ENSIAS

Rapport WEP

Réalisé par :
EL MANITI MOHAMMED
ES-SBAIY OUMAIMA
LOUKAH MOHAMMED-AYMANE
EL YOUBI OUMAIMA
BENLKHDIM AZHAR
RAJOUL ABDELJALIL
HANANE EL MESKINE
ICHIOUI YOUSSEF
EL JADDAOUI MOHAMMED
JEBARI BOUTAINA

Encadré par :
Mr.Amine Berquia

19 avril 2019

Table des figures

Table des matières

Introduction

L'IEEE 802,11 dispose de deux modes de fonctionnement de base : l'infrastructure et le mode ad hoc. Au moment où, en mode ad hoc, les unités mobiles transmettent directement peer-to-peer, en mode infrastructure, les unités mobiles communiquent via un point d'accès qui sert de passerelle vers d'autres réseaux (tels que Internet ou LAN).

Etant donné que la communication sans fil utilise un médium plus ouvert pour la communication par rapport aux réseaux locaux câblés, comment peut-on alors assurer le volet sécuritaire dans un tel environnement ? Pour renforcer le volet sécuritaire, les concepteurs de 802,11 ont ainsi inclus des mécanismes de cryptage : Wired équivalent Privacy (WEP), Wi-Fi Protected Access (WPA, WPA2, WPA3), pour sécuriser les réseaux informatiques sans fil.

Le présent projet a pour objet de configurer le routeur Cisco Aironet 1200 en intégrant les protocoles Wep et les WPA, aux fins de récupération des clés y afférentes. Par ailleurs, et dans le même esprit sécuritaire, une couche d'authentification sera assurée par le protocole Radius, empêchant tout utilisateur non inscrit au serveur d'accéder au réseau.

Chapitre 1

Etude théorique sur le WLAN infrastructure

1.1 wlan

Le principe de la technologie Wi-Fi est d'établir des liaisons radio entre des équipements terminaux. Ces équipements peuvent être des stations et des points d'accès permettant de se connecter sur un réseau local, puis sur Internet. Il existe trois modèles de déploiementd'un réseau WI-FI :ad hoc, infrastructure, et hybride.

1.1.1 Le mode infrastructure

En mode infrastructure chaque ordinateur station (notée STA) se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situés dans sa zone de couverture est appelé ensemble de services de base (en anglais basic service set, noté BSS) et constitue une cellule. Chaque BSS est identifié par un BSSID, un identifiant de 6 octets (48 bits). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès.

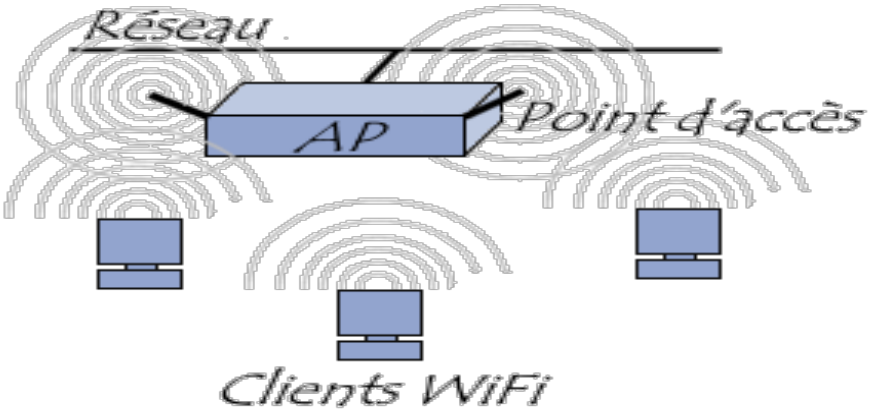

FIGURE 1.1 – infrastructure des wlans

Il est possible de relier plusieurs points d'accès entre eux (ou plus exactement plusieurs BSS) par une liaison appelée système de distribution (notée DS pour Distribution System) afin de constituer un ensemble de services étendu (extended service set ou ESS). Le système de distribution (DS) peut être aussi bien un réseau filaire, qu'un câble entre deux points d'accès ou bien même un réseau sans fil !

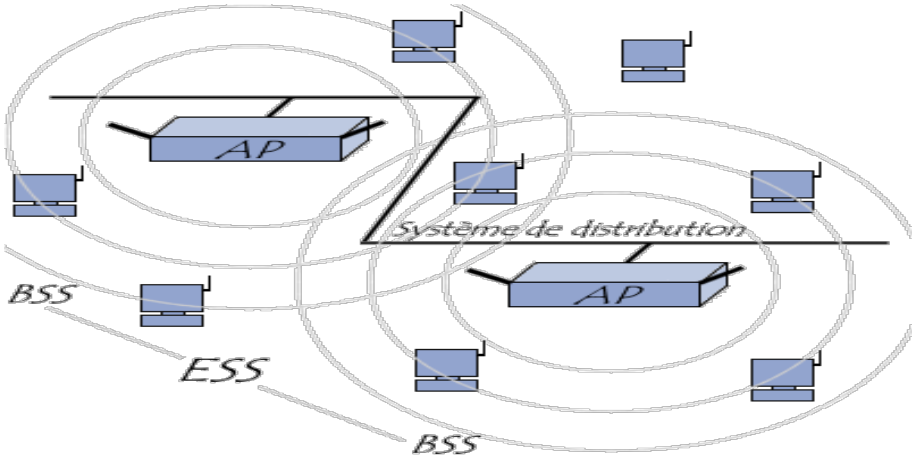

FIGURE 1.2 – Architecture Schéma

Un ESS est repéré par un ESSID (Service Set Identifier), c'est-à-dire un identifiant de 32 caractères de long (au format ASCII) servant de nom pour le réseau. L'ESSID, souvent abrégé en SSID, représente le nom du réseau et représente en quelque sort un premier niveau de sécurité dans la mesure où la connaissance du SSID est nécessaire pour qu'une station se connecte au réseau étendu.

Lorsqu'un utilisateur nomade passe d'un BSS à un autre lors de son déplacement au sein de l'ESS, l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès. Les points d'accès communiquent entre eux grâce au système de distribution afin d'échanger des informations sur les stations et permettre le cas échéant de transmettre les données des stations mobiles. Cette caractéristique permettant aux stations de "passer de façon transparente" d'un point d'accès à un autre est appelé itinérance (en anglais roaming).

Connexion à un réseau Wi-Fi en mode infrastructure

d'après ce qui précède on dire que La connexion d'une station à un AP s'effectue en deux phases. La première correspond à une phase d'authentification, la seconde à l'association.

1.1.2 La communication avec le point d'accès

Lors de l'entrée d'une station dans une cellule, celle-ci diffuse sur chaque canal un requête de sondage (probe request) contenant l'ESSID pour lequel elle est configurée ainsi que les débits que son adaptateur sans fil supporte. Si aucun ESSID n'est configuré, la station écoute le réseau à la recherche d'un SSID.

En effet chaque point d'accès diffuse régulièrement (à raison d'un envoi toutes les 0.1 secondes environ) une trame balise (nommée beacon en anglais) donnant des informations sur son BSSID, ses caractéristiques et éventuellement son ESSID. L'ESSID est automatiquement diffusé par défaut, mais il est possible (et recommandé) de désactiver cette option.

