Article technique

Chiffrement AES 128 bits ou 256 bits

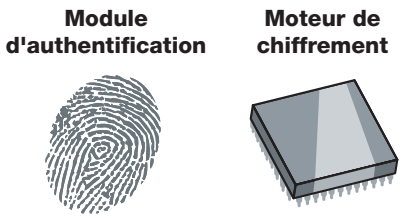
Solutions 128 bits : démonstration d'un niveau de sécurité absolu adapté à chaque besoin

Contexte

Il règne une certaine confusion autour du marché des produits de chiffrement matériel complet (FDE). Tandis que Seagate Technology LLC propose une gamme de produits dotés d'un chiffrement AES-128, d'autres produits logiciels et matériels concurrents offrent un chiffrement AES-256. La question qui se pose est la suivante : les produits AES-256 sont-ils plus performants que leurs équivalents AES-128 ?

Pour répondre à cette question, nous devons déjà définir ce que signifie « plus performants ». Dans notre contexte de protection des données au repos, il semble logique d'appliquer cette expression aux produits qui rendent l'accès aux données protégées bien plus difficile pour toute personne ne disposant pas des autorisations nécessaires.

Pour faire court, la réponse est « non ». Les techniques de recherche de clé exhaustives dans un espace de clé de 128 bits, à l'aide des derniers processus de rationalisation, nécessitent des ressources (MIPS, mémoire, alimentation et temps) bien supérieures aux capacités actuelles. Toute innovation importante s'appliquerait sans doute aussi bien aux technologies 256 bits que 128 bits.



(Explication rapide des termes AES-128 et AES-256 : l'AES est un algorithme de chiffrement symétrique qui permet de chiffrer et de déchiffrer des données par blocs de 128 bits, à l'aide de clés 128, 192 ou 256 bits. La nomenclature AES *(Advanced Encryption Standard)* pour les différentes tailles de clé est AES-x, x représentant la taille de la clé.)

Afin de comprendre la méthode utilisée par un pirate pour accéder aux données, il est nécessaire de commencer par décrire le système. Le module d'authentification et le moteur de chiffrement constituent les principaux composants d'un système de sécurisation des données au repos.

Les applications d'entreprise incluent bien sûr de nombreux outils de gestion qui varient selon l'installation. Ces outils peuvent servir à générer ou à remettre des mots de passe et des clés à des tiers, ainsi qu'à définir des utilisateurs et leurs identités numériques et à en effectuer le suivi. Nous ne nous attarderons pas sur ces outils de gestion ici, mais nous nous attacherons plutôt à l'étude des avantages offerts par une sécurisation des principaux composants, à savoir le module d'authentification et le moteur de chiffrement.

Module d'authentification

Il serait tout à fait illogique pour une personne investissant un million de dollars dans des mesures de sécurité à chaque point d'entrée de sa résidence (portes, fenêtres, etc.) d'utiliser « 1234 » comme code d'accès à sa porte d'entrée principale.

Chiffrement AES 128 bits ou 256 bits

Solutions 128 bits : démonstration d'un niveau de sécurité absolu adapté à chaque besoin

Cela montre qu'une sécurité optimale passe obligatoirement par des contrôles d'accès au système renforcés, associés à des processus de gestion et de traitement des données et des codes d'accès sécurisés.

Comme le dit l'adage : la force d'une chaîne se mesure à la résistance de son maillon le plus faible.

Alors que nous débutions notre article en mentionnant la confusion qui règne autour des longueurs de clés de chiffrement, le reste de notre propos devrait vous convaincre que les performances des moteurs de chiffrement ne sont aucunement remises en question, de par les composants mêmes qu'ils intègrent. Dans le cadre d'une mise en place de tels moteurs de chiffrement, la clé d'une sécurité optimale (sans aucun jeu de mot) est de garantir que la fonction d'authentification du système est au moins aussi performante que la fonction de chiffrement. Ne pas respecter ce principe revient à s'exposer à une réelle menace de piratage du système, plus que du processus de chiffrement.

