Outils pour l'informatique confidentielle

Posted on **24/07/2023** by **Fabien A. P. Petitcolas**

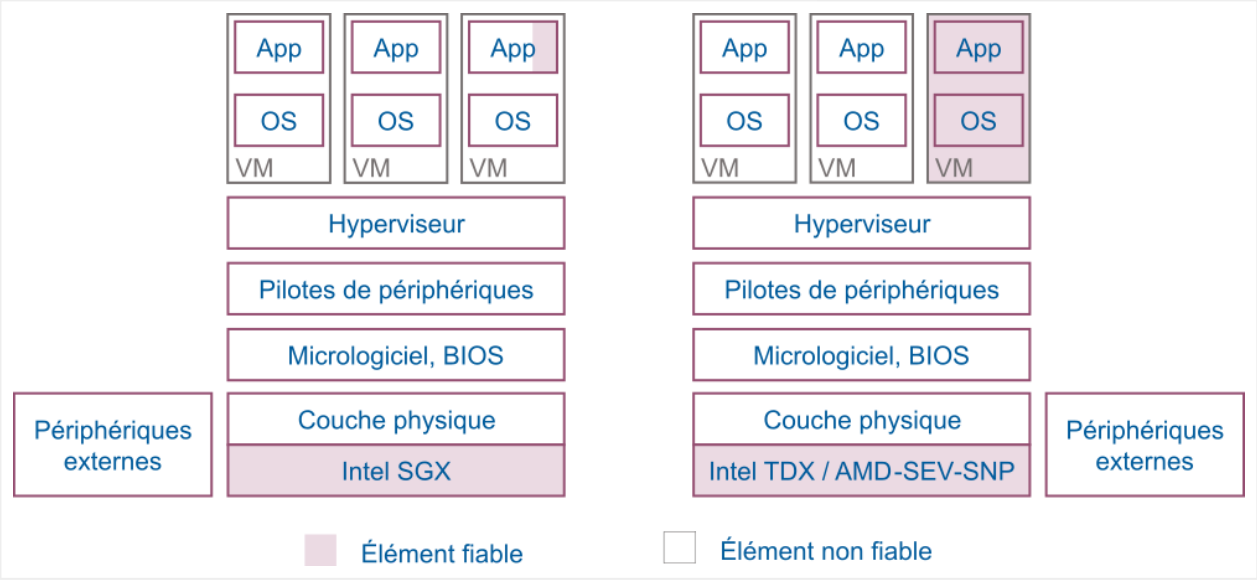
Pour répondre à la demande de leurs clients traitant des données sensibles ou attirer de nouveaux clients, les fournisseurs d'infrastructures informatiques publiques mettent d'importants moyens en œuvre afin d'améliorer leur sécurité et notamment de mieux protéger les données de leurs clients. Microsoft, par exemple, déclare investir environ un milliard de dollars chaque année dans la sécurité de ses infrastructures [1]. Depuis le milieu des années 2010, ces fournisseurs d'infrastructures investissent notamment dans une offre d'informatique confidentielle. Principalement basée sur des environnements d'exécution de confiance (« *Trusted Execution Environments (TEE)* »), celle-ci permet en principe de réduire la confiance accordée par le client au fournisseur d'infrastructure.

Dans un article précédent, nous avons présenté de manière générale ce qu'étaient ces TEE et leur utilité. Dans cet article nous regardons plus en détail le fonctionnement des principales mises en œuvre commerciales. Cependant, il convient de garder à l'esprit que les définitions d'informatique confidentielle et de TEE diffèrent et sont parfois incomplètes. Cela peut conduire à un faux sens de sécurité, à des incertitudes légales et à rendre les comparaisons difficiles [2]. Afin de répondre à ce manque de standardisation et d'interopérabilité entre les différentes approches d'informatique confidentielle, le « *Confidential Computing Consortium* » a été créé par des acteurs importants du secteur, dont AMD, Google, Intel, et Microsoft. Il est à noter qu'Amazon ne fait pas partie de ce regroupement et que son système Nitro (voir ici) est très différent des autres approches[1].

Une version plus approfondie de cet article, réservée aux clients de Smals, est disponible sur demande.

