu'à quatre voies PCIe. Disponibles en 2,5 pouces et 3,5 pouces, les disques SSD U.2 offrent une grande variété de capacités de stockage. Ils sont populaires en raison de leur compatibilité avec les fonds de panier des serveurs .
- **U.3** : Bien que la source ne mentionne pas explicitement U.3, il est important de noter que U.3 est une évolution de U.2. Les SSD U.3 conservent la compatibilité ascendante avec U.2 tout en ajoutant des améliorations telles que des connexions plus robustes et une meilleure gestion thermique. Ils sont conçus pour être interchangeables avec les disques U.2, offrant ainsi une plus grande flexibilité et une meilleure intégration dans les infrastructures existantes.
- **M.2** : Les SSD M.2 sont beaucoup plus petits que les disques U.2, offrant une conception compacte à faible dégagement de chaleur. Ils sont idéaux pour les ordinateurs portables et les PC de bureau où l'espace est limité. Pour utiliser un SSD M.2, il faut s'assurer que la carte mère dispose d'un emplacement approprié.
- **M.2 SATA** : Une version plus compacte du facteur de forme 2.5", compatible avec l'interface SATA. Il est souvent utilisé dans les ordinateurs portables et les PC de bureau.

- **M.2 NVMe** : Un facteur de forme similaire à celui de M.2 SATA, mais utilisant l'interface NVMe pour une connexion via le bus PCIe, offrant des performances de stockage plus élevées.
- **EDSFF (Enterprise and Data Center Standard Form Factor)** : Principalement utilisé dans les systèmes de stockage des entreprises et des centres de données, avec un accent sur l'efficacité thermique pour réguler la température du système. Un consortium de fabricants a développé l'ensemble de spécifications EDSFF. Les variantes EDSFF partagent le même protocole d'opération, interface, connecteur et configuration de broche.

3.4.0 - Les différentes interfaces de connexion

Les disques durs sont connectés aux systèmes via diverses interfaces telles que IDE, SCSI, SAS, FC, PATA, SATA, ou USB.

IDE (Integrated Drive Electronics)

L'IDE a été développée dans les années 1980 par Western Digital et Compaq dans le cadre d'un effort pour combiner le contrôleur de stockage et le disque dur en un seul dispositif. Après la normalisation de la technologie par l'American National Standards Institute (ANSI), les termes ATA et IDE ont commencé à être utilisés indifféremment. L'interface fournissait un connecteur à 40 broches pour attacher un disque dur IDE (HDD) à l'ordinateur. Un câble en ruban plat reliait le disque dur à la carte mère en s'attachant aux interfaces IDE sur l'ordinateur et le HDD.

SCSI = (Small Computer System Interface)

Ce bus diffère des autres en ce qu'il déporte la complexité vers le périphérique lui-même. Ainsi, les commandes envoyées au périphérique peuvent être complexes, le périphérique devant alors (éventuellement) les décomposer en sous-tâches plus simples.

SAS = (Serial Attached SCSI)

Interface qui constitue une évolution des bus SCSI en matières de performances, et apporte le mode de transmission en série de l'interface SATA (Serial Advanced Technology Attachment).

FC = (Fibre Channel)

Protocole de communication en point à point. FC-AL s'appuie le plus souvent sur un support fibre optique mais supporte néanmoins des câblages en cuivre beaucoup moins onéreux. Le FC-AL (*Fibre Channel - Arbitrated Loop*, en anglais) peut être utilisé dans des architectures SAN offrant de hauts niveaux de performance pour les systèmes de stockage en informatique.

PATA = (Parallèle Advanced Technology Attachment)

Cette norme utilise les normes ATA (*Advanced Technology Attachment*) et ATAPI (*ATA Packet Interface*). En pratique, l'ATAPI qui étend ce standard de communication à des périphériques différents des disques durs, sert à faire passer des commandes SCSI sur la couche physique de l'ATA.

SATA = (Serial Advanced Technology Attachment)

Le plus grand changement par rapport au Parallel ATA se trouve dans l'aspect physique des câbles utilisés. Les données sont transmises par deux paires différentielles (une paire pour l'émission et une pour la réception), protégées par trois fils de masse. Ces sept conducteurs étant regroupés sur une nappe plate, peu flexible, avec des connecteurs de 8 mm à chaque extrémité. Elle peut atteindre une longueur de 1 m. Comparé au court (45 cm) câble de 40 ou 80 fils du Parallel ATA, le

flux d'air, et donc le refroidissement des équipements, est amélioré grâce à cette plus faible largeur de câble. Le concept de rapport maître/esclave entre les dispositifs a été abandonné.

USB = (Universal Serial Bus)

Le bus USB permet de connecter des périphériques « à chaud » (quand l'ordinateur est en marche) et en bénéficiant du plug and play qui reconnaît automatiquement le périphérique. Il peut alimenter les périphériques peu gourmands en énergie (clé USB, disques SSD) et, pour ses dernières versions à prise USB Type-C, des appareils réclamant plus de puissance (60 W en version standard, 240 W au maximum).

NVME = (Non-Volatile Memory Express)

L'interface NVMe (Non-Volatile Memory Express) est une spécification d'interface de dispositif logique ouverte pour accéder au stockage non volatile d'un ordinateur, généralement via le bus PCI Express (PCIe). Elle a été conçue pour tirer parti de la faible latence et du parallélisme interne des dispositifs de stockage à état solide (SSD). L'initialisation de NVMe fait référence au stockage non volatile, souvent du flash NAND qui existe sous plusieurs formes physiques, y compris les disques SSD, les cartes d'extension PCIe et les cartes M.2, successeurs des cartes mSATA

4.0.0 - Les différents adressages

4.1.0 - Introduction

L'adressage est un concept fondamental en informatique qui concerne la manière dont les ordinateurs identifient et accèdent aux différents éléments de leurs systèmes, tels que les registres, la pile d'exécution, la mémoire statique et dynamique, et les ports d'E/S.

Il existe plusieurs types d'adressage, chacun ayant son propre objectif et sa propre application.

4.1.1 - Adressage implicite

Certaines opérations ne peuvent être réalisées que sur une donnée se trouvant en un endroit bien précis du processeur, comme l'accumulateur ou la pile. Dans ce cas, il n'est pas nécessaire de spécifier l'adresse du registre en question.

4.1.2 - Adressage immédiat

Ce type d'adressage est utilisé lorsque la valeur à manipuler est présente directement dans l'instruction. L'opérande est donc un littéral directement inclus dans l'instruction.

4.1.3 - Adressage direct

Dans l'adressage direct, l'adresse de l'objet à manipuler est directement incluse dans l'instruction. Cela signifie que l'opérande est une variable ou un champ de données situé à un endroit spécifique de la mémoire.

4.1.4 - Adressage registre ou inhérent

Dans cet adressage, l'opérande est un registre du processeur. L'instruction utilise le nom du registre pour indiquer quel registre doit être utilisé pour l'opération.

4.1.5 - Adressage indirect à registre

Ce type d'adressage est utilisé lorsque l'opérande est un registre qui contient l'adresse d'une autre donnée. L'adresse est donc indiquée dans le registre.

4.1.6 - Adressage indirect à registre avec incrément ou décrément

Similaire à l'adressage indirect à registre, mais avec l'ajout d'une opération d'incrément ou de décrément sur le registre.

4.1.7 - Adressage indexé absolu

Ce type d'adressage est utilisé lorsque l'opérande est une variable située à un endroit spécifique de la mémoire, mais l'adresse est modifiée par un index.

4.1.8 - Adressage Base + Index

Dans cet adressage, l'opérande est une variable située à un endroit spécifique de la mémoire, mais l'adresse est calculée en ajoutant l'index à la base.

La compréhension de ces différents types d'adressage est essentielle pour toute personne impliquée dans la construction, la maintenance ou le dépannage des systèmes informatiques.

4.2.0 - RAID

4.2.1 - Introduction

Redundant Array of Independent Disks est une technique de stockage de données qui combine plusieurs disques durs en un tableau logique. RAID peut améliorer la performance, la fiabilité et la capacité de stockage. Il existe plusieurs niveaux de RAID, chacun ayant ses propres avantages et inconvénients en termes de performance, de capacité et de redondance.

4.2.2 - Les différents types de RAID

RAID 0

Il s'agit d'un niveau de RAID qui divise les données en blocs et les écrit sur plusieurs disques simultanément. Cela permet d'augmenter significativement la vitesse de lecture et d'écriture. Cependant, si un disque tombe en panne, toutes les données du tableau sont perdues.

RAID 1

Il s'agit d'un niveau de RAID qui écrit identiquement les mêmes données sur deux disques. Cela permet d'avoir une copie de sauvegarde des données en cas de défaillance d'un disque. Cependant, cela réduit la capacité totale du système de moitié.

RAID 5

Il s'agit d'un niveau de RAID qui utilise trois disques minimum et écrit les données sur tous les disques. Il utilise également un espace de parité pour stocker des informations de correction d'erreur. Cela permet de restaurer les données si un disque tombe en panne.

RAID 6

Il s'agit d'un niveau de RAID qui utilise au moins quatre disques et écrit les données sur tous les disques, ainsi que des informations de correction d'erreur sur deux disques. Cela permet de restaurer les données si deux disques tombent en panne.

RAID 10

Il s'agit d'une combinaison de RAID 1 et RAID 0. Il utilise au moins quatre disques et écrit les mêmes données sur deux disques pour chaque paire. Les données sont ensuite combinées pour une vitesse de lecture plus rapide.

4.3.0 - JBOD

4.3.1 - Introduction

Just a Bunch Of Disks est une méthode de configuration de disques où tous les disques sont traités individuellement. Contrairement au RAID, où les données sont divisées et distribuées sur plusieurs disques, dans un JBOD, chaque disque est considéré comme une entité distincte. Cela signifie que si un disque tombe en panne, il n'affecte pas les autres disques du tableau.

4.3.1 - Les différents types d'adressage dans un environnement JBOD

Adressage direct

Dans l'adressage direct, chaque disque est adressé directement. Cela signifie que chaque disque a une adresse unique qui lui est attribuée lors de sa création. Cela permet d'accéder directement à un disque spécifique, mais cela peut rendre difficile la gestion globale du tableau de disques.

Adressage par bloc

Dans l'adressage par bloc, les données sont stockées en blocs sur plusieurs disques. Chaque bloc a une adresse unique qui lui est attribuée lors de sa création. Cela permet de gérer facilement les données sur le tableau de disques, mais cela peut rendre difficile l'accès direct à un disque spécifique.

Adressage par file

Dans l'adressage par file, les données sont stockées en files sur plusieurs disques. Chaque file a une adresse unique qui lui est attribuée lors de sa création. Cela permet de gérer facilement les données sur le tableau de disques, mais cela peut rendre difficile l'accès direct à un disque spécifique.

Adressage par segment

Dans l'adressage par segment, les données sont stockées en segments sur plusieurs disques. Chaque segment a une adresse unique qui lui est attribuée lors de sa création. Cela permet de gérer facilement les données sur le tableau de disques, mais cela peut rendre difficile l'accès direct à un disque spécifique.

4.3.2 - Les différents types de JBOD

JBOD simple

Dans un JBOD simple, chaque disque est présenté individuellement à un serveur sans amalgame, pooling ou structure appliquée. Les données sont écrites dans un ordre séquentiel, évitant les étapes plus complexes impliquées dans l'écriture de données dans les systèmes RAID.

JBOD espacé

Dans un JBOD espacé, les disques sont combinés pour former un grand disque logique. Cela permet d'utiliser tous les disques ensemble pour créer une grande quantité de stockage. Cependant, si un disque tombe en panne, les données sur ce disque sont perdues.