Prenons pour exemple des mots de passe ATA standard. Avec les ordinateurs plus anciens, de nombreux utilisateurs dépendaient d'une sécurité ATA au niveau du BIOS pour la protection de leur système. Il est d'ailleurs facile de constater que bon nombre de BIOS utilisés aujourd'hui prennent uniquement en charge des mots de passe d'une longueur maximale de 8 caractères (ou 64 bits). En outre, ces mots de passe sont souvent choisis pour leur facilité de mémorisation par les utilisateurs, ce qui en fait des cibles faciles pour les pirates amateurs.

Face à cette situation, certaines sociétés ont choisi de déployer des lecteurs d'empreintes digitales afin de renforcer la sécurité de leurs systèmes. Toutefois, il est important d'examiner avec attention la résolution et les capacités de différenciation des « signatures » que ces lecteurs tirent des empreintes digitales numérisées. En faisant une recherche rapide sur Internet, on trouve des modèles de lecteurs capables de prendre en charge de 30 à 100 000 utilisateurs. Ce qui donne une longueur de 2^5 (5 bits) à 2^{17} (17 bits) environ. En associant la plus grande longueur (17 bits) à un mot de passe à 10 caractères efficace, généré de manière aléatoire (80 bits), il est possible de bénéficier d'une longueur totale de 97 bits pour le mot de passe d'authentification. N'oublions pas que la plupart des BIOS ne prennent pas en charge cette longueur de clé d'authentification ; cette clé 97 bits sera donc réduite à une longueur inférieure.

Pour connaître le maillon le plus faible des systèmes qui utilisent un chiffrement matériel performant, il faut s'intéresser au module d'authentification.

Quelques comparaisons suffisent à mettre en évidence l'avantage des solutions de chiffrement matériel sur les solutions de chiffrement logiciel :

- Avec le chiffrement logiciel, le système d'exploitation peut accéder au stockage des clés, ce qui constitue une réelle menace de piratage pour ce dernier. Le chiffrement du disque dur remédie à cette faille.
- De même, le processus de chiffrement du chiffrement logiciel est observable dans la mémoire, ce qui n'est pas le cas avec le chiffrement matériel.

Récapitulatif des failles du chiffrement logiciel

	Chiffrement matériel	Chiffrement logiciel
Stockage des clés accessible au système d'exploitation (ouvert aux attaques)	Non	Oui
Processus de chiffrement observable dans la mémoire (susceptible d'être espionné)	Non	Oui
Performances système réduites par le processus de chiffrement	Non	Oui
Intervention de l'utilisateur requise pour la spécification de dossiers ou de fichiers à chiffrer	Non	Oui
Mises à niveau du système d'exploitation plus fastidieuses que celles d'un système non chiffré	Non	Oui

Chiffrement AES 128 bits ou 256 bits

Solutions 128 bits : démonstration d'un niveau de sécurité absolu adapté à chaque besoin

- Le chiffrement logiciel peut réduire les performances du système. Le chiffrement matériel n'a aucune conséquence sur les performances du système.
- Avec le chiffrement logiciel, l'utilisateur doit spécifier des dossiers ou des fichiers à chiffrer. Avec le chiffrement matériel, tout ce qui est écrit sur le disque est chiffré, sans que l'utilisateur ait à intervenir.
- Les mises à niveau du système d'exploitation des systèmes utilisant le chiffrement logiciel sont plus fastidieuses que celles des systèmes non chiffrés. Les systèmes dotés de solutions de chiffrement matériel peuvent au contraire être mis à niveau aussi facilement que n'importe quel système ordinaire.

Si vous souhaitez obtenir plus de détails sur les comparaisons ci-dessus, d'autres livres blancs sont à votre disposition.

Comme indiqué dans les exemples précédents, le chiffrement logiciel est exposé aux menaces logicielles traditionnelles. Cela s'applique non seulement au moteur de chiffrement, mais également aux processus d'authentification. Pour boucler un système de manière efficace, tous ces processus logiciels doivent être traités bien avant que la question d'un chiffrement 128 bits ou 256 bits ne se pose.

Enfin, à l'issue de notre discussion sur le moteur de chiffrement, nous arrivons à l'observation suivante. Les disques durs Seagate Secure™ ont été conçus avec une taille de clé d'authentification de 256 bits. Ainsi, bien que le disque soit commercialisé en tant que disque à chiffrement AES 128 bits, la clé d'authentification réelle permettant de déverrouiller le disque prend en charge un chiffrement complet à 256 bits, le niveau le plus performant de l'ensemble des solutions de chiffrement habituellement disponibles.

