# Des chercheurs piratent Siri et Google Now sans un mot

« Vous ne m'entendez pas ; votre téléphone, si ». C'était l'intitulé de l'une des conférences organisée le 18 juin dernier dans le cadre de l'événement Hack in Paris, dédié à la sécurité informatique.

La démonstration réalisée par José Lopes Esteves et Chaouki Kasmi était passée relativement inaperçue. Les deux chercheurs employés de l'ANSSI étaient pourtant parvenus à prendre le contrôle d'un iPhone sous iOS 8 en exploitant les fonctions de commande vocale… sans dire un mot.

Applicable à d'autres assistants vocaux que Siri, leur technique refait l'actualité à la faveur d'une republication par l'IEEE (Institute of Electrical and Electronics Engineers). Décrite dans un document PDF de 40 pages, elle est exploitable sur les téléphones associés à une paire d'écouteurs filaires avec microphone intégré.

Les écouteurs font office d'antenne, comme lorsque l'on écoute la radio FM. C'est par ce biais que les deux chercheurs ont envoyé des signaux électromagnétiques (sur la bande VHF, en utilisant le filtre passe-bas), interprétés par le système d'exploitation comme des commandes vocales venant du microphone.

Ce hack a été réalisé avec un PC équipé du logiciel Open Source GNU Radio, couplé à une carte d'interface USRP (Universal Software Radio Peripheral) additionnée d'un amplificateur et d'une antenne.

## Le ciel comme seule limite

Sous sa forme la plus simple, l'ensemble tient dans un sac à dos et offre une portée d'environ 2 m. Suffisant a priori pour causer des dégâts dans un lieu public. Il existe une configuration plus évoluée opérationnelle jusqu'à 5 m de distance, mais elle est plus volumineuses (on l'installera par exemple dans l'habitacle d'une voiture).

L'expérimentation, réalisée dans une cage de Faraday en respect de la loi française interdisant l'exploitation sans licence de certaines fréquences radio, a permis, sur plusieurs terminaux, d'activer les interfaces de communication sans fil, d'envoyer des SMS vers des numéros surtaxés, d'espionner l'environnement sonore via le microphone ou encore d'ouvrir des sites Web malveillants, selon ITespresso.

La manipulation est plus difficile avec Google Now, qui, sur de nombreux smartphones Android, n'est souvent pas accessible lorsque l'écran est verrouillé. Il est, en outre, parfois programmé pour ne réagir que lorsqu'il reconnaît la voix de l'utilisateur.

Sur iPhone, en revanche, aucune de ces deux protections n'est active par défaut. Dire « Hey Siri » sur l'écran de verrouillage est suffisant. Sur les anciennes versions du système d'exploitation, José Lopes Esteves et Chaouki Kasmi ont pratiqué la rétroingénierie pour pouvoir reproduire le signal

électromagnétique émis par les écouteurs Apple lorsqu'on appuie sur le bouton destiné à activer Siri.

Conclusion des deux chercheurs : « *Le ciel est la seule limite. Tout ce qu'on peut faire par la voix, on peut le faire à distance par les ondes électromagnétiques* ». Ils recommandent donc de débrancher les écouteurs quand ils ne sont pas utilisés, de n'activer les commandes vocales que si besoin, de personnaliser les mots-clés « Hey Siri » et « OK Google », de limiter le nombre de commandes exploitables et si possible de réduire la sensibilité du microphone.

**A lire aussi :**

Apple serait prêt à intégrer Siri sur Mac OS X

Le moteur de Siri, Nuance, bientôt propriété de Samsung ?