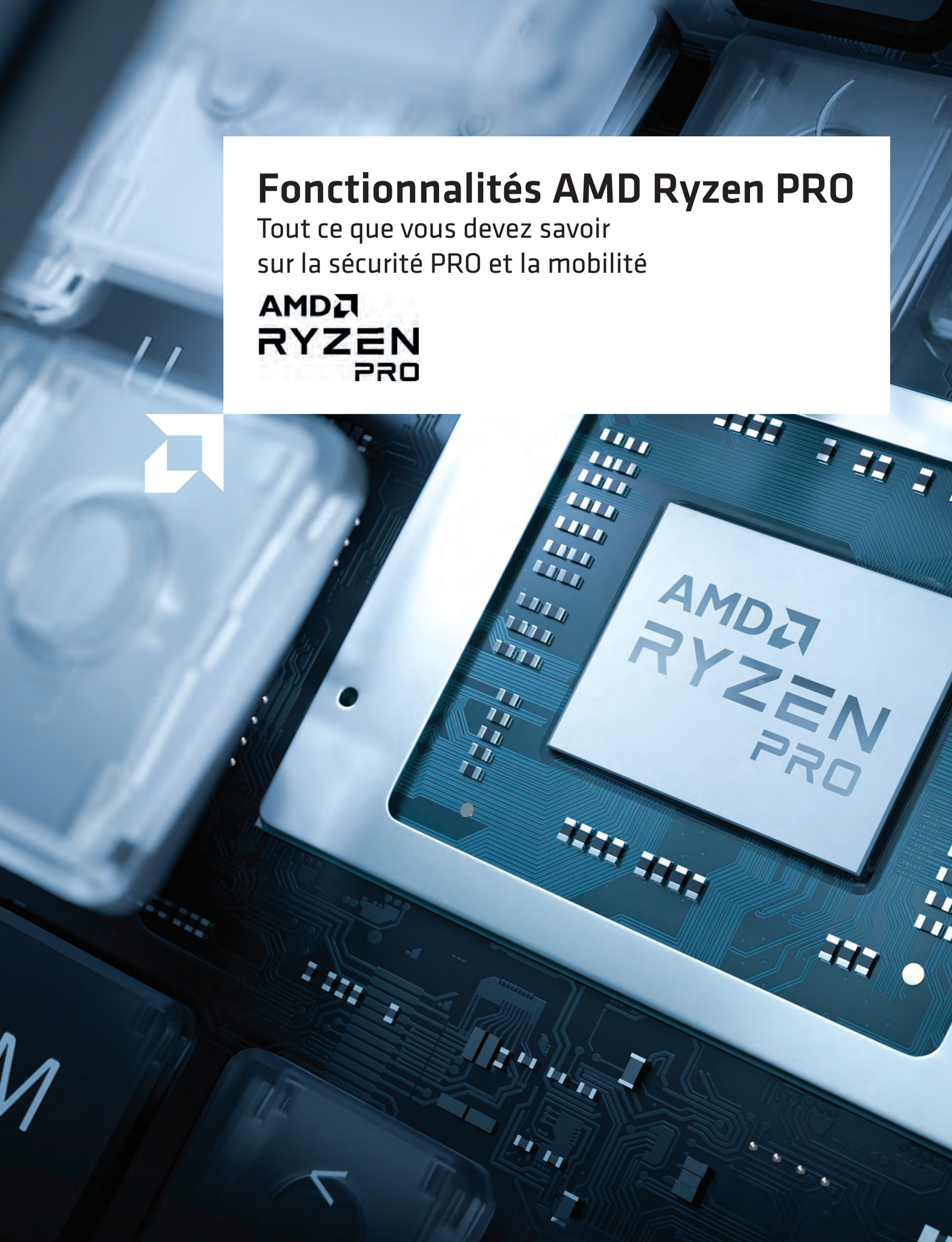
Fonctionnalités AMD Ryzen PRO

Tout ce que vous devez savoir
sur la sécurité PRO et la mobilité

AMD RYZEN PRO



PROCESSEURS POUR PC PORTABLE AMD RYZEN™ PRO SÉRIE 5000 : DES PERFORMANCES ET UNE AUTONOMIE SANS COMPROMIS

Il n'est probablement pas surprenant que la plupart des enquêtes d'opinion fassent apparaître que l'autonomie soit le premier ou parmi les premiers facteurs ayant une influence sur l'achat d'un notebook. Plus on travaille sans être connecté à une prise de courant, plus on se sent libre et plus on éprouve un sentiment de confiance. Et, bien sûr, nous en voulons toujours plus. Il n'y a pas longtemps, huit heures était la référence, puis dix… et ce chiffre augmente sans cesse. Puisque nos tâches pour la maison et le bureau consomment davantage d'énergie, qu'il s'agisse de streaming ou de calculs traitant un nombre considérables de données, l'optimisation de l'efficacité énergétique devient encore plus difficile. Comment peut-on construire des PC portables capables de répondre à l'évolution des demandes des utilisateurs finaux ?

ATTENTES EN CONSTANTE ÉVOLUTION

En réalité, dès que l'objectif a été atteint, la barre est placée plus haut. Le système d'exploitation et les charges de travail continueront à exiger plus de performances (ce qui équivaut à plus d'exigences en termes de puissance sur le système), tandis que les capacités de batterie ont tendance à diminuer pour optimiser les PC ultra portables les plus fins et les plus légers.

Aussi, de même que certains écrans LCD TFT ont désormais de faibles consommations énergétiques, les nouveaux écrans OLED sont en général de plus gros consommateurs d'énergie, surtout dans le cas des anciens modèles. La résolution joue également un certain rôle : plus le nombre de pixels est élevé, plus le processeur et la mémoire doivent travailler, et il ne s'agit pas là d'une augmentation insignifiante des exigences en matière de performances.

COMMENT RÉSOUDRE CE DILEMME : L'APPROCHE D'AMD VIS-À-VIS DE L'AUTONOMIE

AMD résout le dilemme de l'autonomie (consommation énergétique vs. performances) en optimisant la gestion de la consommation énergétique et l'autonomie pour diverses charges de travail plutôt qu'en mettant un accent précis sur un scénario de cas d'utilisation spécifique. Puisque l'expérience de chaque utilisateur vis-à-vis de l'autonomie est unique par rapport à la façon dont il utilise son PC portable, notre objectif doit être d'offrir la meilleure autonomie de sa catégorie pour une grande diversité de scénarios de cas d'utilisation.

Cela doit être accompli indépendamment de la façon dont le PC portable est utilisé ou de la façon dont son utilisation change au cours d'une même journée, voire même de périodes plus longues. L'objectif final est une stratégie AMD axée sur la meilleure autonomie de sa catégorie. Cela nécessite que nous travaillions en étroite collaboration avec nos partenaires OEM afin de garantir que leurs plateformes AMD soient toujours en tête du classement en ce qui concerne l'autonomie.

TROUVER LE BON ÉQUILIBRE ENTRE PERFORMANCES ET CONSOMMATION ÉNERGÉTIQUE POUR UNE AUTONOMIE OPTIMALE

Alors que la conception et le développement de processeurs pour PC portables et de bureau sont extrêmement difficiles, la complexité de la gestion de la consommation énergétique ne l'est pas. Le principal indicateur de basse consommation pour les PC de bureau est la conformité aux normes réglementaires telles que le programme Energy Star et les exigences de la California Energy Commission. Bien qu'il ne soit pas facile de planifier ces exigences, les ingénieurs n'ont qu'à optimiser le mode de puissance faible au repos le plus facile à atteindre.

Un processeur pour PC portable/de bureau est bien plus complexe lorsqu'il s'agit de trouver l'équilibre entre performances et consommation énergétique. La vitesse reste absolument nécessaire, mais il convient d'être beaucoup plus attentif à la consommation énergétique non seulement du processeur lui-même, mais également de tous les composants du système adjacents. Cela nécessite de se focaliser davantage sur les performances par watt, et c'est là que les fonctionnalités avancées et les optimisations entrent en jeu. Cet équilibre délicat entre performances et autonomie est particulièrement évident avec le curseur d'alimentation des performances du système d'exploitation. Nous l'examinerons un peu plus loin.

LORSQU'IL S'AGIT DE L'EXPÉRIENCE UTILISATEUR, LA RÉACTIVITÉ PRIME SUR LES PERFORMANCES BRUTES

Que vous parliez de charges de travail de cœurs de CPU ou de tâches graphiques, une bonne réactivité diffère des performances brutes. La réactivité concerne la rapidité du système lorsque l'utilisateur

navigue d'une fenêtre à l'autre, explore des fichiers, utilise des applications de productivité, et plus encore. Une bonne réactivité permet de garantir une expérience aussi fluide et immersive que possible. Il s'agit d'une optimisation pertinente des performances.

Pour l'utilisateur professionnel/d'entreprise type, cette réactivité est souvent bien plus importante que les performances brutes. Donc un PC portable qui offre la meilleure autonomie de sa catégorie, mais qui n'est pas précis et réactif, ne répondra pas aux attentes de l'utilisateur et aux besoins fondamentaux de l'entreprise pour une meilleure expérience utilisateur.

COMMENT AMD FAIT-ELLE MIEUX ?

Voilà ce qu'AMD optimise : la meilleure autonomie de sa catégorie qui reste réactive et rapide lorsque le PC est branché sur une alimentation CC. AMD apporte d'importantes améliorations architecturales dans « Zen 3 » qui améliorent les performances pures des processeurs pour PC portable AMD Ryzen™ PRO Série 5000 sur les modes d'alimentation CA et CC, mais restent concentrées sur la réactivité.

