Le WiFi WPA une nouvelle fois craqué… en 60 secondes

Les universitaires japonais font très fort. En 60 secondes, **Masakatu Morii**, chercheur en sécurité à l'Université de Kobe, et **Toshihiro Ohigashi** ont trouvé le moyen de craquer un réseau sans fil en utilisant un **certificat WPA.**

L'attaque est relativement simple car elle se base sur la parade employée par Erik Tews et Martin Beck qui avaient réussi à **craquer un réseau Wi-Fi WPA en 15 minutes**. Toujours est-il que la méthode employée permet d'intercepter les communications qui circulent sur ce réseau.

Pour rappel, **Erik Tews et Martin Beck** avaient choisi de jeter leur dévolu sur le système de protection des connexions Internet WPA TKIP (Temporal Key Integrity Protocol) qui équipe la majorité des routeurs WiFi.

Leur méthode : ils ont **mis à jour une faille de sécurité** dans ce protocole qui permet les échanges de données entre le routeur et le PC. Ils ont envoyé une grande quantité de données par le routeur WiFi ciblé, ensuite, grâce à un procédé mathématique ils ont réussi à trouver la clé WPA grâce aux paquets de données récoltés. Un calcul qui prend entre 12 et 15 minutes.

Si le procédé permet la lecture des données entre le routeur et le PC, l'inverse est pour le moment impossible. De même, des sécurités sont toujours (pour l'instant) vierges de craquage. C'est le cas des paquets utilisant une protection **AES** (Advanced Encryption Standard) et **WPA 2, encore indéchiffrables.**

Pour autant, les études menées par les chercheurs japonais montrent qu'un réseau WiFi reste vulnérable. Elles sont aussi la preuve qu'à plus ou moins long terme une technologie a vocation à être piratée…