Le chiffrement des smartphones Android incassable ?

Le chiffrement des smartphones Android incassable ?

Un chercheur en sécurité décrit comment faire sauter la protection par chiffrement des données sur les smartphones Android équipés de puces Qualcomm.

Chiffrer l'ensemble de ses données sur un support de stockage est un bon moyen de les protéger en cas de perte ou vol du dit support. Néanmoins, il n'est pas infaillible. Particulièrement sur les smartphones Android équipés de processeurs Qualcomm. C'est ce que démontre le chercheur en sécurité Gal Beniamini. Dans un document très détaillé, il indique comment contourner les systèmes de protection. Et plus particulièrement, *« comment l'exécution du code TrustZone du noyau peut être utilisé pour briser efficacement le schéma de l'Encryption Full Disk d'Android »*, précise le chercheur.

Le Full Disk Encryption (FDE), la technique de chiffrement du disque d'Android, est proposé par Google depuis la version 5.0 de l'OS mobile. Il permet de générer des clés de chiffrement maître et esclave de 128 bits. La clé maître, également appelée DEK (pour Device Encryption Key) est protégée par chiffrement à partir du mot de passe, du code PIN ou du schéma de déverrouillage choisi par l'utilisateur. La DEK est stockée sur le smartphone (ou la tablette) dans un espace non chiffré de l'appareil, le *crypto footer*. Et c'est là que le problème survient. A cause d'une faille dans les processeurs de Qualcomm.

Utiliser une Trustlet

Pour comprendre pourquoi, il faut savoir que Android dispose, comme iOS, de mécanismes de temporisation et de blocage de l'appareil pour interdire les attaques par force brute (essais successifs de saisie des identifiants). Ces mécanismes sont liés au module KeyMaster qui s'exécute dans un environnement séparé de l'OS et considéré comme sécurisé, le Trusted Execution Environment (TEE). Le KeyMaster peut ainsi générer des clés de chiffrement sans les révéler au système d'exploitation. Une fois générées, ces clés sont à leur tour chiffrées et communiquées à l'OS. Quand ce dernier les sollicite, un bloc de données (le Blob, Binary Large OBject, un type de données qui permet l'intégration d'un pilote, souvent propriétaire, dans le code du noyau Linux) est fourni au KeyMaster sous forme d'une clé RSA de 2048 bits.

Mais le KeyMaster dépend de l'implémentation qu'en fait le fabricant sur son matériel. En l'occurrence, Qualcomm exploite bien le KeyMaster dans la TrustZone. Sauf que le TEE fourni par le constructeur, le QSEE (Qualcomm Secure ExecutionEnvironment), autorise des appliquettes (Trustlets) a s'exécuter dans cette zone sécurisée. Et, selon le chercheur, il est possible d'exécuter sa propre Trustlet dans la TrustZone en exploitant potentiellement une vulnérabilité Android. A partir de là, l'attaquant peut obtenir des privilèges administrateur et accéder au Blob qui contient les clés générées. Il ne reste alors plus qu'à lancer une attaque par force brute pour retrouver le code secret de l'utilisateur et disposer ainsi de la clé de déchiffrement du support de stockage.

Une correction difficile

Certes, la manœuvre n'est pas à la portée du premier venu. Et nécessite de disposer du terminal en main. Mais le déchiffrement d'un disque peut visiblement être exécuté par le fabricant des puces. Lequel peut avoir à se plier à une requête judiciaire comme on l'a vu avec Apple dans l'affaire de l'attentat de San Bernardino. Qui plus est, selon Qualcomm, le « bug » n'est pas facile à corriger. La correction demandera probablement une modification de l'architecture des processeurs. Lesquels équipent aujourd'hui une majorité de smartphones Android de la planète.

Néanmoins, le chercheur reste optimiste. *« J'espère qu'en jetant la lumière sur le sujet, cette recherche va motiver les équipementiers et Google à se réunir pour penser à une solution plus robuste pour le FDE*, écrit-il. *[…] Je crois qu'un effort concentré des deux côtés peut aider à rendre la prochaine génération d'appareils Android vraiment « inviolable ». »*

Article original de Christophe Lagane

Réagissez à cet article

Original de l'article mis en page : Le chiffrement des smartphones Android n'est pas incassable