NY - Juin 2023

Attaques Wi-Fi

Les réseaux Wi-Fi sont devenus omniprésents dans notre vie quotidienne et ont révolutionné la manière dont nous communiquons et accédons à l'information. Cependant, avec cette commodité viennent également des risques de sécurité importants, car les réseaux Wi-Fi peuvent être, plus ou moins facilement, compromis par des attaquants malveillants.
Dans cet état de l'art, nous allons examiner les différentes attaques Wi-Fi qui ont été identifiées au fil du temps, en mettant l'accent sur le cassage des protocoles de sécurité les plus couramment utilisés, tels que WEP, WPA, WPA2 et WPA3.

Ce rapport détaillera en premier les normes 802.11 puis on développera dans plusieurs parties la sécurité de WEP, WPA, WPA2 et WPA3.

Sommaire

Normes 802.11

IEEE 802.11 est un ensemble de normes pour les réseaux locaux sans fil (Wireless Local Area Network - WLAN) qui a été développé par l'Institute of Electrical and Electronics Engineers (IEEE).
Les normes IEEE 802.11 définissent des spécifications pour l'implémentation de réseaux locaux sans fil au niveau de la couche physique et de la couche liaison de données du modèle OSI ou de la couche Accès Réseau pour le modèle TCP/IP.
La principale application commerciale de ces spécifications est la technologie Wi-Fi.
Le terme “Wi-Fi” est un terme commercial possédé par la Wi-Fi Alliance introduit pour avoir un nom plus attractif que la dénomination technique “802.11” et qui certifie qu’un matériel est conforme aux spécifications de la norme 802.11.

La couche physique définit des exigences concernant les fréquences radio, les débits de données, les modulations et la puissance de transmission alors que la couche liaison de données définit les exigences pour les accès au canal, la gestion des erreurs, le chiffrement des données et le contrôle de la qualité de service.

Les spécifications IEEE 802.11 définissent également plusieurs modes de fonctionnement pour les réseaux Wi-Fi.
Le mode Infrastructure, le plus couramment utilisé, permet aux appareils de se connecter à un point d'accès qui gère le trafic réseau. Le point d'accès sert de passerelle entre les appareils et le réseau câblé, ce qui facilite la gestion du réseau et assure une meilleure sécurité.
Le mode Ad Hoc permet à des appareils de se connecter directement entre eux sans l'intermédiaire d'un point d'accès. Les certifications Wi-Fi direct et TDLS tentent de promouvoir l’utilisation de ce mode.

Les spécifications IEEE 802.11 évoluent en permanence pour prendre en compte les besoins en matière de performance, d'interopérabilité et de sécurité des réseaux sans fil.
Les nouvelles versions sont désignées par 802.11 suivi d’une lettre permettant d’identifier la version ainsi que le nom commercial, par exemple :

- La version 802.11ax aussi appelée Wi-Fi 6 qui apporte une amélioration du débit et de la portée
- La version 802.11be ou Wi-Fi 7, la prochaine version attendue pour 2024.

Les normes de sécurité pour les réseaux Wi-Fi incluent le WEP (Wired Equivalent Privacy), le WPA (Wi-Fi Protected Access), le WPA2 et récemment le WPA3.

WEP

Présentation

Wired Equivalent Privacy (WEP) est un protocole de sécurité Wi-Fi introduit en 1999 dans la norme IEEE 802.11.
Son nom vient du fait qu'il devait fournir une confidentialité comparable à celle d'un réseau local filaire.
Cet algorithme a été retenu car il était considéré comme rapide pour une machine de cette époque.
Cependant, WEP a été rapidement considéré comme vulnérable avec la découverte de plusieurs failles majeures et a été considéré comme déprécié en 2004, depuis WEP porte le surnom “Weak Encryption Protocol”.
Il a été remplacé par le WPA en 2003 puis par le WPA2 en 2004.

Eléments techniques

Le fonctionnement de WEP repose sur deux éléments principaux :

- un algorithme de chiffrement de données
- un système d'authentification.

L'algorithme de chiffrement utilisé par WEP est le RC4 (Rivest Cipher 4), qui est un algorithme de chiffrement par flots. Cela signifie qu'un flot de bits pseudo-aléatoire, généré par une clé et un vecteur d'initialisation, est combiné par un XOR avec les données à envoyer pour les chiffrer.
Le WEP N-bits utilise une clé de chiffrement de N - 24 bits à laquelle est concaténée un vecteur d'initialisation (Initialization Vector - IV) de 24 bits.

Le système d'authentification de WEP repose sur deux modes :

- le mode Open System : toute station est autorisée à rejoindre le réseau sans fil sans être authentifiée.
- le mode Shared Key : une clé partagée est utilisée pour l'authentification. Le processus d'authentification commence par une étape de demande d'authentification envoyée par la station Wi-Fi. Le point d'accès répond ensuite avec un défi qui doit être chiffré à l'aide de la clé partagée. Si la réponse chiffrée est correcte, la station est authentifiée et peut rejoindre le réseau.

Faiblesses

WEP souffre de plusieurs faiblesses qui ont permis la mise en œuvre d’attaques permettant de casser sa sécurité. Parmi ces faiblesses, on peut citer :

- l’utilisation de clés faibles RC4 : ainsi on peut parvenir à deviner certains octets de la suite chiffrée en observant certains octets de la clé
- la collision de vecteurs d’initialisation (IV) : la clé utilisée est statique et ne change pas souvent. Ainsi, si deux trames sont chiffrées avec le même IV alors on peut retrouver le message original en utilisant les propriétés du XOR.
  Cette attaque est possible car le nombre d’IV unique est limité à 2^24.