Ce point éclairci, nous pouvons désormais nous attacher au moteur de chiffrement.

Moteur de chiffrement

Pourquoi AES

Les algorithmes de chiffrement approuvés par le NIST sont répartis en trois classes de base :

- Les algorithmes permettant de chiffrer les messages relativement courts ;
- Les algorithmes permettant de calculer des signatures numériques ;
- Les algorithmes permettant de définir ou de vérifier un composant matériel de chiffrement.

Le but du chiffrement des données au repos étant de transformer les données de sorte à les rendre quasiment inaccessibles sans la clé confidentielle, des algorithmes de chiffrement symétrique sont déployés dans le cadre d'applications FDE.

Les algorithmes approuvés par le NIST pour le chiffrement symétrique sont les algorithmes AES et TDES. L'algorithme AES est spécifié dans la publication FIPS Pub 197[2]. Cet algorithme permet de chiffrer et de déchiffrer des données par blocs de 128 bits, à l'aide de clés 128, 192 ou 256 bits. Le NIST stipule que « ces trois tailles sont jugées acceptables pour les applications du gouvernement fédéral américain, des plus basiques à celles classées secret défense. »

L'algorithme Triple DES (TDES) est défini dans la publication FIPS Pub 46-3. Cet algorithme permet de chiffrer et de déchiffrer des données par blocs de 64 bits, à l'aide de clés 56 bits. Les applications gouvernementales peuvent utiliser ces trois clés distinctes.

Une analyse approfondie du NIST (rapportée dans la publication spéciale du NIST numéro 800-57) démontre la supériorité de l'algorithme AES (en termes de volume de travail à effectuer afin de « casser l'algorithme ») sur le TDES. Ce point a notamment joué en faveur de la sélection de cet algorithme.

[2] Federal Information Processing Standards Publications (publications de standards FIPS du gouvernement américain)

Chiffrement AES 128 bits ou 256 bits

Solutions 128 bits : démonstration d'un niveau de sécurité absolu adapté à chaque besoin

Choix de la longueur de clé AES

Lors de la mise en œuvre du chiffrement AES, Seagate a dû sélectionner une longueur de clé. Les éléments suivants ont été pris en compte :

- Dans ce document de référence, le NIST[1] conclut que les trois longueurs de clé (128 bits, 192 bits et 256 bits) du chiffrement AES offrent un niveau de chiffrement acceptable ou moins jusqu'à l'année calendaire 2031, voire après.
- La recommandation du NIST mentionnée précédemment inclut le modèle de menace que constituent non seulement la découverte de la clé, mais également le piratage de l'algorithme de chiffrement. La différence entre le piratage d'un algorithme AES-128 et le piratage d'un algorithme AES-256 est jugée comme infime. Le petit malin qui réussit à pirater le 128 bits réussira sans doute également à pirater le 256 bits.

En outre, Seagate souhaitait optimiser le succès de sa solution en prenant en compte les préoccupations supplémentaires émergeant du côté des professionnels :

- Promouvoir la conformité aux règles d'exportation à partir des États-Unis et d'importation dans d'autres pays ;
- Garantir une rentabilité optimale ;
- Répondre aux besoins de TOUS les marchés cibles.

L'AES-128 répond à l'ensemble des critères exposés plus haut, les dépassant même parfois.

Pour resituer cela dans notre propos, examinons maintenant l'importance de la taille réelle que représentent ces 128 bits. Cette taille équivaut à 2 puissance 128 ou 3,4 x 10 puissance 38 (38 zéros) : 3 400 000 000 000 000 000 000 000 000 000 000 000.

Si l'on considère les données suivantes :

- Chaque personne sur Terre possède 10 ordinateurs.
- Notre planète compte 7 milliards d'habitants.
- Chacun de ces ordinateurs peut tester 1 milliard de combinaisons de clés par seconde.
- En moyenne, il est possible de découvrir la clé après avoir essayé 50 % des possibilités.

