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,

© Pour la Science - n° 463 - Mai 2016

lorsque Edward Snowden a annoncé que la NSA (l'Agence américaine de sécurité) récoltait des données sur les citoyens américains en outrepassant ses prérogatives, un des programmes de la NSA exploitait des failles présentes dans certains logiciels de chiffrement. L'agence est obligée d'utiliser ce genre d'approches car, malgré ses moyens informatiques, elle ne parvient probablement pas à casser le code symétrique ou à factoriser les clés publiques du RSA.

PLS

Avec les révélations d'Edward Snowden, les gens se sont demandé comment mieux protéger leur vie privée. Quelle a été la réponse des grands groupes informatiques tels que Google ou Apple ?

© shutterstock.com/Suwin

DANS LE CONFLIT QUI OPPOSE APPLE AU FBI, le second voudrait que le groupe informatique développe un logiciel pour accéder aux données chiffrées d'un téléphone. Apple refuse, dans la mesure où un tel logiciel affaiblirait la protection de la vie privée des utilisateurs.

D. P. : Une autre technique d'écoute de la NSA était de se brancher directement sur les serveurs des grands opérateurs américains de téléphonie ou d'Internet. Les données y sont chiffrées par l'opérateur (et non par l'utilisateur) au cas où une personne malveillante s'introduirait sur les serveurs. La NSA a eu accès aux clés de déchiffrement des opérateurs – avec ou sans leur aide, difficile de le savoir –, elle avait alors accès aux données de tout le monde.

Les grands groupes ont compris qu'ils devaient s'extraire de la chaîne de chiffrement des données pour éviter une telle situation et ainsi améliorer la sécurité des données des utilisateurs. De fait, les dernières versions des iPhone et des téléphones Android permettent aux utilisateurs de chiffrer leurs données sur le téléphone avec une clé qu'Apple, par exemple, ne connaît pas.

Les autorités ne peuvent plus solliciter l'opérateur pour déchiffrer les données sur le téléphone. C'est une partie du problème qui opposait Apple et le FBI. Par ailleurs, les iPhone sont dotés d'un système qui efface toutes les données si le mot de passe est entré de façon erronée dix fois de suite, une option qui empêche le FBI de s'attaquer au téléphone sans risquer de perdre les données.

Apple, qui a coopéré par le passé avec les autorités dans des situations similaires, refuse aujourd'hui de fournir son aide. Le constructeur explique que le logiciel qui devrait être développé pour accéder aux données menace de façon générale la vie privée des utilisateurs d'appareils iPhone. L'enjeu de ce contentieux est celui des logiciels de chiffrement munis d'une trappe, c'est-à-dire un accès utilisable par les autorités pour contourner le cryptage et accéder aux données.

PLS

La plupart des industriels soutiennent Apple. Une voix qui détonne est celle d'Adi Shamir. Quels sont ses arguments ?

D. P. : Selon Adi Shamir (le S dans RSA), Apple devrait collaborer dans ce cas précis. D'abord, le tueur étant mort et clairement coupable, sa vie privée n'est pas à défendre.

Il y a aussi un argument technique. Depuis la version 8 du système d'exploitation des téléphones Apple, les données sont chiffrées sur le terminal avec une clé inconnue d'Apple. Mais d'après Adi Shamir, Apple aurait les moyens de désactiver l'effacement après dix codes de déverrouillage erronés, rendant possible la recherche exhaustive des codes de déverrouillage sans endommager le contenu du téléphone. C'est cette dernière « trappe » qu'Adi Shamir souhaiterait qu'Apple n'ait plus les moyens d'utiliser. Apple ne pourrait alors plus aider le FBI.

Une trappe est une faille voulue dans le logiciel de chiffrement, une catastrophe en termes de sécurité

Dans le cas du téléphone du tueur de San Bernardino, le FBI a annoncé le 28 mars qu'il aurait débloqué le téléphone sans l'aide d'Apple. Néanmoins, la question fondamentale demeure. Il y aura certainement d'autres affaires avec des téléphones que le FBI ne saura pas décrypter et la question d'une trappe surgira de nouveau.

PLS

Quelles seraient les conséquences d'un système équipé d'une trappe ?

D. P. : Si l'État américain impose aux industriels de prévoir une trappe dans les systèmes de chiffrement, ce sera catastrophique. Tous les spécialistes de la cryptographie s'accordent à dire que c'est une très mauvaise solution. Une trappe est une faille volontairement installée dans le logiciel de chiffrement. Comment garantir qu'elle sera bien protégée de toute intrusion non officielle ? Cette trappe serait évidemment munie d'une clé détenue par le FBI, mais comment cette agence assurera-t-elle que la clé ne tombe pas entre de mauvaises mains ?

Par ailleurs, une fois que les États-Unis auront imposé aux opérateurs la mise en place d'une trappe, tous les autres gouvernements exigeront la même chose. Autant de risques de voir des fuites et de mauvaises utilisations de ces trappes. Cela ne menacera pas seulement les données des criminels, mais aussi la vie privée de tout le monde.