Fabricants de microprocesseurs

AMD et Intel sont les deux principaux fabricants de microprocesseurs offrant des fonctionnalités nécessaires à l'informatique confidentielle dans de larges centres informatiques[2]. Alors que les technologies TDX d'Intel et SEV-SNP d'AMD ont pour but de protéger des machines virtuelles (VM) entières, la technologie SGX est très différente et sa surface d'attaque plus faible. La Figure 1 montre les éléments faisant partie de la base informatique de confiance (« *Trusted Computing Base (TCB)* ») pour ces trois technologies que nous décrivons dans les paragraphes suivants.



— Figure 1 – La technologie SGX d'Intel permet d'isoler un processus, tandis que les technologies TDX d'Intel et SEV-SNP d'AMD permettent l'isolation de machines virtuelles entières.

Technologie SEV-SNP d'AMD

En 2016, AMD a introduit la technologie de virtualisation sécurisée par chiffrement (« *Secure Encrypted Virtualisation (SEV)* ») afin d'isoler les VM de l'hyperviseur au niveau matériel [3], [4]. Chaque VM reçoit sa propre clé de chiffrement AES pour le chiffrement de la mémoire. L'état des registres du microprocesseur de chaque VM est également chiffré, empêchant l'hyperviseur de lire les données contenues dans la VM. Par la suite, AMD a ajouté une technologie de pagination imbriquée sécurisée (« *Secure Nested Paging (SNP)* ») offrant une protection de l'intégrité de la mémoire, et permettant d'empêcher les attaques d'un hyperviseur malicieux (par ex. attaques par rejeu, reconfiguration du mécanisme de traduction de mémoire virtuelle, corruption des données mémoires) [5]. Le principe fondamental de SEV-SNP est que si une VM est en mesure de lire une page mémoire lui étant réservée (et donc chiffrée), alors elle doit toujours lire la dernière valeur qu'elle a elle-même écrite. Par ailleurs dans le modèle de sécurité utilisé pour SNP, seule la VM du client et le microprocesseur AMD font partie de la base de confiance. N'en font donc pas partie l'hyperviseur, le BIOS, les autres VM, etc. (voir Figure 1). Enfin, une option de SEV-SNP permet aux VM de diviser, d'une manière similaire aux anneaux de protection dans l'architecture x86, leur mémoire virtuelle en quatre niveaux de privilèges (« *Virtual Machine Privilege Levels (VMPL)* »).

Le mécanisme d'attestation à distance d'AMD, permet de vérifier que la machine hôte est bien un processeur AMD qui prend en charge la technologie SEV-SNP et qu'une VM a bien été déployée avec la protection SEV-SNP. Chaque processeur AMD, contient un coprocesseur sécurisé qui permet de générer une paire de clés dédiées (« *Platform Endorsement Key (PEK)* »), elle-même signée par une clé unique dérivée de secrets enregistrés grâce à des fusibles dans la puce elle-même. Cette PEK est également indirectement utilisée pour établir un secret partagé entre la plate-forme SEV et le client [6]. Au moment du lancement de la VM sécurisée sur la plate-forme SEV par l'hyperviseur, le micrologiciel (« *firmware* ») SEV calcule la mesure (valeur du hachage cryptographique) de la mémoire de la VM. Cette mesure peut être communiquée de manière sécurisée au client afin qu'il vérifie que la VM déployée n'a pas été altérée.

La technologie SEV-SNP est disponible sur les processeurs AMD EPYC de 3^{e} génération (série 7003) et 4^{e} génération (série 9004). On peut trouver ces processeurs chez différents fournisseurs comme Dell (serveurs « PowerEdge »), Lenovo ou HP. Les prix varient de quelques milliers à plusieurs dizaines de milliers d'euros en fonction de la configuration.

