UOC
Universitat Oberta de Catalunya
www.uoc.edu

Treball Final de Carrera

Riscos i amenaces existents en les xarxes sense fils. Solucions actuals.

Jaume Echevarría Borràs
Universitat Oberta de Catalunya
Treball Final de Carrera Curs 2012-2013

Index

Índex de figures

1. Introducció

1.1 Preàmbul

L'objectiu d'aquest treball final de carrera és donar una visió sobre els riscos i amenaces existents en les xarxes sense fils, detallar quines són les principals característiques de les solucions que ofereix el mercat actual i comparar-les.

Com a introducció, val a dir que les tecnologies sense fils en els darrers anys, han anat guanyant protagonisme en la vida diària de les empreses, les institucions i els entorns domèstics. L' *IEEE 802.11* agrupa un conjunt d'estàndards de comunicació sense fils que ofereixen solucions per a compartir informació sense necessitat d'utilitzar medis cablejats. Així, assolim la possibilitat d'establir canals de dades entre entorns mòbils i estàtics, eliminant barreres arquitectòniques i facilitant l'accés a la comunicació de "qualsevol" dispositiu.

IEEE 802.11 suposa un dels estàndards de comunicació per radiofreqüència més utilitzats i popular per a les xarxes d' àrea local (*LAN*). No és estrany, doncs, que dispositius com portàtils, *PDA's*, tauletes, mòbils o inclús maquinària industrial facin ús d'aquest tipus d'estàndard com a solució sense fils per a interconnectar i transferir qualsevol tipus de dades, veu o senyals de vídeo. Per exemple, només cal realitzar una recerca manual des d' un dispositiu amb connexió *Wi-Fi* per adonar-se de la quantitat de xarxes sense fils que hi ha al seu voltant, i ser conscients de la gran acollida que té aquesta tecnologia entre la societat actual.

Gairebé el 52% dels internautes accedeixen a la xarxa a través de la tecnologia sense fils que defineix *IEEE 802.11*. Tot apunta a que el creixement i desplegament d' aquest tipus de xarxes seguirà creixent els propers anys. Però no només els usuaris domèstics adquireixen productes amb aquesta tecnologia, també ho fan les petites, mitjanes i grans empreses, institucions i organismes públics, que cada vegada fan més ús de l'estàndard com a solució de comunicació no cablejada. És per tot això, que la seguretat es fa encara més fonamental quan fem servir aquesta tecnologia connectant-nos la xarxa via *802.11*, doncs, un mal ús pot suposar una finestra oberta a l'exterior per on qualsevol persona malintencionada pot robar informació, podent inclús obtenir el

control dels nostres actius. Aquest treball final de carrera pretén identificar les diferents tecnologies sense fils que hi ha a l' actualitat, analitzar els diferents protocols i metodologies de protecció del canal sense fils, realitzar un estudi de les vulnerabilitats i mètodes d'atac existents i comparar les solucions que ofereix actualment el mercat de les tecnologies.

1.2 Inici

En aquest TFC es realitza una recopilació sobre diferents aspectes de l' arquitectura per a xarxes sense fils, en concret, la basada en tecnologia *Wireless* (sense fil). Ens centrarem tant en el camp de la seguretat dins aquest tipus de xarxes, com en l'anàlisi dels riscos i amenaces existents. A més a més, descriurem les diferents eines que hi ha per atacar aquest tipus de xarxes i les solucions per a lluitar contra elles.

1.3 Objecte i abast del projecte

L' objectiu d'aquest treball és consolidar els coneixements adquirits en el desenvolupament dels estudis universitaris d' *Enginyeria Tècnica de Telecomunicacions, especialitat Telemàtica de la Universitat Oberta de Catalunya*. Realitzarem un estudi sobre els riscos i amenaces existents en les xarxes sense fils i detallarem les característiques d' algunes de les solucions que ofereix el mercat actual per a pal·liar-les degudament.

1.4 Objectius concrets

Els objectius concrets marcats dins aquesta proposta inicial de TFC son els següents:

- Introducció sobre les diferents infraestructures de xarxes sense fils més comuns.
- Identificar i analitzar els riscos i amenaces de les xarxes sense fils.
- Analitzar les propostes de seguretat per a sistemes de comunicacions sense fils existents.
- Descripció de les polítiques de seguretat, *best practices* i directrius de seguretat per ajudar a millorar la seguretat dels sistemes tractats.
- Identificar i comparar les solucions de seguretat existents al mercat.

1.5 Planificació del treball

Per assolir els objectius proposats, és necessari desglossar i planificar les tasques que durem a terme durant tot el procés de desenvolupament del treball, identificant les tasques i fites mitjançant eines de planificació de projectes (concretament, *Microsoft Project 2007*). Els documents a entregar en aquest projecte son els següents:

Prova d'Avaluació Continuada 1 (PAC1)
Proves d' Avaluació Continuada 2 i 3 (PAC2 i PAC3)

Memòria
És el resultat dels treballs elaborats durant les proves d'avaluació continuada prèvies i està fixada per al proper 10 de gener de 2013. Estarà formada per:

- Contingut del *TFC*.
- Assoliment dels objectius proposats.
- Aspectes formals.
- Bibliografia utilitzada.
- Contribucions personals.

Presentació
Ha de resumir clarament el treball realitzat fins aleshores i el resultat final de la memòria. La data d'entrega d' aquesta presentació virtual serà el proper 17 de gener de 2013. Basant-nos en la metodologia de planificació de projectes que dictamina el *Project Management Institute (PMI)*, el pla de treball amb la descripció de les tasques i l' esforç necessaris per assolir aquests objectius son els que es mostren en les figures 1.1 i 1.2, i que sempre es fonamenten en el què el tutor i l' avaluació continuada exigeixen a l' estudiant. El termini final d' entrega del TFC es el proper 17/01/2013. Les entregues parcials comentades anteriorment es detallen i es descriuen també en les figures 1.1 i 1.2.

Task Name	Duration	Start	Finish	Predecessors
Treball Final de Carrera	**84 days**	**Mon 01/10/12**	**Thu 24/01/13**	
PAC1	**20 days**	**Mon 01/10/12**	**Fri 26/10/12**	
El·laboració PAC1	20 days	Mon 01/10/12	Fri 26/10/12	
Revisió Documentació a Entregar	20 days	Mon 01/10/12	Fri 26/10/12	3SS
Entrega PAC1 - Planificació	3 days	Mon 01/10/12	Wed 03/10/12	4SS
PAC2	**32 days**	**Thu 04/10/12**	**Mon 19/11/12**	
Búsqueda d' linformació a Internet	20 days	Thu 04/10/12	Thu 01/11/12	5FS+1 day
Organització de la Informació	20 days	Thu 04/10/12	Thu 01/11/12	7SS
El·laboració Esborrany de Memòria	5 days	Thu 01/11/12	Thu 08/11/12	8
Revisió Documentació a Entregar	5 days	Thu 08/11/12	Thu 15/11/12	9
Entrega PAC2	3 days	Thu 15/11/12	Mon 19/11/12	10FS-1 day
PAC3	**19 days**	**Tue 20/11/12**	**Mon 17/12/12**	
Búsqueda Solucions al Mercat	5 days	Tue 20/11/12	Tue 27/11/12	11FS+1 day
Comparació Detalls Solucions	5 days	Tue 27/11/12	Tue 04/12/12	13
El·laboració Esborrany de Memòria	7 days	Tue 04/12/12	Thu 13/12/12	14
Revisió Documentació a Entregar	3 days	Thu 13/12/12	Mon 17/12/12	15FS-1 day
Entrega PAC3	3 days	Wed 12/12/12	Fri 14/12/12	16SS-1 day
Entrega Final del TFC	**30 days**	**Fri 14/12/12**	**Thu 24/01/13**	
El·laboració Memòria Final	5 days	Fri 14/12/12	Fri 21/12/12	17
Revisió Documentació a Entregar	20 days	Fri 14/12/12	Thu 10/01/13	19SS-1 day
Entrega Memòria Definitiva	1 day	Thu 10/01/13	Thu 10/01/13	20FS-1 day
El·laboració Presentació	3 days	Thu 10/01/13	Tue 15/01/13	21
Revisió de la Documentació a Entregar - Presentació	2 days	Tue 15/01/13	Thu 17/01/13	22
Entrega Presentació	2 days	Tue 15/01/13	Thu 17/01/13	23SS
Questions & Answers	5 days	Thu 17/01/13	Thu 24/01/13	24
Final TFC	5 days	Fri 18/01/13	Thu 24/01/13	24

Figura 1.1. Planificació del TFC

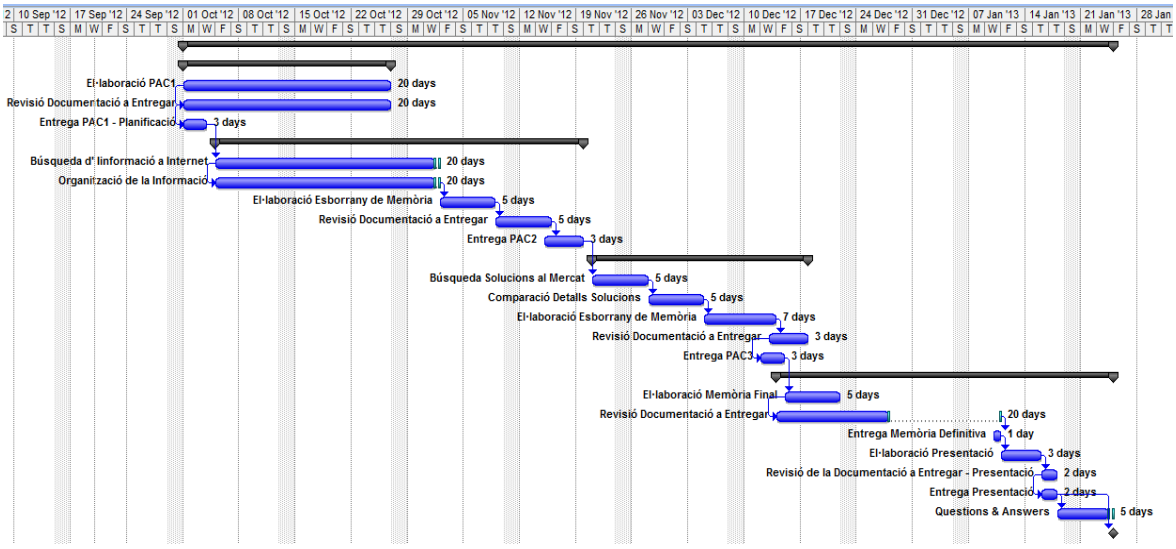

Figura 1.2. Diagrama de Gantt

2. Xarxes sense fil

2.1 Introducció a les xarxes sense fil

La gran proliferació de les xarxes sense fils en diferents àmbits és avui dia una realitat que ofereix un gran ventall de possibilitats. Darrerament han proliferat les noves tecnologies com *Wi-Fi, WiMax, Bluetooth, Infrarojos, GPRS, GSM, UMTS, 4G*...Un motiu principal és la rapidesa i facilitat d'implantació d'aquestes tecnologies que ha permès la realització d'experiències interessants durant els darrers anys. Tot sovint aquestes iniciatives permeten l'activació de la societat de la informació i la promoció de serveis d'administració electrònica municipal o simplement accés a Internet (entre d' altres). Cal tenir en compte que, per oferir serveis de telecomunicació, en tractar-se d'un mercat regulat per l'administració central, cal seguir la legislació en matèria de telecomunicacions, a més de respectar les regles de competència bàsica en tot sector. En aquest sentit, aquest document preveu l'anàlisi de la seguretat en aquestes xarxes i les solucions que ofereix el mercat actual per a superar-les. Les tecnologies sense fils han esdevingut molt econòmiques i possibiliten la realització de desplegaments d'accés amb poca inversió inicial. La figura 2.1 és un exemple genèric de xarxa sense fis, Wi-Fi.

