BIOS / UEFI

• Le BIOS

Le BIOS (Basic Input/Output System) est un logiciel intégré à la carte mère d'un ordinateur qui permet de configurer et de gérer les paramètres de base du système. Il est responsable de l'initialisation du matériel et de la mise en route du système d'exploitation.

Le BIOS est chargé de :

- Détecter et configurer les périphériques matériels tels que la mémoire, les disques durs, les lecteurs de CD/DVD, etc.

- Gérer les paramètres de boot, tels que l'ordre de boot et les options de démarrage.

- Fournir des fonctionnalités de base pour les opérations d'entrée/sortie, telles que la lecture et l'écriture sur les disques durs et les lecteurs de CD/DVD.

- Offrir des options de configuration pour les paramètres du système, tels que la date et l'heure, les paramètres de sécurité, etc.

Le BIOS est généralement accessible en appuyant sur une touche spécifique pendant le démarrage de l'ordinateur, telle que F2, F12 ou Del. Une fois dans le BIOS, vous pouvez naviguer à travers les menus pour configurer les paramètres de votre système.
Il est important de noter que le BIOS est en train d'être progressivement remplacé par l'UEFI (Unified Extensible Firmware Interface), qui offre des fonctionnalités plus avancées et une meilleure sécurité. Cependant, le BIOS reste encore largement utilisé sur de nombreux ordinateurs.

L'évolution des BIOS a été marquée par plusieurs changements importants au fil des ans. Voici quelques-uns des principaux développements :

- Les premiers BIOS : Les premiers BIOS étaient très simples et ne permettaient que des configurations limitées. Ils étaient souvent stockés dans une mémoire ROM (Read-Only Memory) et ne pouvaient pas être mis à jour.

- Les BIOS avec jumpers : Les cartes mères des années 1980 et 1990 utilisaient des jumpers pour configurer les paramètres du système. Les jumpers étaient des petits connecteurs qui pouvaient être déplacés pour activer ou désactiver certaines fonctionnalités. Cependant, cette méthode était souvent fastidieuse et pouvait être source d'erreurs.
- Les cartes mères jumperless : Les cartes mères jumperless ont été introduites dans les années 1990. Elles utilisaient des interrupteurs ou des boutons pour configurer les paramètres du système, plutôt que des jumpers. Cela a rendu la configuration du système plus facile et plus pratique.

- Les BIOS avec interface graphique : Les BIOS modernes ont une interface graphique qui permet aux utilisateurs de configurer les paramètres du système de manière plus intuitive. Cette interface est souvent accessible via une clé spécifique pendant le démarrage de l'ordinateur.

- Les BIOS avec prise en charge de la technologie Plug and Play : Les BIOS modernes prennent en charge la technologie Plug and Play, qui permet aux périphériques d’être détectés et configurés automatiquement.

- Les BIOS avec prise en charge de la sécurité : Les BIOS modernes ont des fonctionnalités de sécurité avancées, telles que la vérification de l'intégrité du système et la protection contre les logiciels malveillants.

• L’UEFI

L'UEFI (Unified Extensible Firmware Interface) est un remplacement du BIOS (Basic Input/Output System) qui offre des fonctionnalités plus avancées et une meilleure sécurité pour les ordinateurs. L'UEFI est conçu pour être plus flexible et plus évolutif que le BIOS, et il prend en charge des fonctionnalités telles que la gestion de la mémoire, la prise en charge de la technologie Secure Boot et la gestion des périphériques.

Voici quelques-unes des principales caractéristiques de l'UEFI :

- Interface graphique : L'UEFI a une interface graphique qui permet aux utilisateurs de configurer les paramètres du système de manière plus intuitive.
- Gestion de la mémoire : L'UEFI prend en charge la gestion de la mémoire, ce qui permet aux ordinateurs de gérer plus efficacement la mémoire disponible.
- Prise en charge de la technologie Secure Boot : L'UEFI prend en charge la technologie Secure Boot, qui permet de vérifier l'intégrité du système d'exploitation et des logiciels avant de les lancer.
- Gestion des périphériques : L'UEFI prend en charge la gestion des périphériques, ce qui permet aux ordinateurs de détecter et de configurer automatiquement les périphériques connectés.
- Extension de firmware : L'UEFI permet aux fabricants de matériel de créer des extensions de firmware pour ajouter de nouvelles fonctionnalités à l'UEFI.
- Compatibilité avec les systèmes d'exploitation : L'UEFI est conçu pour être compatible avec les systèmes d'exploitation modernes, tels que Windows, Linux et macOS.

L'UEFI offre plusieurs avantages par rapport au BIOS, notamment :

- Meilleure sécurité : L'UEFI offre une meilleure sécurité que le BIOS, grâce à la prise en charge de la technologie Secure Boot et à la vérification de l'intégrité du système.

- Meilleure flexibilité : L'UEFI est plus flexible que le BIOS, grâce à la possibilité de créer des extensions de firmware et de configurer les paramètres du système de manière plus intuitive.

- Meilleure gestion de la mémoire : L'UEFI prend en charge la gestion de la mémoire, ce qui permet aux ordinateurs de gérer plus efficacement la mémoire disponible.

Cependant, l'UEFI a également quelques inconvénients, notamment :

- Compatibilité avec les anciens systèmes : L'UEFI peut ne pas être compatible avec les anciens systèmes d'exploitation ou les anciens périphériques.