JBOD espacé et redondant

Dans un JBOD espacé et redondant, les disques sont combinés pour former un grand disque logique, et une copie des données est également stockée sur un autre disque. Cela permet d'avoir une copie de sauvegarde des données en cas de défaillance d'un disque.

JBOD avec mise en miroir

Dans un JBOD avec mise en miroir, les données sont écrites simultanément sur deux disques. Cela permet d'avoir une copie de sauvegarde des données en cas de défaillance d'un disque.

4.4.0 - SLED

4.4.1 - Introduction

Le Self Encrypting Drive est un type de disque dur qui a la capacité de crypter automatiquement les données qu'il stocke. SLED peut être configuré pour crypter toutes les données, ou seulement certaines parties du disque. Cela peut être particulièrement utile pour le stockage de données sensibles, car même si le disque est perdu ou volé, les données restent sécurisées.

4.4.2 - Les différents types de SLED

Opteron

Opteron est une gamme de processeurs de serveur produits par AMD. Certains modèles de ces processeurs supportent les SLED. Les SLED Opteron peuvent être configurés pour crypter toutes les données, ou seulement certaines parties du disque, ce qui peut être particulièrement utile pour le stockage de données sensibles.

Intel

Intel produit également des SLED dans sa gamme de produits. Les SLED Intel peuvent être configurés pour crypter toutes les données, ou seulement certaines parties du disque. Ils sont compatibles avec les serveurs Intel Xeon et d'autres systèmes de serveur Intel.

Samsung

Samsung produit une gamme de SLED qui utilisent le chiffrement AES (Advanced Encryption Standard) pour crypter les données. Les SLED Samsung peuvent être configurés pour crypter toutes les données, ou seulement certaines parties du disque. Ils sont compatibles avec une variété de systèmes d'exploitation, y compris Windows et Linux.

Seagate

Seagate produit également des SLED dans sa gamme de produits. Les SLED Seagate peuvent être configurés pour crypter toutes les données, ou seulement certaines parties du disque. Ils sont compatibles avec une variété de systèmes d'exploitation, y compris Windows et Linux.

5.0.0 - Normes et référentiels

5.1.0 - introduction

La normalisation de la destruction de données à l'échelle internationale est un domaine crucial pour assurer la sécurité des informations, surtout lorsqu'il s'agit de matériel de stockage de masse qui est retiré de services ou réutilisé. En Europe, plusieurs organismes et institutions jouent un rôle clé dans la définition, la promotion et le contrôle des normes liées à cet aspect.

5.1.1 - Les organismes

5.1.2 - Organismes Internationaux

- **ANSI (American National Standards Institute)** : ANSI est l'organisme de normalisation des États-Unis qui développe des normes industrielles. Bien que principalement basé aux États-Unis, ANSI joue un rôle international dans la normalisation des technologies et des produits.
- **ISO (International Organization for Standardization)** : L'ISO est une organisation mondiale qui développe des normes techniques. Elle travaille en collaboration avec les comités nationaux d'normalisation, dont l'AFNOR en France. L'ISO a publié des normes relatives à l'effacement des données, comme ISO/IEC 27040:2015, qui couvre la sécurisation des données sur les supports de stockage.
- **IEEE (Institute of Electrical and Electronics Engineers)** : L'IEEE est une organisation professionnelle et technique qui développe des normes pour l'industrie électrique, électronique et informatique. L'IEEE 2883-2022 est une norme qui se concentre sur les directives pour effacer les données stockées sur les supports de stockage.
- **NIST (National Institute of Standards and Technology)** : Bien que basé aux États-Unis, le NIST joue un rôle international dans la définition des meilleures pratiques pour la sécurité des informations, y compris l'effacement sûr des données. Ses publications et guides sont souvent référencés dans les normes européennes et internationales.
- **Department of Defense (DoD)** : Similaire au NIST, le DoD américain publie des lignes directrices et des normes pour l'effacement sûr des données, qui sont adoptées et utilisées par des organisations à travers le monde, y compris en Europe.

5.1.3 - Organismes Européens

- **CEN (Comité Européen de Normalisation)** : Le CEN est l'organisation européenne de normalisation, qui coordonne l'adoption des normes internationales au niveau européen. Il travaille en partenariat avec les comités nationaux de normalisation des pays membres, dont le DIN en Allemagne, AFNOR en France, etc. Le CEN promeut l'harmonisation des normes européennes avec celles internationales.
- **ENISA (European Union Agency for Cybersecurity)** : ENISA aide les États membres de l'UE à renforcer leur cybersécurité. Bien qu'elle ne soit pas directement chargée de la création de normes, elle joue un rôle important dans la promotion de pratiques de sécurité des données, y compris l'effacement sûr des données.

5.1.4 - Institutions Nationales

- **AFNOR (Association Française de Normalisation)** : En France, l'AFNOR est l'organisme national de normalisation. Elle traduit, publie et commercialise les normes françaises et internationales, y compris celles liées à l'effacement des données.
- **BSI (Bundesamt für Sicherheit in der Informationstechnik)** : Au niveau allemand, le BSI est responsable de la sécurité de l'information. Il contribue à la mise en œuvre des normes de sécurité des données, y compris celles concernant l'effacement sûr des données.

5.2.0 - Les principales normes

La normalisation de la destruction de données à l'échelle internationale est un domaine crucial pour assurer la sécurité des informations, surtout lorsqu'il s'agit de matériel de stockage de masse qui est retiré de service ou réutilisé. Plusieurs organismes et institutions jouent un rôle clé dans la définition, la promotion et le contrôle des normes liées à cette pratique. Voici une introduction à quelques-unes des normes internationales importantes dans ce domaine :

5.2.1 - IEEE 2883-2022

L'IEEE 2883-2022 est une norme établie par l'Institute of Electrical and Electronics Engineers (IEEE) qui se concentre sur les directives pour effacer les données stockées sur les supports de stockage. Cette norme a été développée après la publication de la NIST SP 800-88, Rev. 1, et vise à combler le vide laissé depuis la dernière révision des normes NIST. L'IEEE 2883-2022 propose des exigences et des orientations technologiques spécifiques pour l'oblitération des données enregistrées, en distinguant trois catégories de médias : Clear, Purge, et Destruct. Chaque catégorie correspond à un niveau de destruction des données, allant de l'effacement logique sans intrusion via le logiciel à la destruction physique par incinération ou broyage.

5.2.2 - NIST SP 800-88

La NIST SP 800-88, publiée par le National Institute of Standards and Technology (NIST) des États-Unis, est une autre norme importante dans le domaine de la destruction de données. Elle fournit des directives pour la sanitisation des supports de stockage, y compris les méthodes d'effacement logique et physique. La norme recommande l'utilisation de logiciels d'effacement sécurisé qui répondent aux normes de la NIST SP 800-88 pour assurer une suppression complète des données, rendant la récupération des données pratiquement impossible même par des spécialistes utilisant des techniques de laboratoire avancées.

5.2.3 - DIN 66399

La DIN 66399 est un ensemble de normes de destruction de données établi par le Deutsches Institut für Normung (DIN), l'institut allemand de normalisation. Ces normes fournissent des lignes directrices et des exigences pour la destruction sûre des informations stockées sur divers supports, y compris les documents papier et les dispositifs de stockage électronique. La DIN 66399 est particulièrement pertinente pour les entités qui traitent des données classifiées ou sensibles, telles que les agences gouvernementales, les institutions financières, les organisations de santé, et toute autre entité qui traite des informations confidentielles. La norme introduit une approche systématique de la destruction des données en catégorisant les méthodes de désinfection en fonction de la sensibilité des informations.

5.2.4 - ISO/IEC 27001:2022

Bien que principalement axée sur la sécurité de l'information, l'ISO/IEC 27001:2022 inclut des exigences pour la destruction physique des supports de stockage contenant des informations sensibles. La norme recommande de détruire physiquement les supports de stockage par des méthodes telles que l'incinération ou le broyage, en s'assurant que les dispositifs potentiellement

contenant des données sensibles endommagées sont également physiquement détruits.

5.2.5 - OPNAVINST 5239.1A

Établi par la marine américaine, cette norme spécifique à l'effacement des données implique trois passages ou écrasements de données, illustrant une approche technique d'effacement.

5.3.0 - Certifications et qualifications

- **Certified Information Systems Security Professional (CISSP)** : Cette qualification est offerte par l'ISC² (International Information System Security Certification Consortium) et est reconnue mondialement comme une référence en matière de sécurité de l'information. Les CISSPs sont qualifiés pour concevoir, mettre en œuvre et gérer des programmes de sécurité de l'information complexes.
- **Certified Information Privacy Technologist (CIPT)** : Offerte par l'International Association of Privacy Professionals (IAPP), cette certification est spécifique à la protection de la vie privée des données. Elle est destinée aux professionnels qui travaillent sur la collecte, l'utilisation, la distribution et la conservation de données personnelles.
- **ISO/IEC 27001 Lead Auditor** : Cette qualification est destinée aux auditeurs internes et aux experts en sécurité de l'information qui veulent acquérir une compréhension approfondie de la norme ISO/IEC 27001, qui est une norme internationale pour les systèmes de gestion de la sécurité de l'information (SGSI).
- **Data Loss Prevention Certified (DLP-C)** : Cette certification est offerte par l'EC-Council et est conçue pour les professionnels qui travaillent sur la prévention de la perte de données et la protection des informations sensibles. Elle couvre les meilleures pratiques pour identifier, prévenir et répondre aux incidents de perte de données.
- **Common Criteria (ISO 15408)** : C'est une certification indépendante de sécurité reconnue internationalement par les gouvernements dans 31 pays à travers l'Europe, l'Australasie, l'Asie et l'Amérique du Nord. Des logiciels d'effacement de données comme Blancco Drive Eraser ont obtenu cette certification.
- **ANSSI (Agence Nationale de Sécurité des Systèmes d'Information)** : L'ANSSI est l'agence française de cybersécurité. Elle certifie des logiciels d'effacement de données comme Blancco Drive Eraser pour leur conformité avec les exigences de certification.
- **TÜV Saarland** : TÜV Saarland a officiellement approuvé les produits d'effacement de données de Blancco en raison des résultats positifs trouvés. Ils ont constaté que le logiciel de Blancco fournit un mécanisme fiable et efficace pour effacer les données privées.
- **STQC (Standardization Testing & Quality Certification)** : STQC est l'organisme indien de normalisation qui certifie des produits d'effacement de données comme Blancco Drive Eraser pour leur conformité avec les normes indiennes.
- **TTA (Telecommunications Technology Association)** : La TTA est l'association coréenne de télécommunications qui a accordé à Blancco Drive Eraser la plus haute certification de qualité logicielle de Corée.
- **NYCE (National Cybersecurity Excellence)** : NYCE est l'organisme mexicain de certification qui a approuvé et certifié les méthodes d'effacement de données de Blancco.

6.0.0 - Les différents protocoles d'effacements sécurisés

L'effacement des données sur les supports de stockage de masse est une pratique cruciale pour garantir la sécurité des informations, en particulier lorsque des dispositifs de stockage sont retirés de service ou réutilisés. Plusieurs protocoles et normes ont été développés pour assurer un effacement efficace et sécurisé des données, chacun ayant ses propres avantages et limitations.

6.1.0 - État des lieux des protocoles

6.1.1 - Instruction de sécurité du système de l'armée de l'air 5020

L'instruction AFSSI-5020 (Air Force System Security Instruction 5020) est une directive de la United States Air Force (USAF) qui concerne la sécurité de la rémanence des systèmes d'information de l'armée de l'air. Cette instruction s'applique à tous les personnels militaires et civils de l'Air Force, ainsi qu'aux contractants de l'Air Force qui développent, acquièrent, livrent, utilisent, exploitent ou gèrent les systèmes d'information de l'Air Force (AIS), y compris ceux intégrés. Elle aborde notamment la sécurisation des médias de stockage, la protection contre la rémanence (c'est-à-dire la capacité des dispositifs de stockage à conserver des données après leur suppression), et la procédure de désintégration des données sensibles.