Les améliorations essentielles de « Zen 3 » comprennent :

- Le contrôle de performance du processeur collaboratif (CPPC) permet une sélection jusqu'à 20 fois plus rapide de la vitesse d'horloge appropriée lorsque le système d'exploitation demande une plus grande activité. Nous discuterons de ce point ultérieurement.
- Une structure de cache unifiée signifie que tous les cœurs peuvent accéder à l'ensemble du plus grand cache L3, ce qui améliore grandement la latence du cache. Vous trouverez d'autres améliorations de « Zen 3 » ci-dessous.

MESURE DE LA RÉACTIVITÉ

Comme les propres indicateurs de réactivité de Microsoft l'ont montré pour améliorer l'expérience Windows de Microsoft, les processeurs
pour PC portable AMD Ryzen™ PRO Série 5000 font preuve essentiellement d'une réactivité rapide sur les modes de source d'alimentation
CA comme CC. Pour l'utilisateur final, cela signifie que l'expérience ne changera pas que son ordinateur soit branché sur la batterie ou non.

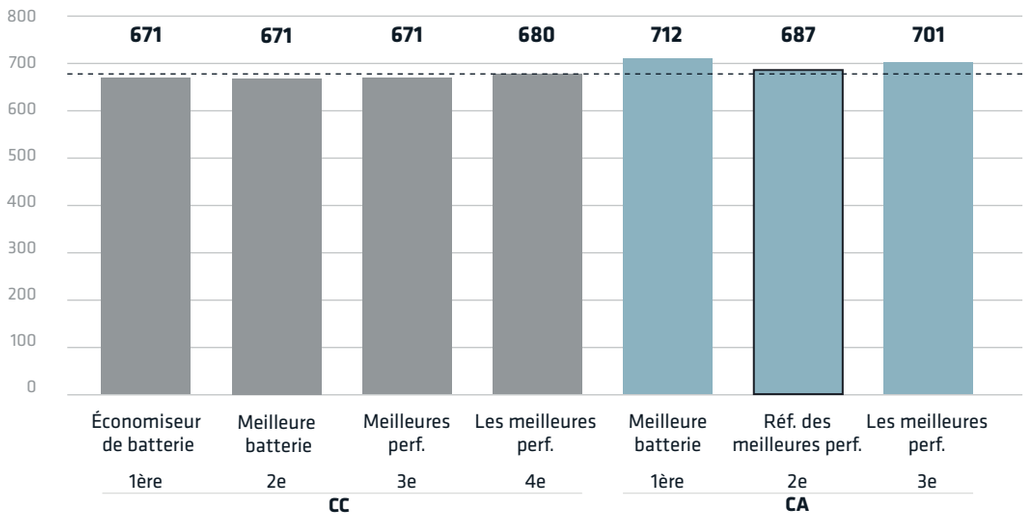
Indicateurs de réactivité de Window

Figure 1.

INDICATEURS DE RÉACTIVITÉ DU SYSTÈME D'EXPLOITATION WINDOWS		CC (MS)	CA (ms)
Individuel – Performances du processus de démarrage Démarrage rapide	Durée de_l'initialisation_du BIOS (moyenne)	20,0	19,4
	Démarrage_total_[hors_BIOS] (moyenne)	5,6	4,9
	Temps_d'arrêt_total (moyenne)	9,0	7,1
Individuel – Performances du démarrage Démarrage complet	Durée de_l'initialisation_du BIOS	21,9	20,7
	Durée de_l'arrêt	6,8	6,7
	Démarrage_total_[hors_BIOS]	7,9	7,4
Individuel – Performances du mode Hibernation	Durée de_l'initialisation_du BIOS (moyenne)	19,3	18,3
	Temps_de suspension_global (moyenne)	7,2	6,2
	Reprise_totale_[hors_BIOS] (moyenne)	4,8	5,4
Mise en veille moderne	Entrée (ms)	5727	5711
	Sortie (ms)	680	687

Le tableau suivant montre le Temps de sortie de la mise en veille moderne dans les sept réglages du curseur d'alimentation du système d'exploitation, souvent considéré comme étant les plus important de tous ces indicateurs puisqu'il est en général plus souvent expérimenté que tous les autres indicateurs combinés.

Temps de sortie de la mise en veille moderne (millisecondes) avec l'AMD Ryzen 7 PRO 5850U *Figure 2.*



Comme vous pouvez le voir dans la ***figure 2***, quelle que soit la position du curseur d'alimentation du système d'exploitation, il n'y a aucune différence perceptible dans l'expérience utilisateur réelle.

PERFORMANCES D'ENSEMBLE : L'APPROCHE MIXTE DES CHARGES DE TRAVAIL

Comme indiqué précédemment, chaque utilisateur aura une expérience différente en termes d'autonomie, même sur un PC portable, déterminée par la façon dont il configure les variables clés. Voici quelques exemples de variables essentielles :

- La première et la plus importante est la luminosité de l'écran. Un utilisateur exigeant une luminosité maximale de l'écran peut réduire l'autonomie de 50 % dans certains cas.
- Le rétroéclairage du clavier, fonctionnalité populaire sur les PC portables professionnels, est une autre variable essentielle. AMD a mesuré que la consommation énergétique du système pouvait augmenter de 2 W, doublant potentiellement la puissance au repos du système. Il s'agit d'une autre occasion d'optimiser les performances.
- Nous devons également mentionner la position du curseur d'alimentation des performances du système d'exploitation. Un réglage de CC n°4 (c.-à-d. Les meilleures performances) offre des performances comme en mode d'alimentation CA, mais au détriment d'une consommation énergétique pratiquement équivalente à l'alimentation CA. Ce réglage est donc à éviter pour bénéficier de la meilleure expérience en termes d'autonomie. La position CC n°2 (c.-à-d. Meilleure batterie) offre une expérience optimale en termes d'autonomie, avec un compromis minimal sur les performances.

Puisque presque chaque aspect du système est un facteur contribuant à la consommation énergétique du système et donc à l'autonomie, toute revendication relative à l'autonomie doit être accompagnée d'une longue liste de conditions pouvant être reproduites de manière fiable.

De nos jours, il semble que chaque testeur, directeur informatique et même utilisateur dispose de sa propre liste de conditions et de charges de travail qui définissent ses attentes vis-à-vis de l'autonomie. Cela est compréhensible, mais une mesure et une comparaison pertinentes s'appuient sur des conditions et des procédures qui peuvent être reproduites précisément à chaque test.

Le respect de ces mesures objectives permet d'effectuer une évaluation pertinente d'éléments comparables en termes de performances, de réactivité et d'autonomie de plateforme en plateforme, ou de configuration en configuration sur la même plateforme.

Pour les PC portables professionnels, les OEM utiliseront principalement une charge de travail d'autonomie mixte basée sur des applications répondant aux normes de l'industrie sous licence de BAPCo, appelé MobileMark® 2018. Elle détermine et contrôle les facteurs contributifs de toutes les plateformes et peut donc être facilement répétée. Il s'agit donc d'un bon moyen de comparer les différentes marques et les différents modèles de PC portables, ainsi que les différentes configurations du même modèle de PC portable. Alors qu'AMD se concentre sur l'optimisation de la consommation énergétique de cette charge de travail mixte répondant aux normes de l'industrie, une approche des charges de travail encore plus large permet également de garantir que, quelles que soient les tâches ou les attentes, les utilisateurs vivront la meilleure expérience possible en termes d'autonomie.

LA SIMPLICITÉ PEUT ÊTRE TROMPEUSE

Les utilisateurs finaux et les testeurs adoptent souvent une approche plus simple pour mesurer l'autonomie, comme lire une vidéo en boucle, soit en streaming soit à partir d'un moyen de stockage local. Bien qu'il s'agisse d'un cas d'utilisation important, il est plutôt unidimensionnel.

Il est très important de s'assurer que 100 % de toutes les conditions de test sont respectées d'un système à l'autre lors de la comparaison. Il convient également de noter qu'en général, les fabricants du secteur n'utilisent pas de contenu en streaming pour les déclarations relatives à l'autonomie car les résultats varient énormément. Ils s'en tiennent aux charges de travail facilement reproductibles et juridiquement défendables pour leurs mesures de l'autonomie et des revendications qui s'ensuivent.

LE CURSEUR DU SYSTÈME D'EXPLOITATION ET LE PROCESSEUR POUR PC PORTABLE AMD RYZEN™ PRO SÉRIE 5000

Le processeur AMD Ryzen™ PRO Série 5000 a été optimisé pour une mise en œuvre complète du curseur d'alimentation des performances du système d'exploitation. La stratégie d'optimisation d'AMD, par position du curseur, est cohérente avec la documentation du système d'exploitation. Il existe sept positions du curseur d'alimentation du système d'exploitation, pour les CC et CA, comme mentionné ci-dessus, et telles que définies dans la ***Figure 3***.

Les sept positions du curseur d'alimentation du système d'exploitation ***Figure 3***

CC				CA		
1ère	**2e**	**3e**	**4e**	**1ère**	**2e**	**3e**
Économiseur de batterie	Meilleure batterie	Meilleures perf. par défaut	Les meilleures performances	Meilleure batterie	Meilleures perf. par défaut	Les meilleures performances

Bien sûr, pour l'autonomie, il s'agit uniquement des quatre positions du curseur CC. La stratégie de performance et de consommation énergétique d'AMD par position se résume comme suit :

Positions du curseur d'alimentation du système d'exploitation CC ***Figure 4***

POSITIONS DU CURSEUR D'ALIMENTATION DU SYSTÈME D'EXPLOITATION CC			
CC – 1ère	**CC – 2e**	**CC – 3e**	**CC – 4e**
Économiseur de batterie	**Meilleure batterie**	**Meilleures performances**	**Les meilleures performances**
Atténue la luminosité de l'écran, orientée vers d'autres systèmes d'exploitation. Les OEM ne l'utilisent pas et il n'est pas possible de la sélectionner par défaut.	Utilisée généralement pour les mesures de l'autonomie et les revendications au détriment des performances.	Les systèmes d'exploitation, AMD et la plupart des OEM l'utilisent par défaut pour l'alimentation CC. Offre le meilleur équilibre entre perf. CC et consommation énergétique.	Les meilleures performances en mode d'alimentation CC. Perf. semblables au mode d'alimentation CC au détriment de l'autonomie. Habituellement, réduction d'un pourcentage à un chiffre par rapport à l'alimentation CA.