- un contrôle d'intégrité réalisé par la fonction CRC32 qui s'avère être linéaire
- utilisation d'une clé unique sans mécanisme de mise à jour

Attaque par force brute et dictionnaire

Avant de passer à des attaques plus complexes, l'attaque la plus simple à mettre en œuvre est l'attaque par force brute en utilisant ou non un dictionnaire.
Ce type d'attaque peut s'avérer efficace en raison du nombre limité de clés possibles mais aussi par le fait que les utilisateurs ont tendance à choisir des clés faibles.

Attaque FMS (Fluhrer, Mantin, and Shamir)

Attaque découverte en 2001 https://www.cs.cornell.edu/people/egs/615/rc4_ksaproc.pdf qui permet de récupérer la clé WEP.
L'attaque FMS exploite une faiblesse dans la génération des IV qui sont considérés comme faible et qui permettent donc de révéler quelques bits de la clé.
Elle exploite aussi le fait que les quatre premiers octets du flux de sortie de RC4 sont toujours prévisibles, car ils contiennent l'entête du protocole SNAP.

Attaque KoreK

L'attaque KoreK est une méthode de craquage de clé RC4 qui a été publiée en 2004 par une personne anonyme avec pour pseudo KoreK.
Cette attaque utilise des corrélations entre certains octets qui permettent de deviner certains octets de la clé.
L'attaque KoreK est considérée comme une amélioration de l'attaque FMS, car elle utilise des corrélations supplémentaires pour récupérer la clé plus rapidement et plus efficacement.
Cependant, cette attaque nécessite toujours la collecte d'un grand nombre de paquets chiffrés pour réussir.

Attaque PTW (Pyshkin, Tews, and Weinmann)

https://eprint.iacr.org/2007/120.pdf
L'attaque PTW publiée en 2007 permet de récupérer une clé WEP.
Contrairement aux attaques précédentes qui imposent que certaines valeurs restent identiques pour calculer les corrélations, l'attaque PTW ne nécessite aucune condition sur ces valeurs.
Cela signifie que chaque paquet capturé peut être utilisé, ce qui augmente considérablement le nombre de paquets permettant de récupérer la clé secrète et augmente donc considérablement l'efficacité de l'attaque.
L'attaque a besoin d'environ 35 000 à 40 000 paquets pour une probabilité de succès de 50%, ce qui peut être collecté en moins de 60 secondes sur un réseau rapide. De plus, les auteurs affirment que pour réussir l'attaque dans 95% des cas, seulement 85 000 paquets sont nécessaires.

Attaque ChopChop

http://www.netstumbler.org/unix-linux/chopchop-experimental-wep-attacks-t12489.html
L'attaque ChopChop est une méthode publiée en 2009 par KoreK permettant de récupérer les derniers octets d'un paquet chiffré.
Cette attaque utilise une technique différente des attaques précédentes.
Pour cela, l'attaquant capture un paquet chiffré et modifie le dernier octet du paquet, il doit aussi modifier le contrôle d'intégrité (ICV). En effet, le paquet sera considéré comme valide si l'attaquant parvient à modifier l'ICV avec l'octet valide. Ensuite, il envoie le paquet modifié au point d'accès sans fil et observe la réponse. Si la réponse indique que le dernier octet était correct, l'attaquant peut alors déduire la valeur correcte de cet octet. L'attaquant répète ce processus pour chaque octet jusqu'à ce qu'il décrypte tous les derniers octets du paquet.
Cette attaque ne révèle pas la clé secrète utilisée pour chiffrer les données et n'est pas basée sur des propriétés spéciales du chiffrement RC4.

Attaque Beck-Tews

https://dl.aircrack-ng.org/breakingwepandwpa.pdf
Cette attaque a été publiée en 2008 et elle permet de récupérer une clé WEP de manière efficace via une amélioration des attaques précédentes. En effet, les auteurs sont parvenus à améliorer l'attaque PTW en modifiant les corrélations utilisées dans l'attaque KoreK.
Les auteurs ont montré que pour obtenir un taux de réussite de 50%, l'attaque n'a besoin que de 24 200 paquets.

Outils

Aircrack-ng est une collection d'outils dont la principale utilisation est le "cassage" de clés WEP et WPA des réseaux WIFI. Il s'agit d'un fork de Aircrack, projet abandonné aujourd'hui.
Aircrack-ng implémente plusieurs des attaques présentées précédemment :

- Attaque PTW (par défaut)
- Attaque FMS
- Attaque KoreK
- Attaque ChopChop
- Attaque par force brute et dictionnaire

De plus, Aircrack-ng propose de nombreux autres outils très intéressants et utiles pour la sécurité des réseaux Wi-Fi.

WPA

Présentation

WPA (Wi-Fi Protected Access) est un protocole de sécurité utilisé pour protéger les réseaux sans fil. Il a été créé en 2003 pour remplacer le protocole WEP, considéré comme peu sûr en raison de ses vulnérabilités.
WPA est implémenté au-dessus de WEP pour pouvoir être utilisé dans des équipements existants sans besoin de modification. Ainsi WPA est considéré comme une solution intermédiaire, avant le passage à WPA2, développée pour pallier rapidement à toutes les faiblesses découvertes avec WEP.

Eléments techniques

WPA repose sur une PSK (Pre-Shared Key) qui correspond à une clé, en réalité il s'agit plutôt d'un mot de passe.

WPA utilise l'algorithme de chiffrement par flot RC4 pour chiffrer les données, tout comme WEP. Cependant, WPA utilise une clé plus longue de 128 bits et un vecteur d'initialisation de 48 bits pour améliorer la sécurité.
La grande amélioration de WPA provient de l'utilisation du protocole TKIP (Temporal Key Integrity Protocol) qui génère des clés de chiffrement dynamiques à partir d'une clé unique (la clé de la box internet) pour chaque paquet de données envoyé sur le réseau.
L'utilisation de TKIP et d'un vecteur d'initialisation beaucoup plus grand que dans WEP permet à WPA d'être résistant aux attaques décrites précédemment.