A chaque requête de sondage reçue, le point d'accès vérifie l'ESSID et la demande de débit présents dans la trame balise. Si l'ESSID correspond à celui du point d'accès, ce dernier envoie une réponse contenant des informations sur sa charge et des données de synchronisation. La station recevant la réponse peut ainsi constater la qualité du signal émis par le point d'accès afin de juger de la distance à laquelle il se situe. En effet d'une manière générale, plus un point d'accès est proche, meilleur est le débit.

Une station se trouvant à la portée de plusieurs points d'accès (possèdant bien évidemment le même SSID) pourra ainsi choisir le point d'accès offrant le meilleur compromis de débit et de charge.

1.2 le protocole WEP

1.2.1 Définition

Le protocole WEP (Wired Equivalent Privacy) fait partie de la norme internationale IEEE 802.11 ratifiée en septembre 1999. Il est très répandu et implémenté dans un grand nombre de cartes réseaux sans fil. Le WEP prétend (comme son l'indique) offrir une solution de confidentialité équivalente à un réseau filaire. En effet, les réseaux câblés sont, par nature, plus sécurisés que les réseaux sans fil car il faut se brancher physiquement sur le réseau. Il ne fut cependant pas créer par des experts en cryptographie. D'un point de vue plus théorique, il protège les communications de la couche liaisons de données (niveau 2 du modèle OSI).
Le WEP est employé dans un WLAN pour rendre inintelligible à un tiers non autorisé les données encapsulées dans des trames. (Un paquet ne peut en effet pas transiter directement sur un réseau.) Le WEP a pour objectif de satisfaire l'association (s'assurer qu'on discute avec les membres du même WLAN), la confidentialité, l'authentification et l'intégrité. Il est défini comme :

- **assez fort (reasonably strong) :** La longueur des clés utilisées rend difficile une attaque de type force brute, c'est-à-dire avec l'utilisation de toutes les clés possibles.
- **à synchronisation automatique (self synchronizing) :** Chaque paquet contient assez d'informations pour permettre à quiconque possède la clé de déchiffrer son contenu. La connaissance du contenu des paquets précédant n'intervient pas dans le déchiffrement. Autrement dit, les paquets sont autonomes.
- **efficace (efficient) :** Sa simplicité fait qu'il peut être implémenté en logiciel aisément. Cela signifie aussi que les opérations de chiffrement et de déchiffrement sont rapides.
- **normalement exportable :** Le standard WEP utilise une longueur de clé variable (jusqu'à 2048 bits mais les USA limitent la taille des clés à l'export).
- **optionnel :** La mise en place et l'utilisation du WEP dans les équipements sont en effet optionnelles.

1.2.2 Le chiffrement WEP

1.2.2.1 Fonctionnement général :

Le WEP (Wired Equivalent Privacy) est un protocole qui permet (en théorie, tout du moins) d'éviter le eavesdropping (écoute clandestine) en chiffrant les communications. Il peut être utilisé pendant la phase d'authentification ou encore pour chacune des trames de données. Il repose sur l'algorithme à clé symétrique RC4. Le mécanisme de distribution des clés n'est pas précisé. Elles doivent dont être saisis manuellement sur les stations et les AP.

C'est dans le champ de contrôle FC (Frame Control) des trames de données et d'authentification qu'est précisée l'utilisation du chiffrement WEP. Le bit positionné à 1 signifie que le corps de la trame est chiffré en WEP.
Le chiffrement se décompose en plusieurs phases :

- La création de la graine
- La création du keystream
- Le calcul ICV
- La constitution du message final et son encapsulation dans une trame

a-Le vecteur d'initialisation :
Le vecteur d'initialisation (IV – Initialization Vector) est une séquence de bits qui change régulièrement (à chaque trame envoyée si l'implémentation est bonne). Combiné à la clé statique, il introduit une notion aléatoire au chiffrement. Ainsi, deux messages identiques ne donneront pas le même contenu chiffré, puisque l'IV est dynamique[2].

La longueur du IV est de 24 bits, soit 224 valeurs possibles. Cela laisse à penser que l'IV ne sera pas réutilisé plusieurs fois.

Comme la clé, le IV doit être connu à la fois de l'émetteur et du récepteur. La solution d'un mécanisme de génération automatique qui devrait être présent sur tous les équipements n'a pas été retenue car elle est difficile à mettre en place. Le IV est donc transporté en clair dans les trames.

Remarque : Certains systèmes sophistiqués offrent des mécanismes de synchronisation qui dérivent des clés de façon automatique et sûre.

b- L'algorithme RC4 dans WEP :

RC4 est un algorithme de chiffrement par flux (par flot ou encore sans état) à clé symétrique développé en 1987 par Ronald Rivest (l'un des créateurs du RSA). RC4 ne nécessite pas trop de puissance de calcul. Il est extrêmement rapide (environ dix fois plus rapide que le DES). Il est considéré comme fiable mais une mauvaise implémentation peut entraîner des failles. Cet algorithme reprend le principe du masque jetable (OTP – One Time Pad ou masque de Vernam). En effet, on génère un flux de données de taille identique au flux de données claires et on fait un XOR entre les deux, le déchiffrement se fait par XOR entre le chiffré et le même flux pseudo-aléatoire[2].

Le procédé mathématique est né d'un vide technique laissé par d'autres procédés de chiffrement extrêmement efficaces mais très gourmands en puissance de calcul. Le gros avantage de RC4 est qu'il fournit un niveau de sécurisation assez élevé, tout en étant implantable de façon logicielle, donc à faible coût. RC4 est l'un des protocoles de chiffrement les plus utilisés dans le monde.

Deux étapes sont nécessaires pour l'opération de chiffrement :

— L'initialisation de la clé

— La réalisation du cryptogramme (texte chiffré ou cyphertext)

clé d'origine :

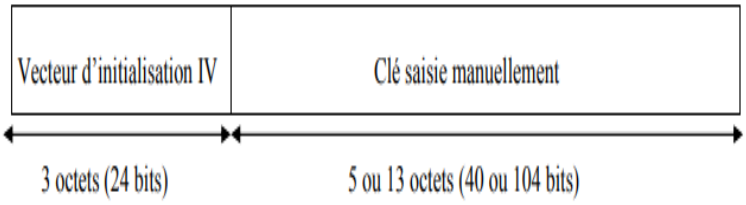

FIGURE 1.3 – le vecteur de la clé

Une table de 256 octets (généralement) est formée. Elle est initialisée en reportant la graine autant de fois que nécessaire. A partir de la même clé, on obtient donc la même table à l'issue de la phase d'initialisation. On appellera ce tableau S (comme seed) par la suite.

1.2.3 Le contrôle d'intégrité

Le WEP prévoit un mécanisme nommé Integrity Check Value (ICV), destiné à contrôler l'intégrité des séquences WEP dites trames (frames en anglais). Pour cela, un code équivalent au CRC32 (i.e. sur 32 bits) est calculé. Il résulte du message en clair M et non du contenu chiffré. Le CRC32 correspond en fait au reste dans la division en binaire du message par un diviseur fixé à l'avance. NB : Le CRC32 est parfois désigné sous l'appellation de FCS (Frame Check Sequence).

Le résultat du calcul d'intégrité : ICV(M) est ensuite concaténé au payload M : M||ICV(M), puis chiffré avec la clé. La clé WEP est donc indispensable pour l'interpréter.