Donc bien que les OEM prévoient habituellement la position du curseur du système d'exploitation n°3, ils mesurent et font leurs revendications finales relatives à l'autonomie par rapport à la position du curseur du système d'exploitation n°2. AMD a également optimisé les positions du curseur. Bien qu'AMD recommande que toutes les plateformes s'accompagnent des valeurs AMD par défaut, la définition et l'équilibre entre performances et consommation énergétique de chaque position du curseur reviennent aux OEM.

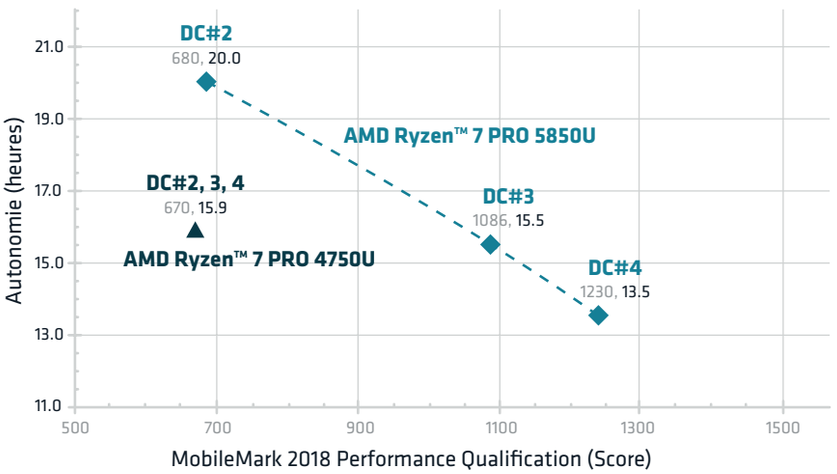
À ce titre, AMD travaille avec les OEM pour modifier les optimisations des performances/de la consommation énergétique par position du curseur selon le souhait des OEM plateforme par plateforme. Un utilisateur final peut facilement modifier ces points d'équilibre de l'optimisation à la volée via l'interface utilisateur du curseur d'alimentation des performances du système d'exploitation au besoin.

EXPÉRIENCE UTILISATEUR ET CARACTÉRISTIQUE D'AUTONOMIE À TRAVERS LES POSITIONS DU CURSEUR D'ALIMENTATION DES PERFORMANCES DU SYSTÈME D'EXPLOITATION

La stratégie d'AMD consiste à fournir à l'utilisateur final un contrôle dynamique de l'équilibre entre performances et consommation énergétique (c.-à-d. l'autonomie) via le curseur d'alimentation des performances du système d'exploitation. Les optimisations du système d'exploitation d'AMD sont conçues pour permettre à tous les utilisateurs de sélectionner le point d'équilibre quelconque dont ils ont besoin. Cela inclut les deux pôles des performances maximales (c.-à-d. Les meilleures performances CC n°4) et de l'autonomie maximale (c.-à-d. Meilleure batterie CC n°2) et une bonne position intermédiaire avec CC n°3 (c.-à-d. Meilleures performances, également le système d'exploitation et AMD par défaut).

Les laboratoires AMD se sont toujours concentrés sur l'étude et l'analyse qui découlent en fin de compte sur les innovations qui apportent performances et améliorations de l'expérience utilisateur de génération en génération. Les processeurs pour PC portable AMD Ryzen™ PRO Série 5000 offrent un avantage significatif par rapport à la génération précédente. En regardant le curseur d'alimentation des performances du système d'exploitation d'une position à l'autre, on peut constater que, même si les processeurs pour PC portable AMD Ryzen™ PRO Série 4000 offrent une autonomie prolongée, il n'existe aucune différence entre une position du curseur du système d'exploitation et une autre. Les processeurs pour PC portable AMD Ryzen™ PRO Série 5000 améliorent non seulement considérablement cette meilleure autonomie, mais offrent également une différence significative au niveau du point d'équilibre entre performances et consommation énergétique dans toutes les positions du curseur du système d'exploitation, offrant à l'utilisateur final le contrôle dynamique précédemment mentionné.

Comparaison générationnelle de l'AMD Ryzen™ PRO à propos de l'autonomie et des performances[1,2] ***Figure 5***



Comparaison générationnelle du processeur AMD PRO en ce qui concerne l'autonomie et les performances. Il convient de noter que l'utilisateur dispose d'une liberté entière et d'un contrôle total en matière d'autonomie et de performances avec le processeur AMD Ryzen™ PRO Série 5000. Comparé au processeur AMD Ryzen™ 7 PRO 4750U, l'utilisateur du processeur AMD Ryzen™ 7 PRO 5850U peut sélectionner :

1. *CC n°2 avec des performances similaires à une amélioration de l'autonomie de 26 %,*
2. *CC n°3 avec une autonomie similaire à une amélioration des performances de 62 %, ou*
3. *CC n°4 à un compromis sur l'autonomie de 15 % maximum, offrant néanmoins une amélioration des performances de 84 %*

[1]Tests réalisés par AMD Labs en utilisant le test du benchmark MobileMark® 2018 pour mesurer l'autonomie et les performances d'un processeur Ryzen™ 7PRO 5850U vs. un processeur Ryzen™ 7 PRO 4750U. Les scores MM18 pour le Ryzen™ 7PRO 5850U au niveau des points de données CCn°3 et CCn°4 et pour le Ryzen™ 7 PRO 4750U au niveau des points de données CCn°2 et CCn°4 sont des estimations.
[2]L'autonomie Windows 10 MobileMark® 2018 varie en fonction de divers facteurs, notamment le modèle du produit, la configuration, les applications chargées, les fonctionnalités, l'utilisation, la fonctionnalité sans fil, la capacité de la batterie et les réglages de la gestion de la consommation énergétique.

RÉSOUDRE LA QUESTION DE LA SÉCURITÉ VS. LES PERFORMANCES

Les fonctions de sécurité sont une exigence clé pour la productivité de l'entreprise et toujours une partie essentielle de la philosophie de conception d'AMD. Cela est toujours vrai pour le processeur AMD Ryzen™ PRO Série 5000, pour lequel nous améliorons les fonctions de sécurité avec l'impact le plus négligeable possible sur les performances et la consommation énergétique. Et cet engagement pour arriver à une position de leadership en matière de sécurité ne date pas d'aujourd'hui – les capacités et fonctions uniques de sécurité d'AMD garantissent une sécurité robuste et une efficacité énergétique maximales dans les années à venir.

Les critères déterminants seront toujours un minimum de compromis et l'expérience utilisateur maximale.

La preuve de cet engagement est une liste croissante de fonctions de sécurité sur silicium AMD très recherchées, sans pénaliser la consommation énergétique ou l'autonomie, y compris un nouvel ajout au processeur Ryzen™ PRO Série 5000.

- Transparent Secure Memory Encryption (TSME, également appelée AMD Memory Guard)
- Indirect Branch Control (IBC)
- Guest Mode Execute Trap (GMET)
- User Mode Instruction Prevention (UMIP)
- AMD Shadow Stack (nouvelle fonctionnalité pour le Ryzen™ PRO Série 5000)

CONSOMMATION ÉNERGÉTIQUE DU SYSTÈME ET ALIMENTATION ÉLECTRIQUE (EFFICACITÉ CC-CC)

Un autre domaine dans lequel AMD a apporté des améliorations générationnelles importantes est l'alimentation via la plateforme jusqu'au processeur. Faisant partie des plus gros consommateurs d'énergie dans un système de PC portable, une gestion attentive et précise de l'alimentation du processeur peut permettre d'économiser des centaines de mW de puissance sous forme d'efficacité CC-CC, essentiellement sans compromis.

La perte CC-CC dans une plateforme est souvent passée sous silence et mal comprise en tant que gros consommateur d'énergie dans un PC portable. Une gestion attentive de l'alimentation du processeur ainsi que des sous-systèmes d'alimentation au niveau de la carte peuvent faire la différence entre une autonomie passable et la meilleure expérience de sa catégorie.

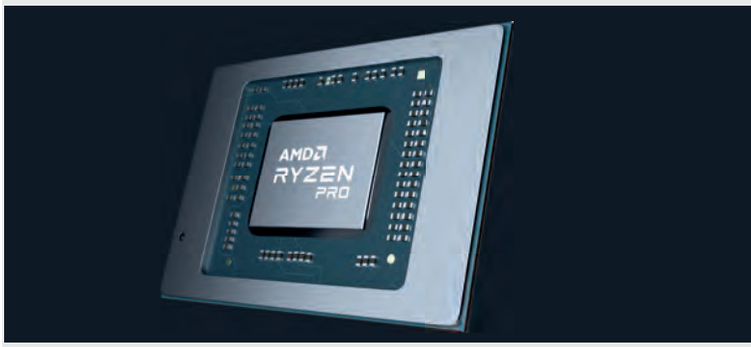
LES CHIFFRES DE PRÈS

Nous pouvons également regarder de près, dans les principaux composants du système, pour voir quelle est la consommation énergétique du système. Les ***figures 6 et 7*** montrent deux charges de travail différentes, Windows Idle et la charge de travail mixte répondant aux normes de l'industrie dont nous avons précédemment parlé, utilisée par les plateformes professionnelles.

