Les capteurs des smartphones sont de vrais mouchards

Ceux qui pensent parvenir à se protéger en refusant de partager leur géolocalisation, leur nom et toutes autres informations personnelles, vont apprendre que toute tentative est vaine dès lors qu'ils utilisent un smartphone. On ne parle pas ici d'écoutes mais **d'empreintes spécifiques pour chacun des capteurs dont sont bardés les smartphones**.

Les capteurs ont une signature unique

Ce sont des chercheurs des universités de l'Illinois, de Caroline du Sud et de Zhejiang qui l'indiquent dans un rapport. Avant sa publication, l'équipe avait présenté ses recherches au *Network and Distributed System Security Symposium* en février dernier à San Diego.

En substance, **le rapport indique que malgré toute tentative de standardisation et de contrôle qualité des capteurs, ceux-ci présentent des imperfections uniques**. Elles permettent non seulement d'identifier le composant (référence du capteur) mais représentent donc également **une signature pour chaque smartphone**. Cette signature est de surcroît indélébile car non aliénée aux logiciels qui exploitent les-dits capteurs.

« *Même si vous effacez l'application dans le téléphone, ou encore effacez et réinstallez tous les logiciels, l'empreinte reste toujours présente,* » déclare **Romit Roy Choudhury**, le professeur agrégé qui a dirigé l' équipe de recherche. » *C'est une menace sérieuse.* »

Un véritable identifiant

Les données enregistrées par les accéléromètres de 100 capteurs différents ont ainsi présenté des différences certes minimes mais uniques. Ces différences permettraient d'identifier un accéléromètre avec une précision de 96%.

De surcroît, si l'équipe s'est penchée sur le cas des accéléromètres, celles enregistrées par les gyroscopes, magnétomètres, microphones, capteurs CMOS des caméras et autres capteurs contiennent également des marqueurs uniques qui permettent d'identifier un smartphone. E**n examinant les données issues de deux capteurs, la précision dans l'identification peut donc se rapprocher de 100%**.

Sanorita Dey, une étudiante diplômée de l'Université de l'Illinois et membre de l'équipe de recherche, ajoute : » *Nous n'avons pas besoin de connaître d'autres informations sur le téléphone – ni le numéro de téléphone ou celui de la carte SIM. Simplement en regardant les données, nous pouvons vous dire de quel appareil ça vient.* ***C'est presque un autre identifiant*** . »

Dès lors, **des applications malveillantes peuvent parfaitement collecter les données et les exploiter pour vous identifier** (via le smartphone que vous utilisez) et vous « suivre ».

L'**Internet des Objets** largement basé sur des capteurs est **logé à la même enseigne**.

crédit photo © Lisa S. – shutterstock

A lire aussi :

Le Raspberry Pi au secours de la protection de la vie privée

Vie privée : l'iPhone traque ses utilisateurs