La modification de la trame chiffrée semble inconcevable sans la clé puisque le résultat de l'ICV changerait.

1.2.4 Le déchiffrement WEP

On détient dans la trame deux informations en clair : le KeyID et l'IV. On récupère la graine en concaténant la clé WEP indiquée par le Key ID avec l'IV qui se trouve en clair dans la trame.
On peut retrouver alors le keystream utilisé pour le chiffrement. On opère un XOR entre le cryptogramme et le keystream et on récupère ainsi le payload et le CRC. Prenons un message chiffré C, un plaintext P et une graine G, on a : C + RC4(G) = (P + RC4(G)) + RC4(G) = P
On applique alors l'algorithme de contrôle d'intégrité et on peut dès lors comparer les résultats. Si les résultats coïncident, la trame est acceptée, sinon elle est rejetée et supprimée. La probabilité qu'un contrôle d'intégrité se révèle positif alors que la clé utilisée serait invalide est considérée comme nulle[2].

Opérations de chiffrement et de déchiffrement (schéma complet) :

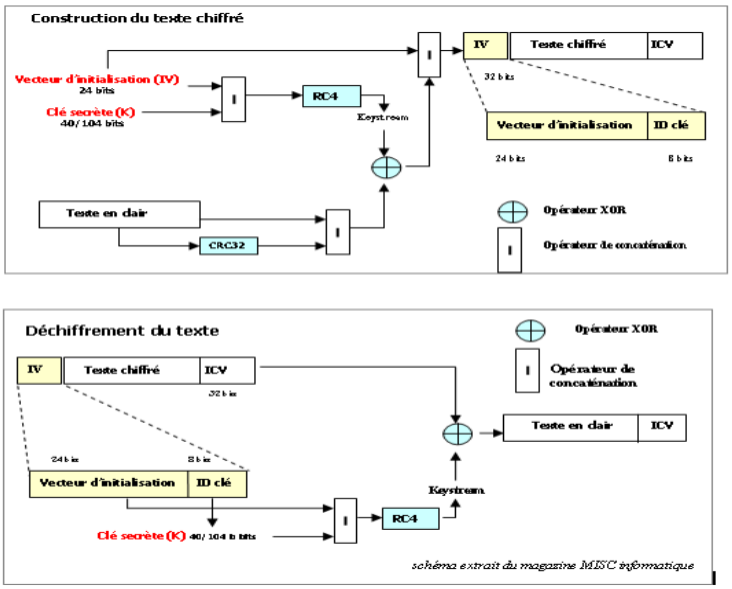

FIGURE 1.4 – processus de chifferement et déchifferement

1.3 le protocole WPA

1.3.1 Définition

WPA (Wi-Fi Protected Access) est un mécanisme pour la sécurisation des réseaux sans fils de type WI-FI. Il a été créé en 2000 en réponse aux nombreuses faiblesses que les chercheurs ont trouvées dans le WEP. Il respecte la majorité de la norme IEEE 802.11i. WPA utilise en général le protocole de chiffrement TKIP.

WPA-PSK : Le fonctionnement de WPA repose sur la mise en œuvre d'un serveur d'authentification (la plupart du temps un serveur RADIUS), permettant d'identifier les utilisateurs sur le réseau et de définir leurs droits d'accès. Néanmoins, il est possible pour les petits réseaux de mettre en œuvre une version restreinte du WPA, appelée WPA-PSK, en déployant une même clé de chiffrement dans l'ensemble des équipements, ce qui évite la mise en place d'un serveur RADIUS.[3]

1.3.2 l'algorithme de fonctinnement

TKIP (Temporal Key Integrity Protocol) est un protocole de communication utilisé pour la protection et l'authentification des données transitant sur un réseau Wi-Fi. Destiné à remplacer

le WEP, protocole ayant de nombreuses faiblesses, TKIP est spécifié dans la norme IEEE 802.11i et permet de conserver le matériel supportant WEP. Ce protocole était nécessaire parce que le cassage du WEP a rendu les réseaux Wi-Fi sans solution de sécurité crédible. La sécurisation des réseaux déjà déployés étant vitale et le remplacement de tout le matériel existant peu réaliste. TKIP emploie des solutions techniques proches de WEP (utilisation de l'algorithme de chiffrement RC4) mais sans les erreurs de conception de WEP. Par exemple, contrairement à WEP qui chiffre chaque paquet avec une clé de base constante de 128 bits concaténée avec un vecteur d'initialisation différent, WPA chiffre chaque paquet avec une clé de base qui est périodiquement modifiée et concaténée avec un vecteur d'initialisation. Le vecteur d'initialisation est haché contrairement à WEP qui l'envoie en clair.[4]

1.3.3 Les attaques de l'algorithme

1.3.3.1 Attaque Beck et Tews visant TKIP

En novembre 2008, deux chercheurs allemands en sécurité, Erik Tews et Martin Beck3, ont annoncé avoir découvert une faille de sécurité dans le mécanisme de sécurité WPA utilisé avec l'algorithme TKIP (Temporal Key Integrity Protocol) Martin Beck a intégré l'outil pour exploiter cette faille dans son outil d'audit de sécurité des liaisons sans fil, nommé Aircrack-ng.

1.3.3.2 Amélioration de l'attaque Beck et Tews visant TKIP

En juillet 2010, un chercheur, Md Sohail Ahmad, technology manager chez AirTight, a annoncé la découverte d'une faille (nommée "Hole 1966") dans le protocole WPA2, jusqu'alors considéré comme le plus sécurisé des mécanismes de sécurité WiFi existants. Il s'agit d'une méthode permettant à un utilisateur authentifié sur un point d'accès (ayant donc préalablement la connaissance de la clé partagée et s'étant associé sur le point d'accès) d'injecter du trafic à destination des autres machines également associées au même point d'accès, tout en évitant de se faire détecter par le point d'accès. Un pirate disposant de la clé partagée pourrait donc procéder à une attaque de l'homme du milieu, ce qui lui permettrait d'accéder au trafic d'un autre utilisateur connecté, voire de modifier au vol ces informations.[5]

1.3.4 la vulnérabilité de Octobre 2017

En octobre 2017, une vulnérabilité baptisée KRACK (Key Reinstallation Attacks) qui permet une attaque du type attaque de l'homme du milieu (en anglais man in the middle) a été révélée. Cette vulnérabilité concerne la plupart des réseaux wifi publics et privés

1.4 le protocole WPA2

1.4.1 Définition

WPA2, le successeur de WPA, comprend tous les éléments obligatoires de la norme 802.11i . La norme de sécurité sans fil 802.11i basée sur le protocole a été introduit en 2004. L'amélioration plus importante de WPA2 sur WPA était l'usage d'Advanced Encryptions Standard (AES).

1.4.2 algorithme AES

Advanced Encryptions Standard ou AES (soit « norme de chiffrement avancé » en français), aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique.

L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite

placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(28) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un OU exclusif XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.