Technologies SGX et TDX d'Intel

Introduit en 2015, le système « *Software Guard eXtensions (SGX)* » d'Intel permet à un logiciel de définir des zones de mémoire protégées pour des « enclaves » sécurisées isolées des autres processus fonctionnant sur la même machine (noyaux du système d'exploitation, hyperviseur, etc.) ainsi que des accès directs par des périphériques. Le processeur s'assure que chaque enclave a sa zone mémoire dédiée et chiffrée, enregistrant chaque allocation par le système d'exploitation [7]. Une enclave est générée en tant que bibliothèque partagée dynamiquement à l'aide d'outils de compilation standards. Lors de l'initialisation d'une enclave, le système d'exploitation demande au processeur de copier l'application dans des pages mémoire de la zone protégée chiffrée. Lors de ce chargement en mémoire, le processeur calcule une mesure de l'application. Cela permet par la suite de vérifier l'intégrité de l'application par un mécanisme d'attestation. Intel a introduit en 2020, la technologie « *Trusted Domain Extensions (TDX)*, » qui est un module logiciel signé, exécuté dans un nouveau mode du processeur et qui permet de protéger et d'isoler cryptographiquement des machines virtuelles. Plus de détails sur le fonctionnement et l'architecture de TDX peuvent être trouvés dans [8].

Deux types d'attestation à distance sont disponibles avec SGX « *Enhanced Privacy ID (EPID)* » et « *Data Centre Attestation Primitives (DCAP)*. » Le premier est un mode d'attestation dans lequel le serveur d'attestation d'Intel doit être contacté pour obtenir des informations sur l'enclave requérante. Le second ne nécessite pas de contacter le serveur d'attestation d'Intel. Durant le processus de construction d'une enclave, deux mesures sont faites. `MRENCLAVE` est la valeur de hachage cryptographique de la disposition de la mémoire virtuelle assignée à l'enclave au moment de son lancement. L'autre mesure, `MRSIGNER`, est la valeur de hachage cryptographique de la clé publique de l'auteur de l'application fonctionnant dans l'enclave [9].

Alors que la technologie SGX a été retirée de la 12^{e} génération des processeurs Core d'Intel, elle reste disponible sur la 3^{e} génération de processeurs Xeon [10]. Les processeurs Xeon de 4^{e} génération prennent en charge la technologie TDX et sont disponibles chez les partenaires et distributeurs agréés d'Intel.

Notons que l'utilisation de la technologie SGX demande une réécriture importante des applications existantes[3]. Il est en effet nécessaire de partitionner l'application en identifiant quelle partie du code doit pouvoir avoir accès aux données sensibles. Bien que cette étape essentielle soit complexe, elle permet en principe d'améliorer la sécurité de l'application étant donné qu'il est généralement accepté qu'une application de petite taille – en l'occurrence celle fonctionnant dans l'enclave – a moins de chances d'avoir des défauts tout en étant plus facilement vérifiable qu'une application de grande taille. La communication entre la partie sécurisée de l'application (dans l'enclave) et le reste de l'application (en dehors de l'enclave) se fait via des appels à des fonctions devant être déclarées avant le lancement de l'enclave. Enfin, les applications écrites pour la plate-forme SGX ne peuvent pas être utilisées sur d'autres plates-formes.

Fournisseurs d'infrastructures informatique

Plusieurs fournisseurs d'infrastructures informatiques publiques proposent aujourd'hui des solutions d'informatique confidentielle basées sur les TEE. Nous décrivons ici les trois principaux[4].

AWS

Amazon définit l'informatique confidentielle comme l'utilisation de matériel spécialisé et de micrologiciels associés pour protéger le code et les données du client pendant le traitement contre tout accès extérieur. Amazon traduit cela selon deux dimensions :

- La protection vis-à-vis de de l'opérateur de l'infrastructure informatique sous-jacente, en l'occurrence AWS ;

- La capacité des clients à diviser leurs propres charges de travail en composants plus ou moins fiables, ou à concevoir des systèmes multi-agents.

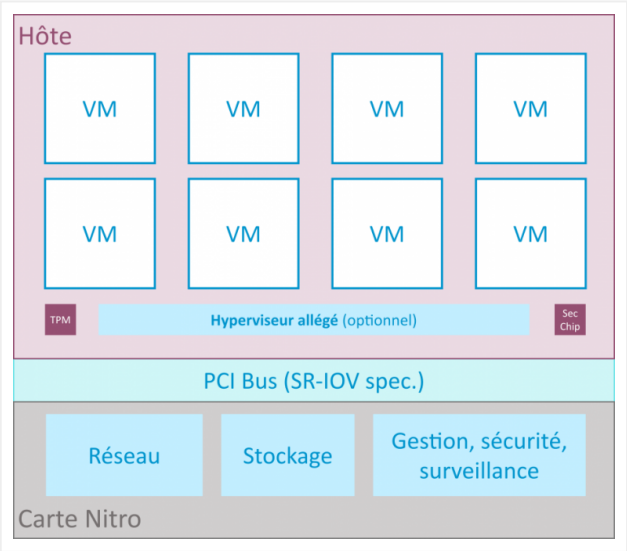
L'accent est mis par Amazon sur l'architecture du système Nitro, plutôt que sur la disponibilité d'un microprocesseur particulier en charge de fournir un TEE. Cependant, depuis avril 2023, AWS offre aussi la possibilité de créer des instances EC2 avec la technologie SEV-SNP d'AMD (voir 1.1).