La version entreprise du WPA propose également un protocole d'authentification plus robuste appelé EAP (Extensible Authentication Protocol), qui permet l'authentification basée sur le certificat numérique, le mot de passe, ou tout autre moyen d'identification configurable par l'utilisateur.
La version personnelle de WPA repose sur l'utilisation du clé secrète partagée (PSK), on nomme cette méthode d'authentification WPA-PSK.

WPA utilise également un MIC (Message Integrity Check) qui correspond à 64 bits inclus dans chaque paquet. Cela permet de vérifier l'intégrité des paquets de données pour détecter toute tentative de modification ou d'injection malveillante.
En effet, cela permet d'empêcher les attaques sur le mécanisme de protection de l'intégrité CRC32 qui s'est avéré vulnérable dans le cas de WEP.
De plus, MIC inclut aussi un compteur de trame (TSC - TKIP Sequence Counter) qui empêche les attaques par rejeu, une autre faiblesse du WEP.
Notamment, si la vérification du MIC échoue alors le paquet sera considéré comme une attaque. Si deux paquets incorrects (deux attaques) sont reçus dans un délai de 60 secondes, la communication sera interrompue et toutes les clés seront renégociées après une période de 60 secondes.
Lorsqu'un paquet valide est reçu, le compteur de séquence TKIP (TSC) correspondant au canal sur lequel il a été reçu est mis à jour. Si un paquet avec un TSC inférieur est reçu, il sera rejeté.

Enfin, WPA prend en charge une fonctionnalité appelée "handshake à quatre voies" qui permet aux clients et au point d'accès sans fil de négocier une clé de session commune pour chiffrer les données échangées sur le réseau.

Attaque Beck-Tews sur TKIP

Cette attaque rendue publique par Erik Tews et Martin Beck en 2008 est la première attaque sur WPA. Plusieurs conditions sont nécessaires pour que cette attaque réussisse :

- Le réseau attaqué utilise TKIP
- Le protocole IPv4 est utilisé et la plage d'adresses IP est connue de l'attaquant
- Un long intervalle de re-négociation de clés est utilisé pour TKIP, par exemple 3600 secondes
- Le réseau prend en charge les fonctionnalités de qualité de service (QoS) IEEE 802.11e
- Une station est actuellement connectée au réseau

Les auteurs de l'attaque précisent que ces hypothèses sont assez réalistes pour la plupart des réseaux déployés.

Cette attaque nécessite un temps important pour s'exécuter de l'ordre de 15 minutes environ.

Cette attaque ressemble à l'attaque ChopChop mais elle cherche ici à déchiffrer des paquets de requête ARP (Address Resolution Protocol).
L'attaquant capture des paquets jusqu'à récupérer un paquet d'une requête ARP chiffré ou sa réponse.
Dans ce type de paquet, la plupart du contenu est connu par l'attaquant, il lui manque seulement les 8 octets (MIC) et les 4 octets du checksum ICV qui constituent les 12 derniers octets de la partie claire du message.
L'attaquant peut alors lancer une attaque de type ChopChop modifiée afin de décoder les octets manquants comme il le ferait sur WEP.
Cependant WPA avec TKIP dispose de contre-mesures pour lutter contre ce type d'attaque. Pour contourner ces défenses, l'attaquant peut utiliser les différents canaux de Qualité de Service. L'attaquant doit exécuter l'attaque sur un canal QoS différent de celui sur lequel le paquet a été initialement reçu, en particulier l'attaquant privilégie les canaux encore peu utilisés où le trafic est bien moindre afin de disposer d'un TSC bien inférieur, pour continuer son attaque.
Si la supposition pour le dernier octet pendant l'attaque ChopChop est incorrecte, le paquet est toujours abandonné silencieusement. Si la supposition est correcte, un paquet MIC failure report frame est envoyé par le client, l'attaquant devra attendre 60 secondes afin d'éviter que le point d'accès n'enclenche ses contre-mesures.
Ainsi, en 12 minutes, il est possible de récupérer les derniers 12 octets du paquet (le MIC et l'ICV).
Pour déterminer les octets restants inconnus (adresses IP exactes de l'expéditeur et du destinataire), l'attaquant peut deviner les valeurs et les vérifier par rapport à l'ICV déchiffré.
Maintenant, l'attaquant peut lancer l'inverse de l'algorithme MIC, l'algorithme est réversible ce qui est une faiblesse, pour en déduire la clé MIC utilisée pour le chiffrement des paquets.

En utilisant cette attaque, on peut récupérer la clé MIC et ainsi avoir accès à un flux de données entre un point d'accès et un client, on peut ainsi envoyer des paquets personnalisés au client en utilisant le même flux de données. Cela peut causer des perturbations dans la communication ou même entraîner un déni de service. L'attaquant pourrait également essayer de rerouter le trafic en utilisant des faux paquets ARP. Toutefois, cette attaque ne permet pas de décoder complètement la clé PSK de WPA, donc le risque n'est pas aussi élevé qu'avec WEP qui est entièrement cassé.

Amélioration de l'attaque de Beck-Tews sur TKIP

En 2009, Ohigashi et Morii, améliore l'attaque de Beck-Tews et propose une nouvelle attaque dont le temps de réalisation est plus court. Cette attaque comme celle de Beck-Tews ne casse pas WPA mais permet d'améliorer l'efficacité de l'attaque et de supprimer certains prérequis comme le fait d'utiliser le QoS.

