Sécurité : Android n'arrive toujours pas au niveau d'iOS

Même s'il a connu une mise à jour de ses techniques de chiffrement à l'occasion de la sortie de la version Nougat, Android n'arrive toujours pas au niveau de la sécurité d'iOS. C'est en tout cas la conclusion de Matthew Green, spécialiste reconnu de cryptographie et professeur à l'université John Hopkins. Pour le chercheur, si l'OS de Google est « *clairement en train d'aller dans la bonne direction* », le compte n'y est pas. Il estime que Mountain View continue à considérer le chiffrement comme une priorité relativement secondaire : « *Cela pourrait contribuer à garder le FBI à distance de Google, mais, sur le long terme, c'est une erreur de jugement de la part de l'entreprise* », raille Matthew Green.

Pour bien comprendre les griefs du scientifique, il faut revenir à l'architecture même des systèmes de chiffrement. Deux designs principaux cohabitent : le chiffrement de disque (comme TrueCrypt ou BitLocker) où on chiffre l'ensemble des secteurs du support de stockage, et le chiffrement par fichier, qui fournit un contrôle plus granulaire de l'information protégée, mais nécessite une modification du système de fichier lui-même.

Android Nougat passe au chiffrement par fichier

Sur ses versions 4.4 (KitKat) et 6.0 (Marshmallow), Android reposait sur un système de chiffrement au niveau disque (Full Disk Encryption ou FDE), une approche en vogue sur les PC. « *Le problème, c'est qu'un smartphone n'est pas un PC* », relève le professeur du département d'informatique de la John Hopkins University. Tout simplement parce ces terminaux sont rarement éteints, ce qui signifie que la clef de chiffrement demeure en mémoire vive, y compris quand le téléphone est en veille (et que l'utilisateur doit entrer son code secret pour le rallumer). Ce qui permet donc à un assaillant d'accéder aux données, une fois passée l'étape de déverrouillage du terminal. « *En principe, une implémentation intelligente peut éviter de placer des clefs de chiffrement sensibles dans la Ram quand le terminal est verrouillé, et ensuite redélivrer ces clefs (autrement dit les recréer, NDLR) quand l'utilisateur se reconnecte* », détaille le chercheur. Mais, pour des questions de confort d'usage (un tel choix impliquerait que le système perde l'accès à toutes les données en veille), ce n'est pas ce que fait Android.

Bref, Android reposait jusqu'à sa version 6.0 sur une approche assez basique du chiffrement, peu satisfaisante d'un point de vue de la sécurité. D'où la mutation vers un système de chiffrement par fichier initiée avec Android Nougat (ou 7.0). Ce nouveau mécanisme, appelé Direct Boot, permet au smartphone de chiffrer différemment les données en fonction de leur criticité et de leurs usages. « *L'avantage principal de ce nouveau modèle, c'est qu'il permet au téléphone d'accéder à certaines données même avant que vous entriez votre mot de passe* », écrit le chercheur. Concrètement, pour implémenter cette sécurité fichier par fichier, les développeurs Android ont deux options : dans le premier cas, les données sont chiffrées tant que le code de déverrouillage n'est pas saisi, dans le second cas, elles ne le sont pas.

iOS retire la clef de la Ram au verrouillage

Une avancée ? Indéniablement. Mais, pour Matthew Green, le compte n'y est toujours pas. A l'appui de sa démonstration, le professeur à l'université John Hopkins se lance dans une comparaison avec iOS, qui fournit de son côté aux développeurs non pas 2 classes de chiffrement, mais 4. Dont un mode appelé 'protection complète', dans lequel la clef de chiffrement est retirée de la Ram quelques secondes après le verrouillage de l'appareil. S'y ajoute une approche permettant de créer des fichiers chiffrés même quand la clef a été retirée de la mémoire vive (via l'utilisation de clefs de chiffrement publiques). Ce qui permet par exemple à l'iPhone de prendre des photos de façon sécurisée même quand le terminal est verrouillé.

Pour Matthew Green, c'est précisément l'absence de ces deux catégories – et particulièrement de la première – qui est la source des insuffisances d'Android. D'autant que Google ne fournit ni directive aux développeurs pour retirer les clefs de la mémoire vive au verrouillage, ni même d'instruction claire indiquant aux applications que le système a été verrouillé. « *Le problème est que, tant que Google ne donne pas aux développeurs des directives appropriées, l'entreprise pourrait bien enfermer Android dans des années d'insécurité* », juge Matthew Green. Car, même si la future version de l'OS mobile (Android O) fournit un moyen de retirer les clefs de la mémoire vive au verrouillage, la base installée des apps ne sera pas en mesure de l'implémenter.

Bypasser l'écran de verrouillage

Notons toutefois que les limites pointées par Matthew Green ne laissent entrevoir qu'une surface d'attaque circonscrite, que le chercheur résume de la façon suivante : « S*i vous trouvez un moyen de bypasser l'écran de verrouillage, vous pouvez accéder aux fichiers présents sur le disque.* » Pour y parvenir, la solution la plus sûre réside probablement dans une attaque matérielle, nécessitant un accès physique au terminal. Des organisations, disposant de moyens importants (comme des services d'enquête ou de renseignement) et capables d'accéder physiquement à la Ram ou au bus de données des terminaux, trouveront dans les faiblesses d'Android un chemin assez aisé pour accéder aux informations stockées sur les smartphones.

Une attaque logicielle semble plus difficile à mettre en œuvre, car elle devrait trouver une façon de bypasser à distance le système de verrouillage. Mais, là encore, Matthew Green relève un choix étonnant de la part de Google : celui de stocker les clefs non pas dans le noyau (ce qui pousserait un assaillant ayant contourné le système de verrouillage à trouver ensuite une façon d'élever ses privilèges), mais dans un *daemon*, qui tourne comme un utilisateur standard du système. « *Ceci ne rend pas les exploits triviaux, mais ce n'est certainement pas la meilleure façon de gérer cette question* », raille le chercheur. Une nouvelle confirmation d'une certaine forme de négligence de la part de Google. A moins que Mountain View n'ait fait ces choix sciemment afin de s'épargner une opposition frontale aux autorités, comme celle qui avait opposé Apple au FBI au sujet du déchiffrement d'un iPhone ayant appartenu à un des auteurs de la tuerie de San Bernardino.

A lire aussi :

iOS 10 : les sauvegardes sont à la portée des hackers

Message au FBI : hacker un iPhone ne coûte que 100 dollars

Le chiffrement des smartphones Android n’est pas incassable