Dans sa conception, selon AWS, le système Nitro n'offre aucun mécanisme permettant à un système ou à une personne de se connecter aux serveurs EC2, de lire la mémoire des instances EC2 ou d'accéder aux données stockées. Les travaux de maintenance ne peuvent se faire qu'à travers des API limitées.

Le système AWS Nitro (Figure 2) s'inscrit dans une refonte de l'infrastructure de virtualisation du service EC2 d'Amazon, notamment réduire au maximum les parties de l'hyperviseur fonctionnant sur la carte mère. Le système AWS Nitro est une combinaison de serveurs, de processeurs, de composants de gestion et de micrologiciels spécialisés qui fournissent la plate-forme sous-jacente pour toutes les instances Amazon EC2. Il se compose de trois éléments principaux :

- **Cartes Nitro spécifiques** – Dispositifs matériels conçus par AWS qui assurent le contrôle global du système et la virtualisation des entrées/sorties indépendamment de la carte mère du système avec ses processeurs et sa mémoire ;
- La **puce de sécurité Nitro** – Celle-ci est intégrée à la carte mère du serveur et permet un démarrage sécurisé basé sur une racine de confiance matérielle, la capacité d'offrir des instances « bare metal » (permettant de se passer de l'hyperviseur d'AWS), ainsi qu'une protection du serveur contre les modifications non autorisées du micrologiciel du système ;
- L'**hyperviseur Nitro** – Un hyperviseur minimisé, semblable à un micrologiciel, conçu pour fournir une isolation des ressources et des performances.

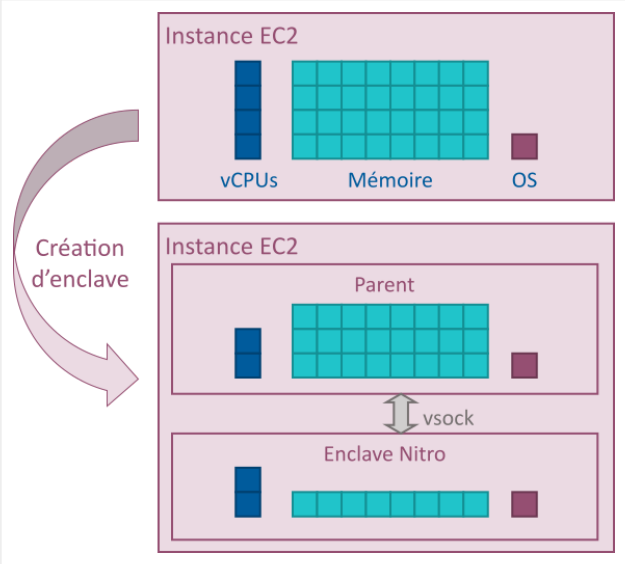
Les considérations de sécurité de ce système sont détaillées dans [12].



— Figure 2 - Architecture d'une machine AWS.

Les enclaves Nitro, quant à elles, sont des machines virtuelles isolées fonctionnant avec une instance EC2 classique, appelée instance « parent » (Figure 3).

Selon AWS, l'enclave Nitro n'offre pas de sécurité supplémentaire vis-à-vis d'une opératrice d'AWS [13], mais permet en revanche d'empêcher un administrateur du client d'accéder au contenu de l'enclave (code et données).



— Figure 3 - Création d'une enclave Nitro à partir d'une instance EC2. Une enclave est créée en partitionnant le processeur et la mémoire d'une instance EC2, appelée instance parent. Il est possible de créer des enclaves avec des combinaisons variées de cœurs de processeur et de mémoire.