En 2013, Vanhoef et Piessens ont proposé 3 attaques qui sont des améliorations importantes de l'attaque de Beck-Tews https://papers.mathyvanhoef.com/asiaccs2013.pdf.
En effet, l'attaque de Beck-Tews peut déchiffrer seulement des paquets ARP avec du contenu principalement connu et ne permet l'injection que de 3 à 7 paquets d'au plus 28 octets. L'attaque de Vanhoef et Piessens quant à elle peut injecter un nombre arbitraire de paquets contenant au plus 112 octets de données utiles et ne nécessite pas l'utilisation de la QoS.
De plus, les auteurs ont montré comment déchiffrer des paquets arbitraires envoyés à un client. Cela signifie qu'un attaquant pourrait potentiellement intercepter des paquets envoyés d'un point d'accès à un client protégé par WPA-TKIP et les déchiffrer.
Il convient de remarquer qu'encore une fois, cette attaque ne casse pas WPA car elle ne permet pas de récupérer la PSK.
Enfin, ils ont aussi présenté une attaque par déni de service qui peut être exécutée en injectant seulement deux trames toutes les minutes. Cela signifie que l'attaquant peut perturber la connexion d'un client en envoyant très peu de données.

Outils

Aircrack-ng propose une implémentation de l'attaque de Beck-Tews sur TKIP via l'outil tkiptun-ng.
L'outil mdk3 https://www.kali.org/tools/mdk3/ propose une implémentation de l'attaque de Vanhoef et Piessens en particulier la possibilité de réaliser un déni de service. C'est un outil très puissant qui met à disposition de nombreuses attaques et qui doit être considéré lorsqu'on s'intéresse à la sécurité du protocole Wi-Fi.

Défenses

Concernant les attaques sur WPA, des défenses très simples sont proposées, une des solutions suivantes pourra être envisagées :

- Configurer un temps de renégociation des clés très court, il est recommandé de ne pas dépasser 120 secondes

- Désactiver l'envoi de messages de rapport d'échec de MIC aux clients, ce qui empêcherait à l’attaquant de connaître le moment où il doit patienter 60 secondes pour éviter la mise en place de contre-mesures.
- Utiliser CCMP au lieu de TKIP

Aujourd’hui, CCMP basé sur AES est considéré comme sécurisé et il a été approuvé par le NIST (National Institute of Standards and Technology).

WPA2

Présentation

En 2004, la Wi-Fi Alliance a introduit WPA2 en tant que nouvelle norme de sécurité pour remplacer WPA. WPA2 met en œuvre les éléments obligatoires de IEEE 802.11i certifiée par la Wi-Fi Alliance. A partir de 2006, le WPA2 devient obligatoire pour tous les appareils certifiés Wi-Fi,

Eléments techniques

La grande différence avec WPA est le choix de la méthode de chiffrement. En effet, comme vu précédemment, les attaques sur WPA visent les faiblesses de la méthode de chiffrement TKIP basé sur l'algorithme de chiffrement RC4.
WPA2 se base sur la méthode de chiffrement CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) qui utilise l'algorithme de chiffrement AES (Advanced Encryption Standard).
Il convient de noter que l'on peut configurer WPA2 pour utiliser TKIP basé sur RC4 mais cela reste déconseillé.

Le mode WPA2-PSK utilise, pour l'authentification au réseau, une seule clé secrète (PSK) partagée entre les appareils et le point d'accès (AP).
À partir de ce PSK, chaque appareil dérive et stocke une Pairwise Master Key (PMK) jusqu'à ce que le PSK ou le SSID (nom du point d'accès) change. Lorsqu'un client tente de se connecter, un protocole appelé "4-ways handshake" est initié pour générer une Pairwise Transient Key (PTK). Cette clé est utilisée pour chiffrer les données entre un client et le point d'accès.
La poignée de mains à 4 temps (4-ways handshake) se déroule selon les étapes suivantes :

1. Le point d'accès envoie un nonce au client qui va créer une clé de session temporaire la PTK basée sur la PMK, des nonces et l'adresse MAC du client et de l'AP.
2. Le client envoie à l'AP son SNONCE qui peut lui aussi maintenant générer la PTK.
3. L'AP envoie au client le GTK (Group Transient Key)
4. Le client envoie une confirmation au AP pour indiquer que les clés de chiffrement ont été correctement établies.

Ces quatre étapes du "4-way handshake" garantissent l'authentification mutuelle et l'établissement de clés de chiffrement sécurisées entre le client et le point d'accès.

Hole196

Cette attaque rendue publique en 2010 permet à un attaquant, ayant connaissance de la clé partagée du réseau, de réaliser une attaque de l'homme du milieu et ainsi accéder ou modifier les données des autres utilisateurs du réseau. Elle peut aussi permettre de réaliser une attaque de type DoS.

Le nom de l'attaque Hole 196 fait référence à la page 196 de la description du standard WPA2 où se trouve cette vulnérabilité. En particulier, le standard précise que contrairement aux PTK, les GTK ne possèdent pas de propriété de détection d'usurpation d'adresse et de falsification de données. Si un client diffuse un paquet GTK spécialement conçu, les autres clients vont répondre avec leur propre adresse MAC et information de clé privée.

Bien que cette vulnérabilité ne soit aujourd'hui pas corrigée, il est important de noter que son exploitation est limitée. En effet, l'attaquant doit déjà avoir accès à la clé partagée PSK pour pouvoir mettre en œuvre cette attaque.
Sur les réseaux utilisant une clé partagée, comme WPA/WPA2 Personal, cette attaque est en grande partie sans conséquence car un utilisateur possédant la clé, commune à tous les utilisateurs du réseau, peut intercepter le trafic des autres utilisateurs.
Cependant, cette vulnérabilité peut être plus dangereuse pour les réseaux WPA/WPA2 Entreprise, qui reposent sur le standard 802.1X qui permet un contrôle d'accès.

MS-CHAPv2

WPA2-Entreprise qui se base sur le protocole EAP est parfois configuré avec MSCHAPv2 en raison de la facilité de mise en place sur une infrastructure Windows.
Cependant, il est important de savoir que plusieurs vulnérabilités ont été trouvées dans le protocole MSCHAPv2 dont une qui notamment permet de réduire la complexité de "cassage" de MS-CHAPv2 à celle de casser une seule clé DES.
Pour se protéger contre l'exploitation de cette vulnérabilité, les méthodes d'authentification EAP tunnelisées comme TTLS ou PEAP sont utilisées pour chiffrer l'échange MSCHAPv2. Cependant, ces configurations peuvent être aussi vulnérables à une attaque Man In The Middle ce qui peut permettre de récupérer les identifications et mots de passe des utilisateurs du réseau.

