Sujet :[correspondants-ssi] [ecorses] [CERT-FR] CERTFR-2018-ACT-013 [Bulletin d'actualité CERTFR-2018-ACT-013]
Date : Mon, 13 Aug 2018 14:30:04 +0200 (CEST)

BULLETIN D'ACTUALITÉ DU CERT-FR

Objet : Bulletin d'actualité CERTFR-2018-ACT-013
Référence : CERTFR-2018-ACT-013

Nouvelle méthode d'attaque sur le WPA2-PSK

Résumé

Le 04 août 2018, le créateur du logiciel HashCat a publié sur le forum de hashcat.net [1] une nouvelle méthode pour attaquer des réseaux Wi-Fi protégés par WPA2 en mode PSK (WPA2 Personnel). Les réseaux WPA2 protégés par WPA2-EAP ne sont en pratique pas touchés par cette nouvelle attaque.

Jusqu'à présent, les attaques sur WPA2-PSK nécessitaient la capture de l'initialisation d'une connexion d'un client légitime au point d'accès suivie d'une phase de recherche exhaustive. Une fois l'attaque menée, l'attaquant possédait la phrase secrète du réseau Wi-Fi.

Cette nouvelle attaque nécessite un simple échange entre l'attaquant et le point d'accès suivi d'une recherche exhaustive. A l'issue de l'attaque, l'attaquant possède comme précédemment la phrase secrète du réseau Wi-Fi.

Cela lui permet d'accéder au réseau. Il peut aussi déchiffrer toutes les communications en cours, passées ou futures échangées entre n'importe quel client légitime et le point d'accès sous réserve de capturer l'initialisation de la connexion des clients avec le point d'accès.

Cette attaque fonctionne sur l'ensemble des implémentations qui respectent strictement la norme IEEE 802.11. Cependant, certaines implémentations s'écartant de la norme ne sont pas vulnérables.

Implémentations vulnérables

Par défaut tous les logiciels implémentant le protocole WPA2 sont vulnérables. Il a pu être vérifié que plusieurs points d'accès Wi-Fi utilisant une implémentation par la société Broadcom, ainsi que certains points d'accès de marque Cisco étaient vulnérables.

Le logiciel open source hostapd [2] n'est pas vulnérable. Les points d'accès utilisant ce logiciel ne sont donc pas vulnérables.

Le protocole WPA, d'une sécurité intrinsèque inférieure à celle de WPA2 et considéré comme obsolète, n'est pas vulnérable à cette attaque.

Mesures correctives

Le CERT-FR recommande la mise à jour des micrologiciels des points d'accès vulnérables.

Dans tous les cas, l'usage d'une phrase secrète complexe [3] est nécessaire et suffisant pour se prémunir des attaques contre les réseaux protégés par les protocoles WPA et WPA2 utilisés en mode PSK.

Il n’est pas recommandé de passer en WPA car l’algorithme de chiffrement TKIP présente plusieurs vulnérabilités.

Détails de l’attaque

Rappels sur WPA2

Le protocole WPA2 est spécifié initialement dans l’amendement IEEE 802.11i de la norme IEEE 802.11 originale avant d’être intégré dans la norme IEEE 802.11 [4]. Le protocole WPA consiste en une version préliminaire de IEEE 802.11i standardisée par la Wi-Fi Alliance.

Le protocole WPA2 est décliné en deux modes : WPA2-PSK (« Personnel », clé pré-partagée) et WPA2-EAP (« Entreprise », authentification à l’aide du protocole IEEE 802.1X). Alors que la version PSK se configure à l’aide d’une phrase secrète (ou, plus rarement, avec une clé pré-partagée), la version EAP utilise un serveur d’authentification externe responsable de l’établissement du secret partagé.

Afin de garantir la sécurité des communications, différentes clés sont spécifiées dans la norme :

- la PMK (Pairwise Master Key) est la clé maître sécurisant l’ensemble des communications protégées par WPA2 ; elle est constante sur toute la durée de la connexion Wi-Fi ;
- la PTK (Pairwise Transient Key) est dérivée de la PMK et est renouvelée régulièrement à l’aide du mécanisme de 4-way handshake ;
- les KCK (Key Confirmation Key), KEK (Key Encryption Key), TK1 et TK2 (Temporal Keys) sont dérivées de la PTK et servent à différents usages (authentification, distribution de clés, chiffrement et protection en intégrité des données).

La PMK est la racine de toutes les autres clés décrites ci-dessus. Sa possession permet donc d’accéder au réseau et de déchiffrer toutes les communications en cours, passées et futures. La preuve de possession de la PMK par les deux parties est établie lors du 4-way handshake. Cette étape déjà évoquée ci-dessus permet de générer une PTK et d’authentifier le point d’accès et le client.

La génération de la PMK dépend du mode WPA2 utilisé.