La contrainte principale imposée par les enclaves Nitro est que l'application fonctionnant dans l'enclave n'a pas de connexion au réseau. Elle peut seulement communiquer avec l'instance parent via une interface point à point appelée « vsock » qui est définie par un identifiant de contexte et un numéro de port[5]. Un simple « lift and shift » n'est donc pas possible.

Au moment de sa création, l'application fonctionnant dans l'enclave peut générer une paire de clés asymétriques et faire inclure la clé publique dans l'attestation. Par conséquent l'application client vérifiant l'attestation peut utiliser cette clé afin d'établir une communication sécurisée avec l'enclave.

Microsoft Azure

Microsoft Azure propose trois types d'informatique confidentielle basée sur les TEE :

- Les **enclaves d'applications** sont basées sur la technologie SGX d'Intel. Comme indiqué précédemment, il est nécessaire de modifier en profondeur les applications existantes afin de les adapter. Cela impose une réflexion importante sur le choix des parties de l'application à sécuriser et de leur interaction avec les autres parties, mais l'avantage de cette approche est de réduire la quantité de code auquel il faut faire confiance. L'inconvénient est bien évidemment la complexité de la mise en œuvre, requérant notamment une formation particulière des analystes, architectes et programmeurs ;
- Les **machines virtuelles confidentielles** utilisent la technologie SEV-SNP d'AMD (voir ici) et Microsoft a annoncé en avril 2023, la mise à disposition prochaine de la technologie TDX d'Intel (voir ici) [14]. Azure met également à disposition un module de plate-forme fiable (« *trusted platform module (TPM)* ») utilisé notamment pour l'attestation des machines virtuelles ;

- Les **conteneurs confidentiels** permettent au client d'avoir un niveau de contrôle plus fin que les machines virtuelles sur la base informatique de confiance (TCB). Ce modèle d'empaquetage permet en principe d'exécuter des conteneurs existants dans une enclave SGX sans devoir modifier ou recompiler le logiciel (« *lift-and-shift* »).

L'option permettant l'existence de plusieurs fils d'exécution en parallèle (technologie « *hyper-threading* ») au sein du même processeur est désactivée sur toutes les instances SGX. Cela permet d'éviter des attaques conduisant à des fuites de données entre applications partageant le même processeur.

Google

Google propose différentes façons de mettre en œuvre l'informatique confidentielle sur son infrastructure :

- Les **machines virtuelles confidentielles** utilisent la technologie d'AMD ;
- Les **nœuds Kubernetes confidentiels** reposent également sur la technologie SEV d'AMD. Le moteur Kubernetes de Google peut imposer l'utilisation de machines virtuelles confidentielles pour tous les nœuds Kubernetes.

Alors que toutes les machines virtuelles confidentielles contiennent des TPM virtuels qui valident l'intégrité d'une machine virtuelle avec le démarrage mesuré, les machines virtuelles confidentielles avec la technologie SEV-SNP offrent également des rapports d'attestation signés cryptographiquement par le matériel. Cependant la technologie SEV-SNP n'est pas encore disponible de manière généralisée sur l'infrastructure de Google.

Limite pratique des attestations

Comme nous l'expliquions dans notre article précédent, un point essentiel de l'utilisation des TEE est d'obtenir la garantie que le logiciel fonctionnant sur l'infrastructure louée est réellement le logiciel auquel s'attend le client et que les données qu'il traite ne peuvent être lues par aucun autre logiciel. Cette garantie, appelée attestation et obtenue à travers un mécanisme fiable, devrait contenir des informations complètes, récentes et explicites sur le plan sémantique [15].

En supposant que l'on fasse confiance à la sécurité physique du microprocesseur ou de la puce spécialisée, que les attaques connues ont été atténuées et que le code de l'enclave n'est pas vulnérable aux attaques par canaux auxiliaires (« *side-channel attacks* »), comment peut-on être certain que la sortie d'une enclave est fiable?