Figura 2.1 Xarxes sense fils

No s'ha de perdre de vista que les xarxes de telecomunicacions són el mitjà de transmissió i que el seu valor principal rau en els serveis i aplicacions que aquestes xarxes suporten, així com en el valor afegit que ofereixen, ja que

permeten estendre tots aquests serveis de forma flexible a un munt de dispositius diferents. Aquestes tecnologies permeten oferir serveis dels que anomenem de "banda ampla", amb velocitats superiors a 1 *Mbps* i amb una qualitat de servei i disponibilitats notables sempre que el desplegament s'hagi realitzat de forma òptima. L' ús d'aquesta capacitat per terminal permet oferir un gran assortiment de serveis i aplicacions, de fet la gran majoria de serveis i aplicacions que s'ofereixen a l' Internet convencional es poden utilitzar de forma òptima sobre aquest tipus de xarxes concretes. Aquest desplegament cal que sigui planificat de forma acurada per poder donar una cobertura geogràfica adequada i una bona qualitat en la recepció del senyal. En aquest esquema, el punt d'accés sense fils dóna servei a tot un seguit de clients (ordinadors de sobretaula o portàtils i dispositius lleugers) que els permet comunicar-se a una xarxa fixa tot sovint connectada a Internet. Un factor decisiu en l'evolució de les xarxes sense fils ha sigut l' ús dels dispositius mòbils amb accés a Internet. Els *smartphones* han sigut els dispositius que han incrementat més la seva utilització i prestacions, sobretot des de l'aparició del *iPhone* d' Apple a mitjans de 2007, que va ser el tret de sortida a la revolució digital que encara estem vivint. Com dèiem, les tecnologies sense fils més importants alhora que crítiques son les corresponents a les xarxes mòbils: a principis dels anys 90 va aparèixer *GSM* (*Global System for Mobile Communications*) que proporcionava certa capacitat de transferència de dades amb prestacions però, molt reduïdes. *GSM* es considera, per la seva velocitat de transmissió i altres característiques, un estàndard de segona generació (*2G*). La primera tecnologia que va permetre connexions acceptables fou la tecnologia *GPRS* (*EDGE* a USA), entesa com a l' evolució de la seva predecessora i coneguda com a *2,5G*. Però, realment el canvi va arribar amb els mòbils de tercera generació (*3G*). En un primer moment ja que l' usuari no el reclamava, el *3G* va semblar que s' estancava i les operadores no van promoure' l comercialment. Així doncs, el mercat de les connexions 'no mòbils' sense fils creixia exponencialment mentre que el *3G*, que oferia velocitats de poc centenars de *Kbps*, es quedava enrere. Més endavant, els operadors mòbils van desenvolupar algunes modificacions en l'estàndard, donant entrada al *HSDPA/HSUPA*, que arribava a majors velocitats (fins a 7,2 Mbps) i presentava una asimetria entre els enllaços de pujada i baixada. Es va comercialitzar com a *3,5G*. És aleshores quan l' ús de les xarxes *3G* i *3,5G* es va disparar (2007-2008). Un conjunt de factors van contribuir a potenciar-lo: ofertes comercials més atractives, l' acceptació per part dels usuaris a aquest tipus d' aplicacions i l' aparició de terminals mòbils més atractius i complets: l' explosió dels smartphones de *RIM* (*Blackberry*) i l' arribada de l' *iPhone* d' *Apple*, principalment. Tot això va provocar un esclat en el desenvolupament de les

aplicacions de tercers per a aquests dispositius i el creixent interès dels usuaris en tenir-les disponibles als seus mòbils.
El mercat ha explotat: ara doncs, les operadores ja no només s'han de preocupar de la velocitat de connexió sinó també de la capacitat de la xarxa, per a cobrir les necessitats dels usuaris en descarregar-se informació via *3G* o fins i tot, via *4G*, la quarta generació, ja viva als Estats Units (*iPhone5*) i aquí, encara per estrenar.

2.2 Tipus de xarxes sense fils

La classificació de les tecnologies sense fils comentades a l' apartat anterior es pot fer considerant diferents paràmetres: el seu àmbit d'aplicació o abast, els seus avantatges i les seves limitacions. Cadascuna és útil en unes circumstàncies concretes, segons el què vulguem o necessitem fer. En aquest projecte, ens centrarem en les xarxes *Wi-Fi* o *WLAN* (*IEEE 802.11*) però donar una visió, per petita que sigui, de les diferents tecnologies comentades anteriorment, és necessari, entre d'altres motius, per a ubicar-les degudament.

En funció de la velocitat i el rang d'abast de les tecnologies sense fils, la classificació dels estàndards es correspon amb la figura 2.2:

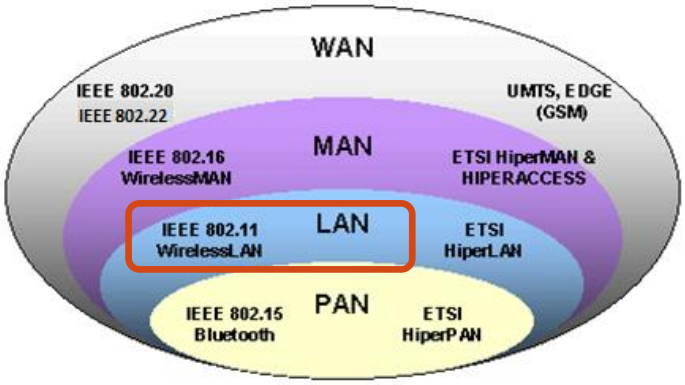

Figura 2.2 Classificació segons els estàndards de les tecnologies sense fils

D'altra banda, en funció de l'àrea geogràfica des de la que l' usuari es connecta a la xarxa i la definició de la figura 2.2, podem classificar-les com es veu a la figura 2.3:

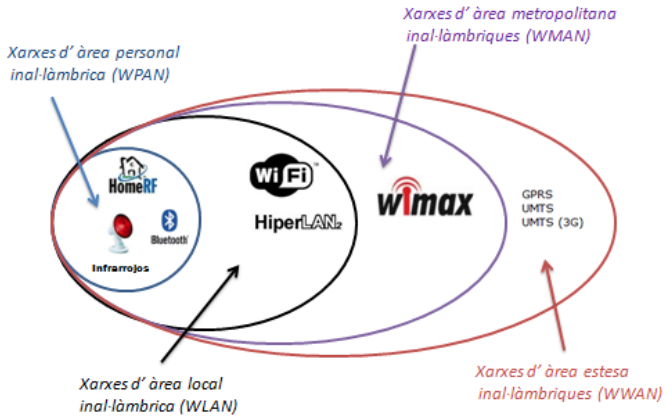

Figura 2.3 Classificació xarxes sense fils segons el seu abast

Per tant, en funció de la tecnologia emprada tindrem la següent classificació:

***XARXES D'ÀREA PERSONAL SENSE FILS*:** son les *WPAN*, *Wireless Personal Area Networks*. Les *WPAN* son xarxes caracteritzades per una cobertura limitada: son, principalment, els infrarojos, el *Bluetooth* i *ZigBee*.

Infrarojos son xarxes molt limitades degut al seu curt abast, la necessitat de visió total entre dispositius que es comuniquen i les baixes velocitats a les que arriba. Son exemples, el comandament a distància de la nostra televisió i l' intercanvi de dades entre ordinadors o dispositius de butxaca, per exemple.

Figura 2.4 Dispositius IR

Pel que fa a la seguretat, val a dir que en tractar-se d' un medi de transmissió òptic és immune a les radiacions electromagnètiques produïdes pels equips domèstics o pels demés medis de transmissió (cables coaxial, cables parells, xarxa elèctrica, etc.). En canvi, caldrà prendre precaucions en els següents casos: a) Les interferències electromagnètiques només afectaran els extrems del medi *IR*, és a dir, a partir dels dispositius optoelectrònics (emissor i foto receptor) i b). És necessari tenir en compte altres fonts d' IR. Avui dia, sense anar més lluny, existeixen dispositius d' il·luminació que emeten certa radiació IR.

Bluetooth és una especificació industrial per a les *WPAN* que possibilita la transmissió de veu i dades entre diferents dispositius mitjançant un enllaç per radiofreqüència a la franja dels 2,4GHz i fins a distàncies de 100 metres, segons el dispositiu. Els principals objectius que es pretén aconseguir amb el Bluetooth son: facilitar les comunicacions entre equips mòbils i fixes, eliminar cables i connectors i, oferir la possibilitat de crear petites xarxes inal·làmbriques facilitant la sincronització de dades entre equips personals (agendes, correus electrònics...). Els dispositius que més utilitzen aquesta tecnologia son dels sectors de les telecomunicacions i la informàtica personal: *PDA's*, telèfons mòbils, ordinadors portàtils, ordinadors personals, impressores i càmeres digitals. El perfil d' accés genèric *Bluetooth*, que és un marc en el qual es centren tots els perfils, defineix tres nivells de seguretat: 1.) mode 1 de seguretat no segur; 2.) mode de seguretat imposada a nivell de servei: el dispositiu Bluetooth inicia el procediment de seguretat abans que el canal s' hagi establert (capes baixes de la pila de protocols); 3.) Mode de seguretat 3, seguretat imposada a nivell d'enllaç: el dispositiu de seguretat inicia el procediment de seguretat abans que el canal s'hagi establert (capes baixes de la pila de protocols). L'accés a les dades entre dispositius *Bluetooth* pot ser mitjançant l'establiment de dispositius de confiança o no (accés limitat). Els serveis també es poden categoritzar en nivells de seguretat: oberts, que requereixen autenticació i que requereixen autenticació i autorització. El sistema, per tant, pot proveir seguretat tant a nivell d'aplicació com a nivell d' enllaç.

Figura 2.5 Dispositius Bluetooth

ZigBee és el nom de l' especificació d' un conjunt de protocols d' alt nivell de comunicació sense fils per a utilitzar en el món de la radiodifusió digital de baix consum (*IEEE 802.15.4*). El seu objectiu son les aplicacions que requereixen comunicacions segures amb baixa taxa d' enviament de dades i maximització de la vida útil de les seves bateries. *ZigBee* té més presència en l' àmbit de la domòtica on el baix consum, la topologia en xarxa de malles i la fàcil integració son característiques determinants en aquest sector. Un dels aspectes més característic de *ZigBee* son els serveis que ofereix per al suport de comunicaci-

ons segures. Es protegeixen l'establiment i el transport de claus, el xifrat de trames i el control dels dispositius. La seguretat depèn de la correcta gestió de les claus simètriques i l'adequada implementació dels mètodes i polítiques de seguretat. La pedra angular de la confidencialitat en *ZigBee* és la protecció de tot el material xifrat. Les claus son la base de l'arquitectura de seguretat i la seva protecció és fonamental per a la integritat del sistema. Totes les dades de les trames del nivell de xarxa han d'estar xifrades, ja que podria haver-hi dispositius maliciosos, de forma que el tràfic no autoritzat es preveu d' arrel. L' excepció és la transmissió de la clau de xarxa a un dispositiu nou, el que proporciona a tota la xarxa un nivell de seguretat únic. També es pot emprar criptografia en enllaços punt a punt.

Figura 2.6 Logotip ZigBee

XARXES DE CONSUM SENSE FILS: engloben els grups: *WLAN*, *WMAN* i *WWAN*.

WLAN (Wireless Local Area Network): xarxes alternatives a les xarxes d'àrea local cablejades, creant un sistema de comunicació de dades més flexible i facilitant la mobilitat als usuaris o dispositius que es connecten a la mateixa. Aquestes son les xarxes que tractarem abastament en aquest projecte, concretament, en els capítols 3, 4 i 5.