Voici les points clés de l'instruction AFSSI-5020 :

Responsabilités

- **Autorité Approuvante Définie (DAA)** : approuve l'utilisation de matériel, de firmware et de logiciel, ainsi que les procédures pour le nettoyage, la désinfection et la destruction des médias de stockage.
- **Bureau de Protection de l'Information de la Brigade (IP)** : maintient des informations sur les incinérateurs les plus proches, les installations de destruction métallique et le personnel formé à l'utilisation de dissolvants chimiques pour les surfaces des disques.
- **Programmeurs/Systèmes Analystes** : testent et évaluent les routines d'écrasement pour s'assurer de leur conformité avec cette instruction.

Procédures de Sécurisation

- **Nettoyage des Médias de Stockage** : les médias doivent être nettoyés lors du changement de mode d'opération ou avant une nouvelle utilisation à un niveau de classification plus élevé. Ils doivent également être nettoyés si ils ont contenu des informations SBU (Sensitive But Unclassified) avant une nouvelle utilisation ou une sortie du contrôle de l'Air Force.
- **Sanitisation des Médias de Stockage** : la sanitisation vise à supprimer toutes les informations sensibles des médias de stockage de manière à garantir qu'elles ne peuvent pas être récupérées par des moyens techniques. Tous les médias de stockage doivent être sanctuarisés avant d'être mis à disposition de personnes qui n'ont pas de sécurité d'accès et besoin de savoir pour les informations stockées sur les médias.

Méthode de Sanitisation AFSSI-5020

La méthode de sanitisation AFSSI-5020 implique trois passes :

1. Formatage du disque avec zéros.
2. Effacement complet de toutes les données.
3. Programmation d'un caractère aléatoire et vérification de l'écriture.

Cette méthode est conçue pour empêcher toute récupération de fichiers par des méthodes basées sur logiciel et matériel, garantissant ainsi que les informations précédemment stockées ne peuvent pas être récupérées.

L'instruction AFSSI-5020 joue un rôle crucial dans la gestion sécurisée des données sensibles par l'USAF, en particulier dans le cadre de l'éradication de la remanence et de la protection contre la divulgation non autorisée d'informations.

6.1.2 - Écrasement aléatoire apériodique/aléatoire

L'écrasement aléatoire apériodique et aléatoire fait référence à des méthodes avancées d'effacement de données sur les supports de stockage numérique, visant à garantir que les données précédemment stockées ne puissent pas être récupérées, même par des moyens techniques avancés. Ces méthodes sont particulièrement importantes pour la sécurité des données, surtout dans des contextes où la confidentialité et l'intégrité des informations sont cruciales. Voici une explication détaillée de ces méthodes :

Écrasement Aléatoire Apériodique

L'écrasement aléatoire apériodique consiste à écraser les données avec des nombres aléatoires. Cette méthode est efficace pour rendre impossible la récupération des données par des logiciels de récupération de données. Cependant, il est important de noter que certaines technologies, comme celles qui lisent la magnétisation résiduelle, pourraient théoriquement restaurer des données écrasées de cette manière. Cela dit, l'écrasement aléatoire apériodique reste une méthode robuste pour empêcher la récupération de données sensibles.

Écrasement Aléatoire et Zéro

L'écrasement aléatoire et zéro consiste à écraser d'abord les données avec des nombres aléatoires, puis à écraser ces données avec des zéros (0x00). Cette méthode double la couche de protection en ajoutant une étape supplémentaire d'écrasement après l'écrasement aléatoire initial. Comme pour l'écrasement aléatoire apériodique, cette méthode rend très difficile, voire impossible, la récupération des données par des logiciels de récupération. De plus, elle offre une barrière supplémentaire contre les tentatives de récupération basées sur la magnétisation résiduelle.

6.1.3 - Effacement SSD Blancco

Blancco est une société internationale qui, depuis le début du XXIe siècle, travaille avec des gouvernements et de grandes entreprises sur l'effacement sécurisé des données. Ses normes d'effacement pour les disques durs solides (SSD) englobent les écrasements aléatoires, la suppression des verrouillages, l'effacement des données au niveau du micrologiciel et, enfin, la vérification complète. Le processus s'appuie sur de nombreux protocoles standard de désinfection des SSD pour créer un processus d'effacement plus complet pour les SSD. Seul Blancco connaît le nombre précis de passages utilisés dans l'ensemble du processus.

La méthode d'éffacement Blancco est une approche logicielle avancée pour assurer l'effacement sûr des données à partir de tout support de stockage numérique. Elle utilise des zéros et des uns pour écraser toutes les secteurs du dispositif de stockage, rendant les données irrécupérables. Voici comment fonctionne cette méthode :

Processus d'Effacement Blancco

1. **Écriture sur Tous les Secteurs** : La méthode Blancco commence par écraser les données sur le dispositif de stockage en utilisant des zéros et des uns. Cet écriture s'étend à tous les secteurs du dispositif, garantissant que chaque bit de données est remplacé.

2. **Vérification de l'Effacement** : Une fois l'effacement effectué, le logiciel Blancco vérifie que les données ont été correctement écrasées sur tous les secteurs du dispositif. Cette vérification assure que l'effacement a été réalisé de manière complète et réussie.
3. **Certificat d'Effacement** : Après la vérification, le logiciel Blancco génère un certificat qui atteste que l'effacement a été effectué avec succès. Ce certificat est conçu pour être résistant à toute tentative de falsification et est prêt à être présenté à des audits. Il fournit une preuve tangible que les données ont été sécurisamment éradiquées.

Avantages de l'Effacement Blancco

- **Contrôle Amélioré** : L'effacement Blancco peut être effectué sur site ou à distance, offrant un meilleur contrôle que d'autres méthodes d'effacement de données. Il peut également être automatisé pour économiser du temps.
- **Conformité et Sécurité** : Grâce à son processus de vérification et à ses rapports auditable, l'effacement Blancco répond aux exigences de conformité et de sécurité. Il est testé, certifié, approuvé et recommandé par plus de 14 organismes régulateurs dans le monde entier.
- **Initiatives Environnementales** : L'effacement Blancco soutient les initiatives environnementales en permettant aux organisations de conserver la valeur de revente de leurs dispositifs de stockage, tout en assurant que les données sont sécurisément éradiquées.
- **Solution Patente pour SSD** : Blancco propose une solution patente pour les SSD qui gère les différences de fonctionnalités entre divers fabricants de SSD, garantissant ainsi un effacement sûr et efficace.

L'effacement Blancco est considéré comme la meilleure méthode pour réaliser l'effacement des données, grâce à son processus de validation pour s'assurer que les données ont été correctement écrasées et à ses rapports facilement auditable. Il est particulièrement adapté pour les organisations cherchant à sécuriser l'élimination des données sensibles avant de revendre, de réaffecter ou de détruire des SSD et des HDD

6.1.4 - L'algorithme de Bruce Schneier

L'algorithme de Bruce Schneier, également connu sous le nom de Blowfish, est un algorithme de chiffrement à sept passages. L'algorithme de Bruce Schneier pour l'effacement des données, connu sous le nom de "Bruce Schneier's Algorithm", est une méthode recommandée par le célèbre spécialiste de la sécurité informatique pour assurer un effacement sûr des données sur un support de stockage. Cette méthode est particulièrement utile pour les situations où la sécurité des données est une préoccupation majeure, comme dans le cas de la vente, du recyclage ou de la destruction de disques durs et autres supports de stockage.

Description de l'Algorithme

L'algorithme de Bruce Schneier comprend sept passes d'effacement, chacune ayant un effet différent sur les données stockées :

1. **Première Passe** : L'ensemble du disque est écrasé avec le motif binaire "00".
2. **Deuxième Passe** : Le disque est écrasé avec le motif binaire "11".
3. **Troisième Passe** : Le disque est écrasé avec un motif binaire aléatoire.
4. **Quatrième Passe** : Le disque est écrasé avec un autre motif binaire aléatoire.
5. **Cinq Passes Suivantes** : Le disque est écrasé cinq fois consécutivement avec des motifs binaires aléatoires.

Ce processus a pour objectif de rendre les données extrêmement difficiles à récupérer, même avec des techniques avancées de récupération de données. La nature aléatoire des motifs binaires utilisés dans les cinq dernières passes rend particulièrement difficile pour un attaquant de déterminer comment l'effacement a affecté les restes de données autour des bords de la piste sur le disque ou aux transitions de bits sur le disque.

Avantages et Limitations

- **Sécurité Augmentée** : Bien que probablement une méthode plus sécurisée pour effacer les données que le standard VSITR (Verbatim Secure Erase), l'algorithme de Bruce Schneier offre une couche supplémentaire de sécurité grâce à l'utilisation de motifs binaires aléatoires.
- **Temps d'Effacement Plus Long** : La création de motifs binaires aléatoires rend cette méthode significativement plus lente que d'autres méthodes d'effacement, car cela nécessite plus de temps pour générer et écrire ces motifs.

En résumé, l'algorithme de Bruce Schneier offre une méthode robuste pour l'effacement sûr des données, en particulier dans des contextes où la sécurité est une préoccupation majeure. Sa complexité et son temps d'exécution prolongé le rendent cependant moins approprié pour les applications nécessitant un effacement rapide des données

6.1.5 - BSI-2011-VS

Le standard BSI-2011-VS est un protocole d'effacement des données développé initialement par le Bundesamt für Sicherheit in der Informationstechnik (BSI), l'Office fédéral allemand de sécurité de l'information. Ce standard est recommandé pour la destruction sécurisée des données par les agences gouvernementales et privées. Il implique deux passes d'effacement et deux vérifications pour garantir un effacement efficace des données. Voici les détails de ce processus :

Projet BSI-2011-VS

- **Objectif** : Assurer l'effacement sûr des données sur les supports de stockage pour éviter leur récupération par des acteurs malveillants.
- **Procédure** : Le processus comprend deux passes d'effacement et deux vérifications pour garantir un effacement efficace. Cela signifie que les données sont écrasées deux fois avec des motifs spécifiques, suivi de vérifications pour confirmer que l'effacement a été effectué correctement.

Avantages du BSI-2011-VS

- **Sécurité** : En appliquant deux passes d'effacement et en effectuant des vérifications, ce standard minimise le risque de récupération des données.
- **Conformité** : Pour les organisations qui traitent des données sensibles, le BSI-2011-VS offre une méthode conforme aux normes de sécurité de l'information, facilitant ainsi la conformité aux réglementations telles que le RGPD en Europe.

Utilisation

Ce standard est particulièrement pertinent pour les organisations qui doivent garantir l'effacement sûr des données avant la réaffectation, la vente ou la destruction de supports de stockage. Il est utilisé dans divers secteurs, y compris le gouvernement, les banques, et les entreprises qui manipulent des données sensibles.

Comparaison avec d'autres standards

Bien que d'autres standards d'effacement des données existent, tels que ceux proposés par le DoD, NIST, et d'autres agences gouvernementales, le BSI-2011-VS se distingue par sa simplicité et son efficacité. Il offre une méthode fiable pour l'effacement des données qui est facile à mettre en œuvre et à vérifier, ce qui en fait une option attrayante pour les organisations cherchant à sécuriser l'élimination des données sensibles.