Il existe toutefois certains paramètres de compatibilité comme le support dit “Legacy” qui permet de contourner cette limitation. L’option n’est, en revanche, pas disponible sur toutes les cartes mère.

• Quelques paramètres importants

Secure Boot

Secure Boot est une fonctionnalité de sécurité intégrée à l'UEFI (Unified Extensible Firmware Interface) qui permet de vérifier l'intégrité du système d'exploitation et des logiciels avant de les lancer. Cette fonctionnalité est conçue pour empêcher les logiciels malveillants de s'exécuter sur un ordinateur, en particulier les rootkits et les bootkits qui peuvent infecter le système d'exploitation et prendre le contrôle de l'ordinateur.

Voici comment fonctionne Secure Boot :

- Vérification de l'intégrité : Lorsque l'ordinateur démarre, l'UEFI vérifie l'intégrité du système d'exploitation et des logiciels en utilisant des clés de signature numérique.

- Vérification de la signature : L'UEFI vérifie si les logiciels et le système d'exploitation ont été signés avec une clé de signature numérique valide.

- Autorisation : Si les logiciels et le système d'exploitation sont autorisés, l'UEFI les lance. S’ils ne sont pas autorisés, l'UEFI les bloque et empêche leur exécution.

Secure Boot utilise des clés de signature numérique pour vérifier l'intégrité des logiciels et du système d'exploitation. Ces clés sont stockées dans une base de données appelée "Database" (DB) qui est stockée dans l'UEFI. La DB contient les clés de signature numérique des logiciels et du système d'exploitation autorisés.

Il existe trois types de clés de signature numérique utilisées par Secure Boot :

- Clés de signature numérique de confiance : Ces clés sont utilisées pour signer les logiciels et le système d'exploitation autorisés.

- Clés de signature numérique de révocation : Ces clés sont utilisées pour révoquer les clés de signature numérique de confiance qui ont été compromises.

- Clés de signature numérique de plateforme : Ces clés sont utilisées pour signer les logiciels et le système d'exploitation spécifiques à la plateforme.

TPM

TPM (Trusted Platform Module) est un module de sécurité intégré à l'ordinateur qui permet de stocker et de gérer des clés de cryptage, des certificats et d'autres informations sensibles de manière sécurisée. Le TPM est conçu pour fournir une plateforme de sécurité robuste et fiable pour les ordinateurs, en particulier pour les applications qui nécessitent une sécurité élevée, telles que les transactions financières, les communications sécurisées et la protection des données sensibles.

Le TPM est généralement un petit circuit intégré qui est installé sur la carte mère de l'ordinateur. Il est conçu pour être un environnement de sécurité isolé, ce qui signifie qu'il est protégé contre les accès non autorisés et les attaques de sécurité.

Les principales fonctionnalités du TPM sont :

- Génération de clés de chiffrement : Le TPM peut générer des clés de chiffrement sécurisées pour les applications qui nécessitent une sécurité élevée.

- Stockage de clés de chiffrement : Le TPM peut stocker des clés de chiffrement de manière sécurisée, ce qui empêche les accès non autorisés.

- Gestion de certificats : Le TPM peut gérer des certificats de manière sécurisée, ce qui permet de vérifier l'identité des utilisateurs et des applications.

- Vérification d'intégrité : Le TPM peut vérifier l'intégrité du système d'exploitation et des applications, ce qui permet de détecter les attaques de sécurité.

- Gestion de la sécurité : Le TPM peut gérer les paramètres de sécurité de l'ordinateur, tels que les paramètres de connexion et les paramètres de chiffrement.

XMP

Les profils XMP (Extreme Memory Profile) sont des paramètres de configuration de la mémoire RAM qui permettent d'optimiser les performances de la mémoire pour les applications qui nécessitent des débits de transfert élevés.

Les profils XMP sont développés par Intel et sont supportés par la plupart des cartes mères modernes. Ils permettent de configurer les paramètres de la mémoire RAM pour obtenir les meilleures performances possibles, en particulier pour les jeux vidéo, les applications de traitement de l'image et de la vidéo, et les simulations.

Les profils XMP peuvent inclure des paramètres tels que :

- La fréquence d'horloge de la mémoire (en MHz)
- La latence de la mémoire (en cycles d'horloge)
- La tension de la mémoire (en volts)
- Le timing de la mémoire (en cycles d'horloge)

En utilisant un profil XMP, vous pouvez optimiser les performances de votre système en ajustant les paramètres de la mémoire RAM pour répondre aux besoins spécifiques de vos applications. Les profils XMP peuvent être configurés à l'aide de l'UEFI (Unified Extensible Firmware Interface) ou de logiciels de configuration de la mémoire.

Il existe différents types de profils XMP, notamment :

- Le profil XMP par défaut, qui est configuré pour offrir un équilibre entre les performances et la stabilité

- Le profil XMP pour les jeux, qui est configuré pour offrir des performances élevées pour les jeux vidéo

- Le profil XMP pour les applications de traitement de l'image et de la vidéo, qui est configuré pour offrir des performances élevées pour ces types d'applications

Il est important de noter que les profils XMP ne sont pas compatibles avec toutes les cartes mères et les modules de mémoire RAM. Il est donc important de vérifier la compatibilité de votre matériel avant de configurer un profil XMP.

Par exemple lorsqu’un fabricant de barrettes de mémoire sort un nouveau modèle, il se peut que ce dernier ne soit pas bien reconnu par une carte mère qui serait sortie avant ce modèle.
Il est donc généralement nécessaire de mettre à jour l’UEFI.