Mobiles: des chercheurs cassent le code du GSM

On parle beaucoup des failles et des virus qui s'attaquent à nos ordinateurs. Mais on parle beaucoup moins des téléphones mobiles qui sont eux-aussi dotés de programmes informatiques et donc vulnérables aux attaques. Des chercheurs israéliens viennent de démontrer que cette vulnérabilité est assez importante.

Un groupe de chercheurs est en effet parvenu à briser le code d'encyptage qui protège les conversations transmises par les téléphones cellulaires utilisant le système GSM, selon le quotidien hébreu *Haaretz*. Le GSM (Système mondial de communications mobiles), est l'un des deux systèmes utilisés pour les téléphone cellulaire et représente 70% du marché mondial. Eli Biham, professeur à l'Institut Technion de Haïfa, raconte qu'il a été abasourdi lorsqu'un de ses doctorants, Elad Barkan, lui a annoncé avoir trouvé une erreur fondamentale dans l'algorithme de cryptage du protocole de communication GSM. *« Je lui ai répondu que c'était impossible »*, a déclaré Biham à Reuters. *« Une erreur aussi commune aurait déjà due être repérée par quelqu'un. Pourtant, il avait raison, l'erreur était bien là. »* Avec cette faille, votre mobile se transforme en moulin: *« Il est possible d'écouter un appel alors qu'il n'en est qu'au stade de la sonnerie, puis, en une fraction de seconde, d'apprendre tout sur l'utilisateur du portable »*, précise-t-il. *« Ensuite, nous pouvons écouter la conversation. »* Selon lui, les rédacteurs du code informatique du GSM ont fait l'erreur de privilégier la qualité sonore de l'appel – c'est à dire la correction des parasites et des interférences – avant le cryptage. Toutefois, il n'est pas nécessaire de paniquer. Selon la GSM Association la faille découverte à Haïfa ne peut être exploitée qu'au moyen d'une technologie chère et complexe et ne permet d'identifier un utilisateur précis qu'au terme d'une longue recherche. Par ailleurs, une telle attaque ne peut réussir que si le pirate émet des signaux de manière à faire passer son appareil pour le relais GSM par lequel transitent les communications. L'auteur de l'attaque doit également se trouver physiquement entre le relais et sa victime pour intercepter l'appel. Les scientifiques ont fait parvenir une copie de leurs travaux à la GSM Association afin de l'aider à corriger le problème. malin, ils sont également fait breveter leur découverte dont l'usage sera réservé aux forces de l'ordre, affirment-ils.