Attaque sur le WPS

Wi-Fi Protected Setup (WPS) est un standard apparu en 2006 qui facilite la configuration sécurisée des équipements connectés à un réseau Wi-Fi. Il a été développé pour permettre aux utilisateurs sans connaissances approfondies en sécurité de configurer un accès Wi-Fi en facilitant l'ajout de nouveaux appareils à un réseau existant sans avoir à saisir une longue phrase secrète (passphrase).
WPS propose quatre méthodes pour ajouter un nouveau périphérique à un réseau domestique :

- La méthode PIN : un code doit être saisi au niveau du point d'accès ou du nouvel appareil pour établir la connexion.
- La méthode Push Button : l'utilisateur appuie sur un bouton, physique ou virtuel, à la fois sur le point d'accès et sur le nouvel appareil pour les synchroniser.
- La méthode NFC : l'utilisateur approche le nouvel appareil du point d'accès pour établir une communication entre eux.
- La méthode USB : l'utilisateur utilise une clé USB pour transférer les données de configuration entre le nouvel appareil et le point d'accès.

En 2011, une vulnérabilité affectant la méthode PIN est découverte. Cette faille permet à un attaquant distant de récupérer le code PIN WPS en quelques heures et donc la capacité de

se connecter au réseau. Ainsi la méthode PIN est petit à petit abandonnée. Cette attaque est une simple attaque par force brute facilitée par les messages de retour d'erreur de code PIN qui permettent de savoir si les quatre premiers ou les quatre derniers chiffres du code PIN sont corrects ou non.
Une défense possible est la mise en place d'un système de verrouillage après l'échec d'une authentification WPS.

En 2014, l'attaque Pixie Dust est rendue publique. Cette attaque fonctionne uniquement sur l'implémentation par défaut de WPS de plusieurs fabricants (Ralink, MediaTek, Realtek et Broadcom). L'attaque se concentre sur un manque de randomisation qui permet de récupérer le code PIN en quelques minutes seulement.

Enfin, il convient de noter que les méthodes WPS sont vulnérables si le point d'accès sans fil n'est pas conservé dans une zone physique sécurisée.

Attaques KRACK

https://www.krackattacks.com/
En 2017, les chercheurs Vanhoef et Piessens (chercheurs ayant déjà publié des améliorations de l'attaque de Beck-Tews sur TKIP) rendent publique une vulnérabilité nommée KRACK (Key Reinstallation Attack) qui est une attaque par rejeu sur le protocole Wi-Fi.
La faiblesse se trouve dans le standard Wi-Fi lui-même et non dans une implémentation, par conséquent toutes les plateformes (Windows, Mac et Linux) sont concernées par l'attaque. En particulier, les auteurs de l'attaque précisent que les effets de cette dernière sont particulièrement "catastrophiques" sur wpa_supplicant. Il s'agit d'une implémentation open source largement utilisée notamment sur Linux et Android car au lieu de réinstaller la clef c'est une clef composée uniquement de zéro qui est installée à la place. Ainsi, il est possible de déchiffrer l'ensemble du trafic sans avoir à effectuer de manipulations supplémentaires.

Il existe plusieurs attaques possibles mais une version simple vise la troisième étape du 4-ways handshake de WPA2**.** En réinitialisant plusieurs fois le nonce en transmettant le message 3, un attaquant peut découvrir la clé de chiffrement du trafic.
En détail, lors du handshake l'attaquant se place entre la station (appareil client) et le point d'accès Wi-Fi via une attaque de l'homme du milieu (Man In the Middle). Lorsque la station envoie le message 4 au point d'accès, l'attaquant bloque ce message, ce qui fait réagir le point d'accès en renvoyant un nouveau message 3. L'attaquant transmet alors ce nouveau message 3 à la station. La station, suivant le protocole, envoie une réponse sous la forme d'un message 4 chiffré puis la station réinstalle les clés de chiffrement.
À ce stade, la station envoie des données dans une trame qui est chiffrée avec la même clé que celle utilisée pour le message 4 précédent. Les deux messages partagent le même nonce et le même keystream. Il devient alors facile en utilisant les propriétés du XOR de déchiffrer ce message en utilisant le contenu du message 4 chiffré pour déduire le keystream, puis en combinant le keystream avec le message chiffré pour obtenir le contenu en clair.
Il est important de noter que l'attaquant doit se trouver à portée à la fois du client visé et du réseau lui-même. Cependant les auteurs précisent qu'un attaquant éloigné jusqu'à 12 kilomètres peut mettre en œuvre l'attaque.

De nombreux correctifs de sécurité ont été proposés pour les différentes plateformes et équipements https://github.com/kristate/krackinfo.
On peut tester la vulnérabilité de ses équipements avec ces scripts https://github.com/vanhoefm/krackattacks-scripts.

Attaque Kr00k

https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf
Publiée en 2019, l'attaque Kr00k (ou KrØØk) est une vulnérabilité qui permet de déchiffrer une partie du trafic chiffré avec WPA2. Au moment de la révélation de l'attaque, il a été estimé que cette vulnérabilité affecte plus d'un milliard d'appareils.
Elle a été découverte à partir de l'analyse de variantes de l'attaque KRACK, elle est étonnamment simple mais semble moins inquiétante par rapport à KRACK.
En résumé, cette attaque exploite le fait que lors de la clôture d'une connexion sans fil WPA2, des informations encore en mémoire sont transmises en clair.