En résumé, le standard BSI-2011-VS représente une approche robuste et fiable pour l'effacement sûr des données, offrant une couche supplémentaire de sécurité pour les informations sensibles stockées sur les supports de stockage numériques

6.1.6 - BSI-GS

Le standard BSI-GS est une méthode d'effacement des données recommandée par le Bundesamt für Sicherheit in der Informationstechnik (BSI), l'Office fédéral allemand de sécurité de l'information. Ce standard est conçu pour assurer un effacement sûr des données sur les supports de stockage, en particulier sur les ordinateurs portables et les appareils mobiles. Voici les étapes clés de la procédure BSI-GS :

Étapes du BSI-GS

1. **Suppression des Disques Cachés** : Si présents, les disques cachés (HPA/DCO) sont supprimés. Ces zones sont souvent utilisées pour stocker des informations supplémentaires ou des partitions cachées sur les disques durs.
2. **Surécriture avec Données Aléatoires** : Le disque est ensuite surécrit avec des données aléatoires de manière périodique. Cette étape vise à rendre les données précédemment stockées illisibles.
3. **Effacement au Niveau du Firmware** : Selon le type de support de stockage, une commande d'effacement au niveau du firmware est exécutée. Cette étape est nécessaire pour certains types de disques durs qui ont des fonctionnalités spécifiques nécessitant une commande spécifique pour un effacement complet.
4. **Vérification de l'Effacement** : Enfin, l'effacement est vérifié pour s'assurer que les données ont été correctement éliminées. Cette vérification est cruciale pour confirmer que l'effacement a été effectué de manière adéquate.

Avantages du BSI-GS

- **Simplicité** : Contrairement à d'autres méthodes d'effacement qui nécessitent plusieurs passes d'effacement, le BSI-GS nécessite seulement une passe, rendant le processus plus rapide et plus simple à mettre en œuvre.
- **Efficacité** : En combinant la suppression des disques cachés, la surécriture avec des données aléatoires, et l'effacement au niveau du firmware, le BSI-GS offre une méthode efficace pour l'effacement sûr des données.
- **Flexibilité** : Le processus peut être adapté en fonction du type de support de stockage et des données à effacer, offrant une flexibilité importante pour les organisations.

Le standard BSI-GS est donc une option attrayante pour les organisations qui cherchent à sécuriser l'élimination des données sensibles sur leurs supports de stockage, en particulier dans des contextes où la rapidité et l'efficacité sont des critères clés

6.1.7 - SCEE CPA - niveau supérieur

Le protocole défini par le CESG/NCSC (National Cyber Security Centre) au sujet de l'effacement de données à caractère informatique est connu sous le nom de HMG Infosec Standard 5, qui existe à deux niveaux : un niveau supérieur et un niveau inférieur. Ces standards sont utilisés par le gouvernement britannique pour assurer l'effacement sûr des données sur les supports de stockage, notamment les disques durs et les SSD.

HMG Infosec Standard 5, Niveau Supérieur

- **Nombre de Passes** : 3
- **Description** : Ce standard implique trois passes d'effacement. La première passe consiste à écraser les données avec un motif binaire "00", la deuxième passe avec un motif binaire "11", et la troisième passe avec un motif binaire aléatoire. Chaque passe est suivie d'une vérification pour s'assurer que l'effacement a été effectué correctement.

HMG Infosec Standard 5, Niveau Inférieur

- **Nombre de Passes** : 1
- **Description** : Ce standard est plus simple, comprenant une seule passe d'effacement. Il consiste à écraser les données avec un motif binaire "00" et est également suivi d'une vérification pour confirmer l'effacement.

Importance de ces Standards

Ces standards sont importants car ils fournissent une méthode formelle et vérifiable pour l'effacement sûr des données, ce qui est crucial pour les organisations qui doivent garantir la sécurité des informations sensibles avant de réutiliser ou de détruire des supports de stockage. Ils sont particulièrement pertinents pour les agences gouvernementales et les organisations qui traitent des données classifiées ou sensibles.

Application

L'application de ces standards garantit que les données ne peuvent pas être récupérées par des moyens techniques, même avec des outils de récupération de données avancés. Cela aide à prévenir les violations de données et à protéger la confidentialité, l'intégrité et la disponibilité des informations.

En résumé, le protocole défini par le CESG/NCSC pour l'effacement de données à caractère informatique, sous forme de HMG Infosec Standard 5, offre une approche structurée et vérifiable pour assurer l'effacement sûr des données, répondant ainsi aux exigences de sécurité de l'information dans le contexte gouvernemental britannique

6.1.8 - Effacement cryptographique (crypto erase)

L'effacement cryptographique, également connu sous le nom de "cryptographic erasure" ou "crypto erase", est une méthode d'effacement des données qui se concentre davantage sur l'encryption que sur l'écrasement physique des données. Cette méthode est conçue pour empêcher l'accès non autorisé aux données stockées sur les supports de stockage, en supprimant la clé d'encryption des données, rendant ainsi les données cryptées sur le disque illisibles. Voici les détails de cette procédure :

Procédure d'Effacement Cryptographique

1. **Suppression de la Clé d'Encryption** : La première étape de l'effacement cryptographique consiste à supprimer la clé d'encryption des données stockées sur le support de stockage. Cela rend les données cryptées introuvables pour toute personne qui n'a pas la clé d'encryption.
2. **Activation de la Commande Native du Support de Stockage** : Une fois la clé d'encryption supprimée, l'effacement cryptographique suit la commande native du support de stockage. Cela signifie que la méthode d'effacement est spécifique au type de support de stockage utilisé (par exemple, SSD, HDD).
3. **Limitation à des Supports de Stockage Avec Support Intégré** : L'effacement cryptographique ne fonctionne que sur des supports de stockage qui ont un support intégré pour cette opération. Cela exclut les supports de stockage qui ne disposent pas de cette fonctionnalité intégrée.

Avantages de l'Effacement Cryptographique

- **Sécurité Améliorée** : En supprimant la clé d'encryption, l'effacement cryptographique assure que les données ne peuvent pas être déchiffrées, même si elles sont physiquement récupérées du support de stockage.
- **Moins d'Overwriting** : Contrairement à d'autres méthodes d'effacement qui impliquent plusieurs passes d'écrasement des données, l'effacement cryptographique se concentre sur l'encryption, ce qui peut être plus efficace pour les grands volumes de données.
- **Compatibilité** : Cette méthode est compatible avec les supports de stockage modernes qui disposent d'un support intégré pour l'effacement cryptographique, offrant ainsi une solution flexible pour différents types de dispositifs de stockage.

En résumé, l'effacement cryptographique est une méthode avancée d'effacement des données qui se concentre sur l'encryption pour garantir l'inaccessibilité des données. Elle est particulièrement utile pour les organisations qui traitent des données sensibles et cherchent à maximiser la sécurité de leurs informations stockées

6.1.9 - DoD 5220.22-M ECE

Le DoD 5220.22-M est un standard d'effacement des données publié par le Département de la Défense des États-Unis (DoD) en 1995. Il a été introduit pour les institutions nécessitant des niveaux élevés de sécurité, comme le Pentagone. Ce standard est considéré comme un repère pour l'effacement sûr des données. Plus tard, en 2001, un mémoire du DoD a spécifié des méthodes supplémentaires d'overwriting et de vérification qui sont devenues acceptées comme faisant partie du "standard". Parmi ces méthodes, le DoD 5220.22-M ECE est une version étendue (à 7 passes) de la méthode originale DoD 5220.22-M, couramment appelée "DoD long wipe". Cette méthode exécute le DoD 5220.22-M deux fois, avec une passe supplémentaire (DoD 5220.22-M (C) Standard) insérée entre les deux.

Méthode DoD 5220.22-M ECE

La méthode DoD 5220.22-M ECE implique sept passes d'overwriting des emplacements de mémoire accessibles sur le disque dur avec des motifs binaires spécifiques, suivies d'une vérification à la fin de la dernière passe. Les passes sont les suivantes :

1. Tous les emplacements accessibles sont effacés avec zéros binaires.
2. Tous les emplacements accessibles sont effacés avec uns binaires (complément des zéros).
3. Tous les emplacements accessibles sont effacés avec un motif aléatoire de bits.
4. Répétez les étapes 1 et 2.

5. Répétez l'étape 3.
6. Répétez les étapes 1 et 2.
7. Répétez l'étape 3.
8. Vérifiez la dernière passe d'overwriting.

Limitations et Successeurs

Bien que le DoD 5220.22-M ait été considéré comme le standard de référence pour l'effacement des données, il a été remplacé par d'autres normes plus récentes, telles que la NIST SP 800-88, en raison de ses limites concernant l'effacement des stocks de mémoire flash. Le DoD 5220.22-M n'était pas conçu pour effacer les stocks de mémoire basés sur des puces, comme les SSD, ce qui a conduit de nombreuses organisations gouvernementales à cesser de citer le DoD 5220.22 comme un standard pour l'effacement sûr.

Implémentation

L'implémentation du DoD 5220.22-M peut être réalisée avec l'aide de logiciels professionnels d'effacement des données compatibles avec ce standard, tels que BitRaser Drive Eraser. Ces outils permettent aux organismes gouvernementaux et aux organisations privées d'atteindre la conformité réglementaire en utilisant des méthodes d'effacement avancées.

6.1.10 - Effacement basé sur le micrologiciel

L'effacement basé sur le micrologiciel, également connu sous le nom d'Extended Firmware Based Erasure, est une méthode d'effacement des données qui utilise des commandes spécifiques intégrées dans le firmware du support de stockage pour effacer les données de manière sûre. Cette méthode est définie par Blancco et implique trois étapes principales :

1. **Overwrite Initial** : La première étape consiste à écraser les données avec un motif binaire spécifique, généralement zéros binaires, pour commencer le processus d'effacement.
2. **Firmware Based Erasure** : La deuxième étape active une commande de firmware spécifique au type de support de stockage utilisé. Cette commande est conçue pour effacer les données de manière optimale pour le type de média, en tenant compte des spécificités du matériel.
3. **Verification** : La dernière étape consiste à vérifier que l'effacement a été effectué correctement. Cela peut impliquer une lecture du support de stockage après l'effacement pour s'assurer que les données ont été complètement effacées.

Avantages de l'Effacement Basé sur le Micrologiciel

- **Optimisation Matérielle** : En utilisant des commandes de firmware spécifiques, cette méthode est optimisée pour chaque type de support de stockage, garantissant un effacement efficace et sûr.
- **Sécurité Renforcée** : L'activation de commandes de firmware spécifiques contribue à augmenter la sécurité de l'effacement, en s'assurant que les données sont effacées de manière irréversible.
- **Conformité aux Réglementations** : Cette méthode d'effacement est conforme à plusieurs normes et réglementations internationales, ce qui peut être crucial pour les organisations qui doivent répondre à des exigences spécifiques en matière de protection des données.

Applications

L'effacement basé sur le micrologiciel est particulièrement pertinent pour les environnements où la sécurité des données est une priorité absolue, tels que les institutions gouvernementales, les entreprises de défense, et les organisations qui traitent des données sensibles ou classifiées. Il est également utilisé dans le cadre de la préparation de matériel informatique pour sa réutilisation ou sa destruction, garantissant que les données précédemment stockées ne peuvent pas être récupérées.

En résumé, l'effacement basé sur le micrologiciel offre une méthode robuste et sécurisée pour l'effacement des données sur divers supports de stockage, en tirant parti des capacités intégrées du firmware pour garantir un effacement complet et irréversible.

6.1.11 - HMG infosec standard 5

L'HMG Infosec Standard 5, également connu sous le nom de IS5, est un standard britannique pour l'effacement des données utilisé par le gouvernement britannique. Ce standard définit deux niveaux d'effacement des données, chacun avec des exigences spécifiques pour garantir que les données sensibles soient complètement et irrévocablement effacées de supports de stockage tels que les disques durs, les SSD, et les clés USB. L'objectif principal de l'IS5 est de prévenir la divulgation accidentelle ou malveillante de données sensibles lors de la mise hors service ou de la réutilisation de matériel informatique.