- Dans chaque cas, il convient de noter que les deux plus gros consommateurs d'énergie sont l'écran et le processeur. Si l'on se concentre un peu plus sur l'écran, la modification de la charge de travail en augmentant la luminosité à 100 % (~400 nits par rapport au point de consigne de 150 nits) peut fortement augmenter la consommation énergétique de ce composant.
- De même, la désactivation de la fonction de gestion de l'énergie de l'écran AMD Vari- Bright pourrait également avoir un effet négatif important sur l'autonomie. Vari-Bright est une fonction d'économie d'énergie exclusive d'AMD qui marche avec tous les écrans LCD TFT.
- Le plus important est le modèle d'écran sélectionné pour la plateforme. Vous trouverez un écran LCD TFT standard à la résolution FHD avec la caractéristique de consommation énergétique présentée dans la ***figure 6*** ou même inférieur.
- De plus, les panneaux d'affichage plus onéreux qui se vantent d'avoir des taux de rafraîchissement élevés, des fonctionnalités de confidentialité spéciales et un nombre de pixels élevé (p. ex. UHD) consommeront toujours plus d'énergie. Enfin, bien que les écrans OLED soient visuellement supérieurs, ils sont également plus onéreux et plus gros consommateurs d'énergie.

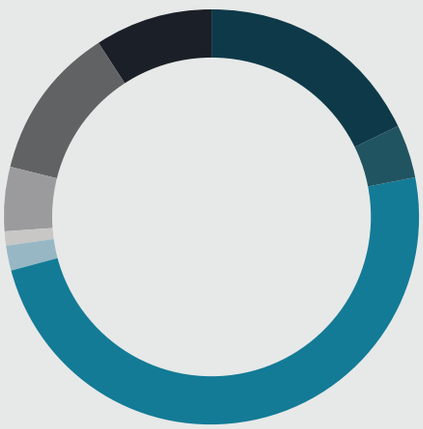
La lecture et la réponse à un email constitue une charge de travail à peine supérieur à Windows en état inactif comme illustré ci-dessus. Il convient également de noter qu'indépendamment de la marque/du modèle ou même de la résolution du panneau d'affichage, il est toujours possible de réduire la consommation de l'affichage en diminuant la luminosité, par conséquent, les préférences de l'utilisateur concernant le réglage de la luminosité de l'écran contribuent à préserver l'autonomie. La consommation énergétique faible du système, et donc l'autonomie accrue, sont fragiles.

De nombreux utilisateurs pourraient ne pas bien comprendre comment les choix qu'ils font ont une incidence sur l'autonomie. Même s'ils le savent, ils peuvent être animés de bonnes intentions qui disparaissent rapidement. Ils peuvent commencer la journée en tentant de préserver l'autonomie, mais très rapidement, ils streament des vidéos, ouvrent 30 à 40 onglets dans plusieurs navigateurs, mettent la luminosité de l'écran au maximum et utilisent plusieurs applications dont de nombreux processus sont en cours d'exécution.



Répartition de la consommation énergétique moyenne de Ryzen PRO 15 W Windows étant en état inactif

Figure 6



9 %	Reste du système
12 %	Perte CC-CC
5 %	Alimentation du système
1 %	WLAN/BT WiFi6
2 %	M2.SSD 512GB PCIe Gen3
18 %	Processeur Ryzen PRO 5850U
4 %	Mémoire 2X4 Go de DDR4
49 %	Écran TFT LCD 13”

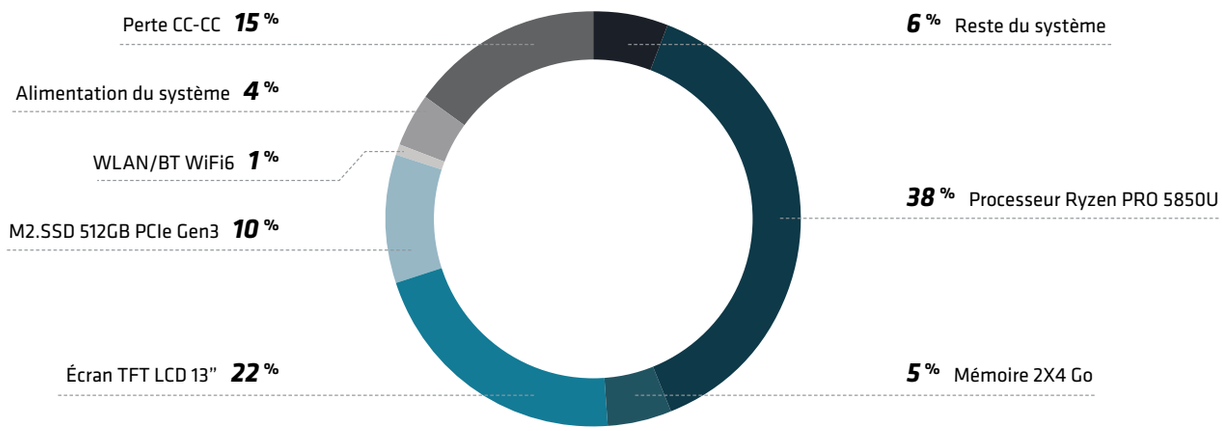
Le scénario utilisateur ci-dessus ne se reflète pas dans le tableau Windows en état inactif ci-dessus. Finalement, peu importe la façon dont un processeur est conçu et optimisé, l'optimisation de l'autonomie n'est pas un hasard – le comportement de l'utilisateur fait toute la différence.

Et nous avons ci-dessous une charge de travail due à une plus grande activité avec la répartition de la consommation énergétique des composants du système. C'est cette charge de travail mixte répondant aux normes de l'industrie utilisée par les plateformes commerciales qui consomme ~2 fois plus d'énergie qu'en état inactif :

- Le processeur consomme presque 4,5 fois
- La puissance d'affichage est en fait un peu plus faible
- La perte CC-CC est le 3e plus gros consommateur d'énergie

Il convient de noter qu'il est impossible d'optimiser la consommation énergétique du système sans se concentrer sur ces trois ou quatre plus gros consommateurs d'énergie.

Ventilation de la consommation énergétique moyenne de la charge de travail mixte répondant aux normes de l'industrie Ryzen PRO 15 W *Figure 7*



Pour résoudre cela, AMD s'est concentrée sur l'ensemble de la plateforme professionnelle lors du développement du processeur Ryzen PRO. Puisque la consommation énergétique du système de plateforme se cumule, non seulement les trois ou quatre plus gros consommateurs, mais chaque composant s'ajoute au total. **Négliger les composants du système consommateurs d'énergie signifie invariablement que ces composants limitent l'étendue de la meilleure autonomie possible.**

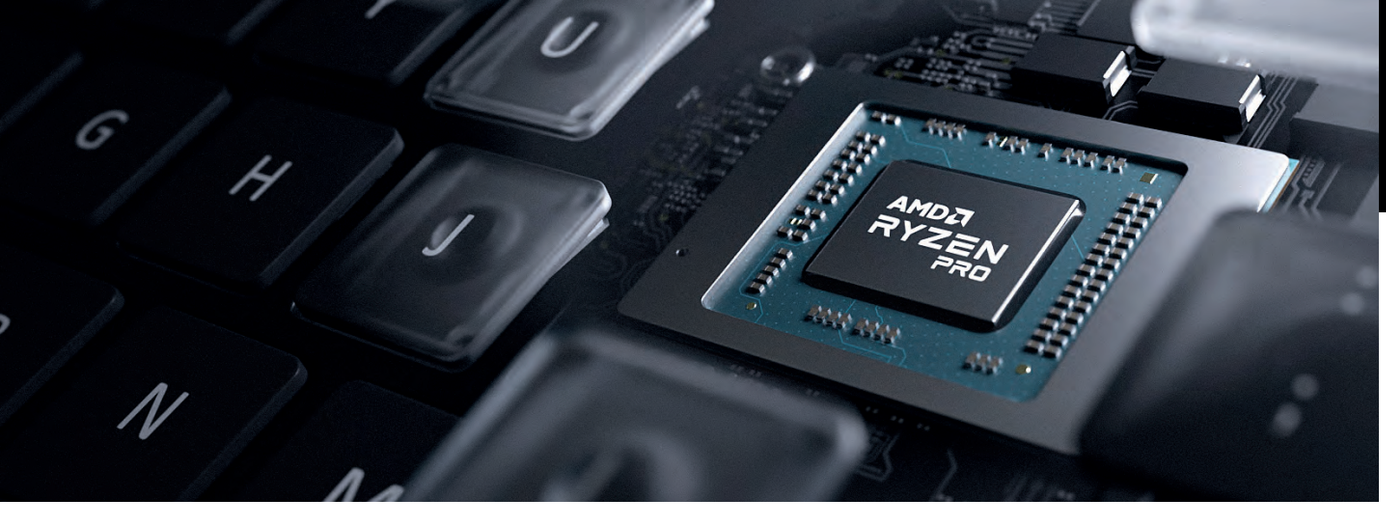
IMPACTS THERMIQUES SUR L'AUTONOMIE

Un autre indice concernant les préférences de l'utilisateur ayant une incidence sur l'autonomie est la solution thermique du PC portable – et plus particulièrement le ventilateur. Même dans le scénario ci-dessus avec une consommation énergétique du système de l'ordre d'environ 3 W, le ventilateur du système devrait être silencieux et éteint. En général, la consommation énergétique du processeur doit être de l'ordre d'environ 3 W juste pour que le ventilateur lui-même commence à tourner, consomme de l'énergie et fasse du bruit.

Donc, si le ventilateur de l'utilisateur fait du bruit, c'est que le PC travaille beaucoup trop pour une expérience optimale en termes d'autonomie. Qu'il y ait 50 onglets de navigateur ouverts ou à peine quelques processus effectuant un travail lourd, la charge de travail est déjà trop élevée pour une expérience utilisateur optimisée au niveau de l'autonomie.

