Par Marc Zaffagni, Futura

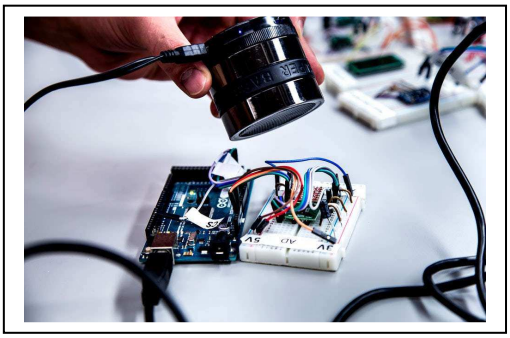
Publié le 18/03/2017

Grâce à une technique d'attaque utilisant des ondes sonores, des chercheurs ont réussi à perturber le fonctionnement des accéléromètres — ces capteurs présents dans de nombreux appareils électroniques — et à en prendre le contrôle. Une méthode qui pourrait potentiellement servir à pirater des smartphones voire des voitures autonomes.

Des ondes sonores pourraient être exploitées pour pirater les capteurs qui équipent nos smartphones, nos bracelets d'activité, certains équipements médicaux, des objets connectés et même des voitures autonomes. C'est ce qu'affirment des chercheurs de l'université du Michigan (États-Unis), démonstrations à l'appui. Sous la houlette du professeur Kevin Fu, spécialiste en informatique et ingénierie, ils ont trouvé le moyen d'exploiter un point faible sur les accéléromètres (la vulnérabilité de ces capteurs a déjà fait l'objet de plusieurs articles sur Futura ; voir notamment notre article Un smartphone pourrait espionner nos frappes sur un ordinateur).

Les accéléromètres utilisés dans les appareils électroniques fonctionnent avec un système de masse montée sur ressort qui mesure l'accélération linéaire de l'objet. En général, les appareils mobiles sont équipés d'accéléromètres à trois axes afin d'obtenir des relevés en trois dimensions. Ces informations sont numérisées puis transmises au système d'exploitation et aux logiciels qui en ont besoin.

C'est ainsi, par exemple, que le terminal détermine l'orientation de l'affichage en mode portrait (vertical) ou paysage (horizontal) selon le sens dans lequel l'utilisateur le tient. Nombre d'applications mobiles exploitent les accéléromètres pour permettre de contrôler l'action avec des mouvements. Il est même possible de piloter un drone de cette manière avec un smartphone.



Pour fonctionner, le piratage d'un accéléromètre par ondes acoustiques doit se faire à distance très courte. Durant leurs essais, les chercheurs de l'université du Michigan ont travaillé à 10 cm de la cible. © Joseph Xu, Michigan Engineering

Trouver la fréquence de résonance de l'accéléromètre

Or, il s'avère que les masses de ces accéléromètres sont sensibles à la pression générée par des ondes acoustiques. À la manière du chanteur d'opéra qui parvient à briser un verre en trouvant sa fréquence de résonance, les chercheurs ont réussi à identifier la fréquence de résonance propre à 20 modèles d'accéléromètres fabriqués par 5 marques.

Partant de là, il leur a suffi d'envoyer un signal sonore pour leurrer le capteur et le forcer à transmettre des informations sur des mouvements factices. L'accéléromètre devient alors une sorte de porte dérobée (*backdoor*, en anglais) qui permet de prendre le contrôle d'un terminal pour lui faire accomplir des actions ou fausser son fonctionnement.

Pour illustrer sa découverte, l'équipe du professeur Kevin Fu a réalisé plusieurs expériences de piratage assez étonnantes. À l'aide d'un haut-parleur du commerce à 5 dollars (4,70 euros au cours actuel) diffusant le signal sonore adéquat, ils ont trompé un bracelet connecté de la marque Fitbit en lui faisant enregistrer des milliers de pas totalement fictifs (voir la vidéo ici). Les chercheurs ont aussi modifié un clip vidéo YouTube lu par un smartphone Galaxy S5 de Samsung pour y superposer un signal sonore épelant le mot « noyer » (*walnut*, en anglais) (voir la vidéo ici).

Une vulnérabilité pas encore exploitée par des pirates

Encore plus impressionnant, ils ont réussi à prendre le contrôle d'une application Android servant à piloter une voiture radiocommandée avec les mouvements du smartphone (voir la vidéo ici). Il a suffi d'un simple morceau de musique piégé et diffusé *via* le haut-parleur du mobile pour tromper l'accéléromètre et ainsi faire avancer et reculer la voiture alors qu'aucun mouvement physiquen'avait lieu au niveau du terminal.

L'article scientifique sera présenté le mois prochain lors de l'IEEE (*European Symposium on Security and Privacy*) qui se tiendra à Paris. Les experts de l'université ont indiqué qu'à leur connaissance, ce type d'attaque n'était pas exploité par des pirates. Il faut dire que cela requiert de se trouver à portée directe de l'accéléromètre et d'émettre un signal sonore de haute intensité (110 dB SPL), ce qui ne passerait pas inaperçu.

Les chercheurs adressent tout de même deux recommandations techniques à l'attention des fabricants :

- Tout d'abord, limiter l'exposition acoustique des accéléromètres à l'aide d'un isolant phonique.
- Ensuite, concevoir des algorithmes de traitement du signal qui soient capables de rejeter des informations proches de la fréquence de résonance du capteur.