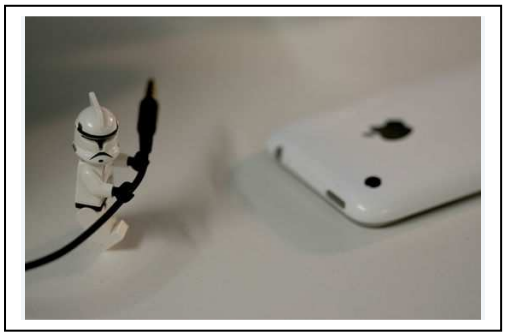
Les kits mains libres, porte d'entrée pour pirater les téléphones mobiles

Le Monde.fr | 26.10.2015 à 15h03 • Mis à jour le 26.10.2015 à 15h36 | Par **Yves Eudes**



Lorsque vous branchez vos écouteurs sur votre smartphone pour passer un appel, pourdicter un SMS ou pour écouter de la musique, vous ouvrez sans le savoir une porte dérobée, qui peut permettre à un hackeur de pénétrer subrepticement dans votre appareil. Deux chercheurs de l'Agence nationale des systèmes informatiques (Anssi) ont réussi à « parler » à distance à un téléphone, grâce à des ondes radios transmises via le câble d'un kit main libre.

Le cordon de ces kits possède en effet plusieurs fonctions : il transmet les sons depuis le téléphone vers l'oreille, achemine la voix depuis le micro vers le téléphone, et agit comme une antenne radio externe – permettant par exemple d'écouter une station FM. Par ailleurs, les smartphones récents sont dotés de systèmes de reconnaissance vocale permettant de poser des questions ou de donner des ordres (« appelle le service comptabilité », ou « quel temps fera-t-il demain à Marseille ? ») : Siri pour Apple, S-Voice pour Samsung, Cortana pour Microsoft, Google Voice Search…

Signal pirate

En théorie, il est donc possible d'envoyer une onde radio contenant un message qui sera capté et transmis par le cordon, puis interprété par l'appareil comme s'il s'agissait d'une commande prononcée par une voix humaine. Deux chercheurs de l'Anssi, José Lopes Esteves et Chaouki Kasmi, ont tenté l'expérience dans leur laboratoire parisien, et ont réussi sur toute la ligne.

Pour cela, ils ont dû s'outiller : en plus de leurs ordinateurs, ils ont eu besoin d'une *software radio* capable d'émettre sur différentes fréquences – en vente libre dans le commerce pour quelques centaines d'euros –, d'une grosse antenne et d'un appareil de mesure de l'intensité du signal. Ils ont émis leur signal pirate sur la fréquence 103 FM, idéale pour le type de câble utilisé lors de l'expérience. Dès lors, « *il ne reste plus qu'à injecter un signal sonore correspondant à de la voix et contenant la commande vocale souhaitée* »

Accès au navigateur, installation de virus…

Les deux chercheurs ont ainsi pu passer des appels vers un numéro surtaxé, ouvrir le micro, déclencher une communication pour entendre les conversations environnantes, activer les interfaces permettant de suivre l'utilisateur à la trace, et connecter le navigateur Internet de l'appareil sur une page Web contenant un logiciel malicieux, pour voler les données contenues dans le téléphone, y déposer des virus, etc.

L'attaque initiale peut se faire directement, car le plus souvent, la reconnaissance vocale est activée par défaut sur les smartphones. Mais si l'utilisateur l'a désactivée, ce n'est pas grave : il suffit d'envoyer par radio la commande d'activation (équivalent à une pression prolongée sur le bouton de l'appareil), qui fonctionnera même si le téléphone est verrouillé.

Dans leur compte rendu d'expérience, les deux chercheurs se placent dans un contexte géostratégique plus vaste : *« L'intérêt des sources à énergie dirigée dans les applications militaires a largement été démontré afin de perturber voire détruire des systèmes électroniques. »* Ils rappellent aussi que de nombreux experts en sécurité se méfient des systèmes de reconnaissance vocale : dès 2012, aux Etats-Unis, la société IBM a ordonné à sesemployés possesseurs d'iPhones de désactiver Siri.

« Des attaques subtiles »

Vincent Strubel, sous-directeur de l'expertise à l'Anssi, va plus loin : *« Nous devons prendre en compte ce type de menace dans notre stratégie dedéfense, même si on ne connaît pas d'exemple à ce jour – sauf dans les films de Hollywood. Nous voulons que les fabricants de matériel réfléchissent à ce type de risque émergent. Notre expérience sur les cordons de téléphone est une application rigolote de ce qui est faisable. Avec des émissions de faible puissance, on peut faire des attaques subtiles, et pas seulement bêtement destructrices. »*

Pour éviter ce genre d'intrusion, vous pourrez peut bien sûr cesser d'utiliser vos kits mains libres – si vous êtes prêts à ce sacrifice. Sur ce point, MM. Esteves et Kasmi sont réalistes : *« Malheureusement, il y a un compromis à faire entre la sécurité et l'ergonomie que proposent ces services. »*

- **Yves Eudes**
  Grand reporter