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.