La panoplie du hacker pour voler une voiture connectée | Le Net Expert Informatique

La panoplie du hacker pour voler une voiture connectée

Interception de paquets wifi, brouillage de signal, détection de mots de passe… L'utilisation grandissante des technologies sans fil dans les automobiles multiplie les vecteurs d'attaque. Démonstration.

Depuis qu'elles deviennent connectées, les voitures aiguisent de plus en plus l'appétit des hackers. A l'occasion de la conférence DEF CON 23, le chercheur Samy Kamkar — connu pour ses bricolages hors du commun — a montré différentes techniques permettant de voler une voiture en toute discrétion.
Pour ses besoins d'étude, il s'est penché sur la Chevrolet Volt d'un ami. Comme beaucoup d'automobiles aujourd'hui, elle dispose d'une application mobile compagnon, fournie par le constructeur General Motors (GM) et baptisée OnStar RemoteLink MobileApp. Elle permet de localiser le véhicule, de vérifier certains paramètres techniques, de le déverrouiller, d'allumer ses phares, de klaxonner et même de le démarrer. Pour réussir cela, l'application mobile se connecte aux serveurs de GM qui eux feront le lien avec le véhicule, grâce à une connexion cellulaire.

L'application mobile utilise des connexions SSL, mais ne vérifie pas les certificats. Elle est donc vulnérable à des attaques de type « Man in the middle ». Samy Kamkar a fabriqué un boîtier tout-en-un basé sur Raspberry Pi capable de créer un hotspot wifi, d'usurper l'identité des serveurs de GM quand un utilisateur s'y connecte, d'extraire ses données d'accès (login et mot de passe) et de les renvoyer au pirate par une connexion cellulaire. L'appareil, baptisé « OwnStar », est totalement autonome. On peut donc la placer à proximité de la cible et attendre que la connexion se fasse.

Mais comment inciter la future victime à se connecter sur ce faux réseau wifi? « On peut utiliser un nom de réseau usuel tel que 'attwifi' (le réseau de hotspots de l'opérateur américain ATT, ndlr) qui sont utilisés par beaucoup de personnes. Si on l'on est à proximité de la cible, on peut également intercepter les requêtes de connexion que son smartphone envoie automatiquement. C'est un bon moyen pour connaître les hotspots sur lesquels il se connecte habituellement », explique le hacker. Contacté par M. Kamkar, GM a depuis mis à jour son application mobile.

Si la cible n'utilise pas d'applications mobiles, le hacker propose un autre vecteur d'attaque: la clé de contact. Souvent, celles-ci permettent désormais de déverrouiller une voiture à distance, au moyen d'un code envoyé par un bref signal électromagnétique. Ce code n'est pas chiffré, mais il est à usage unique: à chaque fois que l'utilisateur appuie sur le bouton, un nouveau code est envoyé, et celui-ci n'est accepté qu'une seule fois. L'intercepter n'apporte donc rien à priori… à moins de faire en sorte que le code n'arrive pas à destination. Samy Kamkar a créé un autre boîtier qui va brouiller le signal pour que la voiture ne puisse pas capter les messages de la clé de contact, tout en étant capable d'extraire le code que l'attaquant pourra utiliser ultérieurement pour déverrouiller la voiture.

Reste enfin un dernier petit obstacle: ouvrir le garage dans lequel la voiture est éventuellement garée. Là encore, il n'est pas rare qu'une porte de garage puisse s'ouvrir à distance, au moyen d'un d'un badge. En décortiquant ces badges, Samy Kamkar découvre qu'ils utilisent généralement un code de 8 à 12 bits. Ce qui fait au total 88.576 possibilités. C'est suffisamment bas pour tenter une attaque par force brute. Originalité de la manoeuvre: pour créer ses signaux, il utilise un jouet Barbie, le Mattel IM-ME, un joli petit boîtier rose pour envoyer des messages texte. « C'est un appareil très pratique. Il dispose d'un bon chipset, d'un écran, d'un clavier et en plus il a une jolie couleur », souligne Samy Kamkar.

Une fois l'appareil reprogrammé, le hacker n'a besoin que de 8 secondes pour essayer toutes les possibilités et ouvrir la porte de garage. Une belle performance qui s'appuie notamment sur l'algorithme de De Bruijn, une méthode qui permet de scanner plus rapidement un espace de valeurs.

Source : http://www.01net.com/actualites/def-con-23-la-panoplie-de-hacker-pour-voler-une-voiture-connectee-661671.html
Par Gilbert Kallenborn