La sécurité du protocole WEP de nouveau remise en question

- Informatique - Sécurité Informatique -

Date de mise en ligne : mercredi 4 avril 2007

Spyworld Actu

Des chercheurs en cryptographie de l'université de Darmstadt en Allemagne ont publié un communiqué indiquant que WEP (un protocole servant à sécuriser les réseaux sans fils) n'est pas suffisamment sécurisé pour être utilisé sur les réseaux contenant des informations sensibles.

Le protocole WEP a déjà été remis en question en 2001 lorsque Scott Fluhrer, Itsik Mantin, et Adi Shamir ont publié une analyse compromettant la sécurité de l'algorithme RC4. Depuis, les pirates ont réussi à retrouver des clés RC4 (avec plus ou moins de succès).

En 2005, la sécurité de WEP a de nouveau été remise en question par l'analyse de Andreas Klein qui a trouvé de nombreuses corrélations entre les données chiffrées, et la clé secrète générée.

Les chercheurs de Darmstadt se sont appuyés d'une part sur les recherches de Andreas Klein, et d'autre part sur le fait que WEP génère un flux RC4 pour encrypter les données en n'utilisant qu'une clé secrète d'une longueur allant de 40 à 104 bits. Ainsi ils sont parvenus à adapter les recherches d'Andreas Klein de sorte qu'il est désormais possible de retrouver la clé de cryptage avec un taux de réussite de 50% en n'analysant que 40.000 paquets émis.

D'après ces chercheurs, il faut maintenant moins d'une minute pour capturer 40.000 paquets, et moins de trois secondes pour effectuer les calculs nécessaires afin de trouver la clé de cryptage et ce sur un Pentium M 1.7Ghz.

Ces chercheurs recommandent de migrer au plus vite vers les protocoles WPA1 et WPA2 , qui sont aujourd'hui supportés par la majorité des constructeurs présents sur le marché.

Pour en savoir plus :

Le communiqué de l'université de Darmstadt.

Adaptation d'un article de Nick farrell du 04 Avril 2007.

Post-scriptum :

http://fr.theinquirer.net/2007/04/0...