Alors (voir la référence de calcul en annexe) :

- La population de la Terre peut pirater une clé de chiffrement (un disque seulement) en 77 000 000 000 000 000 000 000 000 ans !
- Pour information, le piratage d'une deuxième clé/d'un deuxième disque prendrait 77 000 000 000 000 000 000 000 000 années supplémentaires.

Cette analyse est quelque peu simplifiée. Le Réseau d'excellence européen en cryptologie (*European Network of Excellence in Cryptology*) procède régulièrement à une analyse plus approfondie dans le cadre de la publication « Yearly Report on Algorithms and Keysizes » (rapport annuel sur les algorithmes et les tailles de clés). Son dernier rapport, datant de janvier 2007, analyse, de manière bien plus détaillée, l'évolution de la puissance de calcul (comme fonction de l'évolution des technologies et des investissements) ; les conclusions obtenues à l'issue de cette analyse sont consignées dans le tableau suivant :

Taille minimale de clé symétrique (en bits) par type de pirate

Pirate	Budget	Matériel	Sécurité minimale
« Pirate »	0 < 400 $ 0	PC PC/FPGA « Programme malveillant »	52 57 60
Petite société	10 000 $	PC/FPGA	62
Société de taille moyenne	300 000 $	FPGA/ASIC	67
Grande société	10 M $	FPGA/ASIC	77
Agence de renseignement	300 M $	ASIC	88

[1] Le NIST (*National Institute of Standards and Technology, Institut national des standards et de la technologie*) est chargé du développement des standards et des directives, notamment des configurations minimales requises afin de fournir une protection des informations adaptée à l'ensemble des opérations et des actifs du gouvernement américain. Les standards de protection des systèmes de sécurité nationale américains sont spécifiés par la NSA (*National Security Agency*).

Chiffrement AES 128 bits ou 256 bits

Solutions 128 bits : démonstration d'un niveau de sécurité absolu adapté à chaque besoin

Bien que ces tailles de clés soient jugées acceptables à l'heure actuelle, l'analyse a permis d'arriver à la conclusion que 14 bits supplémentaires dans la longueur de clé permettraient d'assurer la sécurité des données pendant les 20 prochaines années. Ce qui donne donc une longueur de clé recommandée de 102 bits (88 + 14), pour une sécurité optimale au cours des 20 prochaines années, voire plus.

Alors pourquoi les solutions sont-elles commercialisées avec un chiffrement 256 bits ? Pur marketing.

Les chiffres élevés sont perçus comme synonymes de meilleures performances. C'est aussi simple que cela. Lors de la commercialisation d'une solution logicielle notamment, il est important de véhiculer l'idée de puissance. Il est bien plus facile d'ajouter des bits à l'algorithme de chiffrement que de colmater toutes les failles d'un environnement ouvert.

Les options 192 bits et 256 bits ont été proposées afin de répondre à la déception des sociétés face à l'algorithme TDES, approuvé uniquement pour une seule longueur de clé. Le NIST a alors évalué trois options de longueurs de clé différentes pour le chiffrement AES : 128, 192 et 256. Ces trois longueurs de clé pourront être mises en œuvre en raison de leur nature même, plutôt qu'en réponse à des besoins spécifiques. Les applications classées secret défense peuvent nécessiter une longueur de clé de 256 bits car elles le peuvent, mais aussi parce que cette longueur est disponible.

Autres considérations importantes

Lors de la sélection d'un système de chiffrement, certains facteurs au niveau de la solution s'avèrent nettement plus importants que toute question relative à une longueur de clé supérieure à 128 bits.

Il est nécessaire de prendre en compte les points suivants pour pouvoir bénéficier d'une protection des données au repos complète et fiable :

- Appliquez-vous des mesures suffisamment performantes pour garantir la protection de vos mots de passe/informations d'authentification ?
- Votre système de chiffrement est-il suffisamment renforcé (traitement avec ASIC personnalisé ou logiciel piratable) ?
- Le chemin de communication entre le module de chiffrement et les informations du système/de l'utilisateur est-il sécurisé ?
- La solution envisagée a-t-elle été approuvée par la NSA ?
- Votre solution peut-elle être importée et exportée vers et depuis vos emplacements cibles ?
- Votre solution offre-t-elle des services de gestion de clés et de mots de passe sécurisés et adaptés, comme requis par les organisations de gestion informatique centralisée ?
- Votre solution de chiffrement est-elle conçue de telle sorte que les clés ne quittent jamais les environnements protégés ?

