ENTRETIEN

Apple et le FBI : « Un système de chiffrement muni d'une trappe serait catastrophique »

Les données que contient un téléphone peuvent être cruciales dans une enquête judiciaire, mais prévoir un moyen d'y accéder en contournant le cryptage menace les libertés individuelles. Un compromis est-il possible ?

David POINTCHEVAL, chercheur au CNRS, est directeur adjoint du département d'informatique de l'ENS à Paris.

Dans l'enquête sur le massacre de San Bernardino commis fin 2015, le FBI n'arrivait pas à lire les données chiffrées du téléphone du tueur. Il a donc demandé l'aide du constructeur de l'appareil, Apple, qui a refusé. Les enquêteurs ont finalement réussi à débloquer le téléphone, mais, à terme, une solution envisagée par les autorités est que les logiciels de chiffrement soient dotés d'une trappe donnant accès, en cas d'enquête, aux informations cryptées. Sont ainsi posées de nombreuses questions sur la protection de la vie privée, mais aussi sur les moyens techniques qui offriraient un compromis. L'éclairage de David Pointcheval, directeur de recherche au CNRS, directeur adjoint du département d'informatique de l'ENS et responsable de l'équipe Inria Cascade.

POUR LA SCIENCE

Le chiffrement semble omniprésent sur nos ordinateurs et nos téléphones portables. Quel en est le principe ?

DAVID POINTCHEVAL : Aujourd'hui, quand vous faites un achat en ligne ou que vous envoyez un courriel, les informations sont chiffrées pour des raisons de sécurité. En général, l'objectif est de protéger vos données d'un usage malhonnête. Mais on ne peut éviter que le chiffrement soit parfois un frein à une enquête, en protégeant les données d'une personne ayant des activités criminelles.

Pour comprendre les enjeux du conflit entre Apple et le FBI, il faut présenter les deux types de chiffrement, l'un dit symétrique et l'autre asymétrique. Le premier sert, par exemple, à chiffrer les données sur votre appareil. Il est la version moderne des codes utilisés par le passé : le mécanisme qui transforme vos données en un code illisible utilise une clé que vous êtes le seul à détenir. Et cette même clé sert à retraduire vos données en clair. Si vous voulez communiquer un message chiffré à un interlocuteur, celui-ci doit aussi détenir la clé de déchiffrement. Or, en général, vous ne partagez pas un tel secret avec le destinataire.

En 1976, les Américains Whitfield Diffie et Martin Hellman ont trouvé une solution (pour laquelle ils viennent de recevoir le prix Turing, l'équivalent du prix Nobel en informatique) : le chiffrement asymétrique. La méthode comprend deux clés, l'une privée et l'autre publique. Le destinataire d'un message à chiffrer vous envoie sa clé publique, que vous utilisez pour coder le message. Mais seule la clé privée du destinataire peut déchiffrer ce dernier.

L'algorithme RSA (du nom de ses inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman) met en œuvre ce chiffrement asymétrique. La clé publique y est un nombre très grand, produit de deux nombres premiers. La clé privée est formée justement par ces deux nombres premiers. La sécurité du système est fondée sur le fait que trouver les facteurs premiers à partir de la clé publique prendrait beaucoup trop de temps.

PLS

Quelle est la robustesse de ces méthodes de chiffrement ?

D. P. : L'algorithme symétrique standard AES *(Advanced Encryption System)* impose que les clés du chiffrement soient d'au moins 128 bits, soit environ 30 caractères. L'attaque classique consiste en une énumération exhaustive des combinaisons possibles. Pour donner une idée, une clé de 256 bits représente autant de combinaisons qu'il y a d'atomes dans l'Univers observable. D'autres types d'attaques ont été tentés, mais aucune n'a mis AES en défaut, pour l'instant.

Pour l'algorithme RSA, certaines attaques sont plus performantes que l'énumération exhaustive. Il y a quinze ans, on recommandait d'utiliser une clé de 150 chiffres (décimaux) ; elle est maintenant de 600 chiffres, afin que le temps de calcul requis pour trouver les facteurs premiers reste hors de portée.

Le point faible des systèmes de chiffrement se situe souvent au niveau du logiciel qui réalise le chiffrement. Par exemple, en 2013,