WMAN (Wireless Metropolitan Area Networks): xarxes d'àrea metropolitana que poden arribar fins a distàncies de 10.000 metres. Com hem indicat al gràfic anterior, dins les *WMAN* hi tenen cabuda les xarxes *LMDS* i *Wi-Max*, semblants a les anteriors però basades en l'estàndard *IEEE 802.16*.

WiMax (interoperabilitat mundial d' accés per microones) és un sistema de transmissió sense fils via microones capaç de proporcionar serveis de banda ampla. Les comunicacions s' efectuen a través d' una antena local a les llars i empreses que estan dins l'àrea de cobertura de l'estació base. *WiMax* suposa una solució econòmica al problema tecnològic de la darrera milla per a oferir serveis de gran ample de banda a molts usuaris i és una alternativa viable a la instal·lació de fibra òptica fins a l'usuari o a l' adaptació dels sistemes de televisió per cable per a oferir serveis de banda ampla. *WiMax* forma part de la família d' estàndards 802.16 de l' IEEE i *HyperMAN* de la ETSI, com hem vist anteriorment, i utilitza bandes llicenciades i no llicenciades. Aquest tipus de xarxes son totalment segures, configurades adequadament. En funció del seu ús final, les xarxes WiMax poden

implementar-se amb diferents graus de seguretat. L' ús de protocols de xifrat de dades, el filtre MAC, ocultar el nom de la xarxa o l'autenticació d'usuaris son tècniques d' ús habituals per assegurar el client que només podran accedir a la xarxa els aparells o persones que estiguin autoritzats.

WWAN (Wireless Wide Area Network)*:* xarxa amb gran cobertura mundial, en la que destaquen tecnologies com *GSM*, *GPRS* i *UMTS*, utilitzades per a la tecnologia mòbil.

El sistema ***GSM*** (*Global System for Mobile Communications*) és el sistema de comunicació de mòbils digitals de 2a generació basat en cèl·lules de ràdio i va aparèixer per donar resposta als problemes dels sistemes analògics. En realitzar la transmissió mitjançant commutació de circuits, els recursos queden ocupats durant tota la comunicació i la tarificació és per temps. Aquestes limitacions van donar entrada a *GPRS*. El sistema *GPRS* (**General Packet Radio Service**) actualitza els serveis de dades *GSM* per fer-los compatibles amb *LAN's*, *WAN's* i Internet. Mentre *GSM* fou dissenyat amb un especial èmfasi per a les sessions de veu, l' objectiu principal de *GPRS* fou oferir un accés a xarxes de dades estàndards, com *TCP/IP*. Aquestes xarxes consideren *GPRS* com una subxarxa normal. *GPRS* utilitza els recursos ràdio només quan hi ha dades a enviar o rebre, adaptant-se així perfectament a la molt intermitent naturalesa de les aplicacions de dades. L' ús dels enllaços d'aquest mode conserva la capacitat de xarxa i la interfície. A més a més, permet a les operadores oferir un servei a millor preu, doncs, la facturació la pot realitzar en funció de la quantitat de dades enviades o rebudes. Així doncs, *GPRS* és una nova tecnologia que comparteix el rang de freqüències de la xarxa *GSM* utilitzant una transmissió de dades per mitjà de paquets. La commutació de paquets és un procediment més adequat per a transmetre dades. *GPRS* permet proporcionar serveis de transmissió de dades d'una forma més eficient a com es venia fent abans. Podem dir que *GPRS* és una evolució no traumàtica de *GSM*: no suposa grans inversions i reutilitza part de les infraestructures de *GSM*; és en definitiva, una tecnologia que corregeix les deficiències de *GSM*.

UMTS, amb el seu nom comercial 3G, és la tecnologia utilitzada actualment per a proveir serveis mòbils de dades d'alta velocitat a les xarxes mòbils. La tercera generació (3G) o International Mobile Telecommunications-2000, és una família d'estàndards per a telecomunicacions mòbils que compleix les especificacions de la Unió de telecomunicacions internacional (ITU) que inclou UMTS, CDMA2000, DECT y WiMAX. Els serveis inclouen: telefonia sense fils, vídeo trucada i transferències sense fils de gran abast. Comparat amb els serveis 2G i 2.5G, 3G

permet l' ús simultani de veu i dades a altes velocitats (al menys 200 Kbps). Els serveis actuals, arriben a assolir els 14Mbps i està previst que més al futur.
Les xarxes 3G ofereixen millor seguretat que les seves predecessores 2G i 2.5G. Permetent a l'equip de l'usuari autentificar la xarxa a la que s'estan unint, l' usuari pot estar segur que la xarxa a la que es connecta és la que creu i no una xarxa il·legal que la suplanta. Tot i que en els darrers anys s'han identificat diferents problemes en la nova tecnologia d' encriptació de les dades. A més a més de la seguretat en la infraestructura de la xarxa, s'ha afegit seguretat *end-to-end* tot i que no és estrictament una propietat de 3G. L' evolució d'aquestes tecnologies es mostra en la figura 2.7.

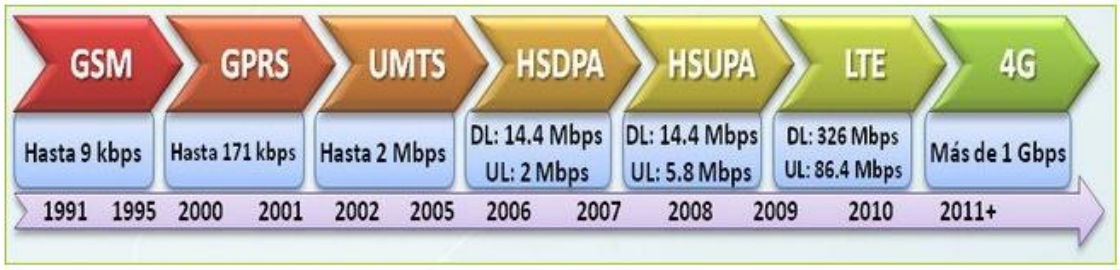

Figura 2.7 Evolució de les tecnologies GSM

Per últim, *4G LTE* és un conjunt de tecnologies de telefonia mòbils ja desenvolupades, en desenvolupament i per a desenvolupar. El grup 3GPP es tracta d'un projecte de col·laboració internacional de planificació de la propera generació de serveis de telecomunicacions cel·lulars. La millora de la tecnologia cel·lular UMTS s'ha anomenat LTE (*Long Term Evolution*). La idea és que 4G LTE permetrà velocitats molt més grans emprant una latència de paquet molt menor. La situació actual es que es compta amb la tecnologia HSPA (High Speed Packet Access), una combinació de *HSDPA* i *HSUPA*, a més a més la tecnologia HSPA+ s'està desenvolupant en l'actualitat. No entrarem en detall sobre el funcionament de les xarxes *4G LTE*, però sí val a dir que son actualment importantíssimes donada la massificació de telèfons mòbils que hi ha al món actualment; aquesta alta utilització està duent a terme una sobrecàrrega de les xarxes *3G*, per això considerem important parlar-ne i contemplar l' ús de les xarxes *Wi-Fi* en mode *Ad-Hoc* com a alternativa a molts dels actuals usos de *3G*. Podem veure a la figura 2.8 la utilització i previsió d'utilització de les comunicacions mòbils.

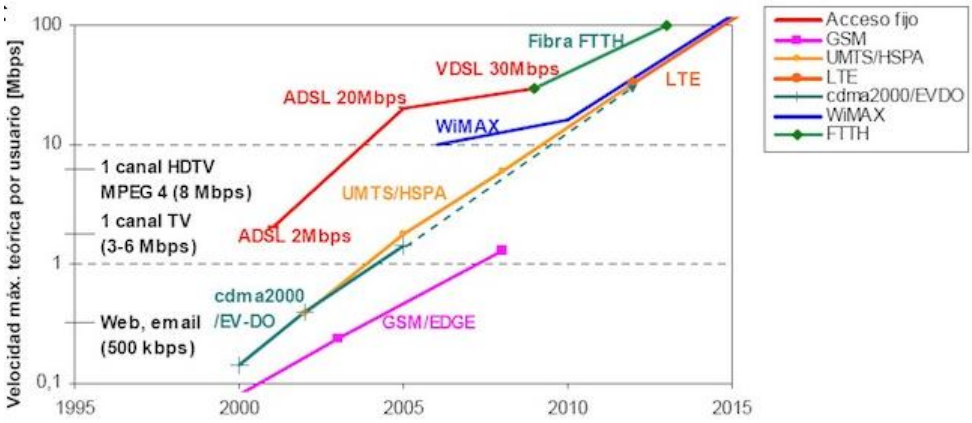

Figura 2.8 Ús de les tecnologies mòbils

Tot i que *4G* és realment innovadora al costat de les seves predecessores, és una evolució del *3G*. Utilitza diferents interfícies de ràdio, no obstant hi ha moltes concordances amb l'actual tecnologia *3G* amb la qual cosa, hi ha molt àmbit per a la reutilització. *LTE* està basat en xarxes IP amb suport a *IPV4* i Ipv6. No hi ha previsió per a la veu, però podrien arribar a utilitzar serveis *VoIP* (veu sobre IP). *LTE* ha introduït un gran nombre de tecnologies comparant amb els sistemes cel·lulars previs. Aquestes permeten operar de forma molt més eficient respecte a l' ús de l'espectre i també proporcionen ratis de transferència molt més alts. D' entre elles, comentarem dues d'elles força importants.

OFDM (*Orthogonal Frequency Division Multiplex*): Aquesta tecnologia, emprada per exemple en els estàndards 802.11g i 802.11a, s'ha incorporat a *LTE* perquè permet transmetre de forma eficient dades a molt altes velocitats mentre que segueixen proporcionant un alt nivell de resistència a reflexions i interferències, enfortint la seva seguretat.

MIMO (*Multiple Input Multiple Output*): un dels principals problemes dels sistemes de telecomunicacions previs foren les senyals derivades de les reflexions que es trobaven. Emprant MIMO aquests camins addicionals del senyal poden utilitzar-se per a incrementar el rendiment. Amb MIMO es necessiten antenes per a permetre distingir els diferents camins. Amb això hem de tenir en compte que aquestes s'han d'instal·lar. A l'estació base pot ser senzill, però instal·lar les antenes en els telèfons mòbils clients serà prou difícil donades les dimensions i resta de requisits d'aquests dispositius. Aquesta tecnologia s'utilitza en 802.11n per a poder assolir majors velocitats i rang d'abast.

3. Xarxes *Wi-Fi*

3.1 Introducció a les xarxes *Wi-Fi*

Wi-Fi significa *Wireless Fidelity.* És un conjunt d' especificacions de comunicació sense fils, que, com hem vist a l' inici d' aquest treball, es basen en l' estàndard 802.11. A vegades, se'l defineix tan sols com a *Wireless* (sense fils), en contraposició a *Wired*, que ve a ser "cablejat", en referència a una xarxa que utilitza fil de coure com a mitjà de transport principal. Val a dir que, si bé totes les connexions *Wi-Fi* son *Wireless*, com hem estat veient NO totes les connexions *Wireless* son *Wi-Fi* (*GPRS*, *UMTS*, *Bluetooth*...).