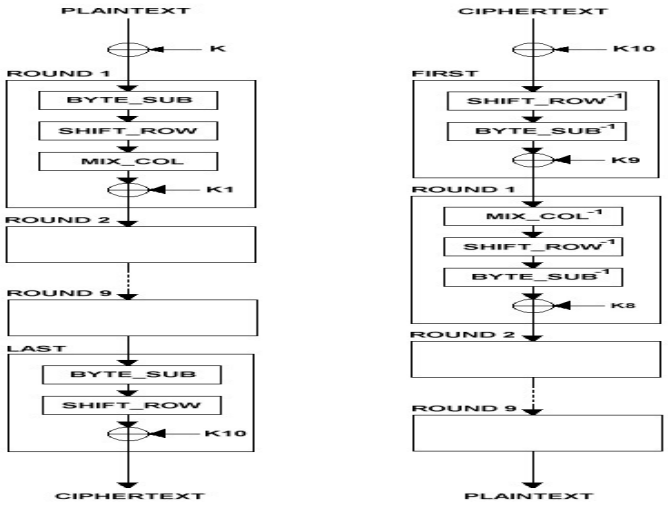

FIGURE 1.5 – Algorithme AES

1.4.3 Les attaques d'algorithme AES

Rijndael a été conçu de façon à résister aux méthodes classiques en particulier la cryptanalyse linéaire et la cryptanalyse différentielle. Le nombre de tours de l'AES est calculé en fonction de la taille de la clef pour que chacune de ces deux attaques (linéaire et différentielle) ne soit pas plus efficace qu'une attaque par force brute. L'AES n'a pour l'instant pas été cassé, même théoriquement, au sens où il n'existe pas d'attaque significativement plus efficace que la recherche exhaustive quand le chiffrement est correctement utilisé.

1.4.3.1 Attaques sur des versions simplifiées

Des attaques existent sur des versions simplifiées d'AES. Niels Ferguson et son équipe ont proposé en 2000 une attaque sur une version à 7 tours de l'AES 128 bits. Une attaque similaire casse un AES de 192 ou 256 bits contenant 8 tours. Un AES de 256 bits peut être cassé s'il est réduit à 9 tours avec une contrainte supplémentaire. En effet, cette dernière attaque repose sur le principe des « related-keys » (clés apparentées). Dans une telle attaque, la clé demeure secrète mais l'attaquant peut spécifier des transformations sur la clé et chiffrer des textes à sa guise. Il peut donc légèrement modifier la clé et regarder comment la sortie de l'AES se comporte.

1.4.3.2 Attaques sur la version complète

La simplicité algébrique de l'AES a été mise en avant, par exemple en 2001 par Niels Ferguson, comme une potentielle faiblesse3. Elle n'a cependant pu être exploitée jusqu'à présent. En 2002 Nicolas

Courtois et Josef Pieprzyk avaient présenté une attaque algébrique théorique l'attaque XSL, dont ils estimaient qu'elle était plus efficace que l'attaque par force brute, mais, cela n'a pas été confirmé par les travaux ultérieurs4. En 2011, des chercheurs de Microsoft publient une attaque sur la version complète d'AES.

1.4.3.3 Attaques par canal auxiliaire

Les attaques par canal auxiliaire exploitent les faiblesses du système implémentant l'algorithme de chiffrement et ne le visent donc pas directement. Il existe plusieurs attaques connues de ce type pour l'AES. En avril 2005, Daniel J. Bernstein a publié une attaque temporelle utilisée pour casser une clé AES sur un serveur spécifique tournant avec OpenSSL. En novembre 2010, Endre Bangerter, David Gullasch et Stephan Krenn ont publié un article décrivant la récupération d'une clé secrète AES-128 quasiment en temps réel qui fonctionne pour tout type d'implémentation. Comme les précédentes attaques de ce type, elle nécessite de lancer un programme sur la machine qui effectue le chiffrement.

1.4.4 Exemple de vulnérabilité de WPA2

Des chercheurs belges ont démontré une attaque contre le protocole de chiffrement WPA2 utilisé par tous les appareils se connectant à un réseau wifi. L'attaque permet de lire les informations sensibles envoyées par l'utilisateur. Des chercheurs belges sont parvenus à exploiter une vulnérabilité dans le protocole de chiffrement WPA2 employé par tous les appareils et réseaux wifi actuels. La technique d'attaque qu'ils ont développée permet à un pirate se trouvant à proximité du réseau wifi de lire les informations envoyées par un appareil (smartphone, laptop) et censées être chiffrées, comme les e-mails, les mots de passe ou les numéros de carte de crédit. Dans certains cas, un hacker pourrait également accéder aux informations envoyés vers la victime. Les chercheurs, qui présenteront leur recherche lors de la conférence Black Hat Europe, ont démontré leur technique sur un smartphone Android, mais elle fonctionne aussi contre les appareils Apple, Windows, Linux et d'autres.
L'attaque ne repose pas sur une mauvaise implémentation de WPA2, mais sur le standard lui-même - précisément la procédure 4-way handshake - de sorte que tous les terminaux sont susceptibles d'être attaqués. La technique KRACKs (key reinstallation attacks) amène la victime à réinstaller une clé déjà employée, en manipulant et en rejouant les messages cryptographiques du handshake.

1.5 le protocole WPA3

1.5.1 Définition

Wi-Fi CERTIFIED WPA3 offre les fonctionnalités nécessaires pour répondre aux besoins de différents déploiements de réseaux, allant d'environnements d'entreprise hautement contrôlés à des réseaux domestiques plus flexibles, et pour fonctionner sous différents formats. Quel que soit l'environnement ou le type de périphérique, tous les périphériques WPA3 ^{TM} offrent deux avantages clés :

- Cryptographic consistency WPA3 réduit la susceptibilité des réseaux à une attaque réussie en imposant des règles relatives à l'utilisation de la norme AES (Advanced Encryption Standard) avec des protocoles existants, tels que le protocole TKIP (Temporal Key Integrity Protocol).
- Network Resiliency Les cadres de gestion protégés (PMF) offrent un niveau de protection contre les écoutes clandestines et la falsification pour des cadres de gestion robustes. L'utilisation constante de ces protections améliore la résilience des réseaux critiques.

Wi-Fi Alliance a tout d'abord introduit le cadre de protection protégée (PMF) en tant que fonction optionnelle de WPA2 en 2012, puis a rendu obligatoire la fonctionnalité de tous les périphériques Wi - Fi CERTIFIED ^{TM} ac. Avec la sortie de WPA3, Wi - Fi Alliance rend désormais obligatoire l'utilisation de trames de gestion protégées dans tous les modes WPA3, offrant ainsi une protection aux trames

de gestion robustes monodiffusion et multidiffusion afin d'inclure les trames Action, Dissociation et Désauthentification

1.5.2 WPA3-Personal fournit une authentification robuste basée sur un mot de passe

WPA3-Personal remplace la clé pré-partagée (PSK) par l'authentification simultanée simultanée (SAE), offrant ainsi une authentification basée sur un mot de passe plus robuste. WPA3-Personal utilise des mots de passe pour l'authentification en prouvant la connaissance du mot de passe et non pour la dérivation de clé, offrant ainsi aux utilisateurs une protection renforcée comme : Résistance aux attaques par dictionnaire hors ligne : il n'est pas possible pour un adversaire d'observer passivement un échange WPA3-Personnel ou de participer activement à un seul échange WPA3-Personnel, puis d'essayer tous les mots de passe possibles sans autre interaction avec le réseau pour déterminer le mot de passe correct. La seule méthode permettant de déterminer le mot de passe du réseau consiste à utiliser des attaques actives répétées au cours desquelles l'adversaire ne peut deviner le mot de passe par attaque.
Résistance à la récupération de clé : Même si un adversaire détermine le mot de passe, il n'est pas possible d'observer passivement un échange ni de déterminer les clés de session, ce qui assure la confidentialité du trafic réseau. Utilisation naturelle des mots de passe : les exigences complexes liées à la sélection d'un mot de passe rendent son utilisation difficile et entravent la fourniture des protections de sécurité souhaitées. WPA3-Personal étant résistant aux attaques hors ligne par dictionnaire, les utilisateurs peuvent choisir des mots de passe plus faciles à retenir et à saisir, tout en conservant un haut niveau de sécurité.
Continuité de flux de travail simple : WPA3-Personal conserve la facilité d'utilisation et la maintenance du système associées aux versions précédentes de la sécurité Wi-Fi personnelle.

