Texas Instrument et le MIT élaborent une puce RFID inattaquable

Dans le développement des objets connectés ou plus couramment l'Internet des objets, les technologies réseaux se livrent une guerre sans merci. LoRa, Sigfox, WiFi, Bluetooth veulent en croquer et tirer bénéfice d'un marché en pleine expansion. Une autre technologie intéresse les chercheurs, le RFID (radio frequency identification). Pour rappel, il s'agit d'une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs. Ces derniers sont en général des étiquettes ou des puces que l'on trouve sur des produits (pour la traçabilité) ou sur des cartes de paiement (sans contact) par exemple. On comprend donc que la sécurité en soit un composant crucial.

Des chercheurs du MIT (Massachusetts Institute of Technology) et Texas Instrument ont élaboré des puces RFID ultra sécurisées pour éviter le piratage. Chiraag Jukevar, étudiant en génie électrique, explique que cette puce a été conçue à l'origine pour empêcher des attaques par canaux auxiliaires (**side-channel attacks**).

Une attaque en cache une autre

Ce type d'attaques est capable d'analyser les schémas d'accès à la mémoire ou d'enregistrer les fluctuations électriques d'un terminal lors d'une opération chiffrée afin de déduire la clé. Pour le chercheur, « *l'objectif d'une attaque par canal auxiliaire est de capter les bribes d'informations émises lors de l'exécution d'un algorithme de chiffrement. Si cette exécution se répète plusieurs fois, le pirate aura suffisamment d'éléments pour réunir les informations complètes* ».

Un des moyens pour freiner ce type d'attaques est de changer régulièrement les clés de chiffrement. Dans ce cas, la puce RFID fonctionne comme un générateur de nombres aléatoires capable de créer des nouvelles clés après chaque transaction. Il faut installer un serveur central disposant du même générateur pour valider la clé quand le lecteur RFID envoie une requête. Cependant, cette méthode est vulnérable à une attaque dite « **power glitch** » (panne électrique) qui consiste à couper l'alimentation de la puce RFID avant la modification de la clé. Un cybercriminel pourrait alors exécuter la même attaque par canaux auxiliaires des milliers de fois avec la même clé. Le chercheur souligne que les puces RFID sont particulièrement sensibles aux attaques par coupure de courant, car elles sont chargées par les scanners et ne disposent pas de batteries embarquées.

Alimentation embarquée et mémoire persistante

Pour contrecarrer l'attaque par panne électrique, les chercheurs du MIT ont élaboré deux innovations dans les puces RFID. La première concerne **l'intégration d'une alimentation sur la puce**, dont les connexions aux circuits de la puce seraient impossibles à interrompre. La seconde innovation se base sur **un ensemble de cellules de mémoire « non volatiles »** capables de stocker toutes les données de la puce quand il y a une perte de puissance.

Texas Instrument, partenaire de la recherche, a construit plusieurs prototypes de puces RFID à partir des innovations des chercheurs du MIT. Ces prototypes ont été éprouvés à plusieurs reprises et les puces se sont comportées comme prévues. Ahmad Bahai, directeur de la technologie chez Texas Instrument, indique : « *à l'ère de la connectivité omniprésente, la sécurité est un des plus grands défis auxquels nous sommes confrontés. Les travaux du MIT sont importants pour construire des puces robustes pour l'Internet industriel, à faible coût et avec un protocole d'authentification à faible consommation* ».

A lire aussi :

Sécurité des accès : et pourquoi pas une puce RFID sous la peau ?
RFID, Big Data… : Cegid dessine le magasin de demain