Soixante secondes pour percer le chiffrement WPA du Wi-Fi

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 31 août 2009

Deux chercheurs japonais ont réduit d'un facteur 15 le temps nécessaire pour déjouer la protection WPA/TKIP des réseaux Wi-Fi.

C'est ce qui s'appelle mettre les bouchées doubles. Les chercheurs japonais Toshihiro Ohigashi et Masakatu Morii viennent de montrer une nouvelle technique qui permet de briser le chiffrement WPA/TKIP des communications Wi-Fi en une minute, montre en main.

Cette nouvelle technique s'appuie sur l'attaque dite de « Beck-Tews », qui a été découverte en novembre 2008 par deux chercheurs allemands et qui permettait déjà d'intercepter en clair quelques paquets Wi-Fi et de les modifier.

Plus rapide et mieux applicable

En couplant cette technique avec une interception de type « man-in-the-middle » (1), les deux Japonais arrivent à réduire le temps d'exécution de l'attaque de quinze minutes à quelques minutes, voire à seulement soixante secondes.

Ils arrivent également à élargir le cadre d'application. L'attaque Beck-Tews ne fonctionnait qu'avec des équipements supportant certaines fonctions de qualité de service du WPA. Toshihiro Ohigashi et Masakatu Morii, au contraire, sont capables de cibler toutes les implémentations du WPA/TKIP. Les deux chercheurs donnent les détails de leur attaque dans un article scientifique.

Il faut souligner que le chiffrement basé sur WPA/AES ou WPA2 n'est pas concerné par cette attaque. Les entreprises qui utilisent des réseaux Wi-Fi ont donc tout intérêt à délaisser le WPA/TKIP et à s'orienter vers ces deux technologies alternatives.

(1) L'attaque man-in-the-middle a pour but d'intercepter les communications entre deux parties, sans que celles-ci ne puissent s'en douter. Ce type d'attaque est utilisée, par exemple dans le spoofing de DNS, qui permet de rediriger les internautes vers des sites tiers à leur insu.

Post-scriptum :

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