Kr00k se manifeste après une dissociation (lorsqu'un client désactive le WI-Fi sur son appareil par exemple). Cette procédure est régie par des trames qui ne sont pas authentifiées et chiffrées. Ainsi, un attaquant peut manuellement déclencher une dissociation.
Il a été montré que la clé de session (TK) stockée dans la puce Wi-Fi est effacée de la mémoire et mise à zéro car aucune autre donnée ne doit être transmise après la dissociation. Cependant, les chercheurs ont découvert que tous les paquets de données qui étaient restés dans le tampon d'émission de la puce étaient transmis après avoir été chiffrés avec cette clé mise à zéro.
Ces paquets de données, qui peuvent contenir des informations sensibles, peuvent être capturés par un attaquant et ensuite déchiffrés.
En déclenchant plusieurs dissociations à la suite, l'attaquant peut capturer un nombre important de paquets.
De plus, l'attaquant n'a même pas besoin d'être connecté au réseau pour réaliser cette attaque, il peut utiliser le mode moniteur https://fr.wikipedia.org/wiki/Mode_moniteur.

Ce qui est très préoccupant avec cette attaque, c'est que les appareils clients mais aussi les points d'accès Wi-Fi et les routeurs peuvent être affectés par Kr00k. Cela signifie que même si certains appareils clients ne sont pas affectés par la vulnérabilité ils peuvent être connectés à un point d'accès qui est vulnérable. Ainsi, la surface d'attaque est considérablement augmentée, car un attaquant peut déchiffrer les données transmises par un point d'accès vulnérable à un client spécifique (qui peut être vulnérable ou non).

Cependant il convient de noter que cette attaque peut être exploitée pour casser le chiffrement utilisé pour sécuriser le canal WiFi mais si les communications originales de l'utilisateur étaient déjà chiffrées (HTTPS) alors ces communications resteront sécurisées même après une attaque.
De plus, comme KRACK, une proximité géographique est nécessaire pour réaliser cette attaque.
Ces points permettent de diminuer fortement l'impact de l'attaque.

Autres attaques

WPA et WPA2 ne garantissent pas une confidentialité persistante. En effet, si un attaquant récupère la PSK, il peut déchiffrer les paquets chiffrés avec cette clé, même s'il s'agit de paquets chiffrés dans le passé ou dans le futur.
De plus, WPA et WPA2 protègent uniquement contre les attaquants qui n'ont pas accès à la PSK, cela signifie que dans les lieux publics les attaquants peuvent capturer et déchiffrer les données des autres utilisateurs car la PSK est généralement partagée avec tout le monde. Pour une meilleure sécurité, il est recommandé d'utiliser une couche de sécurité supplémentaire telle que Transport Layer Security (TLS) lors de la transmission des données. Ce problème a été résolu avec l'introduction de WPA3.

Il est important de noter que WPA et WPA2 sont vulnérables aux attaques de craquage de mot de passe si les utilisateurs choisissent une phrase secrète faible. En effet, des rainbow tables (tables arc-en-ciel), structures de données optimisées pour retrouver un mot de passe à partir de son hash, peuvent être utilisées pour casser WPA et WPA2.

WEP, WPA et WPA2 peuvent être vulnérables à une attaque de désauthentification Wi-Fi qui est un type particulier d'attaque par déni de service.
En effet, le point d'accès peut envoyer à une station une trame de désauthentification qui permet d'indiquer à un appareil qu'il n'est plus authentifié. Le protocole n'exigeant pas que ces trames soient chiffrées, un attaquant peut simplement envoyer une telle trame pour déconnecter un appareil. L'attaquant a besoin seulement de l'adresse MAC de la victime qui peut être récupéré en clair en "écoutant" le réseau.
L'extension 802.11w permet de se protéger de ce type d'attaque.

https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_vanhoef.pdf
Enfin en 2016, Vanhoef et Piessens (encore eux) ont démontré que les normes WPA et WPA2 contiennent un générateur de nombres aléatoires non sécurisé. Ainsi, un attaquant pourrait être capable de prédire la clé de groupe (GTK) qui est censée être générée de manière aléatoire par le point d'accès. De plus, il a été montré que la possession de la GTK permet à l'attaquant d'injecter et de déchiffrer du trafic unicast.
Les fabricants doivent utiliser un générateur de nombres aléatoires sécurisé pour se protéger contre cette attaque.

Outils

Concernant l'attaque sur MSCHAPv2, ces outils peuvent être utiles https://github.com/moxie0/chapcrack et https://github.com/sensepost/hostapd-mana.

L'attaque par force brute sur le code PIN du WPS est réalisable via plusieurs outils https://github.com/t6x/reaver-wps-fork-t6x et https://www.kali.org/tools/bully/.

Une implémentation de l'attaque Pixie dust (WPS) est disponible via l'outil pixiewps https://www.kali.org/tools/pixiewps/.

Une implémentation de l'attaque Kr00k est disponible via l'outil r00kie-kr00kie. https://github.com/hexway/r00kie-kr00kie.

Aircrack-ng propose aussi de nombreux outils qui permettent de mettre en œuvre les attaques présentées précédemment https://aircrack-ng.org/documentation.html.

Défenses

Bien qu'aujourd'hui WPA2 soit considéré comme sûr, la protection est réelle si les équipements (appareils et point d'accès) utilisés ont reçu un correctif de sécurité permettant de protéger contre les dernières attaques.
En effet, ces dernières années, les mises à jour de ces attaques (Krack, Kr00k) ne dépendent plus du protocole en lui-même mais des constructeurs, ce qui peut être problématique au niveau sécurité. Ainsi, un nouveau protocole semblait nécessaire.

WPA3

Présentation

Le WPA3, annoncé en 2018 par la Wi-Fi Alliance, est aujourd'hui la dernière norme de sécurité pour les réseaux Wi-Fi.
Il offre des améliorations significatives de sécurité en introduisant de nouveaux concepts pour pallier aux faiblesses de WPA2.
Depuis juillet 2020, la prise en charge de WPA3 est obligatoire pour les appareils portant le logo Wi-Fi.