COMPARAISON ET CONTRASTE : AUTONOMIE AVEC L'AMD RYZEN™ PRO 4000 VS. L'AMD RYZEN™ PRO SÉRIE 5000

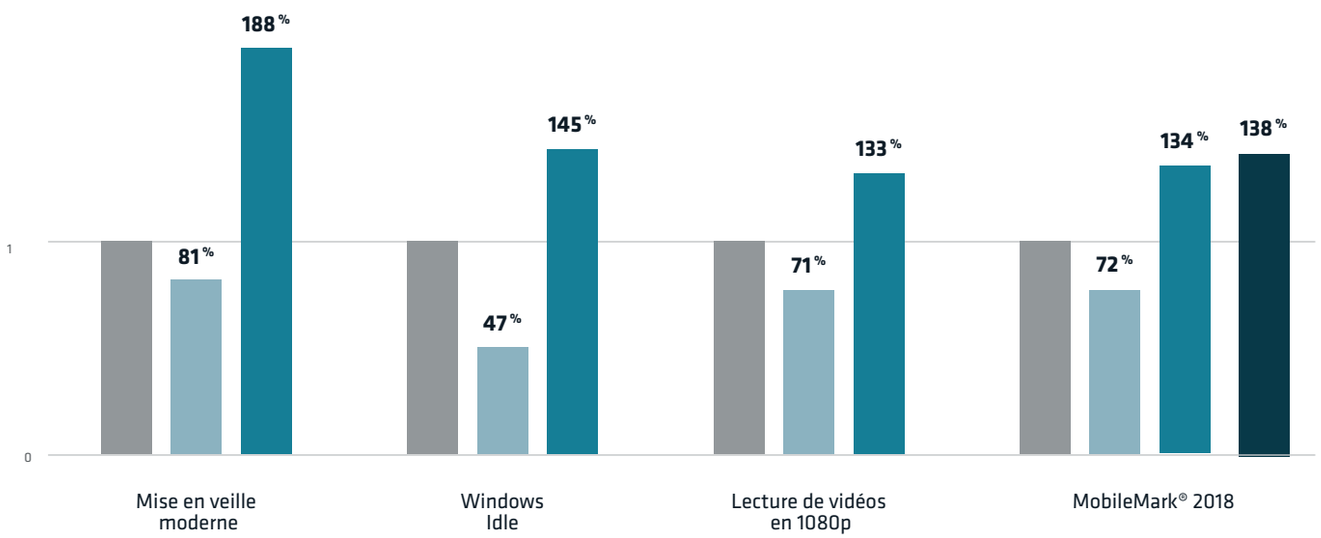
Dans l'analyse finale, c'est vraiment la consommation énergétique totale du système qui est importante pour l'autonomie et pas seulement l'APU – ou plutôt, la consommation énergétique du processeur. La capacité de la batterie est tout aussi importante, et donc plus celle-ci est élevée et mieux c'est.



La ***figure 8*** met en évidence certaines des améliorations de la consommation énergétique du processeur et de l'autonomie du système apportées en passant des processeurs pour PC portable PRO Série 4000 basés sur « Zen 2 » aux tout nouveaux processeurs pour PC portable Ryzen PRO Série 5000 basés sur « Zen 3 ».

Améliorations de la consommation énergétique, de l'autonomie et des performances ***Figure 8***

Des processeurs pour PC portable AMD Ryzen™ PRO Série 4000 aux processeurs pour PC portable AMD Ryzen™ PRO Série 5000



Donc, de quelle manière le Ryzen PRO 5000 « Zen 3 » d'AMD a-t-il amélioré de manière significative la consommation énergétique et les performances par rapport à la génération précédente ?

Voici les faits marquants :

- La gestion de la consommation énergétique sur chip par cœur permet à chaque cœur de fonctionner à une tension et une fréquence optimales, à l'opposé de tous les cœurs reliés ensemble, comme c'était le cas pour le Ryzen PRO Série 4000.
- L'établissement de liaisons CPPC entre le processeur et le système d'exploitation optimise les horloges dans toutes les conditions de fonctionnement, réduit la consommation énergétique du système/maintient des températures inférieures et améliore en même temps les performances, améliorant ainsi les performances par watt.
- L'efficacité CC-CC est améliorée, ce qui fait grandement baisser ce gros consommateur d'énergie du système.
- Les optimisations de la consommation de la mémoire (également appelée État de veille profonde de la mémoire PHY) sur le Ryzen PRO Série 5000 permettent des tensions plus faibles et 20 % d'économie sur la consommation de la mémoire.
- Notre processus de fabrication 7 nm continue à être affiné et optimisé.

Alors que nos processeurs pour PC portable de nouvelle génération sont en cours de développement, nos projections basées sur les premières mesures indiquent encore une autre amélioration importante de la réduction de la consommation énergétique, une amélioration des performances et des gains de performances par watt.

AMD RYZEN PRO

QU'INDIQUENT LES OEM DANS LEURS REVENDICATIONS RELATIVES À L'AUTONOMIE SUR LEURS PLATEFORMES PROFESSIONNELLES ?

Les plateformes professionnelles s'appuient presque exclusivement sur l'indicateur MobileMark® 2018 pour leurs revendications relatives à l'autonomie sur leurs plateformes 2021. Certains peuvent inclure la Mise en veille moderne et pratiquement aucun ne mentionnera les lectures de vidéos, ou même MobileMark® 2014.

Du point de vue de l'autonomie, MobileMark® 2018 indique une autonomie considérablement inférieure à MobileMark® 2014. Même si la plateforme offrira la même autonomie en conditions réelles à un utilisateur, indépendamment de ce qu'une mesure quelconque puisse indiquer, le compte-rendu de MobileMark® 2018 sera bien plus proche de l'expérience d'un utilisateur en conditions réelles.

La meilleure pertinence de MobileMark® 2018 est due à la consommation énergétique supérieure en général, et aux suites Creativity et Web Browsing/Video PlayBack qui s'ajoutent à la suite Office Productivity qui était utilisée exclusivement dans MobileMark® 2014 par les OEM.

Le lien suivant donne le classement en fonction de la meilleure autonomie de batterie des plateformes exécutant MobileMark® 2018 : *https://bapco.com/products/mobilemark-2018/*

REMARQUE IMPORTANTE

Les plateformes de classe professionnelles AMD sont classées aux 3e, 4e, 5e et 6e places. Il convient de noter que les plateformes occupant les 1ère et 2e places présentent une capacité de la batterie bien supérieure à la moyenne. Donc, si elles étaient normalisées en termes de capacité de batterie équivalente, AMD occuperait les neuf premières places. Cela témoigne de l'efficacité énergétique de la plateforme AMD, qui est indépendante de la capacité de la batterie.

CAPACITÉ DE LA BATTERIE

Voici quelques mots rapides sur la capacité réelle de la batterie. D'une manière générale, plus la batterie est grosse, plus sa capacité réelle sera bonne, mais comme mentionné précédemment, une capacité plus importante signifie également un poids plus important.

Et bien qu'il y ait eu de nombreuses améliorations avec les batteries Li-ion de dernière génération, elles n'arrivent toujours pas à atteindre et maintenir cette capacité maximale au fil du temps. Les pertes ici peuvent être importantes, et la plupart des OEM savent que les utilisateurs finaux vont remplacer leur batterie après trois années d'utilisation. Voir les liens dans la section Ressources complémentaires pour en savoir plus.

LE RÉSULTAT FINAL EST LA MEILLEURE EXPÉRIENCE DE SA CATÉGORIE EN TERMES D'AUTONOMIE

Entre un plus grand nombre de charges de travail et les contraintes de fonctionnement en conditions réelles, AMD s'efforce d'offrir la meilleure expérience utilisateur et la meilleure autonomie. Nos plateformes Ryzen PRO Série 5000 maintiennent ce leadership.

Notre approche d'ensemble est axée sur une solution de plateforme optimisée, et non pas simplement sur le silicium AMD seul. Il est nécessaire d'avoir un processeur faible consommateur d'énergie, mais ce n'est pas suffisant. L'autonomie leader du secteur est fragile, comme indiqué précédemment, et tous les composants jouent un rôle dans la consommation énergétique cumulée du système. Par exemple, si l'autonomie d'une plateforme est compromise par un panneau d'affichage gros consommateur d'énergie, aucune « compensation » ne demeure possible dans le reste du système et vous ne pouvez espérer bénéficier de la meilleure expérience de sa catégorie en termes d'autonomie.

Un autre domaine auquel AMD fait particulièrement attention pour ses produits de classe professionnelle est la répartition du processus de fabrication elle-même. AMD limite le nombre de processeurs pour s'assurer que les processeurs professionnels ne présentent pas seulement la consommation énergétique moyenne la plus faible, mais établit également des limites de contrôle statistique du processus (CSP) pour garantir que la variabilité de puissance d'un processeur à l'autre reste aussi faible que possible.

Cette approche de solutions de systèmes multicouche visant à optimiser l'équilibre entre performances et consommation énergétique, offre aux utilisateurs une autonomie de pointe dans le secteur informatique et une expérience encore meilleure. Il s'agit d'une question compliquée avec une solution simple : AMD a compris comment offrir à chaque fois la meilleure expérience.