Il faut s'assurer que :

- Le **fichier binaire exécuté dans l'enclave a bien été construit avec le code attendu**. Pour ce faire le client peut compiler son application sur une machine de confiance (par ex. lui appartenant), puis copier le binaire de manière sécurisée sur la plate-forme d'informatique confidentielle. Une autre méthode est d'utiliser un outil de compilation reproductible[6] ;
- Le **fichier binaire en cours d'exécution correspond bien au binaire attendu**. Un système d'attestation utilise des clés cryptographiques dérivées de secrets figés dans le microprocesseur de confiance pour signer une preuve que le binaire est dans un état donné sur un véritable matériel (pas une simulation). La preuve contient une mesure (valeur de hachage cryptographique) du binaire ;
- L'**état de l'application au moment de son démarrage** est celui attendu " la mesure de la partie exécutable du binaire n'est pas suffisante pour prédire son comportement futur ;
- L'**attestation est signée par une entité de confiance**, en principe par le fabricant du microprocesseur ou de la puce sécurisée.

Pourtant dans les solutions étudiées, excepté les enclaves SGX, soit l'attestation est signée par le fournisseur de l'infrastructure (et non par le fabricant du matériel), soit il n'est pas possible de vérifier la mesure du logiciel sécurisé car il inclut des bibliothèques propriétaires. Le risque est donc que l'entité attestée mente sur son état.

Conclusion

Dix ans après les révélations d'Edward Snowden en juin 2013, concernant les méthodes de surveillance des États-Unis, nous devons partir du principe que des informations pourront être obtenues si elles sont suffisamment précieuses. L'impression de plus grande sécurité des infrastructures informatiques nationales peut alors être trompeuse[7]. Il existe en effet une tension entre une volonté d'indépendance des services informatiques étatiques et la capacité à égaler les niveaux de ressources (matérielles, humaines, R&D), de redondance et de sécurité qu'offrent les entreprises dominantes du secteur[8]. L'ajout de l'informatique confidentielle basée sur des TEE ajoute un nouvel argument en faveur des infrastructures informatiques publiques.

Lorsqu'ils sont mis en œuvre correctement, et toutes autres choses égales par elles-mêmes, les TEE fondés des composants physiques permettent d'augmenter significativement le niveau de protection des données au sein d'une infrastructure informatique, en particulier vis-à-vis de tiers, et notamment de cybercriminels[9]. En effet ils permettent d'éviter la plupart des attaques logiques affectant les systèmes habituels, et ce, grâce à une meilleure isolation des processus, un chiffrement de la mémoire par la couche matérielle, un démarrage sécurisé, des mécanismes de contrôle de mise à jour du micrologiciel, et, d'une manière générale à une réduction de la taille de la base informatique de confiance. En d'autres termes les mesures de sécurité mises en place dans les TEE rendent une attaque beaucoup plus complexe et coûteuse.

Les offres d'informatiques confidentielles basées sur des TEE varient entre les fournisseurs, notamment en fonction du type d'abstraction offert : librairie logiciel, conteneur, machine virtuelle. Le choix de ces options conduit à des différences dans la taille de code de la base de confiance (et donc de la surface exposée aux attaques), mais également dans l'effort d'adaptation nécessaire des applications existantes à ces nouveaux environnements.

Lors du choix d'une solution d'informatique confidentielle basée sur les TEE, il conviendra donc de vérifier les points suivants :

- La protection doit être ancrée dans la couche physique du système et chaque appareil doit avoir une identité unique ;
- Le mécanisme d'attestation doit permettre de pouvoir vérifier le contenu[10] du TEE de manière indépendante du fournisseur d'infrastructure[11];
- L'attestation doit être signée au moins par le fabricant du composant physique et pas uniquement par le fournisseur d'infrastructure[12];
- Le service permet au minimum d'importer ses propres clés cryptographiques dans une boîte noire transactionnelle (HSM) dédiée, et au mieux d'utiliser sa propre boîte ;
- Il devrait être possible de vérifier le code source des librairies critiques incluses par le fournisseur d'infrastructure dans la base de confiance pour le bon fonctionnement de l'application du client ;
- Un service permettant de traquer les différentes dépendances logicielles, d'environnement de compilation, et des binaires utilisés pour le TEE devrait être mis à disposition du client par le fournisseur d'infrastructure.

Finalement, la protection des données en cours d'utilisation permise par l'informatique confidentielle ne représente qu'un des multiples aspects techniques à considérer concernant la confidentialité des données sensibles (sans compter les aspects juridiques, économiques et politiques). Tout comme la meilleure serrure sur la porte d'entrée principale d'une maison ne résout pas le problème d'une porte secondaire grande ouverte, l'utilisation de l'informatique confidentielle suppose que les données sont effectivement protégées au repos et en mouvement, mais requiert également une formation spécifique des personnes en charge de l'adaptation (plus ou moins importantes en fonction du type d'informatique confidentielle choisie) et du transfert des applications existantes, notamment les analystes, architectes, et programmeurs.

