Les cartes graphiques à l'assaut des protections du Wi-Fi

Notre confrère MacBidouille a mis le doigt sur un article très intéressant de SC Magazine . La puissance des cartes graphiques permettrait de réduire le temps nécessaire au cassage d'un réseau sans fil crypté.

Les systèmes de chiffrement **WPA et WPA2** sont en principe suffisamment complexes pour éviter toute possibilité de découvrir la clé dans un délai raisonnable. De fait, il convient d'essayer toutes les clés possibles (attaque par force brute), afin de découvrir celle utilisée par le réseau sans fil.

Le WPA utilise l'algorithme de chiffrement RC4, avec une clé de 128 bits, alors que le WPA2 utilise une technique basée sur l'AES. Ces procédés sont à priori très efficaces. ElcomSoft (une société russe) aurait cependant pu **réduire le temps de calcul des différentes clés d'un facteur de 10.000** (soit quelques jours pour lire des données protégées en WPA). Elle utilise la puissance des cartes graphiques Nvidia.

Nous présumons que Cuda a été utilisé pour la mise au point de ce programme. Toute carte graphique apportant une accélération OpenGL pourra cependant être utilisée, au travers des techniques de programmation GPGPU (*General Purpose computing on Graphics Processing Units*). Le résultat sera toutefois probablement un peu plus lent.

Le problème est maintenant double. **La Wi-Fi Alliance va-t-elle proposer de nouveaux systèmes de chiffrement pour les réseaux sans fil ?** Dans l'affirmative, les constructeurs pourront-ils implémenter ces nouveaux protocoles, sans que le débit des connexions sans fil s'écroule ?

Cette seconde question est la plus importante. Effectivement, dans de nombreux cas, le simple fait d'activer le WPA provoque des baisses de débit (parfois importantes) sur les routeurs et cartes de réception Wi-Fi.