Processus d'Effacement

Le processus d'effacement conforme à l'IS5 implique trois passes d'effacement. À chaque étape, les données stockées sur le support de stockage sont réécrites avec des valeurs spécifiques :

1. **Première Passe** : Les données sont réécrites avec des 1s.
2. **Deuxième Passe** : Les données sont ensuite réécrites avec des 0s.
3. **Troisième Passe** : Finalement, les données sont réécrites avec des 1s et des 0s générés aléatoirement.

Ce processus assure que les données originales soient complètement effacées et rendues illisibles, même avec des outils de récupération de données avancés.

Exigences Clés

- **Auditabilité** : Le processus d'effacement doit être entièrement auditible, ce qui signifie que chaque étape de l'effacement doit être documentée et vérifiable. Cela inclut la date et l'heure de l'effacement, le type de média de stockage traité, et la méthode spécifique d'effacement utilisée.
- **Mesures de Sécurité Physique** : Des mesures de sécurité physiques sont nécessaires pour protéger le matériel de stockage pendant le processus d'effacement. Cela comprend l'utilisation de stockages sécurisés et la présence de personnel autorisé pendant le processus d'effacement.
- **Conséquences de la Non-Conformité** : Le non-respect de l'IS5 peut entraîner des conséquences sévères, y compris des dommages financiers et réputés significatifs si des données sensibles sont compromises en raison d'un effacement insuffisant des données. De plus, la non-conformité peut entraîner des actions légales et réglementaires, y compris des amendes et des sanctions.

En résumé, l'HMG Infosec Standard 5 est un standard rigoureux pour l'effacement des données qui vise à garantir que les données sensibles soient complètement et de manière sécurisée effacées de tous supports de stockage, protégeant ainsi contre les risques de divulgation de données sensibles.

6.1.12 - Centre national de sécurité informatique (NCSC-TG-025)

La NSA a développé sa norme d'effacement des données en 2000. Communément connu sous le nom de NCSC-TG-025, le processus utilise trois passages et nécessite une vérification après chaque passage. La première passe écrit des 0 binaires sur un disque dur, la deuxième passe écrit des 1, et la dernière passe écrit des valeurs aléatoires.

Le protocole d'effacement de données selon le NCSC-TG-025, initialement défini dans le Forest Green Book, fait partie de la série Rainbow de directives de sécurité informatique publiées par le National Computer Security Center (NCSC), qui était une entité de la National Security Agency (NSA) des États-Unis. Bien que le NCSC-TG-025 ne soit plus actuellement un standard d'effacement de données pour le NSA, il a joué un rôle important dans la définition des pratiques d'effacement sécurisé des données.

Le protocole NCSC-TG-025 implique trois passes d'effacement, combinant zéros, uns et des caractères aléatoires, comme suit :

1. **Première Passe** : Écriture d'un zéro et vérification de l'écriture.
2. **Deuxième Passe** : Écriture d'un un et vérification de l'écriture.
3. **Troisième Passe** : Écriture d'un caractère aléatoire et vérification de l'écriture.

Ce processus est similaire à celui du DoD 5220.22-M, avec des variations potentielles dans son exécution. Il est important de noter que depuis la publication du Forest Green Book, le NSA/CSS Storage Device Declassification Manual (NSA/CSS SDDM) liste uniquement la démagnétisation et la destruction physique par incinération comme moyens approuvés par le NSA pour nettoyer les données des disques durs. Cela reflète une évolution des pratiques et des normes d'effacement de données au sein de l'agence.

6.1.13 - Publication du bureau du personnel de la marine (NAVSO P-5239-26)

Le NAVSO P-5239-26 est une méthode d'effacement des données originalement définie dans la publication de la Navy Staff Office 5239 Module 26 : Directives du programme de sécurité des systèmes d'information, publiée par la Marine américaine. Cette méthode est conçue pour s'assurer que toutes les données stockées sur un support de stockage, comme un disque dur, un SSD, une carte Flash ou tout autre dispositif de stockage, soient complètement effacées et rendues inutilisables, empêchant ainsi toute récupération de données par des méthodes logicielles ou matérielles.

La méthode NAVSO P-5239-26 est généralement mise en œuvre de la manière suivante :

1. **Pass 1** : Supprime totalement toutes les données.
2. **Pass 2** : Programme un caractère aléatoire et vérifie l'écriture.
3. **Pass 3** : Supprime totalement toutes les données.

Cette séquence d'effacement est conçue pour être très efficace dans l'effacement des données, rendant impossible la récupération de l'information stockée précédemment sur le support de stockage. Elle est particulièrement recommandée pour les dispositifs de stockage qui présentent des défis spécifiques à l'effacement, tels que les SSD (Solid State Drives).

Il est important de noter que bien que la méthode NAVSO P-5239-26 ait été définie par la Marine américaine, il n'est pas clair si elle est encore utilisée comme standard d'effacement des données par l'US Navy. Cependant, elle continue d'être mentionnée comme une option viable pour l'effacement sécurisé des données sur divers supports de stockage.

6.1.14 - NIST 800-88

La NIST SP 800-88, Revision 1, intitulée "Guidelines for Media Sanitization", est une publication du National Institute of Standards and Technology (NIST) des États-Unis qui fournit des directives sur la manière d'effacer efficacement les données sur divers supports de stockage électroniques. Publiée pour la première fois en 2006 et révisée en décembre 2014, cette publication est largement reconnue et utilisée par le gouvernement américain, ainsi que par de nombreuses entreprises privées, pour minimiser les risques de récupération de données sensibles.

Objectifs et Utilisation

L'objectif principal de la NIST SP 800-88 est de guider les organisations sur les meilleures pratiques pour l'effacement sécurisé des données, en particulier lorsque les dispositifs de stockage atteignent la fin de leur cycle de vie ou sont mis hors service. En suivant ces directives, les organisations peuvent s'assurer qu'elles ont pris les mesures nécessaires pour rendre les données irrecevables, réduisant ainsi les risques de divulgation accidentelle ou malveillante de données sensibles.

Méthodes d'Effacement

La publication propose trois niveaux d'effacement des données, chacun adapté à différents besoins en matière de sécurité et de confidentialité :

- **Clear** : Ce niveau d'effacement est destiné à rendre les données irrecevables par des méthodes logicielles simples, mais il ne garantit pas une effacement complet.
- **Purge** : Ce niveau implique un effacement plus profond, généralement réalisé par des méthodes logicielles complexes ou des techniques physiques, comme la démagnétisation ou la destruction physique.
- **Destroy** : Ce niveau d'effacement est le plus sûr, impliquant la destruction complète du support de stockage pour garantir que les données ne puissent jamais être récupérées.

Importance de la Vérification

Une partie importante des directives de la NIST SP 800-88 souligne l'importance de vérifier les résultats de l'effacement. Cela signifie que les organisations doivent confirmer que les données ont été effectivement effacées de manière sécurisée, en utilisant des outils appropriés et en suivant des procédures de documentation.

En résumé, la NIST SP 800-88, Revision 1, offre des lignes directrices claires et détaillées pour l'effacement sécurisé des données sur divers supports de stockage électroniques. En adoptant ces directives, les organisations peuvent renforcer leur posture de sécurité et minimiser les risques associés à la divulgation de données sensibles.

6.1.15 - Méthode de Gutmann

La méthode de Gutmann est une approche d'effacement des données développée par Peter Gutmann et Colin Plumb en 1996. Elle est conçue pour effacer de manière exhaustive et sécurisée les données contenues sur un support de stockage électronique, comme un disque dur, en écrivant une série de 35 motifs différents sur le disque. Ce processus est divisé en quatre phases principales, chacune comprenant un nombre spécifique de passages :

1. **Quatre passages aléatoires** : Ces passages utilisent des valeurs aléatoires pour écraser les données.
2. **Vingt-sept passages complexes** : Ces passages utilisent des motifs d'écrasement complexes pour augmenter la probabilité que les données soient irrécupérables.

3. **Quatre passages aléatoires supplémentaires** : Encore une fois, des valeurs aléatoires sont utilisées pour écraser les données.

La méthode de Gutmann est considérée comme l'une des plus exhaustives pour l'effacement des données, car elle vise à rendre les données irrecevables par n'importe quelle méthode de récupération de données. Cependant, en raison du grand nombre de passages nécessaires, l'effacement selon la méthode de Gutmann peut prendre beaucoup de temps, ce qui peut être un inconvénient pour les utilisateurs qui ont besoin d'effacer rapidement leurs données.

Pour mettre en œuvre la méthode de Gutmann, il est recommandé d'utiliser un logiciel d'effacement qui prend en charge cette méthode, comme AOMEI Backupper Professional. Ce logiciel permet non seulement d'effacer les disques selon la méthode de Gutmann, mais aussi d'autres méthodes d'effacement, telles que l'effacement avec des zéros, l'effacement avec des données aléatoires, et la méthode DoD 5220.22-M. La comparaison entre la méthode de Gutmann et la méthode DoD montre que, bien que la méthode de Gutmann soit plus sûre, elle nécessite également plus de temps pour accomplir l'effacement.

6.1.16 - NSA 130-1

La NSA 130-1, également connue sous le nom de NSA Media Sanitization Guideline, est une directive de la National Security Agency (NSA) des États-Unis qui fournit des instructions sur la manière d'effacer de manière sécurisée les données stockées sur divers supports de stockage. Cette directive est conçue pour aider les organisations à s'assurer que les données sensibles ne soient pas divulguées accidentellement ou malveillamment lors de la mise hors service ou de la réutilisation de matériel informatique.

La NSA 130-1 recommande plusieurs méthodes d'effacement des données, en fonction du niveau de sécurité requis et du type de support de stockage concerné. Ces méthodes incluent :

- **Écrasement** : Réécrire les données avec des zéros ou des uns jusqu'à ce que le support de stockage soit plein.
- **Démagnétisation** : Utiliser un dégausseur pour effacer les données stockées sur des supports magnétiques, comme les disques durs.
- **Destruction physique** : Endommager ou détruire le support de stockage de manière à ce que les données ne puissent plus être récupérées.

La directive met également l'accent sur l'importance de documenter le processus d'effacement, y compris les dates, les heures, les méthodes utilisées et les résultats obtenus. Cela aide à maintenir la transparence et à faciliter les audits de conformité.

Il est important de noter que la NSA 130-1 est spécifique aux besoins de sécurité du gouvernement américain et peut ne pas être applicable à toutes les situations commerciales ou industrielles. Cependant, elle offre des principes et des pratiques valables pour l'effacement sécurisé des données sur divers supports de stockage.

La NSA publie également une liste de produits qui répondent à ses critères de performance pour l'effacement, la destruction ou la disposition des supports de stockage contenant des informations sensibles ou classifiées. Cette liste couvre des équipements tels que les shredders à tranchage croisé, les lecteurs optiques, les dégausseurs, les dispositifs de stockage et les désintégrateurs.

6.1.17 - OPNAVINST 5239.1A

L'OPNAVINST 5239.1A est une instruction de la Navy Staff Office (Office de la Direction de la Marine) des États-Unis qui définit un protocole spécifique pour l'effacement sécurisé des données sur les supports de stockage. Cette instruction est conçue pour s'assurer que les données sensibles ne soient pas divulguées accidentellement ou malveillamment lors de la mise hors service ou de la réutilisation de matériel informatique.

Selon les informations disponibles, l'OPNAVINST 5239.1A implique un processus d'effacement à trois passes, qui comprend les étapes suivantes :

1. **Première Passe** : Écriture d'un octet aléatoire.
2. **Deuxième et Troisième Passes** : Écriture d'un motif statique (par exemple, zéros ou uns).