Dans le cas du WPA2-PSK, la PMK est dérivée de la phrase secrète en utilisant la formule suivante :

La fonction PBKDF2 est une fonction de dérivation de clé à partir d’un mot de passe utilisant une primitive cryptographique (ici HMAC-SHA1) avec un nombre d’itérations important (ici 4096) afin de ralentir les attaques par recherche exhaustive.

Ici, la PMK dépend de la phrase secrète et du SSID du point d’accès. Elle est donc commune à l’ensemble des clients connectés au point d’accès et sa durée de vie dépend de la fréquence de changement de la configuration.

Lorsque l’utilisateur configure une clé pré-partagée, il s’agit directement de la PMK.

Dans le cas du WPA2-EAP, la PMK est générée lors de lors de l’authentification de chaque client à l’aide du protocole IEEE 802.1X. Cela veut dire que la PMK est spécifique à chaque client et change à chaque authentification.

Mise en cache des PMK

L'échange IEEE 802.1X est complexe et ralentit la connexion d'un utilisateur. Pour accélérer le processus, la norme IEEE 802.11i introduit un mécanisme de mise en cache des PMK. Une fois que l'utilisateur est authentifié, sa clé est gardée en mémoire par le terminal et par le point d'accès. Lorsque l'utilisateur se reconnecte, il indique alors au point d'accès qu'il possède déjà une ou plusieurs PMK en lui fournissant une liste de PMKID. Le PMKID est défini par la norme comme suit :

La fonction HMAC-SHA1-128 est une fonction cryptographique à sens unique. Il est donc impossible à partir d'un PMKID de retrouver la PMK sans recherche exhaustive. Le PMKID dépend de la PMK et des adresses MAC du point d'accès (AA) et du client (SPA).

Après la phase d'association entre le client et le point d'accès, ce dernier initie le 4-way handshake et informe au client la PMK qu'il va utiliser en lui communiquant le PMKID correspondant.

Vulnérabilité

Lors d'une attaque par recherche exhaustive, l'attaquant génère une liste de solutions possibles. Afin de déterminer si cette solution est valide, l'attaquant réalise un calcul et compare le résultat avec un jeu de test obtenu préalablement.

Jusqu'à présent le jeu de test était un 4-way handshake valide. A partir d'une phrase secrète possible, l'attaquant dérivait la PMK et la validait contre un code d'intégrité présent dans les messages.

Dans cette nouvelle attaque, l'attaquant part d'une phrase secrète possible, dérive la PMK et calcule le PMKID associé. L'égalité avec le PMKID obtenu du point d'accès détermine la réussite de l'attaque.

Dans les deux attaques, il est nécessaire de partir d'une phrase secrète que l'attaquant peut constituer à partir d'un dictionnaire. WPA2-EAP n'est pas concerné en pratique par cette attaque car la PMK est générée aléatoirement et non dérivée d'une phrase secrète, prévenant donc les attaques par force brute. Il faudrait en effet essayer exhaustivement les 2256 PMK possibles.

Nécessité du PMKID

Lors de l'utilisation de WPA2-EAP, la mise en cache des PMK et l'utilisation des PMKID est une optimisation pour éviter de faire des échanges IEEE 802.1X. Le PMKID permet aux parties de déterminer quelle PMK utiliser sans révéler cette dernière. Dans le cas du WPA2-PSK, cependant, cette information est superflue car les parties ne manipulent qu'une seule PMK qui est dérivée de la phrase secrète. De plus, la mise en cache de la PMK n'a pas lieu d'être car cela ne permet pas d'économiser d'échanges (le protocole IEEE 802.1X n'est pas utilisé en WPA2-PSK). Ce mécanisme d'optimisation pour WPA2-EAP n'a donc aucun intérêt pour le mode WPA2-PSK.

Clarification

Contrairement à ce qui est indiqué sur le forum du logiciel Hashcat, cette attaque ne dépend ni des fonctionnalités d'itinérance du point d'accès ni des standards IEEE 802.11p/q/r. En effet, la mise en cache des PMK est décrite dans IEEE 802.11i et sert dans des situations d'itinérance mais aussi lors d'une ré-association avec un même point d'accès.

Le protocole WPA n’est pas vulnérable. En effet, WPA étant issu d’une version préliminaire de IEEE 802.11i, il ne possède pas les fonctionnalités de mise en cache des PMK. Ce comportement a été vérifié sur des implémentations vulnérables en WPA2.

Documentation

- Publication sur le forum du logiciel Hashcat
https://hashcat.net/forum/thread-7717.html
- Logiciel hostapd
https://w1.fi/hostapd/
- Recommandations de sécurité relatives aux mots de passe
https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf
- Norme IEEE 802.11-2016
https://ieeexplore.ieee.org/document/7786995/

Dernière version de ce document:
https://www.cert.ssi.gouv.fr/actualite/CERTFR-2018-ACT-013/