1.5.3 conclusion

La prochaine génération de connectivité Wi-Fi nécessite des outils et des pratiques robustes pour préserver la confidentialité et la sécurité des données utilisateur. La Wi-Fi Alliance a continué à faire évoluer constamment la famille de technologies Wi-Fi Protected Access afin de fournir la sécurité la plus récente à mesure que le paysage change. Grâce à l'utilisation de mécanismes normalisés, à l'application cohérente de protocoles et à des outils d'interface de sécurité faciles à utiliser, les propriétaires de réseau peuvent mieux protéger les données des utilisateurs et promouvoir l'adoption des meilleures pratiques de sécurité. Cela dit, chaque environnement réseau est différent. Wi-Fi Alliance reconnaît le besoin de solutions robustes répondant aux exigences de sécurité de divers types d'appareils et de réseaux.
Grâce à WPA3 et à d'autres programmes tels que Wi-Fi Easy Connect ^{TM}, Wi Fi Alliance apporte de nouvelles fonctionnalités qui prennent en charge la manière dont le monde fonctionne et vit aujourd'hui. Assurer une intégration plus simple et sécurisée de chaque type d'appareil et permettre la protection des données utilisateur pour les environnements réseau Wi-Fi personnels et sensibles aux données augmentent l'expérience utilisateur Wi Fi, ainsi que la dépendance au Wi-Fi. WPA3 s'appuie sur le succès éprouvé de WPA2 pour apporter un nouveau niveau de sécurité aux environnements personnels et d'entreprise avec des protocoles de sécurité robustes. L'accent mis sur la cohérence cryptographique, une authentification basée sur un mot de passe robuste et une sécurité 192 bits ouvre le marché à une nouvelle ère de connectivité en toute confiance.[8]

1.5.4 RADIUS

1.5.4.1 Principe du Protocole Radius

RADIUS ou Remote Authentication Dial-In User est un Protocole standard d'authentification qui est décrit comme suit :

- Défini au sein des RFC 2865 et 2866.
- Fonctionnement basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau.
- Protocole de prédilection des fournisseurs d'accès à internet : relativement standard, propose des fonctionnalités de comptabilité permettant de facturer précisément les clients.
- Le protocole RADIUS permet de faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée
- RADIUS repose principalement :
  - sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.).
  - sur un client RADIUS, appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur.
- L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffré.
- Le serveur RADIUS peut faire office de proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS.
- Le serveur traite les demandes d'authentification en accédant si nécessaire à une base externe : base de données SQL, annuaire LDAP, comptes d'utilisateurs, de machines ou de domaines. un serveur RADIUS dispose pour cela d'un certain nombre d'interfaces ou de méthodes.[6]

1.5.4.2 Scénario de fonctionnement

- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance.
- Le NAS achemine la demande au serveur RADIUS.
- Le serveur RADIUS consulte sa base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur.
- Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur.
- Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :
  - ACCEPT : l'identification a réussi.
  - REJECT : l'identification a échoué.
  - CHALLENGE : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi ».
- Une autre réponse est possible : CHANGE PASSWORD où le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.
- Suite à cette phase dite d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

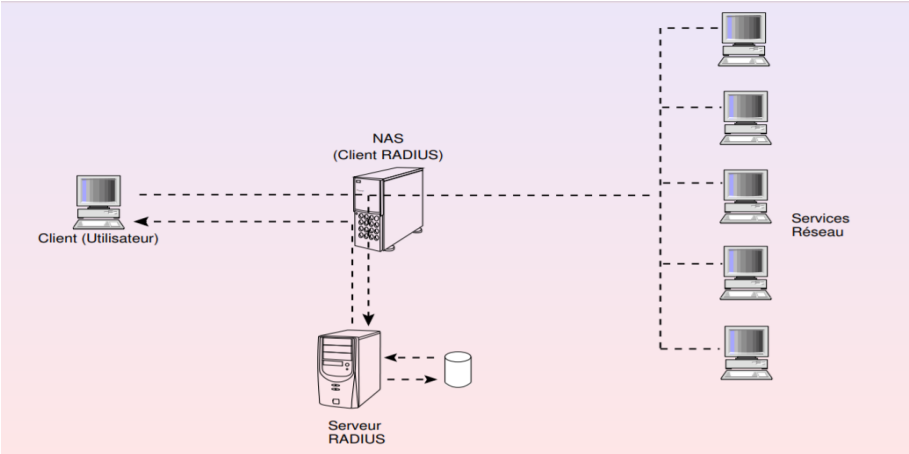

FIGURE 1.6 – Schéma de fonctionnement du protocole Radius [1]

Il ne faut point perdre de vue une lacune frappante dont souffre Radius. En effet, Radius n'assure pas de mécanismes d'identification du serveur : se faire passer pour un serveur est un excellent moyen de récolter des noms et mots de passe.

Chapitre 2

configuration et crackage de clé

2.1 configuration routeur

la configuration du routeur consiste à attribuer une adresse IP à notre routeur,qui se fait selon trois étapes :

1-Installer le logiciel Putty : qui permet de faire la configuration en mode console

2-ouvrir le terminal Putty et Entrer le nom d'utilisateur et le mot de passe par défaut est Cisco

3-Apres on attribuer une adresse IP = 10.0.0.1 avec le maque 225.0.0.0

2.1.1 Connexion réseaux sans fil

La première étape qu'on doit faire est de changer les propriétés de la connexion réseaux sans fil, et donc on a décoché la case « obtain an IP address automatically » et on a coché la deuxième case pour pouvoir remplir les champs manuellement.

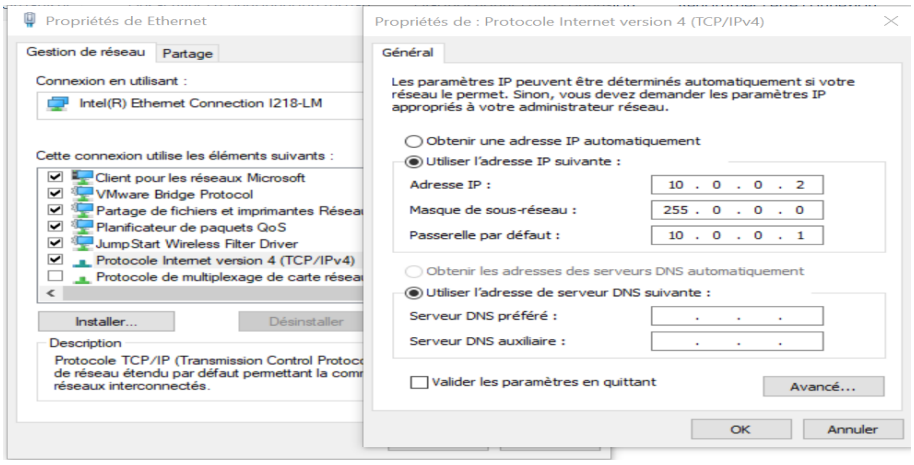

FIGURE 2.1 – configuration adresse ip

Apres, on accède à la plateforme Cisco en entrant le nom d'utilisateur et le mot de passe par défaut est Cisco/Cisco.