Chaque pass est suivie d'une vérification pour s'assurer que l'écriture a été effectuée correctement. Ce processus est conçu pour être très efficace dans l'effacement des données, rendant difficile, voire impossible, la récupération des informations stockées précédemment sur le support de stockage 3.

Il est important de noter que l'OPNAVINST 5239.1A est spécifique aux besoins de sécurité du gouvernement américain et peut ne pas être applicable à toutes les situations commerciales ou industrielles. Cependant, elle offre des principes et des pratiques valables pour l'effacement sécurisé des données sur divers supports de stockage.

Pour mettre en œuvre l'OPNAVINST 5239.1A, il est recommandé d'utiliser un logiciel d'effacement qui prend en charge ce protocole spécifique, ou un outil capable de réaliser un effacement à trois passes avec une vérification après chaque passe. Cela garantira que l'effacement est effectué de manière sécurisée et conforme aux exigences de l'instruction.

6.1.18 - Démagnétisation

La démagnétisation est une méthode d'effacement des données qui consiste à utiliser un champ magnétique puissant pour éliminer les traces des données stockées sur un support de stockage magnétique, comme un disque dur. Ce processus est crucial pour garantir que les données sensibles ne soient pas récupérables après la mise hors service d'un dispositif de stockage. Voici une description détaillée de la procédure de démagnétisation pour l'effacement de données à caractère numérique :

Procédure de Démagnétisation

1. **Choix du Dispositif de Stockage** : Identifiez le type de dispositif de stockage à démagnétiser. La démagnétisation est principalement utilisée pour les supports de stockage magnétiques, tels que les disques durs, les disquettes, et les bandes magnétiques.
2. **Sélection d'un Démagnétiseur** : Choisissez un démagnétiseur compatible avec le type de dispositif de stockage. Les démagnétiseurs varient en termes de capacité à effacer différents types de supports de stockage. Assurez-vous que le démagnétiseur est capable de gérer la valeur magnétique du disque dur ou de la bande.
3. **Préparation du Dispositif de Stockage** : Avant de commencer le processus de démagnétisation, retirez toutes les données importantes du dispositif de stockage. La démagnétisation effacera toutes les données, rendant le dispositif de stockage inutilisable pour le stockage de nouvelles données.

4. **Exécution de la Démagnétisation** : Placez le dispositif de stockage dans le démagnétiseur et commencez le processus de démagnétisation. Le démagnétiseur utilisera un champ magnétique puissant pour effacer les données stockées sur le dispositif. Le temps nécessaire pour compléter le processus dépendra de la taille du disque dur et de la puissance du démagnétiseur.
5. **Vérification** : Après la démagnétisation, il est recommandé de vérifier que le processus a été effectué correctement. Cela peut impliquer de tester le dispositif de stockage pour s'assurer qu'aucune donnée n'est accessible. Notez que les disques durs démagnétisés ne sont généralement pas réutilisables pour le stockage de nouvelles données.

Avantages de la Démagnétisation

- **Rend les données irrécupérables** : La démagnétisation garantit que les données sont complètement effacées, rendant leur récupération impossible.
- **Compatibilité étendue** : La démagnétisation peut être utilisée avec une large gamme de supports de stockage magnétiques, y compris les disques durs, les disquettes, et les bandes magnétiques.
- **Réduction des risques de violation de données** : En effaçant les données de manière sécurisée, la démagnétisation aide à réduire le risque de violation de données et de fuites d'informations.

Les dégausseurs de disque dur sont souvent utilisés dans des environnements nécessitant une haute sécurité, comme les institutions gouvernementales, les organisations militaires et certaines entreprises, pour prévenir la fuite ou la récupération non autorisée d'informations sensibles. Ces appareils varient en termes de taille, de puissance et de méthode de dégaussage.

Il existe deux types principaux de dégausseurs : les dégausseurs à impulsions et les dégausseurs continus. Les dégausseurs à impulsions génèrent un champ magnétique très fort mais de courte durée, tandis que les dégausseurs continus produisent un champ magnétique moins intense mais constant pendant une période plus longue.

Il est important de noter que la démagnétisation est une mesure de sécurité importante, surtout pour les entreprises qui doivent s'assurer que les données sensibles ne soient pas accessibles après la mise hors service des dispositifs de stockage.

6.1.19 - Irradiation

La destruction de données par irradiation est une méthode avancée et peu courante pour effacer de manière permanente les données stockées sur les supports de stockage électroniques. Cette technique utilise des rayons ionisants pour endommager les structures chimiques des matériaux de stockage, rendant les données irrécupérables. Voici une procédure hypothétique basée sur les principes généraux de la destruction de données par irradiation, sans référence directe aux sources fournies car elles ne traitent pas explicitement de cette méthode :

Procédure Hypothétique de Destruction de Données par Irradiation

1. **Identification du Support de Stockage** : Identifiez le type de support de stockage à traiter. La destruction par irradiation est généralement utilisée pour les supports de stockage électroniques, tels que les disques durs, les cartes flash, et les modules de mémoire.
2. **Préparation du Support de Stockage** : Assurez-vous que toutes les données importantes sont sauvegardées ailleurs, car le processus d'irradiation rendra le support de stockage inutilisable.

3. **Sélection d'un Equipement d'Irradiation** : Choisissez un équipement d'irradiation approprié pour le type de support de stockage. Les équipements d'irradiation peuvent varier en termes de technologie utilisée (par exemple, gamma, X-ray, particules alpha/bêta) et de capacité.
4. **Configuration de l'équipement d'Irradiation** : Configurez l'équipement d'irradiation selon les spécifications du fabricant et les normes de sécurité applicables. Assurez-vous que l'équipement est installé et opéré conformément aux directives de sécurité.
5. **Exécution de l'Irradiation** : Placez le support de stockage dans l'équipement d'irradiation et commencez le processus d'irradiation. Le temps nécessaire pour compléter le processus dépendra de la dose d'irradiation requise pour effacer les données et de la capacité de l'équipement.
6. **Vérification** : Après l'irradiation, il est crucial de vérifier que le support de stockage ne contient plus de données. Cela peut impliquer des tests pour s'assurer que les données ne sont pas accessibles.
7. **Documentation** : Documentez le processus d'irradiation, y compris les paramètres utilisés, la date et l'heure de l'opération, et les résultats obtenus. Cette documentation est importante pour les audits de conformité et la justification de la destruction des données.

Considérations Importantes

- **Sécurité** : L'irradiation est une technique qui nécessite une attention particulière en matière de sécurité, tant pour l'opérateur que pour l'environnement. Assurez-vous de suivre strictement les directives de sécurité de l'équipement d'irradiation.
- **Coûts et Durabilité** : L'irradiation est une méthode coûteuse et peut ne pas être durable pour certains types de supports de stockage, en particulier ceux qui contiennent des matériaux sensibles à l'irradiation.
- **Alternatives** : Avant de recourir à l'irradiation, envisagez d'autres méthodes d'effacement des données, comme la démagnétisation, la destruction physique, ou l'utilisation de logiciels d'effacement spécifiques.

Il est important de noter que la destruction de données par irradiation est une technique spécialisée qui nécessite une expertise technique et réglementaire spécifique.

6.1.20 - Ponçage et perçage

La destruction de données à caractère numérique par perçage du disque dur est une méthode physique de sécurisation des données qui vise à rendre les données stockées sur un disque dur irrécupérables. Cette technique implique l'utilisation d'un outil mécanique pour percer ou poncer la surface du disque dur, causant des dommages irréparables qui rendent la récupération des données absolument impossible. Voici une procédure hypothétique basée sur les principes généraux de la destruction de données par ponçage, tirée des informations disponibles :

Procédure Hypothétique de Destruction de Données par Ponçage du Disque Dur

1. **Identification du Disque Dur** : Identifiez le disque dur dont vous souhaitez effacer les données de manière permanente. Assurez-vous que toutes les données importantes ont été sauvegardées ailleurs, car le processus de ponçage rendra le disque dur inutilisable.
2. **Sélection d'un Outil de Ponçage** : Choisissez un outil de ponçage spécialement conçu pour la destruction de disques durs. Ces outils sont généralement disponibles auprès de fournisseurs de services de destruction de données professionnels.

3. **Préparation du Disque Dur** : Retirez le disque dur du système informatique ou du serveur pour éviter tout dommage accidentel pendant le processus de ponçage.
4. **Exécution du Ponçage** : Utilisez l'outil de ponçage pour percer ou poncer la surface du disque dur. Le processus doit être effectué avec soin pour s'assurer que les plateaux du disque sont endommagés de manière à rendre les données irrécupérables.
5. **Vérification** : Après le ponçage, il est essentiel de vérifier que le disque dur est effectivement défectueux et que les données ne peuvent plus être récupérées. Cela peut impliquer de tester le disque dur pour s'assurer qu'il ne fonctionne plus.
6. **Recyclage Sécurisé** : Une fois que le disque dur a été détruit, il peut être recyclé de manière sécurisée. Certains fournisseurs de services de destruction offrent des solutions de recyclage sécurisé pour les disques durs détruits.

Avantages de la Destruction par Ponçage

- **Rend les données irrécupérables** : La destruction par ponçage garantit que les données sont complètement détruites, rendant leur récupération impossible.
- **Contrôle total** : Vous avez un contrôle total sur le processus de destruction, ce qui peut être crucial pour les organisations traitant des informations hautement sensibles.
- **Conformité réglementaire** : Pour les organisations soumettant à des réglementations spécifiques, la destruction par ponçage peut aider à s'assurer la conformité en éliminant définitivement les données sensibles.

Il est important de noter que la destruction de données par ponçage est une méthode spécialisée qui nécessite une expertise technique et réglementaire spécifique. Pour des raisons de sécurité et d'efficacité, il est souvent recommandé de faire appel à des services professionnels pour effectuer la destruction des disques durs

6.1.21 - Broyage

La destruction de données à caractère numérique par broyage du support de stockage est une méthode physique de sécurisation des données qui vise à rendre les données stockées sur un support de stockage irrécupérables. Cette technique implique l'utilisation d'un outil mécanique pour broyer le support de stockage, transformant les données en morceaux physiques qui ne peuvent plus être utilisés pour accéder aux informations stockées. Voici une procédure hypothétique basée sur les principes généraux de la destruction de données par broyage, tirée des informations disponibles :

Procédure Hypothétique de Destruction de Données par Broyage du Support de Stockage

1. **Identification du Support de Stockage** : Identifiez le type de support de stockage à traiter. La destruction par broyage est généralement utilisée pour les supports de stockage électroniques, tels que les disques durs, les cartes flash, et les modules de mémoire.
2. **Préparation du Support de Stockage** : Assurez-vous que toutes les données importantes sont sauvegardées ailleurs, car le processus de broyage rendra le support de stockage inutilisable.
3. **Sélection d'un Outil de Broyage** : Choisissez un outil de broyage spécialement conçu pour la destruction de supports de stockage. Ces outils sont généralement disponibles auprès de fournisseurs de services de destruction de données professionnels.
4. **Exécution du Broyage** : Utilisez l'outil de broyage pour broyer le support de stockage. Le processus doit être effectué avec soin pour s'assurer que le support est complètement détruit, rendant les données irrécupérables.

5. **Vérification** : Après le broyage, il est essentiel de vérifier que le support de stockage est effectivement détruit et que les données ne peuvent plus être récupérées. Cela peut impliquer de tester le support de stockage pour s'assurer qu'il ne fonctionne plus.
6. **Élimination Sécurisée** : Une fois que le support de stockage a été détruit, il doit être éliminé de manière sécurisée. Certains fournisseurs de services de destruction offrent des solutions d'élimination sécurisée pour les supports de stockage détruits.