Eléments techniques

La Wi-Fi Alliance a décidé d'inclure certaines des améliorations de WPA3 dans une version améliorée de WPA2 qui vise à renforcer la sécurité de ce dernier. Parmi ces améliorations, on peut trouver :

- Utilisation obligatoire du Protected Management Frames (PMF) : permet de garantir l'intégrité du trafic de gestion du réseau. Cela permet de protéger contre l'écoute clandestine, les attaques de rejeu et la falsification des trames de gestion. En particulier, cela offre une protection contre les attaques de déni de service utilisant la déauthentification où un adversaire tente de déconnecter de force des clients d'un réseau Wi-Fi en falsifiant ces trames.
- Validation renforcée des implémentations de sécurité des fournisseurs : des tests supplémentaires sur les appareils certifiés Wi-Fi sont nécessaires pour réduire les vulnérabilités dues à une mauvaise configuration ou à une mise en œuvre défectueuse. En particulier, des tests mettant en œuvre les attaques connues comme Krack.
- Meilleure cohérence dans la configuration de sécurité du réseau : définir un ensemble de suites de chiffrement sécurisées pour assurer que tous les composants de sécurité ont une force cryptographique similaire.

WPA3 introduit de nouveaux concepts qui apportent une sécurité supplémentaire au regard de ses prédécesseurs.

WPA3 introduit une nouvelle poignée de main appelée "Simultaneous Authentication of Equals" (SAE).
SAE est une variante de Dragonfly Key Exchange (basé sur l'échange de clés Diffie-Hellman utilisant des groupes cycliques finis) qui ajoute un mécanisme d'authentification.
SAE oblige une interaction avec le point d'accès pour tester un mot de passe ce qui limite ainsi le nombre de tentatives et offre une résistance aux attaques par force brute et dictionnaire dite "hors ligne".
De plus, cette nouvelle poignée de main garantit la "forward secrecy" car le mot de passe de chiffrement est renouvelé à l'établissement de chaque nouvelle connexion. Ainsi la confidentialité des anciens trafics est préservée en cas de compromission du mot de passe.

WPA3 (via le mode Easy Connect) remplace le protocole WPS par le protocole Device Provisioning Protocol (DPP). Ce nouveau protocole permet une configuration et une

intégration sécurisées des appareils sur le réseau en utilisant des codes QR, des mots de passe, NFC ou Bluetooth. DPP utilise des clés publiques pour l'identification et l'authentification des appareils, assurant ainsi une meilleure sécurité lors de l'ajout de nouveaux appareils au réseau.
Cela permet la configuration des appareils qui ne disposent pas d'une interface utilisateur suffisante en permettant aux appareils à proximité de servir d'interface utilisateur adéquate à des fins de configuration réseau.

WPA3 (via le mode Enhanced Open) renforce la confidentialité des utilisateurs sur les réseaux ouverts grâce à un chiffrement des données individualisé. Il introduit la méthode de chiffrement Opportunistic Wireless Encryption (OWE), qui empêche un attaquant passif de lire le trafic des clients connectés à un point d'accès public. Cependant, les attaques actives, telles que la création d'un faux point d'accès, restent possibles.

WPA3 prend en charge des tailles de clés plus grandes et utilise l'algorithme de chiffrement Galois/Counter Mode (GCM). Ces améliorations permettent un chiffrement de 128 bits en WPA3 Personal et 192 bits en WPA3 Entreprise.

Attaques Dragonblood

https://papers.mathyvanhoef.com/dragonblood.pdf et https://wpa3.mathyvanhoef.com/
En 2019, un an après l'annonce de WPA3 par la Wi-Fi Alliance, Mathy Vanhoef et Eyal Ronen ont publié plusieurs vulnérabilités regroupées sous le nom Dragonblood qui permettent de réaliser des attaques sur WPA3. On retrouve des attaques très différentes comme : les attaques de rétrogradation (downgrade), les attaques de réduction du groupe de sécurité, les attaques par canal secondaire basées sur le cache, les attaques par canal secondaire basées sur le timing et les attaques par déni de service.

Attaques de rétrogradation : Les attaques de rétrogradation ciblent les réseaux WPA3 en mode transition (WPA3-transition). Dans ce mode, un réseau Wi-Fi prend en charge à la fois WPA3 et WPA2 avec un mot de passe identique. En créant un réseau imposteur qui ne prend en charge que WPA2, même les clients WPA3 sont trompés pour utiliser WPA2. Cela permet à l'attaquant de réaliser des attaques par dictionnaire et par force brute contre les mots de passe des réseaux WPA3.

Attaque de réduction du groupe de sécurité : Pendant la phase d'engagement du handshake Dragonfly, l'initiateur (généralement le client en cas de WPA3) envoie sa première trame d'engagement avec son groupe de sécurité préféré. Si l'AP ne prend pas en charge ce groupe spécifique, il répond par un message de refus, forçant le client à utiliser un groupe potentiellement moins sûr. En interceptant les engagements des clients et en envoyant de faux messages de refus, un attaquant peut forcer le client à utiliser un groupe de son choix et notamment un groupe considéré comme plus faible.

Attaque par canal secondaire basée sur le timing : Lors de l'utilisation de certains groupes de sécurité, le temps mis par un AP pour répondre à une trame d'engagement dépend du mot de passe utilisé. Cette information divulguée permet à un attaquant de réaliser une attaque par dictionnaire en comparant le temps attendu pour un mot de passe avec le temps de réponse réel de l'AP.