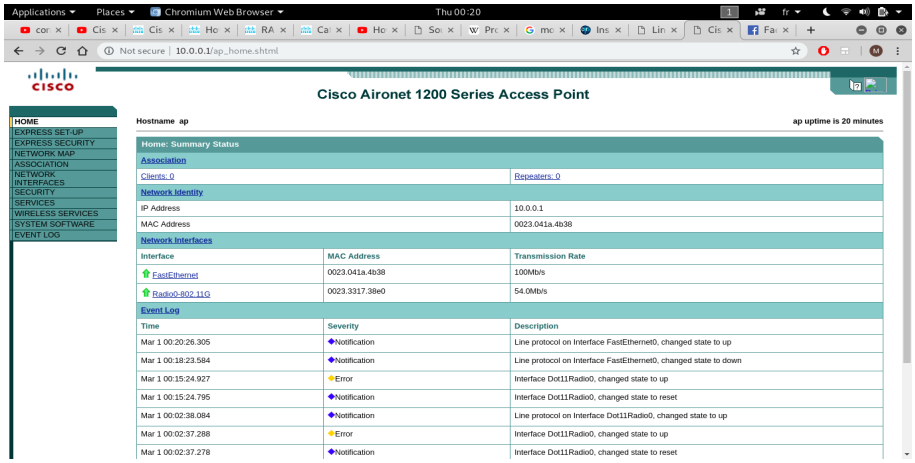

FIGURE 2.2 – configuration adresse ip

2.2 configuration WEP et crackage de clé

2.2.1 Configuration WEP

Pour configurer le WEP dans un routeur Cisco Aironet 1200 series.
Tout d'abord, dans EXPRESS SECURITY, il faut entrer le SSID et activer Broadcast SSID in Beacon.

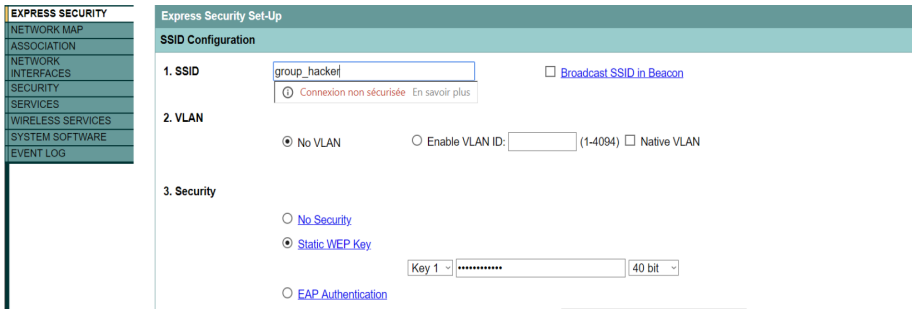

FIGURE 2.3 – configuration avec la clé WEP

2.2.2 Crackage de clé

on serai capable de cracker la clé à l'aide des commandes suivantes :

— Airmon-ng : permet d'activer le mode moniteur permet à un ordinateur équipé d'une carte réseau Wi-Fi d'écouter tout le trafic d'un réseau sans fil

— Airodump-ng :permet de capturer les paquets qui cercule dans le réseau,connaitre le bssid et le essid Airodump-ng interface

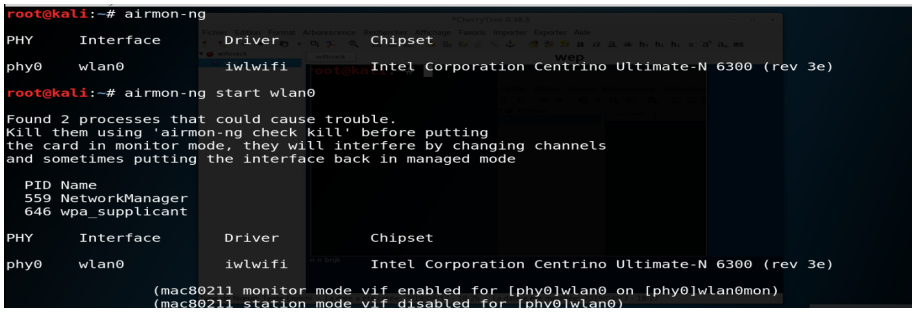

FIGURE 2.4 – Résultat commande airodump-ng

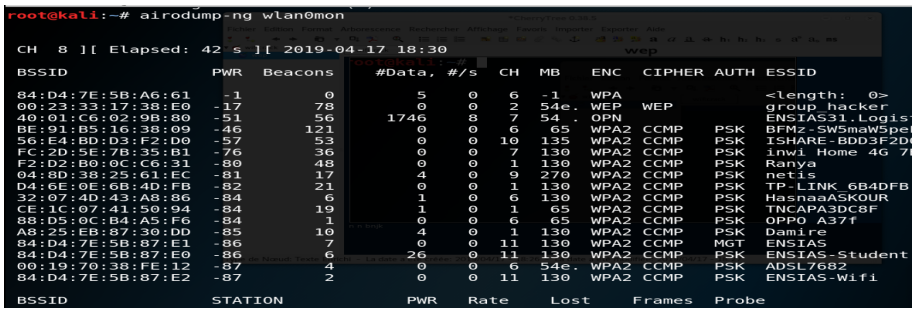

FIGURE 2.5 – découvrir les hotes dans le réseau

— airodump-ng : qui permet de capturer les paquets qui circulent dans le réseau et les faire enregistrer dans un fichier qui sera prochainement exploiter pour l'extraction de clé

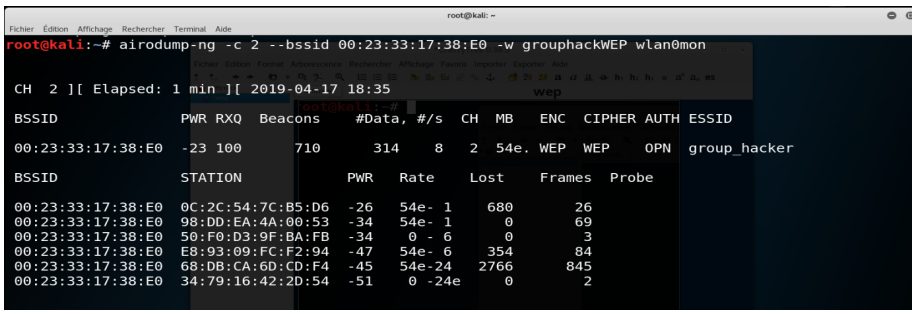

FIGURE 2.6 – capturer les packets

— aircrack-ng : qui permet d'extraire la clé à partir du fichier pcap donné en entré

