iPhone 5s : le lecteur d'empreintes digitales déjà piraté

Pas plus que d'autres scanners d'empreintes digitales, le capteur intégré au tout nouveau iPhone 5s ne résiste aux techniques de piratage.

Dans une vidéo, le Chaos Computer Club (CCC), une association de hackers européens, montre que la technique consistant à photographier le doigt de l'utilisateur, à inverser l'image, à l'imprimer sur une feuille transparente ensuite collée sur un moulage de doigt fonctionne également sur la technologie dévoilée par Apple.

Si la technique du CCC requiert minutie et expérience en la matière, elle reste des plus classiques. « *Une empreinte de l'utilisateur, photographiée sur une surface en verre, a suffi à créer un faux doigt permettant de débloquer un iPhone 5s sécurisée par TouchID (le nom de la technologie biométrique d'Apple, NDLR)* », s'amuse le club de hackers dans un billet de blog.

« les fausses promesses de la biométrie »

« *Cela démontre, une fois de plus, que l'empreinte digitale ne convient pas aux applications de contrôle d'accès* », ajoute le CCC, qui se moque de la prétendue sécurité offerte par le dernier smartphone de la pomme.

« *En réalité, le capteur d'Apple a simplement une meilleure résolution que les capteurs utilisés jusqu'à présent. Nous avons juste été obligé d'augmenter la résolution de notre faux* », raille le CCC. Les hackers ont ainsi réalisé une photo de l'empreinte en 2400 dpi et imprimé le faux en 1200 dpi.

« *Les utilisateurs ne doivent plus se laisser abuser par les fausses promesses de sécurité distillées par les industriels de la biométrie*, explique **Franck Rieger**, un porte-parole du CCC. *La biométrie est fondamentalement une technologie pensée pour l'oppression et le contrôle, pas pour sécuriser l'accès au quotidien à un terminal*. »

Voir aussi

Quiz Silicon.fr – 10 questions sur les iPhone 5s et 5c