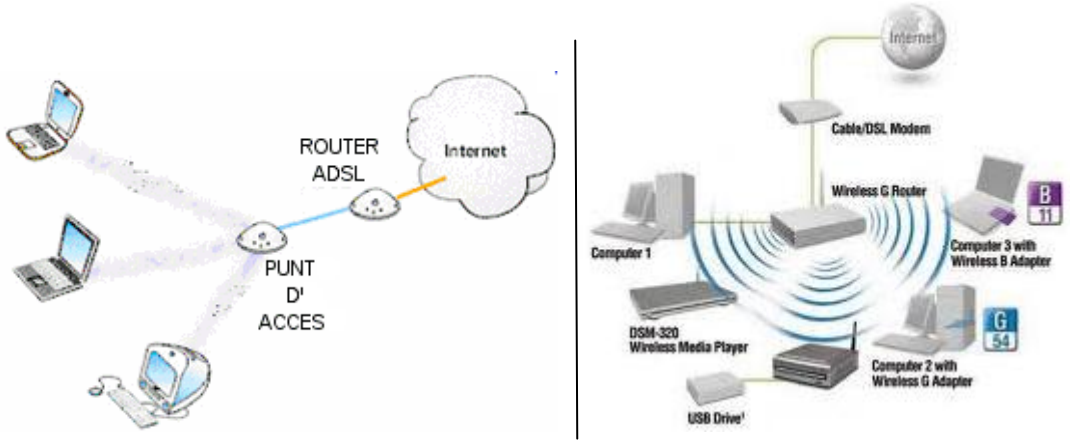

Figura 3.1 Exemple de dues xarxes d'accés sense fils

Tot i que fa força temps que existeixen les comunicacions de xarxa sense fils, la història de les xarxes WLAN és força recent, de poc més d' una dècada. S'ha de tenir en compte que en els seus orígens existia un greu problema d' incompatibilitats, doncs gairebé cada fabricant utilitzava un estàndard diferent. Per aquest motiu, el 1.999 varies empreses (les principals del sector de les comunicacions i les xarxes, com *3com*, *Airones*, *Intersil*, *Lucent Technologies*, *Nokia* o *Symbol Technologies*) van crear la *WECA* (*Wireless Ethernet Compability Aliance*), organització comercial encarregada de provar i certificar que els equips complien amb els estàndards 802.11 i analitzava la seva compatibilitat. Un any després, al 2.000, va certificar l' interoperativitat entre equips (és a dir, que poguessin operar entre ells) sota l' especificació *IEEE 802.11b*, a la que va denominar *Wi-Fi*. Aquesta denominació per extensió s' utilitza per a totes les especificacions posteriors basades en l' estàndard *802.11x* de comunicacions sense fils. Per tant, *802.11b* és una extensió del *802.11* per a *WLAN*

empresarials, amb una velocitat d' 11 Mbps i un abast de 100 m. El 2003, l' IEEE aprova l'estàndard 802.11g, compatible amb l'anterior i capaç d'assolir velocitats dobles i fins i tot arribar a 54 Mbps, per poder competir amb altres estàndards que prometen majors velocitats però incompatibles amb els equips 802.11b, tot i que poden coexistir en el mateix entorn doncs operen a diferents bandes de freqüència.

Figura 3.2 La WECA a www.Wi-Fi.org

Un símbol a l'estil del '*ying-yang'* i que pretén fer un joc de paraules amb el popular *Hi-Fi*, *High Fidelity*, identifica aquesta tecnologia. D'acord amb el que venim explicant, cal tenir en compte que *Wi-Fi* no és compatible amb els altres tipus de connexions *wireless* com *Bluetooth*, *GPRS*, *UMTS*, doncs es regeixen per una altra norma, però totes dins la família de protocols 802.1x.

3.2 Família de protocols 802.11

El *802.11* és una xarxa local sense fils que usa la transmissió per radio a la banda de freqüències de 2,4GHz, o infraroja, amb règims binaris d'1 a 2 Mbits/s. El mètode d' accés al mitjà *MAC* (*Medium Access Mechanism*) és mitjançant escolta però sense detecció de col·lisió, *CSMA/CA* (*Carrier Sense Multiple Access with Collision Avoidance*). La dificultat en detectar la portadora en l'accés WLAN consisteix bàsicament en que la tecnologia utilitza és *Spread-Spectrum* i amb accés per divisió de codi (CDMA), el que comporta a que el mitjà radioelèctric sigui compartit, ja sigui per seqüència directa DSSS o per salts de freqüència en *FHSS*. L'accés per codi CDMA implica que puguin coexistir dos senyals en el mateix espectre utilitzant codis diferents i això per a un receptor de ràdio implicarà que detectaria la portadora inclús amb senyals diferents de les de la pròpia xarxa *WLAN*. Val a dir que la banda de 2,4GHz està reglamentada com a banda d'accés públic i en ella funcionen gran quantitat de sistemes, entre els que s'inclouen telèfons inal·làmbrics *Bluetooth*.
La següent taula pretén donar una breu descripció de la família de protocols 802.11 sense entrar en detall, doncs, no és l'objectiu principal d' aquest TFC.

Estàndard	Descripció
802.11	Estàndard WLAN original. Suporta d' 1 a 2 Mbps
802.11a	Estàndard WLAN d' alta velocitat en la banda dels 5 GHz. Suporta fins a 54Mbps.
802.11b	Estàndard WLAN per a la banda dels 2,4 GHz. Suporta 11 Mbps.
802.11e	Està dirigit als requeriments de qualitat del servei per a totes les interfícies IEEE WLAN de radio.
802.11f	Defineix la comunicació entre punts d' accés per facilitar xarxes WLAN de diferents proveïdors.
802.11g	Estableix una tècnica de modulació addicional per a la banda dels 2,4 GHz. Dirigit a proporcionar velocitats de fins a 54 Mbps.
802.11h	Defineix l' administració de l' espectre de la banda dels 5 GHz per al seu ús a Europa i Àsia-Pacífic.
8021.11i	Està dirigit a vèncer la vulnerabilitat actual en la seguretat per a protocols d' autenticació i de codificació.

Figura 3.3 Família de protocols 802.11

En definitiva, la norma *IEEE 802.11* fou dissenyada per a substituir a les capes físiques i d' enllaç de les xarxes *Ethernet* (802.3) especificant el seu funcionament en xarxes *WLAN*, pel que les xarxes *Wi-Fi* i les *Ethernet* son idèntiques excepte en el mode en què els terminals accedeixen a la xarxa, el que suposa compatibilitat entre ambdues. La comoditat assolida gràcies a la mobilitat que ofereixen les xarxes *Wi-Fi*, junt amb la supressió del cablejat son sens dubte un dels punts forts d'aquest tipus de xarxa. En canvi, a la seva vegada apareixen desavantatges com la pèrdua de velocitat en comparació amb les xarxes cablejades, degut a les interferències i pèrdues de senyal que el medi pot provocar. Com veurem més endavant, el principal problema que sorgeix en les xarxes *WLAN* és la debilitat en la seguretat, ja que amb les eines apropiades en pocs minuts la clau de xarxa pot veure's compromesa si no es protegeix degudament. Amb la finalitat de corregir aquest problema, la *Wi-Fi Alliance* va fer pública la clau *WPA* i posteriorment la *WPA2*, un nou tipus de clau més robusta que les *WEP*. Ho veurem més endavant, en el capítol de seguretat en les xarxes *Wi-Fi*. És necessari considerar així mateix les freqüències concretes que utilitzen els equips *Wi-Fi*. Les xarxes actuals poden utilitzar les bandes de 2,4GHz. O 5GHz.

Estàndard Wi-Fi	*Freqüència*	*Velocitat*	*Rang*
WiFi a (802.11a)	5 GHz	54 Mbit/s	10 m
WiFi B (802.11b)	2,4 GHz	11 Mbit/s	100 m
WiFi G (802.11b)	2,4 GHz	54 Mbit/s	100 m

Figura 3.4 Rang de freqüències Wi-Fi

La banda de 2,4GHz. Conté des de les freqüències de 2.400 GHz fins a 2.4835 GHz. I conté 13 canals, amb un ample de banda de 22 MHz cadascun, a Europa doncs, per regulació dels organismes que apliquen a cada país o regió, varia en alguns casos com EEUU amb 11 canals o el Japó amb 14). En canvi, en contra del que es sol creure, no son canals independents, doncs es solapen parcialment entre ells, de manera que només existeixen tres canals totalment independents, el canal 1, el 6 i l'11.

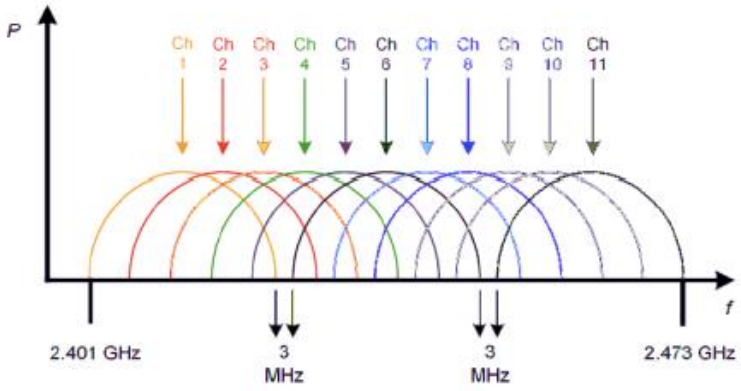

Figura 3.5. Canals i freqüències Wi-Fi

3.3 Topologies de les xarxes *Wi-Fi*

- El *mode d' infraestructura* en la que els clients es connecten a la xarxa a través d' un punt d' accés comú. Aquest és, en termes generals, el mode d'accés més comú i habitual en empreses, escoles, universitats, aeroports, estacions, establiments comercials...Per defecte les targetes *802.11b* venen amb aquest mode predeterminat.

- El mode *Ad-hoc* en el que els clients es connecten entre ells sense comptar amb cap punt d'accés.

El mode d' infraestructura és un mode de funcionament que permet connectar ordinadors equipats amb targeta *Wi-Fi* per mitjà d' un o més punts d'accés que actuen com a connectors (exemple: *hub*/*switch* en una xarxa cablejada). La implementació d'aquest tipus de xarxa requereix posar punts d'accés a intervals regulars en la zona que ha de ser coberta per la xarxa. Els punts d'accés han d'estar configurats amb el mateix SSID per a que puguin comunicar-se els diferents equips que han de veure aquell SSID com a nom d' entrada a la xarxa. L' avantatge d'aquesta topologia és que garanteix un pas obligat pel punt

d'accés, fet que permet verificar qui entra a la xarxa. En canvi, la xarxa no pot créixer, a menys, que es col·loquin més nodes d'accés.

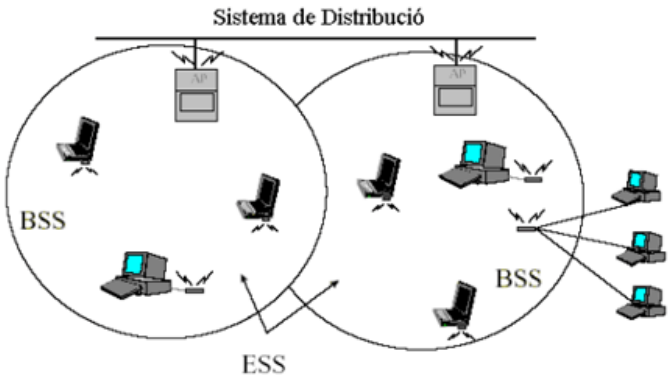

Figura 3.6 Mode d' infraestructura Wi-Fi

En aquest mode, cada estació informàtica es connecta a un punt d' accés a través d' un enllaç sense fils. La configuració formada pel punt d'accés i les estacions ubicades dins l' àrea de cobertura s'anomena servei bàsic o *BSS*. Aquests formen una cèl·lula. Cada *BSS* s' identifica a través d' un *BSSID* (identificador de *BSS*) que és un identificador de 6 Bytes (48 bits). En aquest mode el *BSSID* correspon amb l'adreça *MAC* del punt d'accés. És possible vincular diferents punts d'accés junts, és a dir, diferents *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 inclús una xarxa sense fils. Un ESS s' identifica a través d' un *ESSID*, que conté 32 caràcters en codi *ASCII*. L' *ESSID*, sovint anomenat *SSID*, mostra el nom de la xarxa, d'alguna manera representant una mesura de seguretat de primer nivell, doncs una estació ha de saber l' SSID per a connectar-se a la xarxa estesa. Quan un usuari itinerant va des d' un BSS a un altre, mentre es mogui dins l' ESS, l' adaptador de xarxa sense fils del seu equip pot canviar de punt d'accés, segons la qualitat de la senyal que rebi des de diferents punts d' accés. Aquests es comuniquen entre si a través d'un sistema de distribució amb la finalitat de bescanviar informació sobre les estacions. Aquesta característica que permet a les estacions moure's de forma transparent d' un punt d'accés a un altre, s' anomena *itinerància*.

