Alerte de sécurité sur les cartes SIM

Les cartes SIM seraient le talon d'Achille de nos téléphones mobiles. Des faiblesses en matière de logiciel et de chiffrement compromettent en effet la sécurité des données qui y sont stockées.

C'est ce qu'indique **Karsten Nohl**, un expert allemand en cryptographie et fondateur de la société **Security Research Labs**.

Les travaux de son équipe seront présentés à l'occasion de la prochaine session du Black Hat Security à Las Vegas (27 juillet – 1er août), explique *ITespresso.fr*.

Une menace sérieuse selon Karsten Nohl, qui considère que près d'une carte SIM sur 8 utilisée dans le monde est exposée à cette vulnérabilité selon l'interview accordée à *Forbes*.

Un bug dans le code de la carte

Il y a quelques conditions au préalable pour l'exploitation de ces vulnérabilités, comme l'usage de la norme de chiffrement Data Encryption Standards (DES), inventée par IBM dans les années 70 et améliorée par la NSA.

Toujours selon Karsten Nohl, la clé du piratage réside dans un bug dans le code Java Card utilisé pour programmer les cartes SIM et les réactualiser.

C'est justement dans le canal de transmission *"over-the-air"* (protocole OTA, invisible pour l'utilisateur d'un smartphone) que se trouveraient les moyens de casser la clé de chiffrement propre à chaque carte SIM.

Grâce à la clé, n'importe quel hacker est en mesure d'injecter un virus qui sera accepté par la carte SIM puis de la contrôler à distance.

« Donnez-moi n'importe quel numéro de téléphone et il y a des chances que je vais, quelques minutes plus tard, être en mesure de contrôler à distance cette carte SIM et même en faire une copie », explique Karsten Nohl.

Forcer l'envoi de SMS à des numéros surtaxés, détourner les appels téléphoniques, intercepter les SMS, corrompre les systèmes de paiement intégrés… tout devient possible à partir du moment où la carte SIM est attaquée.

Pas encore d'exploit ?

L'expert en cryptographie doute que la faille ait déjà pu être exploitée. Néanmoins, deux opérateurs télécoms, intrigués par la découverte, se seraient déjà rapprochés de lui.

En décembre 2011, le chercheur Karsten Nohl avait déjà fait parler de lui en pointant des failles relatives au GPRS. Il avait établi une carte des opérateurs concernés (SFR était concerné à l'époque).

Voir aussi

Quiz Silicon.fr – Crimes et châtiments sur Internet