Bibliographie

[1] A. Linn, « Securing the cloud | Microsoft Story Labs », *Securing the cloud | Microsoft Story Labs*, 2017. http://news.microsoft.com/stories/cloud-security (consulté le 6 juin 2023).

[2] M. U. Sardar et C. Fetzer, « Confidential computing and related technologies: a critical review », *Cybersecurity*, vol. 6, n° 1, p. 10, mai 2023, doi: 10.1186/s42400-023-00144-1.

[3] D. Kaplan, « AMD x86 Memory Encryption Technologies », août 2016. Consulté le: 11 mai 2023. [En ligne]. Disponible sur: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kaplan

[4] D. Kaplan, J. Powell, et T. Woller, « AMD Memory Encryption », White Paper, oct. 2021. Consulté le: 1 mai 2023. [En ligne]. Disponible sur: https://www.amd.com/system/files/TechDocs/memory-encryption-white-paper.pdf

[5] « AMD SEV-SNP: Strengthening VM Isolation with Integrity Protection and More », AMD, janv. 2020.

[6] « Secure Encrypted Virtualisation API Version 0.24 », Specification, avr. 2020. [En ligne]. Disponible sur: https://www.amd.com/system/files/TechDocs/55766_SEV-KM_API_Specification.pdf

[7] Victor Costan et Srinivas Devadas, « Intel SGX Explained ». Cryptology ePrint Archive, 2016. [En ligne]. Disponible sur: https://eprint.iacr.org/2016/086

[8] P.-C. Cheng *et al.*, « Intel TDX Demystified: A Top-Down Approach ». arXiv, 27 mars 2023. Consulté le: 23 mai 2023. [En ligne]. Disponible sur: http://arxiv.org/abs/2303.15540

[9] « Intel 64 and IA-32 Architectures Software Developer's Manual, Combined Volumes: 1, 2A, 2B, 2C, 2D, 3A, 3B, 3C, 3D, and 4 ». Intel Corporation, mars 2023. [En ligne]. Disponible sur: https://cdrdv2.intel.com/v1/dl/getContent/671200

[10] A. Rao, « Rising to the Challenge — Data Security with Intel Confidential Computing », 20 janvier 2022. https://community.intel.com/t5/Blogs/Products-and-Solutions/Security/Rising-to-the-Challenge-Data-Security-with-Intel-Confidential/post/1353141 (consulté le 17 mai 2023).

[11] G. Steer, « Finance's big tech problem », *Financial Times*, 6 juillet 2022. Consulté le: 10 juillet 2023. [En ligne]. Disponible sur: https://www.ft.com/content/41f400b6-f83f-4fa1-8dac-731acddcf8f2

[12] « The Security Design of the AWS Nitro System - AWS Whitepaper ». AWS, 18 novembre 2022. [En ligne]. Disponible sur: https://docs.aws.amazon.com/fr_fr/whitepapers/l... nitro-

system/security-design-of-aws-nitro-system.html

[13] « Confidential computing: an AWS perspective | AWS Security Blog », 24 août 2021. https://aws.amazon.com/blogs/security/confidential-computing-an-aws-perspective/ (consulté le 18 avril 2023).

[14] M. McReynolds, « Preview: Introducing DCesv5 and ECesv5-series Confidential VMs with Intel TDX », 24 avril 2023. https://techcommunity.microsoft.com/t5/azure-confidential-computing/preview-introducing-dcesv5-and-ecesv5-series-confidential-vms/ba-p/3800718 (consulté le 16 mai 2023).

[15] G. Coker *et al.*, « Principles of remote attestation », *Int. J. Inf. Secur.*, vol. 10, n° 2, p. 63-81, juin 2011, doi: 10.1007/s10207-011-0124-7.

[16] « Nix & NixOS | Reproducible builds and deployments ». https://nixos.org/ (consulté le 6 juin 2023).

