L'écoute des GSM bientôt accessible à tous

- Informatique - Sécurité Informatique -

Date de mise en ligne : mardi 1er septembre 2009

Spyworld Actu

Grâce à l'informatique distribuée, un chercheur américain cherche à concevoir une table de calcul qui permettra de casser le chiffrement des communications GSM avec très peu de moyens.

Chercheur à l'université de Virginie aux Etats-Unis, Karsten Nohl prend la relève d'un projet lancé il y a quelques années : créer une table arc-en-ciel (1) permettant d'accélérer le déchiffrement d'une conversation téléphonique cryptée avec le chiffrement A5/1 : autrement dit, rendre beaucoup plus aisée l'écoute des communications classiques affrétées via les téléphones mobiles de deuxième génération, que nous utilisons tous les jours.

Pour éviter les mêmes désagréments que ses prédécesseurs - qui auraient subi des pressions de la part d'opérateurs -, Karsten Nohl a pris le parti (le soin ?) d'utiliser l'informatique distribuée, diluant ainsi les intervenants sur Internet. Les participants ont juste à installer sur leur machine un petit composant - un intergiciel - qui les relie entre eux et leur alloue un temps processeur affecté à des séquences de calcul issues d'un découpage du projet de calcul global. Ce choix plutôt rusé le met à l'abri des pressions pour ce projet, qui, par ailleurs, est tout-à-fait légal tant que la table n'est pas utilisée.

Provoquer pour être « écouté »

Dans le cas présent, à la différence d'un SETI@home, autre projet distribué qui n'en finit pas de chercher des extra-terrestres, le projet de création de table pourrait aboutir d'ici à six mois.

Dès lors, il ne sera plus nécessaire d'investir dans un logiciel onéreux (on parle aujourd'hui d'une fourchette allant de 100 000 à 250 000 dollars), ni de disposer d'une infrastructure matérielle démesurée pour casser la clé : un simple ordinateur et de bonnes connaissances techniques suffiront pour placer un téléphone sur écoute.

Karsten Nohl ne cache pas ses motivations. Il veut tout simplement que la 2G bénéficie d'une protection digne de ce nom au même titre que la 3G et la future 4G, face de cette faille déjà bien connue. Il compte surtout, avec cette énorme provocation, sensibiliser constructeurs et opérateurs autour de cette question.

Il faut savoir qu'en France, au 1er trimestre 2009, le parc 2G était encore de 45 millions d'unités pour un parc mobile total de 58 millions de terminaux.

(1) Structure de données renfermant les différentes combinaisons de chiffrement possibles favorisant un meilleur compromis temps-mémoire.

Post-scriptum :

http://pro.01net.com/editorial/5056...