Black Hat : les carte SIM 3G/4G craquées en 10 minutes

Jusqu'à aujourd'hui, les algorithmes de chiffrement qui accompagnent les carte SIM des téléphones mobiles 3G et 4G étaient réputés inviolables, du moins extrêmement difficiles à casser. A tel point que, pour espionner les conversations mobiles, la NSA et son homologue britannique GCHQ avaient préféré voler des clés de cryptage au fournisseur mondial de SIM Gemalto plutôt que de s'attaquer à leur code de protection selon des révélations d'Edward Snowden en février dernier. Mais, à l'occasion de la conférence Black Hat 2015, un chercheur chinois vient de faire voler en éclat cette prétendue inviolabilité du cryptage AES-128.

Yu Yu, professeur et chercheur à l'université Jiao Tong de Shanghai a présenté une méthode de piratage selon laquelle il parviendrait à casser Milenage, l'algorithme de chiffrement basé sur l'AES-128 qui accompagne les cartes 3G et 4G, en quelques minutes. Pour cela, il ne s'attaque pas au code directement mais s'appuie sur l'analyse du différentiel électrique émis par la carte. Une méthode baptisée Side-channel attacks (attaques par canal alternatif) qui s'appuie sur la mesure de la consommation électrique des appareils, leurs émissions électromagnétiques ou encore leur production de chaleur, voire les sons émis.

8 cartes SIM cassées en 10 à 40 minutes

Pour cela, le chercheur et son équipe utilisent du matériel spécifique : un oscilloscope (pour la consommation électrique), un analyseur de spectre de protocole MP300-SC2 (pour l'interception du trafic), un lecteur de cartes SIM fait maison, et un PC doté d'un logiciel Side Channel Analyser (pour corréler les résultats). L'attaque nécessite donc un accès physique à la carte, ce qui présente tout de même un obstacle bien qu'il soit relativement facile de voler un mobile. Sans entrer dans les détails de la méthode d'analyse (que l'on retrouvera dans ce rapport), Yu Yu déclare être parvenu à casser les protections de 8 cartes SIM 3G/4G d'opérateurs et fabricants, dont les noms ne sont pas cités, en 10 à 40 minutes.

Une fois le sésame ouvert, il permet à l'attaquant de dupliquer facilement la carte SIM pour ensuite espionner les conversations, voire installer des malwares ou usurper l'identité du propriétaire pour des actions frauduleuses. Si le déchiffrement des SIM par attaque Side-Channel n'est pas à la portée du premier venu, nul doute qu'il intéressera les services gouvernementaux de surveillance.

Lire également
Hacker des ordinateurs avec la chaleur des composants
GSMem : Pirater un PC sans connexion via le réseau GSM
Thales : le spécialiste de la cybersécurité piraté

crédit photo © Brian A Jackson – shutterstock