Avantages de la Destruction par Broyage

- **Rend les données irrécupérables** : La destruction par broyage garantit que les données sont complètement détruites, rendant leur récupération impossible.
- **Contrôle total** : Vous avez un contrôle total sur le processus de destruction, ce qui peut être crucial pour les organisations traitant des informations hautement sensibles.
- **Conformité réglementaire** : Pour les organisations soumettant à des réglementations spécifiques, la destruction par broyage peut aider à s'assurer la conformité en éliminant définitivement les données sensibles.

Il est important de noter que la destruction de données par broyage est une méthode spécialisée qui nécessite une expertise technique et réglementaire spécifique. Pour des raisons de sécurité et d'efficacité, il est souvent recommandé de faire appel à des services professionnels pour effectuer la destruction des supports de stockage.

7.0.0 - Description des microprogrammes internes

7.0.1 - Généralités

Voici une liste des principaux types de microprogrammes internes nécessaires au démarrage d'un ordinateur :

- BIOS ou UEFI : Le système de firmware qui contrôle les périphériques de base et gère le démarrage du système.
- Microprogramme de la carte mère : Contenu dans une puce flash sur la carte mère, il initialise le processeur et charge le premier programme.
- POST (Power-On Self-Test) : Une série de tests automatisés effectuée par le BIOS/UEFI pour vérifier l'état du matériel.
- Chargeur de démarrage : Programme chargé pour démarrer le système d'exploitation spécifié.
- Gestionnaire de disque : Pour lire les informations du disque dur ou de la clé USB.
- Pilotes matériels : Pour initialiser et configurer les composants matériels.
- Gestionnaire de mémoire : Pour gérer l'allocation et la gestion de la RAM.
- Gestionnaire de périphériques : Pour reconnaître et configurer les périphériques connectés.
- Gestionnaire de réseau : Pour configurer et gérer les connexions réseau.
- Gestionnaire de sécurité : Pour vérifier et appliquer les paramètres de sécurité comme Secure Boot.
- Gestionnaire de temps réel : Pour gérer les tâches en mode temps réel si nécessaire.
- Gestionnaire de configuration : Pour afficher et modifier les paramètres du BIOS/UEFI.
- Gestionnaire d'erreurs : Pour gérer et signaler les problèmes rencontrés lors du démarrage.

- Gestionnaire de sauvegarde : Pour restaurer des configurations précédentes si nécessaire.

Ces microprogrammes travaillent ensemble pour assurer un démarrage sécurisé et efficace du système d'exploitation. Leur séquence d'exécution dépend des spécificités du matériel et de l'architecture choisie par le fabricant.

7.0.2 - BIOS

Basic Input Output System est l'ancien système de firmware qui contrôle les périphériques de base d'un ordinateur.

- Utilise des interruptions matérielles permettant d'accéder aux fonctionnalités de base du matériel.
- BIOS supporte principalement les systèmes d'exploitation Windows NT.
- BIOS utilise des partitions MBR (Master Boot Record).
- BIOS ne propose pas de fonctionnalités de sécurité native.
- BIOS fonctionne en mode 16 bits.
- BIOS utilise principalement le clavier pour naviguer.
- BIOS a tendance à prendre plus de temps pour démarrer le système.

Voici une description détaillée de la séquence de démarrage d'une machine en BIOS :

Séquence de démarrage BIOS

Voici une description détaillée de la séquence de démarrage d'une machine embarquant un BIOS :

1. Allumage du système

- Le système passe d'un état dormant à un état actif.
- L'alimentation électrique est appliquée aux composants.
- Le microprocesseur commence à fonctionner.

2. Power-On Self-Test (POST)

- Le BIOS exécute une série de tests de diagnostic appelés POST.
- Ces tests vérifient la présence et le bon fonctionnement des composants essentiels.
- Ils identifient tout problème matériel critique.

3. Vérification de la configuration

- Le BIOS vérifie la configuration matérielle (RAM, processeur, etc.).
- Il reconnaît les périphériques connectés.

4. Affichage de l'écran de démarrage

- Un écran noir avec des informations du BIOS s'affiche brièvement.
- Il montre généralement le logo du constructeur et des informations techniques.

5. Sélection de l'option de démarrage

- Le système attend que l'utilisateur presse une touche pour continuer.
- À ce stade, l'utilisateur peut modifier la configuration du BIOS si nécessaire.

6. Vérification des périphériques

- Le BIOS vérifie les périphériques listés dans l'ordre de démarrage.
- Il cherche un système d'exploitation sur le premier périphérique listé.

7. Chargement du Master Boot Record (MBR)

- Si un périphérique bootable est trouvé, le MBR est chargé.
- Le MBR contient le code pour charger le système d'exploitation.

8. Chargement du système d'exploitation

- Le code du MBR charge le système d'exploitation spécifié.
- Il peut passer des paramètres supplémentaires à l'OS.

9. Démarrage complet

- L'OS prend le contrôle du système.
- Il initialise les services et les pilotes nécessaires.

Cette séquence décrit le processus général de démarrage d'une machine BIOS. Le système peut varier légèrement selon les fabricants et les configurations spécifiques.

7.0.3 - EFI

Extensible Firmware Interface est un standard d'interface de firmware pour les ordinateurs personnels développé par Intel en 1998.

- Fournit un environnement d'exécution indépendant du matériel, avec ses propres pilotes et applications qui s'exécutent avant le démarrage du système d'exploitation.
- EFI utilise des interfaces de programmation appelées "protocoles" plutôt que des appels système.
- Les applications et pilotes EFI interagissent avec le firmware en utilisant ces protocoles plutôt que des appels système traditionnels.
- Supporte principalement les systèmes d'exploitation Windows NT.
- Utilise des partitions MBR (Master Boot Record).
- Limité dans son support des formats de disque.
- Principalement utilisé par Intel.
- Contrairement au BIOS qui utilise des interruptions logicielles, EFI utilise une approche orientée objet avec ces protocoles pour fournir ses services.

Séquence de démarrage EFI

Voici une description détaillée de la séquence de démarrage d'une machine en EFI :

1. Initialisation du système

- Le système passe d'un état dormant à un état actif.
- L'alimentation électrique est appliquée aux composants.
- Le microprocesseur commence à fonctionner.

2. Vérification initiale

- Le système vérifie la présence d'alimentation.
- Il initialise la mémoire RAM.

- Il configure les cartes PCI.

3. Lecture des variables NVRAM

- Le système lit les variables NVRAM globales.
- Il récupère la liste d'ordre de démarrage (Boot Order List).
- Il extrait les informations sur chaque option de démarrage.

4. Affichage de l'écran de démarrage

- Si configuré, l'écran de démarrage EFI s'affiche.
- Il montre les options de démarrage disponibles.

5. Sélection de l'option de démarrage

- L'utilisateur sélectionne une option de démarrage.
- Cette sélection est stockée temporairement.

6. Chargement du bootloader EFI

- Le système charge le fichier bootloader EFI spécifié dans la variable NVRAM.
- Ce fichier est généralement situé dans le répertoire EFI.

7. Initialisation du bootloader

- Le bootloader EFI est exécuté.
- Il vérifie les paramètres de démarrage.

8. Chargement de l'OS

- Le bootloader EFI charge le système d'exploitation spécifié.
- Il peut passer des paramètres supplémentaires à l'OS.

9. Démarrage complet

- L'OS prend le contrôle du système.
- Il initialise les services et les pilotes nécessaires.

Cette séquence décrit le processus général de démarrage d'une machine EFI. Le système peut varier légèrement selon les fabricants et les configurations spécifiques.

7.0.4 - UEFI

Unified Extensible Firmware Interface est une évolution d'EFI, développée plus tard pour améliorer ses fonctionnalités et sa sécurité. Il a été publié en 2009.

- Utilise des appels de fonction.
- Plus flexible et extensible que EFI.
- Supporte un large éventail de systèmes d'exploitation, y compris Linux et macOS.
- Conçu pour être rétrocompatible avec le BIOS traditionnel, ce qui n'était pas le cas d'EFI.
- Utilise des partitions GPT (GUID Partition Table).
- Permet l'utilisation de disques SSD et HDD de manière plus efficace.
- Utilise une partition système EFI (ESP) spécifique pour stocker les fichiers de démarrage, alors qu'EFI n'avait pas cette exigence.

Séquence de démarrage UEFI

Voici une description détaillée de la séquence de démarrage d'une machine en UEFI :

1. Initialisation du système

- Le système passe d'un état dormant à un état actif.
- L'alimentation électrique est appliquée aux composants.
- Le microprocesseur commence à fonctionner.

2. Vérification initiale

- Le firmware UEFI exécute une série de tests de diagnostic appelés POST (Power-On Self-Test).
- Ces tests vérifient la présence et le bon fonctionnement des composants essentiels.
- Ils identifient tout problème matériel critique.

3. Lecture des variables NVRAM

- Le système lit les variables NVRAM globales.
- Il récupère la liste d'ordre de démarrage (Boot Order List).
- Il extrait les informations sur chaque option de démarrage.

4. Affichage de l'écran de démarrage

- Un écran EFI s'affiche, montrant les options de démarrage disponibles.
- Il peut inclure des informations sur le matériel et les périphériques.

5. Sélection de l'option de démarrage

- L'utilisateur sélectionne une option de démarrage.
- Cette sélection est stockée temporairement.

6. Chargement du bootloader EFI

- Le système charge le fichier bootloader EFI spécifié dans la variable NVRAM.
- Ce fichier est généralement situé dans le répertoire EFI du système de fichiers.

7. Initialisation du bootloader EFI

- Le bootloader EFI est exécuté.
- Il vérifie les paramètres de démarrage et peut afficher une interface utilisateur graphique.

8. Chargement de l'OS

- Le bootloader EFI charge le système d'exploitation spécifié.
- Il peut passer des paramètres supplémentaires à l'OS.

9. Démarrage complet

- L'OS prend le contrôle du système.
- Il initialise les services et les pilotes nécessaires.

Cette séquence décrit le processus général de démarrage d'une machine UEFI moderne. Le système peut varier légèrement selon les fabricants et les configurations spécifiques. UEFI offre une approche plus flexible et sécurisée que BIOS, avec une meilleure intégration avec les systèmes d'exploitation modernes.

7.0.5 - Stockage

le microprogramme n'est pas obligatoirement stocké sur une puce EEPROM. Voici les principaux points à retenir :

Histoire du stockage du BIOS :

- Avant 1990, le BIOS était stocké sur des puces ROM non programmables.
- Depuis environ 1990, les microprogrammes sont généralement stockés sur des puces EEPROM ou flash reprogrammables.

Types de puces utilisées :

- ROM (Read Only Memory) : Non programmable, utilisée avant 1990.
- PROM (Programmable Read Only Memory) : Programmable une seule fois.
- EPROM (Erasable Programmable Read Only Memory) : Programmable et réprogrammable avec un rayon UV.
- EEPROM (Electrically Erasable Programmable Read Only Memory) : Programmable électriquement.
- Flash ROM : Type de EEPROM qui peut être facilement reprogrammé en place.

Avantages des puces modernes :

- Possibilité de mise à jour du microprogramme sans avoir besoin de changer la puce.
- Réduction des coûts grâce à l'utilisation de technologies plus abordables que les EPROM.

Variations selon les fabricants :

- Certains fabricants peuvent utiliser différentes technologies selon leurs modèles ou préférences.

Sécurité et sauvegarde :

- Certains systèmes incluent une copie de secours du BIOS pour éviter les problèmes de corruption.

En conclusion, bien qu'EEPROM soit très couramment utilisé pour le stockage du BIOS, il n'est pas obligatoire. Le choix dépend des besoins spécifiques du fabricant et des caractéristiques techniques de chaque système.

