Sécurité: une « faille » dans l'algorithme de chiffrement AES ?

Trois chercheurs, au terme d'un « *long projet d'analyse* » du chiffrement AES (*) très répandu dans le monde, ont réussi à détecter une faille. Il s'agit d'Andrey Bogdanov (K.U.Leuven), de Dmitry Khovratovich (Microsoft Research) et de Christian Rechberger (ENS Paris). Ils viennent de mettre en évidence la possibilité de mener une attaque contre l'algorithme d'encryption réputé inviolable.
Mais rien de grave. Ils ont montré que leur attaque peut permettre, tout au plus, d'accélérer de 4 fois un processus de test pour découvrir des clés secrètes, clés inhérentes au protocole de chiffrement. Plutôt que faille, retenons leur terme, une « faiblesse » (*weakness*).

Pour rappel, l'algorithme de chiffrement AES, validé par l'administration américaine en 2001, est utilisé par des centaines de millions d'utilisateurs à travers le monde. Il sert couramment à protéger des transactions bancaires, des communications sans fil (wifi) ou encore des données stockées sur des disques durs ou des bandes pour archivage.

Pas de panique: une probabilité infime…
Peu d'informations ont été livrées sur la nouvelle faille communiquée à la presse ce 17 août 2011. Les auteurs de la découverte parlent bien d'une « *faiblesse* » plus que d'une réelle vulnérabilité. Cette faiblesse concerne toutes les versions d'AES (*) même lorsqu'une seule clé de cryptage est utilisée. L'attaque conduirait donc à ce que la découverte d'une clé AES parmi les innombrables combinaisons possibles prendrait 4 fois moins de temps. Mais tout est relatif…
« *En d'autres termes, l'AES sur clé de 128 bits descend plutôt au niveau 126, ce qui signifie encore un nombre de combinaisons s'écrivant avec* ***un 8 suivi de 37 zéros*** *!*« . Les chercheurs expliquent encore : « *Avec un trillion de machines, où chacune pourrait tester un milliard de clés par seconde, il faudrait plus de 2 milliards d'années pour trouver la combinaison d'une clé AES-128". Or, ajoutent-ils, les plus grandes entreprises peuvent réunir tout au plus des millions de machines et ces machines ne peuvent tester que 10 millions de clés à la seconde*« . Bref une **probabilité non nulle mais infime**!

Au cours de la décennie écoulée, un grand nombre de chercheurs et spécialistes du cryptage ont testé la sécurité de cet algorithme sans réussir à le mettre en défaut. Même en 2009, lorsque certaines vulnérabilités ont été repérées dans le cas d'une utilisation pour encrypter des données selon 4 clés reliées entre elles. En théorie, il devenait possible, pour un 'hacker, d'en prendre le contrôle. Mais cette vulnérabilité, intéressante sur le plan mathématique et des calculs de probabilités, n'aurait jamais pu être exploitée par aucun hacker.

___

*(*) **AES** ou **Advanced Encryption Standard**: cet algorithme, dit à clé symétrique, a été « inventé » en 2000 par deux ingénieurs, Joan Daemen de STMicroelectronics, et Vincent Rijmen (de K.U.Leuven). Il a remporté le prix du très réputé NIST (National Institute for Standards and Technology) qui l'a standardisé aux Etats-Unis. Il existe en trois versions: clés sur 128, 192 or 256 bits. C'est le format de clé sur128 bits qui a été généralisé un peu partout sur la planète.*