Per la seva banda, el mode *'ad-hoc'* és un mode de funcionament que permet la comunicació directa entre ordinadors que posseeixen una targeta de xarxa *Wi-Fi*, sense necessitat d'utilitzar un altre equip suplementari, com els punts d'accés del mètode d' infraestructura. Aquest mètode és ideal per a interconnectar ràpidament equips entre ells sense material addicional.

Figura 3.7 Mode ad-hoc Wi-Fi

La implementació d'una xarxa d'aquest tipus es limita a configurar els equips en mode *ad-hoc*, la selecció del canal (freqüència) i de l' SSID comú per a tots ells. L'avantatge d'aquest mode de treball és que elimina materials suplementaris costosos, doncs és de fàcil implementació. Gràcies a l'addició d'un programa d' encaminament dinàmic, de l' estil *OLSR*, *AODV*, etcètera, la xarxa creix automàticament amb la connexió de nous equips.

3.4 Elements d'una xarxa *Wi-Fi*

Com hem vist de passada en l'apartat anterior, els components principals d'una xarxa *Wi-Fi* son quatre:

Estacions: son els equips terminals destinats a enviar i rebre la informació des de i cap a Internet. Per exemple, els portàtils.
Medi de transport: és el suport que permet la transferència de dades entre estacions. L' estàndard permet dues tecnologies diferents per a la propagació del senyal, radiofreqüència i infrarojos, essent aquesta última la més utilitzada.

Punt d'accés: un punt d' accés és una estació que permet connectar altres estacions al sistema de distribució. Els punts d'accés es situen de forma que poden proporcionar la cobertura necessària per donar servei als terminals que no tenen comunicació directa, augmentant el seu radi de cobertura. A més a més, el punt d'accés centralitza totes les comunicacions entre estacions, doncs, si dues estacions volen comunicar-se entre elles, ho faran a través del punt d'accés. Per tant, el radi de cobertura d' un punt d' accés limita la distància a la qual pot comunicar-se l' estació. Malgrat això, podem augmentar la cobertura de la xarxa mitjançant un sistema de distribució.

Sistema de distribució: un sistema de distribució està format per diferents punts d' accés connectats entre ells mitjançant alguna tecnologia, de forma que

es pugui obtenir una àrea de cobertura major. Els punts d' accés han de comunicar-se per a gestionar la mobilitat de les estacions. La tecnologia més habitual en els sistemes de distribució és *Ethernet*, tot i que s' utilitzen altres tecnologies. Quan una estació mòbil es mou d'una zona de cobertura d' un punt d'accés a una altra, es fa evitant els talls en la comunicació i la pèrdua de cobertura.

3.5 Avantatges i inconvenients

Les xarxes *WLAN* presenten força avantatges:

- La comoditat perquè qualsevol usuari que tingui accés a la xarxa pot connectar-se des de diferents punts dins un rang suficientment ampli d'espai.
- Les xarxes *Wi-Fi* permeten l' accés de molts ordinadors sense cap mena de problema ni despesa en infraestructura, no és així en la tecnologia amb cables (Ethernet).
- La *Wi-Fi Alliance* assegura que la compatibilitat entre dispositius amb la marca *Wi-Fi* és total, amb la quan cosa a qualsevol part del món podrem utilitzar la tecnologia *Wi-Fi* amb una total compatibilitat.

Però como a xarxa sense fils, la tecnologia *Wi-Fi* presenta els problemes intrínsecs de qualsevol tecnologia sense fils:

- Menor velocitat en comparació a una connexió amb fils, degut a les interferències i pèrdues de senyal que l'ambient pot provocar.

- Malgrat això, **el principal desavantatge recau en el camp de la seguretat.** Existeixen programes capaços de capturar paquets, treballant amb la seva targeta *Wi-Fi* en mode promiscu, de forma que poden arribar a obtenir la clau de la xarxa i per tant, accedir a ella. Les claus de tipus *WEP* son relativament fàcils d'aconseguir amb aquest sistema. L' aliança *Wi-Fi* va solucionar aquests problemes publicant l'estàndard *WPA* i posteriorment *WPA2*, basats en el grup de treball *802.11i*. Les xarxes protegides amb *WPA2* es consideren robustes donat que proporcionen molt bona seguretat.

- No es pot controlar l' àrea de cobertura d' una connexió, de manera que un receptor es pot connectar des de fora de la zona de recepció prevista.

3.6 Abast de les xarxes *Wi-Fi*

El rang de cobertura de les xarxes *Wi-Fi* depèn de molts factors, que inclouen els requisits de velocitat de les dades i la capacitat, les fonts d' interferència de les ones de radiofreqüència, les característiques físiques de la zona, d'energia, connectivitat i ús de l'antena. El rang típic per a la connectivitat dels equips o dispositius *Wi-Fi* és de **50 a 100 metres sota sostre**, amb un abast significativament superiors a l'aire lliure. L' ús d amplificadors de senyals pot augmentar el número de dispositius connectats a kilòmetres de distància.

4. Seguretat *Wi-Fi*. Vulnerabilitats, riscos i amenaces

4.1 Introducció

La seguretat en les xarxes és en general una assignatura pendent, però en les xarxes *Wi-Fi* pren una atenció especial, segons hem estat veient en el capítol anterior.

El major problema de la seguretat de les xarxes *Wi-Fi* ve donat per la seva dispersió espacial. No està limitada a una àrea, a un fil o a la fibra òptica, ni tenen punts concrets d'accés o connexió, sinó que s'expandeixen i son accessibles des de qualsevol punt dins el seu radi de cobertura. Això les fa molt vulnerables: la possibilitat de l'accés o monitorització de les dades és una amenaça molt real. És pel motiu indicat anteriorment que els equips permeten l' encriptació de les comunicacions emprant diferents **algoritmes**, que permeten tant autenticar els usuaris com evitar accessos no autoritzats i eviten la captura del tràfic de la xarxa mitjançant sistemes aliens a ella. Una altra de les conseqüències de ser una xarxa via ràdio és la influència d'altres fonts radioelèctriques, ja sigui altres xarxes *Wi-Fi*, equips de ràdio que treballin a la mateixa banda o aparells electrònics que generin interferències. És per tant possible la generació d' una interferència premeditada que bloquegi la xarxa *Wi-Fi* i eviti el correcte funcionament de la mateixa, per exemple. Afegit a això, existeix la possibilitat de la realització d'atacs de denegació de servei (DoS), tant els clàssics, comuns a totes les xarxes, com altres específics de les xarxes *Wi-Fi*. Tant atacs reals als diferents protocols d'autenticació com terminals que

no compleixin amb els temps i regles d'accés imposades per les normes *Wi-Fi*, poden degradar o inclús parar totalment el funcionament de la xarxa *Wi-Fi*.

4.2 Normes preventives d' ús bàsic

Quan es pensa en la vulnerabilitat d' una xarxa *Wi-Fi* es considera la possibilitat que un client no autoritzat accedeix a dades de la xarxa. En canvi, existeix un altre perill vinculat a la vulnerabilitat de les *Wi-Fi*: la inclusió d'un punt d'accés no autoritzat en la xarxa. En una organització, el senyal *Wi-Fi* serà accedit pels usuaris mitjançant punts d' accés, de tal manera, que un atacant pot afegir-ne un que anunciï el mateix nom de xarxa, confonent així altres clients que vulguin connectar-se. Depenent de l' elaboració de la suplantació, el client pot arribar a revelar dades i claus importants. Per a minimitzar el perill que suposa la implementació d' una xarxa sense fils, existeixen una sèrie de **normes bàsiques** a l' hora de configurar una xarxa *WLAN*:

Canviar les configuracions per defecte.
Activar l' encriptació.
Usar claus fortes.
Sobretot, fer o contractar ***auditories de seguretat*** de forma periòdica (veurem un exemple en el punt 6.2 d'aquest TFC).

Desactivar l'anunci del nom de la xarxa, SSID: tot i que no és viable en tots els casos, la desactivació de l' anunci del nom de la xarxa és un element de seguretat afegit. Per un cantó, impedirà que l'atacant identifiqui la naturalesa i propietari de la xarxa, i per un altre, farà necessari introduir el nom de la xarxa manualment per a permetre l' associació a la xarxa *Wi-Fi*, pel que prèviament haurà de ser coneguda per l'atacant.

Filtratge d' adreces MAC: A la majoria de punts d' accés és possible especificar una llista d'adreces *MAC* que seran admeses, essent totes les demés, rebutjades. L'adreça *MAC* és una direcció de nivell 2 que porta la targeta de xarxa *Wi-Fi* gravada de fàbrica (d'igual forma que les *MAC* de les xarxes *Ethernet*). Per tant, si permetem només l'accés a les adreces *MAC* dels equips que volem que entrin a la xarxa, impedirem que algun altre sistema extern pugui connectar-se de forma accidental o premeditada. Existeixen, però, targetes de xarxa que permeten el canvi de l'adreça *MAC* i en aquest cas seria possible per a un atacant de la nostra xarxa, assignar-li una adreça vàlida d'algun dels nostres equips, superant així aquesta mesura de seguretat. Això implica que l'atacant hauria de conèixer alguna de les adreces *MAC* dels nostres

equips, però si les mesures de seguretat física i informàtica estan correctament implementades, no resultaria fàcil.

Ús d' adreces IP estàtiques: no és un problema real per a un *hacker* amb coneixements, però sí dificulta l'accés a intrusos addicionals. És comú tenir a les xarxes *Wi-Fi* l' assignació automàtica d' adreces IP, gateway i DNS. La pràctica d'assignar les adreces manualment als terminals sense fils té l' avantatge que l'atacant ha d' esbrinar en primer les dades de la xarxa, i més important, encara, ens permet habilitar filtres de manera que només les adreces IP assignades seran permeses. Si l'atacant usa alguna d' aquestes IP's assignades, eventualment pot arribar a ser detectat doncs pot entrar en conflicte amb els terminals legals.

VLAN pròpia per a la xarxa Wi-Fi: és interessant la implementació en aquells equips que ho permeten d' una *VLAN (LAN virtual)* específica per a la xarxa *Wi-Fi*. Degut a que és una xarxa insegura per naturalesa pròpia, és recomanable mantenir-la separada en tot moment de la xarxa amb fils. Així doncs, si el punt d'accés o el controlador associat és capaç de gestionar *VLAN*s, mantenir el tràfic de la xarxa *Wi-Fi* en una *VLAN* diferent permetrà implementar mecanismes de seguretat i accés suplementaris que controlin l' accés dels usuaris *Wi-Fi* a les dades de la xarxa corporativa.

Instal·lació d' un firewall: Relacionat amb el punt anterior, l' accés dels clients *Wi-Fi* a la xarxa cablejada hauria de ser gestionat per un firewall, ja sigui actuant de pont entre les corresponents VLANs o com a element físic de control, interposant-se en el flux de tràfic *Wi-Fi*. A qualsevol arquitectura, la inclusió d' un firewall (hardware o software) ens permetrà implementar polítiques d'accés segures i complexes que assegurin que, tot i que algun intrús aconseguís connectar-se a la nostra xarxa *Wi-Fi*, no progressi fins a tenir accés a dades sensibles. Podeu veure el punt 4.4 d'aquest document on ampliem la informació.

