La confidentialité des conversations GSM n'est plus garantie !

Karsten Nohl vient de lancer un pavé dans la mare des opérateurs de télécommunication. Ce spécialiste de la sécurité a réussi à casser le système de chiffrement **A5/1**, utilisé pour la transmission de **80 %** des conversations GSM.

Il a présenté le résultat de ses travaux lors du 26e Chaos Communication Congress, organisé par le célèbre **Chaos Computer Club**. Voici un lien pointant vers la présentation effectuée lors de cette occasion. Au final, il aura fallu 23 ans pour découvrir comment casser l'algorithme A5/1. Il est vrai que les tables permettant de décoder les flux chiffrés pèsent **128 petaoctets** et nécessiteraient plus de 100 000 ans de temps de calcul pour être traitées sur un unique PC.

Le spécialiste allemand a résolu le problème de deux façons. Tout d'abord, il a défini un livre de codes d'une taille de seulement **2 To**, qui reste toutefois suffisant pour déchiffrer 50 % ou 99 % des communications (suivant les cas). De plus, il a mis à profit les technologies modernes (GPU Computing ou utilisation de composants reprogrammables), afin d'accélérer la vitesse de calcul. Avec un ensemble comprenant 40 GPU CUDA, **trois mois sont suffisants pour casser un flux**. Un réseau de calcul distribué sera parfaitement en mesure d'effectuer cette opération en quasi temps réel.

L'A5/1 Cracking Project permet d'accéder au code source des outils utilisés par Karsten Nohl. La communauté les a adaptés à des composants capables d'effectuer des traitements parallèles à grande vitesse, **comme les GPU ou le Cell**. Les tables de codes ne sont pas publiques, mais il semblerait qu'elles soient accessibles **sur les réseaux P2P**. Au préalable, il conviendra de capturer les flux, une opération réalisable à partir de certains récepteurs, coûteux, mais distribués dans le commerce.

Certes, le code utilisé pour l'A5/1 peut être modifié afin de rendre le livre de codes inexploitable. De plus, **les opérateurs prévoient de basculer vers l'A5/3**, un algorithme plus robuste. Karsten Nohl n'est cependant pas optimiste : décrypter de tels flux est toujours possible (quoique la puissance de traitement nécessaire soit encore hors de notre portée) et l'A5/3 utilise les mêmes clés que l'A5/1, ce qui constitue une faiblesse en terme de sécurité.