Un hacker montre comment pirater Samsung Pay

Samsung Pay est-il piratable ? La question est d'autant plus pertinente que le constructeur coréen livre désormais son application de paiement mobile en standard avec les Galaxy S7 et S7 Edge. Lesquels s'écoulent par dizaine de millions d'exemplaires dans le monde. Un nouveau vecteur massif d'attaque pour les pirates ?

C'est en tout cas le propos de Salvador Mendoza. A l'occasion des conférences de sécurité Def Con 24 et Black Hat à Las Vegas, le chercheur en sécurité a présenté sa méthode pour détourner le système de paiement sans fil d'un Galaxy S7. Dans plusieurs vidéos (ici et là), le chercheur démontre comment il réussit à détourner les tokens émis par Samsung Pay pour réaliser à son tour un paiement sur un distributeur de friandises. Il faut en effet savoir que Samsung s'appuie sur le framework Visa Token Service, à base de jetons d'identification uniques, pour sécuriser les paiements sans fil.

Une attaque sophistiquée

La méthode est toutefois loin d'être à la portée du premier hacker en herbe venu. Mais elle semble fonctionner. L'attaquant aura besoin d'un dispositif chargé de capter (discrètement) le signal émis par le smartphone lors d'un achat. Ce qui suppose de s'approcher suffisamment près de la victime au risque d'éveiller sa méfiance. Le token ainsi récupéré lors d'une transaction est alors utilisé pour générer un nouveau jeton d'identification. Lequel est à son tour implémenté dans un dispositif électronique (équivalent à une carte de paiement), à partir duquel il est visiblement possible de réaliser à nouveau des achats sans fil. Sans rien débourser évidemment.

Samsung a répondu à cette démonstration. Le Coréen attire l'attention sur le fait que son application de paiement *« n'utilise pas l'algorithme revendiqué dans la présentation faite lors de la Black Hat pour chiffrer les informations d'identification de paiement ou générer des cryptogrammes »*. Néanmoins, dans une FAQ, le constructeur reconnaît que la possibilité *« qu'un fraudeur exploite un jeton [précédemment capturé] sur un lecteur de carte bancaire pour réussir une transaction est extrêmement improbable »*. Donc pas totalement impossible.

Lire également
Samsung veut faire de l'ombre à Apple Pay
Vaste arnaque à l'Apple Pay aux Etats-Unis
Enquête : Le paiement mobile NFC sécurisé, vraiment ?