Aquestes mesures, per si mateixes, correctament implementades proporcionen seguretat suficient per a entorns no sensibles. En canvi, existeix la possibilitat també **d'augmentar la seguretat** emprant tècniques avançades, part de les quals precisen de la participació d' un controlador de punts d'accés (següents punts).

4.3 Protocols de seguretat. WEP-WPA-WPA2

Les xarxes *Wi-Fi* incorporen, com a principal mesura de seguretat, la possibilitat d' encriptar la comunicació. A més a més de duar a terme les normes bàsiques vistes prèviament, és una pràctica molt recomanable, doncs al ser un medi sense fils, és molt senzill capturar el tràfic que per ella circula i per tant, la captura, per persones no desitjades, de dades sensibles és realment fàcil.

Al llarg del desenvolupament de les xarxes *Wi-Fi* han anat sorgint diferents mètodes d' encriptació de les comunicacions, evolució necessària doncs els diferents mètodes han resultat ser vulnerables i ha sigut necessari implementar algoritmes més segurs que solucionessin els problemes dels anteriors. Aquests, al mateix temps, van demanant més recursos dels equips que els implementen pel que la solució adoptada serà sempre un compromís entre rendiment i velocitat. Els mètodes estàndard disponibles es detallen a continuació.

WEP (Wired Equivalent Privacy): a l' inici de les xarxes *Wi-Fi* ja es va veure que presentaven problemes de seguretat intrínsecs a la seva naturalesa. Per aquesta raó, aquestes xarxes van néixer amb la possibilitat d'activar encriptació i accessos mitjançant claus, essent *WEP* el primer mètode que es va implementar. Ja en el mateix nom s' observa quin era l' objectiu d'aquesta encriptació: donar a les xarxes sense fils la mateixa seguretat que existia en les xarxes cablejades. Per contra, la implementació d'aquest protocol pateix problemes de disseny, que fan que si un equip es troba dins l'abast de la xarxa, pugui capturar els paquets d'aquesta (primera vulnerabilitat de *WEP*); amb una quantitat important de paquets capturats es pot arribar a esbrinar la clau de la xarxa i per tant, es pot accedir a ella. El procés de captació de la clau de xarxa es pot fer amb eines públiques gratuïtes i pot trigar-se tan sols, uns minuts. *WEP* 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 de l' IV), segona gran vulnerabilitat.

Els missatges de difusió de les xarxes sense fils es transmeten per ones de ràdio, fet que els fa més susceptibles, front altres xarxes cablejades, de ser captats amb relativa facilitat. Presentat el 1999, el sistema *WEP* fou pensat per a proporcionar una confidencialitat comparable a la d' una xarxa tradicional cablejada. Permet claus de diferents longituds de bits, el que teòricament fa augmentar la seva seguretat, però en la pràctica, i deguts als problemes existents en la implementació d'aquest protocol, la única repercussió d' utilitzar una clau més llarga és que es augmentarà el temps necessari per esbrinar la

clau de la xarxa, però seguirà sent vulnerable. Dins de *WEP* es reconeixen dos mètodes d'autenticació d' usuaris: *Open System* i *Shared Key*.

El primer d'ells, *Open System* (autenticació de sistema obert), no implementa realment autenticació, debilitant la seguretat del protocol, doncs, el punt d'accés permetrà que s'afegeixi qualsevol client, tot i que posteriorment s' obligarà a que tota la comunicació de dades sigui codificada segons l' algoritme dictat per *WEP* (RC4).

Pel contrari, *Shared Key* dicta que els clients hauran d' utilitzar la seva clau *WEP* per autentificar-se amb el punt d'accés i que només aquells que tinguin les credencials correctes seran admesos pel punt d'accés com a clients (autenticació).

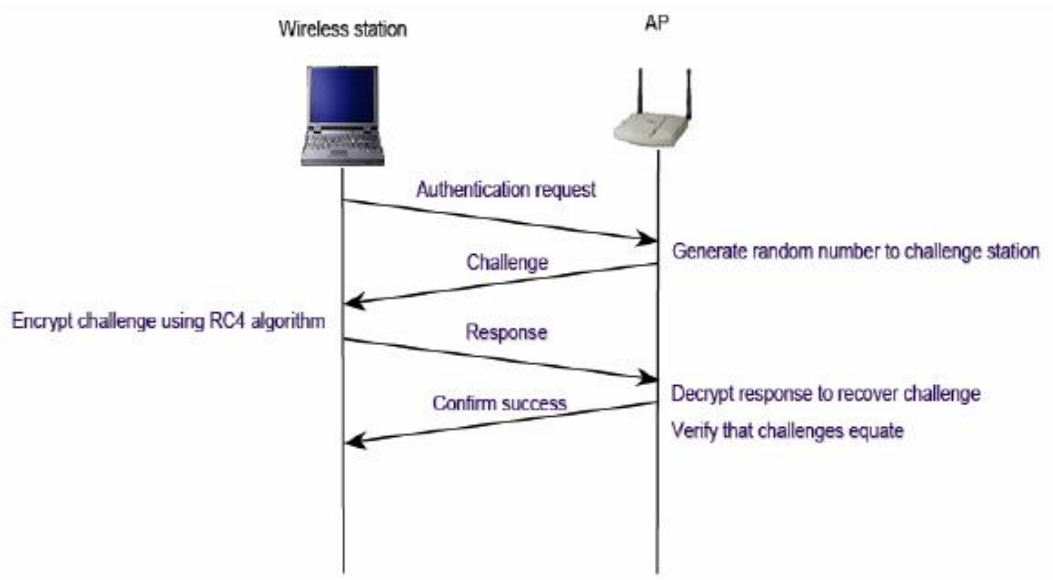

Figura 4.1 Mètode d'autenticació WEP Shared Key Authentication

En la pràctica és recomanable utilitzar autentificació *Shared Key*, doncs *Open System* no proporciona realment una autentificació dels clients, només encriptació de les comunicacions, i tot i que seria suficient per a preservar la confidencialitat de les dades, exposa el punt d'accés a atacs de denegació de servei (DoS). Aquest protocol no implementa cap gestió de claus, el que el fa més vulnerable. La clau utilitzada és compartida pel punt d' accés i tots els clients i ha de ser distribuïda a aquests de forma manual. Una conseqüència d'això és que amb tenir accés a un únic equip, es té la clau que compromet tota la resta d'equips de la xarxa (!). Actualment, pels problemes descrits es recomana utilitzar algun altre mètode dels disponibles, escollint només aquest si no existís alternativa viable i procurant acompanyar-lo d'algun altre protocol d'

encriptació general com *IPSEC* o *SSL*. El principal defecte de *WEP* és que no implementa adequadament el vector d' iniciació (*IV,* conjunt de bits aleatoris de la mateixa longitud que un bloc) de l' algoritme *RC4* (dins la criptografia, *RC4* és el sistema de xifrat de flux *Stream cipher* més utilitzat), ja que utilitza un enfocament directe i previsible per incrementar el vector d' un paquet a un altre. A més a més, existeix un problema amb els tamanys dels vectors d' iniciació. Malgrat 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' iniciació. Coneixent els *IV* utilitzats repetidament i aplicant tècniques relativament senzilles de desxifrat poden finalment vulnerar-se les mesures de seguretat *WEP* implementades. Escollint *IV* diferents cada vegada, encara que el text en clar sigui el mateix, les dades xifrades seran diferents. L' algoritme *RC4* està format per 64 bits, formats per 24 bits corresponents al *IV*, i 40 bits més de la clau secreta. Els 40 bits son els que es distribueixen manualment; l' *IV*, en canvi, és generat dinàmicament i hauria de ser diferent per cada trama; l' objectiu perseguit amb l' *IV* és xifrar amb claus diferents per evitar que un atacant capturi suficient tràfic xifrat amb la mateixa clau i acabar deduint-la; ambdós extrems han de conèixer tant la clau secreta com l' *IV*; la primera és coneguda, doncs està emmagatzemada en la configuració de cada element de xarxa; l' IV, en canvi, es genera en un extrem i s'envia amb la pròpia trama a l'altre extrem, pel que també serà conegut. En viatjar l' *IV* en cada trama, és fàcil interceptar-lo. *Per* atacar una xarxa *Wi-Fi* es solen utilitzar els anomenats *Packet sniffers* i els *WEP crackers* (veure annex d'aquest TFC). Per dur a terme aquest atac es captura una quantitat determinada de paquets (dependrà del número de bits del xifrat) mitjançant un *packet sniffer* i després, amb un *WEP cracker* o *key cracker* es tracta de trencar el xifrat de la xarxa. Un *key cracker* és un programa basat generalment en matemàtiques estadístiques que processa els paquets capturats per desxifrar la clau *WEP*. *Crackejar* una clau més llarga requereix la captura de més paquets, però hi ha atacs actius que estimulen el tràfic necessari (enverinadors d' *ARP*). Per tots aquest motius, *WEP* és vulnerable, no és un protocol segur que proporcioni confidencialitat, integritat de les dades ni autenticació segures, cal veure altres alternatives.

Alternatives a *WEP* poden ser *WEP2*, *WEP Plus*, *WEP dinàmic*. *WEP2* utilitza xifrat i vector d'iniciació de 128 bits. Aquesta millora fou presentada després dels primers models *802.11i*. Aquest es podia desenvolupar sobre alguns (no tots) tipus de hardware que no eren capaços de gestionar *WPA* o *WPA2* (els veurem a continuació). S'esperava que eliminés la deficiència del duplicat del vector d'iniciació així com atacs a les claus per força bruta. Però, com encara es basava

en l'algoritme de xifrat *RC4*, seguia mantenint les mateixes vulnerabilitats que el seu predecessor, *WEP*. Finalment, després que quedés clar que l'algoritme *WEP* era deficient i requeria encara més correccions, tant *WEP2* com *WEP* foren descartats. Les dues longituds de clau ampliades formaren el que més endavant es coneixeria com *TKIP* del *WPA* (ho veiem més endavant).

WEP Plus és una millora desenvolupada per *Agere Systems* (abans, una filial de *Lucent Technologies*) que millora la seguretat *WEP* evitant "IV's febles". Aquest protocol és completament eficaç únicament quan és emprat a ambdós extrems de la connexió sense fils (seria limitació). És possible que tard o d'hora s'aconsegueixin atacs amb èxit al sistema *WEP Plus*.

WEP dinàmic: les claus *WEP* canvien de forma dinàmica. Cada client utilitza dues claus: una d'assignació i una predeterminada. La primera es comparteix entre el client i el punt d'accés i protegeix les trames unidifusió. La clau predeterminada és compartida per tots els clients per a protegir les trames de difusió i multidifusió. WEP de clau dinàmica ofereix avantatges significatius sobre les solucions de WEP amb clau estàtica. La més important es refereix a que es redueix l' àmbit de cada clau. Les claus s'usen amb menys freqüència i es redueix el compromís de la clau utilitzant-la per protegir menys tràfic. Una altra avantatge és que a intervals periòdics les claus s' actualitzen en el punt d'accés. És un sistema distribuït per algunes marques comercials com 3Com. La idea del canvi dinàmic es va fer dins el *802.11i* com a part de *TKIP*, però no per a l'actual algoritme *WEP*.