Attaque par canal secondaire basée sur le cache : Ces attaques nécessitent qu'un attaquant puisse observer le schéma d'accès à la mémoire d'une des parties du handshake Dragonfly. Les schémas d'accès à la mémoire pendant la génération d'une trame d'engagement permettent à l'attaquant d'obtenir des informations sur le mot de passe utilisé. Ces informations peuvent être utilisées pour des attaques par dictionnaire en comparant les motifs observés avec les motifs attendus d'un mot de passe supposé.

Attaque par déni de service : En raison du coût de calcul élevé de la phase d'engagement du handshake Dragonfly, un attaquant peut facilement surcharger un AP en envoyant de fausses trames d'engagement. Cela entraîne une utilisation élevée du processeur de l'AP, ce qui peut provoquer des retards, voire empêcher l'utilisation normale de l'AP. Ces attaques peuvent être aggravées en fonction de la mise en œuvre des défenses contre les attaques par canal secondaire décrites précédemment, en raison de la nécessité de calculs supplémentaires.

Ces attaques montrent qu'un attaquant à portée d'un réseau peut récupérer le mot de passe de ce réseau. Cela peut permettre à l'attaquant de voler des informations sensibles notamment si la victime n'utilise pas de chiffrement supplémentaire comme TLS avec le protocole HTTPS.

Outils

Plusieurs scripts publiés par Mathy Vanhoef permettent de tester certaines vulnérabilités du protocole WPA3 :

- Dragonslayer https://github.com/vanhoefm/dragonslayer : met en œuvre des attaques contre EAP-pwd avec WPA3.
- Dragondrain https://github.com/vanhoefm/dragondrain-and-time : permet de tester dans quelle mesure un point d'accès utilisant SAE de WPA3 est vulnérable aux attaques de déni de service.
- Dragontime https://github.com/vanhoefm/dragondrain-and-time : permet de réaliser des attaques chronométrées (timing attacks) sur SAE si certains groupes de Diffie-Hellman sont utilisés.

Défenses

Bien que WPA3 ait été conçu pour résoudre la plupart des vulnérabilités de WPA2, les attaques Dragonblood révèlent des failles majeures dans son fonctionnement remettant en question sa viabilité à long terme en tant que norme de sécurité. Les vulnérabilités actuelles permettent des attaques par dictionnaire et par force brute sur les mots de passe des réseaux WPA3, annulant ainsi l'un des principaux avantages de WPA3 par rapport à WPA2.

L'attaque de rétrogradation contre le mode de transition, bien que théoriquement temporaire, est très problématique. Étant donné que l'adoption de WPA3 jusqu'à la dépréciation complète de WPA2 prendra probablement plusieurs années, de nombreux réseaux WPA3 seront utilisés en mode de transition. Cela signifie que tant que cette vulnérabilité ne sera pas corrigée, tous ces AP seront vulnérables aux attaques par dictionnaire et par force brute.

La mise en œuvre de défenses contre les attaques par canal secondaire connues actuellement s'est avérée difficile et fastidieuse, et elles ont également augmenté les exigences de calcul déjà élevées de WPA3, ce qui pose problème pour les appareils qui ne peuvent pas les mettre en œuvre. Par conséquent, des mises à niveau coûteuses du matériel peuvent devenir nécessaires.

Tout cela rend l'avenir de WPA3 très incertain, car il dépendra de la faisabilité des solutions possibles, ce qui nécessite des recherches supplémentaires. Malgré ces problèmes, WPA3 reste une amélioration significative par rapport à WPA2 en termes de sécurité et devrait continuer à être utilisé pour le moment.

Conclusion

Le protocole WPA a été développé comme une solution d'urgence pour remédier aux vulnérabilités du protocole WEP. Il visait à fournir une meilleure sécurité pour les réseaux Wi-Fi.
Ensuite, le WPA2 a été développé en tant que solution à plus long terme, avec pour objectif d'être fiable pendant de nombreuses années. Malgré les attaques auxquelles il a été soumis, le WPA2 est considéré comme résistant et continue d'être largement utilisé.
Le WPA3, solution la plus récente, a été introduit pour renforcer la sécurité des réseaux Wi-Fi en réponse aux attaques précédentes. Il apporte aussi des sécurités supplémentaires pour protéger les communications et les données des utilisateurs.
Cependant, il a été montré que le fait d'avoir une preuve formelle d’un protocole ne signifie pas que ce dernier est totalement sécurisé. La sécurité est un processus continu, et de nouvelles vulnérabilités et attaques peuvent émerger avec le temps. Il est donc essentiel de rester vigilant, de suivre les mises à jour de sécurité et d'adopter les meilleures pratiques pour maintenir la sécurité de son réseau Wi-Fi.

Sources

- https://dl.aircrack-ng.org/breakingwepandwpa.pdf
- https://fr.wikipedia.org/wiki/IEEE_802.11
- https://fr.wikipedia.org/wiki/Wi-Fi
- https://fr.wikipedia.org/wiki/Wired_Equivalent_Privacy
- https://fr.wikipedia.org/wiki/Wi-Fi_Protected_Access
- https://archipel.uqam.ca/4850/1/M9822.pdf
- https://cisco.goffinet.org/ccna/wlan/protocoles-securite-sans-fil-wpa-wpa2-wpa3
- https://cylab.be/blog/32/how-does-wpawpa2-wifi-security-work-and-how-to-crack-it
- https://papers.mathyvanhoef.com/ccs2017.pdf
- https://medium.com/@alonr110/the-4-way-handshake-wpa-wpa2-encryption-protocol-65779a315a64
- https://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup
- https://en.wikipedia.org/wiki/KRACK
- https://connect.ed-diamond.com/GNU-Linux-Magazine/glmfhs-099/comprendre-les-attaques-krack
- https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/ctr-cybersecurity-technical-report-wpa3.pdf
- https://www.mathyvanhoef.com/2018/03/wpa3-technical-details.html
- https://wpa3.mathyvanhoef.com/
- https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2020-11-1/NET-2020-11-1_02.pdf
- https://papers.mathyvanhoef.com/dragonblood.pdf