Sécurité : toutes les Volkswagen peuvent être ouvertes sans clef

Nul doute que Volkswagen aurait préféré ne pas revoir de sitôt Flavio D. Garcia. Travaillant à l'université de Birmingham, cet ingénieur en informatique présente, lors de la conférence Usenix qui se tient du 10 au 12 août à Austin (Texas), les conclusions d'une étude (« Lock it and still lose it ») sur les télécommandes permettant l'ouverture des voitures de tourisme.

Des conclusions peu flatteuses pour le groupe automobile allemand : la quasi-totalité des véhicules qu'il a vendus ces 20 dernières années, près de 100 millions pour la seule période allant de 2002 à 2015, peuvent être déverrouillés sans clés… et sans plip, du nom de cette fameuse télécommande aujourd'hui livrée en standard avec la plupart des voitures de tourisme.

Flavio D. Garcia étudie depuis plusieurs années les vulnérabilités associées aux systèmes de commande à distance dans l'univers automobile. En 2012, il avait constaté, avec plusieurs collègues, que les récepteurs RFID Magamos Crypto, adoptés par de nombreuses marques de luxe, pouvaient être détournés non seulement pour ouvrir et fermer les portes, mais aussi pour faire démarrer le moteur, le tout sans disposer des clés.

Contacté par ses soins en mai 2013, Volkswagen avait déposé plainte, arguant qu'une publication de ces recherches exposerait ses véhicules à un risque accru de vol. La Haute Cour du Royaume-Uni lui avait accordé une injonction, retardant d'autant la publication, finalement effectuée il y un an et sous une forme très restreinte : une seule phrase, dans les annexes de la conférence Usenix, comme le souligne *Bloomberg*.

Arduino pour intercepter les données

Cette fois-ci, Flavio D. Garcia s'est épargné les considérations juridiques. Avec deux associés de l'université de Birmingham et la firme allemande Kasper & Oswald, il aborde deux vulnérabilités distinctes ; l'une concernant Volkswagen et l'autre applicable à une longue liste de constructeurs.

Point commun entre ces failles : elles sont fondées sur l'interception des données transmises par les télécommandes, qui fonctionnent sur les bandes de fréquence à 433 ou 868 MHz en Europe et 315 MHz en Amérique du Nord – à l'exception de quelques anciens systèmes basés sur la technologie infrarouge.

Pour intercepter les données envoyées par les télécommandes, les chercheurs ont fabriqué un module radio à partir d'une carte Arduino. Et se sont aperçus que, de manière générale, le niveau de protection des données dépendait de l'âge des véhicules. Sur des modèles du début des années 2000, il arrive qu'aucune méthode de cryptographie ne soit appliquée : un code unique est envoyé à chaque appui sur le(s) bouton(s) d'ouverture et de fermeture des portes. Sur des voitures plus récentes, des paramètres ont été ajoutés. Notamment un compteur incrémenté à chaque pression, permettant d'éviter qu'une commande soit exécutée deux fois.

Clonage des clefs

Mais, dans tous les cas, il est possible de déterminer la structure des paquets de données, d'autant plus que ceux-ci sont souvent transmis à plusieurs reprises, sans doute pour s'assurer que la communication aboutisse dans les environnements difficiles sujets à des interférences.

L'équipe de Flavio D. Garcia a identifié pas moins de 7 schémas de transmission. Parfois, le signal varie en amplitude ; d'autres fois, en fréquence. La quantité de données change elle aussi, au même titre que les algorithmes de chiffrement. Mais dans tous les cas, la sécurité peut être déjouée et la clé, clonée.

Cette opération de clonage ne peut toutefois se faire qu'une fois obtenue la clé logée dans le récepteur RFID de la voiture. Pour cela, les chercheurs en ont extrait le *firmware*. Et ont alors fait une sacrée découverte : cette « clé maîtresse » est la même sur des dizaines de millions de véhicules du groupe Volkswagen.

Mais aussi Nissan, Dacia, et Renault…

Sur la liste – non exhaustive – des modèles considérés comme vulnérables figurent les Audi A1, Q3, R8, S3 et TT, les Skoda City Go, Roomster, Fabia 1 et 2, Octavia, SuperB et Yeti, les Seat Alhambra, Altea, Arosa, Cordoba, Ibiza, Leon, MII et Toledo… ainsi que les Volkswagen Amarok, (New) Beetle, Bora, Caddy, Crafter, e-Up, Eos, Fox, Golf 4, 5 et 6, Golf Plus, Jetta, Lupo, Passat, Polo, T4, T5, Scirocco, Sharan, Tiguan, Touran et Up.

Dans le prolongement de ces conclusions, Flavio D. Garcia et consorts se sont intéressés aux circuits intégrés PCF7946 et PCF7947, que le fabricant de semi-conducteurs NXP fournit à de nombreux constructeurs automobiles, détaillent nos confrères de *ITespresso*.

Avec le même mode opératoire, ils sont ainsi parvenus à pirater une Fiat Punto, un Citroën Jumper, un Dacia Duster, une Renault Modus ou encore un Nissan Qashqai. Il leur a toutefois fallu ici pousser l'expérimentation plus loin, en interceptant plusieurs codes (4 à 8, d'après le rapport, car ces codes changent à chaque pression sur la télécommande) et en utilisant un ordinateur pour déchiffrer certaines données. En l'occurrence, une partie des 28 bits du compteur.

Une étape indispensable : sur un grand nombre de véhicules, la télécommande se bloque si ledit compteur, censé augmenter d'une unité à chaque appui, n'est pas synchronisé avec celui du récepteur RFID.

Des vols bien réels

Le déchiffrement prend moins de 10 minutes en exploitant les failles de HiTag2, un algorithme de cryptographie lancé il y a près de 20 ans et associé aux circuits intégrés PCF7946/7947. Pour intercepter plus rapidement le nombre de codes requis, les chercheurs ont bloqué la transmission des signaux afin que les utilisateurs ciblés pressent à nouveau le bouton de leur télécommande.

La principale limitation de la méthode imaginée par les chercheurs réside dans la portée des

télécommandes. Généralement quelques dizaines de mètres. Il faut donc impérativement se trouver dans ce périmètre. Dès lors, il est possible d'envisager d'autres scénarios d'attaque. Par exemple, une sorte de DDoS à partir du système de blocage de la télécommande.

Ces recherches permettent de mettre le doigt sur un phénomène en pleine explosion : aux États-Unis, les forces de l'ordre constatent de plus en plus de vols de voitures sans effraction. Les images de vidéosurveillance révèlent souvent l'utilisation d'un simple boîtier électronique. Ce mois-ci, une trentaine de Jeep ont ainsi été volées dans le Texas avec un simple ordinateur.

A lire aussi :

Pirater les voitures sans chauffeur en aveuglant leurs capteurs

Volkswagen choisit Mirantis pour construire son Cloud privé OpenStack

Logiciel Volkswagen : Bosch démasqué, mais se dédouane

Crédit Photo : Simone mescolini-Shutterstock