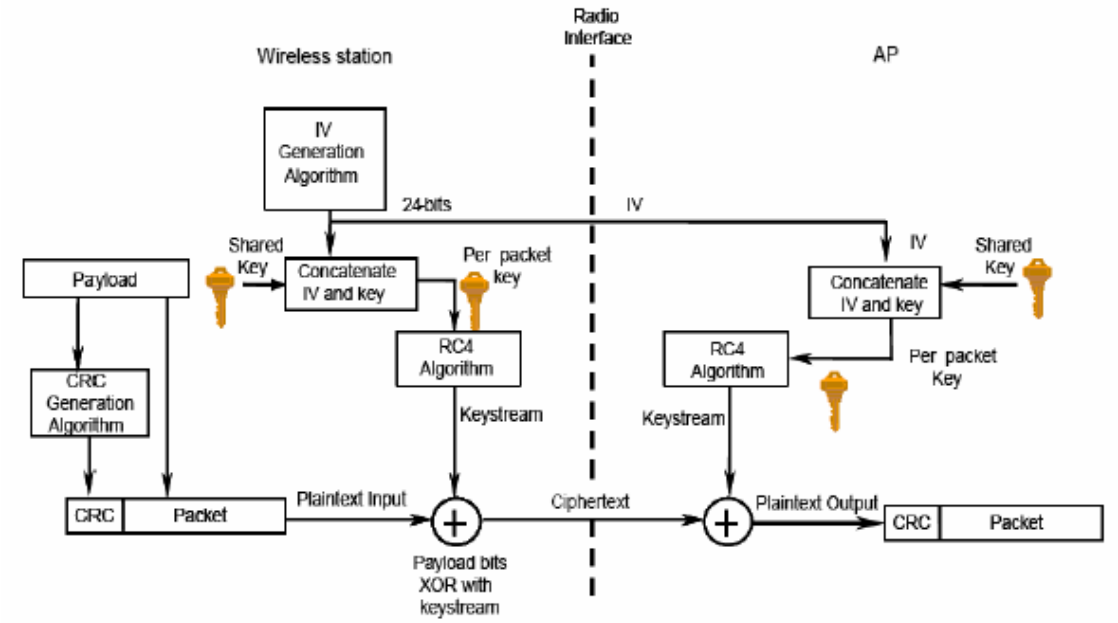

Figura 4.2 Confidencialitat WEP (algoritme RC4)

La solució recomanada pels problemes de seguretat *WEP* és canviar a *WPA2* o *WPA*. Qualsevol d'ells és molt més segur que *WEP*. Per utilitzar *WPA* o *WPA2* alguns punts d' accés vells podrien arribar a ser substituïts o ve patir una actualització de firmware.

***WPA* (Wi-Fi Protected Access)**: desenvolupat per la *Wi-Fi Alliance* com a resposta als errors de seguretat detectats amb *WEP*. Per contra, es va demostrar que la seguretat proporcionada per aquest nou protocol podia ser trencada si es capturaven els paquets que intercanviaven el punt d'accés i el client durant el procés d' autenticació. Amb aquesta informació, si la clau és curta i senzilla, que no hauria de ser lo habitual, però passa, es pot saber la clau fàcilment i per tant es podrà accedir a les dades de la xarxa. També es van detectar punts d' inseguretat en el protocol que, tot i que a dia d'avui no han sigut explotat per eines públiques, no es descarta que aparegui el software necessari per aprofitar aquesta vulnerabilitat.

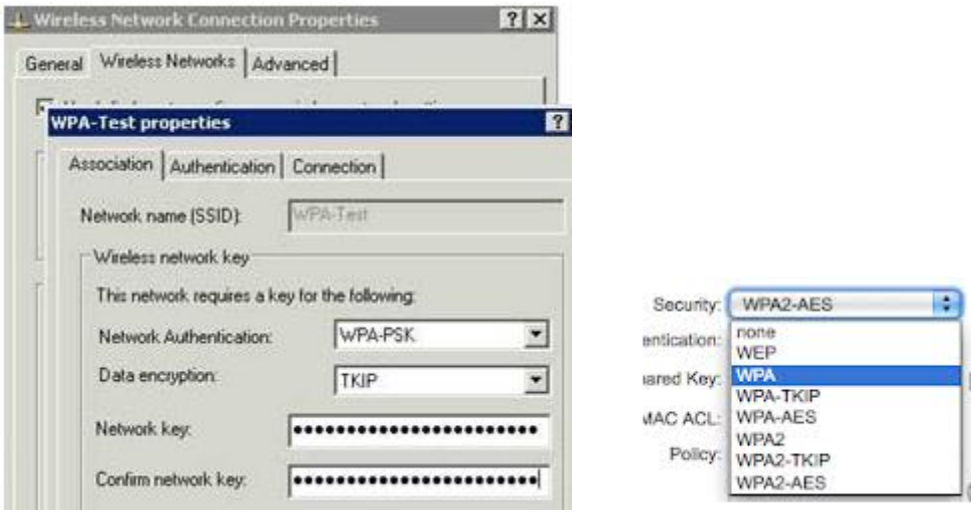

Figura 4.3 Propietats de xarxes Wi-Fi amb WPA

WPA incorpora alguns sistemes d' autentificació i encriptació que aporten seguretat extra, entre els que cal destacar els següents:

TKIP: *Temporal Key Integrity Protocol*: es basa en un sistema de verificació d'integritat del paquet, és a dir, que aquest no ha sigut alterat durant la transmissió, i l' ús d' una clau que varia durant la comunicació, amb el que solucionem problemes de *WEP*, doncs la clau variarà en menor temps i número de paquets dels que es necessiten per esbrinar-la, perquè no es disposarà d'informació suficient per fer-ho i encara que s'arribés a obtenir, ja no seria vàlida per a la comunicació en curs, doncs, la clau hauria canviat.

AES (Advanced Encryption Standard): Algoritme d' encriptació més segur que *TKIP*, la implementació del qual no és obligatòria en sistemes *WPAv1*. Com a contrapartida a aquesta major seguretat, demanda una major capacitat de procés per part dels punts d' accés i els clients. No obstant hauria de ser l' escollit, si és possible, davant *TKIP*.

EAP (Extensive Authentication Protocol): és un protocol d'autentificació i encriptació que va associat al protocol 802.1x, i, que per tant, treballa en conjunció amb servidors d'autentificació tipus *RADIUS*. Fa uns anys es van trobar problemes de seguretat en el protocol *EAP*, fet que va desencadenar en noves variants que, mitjançant l' ús de protocols de seguretat associats, pretenien resoldre els problemes descoberts. D'aquest procés va sorgir *Extended EAP*, amb diferents variants. Cal destacar que alguna d'aquestes variants com *EAP-LEAP* tenen errors coneguts i la seva seguretat pot veure's compromesa amb eines públiques i gratuïtes.

	Authentication	Encryption	Suitable for corporate WAN	Suitable for home and small business WLAN
WEP	none	WEP	poor	less than good
WPA (PSK)	PSK	TKIP	poor	best
WPA2 (PSK)	PSK	AES-CCMP	poor	best
WPA (full)	802.1x	TKIP	better	good (expensive)
WPA2 (full)	802.1x	AES-CCMP	best	good (expensive)

Figura 4.4 Comparació entre WEP-WPA i WPAv2

WPAv2: davant la detecció de l'existència d' un forat de seguretat del protocol utilitzat per WPAv1, la *Wi-Fi Alliance* va desenvolupar una segona versió que corregia aquest problema. Aquesta segona versió obligava la implementació del protocol d' encriptació *AES*, essent aquest d' us per defecte en la norma *WPAv2*. Els protocols *WPA* permeten l' autentificació mitjançant una clau compartida entre client i punt d'accés, o fent us de mecanismes més elaborats mitjançant l' ús d' un servidor de credencials. Originalment ambdós tipus d'arquitectura no tenien un nom normalitzat, i acostumaven a rebre el nom de WPA el que feia ús del servidor centralitzat i *WPA-PSK* el que feia ús de la clau compartida (*Preshared Shared Key*, *PSK*). Actualment s'ha normalitzat l' ús dels termes "personal" per a l' ús de la clau compartida, i "*Enterprise*" a aquella que proveeix autentificació contra un servidor RADIUS mitjançant protocol 802.1x.

Table 1. Main features of WEP, WPA, and WPA-2

	WEP	*WPA*	*WPA-2*
Authentication	N/A	IEEE 802.1X/ EAP/PSK	IEEE 802.1X/ EAP/PSK
Cryptographic algorithm	RC4	RC4	AES
Key size	40 O 104 bits	128 bits	128 bits
Encryption method	WEP	TKIP	CCMP
Data integrity	CRC32	MIC	CCM
Keys for packets	No	Yes	Yes
IV length	24 bits	48 bits	48 bits

Figura 4.5 Comparativa de WEP, WPA i WPA2

A la *Bibliografia* d' aquest document teniu les fonts d' on hem tret la informació referent als protocols *WEP/WPA* i *WPAv2* i el seu funcionament.

4.4 Procés d' autenticació 802.1x

La norma *802.1x* va sorgir com a resposta a la necessitat de proporcionar seguretat a nivell d'usuari. No és d' ús exclusiu de les xarxes *Wi-Fi*, doncs de fet fou creada per donar seguretat a les xarxes *Ethernet*, però es va veure que podria ser un element important per a les xarxes *Wi-Fi* i es va integrar amb aquestes. El protocol *802.1x* utilitza per autentificació i encriptació el protocol *EAP*, vist en l'apartat anterior, normalment en alguna de les variants *Extended EAP* i la referència de la qual dependrà del fabricant dels equips.

En una arquitectura *802.1x* existeixen sempre tres elements:

Suplicant (Peticionari): es designa per aquest terme el client que desitja accedir a la xarxa i intenta autentificar-se. En una xarxa *Wi-Fi* és el client que desitja connectar-se amb el punt d'accés per entrar a la xarxa.
Authenticator (autentificador): és l'equip que rep la petició de connexió del client i que per tant ha de tramitar l'autentificació d'aquest. En el cas de les xarxes *Wi-Fi* aquest rol el du a terme el punt d'accés.
Authenticator Server (Servidor d' Autentificació): és l'equip que manté i gestiona de forma centralitzada les credencials dels usuaris. Aquest servei s' implementa mitjançant un servidor *Ràdius*.
A la figura 4.6 podem veure la comunicació i relació existent entre els diferents elements:

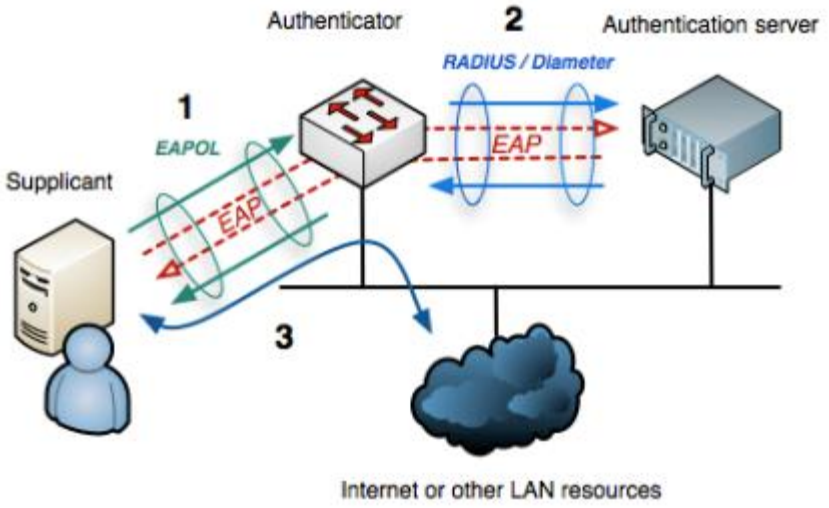

Figura 4.6 Arquitectura 802.1x

En una xarxa amb autentificació 802.1x el funcionament davant la connexió d' un client és com segueix:

- Quan un client intenta connectar-se a un punt d'accés, aquest respondrà al client sol·licitant una autentificació del tipus 802.1x.
- El client haurà d'enviar al punt d' accés les credencials (claus, certificats...) que serveixin per autentificar-se davant la xarxa.
- El punt d'accés no posseeix les dades necessàries per a gestionar les credencials, pel que farà ús del servidor d'autentificació *RADIUS*, a qui li enviarà les credencials del client.
- El servidor *Ràdius* respondrà al punt d' accés indicant-li el tipus d' accés que té li usuari en base a les credencials enviades.
- El punt d' accés, a partir de la resposta del servidor RADIUS, denegarà o concedirà l 'accés a la xarxa al client, en les condicions en què el RADIUS li hagi notificat.