Les disques Seagate Secure fournissent les fonctionnalités et les composants permettant de répondre « oui » à chacune de ces questions.

La citation suivante, tirée de la publication du NIST mentionnée précédemment, offre une vision fidèle de l'approche holistique de la sécurité des données :

> Une gestion adaptée des clés de chiffrement est essentielle pour pouvoir utiliser, de manière efficace, le chiffrement à des fins de sécurisation de données. Les clés fonctionnent comme une combinaison de coffre-fort. Lorsqu'une telle combinaison tombe entre les mains d'une personne mal intentionnée, même le coffre-fort le plus résistant ne peut empêcher l'intrusion. De même, une mauvaise gestion des clés peut rapidement compromettre les algorithmes les plus fiables. Enfin, la sécurité des informations protégées par chiffrement dépend directement de la puissance des clés, de l'efficacité des mécanismes et des protocoles associés à celles-ci et de la protection qu'elles assurent. Chaque clé doit être protégée de toute modification ; les clés confidentielles et privées doivent être protégées de toute divulgation non autorisée. La gestion des clés constitue la base de la génération, du stockage, de la distribution et de la destruction sécurisés des clés.
>
> Utilisateurs et développeurs disposent donc d'un large choix de mécanismes de chiffrement. Un choix non adapté peut entraîner une sécurité illusoire, qui protègera peu voire pas du tout le protocole ou l'application concernée. Cette recommandation (SP 800-57) fournit des informations de base et donne quelques clés pour une prise de décision judicieuse lors de la sélection et de l'utilisation de mécanismes de chiffrement.

Chiffrement AES 128 bits ou 256 bits

Solutions 128 bits : démonstration d'un niveau de sécurité absolu adapté à chaque besoin

Résumé

- Le chiffrement matériel 128 bits est largement suffisant pour les applications commerciales et gouvernementales hors secret défense.
- Lorsque le débat sur les moteurs de chiffrement se sera apaisé, il faudra concentrer cette énergie sur les questions de déploiement au niveau des solutions.
- Les failles susceptibles d'entraîner une fuite de données ne résultent pas de la taille de la clé de chiffrement 128 bits. Les principales failles se situent au niveau du logiciel, du stockage et de l'authentification des clés.
- Lorsque ces points sensibles sont correctement traités, une solution de protection des données déployant un chiffrement AES 128 bits fournit une sécurité complète pour chaque besoin.

Annexe

Référence de calcul pour un exemple de piratage de clé 128 bits

Personnes	7,00E+09
Ordinateurs par personne	10,00
Ordinateurs	1,00E+09
Nombre de combinaisons par seconde par ordinateur	7,00E+19
Nombre total de combinaisons par seconde	7,00E+19
Secondes par an	3,15E+07
Nombre total de combinaisons par an	2,22E+12
Nombre de combinaisons de clés 128 bits (*50 %)	1,70E+38
Années nécessaires au piratage	7,66E+25

Références de publication

Publication spéciale du NIST (*National Institute of Standards and Technology*) numéro 800-57 (mai 2006)
http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf

D.SPA.21ECRYPT Yearly Report on Algorithms and Keysizes (Rapport annuel sur les algorithmes et les tailles de clés), par le Réseau d'excellence européen en cryptologie (*European Network of Excellence in Cryptology*) (janvier 2007)
http://www.ecrypt.eu.org/documents/D.SPA.21-1.1.pdf

http://www.crypto.com/papers/keylength.pdf

AMÉRIQUES Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, États-Unis, +1 831-438-6550
ASIE/PACIFIQUE Seagate Technology International Ltd. 7000 Ang Mo Kio Avenue 5, Singapour 569877, +65 6485 3888
EUROPE, MOYEN-ORIENT ET AFRIQUE Seagate Technology SAS 130-136, rue de Silly, 92773 Boulogne-Billancourt Cedex, France, +33 (0)1 41 86 10 00

TP596.1-0808FR, août 2008