[17] R. Gallagher, « The Inside Story of How British Spies Hacked Belgium's Largest Telco », *The Intercept*, 13 décembre 2014. https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/ (consulté le 8 juin 2023).

[18] R. Gallagher, « How U.K. Spies Hacked a European Ally and Got Away With It », *The Intercept*, 17 février 2018. https://theintercept.com/2018/02/17/gchq-belgacom-investigation-europe-hack/ (consulté le 8 juin 2023).

[19] C. Zhao, « SolarWinds, Probably Hacked by Russia, Serves White House, Pentagon, NASA », *Newsweek*, 14 décembre 2020. Consulté le: 9 janvier 2023. [En ligne]. Disponible sur: https://www.newsweek.com/solar-winds-probably-hacked-russia-serves-white-house-pentagon-nasa-1554447

[20] R. Koppel et C. Kuziemsky, « Healthcare Data Are Remarkably Vulnerable to Hacking: Connected Healthcare Delivery Increases the Risks », *Stud. Health Technol. Inf.*, vol. 257, p. 218-222, 2019.

Notes

[1] Par exemple le terme « enclave » n'a pas du tout le même sens chez Amazon et Intel. Alors que les « Nitro Enclaves » sont des machines virtuelles entières, les « SGX Enclaves » sont des bibliothèques exposant certaines API.

[2] Notons que NVIDIA offre depuis peu un processeur graphique (A100 Tensor Core avec la technologie « Ampere Protected Memory (APM) ») qui introduit un mode d'exécution confidentielle dans le processeur graphique et permet ainsi d'utiliser des ensembles des données pour former et déployer des modèles d'apprentissage automatique (« machine learning ») de manière confidentielle, notamment sur une infrastructure informatique publique. Ces processeurs sont disponibles sur l'offre Azure de Microsoft.

[3] Ce n'est pas le cas avec TDX qui permet de protéger une machine virtuelle entière.

[4] Selon le Financial Times, les trois fournisseurs d'infrastructure informatique les plus importants en 2021 étaient Amazon, Microsoft et Google [11].

[5] Cette « vsock » utilise la même API que les « sockets » POSIX.

[6] Par exemple Nix [16].

[7] Nous avons appris en 2014 que l'agence de surveillance britannique GCHQ avait piraté un système sensible de Belgacom [17], [18].

[8] Les groupes cybercriminels n'hésitent plus à compromettre la sécurité de services informatiques en mettant en œuvre de nouveaux types d'attaques. L'exemple du piratage de SolarWind est symptomatique à cet égard [19]. Un service indépendant national mais insuffisamment sécurisé pourrait représenter un point de défaillance unique posant un risque crucial.

[9] « Les données de santé sont attrayantes pour les cybercriminels car elles contiennent des données financières et personnelles, peuvent être utilisées pour le chantage et, surtout, sont idéales pour la facturation frauduleuse » [20].

[10] Ce contenu, dans le cas de machines virtuelles confidentielles, inclut également le système d'exploitation que l'on préférera de taille minimale.

[11] Si le fournisseur d'infrastructure contrôle en partie le contenu de la machine virtuelle confidentielle ou du conteneur confidentiel et que le client n'a pas de mécanisme pour le vérifier, alors la confiance dans le fournisseur reste totale.

[12] Si le fournisseur d'infrastructure signe l'attestation, alors la confiance dans ce fournisseur reste totale.

Ce post est une contribution individuelle de Fabien A. P. Petitcolas, spécialisé en sécurité informatique chez Smals Research. Cet article est écrit en son nom propre et n'impacte en rien le point de vue de Smals.

This entry was posted in **Cloud**, **Data center**, **Hardware**, **Security** and tagged **confidential computing**, **TEE**, **Trusted Execution Environments** by **Fabien A. P. Petitcolas**. Bookmark the **permalink [https://www.smalsresearch.be/outils-pour-linformatique-confidentielle/]** .

About Fabien A. P. Petitcolas

Fabien A. P. Petitcolas is research consultant at Smals where he focuses on security topics. Before joining Smals, Fabien was with **OneSpan** and **Microsoft** where he took various roles. Fabien graduated from École Centrale, Lyon and then completed his PhD at the University of Cambridge under the guidance of **Prof. Ross Anderson** FRS FREng. List of publications **here**.

View all posts by Fabien A. P. Petitcolas →