7.1.0 - Secure boot

7.1.1 - Principe de base

Le Secure Boot est une fonctionnalité de sécurité développée par le consortium UEFI pour s'assurer que seuls des logiciels immuables et signés sont chargés lors du démarrage du système. Il utilise les signatures numériques pour valider l'authenticité, la provenance et l'intégrité du code qui est chargé.

7.1.2 - Composants clés

Le Secure Boot repose sur plusieurs pièces et étapes principales :

1. Les bases de données DB et DBX :

- La base de données DB (Allow DB) stocke les hachages et clés des chargeurs et applications EFI autorisés à être chargés par le matériel.

- La base de données DBX (Disallow DB) stocke les hachages et clés révoqués, compromis ou non-trustés.

2. Les bases de données de signature :

- La base de données db contient la liste des signataires ou des hachages d'images UEFI autorisées.
- La base de données dbx contient la liste des signatures révoquées.

3. La base de données KEK (Key Enrollment Key) :

- Contient une liste de clés publiques utilisées pour mettre à jour les autres bases de données.

7.1.3 - Processus de fonctionnement

1. Au démarrage du système, le firmware vérifie les signatures de chaque composant de démarrage, y compris les pilotes UEFI, les applications EFI et le système d'exploitation.
2. Si les signatures sont valides, le système démarre normalement et le firmware cède le contrôle au système d'exploitation.
3. Si un composant n'est pas considéré comme fiable, le firmware doit initier une récupération spécifique à l'OEM pour restaurer le firmware fiable.
4. Le processus de vérification se poursuit en chaîne, avec chaque composant s'assurant que le suivant est signé et autorisé par les bases de données de signature.

7.1.4 - Gestion des clés et signatures

1. Les OEM peuvent créer des clés Secure Boot en suivant les instructions du fabricant du firmware.
2. Les applications EFI doivent être signées avec une clé approuvée et inclure dans la base de données de signature appropriée.
3. Les bases de données sont stockées dans le RAM non-volatile du firmware et peuvent être mises à jour de manière sécurisée.

7.1.5 - Avantages et considérations

Le Secure Boot offre plusieurs avantages en termes de sécurité :

- Il empêche l'exécution de logiciels malveillants lors du démarrage.
- Il garantit que seuls les composants autorisés par l'OEM peuvent être chargés.
- Il protège contre certains types de rootkits.

Cependant, il peut également avoir des implications sur la compatibilité avec certains systèmes ou applications qui ne sont pas signés ou n'ont pas été approuvés par l'OEM.

En résumé, le Secure Boot est une couche de sécurité essentielle pour les systèmes UEFI modernes, assurant une chaîne de confiance solide depuis le démarrage jusqu'à l'exécution du système d'exploitation.

7.1.6 - Versions de Secure boot

Version 1.0 de Secure Boot

La première version de Secure Boot, introduite avec le UEFI 2.3.1, était basée sur les spécifications UEFI 2.3.1 Errata C. Elle offrait les fonctionnalités de base suivantes :

- Vérification des signatures pour le démarrage du système
- Utilisation d'un ensemble de clés signataires (db et dbx)
- Support pour la mise à jour sécurisée des bases de données

Cette version était plus limitée en termes de fonctionnalités et de sécurité par rapport aux versions ultérieures.

Version 2.0 de Secure Boot

La version 2.0 de Secure Boot, introduite avec le UEFI 2.3.1 Errata C, apportait plusieurs améliorations :

- Utilisation d'algorithme cryptographiques plus robustes (RSA-2048 avec SHA-256)
- Meilleure gestion de la hiérarchie des clés
- Mécanismes d'autorisation plus flexibles
- Support pour un plus grand nombre d'algorithmes cryptographiques

Cette version est largement considérée comme la référence actuelle et la plus sécurisée.

Version 3.0 de Secure Boot

Bien que moins couramment mentionnée, il existe une version 3.0 de Secure Boot qui a été introduite récemment :

- Amélioration des performances par rapport aux versions précédentes
- Nouvelles fonctionnalités de sécurité avancées
- Optimisations pour les systèmes embarqués

Il est important de noter que cette version n'est pas encore largement adoptée et ses spécifications exactes peuvent varier selon les fabricants.

7.1.7 - Différences principales entre les versions

1. Sécurité : Les versions ultérieures offrent un niveau de sécurité accru grâce à l'utilisation d'algorithms plus robustes et de mécanismes d'autorisation plus complexes.
2. Compatibilité : TPM 2.0 est généralement compatible avec TPM 1.2, mais pas toujours au contraire.
3. Performances : Les versions plus récentes offrent généralement meilleures performances en termes de calculs cryptographiques et de vérification de signatures.
4. Flexibilité : Les versions plus récentes offrent plus de flexibilité dans la gestion des clés et des autorisations.
5. Certifications : Certaines versions peuvent nécessiter des certifications spécifiques, comme FIPS, ce qui peut influencer le choix du type de TPM.

En résumé, bien qu'il y ait eu plusieurs versions de Secure Boot, la version 2.0 reste la référence actuelle et la plus largement supportée. La sélection de la version appropriée dépend souvent des besoins spécifiques de sécurité et de compatibilité de l'organisation ou de l'utilisateur.

7.2.0 - TPM

7.2.1 - Définition et principe de base

Le TPM (Trusted Platform Module) est un module cryptographique intégré dans le matériel informatique qui améliore la sécurité et la confidentialité des systèmes. Il s'agit d'une puce séparée sur la carte mère, bien que certaines implémentations récentes puissent l'intégrer au chipset du système.

7.2.2 - Fonctionnalités principales

Le TPM offre plusieurs fonctionnalités essentielles :

1. Gestion de clés : Il permet de créer, stocker et gérer des clés cryptographiques de manière sécurisée.
2. Authentification : Le TPM peut vérifier l'intégrité et l'autenticité du système d'exploitation et du microprogramme.
3. Chiffrement : Il prend part à la protection des données par le biais du chiffrement et du déchiffrement.
4. Proofs : Le TPM peut prouver quels logiciels sont exécutés sur un système donné.

7.2.3 - Composants et architecture

Le TPM comprend généralement les éléments suivants :

1. Un processeur cryptographique intégré pour effectuer des calculs cryptographiques.
2. Des mémoires tampon sécurisées pour stocker temporairement des données sensibles.
3. Un registre de clés pour stocker et gérer les clés cryptographiques.
4. Une interface avec le système d'exploitation pour communiquer et exécuter des commandes.

7.2.4 - Processus de fonctionnement

1. Initialisation : Le TPM est initialisé lors du démarrage du système par le firmware ou le microprogramme.
2. Vérification de l'intégrité : Le TPM vérifie l'intégrité du système d'exploitation et du microprogramme.
3. Gestion des clés : Le TPM génère et gère des clés cryptographiques pour divers services de sécurité.
4. Exécution de fonctions : Sur demande du système d'exploitation, le TPM peut effectuer des calculs cryptographiques, signer des données, etc.

7.2.5 - Intégration avec Windows

Windows utilise largement le TPM pour améliorer la sécurité de la plateforme :

1. BitLocker : Le TPM aide à protéger les données en chiffrant le lecteur.
2. Windows Hello : Il prend part à la création et au stockage sécurisé des clés utilisées par Windows Hello.
3. Vérification de l'intégrité : Le TPM contribue à vérifier que le système d'exploitation et le microprogramme sont authentiques.

7.2.6 - Avantages et considérations

Les avantages du TPM incluent :

- Amélioration significative de la sécurité matérielle.
- Capacité à prouver l'intégrité du système.
- Support pour des scénarios avancés de sécurité qui ne peuvent pas être atteints uniquement par le logiciel.

Cependant, il faut noter que le TPM doit être approvisionné avant de pouvoir être utilisé pleinement pour les scénarios avancés.

En résumé, le TPM est une technologie essentielle pour la sécurité informatique moderne, offrant une racine matérielle de confiance solide et diverses fonctionnalités cryptographiques intégrées dans le matériel.

7.2.7 - Versions de TPM

TPM 1.0

- Première version de TPM
- Utilise des algorithmes cryptographiques plus anciens
- Moins de fonctionnalités que les versions ultérieures

TPM 1.2

- Version améliorée de TPM 1.0
- Ajout de nouvelles fonctionnalités et algorithmes
- Plus largement supporté que TPM 1.0

TPM 2.0

- Version actuelle la plus répandue
- Meilleures performances et sécurité
- Support pour un plus grand nombre d'algorithmes cryptographiques

7.2.8 - Différences techniques

- Algorithmes cryptographiques : TPM 2.0 utilise des algorithmes plus robustes et largement acceptés
- Hierarchy de clés : TPM 2.0 offre une meilleure gestion de la hiérarchie des clés
- Autorisation : TPM 2.0 propose des mécanismes d'autorisation plus flexibles
- Mémoire non volatile : TPM 2.0 utilise des technologies de mémoire non volatile améliorées

7.2.9 - Types de TPM

1. dTPM (Discrete TPM)

- Module physique séparé connecté à la carte mère
- Offre plus de flexibilité mais nécessite un espace supplémentaire

2. fTPM (Firmware TPM)

- Implémenté dans le chipset du système
- Consomme moins d'énergie et occupe moins d'espace

7.2.10 - Certifications

- dTPM : Souvent certifié FIPS (Federal Information Processing Standards)
- fTPM : Peut ne pas avoir de certification FIPS, sauf mention spécifique

7.2.11 - Compatabilité

- TPM 2.0 est généralement compatible avec TPM 1.2, mais pas toujours au contraire
- Certaines applications peuvent nécessiter un TPM spécifique (1.2 ou 2.0)

7.2.12 - Performances

- TPM 2.0 offre généralement meilleures performances que les versions antérieures
- fTPM peut offrir des performances légèrement inférieures aux dTPM dans certains cas

7.2.13 - Considérations pratiques

- TPM 2.0 est recommandé pour la plupart des nouveaux systèmes
- La compatibilité avec les anciens logiciels peut être un facteur à considérer lors du choix
- Pour les organisations nécessitant des certifications spécifiques, dTPM peut être préférable

Il est important de noter que ces différences peuvent varier selon les fabricants et les modèles spécifiques. La sélection du type de TPM approprié dépend souvent des besoins spécifiques de sécurité et de performance de l'organisation ou de l'utilisateur.

Références et sources

Les différents types de supports de stockage :

- **17ème colloque Louis Néel** - Couches minces et nanostructures magnétiques
- **CNRS** - Les nouveaux défis de la spintronique
- **Commissariat à l'énergie atomique** - Stockage de l'information : les acquis et les promesses du nanomagnétisme et de la spintronique
- **Université de Lyon** - Histoire des supports de stockage : de la carte perforée à la clé USB
- **IUT de Villetaneuse** Département Informatique TD 6
- Site officiel de Kingston
- Les différents types de SSD
- Couple de spin-orbite en vue d'application aux mémoires cache
- Estimation de performances et de consommation énergétique de système de stockage à base de mémoire flash dans les systèmes embarqués - Pierre Olivier - HAL open science

Les différents adressages

- Experimental methods for the evaluation of big data systems
- Simulation générique et contribution à l'optimisation de la robustesse des systèmes de stockage de données à large échelle

Normes et référentiels

- Données personnelles et IA
- Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique
- Une liste actualisée des normes d'effacement des données
- Why are data erasure certifications & third-party validations so important ?

Les différents protocoles d'effacements sécurisés

- Air force system security instruction 5020
- ASIP Santé/DSSIS: Guide pratique spécifique à la destruction de données
- Site web de Blancco
- Wiping standards avaible with BCWipe
- Use of the DoD 5220.22-M standard for drive erasure
- Erasing method according to the disc to be erased and the application
- Data sanitization methods
- Méthode d'effacement Gutmann
- Dégausseur - Démagnétiseur de disques durs
- Nettoyage des supports de TI (ITSP.40.006)