



Éditorial

Ces nouvelles attaques qui ridiculisent encore le WEP

Guillaume Lehembre 

Les vulnérabilités du protocole WEP [1], premier protocole de sécurisation des réseaux Wi-Fi, sont connues et exploitées depuis longtemps. Durant l'été 2006, plusieurs chercheurs en vulnérabilités ont présenté leurs travaux [2] sur des attaques par fragmentation et sont arrivés à la conclusion qu'il était très facile d'injecter des trames arbitraires sur un réseau protégé avec du WEP. Cette nouvelle attaque se base sur l'utilisation astucieuse de la fragmentation autorisée par le standard 802.11 : une trame peut être fragmentée en 16 fragments maximum systématiquement défragmentés par le point d'accès lors de sa retransmission. En exploitant une situation de clair connue sur des entêtes de paquets identifiables (22 premiers octets d'une requête ARP ou les 8 premiers octets d'un paquet IP), un attaquant est capable de trouver au minimum 64 octets de la suite chiffrante (*keystream*). Pour cela, l'attaquant va reconstruire 16 fragments de 4 octets (il faut systématiquement enlever 4 octets de CRC32) et analyser la trame défragmentée renvoyée par le point d'accès. En répétant cette attaque avec des fragments de 64 octets l'attaquant est capable en une trentaine de secondes d'obtenir une suite chiffrante complète couvrant les 1500 octets de la MTU du Wi-Fi pour un vecteur d'initialisation (IV) donné. Comme le rejeu d'un même IV n'est pas interdit dans le protocole WEP, un attaquant est alors en mesure d'injecter n'importe quelle trame arbitraire dans le réseau. Cette attaque, couplée à celles existantes [1], permet de faciliter l'injection de paquets en vue du cassage de la clé WEP ou de réaliser une exploration du réseau.

La seconde attaque [3] parue le 1er avril 2007 par trois chercheurs de l'université de Darmstadt ne fut pas une blague de très bon goût pour le protocole WEP elle expliquait comment retrouver une clé WEP de 128 bits en un temps record : moins d'une minute !

Cette attaque est en fait une optimisation des lacunes du générateur pseudo-aléatoire RC4 mis en avant par A. Klein lors de ces travaux [3] rendant possible la découverte des octets de la clé WEP de manière indépendante les uns des autres alors qu'ils étaient retrouvés séquentiellement par le passé, d'où une nette amélioration des performances.

Leurs expérimentations menées à partir d'une version modifiée [5] d'aircrack-ng [6] ont permis de montrer à l'aide de deux cartes Wi-Fi (une pour injecter et l'autre pour capturer les paquets) qu'un attaquant avait 50% de chance de casser une clé WEP 128 bits en collectant 40000 suites chiffrantes, il en fallait précédemment presque dix fois plus. La capture de 85000 suites chiffrantes fait monter la probabilité à 95% au prix de quelques minutes supplémentaires.

Une nouvelle fois, ces attaques montrent l'extrême faiblesse du protocole WEP. Il doit être abandonné au profit du WPA/WPA2 ou être secondé de mécanismes de sécurité additionnels (VPN) pour les points d'accès ne pouvant être mis à jour pour supporter le WPA/WPA2. ●

À propos de l'auteur

Guillaume Lehembre est un consultant sécurité français travaillant pour le cabinet HSC (Hervé Schauer Consultants – <http://www.hsc.fr>) depuis 2004. Il a travaillé sur différents audits, études et tests d'intrusion et a acquis une expérience certaine dans la sécurité des réseaux sans fils. Il a réalisé des interventions publiques sur ce sujet et a publié plusieurs articles, dont un article dans le numéro 14 de hakin9 intitulé *Sécurité Wi-Fi – WEP, WPA et WPA2*. Il rédige un éditorial mensuel dans hakin9 depuis Janvier 2007. Guillaume peut être contacté à l'adresse suivante : Guillaume.Lehembre@hsc.fr.

Références :

- [1] *Sécurité Wi-Fi – WEP, WPA et WPA2* – Hakin9 1/2006.
- [2] *The Final Nail in WEP's Coffin* – A. Bittau, M. Handley, J. Lackey,
- [3] *Breaking 104 bit WEP in less than 60 seconds* – E. Tews, R.P Weinmann, A. Pyshkin,
- [4] *Attacks on the RC4 Stream Cipher* – A. Klein,
- [5] *Aircrack-ptw* – <http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>,
- [6] <http://www.aircrack-ng.org/>.