RESSOURCES COMPLÉMENTAIRES

[1]https://bapco.com/products/mobilemark-2018/

[2]https://results.bapco.com/results/benchmark/MobileMark_2018

[3]https://bapco.com/news/bapco-technical-paper-battery-degradation-in-notebook-computers/#

REMARQUES

« Zen » et « Zen 3 » sont des noms de code d'architecture AMD, et ne sont pas des noms de produit. GD-122

Les informations contenues dans ce document ne sont fournies qu'à titre indicatif, et sont sujettes à modification sans préavis. Toutes les précautions ont été prises dans la préparation de ce document, cependant, il peut contenir des inexactitudes techniques, des omissions et des erreurs typographiques. AMD n'a aucune obligation de mettre à jour ou de corriger ces informations. En outre, les PRODUITS AMD peuvent contenir des défauts ou des erreurs désignés par le terme « errata », qui peuvent faire dévier le processeur des spécifications publiées. AMD identifiera parfois ces errata sans préavis, mais n'a aucune obligation de le faire. Advanced Micro Devices, Inc. ne fait aucune déclaration ni ne donne aucune garantie eu égard de l'exactitude ou l'exhaustivité des informations contenues dans ce document. Elle décline toute responsabilité de quelque nature que ce soit, y compris les garanties implicites de non-violation, de qualité marchande ou d'adéquation à un usage particulier, eu égard au fonctionnement ou à l'utilisation du matériel, des logiciels ou des autres produits AMD décrits ici. Aucune licence, notamment implicite ou découlant d'une question déjà tranchée, n'est cédée par le présent document pour quelque droit de propriété intellectuelle que ce soit. Les conditions et limitations applicables à l'achat ou l'utilisation de produits AMD sont énoncées dans un accord signé entre les parties, ou dans les conditions générales de vente d'AMD. GD-140

Toutes les déclarations relatives à l'autonomie sont approximatives. Les performances réelles en matière d'autonomie peuvent varier selon plusieurs facteurs, y compris mais sans s'y limiter : la configuration et l'utilisation du produit, les conditions de fonctionnement des logiciels, les fonctionnalités à distance, les paramètres de gestion de la consommation d'énergie, la luminosité de l'écran et d'autres facteurs. La capacité maximale de la batterie diminue naturellement avec le temps et l'utilisation. Pour obtenir plus d'informations sur le test du benchmark MobileMark 18, consultez le site *www.bapco.com*. GD-168

PROCESSEURS POUR PC PORTABLES AMD RYZEN™ SÉRIE 5000 DES DÉFENSES QUI COMPTENT : UNE CONCEPTION QUI VA PLUS LOIN

Par : Akash Malhotra
Groupe Sécurité des produits et stratégie

Dans le contexte d'augmentation des risques en termes de volume comme de nombre, AMD continue de penser qu'une protection judicieuse des ordinateurs modernes exige une approche à plusieurs niveaux, élaborée consciencieusement en s'appuyant sur les meilleurs contrôles de sécurité existants, ainsi que sur des fonctionnalités directement intégrées aux matériels, logiciels et micrologiciels. C'est d'autant plus vrai qu'une mobilité accrue représente la nouvelle norme.

AMD collabore étroitement avec les sociétés éditrices des différents systèmes d'exploitation (OS) et les fabricants d'équipement d'origine (OEM) pour proposer des fonctionnalités de sécurité qui complètent et renforcent leur propres concepts de sécurité.

Ce document souligne les fonctionnalités de sécurité des processeurs pour PC portables AMD Ryzen™ PRO Série 5000 et leur rôle au sein d'une approche de la sécurité des appareils à plusieurs niveaux.

TOUT EST CONSTRUIT EN PENSANT À LA SÉCURITÉ

Les architectures de cœurs AMD reposant sur « Zen » proposent de solides bases de sécurité. L'architecture de sécurité AMD permet de réduire l'exposition aux attaques, peut réduire les temps d'arrêt, nécessiter moins de correctifs et aider à améliorer le coût total de possession.

UNE RACINE DE CONFIANCE MATÉRIELLE INTÉGRÉE

AMD continue d'améliorer son architecture de puce à chaque génération, pour renforcer son efficacité contre les futures cyberattaques.

FONCTIONS DE SÉCURITÉ INTÉGRÉES, DU MICROLOGICIEL AU SYSTÈME D'EXPLOITATION

Après une authentification initiale du micrologiciel et du BIOS de l'OEM, le contrôle vérifie le système d'exploitation via un processus d'amorce sécurisé qui suit la chaîne de confiance, à l'aide de la racine de confiance ancrée dans le matériel.

UNE MEILLEURE PROTECTION DE LA MÉMOIRE : AMD MEMORY GUARD

Les processeurs pour PC portables AMD Ryzen™ PRO sont les premiers processeurs commerciaux du marché à offrir une technologie qui aide à protéger les données des utilisateurs en chiffrant le contenu complet de la mémoire système en standard.

L'ARCHITECTURE DE SÉCURITÉ DES PROCESSEURS POUR PC PORTABLES AMD RYZEN™ PRO SÉRIE 5000

Nous allons désormais aborder certaines fonctionnalités essentielles présentes au niveau même des processeurs pour PC portables AMD Ryzen™ PRO Série 5000, sur ce qu'elles apportent, et surtout, l'expérience de l'utilisateur final.

PROCESSEUR SÉCURISÉ AMD (ASP)

Le processeur sécurisé AMD est un matériel dédié disposé dans chaque système sur puce (SoC), conçu pour ancrer une racine de confiance matérielle. Il permet également d'amorcer et d'initialiser le SoC grâce au flux d'amorçage sécurisé et d'établir un environnement d'exécution de confiance isolé. Même s'il se trouve au niveau de la puce, il est considéré comme étant isolé, car le SoC hôte ne peut pas accéder à sa mémoire. L'ASP est une pièce maîtresse de la sécurité de la plateforme, et comprend les composants suivants :

Le coprocesseur cryptographique (CCP) : Un bloc cryptographique dédié qui assure une fonctionnalité cryptographique de génération et de gestion de clés. Étant donné que les opérations cryptographiques sont mises en œuvre au niveau du matériel, ce qui leur donne un avantage en termes de performance qui est essentiel lors des opérations où le temps est critique.

Boot ROM : Une mémoire en lecture seule qui contient le micrologiciel de ROM pour le démarrage sur la puce.

Static Random-Access Memory (SRAM) : Mémoire RAM avec prise en charge d'un mode d'alimentation en sommeil profond

Memory Management Unit (MMU) : L'unité MMU de l'ASP gère l'accès en vue du démarrage des mémoires ROM et SRAM

AMD PLATFORM SECURE BOOT (PSB)

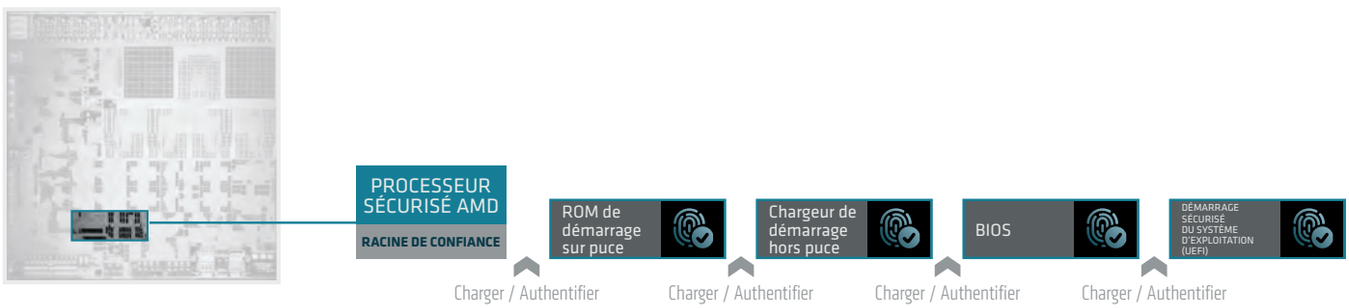
Le démarrage sécurisé de plateforme (PSB) d'AMD fournit une racine de confiance (RoT) matérielle afin d'authentifier le micrologiciel initial du BIOS lors du processus de démarrage de l'appareil. Lors de la mise en tension d'un système, le processeur sécurisé ASP exécute le code ROM de démarrage de l'ASP, qui à son tour authentifie plusieurs codes de chargement de démarrage d'ASP, avant d'initialiser la puce et la mémoire système.

Une fois que la mémoire système est initialisée, le programme de démarrage d'ASP vérifie le code du BIOS OEM, et authentifie d'autres composants micrologiciels avant de démarrer le système d'exploitation.

PSB assure l'intégrité de la plateforme en fournissant une protection supérieure contre les micrologiciels intempestifs ou malveillants, en leur interdisant automatiquement l'accès dès leur détection. AMD PSB aide à offrir une transition fluide et sécurisée du micrologiciel d'origine jusqu'au système d'exploitation.

Démarrage sécurisé de plateforme AMD

Figure 1



AMD MEMORY GUARD

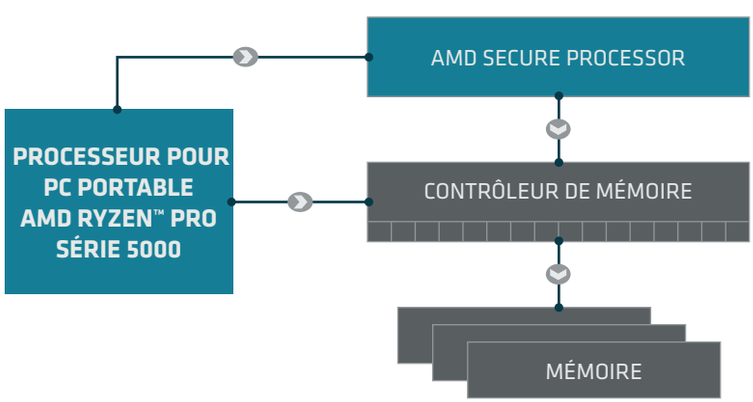
AMD Memory Guard est une technologie de cryptage de la mémoire entière, et représente une solution de sécurité simple et robuste pour participer à la protection des données des clients, notamment en cas de risque d'attaques contre le système. Avec AMD Memory Guard, tout le contenu de la mémoire DRAM est crypté à l'aide d'une clé aléatoire pour assurer une protection contre les attaques par démarrage à froid, l'espionnage d'interface DRAM et autres types d'attaques similaires.