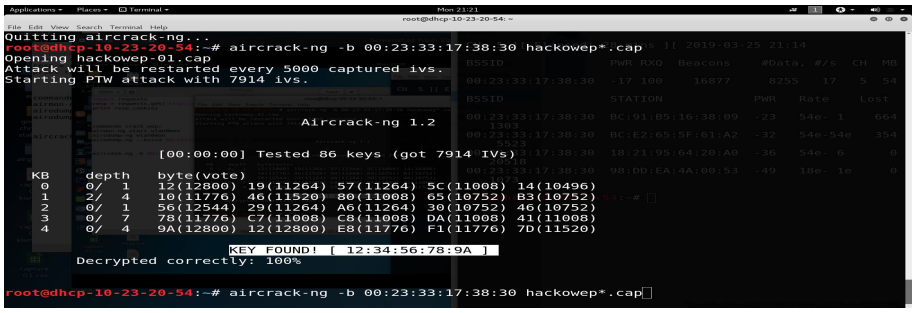

FIGURE 2.7 – la clé WEP

2.3 configuration WPA et crackage de clé

2.3.1 Configuration WPA

Pour configurer le WPA dans un routeur Cisco Aironet 1200 series.
Tout d'abord, dans EXPRESS SECURITY, il faut entrer le SSID et activer Broadcast SSID in Beacon puis saisir la clé.

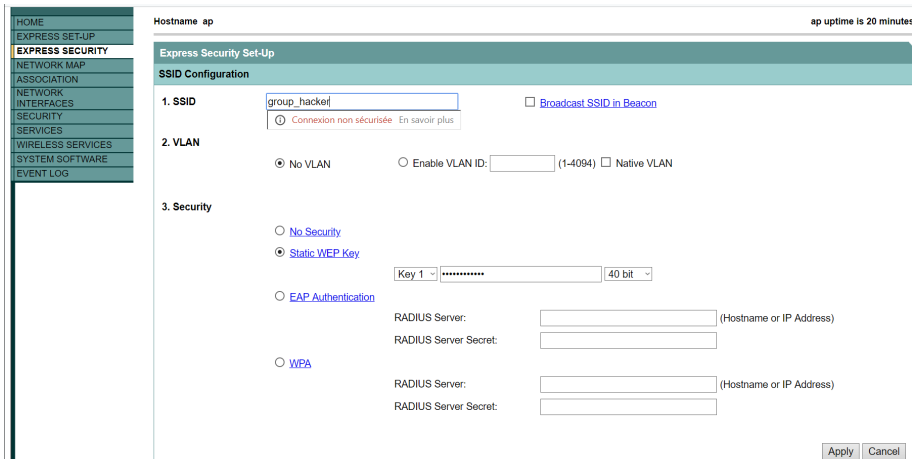

FIGURE 2.8 – configuration WPA

Ensuite, dans Security -> Encryption Manager, choisir Cipher : TKIP

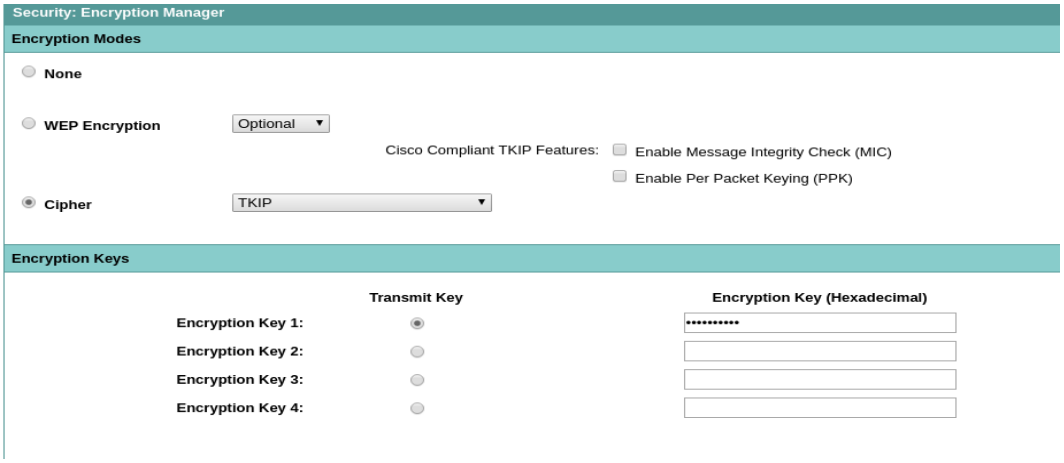

FIGURE 2.9 – WEP interface

Dans Security -> SSID Manager, choisir Open Authentification, key Managment : Mandatory, cocher WPA et entrer la clé WPA

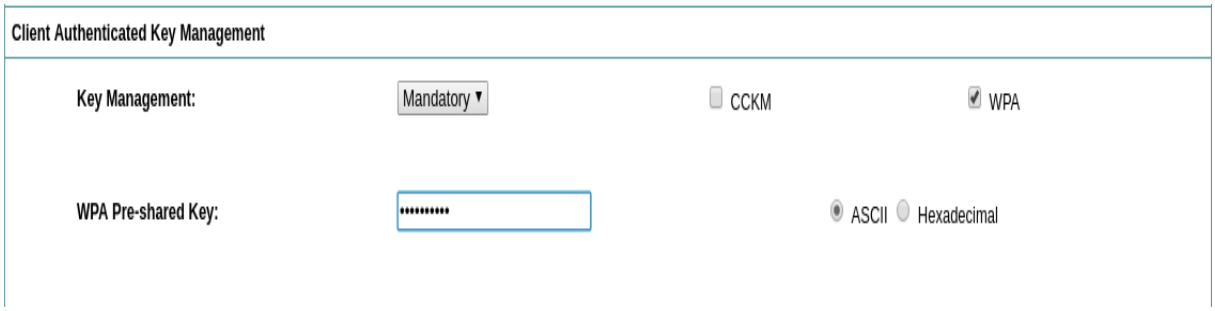

FIGURE 2.10 – key management

2.3.2 Craquage de mot de passe par Fern WIFI Cracker

à l'aide de l'outil Frn wifi cracker qui donne la possibilité de trouver la clé à partir un wordlist (rockyou.txt)

FIGURE 2.11 – interface Fern WIFI Cracker

Aprés quelque minutes,on est réussi à cracker la clé

FIGURE 2.12 – cle cracked

2.4 Configuration RADIUS

la configuration de serveur RADIUS se fait selon les étapes suivantes :

— La commande «gedit /etc/freeradius/3.0/clients.conf » nous permet d'ajouter des clients RADIUSidentifiés par leur nom d'hôte et d'inclure le shared secret.

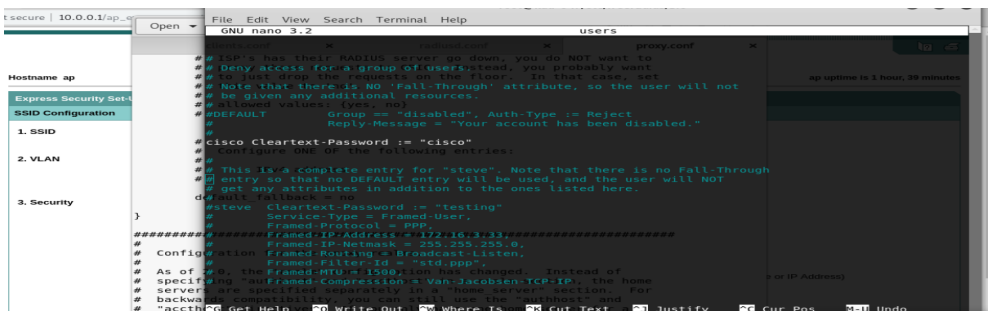

FIGURE 2.13 – serveur radius

— Tout d'abord on a installé « FreeRADIUS » en utilisant la commande «apt-get installfreeradius » . On a tapé la commande «vi /etc/freeradius/3.0/users » puis on a ajouté un utilisateurqu'on a nommé cisco dont son mot de passe est cisco.

