Le schéma de verrouillage des mobiles Android piratable par vidéo

Vous pensez l'accès à votre smartphone Android protégé en activant le schéma de déverrouillage ? Rien n'est moins sûr. Selon des universitaires anglais et chinois, il est possible de déterminer le schéma de déverrouillage d'un utilisateur en scrutant ses gestes filmés par vidéo à plusieurs mètres de distance.

A cette distance il est quasiment impossible de visionner précisément le chemin tracé sur l'écran (jusqu'à 10 points de jonction) pour déverrouiller l'appareil comme pourrait le faire une personne indiscrète par-dessus l'épaule de sa victime. Mais quelques algorithmes bien sentis d'analyse des mouvements permettent de reconstituer le schéma sans même que la caméra soit nécessairement pointée directement sur l'écran du smartphone.

Plus le schéma est complexe, plus il est facile à pirater

Selon les scientifiques des universités de Lancaster et Bath au Royaume-Uni et de la Northwest University en Chine, un attaquant peut discrètement filmer une action de déverrouillage depuis son smartphone avant de la faire analyser par des logiciels spécialisés. En analysant la position de l'écran du téléphone et les mouvements digitaux de l'utilisateur, un algorithme de vision est capable de recalculer le schéma de déverrouillage de l'appareil. Sur les 120 essais effectués sur des schémas créés par 215 utilisateurs indépendants, le logiciel mis au point par les chercheurs a réussi à reconstituer le précieux Sésame la plupart du temps. Autrement dit, la formule fournie par le système était la bonne parmi les 5 essais qu'Android autorise avant de bloquer l'accès au smartphone.

Paradoxalement, les chercheurs avancent que plus le schéma est complexe, mieux il est reconstitué par leur logiciel. En fait, plus grand est le nombre de mouvements effectués par l'utilisateur et plus l'algorithme est en mesure de déterminer la position des points pour reconstruire le dessin de déblocage. Un seul schéma a résisté à leurs essais. Soit un taux de succès de 97,5%. Contre 87,5% de succès pour les dessins moyennement complexes et 60% pour ceux considérés comme faciles à reproduire (4 points à relier au minimum).

Jusqu'à 9 mètres

Selon les travaux des scientifiques, une vidéo capturée depuis un smartphone jusqu'à 2,5 mètres sera utilement exploitable par le logiciel mis au point pour la démonstration. Et jusqu'à 9 mètres si la scène est filmée depuis un appareil photo numérique doté d'une fonction d'enregistrement vidéo. Des appareils sommes toutes des plus banals dans un environnement public comme la rue,

les transports publics, les lieux de restauration… Une méthode de piratage, parmi d'autres, qui nécessite néanmoins l'accès physique au smartphone pour en tirer les bénéfices. Face à ce risque, l'identification par lecture de l'empreinte digitale s'avère plus pertinente.

Lire également

Android en tête des vulnérabilités de sécurité référencées en 2016
Switcher, le malware Android qui s'attaque aux réseaux Wifi
Le malware Gooligan terrorise des millions de terminaux Android