Pour les systèmes avec NVDIMM, AMD Memory Guard aide aussi à se protéger contre les attaques consistant à retirer un module de mémoire et à tenter d'en récupérer le contenu. Il est mis en œuvre par un matériel dédié dans les contrôleurs de mémoire sur puce.

- Chaque contrôleur comprend un moteur de standard de cryptage avancé (Advanced Encryption Standard, AES) hautes performances, qui crypte les données lors de leur écriture dans la DRAM, pour les décrypter à la lecture.
- Une clé 128 bits est produite par un générateur matériel de nombres aléatoires conforme à la norme NIST SP 800-90 dans un mode qui utilise un réglage à base d'adresse physique supplémentaire pour mieux se protéger contre les attaques par déplacement de blocs de cryptogrammes.
- La clé de cryptage utilisée par le moteur AES doté d'AMD Memory Guard est générée de manière aléatoire à chaque réinitialisation du système, et elle est invisible pour tous les logiciels exécutés sur les cœurs CPU. Cette clé est entièrement gérée par le processeur sécurisé AMD (ASP).

AMD Memory Guard

Figure 2



AMD RYZEN PRO

AMD SHADOW STACK

Les attaquants cherchent en permanence de nouvelles manières de s'introduire dans des systèmes en retardant davantage leur détection, et le recours au Return-on-progamming (ROP) devient de plus en plus populaire. Le ROP fait partie des attaques logicielles sophistiquées où l'attaquant ne cherche pas à injecter un code malveillant dans un processus, mais plutôt à contrôler un système en exploitant une vulnérabilité du code légitime.

COMMENT CELA FONCTIONNE-T-IL ?

En programmation informatique, une « routine » consiste à réaliser une série spécifique d'opérations. Lorsqu'un programme logiciel s'exécute, il appelle une routine. Une fois sa tâche accomplie, la routine retourne au programme principal à l'aide de l'adresse de retour. Ce processus comprend un saut (jump) et un retour (return)

Dans les attaques de ROP, les agresseurs modifient l'adresse de retour après le saut de routine. Au lieu de retourner au programme principal, elle passe à d'autres routines, et assemble des codes secondaires de routines en vue de créer un code malveillant susceptible de nuire au système. Et surtout, ce type d'attaques échappe aux détections, car il semble utiliser un code légitime.

Les processeurs pour PC portables AMD Ryzen™ PRO Série 5000 aident à atténuer les attaques de ROP en donnant un accès logiciel à certains registres du CPU où une copie de l'adresse de retour peut être stockée.

Les applications utilisent une pile parallèle, appelée pile cachée ou « shadow stack » pour empêcher les attaques logicielles qui tentent de modifier le flux de contrôle. Au moyen d'un matériel spécifique, la pile cachée est utilisée pour stocker une copie des adresses de retour, qui sont ensuite comparées aux opérations de retour de la pile de programmation normale.

Si le contenu diffère, une exception est générée pour empêcher au code malveillant d'accéder au contrôle du système. Ainsi, le matériel de pile cachée peut aider à atténuer les types de dysfonctionnements logiciels les plus courants et les plus exploitables.

La pile cachée AMD Shadow Stack est un renfort supplémentaire face aux attaques de type ROP ; comme une copie de l'adresse de retour se trouve dans le matériel, un code malveillant aura énormément de mal à la modifier.

La protection de pile matérielle Microsoft, intitulée Microsoft Hardware Enforced Stack Protection, est prise en charge par les processeurs pour PC portables AMD Ryzen™ PRO Série 5000 grâce à AMD Shadow Stack.

MICROSOFT SECURED-CORE PC

Le PC avec cœur sécurisé par Microsoft protège votre PC contre les vulnérabilités des micrologiciels, les attaques contre les systèmes d'exploitation et les accès non autorisés aux appareils et données, au moyen de contrôles d'accès et de systèmes d'authentification avancés.

Secured-Core PC est activé sur les plateformes AMD à l'aide de divers services et technologies de sécurité :

- AMD-V™ avec GMET
- AMD Secure Init and Jump with Attestation (SKINIT)
- AMD Secure Loader (SL)
- AMD Dynamic Root of Trust Measurement (DRTM)
- AMD System Management Mode (SMM) Supervisor
- Direct Memory Access (DMA) Protection

AMD-V AVEC GMET

AMD-V est un ensemble d'extensions matérielles qui permettent la virtualisation sur les plateformes AMD. Guest Mode Execute Trap (GMET) est une fonctionnalité d'accélération de performance sur la puce, qui permet à l'hyperviseur de gérer efficacement des contrôles d'intégrité de code et ainsi de se protéger des logiciels malveillants.

SECURE INIT AND JUMP WITH ATTESTATION (SKINIT)

L'instruction d'initialisation et de saut sécurisés avec attestation (SKINIT) permet de créer une « racine de confiance » commençant par un mode opérationnel initialement non sécurisé SKINIT réinitialise le processeur pour établir un environnement d'exécution de confiance destiné à un composant logiciel de chargement sécurisé (Secure Loader, SL), et démarre l'exécution du SL pour éviter toute altération. SKINIT étend la racine de confiance matérielle jusqu'au SL.

AMD SECURE LOADER (SL)

Le chargeur sécurisé (SL) AMD est chargé de valider la configuration de la plateforme en interrogeant le matériel et en demandant des informations de configuration au service DTRM fourni par le processeur sécurisé AMD (ASP)

AMD DYNAMIC ROOT OF TRUST MEASUREMENT (AMD DRTM)

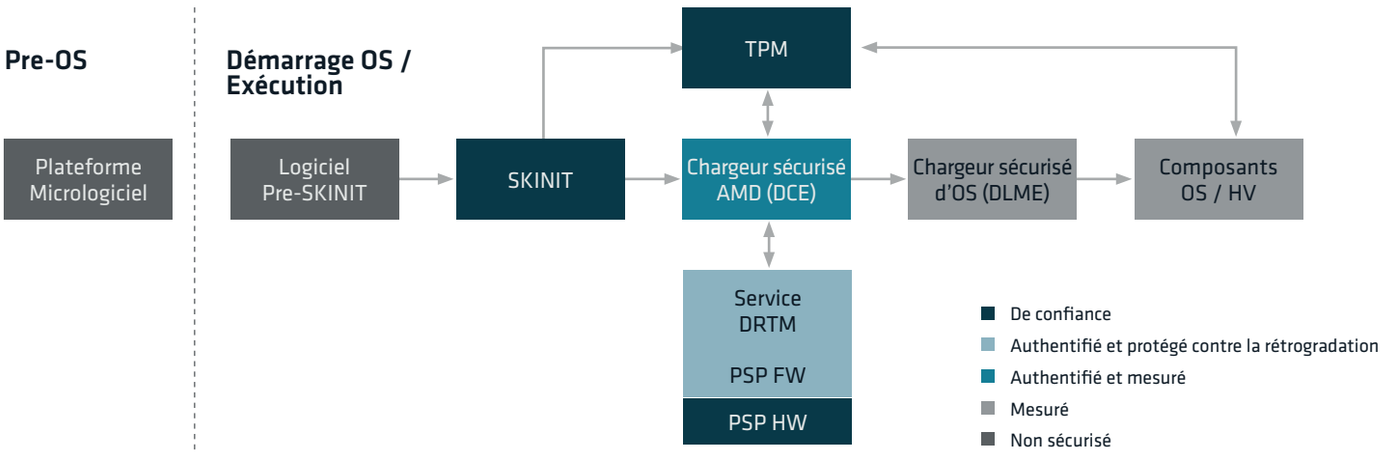
Le bloc AMD DRTM se compose de l'instruction SKINIT du CPU, de l'ASP, et du SL. Ce bloc est chargé de créer et de préserver un chaîne de confiance entre les micrologiciels. La mesure de racine de confiance dynamique AMD DRTM laisse le micrologiciel et le chargeur de démarrage se charger librement, car ce sont des codes sans protection, mais juste après leur lancement, le système adoptera un état de confiance basé sur le matériel, et ce denier renverra le micrologiciel sur un trajet de code mesuré et bien connu.

Le bloc DRTM mesure et authentifie le chargeur de démarrage, et collecte et enregistre aussi de manière protégée les informations système suivantes, qui serviront plus tard au système d'exploitation, notamment à des fins de vérification et d'attestation.

- Carte de mémoire physique
- Emplacement d'espace de configuration PCI
- Configuration locale APIC
- Configuration E/S APIC
- Configuration IOMMU / Configuration TMR
- Configuration de la gestion de la consommation énergétique

Flux DRTM

Figure 3



À tout moment après le démarrage de l'OS par le système, le système d'exploitation peut demander au bloc de service AMD de re-mesurer et attester les valeurs avant de procéder à d'autres opérations. Le système d'exploitation est donc en mesure de protéger le système, du démarrage à l'exécution.

CONFIANCE MATÉRIELLE PARTAGÉE

Cela signifie que le composant micrologiciel est authentifié et mesuré par le bloc ASP au niveau de la puce AMD, puis la mesure est sauvegardée et protégée en vue d'une utilisation par l'OS, notamment à des fins de vérification et d'authentification.

SUPERVISEUR AMD SMM

Le mode de gestion de système (SMM) est un mode CPU spécifique pour micro-contrôleurs x86, qui permet de gérer la gestion de la consommation énergétique, la configuration matérielle, la surveillance thermique et tous les éléments jugés utiles par le fabricant du matériel.