FIGURE 2.14 – installer freeradius

— La figure ci-dessous montre l'affectation de l'adresse ip au serveur radius ainsi que laclé partagé qu'on a déjà fourni dans le fichier clients.conf.

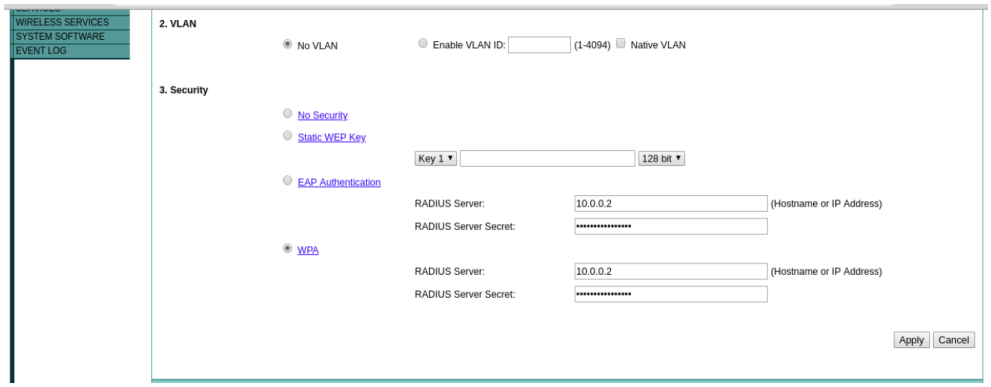

FIGURE 2.15 – adressage de serveur

On doit redémarrer le serveur pour appliquer les modifications qu'on a réalisé. On a essayé de s'authentifié au réseau « tp-security » et voici le résultat :

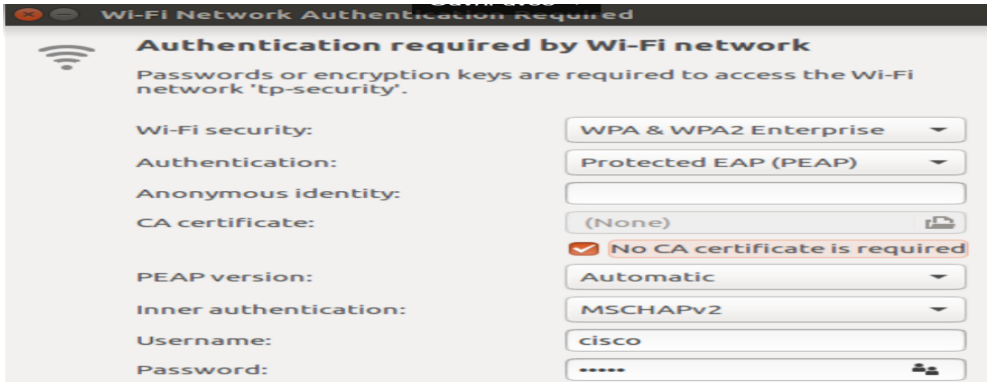

FIGURE 2.16 – authentification réseau

On peut constater donc que le protocole radius met en valeur la sécurité des réseaux sans fil.

Conclusion Générale

Il va sans dire alors que la plupart des réseaux Wi-Fi sont déployés en mode infrastructure. Le mode infrastructure se base sur l'utilisation d'un point d'accès W-Fi central, situé au niveau d'un point de concentration radio. Dans ce cas, les informations envoyées entre les différentes stations transitent par le point d'accès.
La mise en place d'un réseau Wi-Fi n'est pas quelque chose que l'on décide du jour au lendemain. Une étude du réseau et des besoins des utilisateurs doit être réalisée au préalable.
La sécurité, quant à elle, n'est pas à négliger. En effet, il ne suffi pas de brancher un point d'accès sur le réseau pour disposer d'une passerelle Wi-Fi. Les protocoles WEP et WPA renforcent certes le volet sécuritaire du réseau, mais le risque de révélation des clés de cryptage ne doit en aucun cas être perdu de vue. Par ailleurs, il est vivement conseillé de coupler les mesures susmentionnées à un serveur d'authentification Radius. Les utilisateurs passés au crible devant radius et partant non enregistrés seront interdits d'accès pour défaut d'authentification.

Bibliographie

[1] http://litis.univ-lehavre.fr/~duvallet/enseignements/Cours/CNAM/CNAM-Cours-ServeurRadius.pdf.

[2] http%3A%2F%2Frepository.root-me.org%2FR%25C3%25A9seau%2FFR%2520-%2520Wifi%2520protocole%2520WEP%253A%2520m%25C3%25A9canismes%2520et%2520failles.pdf%3Ffbclid%3DIwAR3_RxWHWPWabVbvYIj8W7fC3mwv87f9nqc_oXeggXyzO7IHVD1Kp5SS9ds&h=AT1NVOSumrXCeWrrY0qprSFvQISkNkCpRlxEk6fpOgrmstK93n9u89M_d7JmWVrAjFDLZUv1_uVNq1xrEQPdzjJO-raN99PtKx7-W38MvH8E27UwyDkptQXdLysKAbJNev2gyQ.

[3] https://docplayer.fr/12272276-I-plusieurs-types-de-vlan.html.

[4] =https%3A%2F%2Ffr.wikipedia.org%2Fwiki%2FWi-Fi_Protected_Access%3Ffbclid%3DIwAR2Lv12_dmoPITM-SQmn5Cu95YGzF1lEuVZQ1zaZWgs4DR7amNp0spUl_EU&h=AT1NVOSumrXCeWrrY0qprSFvQISkNkCpRlxEk6fpOgrmstK93n9u89M_d7JmWVrAjFDLZUv1_uVNq1xrEQPdzjJO-raN99PtKx7-W38MvH8E27UwyDkptQXdLysKAbJNev2gyQ.

[5] <https://wigle.net/stats?fbclid=IwAR0aNRHjExX3Wiate351PCnlgBZPmITYCMXwlCsRLEqO433vl2PTAoxrWZC http://dept-info.labri.u-bordeaux.fr/~guermouc/SR/SR/cours//cours6.pdf?fbclid=IwAR2rsl7wastZDwZaqCd5mR-5lmpXQ1TP_jW8p1bZgKzgab41HIr_giOSRMk.

[6] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/xe-16/sec-usr-rad-xe-16-book/sec-cfg-radius.html?fbclid=IwAR2PiYDsysEtHqZOByO7zN3DdkBmk7p8u2u3Yz85-jKihOATHsivAGf_p4s.

[7] https://pdfs.semanticscholar.org/beb2/90fb1db86715c5ddb256245bff2ca1bb1dec.pdf?fbclid=IwAR2Lv12_dmoPITM-SQmn5Cu95YGzF1lEuVZQ1zaZWgs4DR7amNp0spUl_EU.

[8] <https://www.wi-fi.org/discover-wi-fi/security./>,.