

KEYNECTIS apporte son éclairage sur l'actualité liée au SSL-MD5

KEYNECTIS, leader européen des technologies et services de confiance, fait un point sur la récente actualité concernant l'algorithme SSL-MD5 et ses faiblesses :

Le problème

Les certificats SSL sont utilisés par les sites web pour créer une connexion sécurisée avec un internaute. Ces certificats sont achetés auprès d'une Autorité de Certification connue (AC). Mais plusieurs Autorité de Certification continuent à produire des certificats SSL en utilisant une signature de type MD5+RSA, alors que le MD5 a été cassé en 2004.

Le fait d'utiliser le MD5 permet à un attaquant de produire un faux certificat d'AC à partir d'un certificat SSL, et ainsi de signer d'autres certificats SSL, frauduleusement.

Qui est concerné par ce problème ?

Tous les utilisateurs, à partir du moment où ils surfent sur le web sur des sites sécurisés ou échangent des documents signés, tels que des mails.

Les chercheurs ont estimé que sur l'ensemble des sites web ayant un certificat SSL "valide" (reconnus par un navigateur), environ 30% sont concernés par cette faille.

Les détails

Une signature est le résultat d'une fonction mathématique mettant en jeu le document à signer (publique), et la clé privée du signataire (privée).

En pratique, on ne signe pas le document lui-même, pour des contraintes de performance (mettre en œuvre la clé privée est coûteux en temps, surtout si elle est stockée sur une carte à puce). On signe plutôt une empreinte (ou "hash") de ce document. Cette empreinte a une taille fixe, quelle que soit la taille du document initial. Il est évident qu'il existe plus de documents possibles que d'empreintes possibles, et donc que plusieurs documents peuvent avoir la même empreinte. Dans le cas du MD5, l'empreinte fait 16 octets, ce qui lui permet de prendre plusieurs milliards de milliards de valeurs différentes (écrivez un 3 suivi de 37 zéros, vous obtenez une approximation du nombre de valeurs possibles).

On peut donc attribuer la même signature à 2 certificats (ou documents) différents dès lors que ceux-ci ont la même empreinte. Pour être utilisable en cryptographie, une fonction d'empreinte (qu'on appelle plus souvent fonction de hachage) doit répondre à certaines propriétés, l'une d'entre elles étant l'impossibilité pratique de produire des collisions (2 documents donnant la même empreinte); on ne doit pas pouvoir calculer mathématiquement cette possibilité.

Le MD5 a été affaibli à plusieurs reprises, la première fois en 1996, et finalement déclaré non fiable durant l'été 2004[1], au moment où des chercheurs chinois ont pu produire des collisions MD5, en 1 heure environ. Aujourd'hui, pour des documents purement arbitraires, il faut quelques secondes à un PC classique. Un certificat n'est pas un document purement arbitraire, il a une structure imposée, et des informations variables contrôlées par l'autorité de certification. Il faut donc beaucoup plus de temps pour produire 2 certificats ayant la même empreinte. Des résultats publiés en 2006[2] ont montré qu'on pouvait produire 2 certificats ayant la même empreinte (l'attaque montrée au CCC est une extension des résultats de 2006).

Une autre propriété, qu'une bonne fonction de hachage doit avoir, est ce qu'on appelle la résistance à une seconde pré-image. Il s'agit de trouver un document ayant la même empreinte qu'un document existant. MD5 conserve encore cette propriété, c'est pour cette raison qu'on ne peut pas produire un certificat ayant la même signature qu'un certificat existant.

En pratique, l'attaquant doit donc construire ses 2 certificats en même temps (en exploitant la non résistance à la collision de MD5), ce qui signifie qu'il doit pouvoir contrôler tous les champs variables des certificats (ou du moins être capable de les prédire). Ces champs variables sont au nombre de 2 :

- la période de validité, facilement prédictible,



KEYNECTIS

- le numéro de série, qui doit être unique, et est facilement prédictible si l'autorité de certification utilise une séquence comme numéro de série (beaucoup d'autorités le font).

Après le SHA1, il existe la série des SHA2 (4 déclinaisons), supposés plus robustes, mais moins bien supportés par les logiciels actuels. On ne peut donc pas remplacer le SHA1 par un SHA2 facilement.

Le design de SHA0 (le prédécesseur de SHA1, cassé), SHA1, et SHA2 est connu, mais pas les règles ayant permis de produire ce design (on connaît les composants, mais pas la recette). C'est pourquoi le NIST a lancé une compétition permettant à la communauté de produire un successeur à la famille SHA0/1/2. Cette compétition est ouverte, les règles sont connues de tous, les candidats sont publics, les résultats également. C'est ce genre de compétition qui a permis de désigner le successeur du DES (là aussi, un algorithme de chiffrement très utilisé et robuste, mais dont la recette est inconnue), qui est l'AES, un candidat belge. L'AES est considéré comme un très bon algorithme de chiffrement, il a été analysé par plusieurs centaines de cryptologues pendant des mois, comme les autres candidats, tant du point de vue sécurité que performance. Il est aujourd'hui largement déployé et utilisé. On peut espérer que la même chose se produise avec le concours SHA3.

La position de KEYNECTIS

Les solutions de KEYNECTIS ne sont pas impactées par cette faille, et ce pour plusieurs raisons :

- l'utilisation de l'algorithme MD5 a été bannie des certificats produits, au profit du SHA1, encore résistant (un passage vers SHA2 est prévu).
- dans la conception de l'infrastructure PKI Sequoia[®] de KEYNECTIS (qui permet la gestion des certificats), une information non prédictible par un attaquant potentiel a été introduite (dans tous les certificats produits), rendant spécifiquement cette attaque inenvisageable; il s'agit du numéro de série du certificat, qui est garanti à la fois unique et aléatoire.
- KEYNECTIS est le seul opérateur français à être qualifié PRIS/RGS au niveau des certificats SSL.

[1]: <http://eprint.iacr.org/2004/199>

[2]: <http://eprint.iacr.org/2006/360>

A propos de KEYNECTIS

Leader européen des technologies et services de confiance, KEYNECTIS propose une offre globale assurant la gestion des identités numériques et la sécurisation des échanges électroniques au profit des gouvernements, industriels, institutions financières et in fine au bénéfice des usagers à travers le monde. L'offre KEYNECTIS, logiciel et service, bénéficie de l'expérience de plus de 25 millions de certificats électroniques émis à ce jour et 10 millions de documents signés par ses technologies.

Pour en savoir plus : <http://www.keynectis.com>

Les dernières annonces de KEYNECTIS : http://www.rp-net.com/?ID_CONSTRUCTEUR=640

Contacts Presse

RUMEUR PUBLIQUE - Cédric Buisson

Tel : 01 55 74 52 07 / Mobile : 06 20 49 32 06

Email : keynectis@rumeurpublique.fr

Pour en savoir plus : <http://www.keynectis.com>

Les dernières annonces de KEYNECTIS : http://www.rp-net.com/?ID_CONSTRUCTEUR=640