À chaque demande d'exécution d'une de ces opérations système, une interruption (SMI) est invoquée lors de l'exécution, et le code SMM installé par le BIOS s'exécute. Le code SMM s'exécute avec le niveau de priorité le plus élevé, sans être visible par l'OS, car c'est une cible idéale des activités malveillantes qui pourraient l'utiliser pour accéder à la mémoire de l'hyperviseur afin d'en modifier le contenu.

Le gestionnaire SMI est habituellement fourni par un autre éditeur que celui du système d'exploitation, et il a accès à la mémoire et aux ressources de l'OS / hyperviseur. Cela signifie que des vulnérabilités dans le code SMM peuvent conduire à des failles de l'OS Windows / de l'hyperviseur et de la sécurité à base de virtualisation (VBS).

Pour mieux isoler le SMM, AMD propose un module de sécurité intitulé AMD SMM Supervisor, qui s'exécute immédiatement avant le transfert du contrôle au gestionnaire SMI, suite à une interruption SMI. Le superviseur AMD SMM se trouve dans le bloc de service AMD DRTM, et il sert à :

- interdire au SMM de modifier l'hyperviseur ou la mémoire de l'OS, sauf pour un petit tampon de communication entre ceux-ci
- empêcher le SMM d'introduire un nouveau code SMM lors de l'exécution
- empêcher le SMM d'accéder au DMA, aux E/S ou aux registres capables de compromettre l'hyperviseur ou l'OS.

PROTECTION DE DMA

Les plateformes AMD prennent en charge la protection de DMA (accès direct mémoire) dans les environnements de pré-démarrage et d'OS via les technologies sécurisées AMD telles que Input Output Memory Management Unit (IOMMU) avec la technologie de remappage de DMA.

- La protection de DMA permet d'éviter les éventuelles attaques ciblant le micrologiciel de la plateforme, lorsque des agresseurs utilisent des appareils connectés pour viser un accès direct à la mémoire.
- DMA offre un accès direct à l'espace d'adresse de mémoire physique des appareils, pour en améliorer les performances. Mais cela simplifie aussi l'accès à ceux qui souhaiteraient injecter des logiciels malveillants dans le système, sans que l'OS ne parvienne à le détecter.

Pour éviter de telles attaques, AMD a conçu une architecture de sécurité destinée à gérer et contrôler l'accès DMA de l'appareil, via une unité de gestion de mémoire d'entrée-sortie (Input Output Memory Management Unit, IOMMU), au stade du micrologiciel avant l'OS.

L'architecture de sécurité DMA transfère la responsabilité des paramètres de protection de la mémoire système, du niveau du micrologiciel à celui de l'OS, une fois que le chargeur de démarrage de l'OS a été établi en mémoire. La protection DMA à l'aide de l'IOMMU s'applique à chaque démarrage, jusqu'à ce que le système d'exploitation assume lui-même le contrôle de l'IOMMU.

AMD RYZEN PRO

MISE À JOUR DE LA PLATEFORME

Les processeurs pour PC portables AMD Ryzen™ PRO Série 5000 comportent des défenses de sécurité améliorées contre les agresseurs cherchant à accéder au système en temps réel, mais ils offrent également un mécanisme robuste de mise à jour. Cela permet aux organisations de mettre à jour leurs plateformes de manière fluide, et de rectifier les vulnérabilités créées par des bugs matériels ou logiciels.

AMD collabore étroitement avec les OEM pour fournir une architecture de mise à jour de la plateforme sécurisée, qui repose sur l'intégrité et la conformité aux meilleures pratiques et orientations de l'industrie, et qui est intégrée à la solution de mise à jour de la plateforme OEM. Les processeurs pour PC portables AMD Ryzen™ PRO Série 5000 sont dotés de la fonctionnalité « Firmware Anti-Rollback (FAR) » qui permet à une politique basée sur le matériel d'interdire de rétrograder le micrologiciel AMD ASP.

Les processeurs pour PC portables AMD Ryzen™ Série 5000 contiennent également une architecture de récupération sécurisée, « A/B Recovery » qui peut s'intégrer à une solution OEM afin de permettre la récupération en cas de panne grave.

CRYPTO ACCELERATOR

Les opérations cryptographiques sont désormais importantes dans le cadre de la protection des données et des communications. Ces opérations cryptographiques sont importantes, mais elles exigent par ailleurs énormément de ressources de calcul. Pour contribuer à la réduction des coûts liés aux calculs d'algorithmes cryptographiques, AMD propose de fournir de nouvelles instructions optimisées, au niveau de la puce.

L'architecture « Zen 3 » prend désormais en charge le cryptage AES vectorisé 256 bits (vAES256) qui peut servir aux applications et charges de travail complexes afin d'en tirer tous les avantages.

RÉCAPITULATIF

AMD estime que les solutions de sécurité modernes peuvent être réalisées grâce à des défenses en couches. La combinaison des fonctionnalités de sécurité matérielles et des protections logicielles associées facilite une protection contre les cyber-attaques présentes et futures, y compris les agressions sophistiquées contre les micrologiciels de niveau inférieur. Avec chaque génération de cœurs et de produits, AMD continue à innover et repousse les limites de la sécurité du matériel, tout en proposant des solutions de sécurité complètes à ses clients.

Fonctionnalités de sécurité et avantages AMD PRO *Figure 4*

FONCTIONNALITÉ DE SÉCURITÉ	AVANTAGE	SÉCURITÉ AMD PRO
Cryptage de la mémoire	Crypte la mémoire pour empêcher tout pirate de lire les données sensibles stockées dans la mémoire. Permet d'atténuer les attaques par démarrage à froid.	AMD Memory Guard
Démarrage sécurisé	Protection au démarrage qui permet d'empêcher les logiciels non autorisés et les logiciels malveillants de prendre le contrôle des fonctions essentielles du système.	Démarrage sécurisé de plateforme AMD
Sécurité Windows 10	Fonctionnalité de sécurité Microsoft pour aider à atténuer les menaces.	Pris en charge
Sécurité basée sur la virtualisation	Utilise les fonctions de virtualisation matérielle afin de créer et d'isoler une zone sécurisée de la mémoire du système d'exploitation normal.	AMD-V
TPM micrologiciel	Une version « micrologiciel » à la place du matériel réel qui fournit l'authenticité à la plateforme et permet de garantir qu'il n'y a aucun signe de failles de sécurité.	AMD Firmware TPM
Générateur de nombres aléatoires	Un générateur de nombres aléatoires basé sur le matériel destiné aux protocoles cryptographiques. Fournit des capacités cryptographiques.	AMD RDRAND
AES-NI	Permet d'accélérer les protocoles de cryptage et de protéger le trafic réseau (contenu Internet et courrier électronique) et les données personnelles.	AMD AES

Fonctionnalités de sécurité et avantages AMD PRO (suite)

FONCTIONNALITÉ DE SÉCURITÉ	AVANTAGE	SÉCURITÉ AMD PRO
Microsoft Secured-Core PC	Vous permet de démarrer en toute sécurité ; protège votre PC contre les vulnérabilités des micrologiciels, les agressions des systèmes d'exploitation et les accès non autorisés aux appareils et données, au moyen de contrôles d'accès et de systèmes d'authentification avancés.	Compatible Secured-Core PC
Protection contre les attaques du flux de contrôle	Assure une protection renforcée contre les attaques du flux de contrôle en vérifiant la pile de programmes normale par rapport à une copie stockée sur le matériel et en activant Microsoft Hardware Enforced Stack Protection dans le cadre d'une série complète de fonctions de sécurité AMD permettant de sécuriser les PC.	AMD Shadow Stack
Guest Mode Execute Trap	Fonctionnalité d'accélération de performance sur la puce, qui permet à l'hyperviseur de gérer efficacement des contrôles d'intégrité de code et de se protéger contre les logiciels malveillants.	AMD GMET
Superviseur du mode de gestion système	Module de sécurité qui permet d'isoler le mode de gestion système	Superviseur SMM
Initialisation et saut sécurisé avec attestation	Une instruction qui permet de créer une « racine de confiance » en démarrant dans un mode opérationnel initialement non sécurisé	AMD SKINIT
Protection contre les attaques par accès direct à la mémoire	Protège le système contre les tentatives d'injections de logiciels malveillants par le biais d'appareils disposant d'un accès direct à la mémoire, et susceptibles de ne pas être détectés par l'OS.	Protection de DMA
Mesure dynamique du temps d'exécution	Participe à l'intégrité de la plateforme en faisant passer le micrologiciel de niveau inférieur d'un état non sécurisé à un état de confiance.	AMD DRTM

CLAUSE DE NON-RESPONSABILITÉ

« Zen » est le nom de code de l'architecture AMD et n'est pas un nom de produit. GD-122

Les informations contenues dans ce document ne sont fournies qu'à titre indicatif, et sont sujettes à modification sans préavis. Toutes les précautions ont été prises dans la préparation de ce document, cependant, il peut contenir des inexactitudes techniques, des omissions et des erreurs typographiques. AMD n'a aucune obligation de mettre à jour ou de corriger ces informations. Advanced Micro Devices, Inc. n'émet aucune représentation ni garantie concernant l'exactitude ou le caractère complet du contenu de ce document, et n'assume aucune responsabilité de quelque nature que ce soit, notamment les garanties implicites de non-violation, qualité marchande ou adaptation pour des objectifs particuliers lors de l'utilisation ou fonctionnement de matériels, logiciels ou autres produits AMD présentés ici. Aucune licence, notamment implicite ou découlant d'une question déjà tranchée, n'est cédée par le présent document pour quelque droit de propriété intellectuelle que ce soit. Les conditions et limitations applicables à l'achat ou l'utilisation de produits AMD sont définies dans un accord signé entre les parties, ou dans les conditions générales de vente d'AMD. GD-18