Chiffrement : Kraken simplifie l'écoute de communications GSM

- Technologie -

Date de mise en ligne : jeudi 22 juillet 2010

Spyworld Actu

Un groupe d'expert a mis au point une méthode permettant de briser le chiffrement des réseaux GSM en quelques minutes. Reste à voir si elle est utilisable en conditions réelles.

La conférence Black Hat du 28 juillet prochain risque d'être attendue. En plus la mise en cause de la sécurité des mots de passe sur Internet, elle accueillera les créateurs d'une nouvelle méthode permettant de déchiffrer les communications GSM.

L' initiative Open Source A5/1 Security Project vise à prouver que la méthode de chiffrement A5/1 utilisée par l'ensemble des réseaux GSM depuis 20 ans n'est plus aussi infaillible qu'on le croit.

Un déchiffrement en quelques minutes pour un coût moindre

Le vendredi 16 juillet, ils ont mis une touche finale à Kraken, un logiciel permettant de briser en quelques minutes le chiffrement GSM. Selon ses auteurs, il utilise de nouvelles tables de chiffrement optimisée pour casser la sécurité bien plus rapidement qu'auparavant.

En décembre dernier, ils avaient publié des tables permettant le déchiffrement accéléré de communications GSM, dans une version incomplète. Le travail est désormais finalisé.

Frank Stevenson, l'un des développeurs, ne cache d'ailleurs pas sa fierté. « Nous savons que nous pouvons le faire en quelques minutes. La question est : pouvons-nous le faire en quelques secondes ? »

Pour le spécialiste, leur méthode permettrait de lancer le déchiffrement très simplement et pour un coût moindre. Il annonce qu'avec elle le risque de voir cette pratique se généraliser est bien réel. Les détails logiciels et matériels seront donnés lors de la conférence Black Hat.

Déjà en 2008, un autre expert en sécurité indiquait avoir brisé la sécurité des réseaux GSM et appelait à une meilleure sécurisation des communications mobiles. Il reconnaissait tout de même la complexité de l'exploitation réelle de sa découverte.

Une preuve de concept difficile à mettre en oeuvre ?

La méthode n'est pourtant pas complète pour une exploitation réelle. Pour des raisons légales, le groupe n'a pas développé de quoi intercepter le signal GSM. Ils estiment que la connexion est possible avec un mobile classique et le logiciel Open Source OsmocomBB.

De son côté, la GSM Association, association qui regroupe les grands noms du secteur, se veut rassurante. Même si une méthode effective existe, l'application en conditions réelles resterait très difficile selon eux. Avec la multiplication des communications, il serait difficile de cibler puis de tracer une communication unique.

Stevenson calme lui aussi les craintes, la plupart des problèmes de sécurité des réseaux GSM seraient réglés par la 3G et 4G/LTE. Les réseaux 3G utilisent une évolution d'A5/1, A5/3, bien plus sécurisée qui pourrait être déployée sur

les réseaux GSM si A5/1 est réellement compromis.

Post-scriptum :

http://www.businessmobile.fr/actual...