Samsung Knox est-il aussi sûr que Fort Knox ?

Knox, le système de sécurité que Samsung propose sur ses smartphones, ne serait pas exempt de tout reproche. Sur un blog, un chercheur en sécurité met en lumière les insuffisances supposées de ce **système de conteneur censé créer une zone sécurisée** sur les terminaux mobiles du Coréen. Cette technologie est protégée par un mot de passe et un code PIN, ce dernier donnant accès à une fonction d'aide permettant à retrouver le mot de passe en cas d'oubli par utilisateur. Or, ce code PIN est stocké en clair sur le terminal dans un fichier nommé pin.xml, assure le blogueur certainement d'origine allemande.

Selon la démonstration de ce dernier, ce mécanisme pour retrouver un mot de passe oublié conduit à penser que **Samsung stocke aussi le mot de passe sur le terminal**. Et d'exhumer un fichier nommé containerpassword_1.key renfermant possiblement le sésame chiffré en AES. En utilisant des techniques d'ingénierie inversée, et malgré les tentatives de Samsung d'enterrer ces fonctions dans une multitudes de classes Java, le blogueur affirme que la clef de chiffrement dérive de l'identifiant Android propre à chaque terminal couplé à un chaîne de caractères codé en dur.

Une clef généré par un nombre aléatoire ?

« *Pour un produit appelé Knox, j'aurais espéré une approche différente*, pointe le blogueur. *La clef devrait dériver d'une fonction de type PBKDF2 (Password-Based Key Derivation Function 2) qui génère des clefs plus fiables avec un meilleur caractère aléatoire. Le fait que Samsung emploie une clef persistante uniquement pour une fonction permettant à l'utilisateur de retrouver son mot de passe compromet complètement la sécurité du produit. Pour un produit de ce type, le mot de passe ne devrait jamais être stocké sur le terminal.* »

Samsung s'est défendu en arguant d'abord que l'analyse porte sur une version ancienne (certes mais livrée sur le smartphone Galaxy S4, remarque le blogueur) et ensuite que **les conclusions sont « *incorrectes* » pour les solutions d'entreprise Knox**. Selon le constructeur, le blogueur s'est également trompé dans la fonction générant la clef de cryptage : celle-ci dériverait bien du mot de passe de l'utilisateur et d'un nombre aléatoire. La démonstration du constructeur n'est toutefois pas totalement convaincante car elle semble s'appliquer à la seule version entreprise (Knox EMM) et non à la version étudiée par le blogueur anonyme (Knox Personal).

La polémique tombe au mauvais moment pour le Coréen, dont le système Knox vient tout juste de recevoir **l'approbation de la NSA** américaine pour la manipulation d'informations classifiées au sein de l'administration américaine.

A lire aussi :
Sécurité : Samsung déploie sa citadelle Knox 2.0
Smartphones : le coffre-fort Knox de Samsung affaibli par une faille