Aquest tipus d'autentificació proporciona grans avantatges desitjables en xarxes amb un número elevat d'usuaris o que requereixin un control sobre el seu ús a la xarxa. La principal característica és que existeix un sol punt on emmagatze-mar totes les credencials i usuaris i que aquest sistema serà el darrer responsable en assignar el tipus d'accés de cadascun d' ells. Així doncs, el servidor RADIUS podrà dur a terme les tasques de triple A (*Authentication, Authorization and Accounting*) de forma centralitzada, fet que facilita i redueix costos en el manteniment i el control de la xarxa i els usuaris. En disposar d' un servidor RADIUS ja no es disposa d' una sola clau per a garantir l'accés a

qualsevol usuari de la xarxa, sinó que les credencials dependran de cada usuari, fet que permetrà entre altres coses, dur un registre dels accessos a la xarxa i l'assignació de diferents privilegis i nivells d' accés depenent de l' usuari que es connecta. Així mateix, s' incrementa la seguretat del sistema, doncs les claus ja no resideixen en el punt d'accés, que és l'extrem de la xarxa, sinó en un servidor dedicat amb un nivell de seguretat major. També soluciona el problema del robatori de claus o credencials, doncs, en ser úniques per cada usuari, la sostracció d' una sola serà significativa per a l' usuari afectat i no per a la resta d' usuaris de la xarxa. Caldrà tan sols canviar les credencials d' aquest usuari o bloquejar-lo per restablir la seguretat en la xarxa, sense afectar en el procés a la resta de clients como passa en les arquitectures de clau única.

4.5 Amenaces i vulnerabilitats

És molt important entendre les amenaces i vulnerabilitats que afecten els xarxes WLAN IEEE 802.11 per a implementar les mesures de seguretat adequades. Algunes vulnerabilitats que es descriuen en aquesta secció son inherents a la norma *Wi-Fi*, mentre que altres son comuns per a les xarxes sense fils WLAN o genèriques.

4.5.1 La pèrdua de la confidencialitat

Donada la pròpia naturalesa d' una xarxa sense fils és més difícil garantir la confidencialitat de les dades en una xarxa d'aquestes que en una cablejada. El fet de disposar d'un mitjà físic com el cable per a transmetre les dades comporta que un possible atacant tingui els mitjans disponibles per a connectar-se a aquell medi, en canvi, en les xarxes sense fils com el medi de propagació és l'aire, tots ens hi podem connectar d' una manera, si més no, més fàcil. Per tant, l'augment de la importància de la confidencialitat en els xarxes sense fils és una constant a tenir més en compte.

Un intrús pot escanejar els senyals de RF capturant les dades que travessen el medi inal·làmbric. La informació confidencial, els identificadors de xarxa, les credencials i les dades de configuració son exemples de dades que poden ser capturades. A més a més, els atacants amb antenes d'alt guany poden capturar les dades de les xarxes sense fils més enllà de l'abast d' una xarxa normal, per tant, la confidencialitat és una mesura de seguretat crítica. L'espionatge a realitzar amb eines d'anàlisi de xarxes inal·làmbriques (conegudes com sniffers) és relativament senzill i no cal ser un expert informàtic ni per accedir a elles ni

per saber-les gestionar. Els rastrejador parteixen com a avantatge de les debilitats que presenta l'algoritme de clau pel *RC4* utilitzat per *WEP*. Amb l' objectiu d'explotar aquestes debilitats, l'*sniffer* monitoritza de forma passiva la xarxa i calcula claus de xifrat després d' escoltar un número variable de paquets. En una xarxa altament saturada, recollir la quantitat de dades necessàries per calcular les claus WEP requereix un parell d' hores, però si el volum de tràfic és baix, pot trigar-se fins a un dia. Per exemple, un punt d'accés que està transmetent 3.000 bytes a 11 Mbps pot desxifrar la clau en aproximadament 10 hores. Un cop l'atacant ha recuperat els texts xifrats, tant la integritat com la confidencialitat de les dades han perdut tot compromís.

Hi ha moltes eines que utilitzen mètodes per a trencar la seguretat de les xarxes *Wi-Fi*. Després que els paquets de xarxa s'hagin capturat, les claus es poden endevinar en pocs segons. Un cop que l'usuari coneix la clau WEP, ja pot llegir qualsevol paquet que circuli per la xarxa. Un altre dels riscos de les xarxes WLAN és la pèrdua de confidencialitat a través de les escoltes simples en el tràfic de *broadcast*. Els concentradors *Ethernet* transmeten en general el tràfic de xarxa a totes les interfícies físiques i a tots els dispositius connectats, el que deixa el tràfic transmès obert a possibles vulnerabilitats o atacants. Els *switchos* permeten reduir aquest risc en front els concentradors o *hubs*, gràcies a la seva capacitat de proporcionar canals dedicats entre els dispositius de comunicació.

4.5.2 La pèrdua de la integritat

La pèrdua de la integració de la informació vol dir comprometre el seu contingut, alterar-lo a menys que sigui modificat per personal autoritzat, fent que sigui enregistrada la modificació. Així es pot comprometre la precisió i confiabilitat de la informació. Els problemes d' integritat de les dades en xarxes sense fils son similars als de les xarxes cablejades. Donat que les organitzacions amb freqüència posen en pràctica les comunicacions sense fils i per cable sense la protecció adequada del xifrat de les dades, la integritat pot ser difícil d'assolir. Per exemple, un atacant pot comprometre la integritat de les dades mitjançant la supressió o modificació de les mateixes en un correu electrònic a través del sistema *Wi-Fi*. Això pot ser perjudicial per a una organització si el correu electrònic és fonamental, com així és avui dia, i si a més a més es distribueix a tota la organització, o inclús, a l'exterior. Donades les característiques de seguretat de l'estàndard *802.11* que no proporcionen integritat dels missatges, altres tipus d'atacs actius poden comprometre la integritat del sistema basant-se en les deficiències específiques de part del mecanisme CRC-32 d' integritat de *WEP*. *CRC* és un codi de detecció d'errors proporcionat pel protocol IP

(*http://es.wikipedia.org/wiki/Comprobaci%C3%B3n_de_redundancia_c%C3%ADclica*).

4.5.3 La pèrdua de la disponibilitat

Una negació de la disponibilitat de WLAN sovint implica alguna forma d'atac de DoS, tals com inundacions. La saturació es produeix quan un senyal de radiofreqüència emesa per un dispositiu inal·làmbric satura altres dispositius, provocant la pèrdua de les comunicacions. Un usuari malintencionat o un dispositiu legítim que opera sense llicència dins un espectre, son causes de pèrdues de disponibilitat de la connexió. Les trames de gestió de la norma 802.11 son un altre punt de denegació de servei contra les xarxes WLAN. Els usuaris poden ser també els causants d' una pèrdua de disponibilitat en voler monopolitzar la capacitat d'una WLAN, descarregant-se arxius de gran tamany i negant a d'altres l' accés a la xarxa.

4.6 Atacs sobre les xarxes *Wi-Fi*

Els atacs que es poden rebre en una xarxa *Wi-Fi* es poden classificar en dos grans grups:

Atacs Passius: que es produeixen quan una persona no autoritzada accedeix a les dades, però no realitza cap modificació de les mateixes. Aquests atacs es caracteritzen per les activitats d'espionatge o vigilància en què l'atacant monitoritza el contingut de les transmissions per a descobrir el contingut de la informació i per les que analitzen el tràfic capturant la informació transmesa i intentant descobrir dades sobre els paràmetres de la comunicació, com l' *SSID*, claus, adreces *MAC*, *IPs*...

Atacs Actius: que es produeixen quan algú no autoritzat modifica o altera el contingut de la informació, o simplement, impedeix la seva utilització. En aquesta categoria existeixen més activitats, entre les que destaquen: la denegació de servei, l'emmascarament (robar la identitat), la retransmissió (*man-in-the-middle*) i l'alteració, basada en modificar missatges legítims afegint o esborrant part del contingut.

4.6.1 Denegació de servei (DoS)

Els atacs de denegació de servei tenen com a objectiu impossibilitar l'accés als serveis i recursos d' una organització durant un període indefinit de temps. En termes generals, aquest tipus d'atacs està dirigit als servidors d' una companyia, per a que no puguin utilitzar-se ni consultar-se. La denegació de servei és una complicació que pot afectar a qualsevol servidor de la companyia o individu connectat a Internet. El seu objectiu no resideix en recuperar o alterar dades, sinó en fer mal a la reputació de les companyies amb presencia a Internet i potencialment impedir el desenvolupament normal de les seves activitats en cas que aquestes es basin en un sistema informàtic. Tècnicament, aquests atacs no son molt complicats, però no per això deixen de ser eficaços contra qualsevol tipus d'equip Windows, Linux o altres sistemes operatius. La majoria d'aquests atacs aprofiten les vulnerabilitats relacionades amb la implementació d' un protocol *TCP/IP* model. A continuació, a la figura 4.7 un atac *DoS* per saturació.

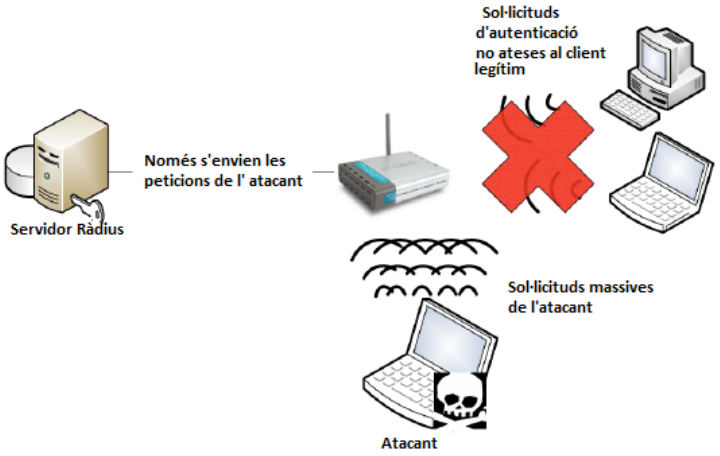

Figura 4.7 Atac DoS mitjançant equips zombie

Generalment, es divideixen en dues classes:

- Denegacions de servei per saturació, que saturen un equip amb sol·licituds per a que no respongui a peticions reals.
- Denegacions de servei per explotació de vulnerabilitats, que aprofiten una vulnerabilitat en el sistema per tornar-lo inestable.

Els atacs per denegació de servei envien paquets o dades de tamanys o formes atípiques que saturen els equips de destí o els tornen inestables i, per tant, impedeixen el funcionament normal dels serveis de xarxa que proporcionen. Quan alguns equips activen una denegació de servei, el procés es coneix com

"sistema distribuït de denegació de servei". Els més coneguts son, per exemple, *Tribal Flood Network, Trinoo, ping of death, smurf, Snork, Teardrop...*

4.6.2 MAC Spoofing

Rep aquest nom, l' atac que consisteix en suplantar l'adreça *MAC* d' un altre equip. Això, en el cas d' una xarxa *Wi-Fi*, permet guanyar l'accés a la xarxa a aquelles màquines que tinguin implementada una autorització de clients basada en les seves adreces de xarxa. És a dir, simplement detectant alguna adreça *MAC* que es trobi associada a un punt d'accés, aquesta podrà ser utilitzada suplantant a la *MAC* original de la targeta de xarxa *Wi-Fi* de l'atacant. Per exemple, un sistema de detecció d' intrusió (vegeu el capítol 5) podrà detectar dos senyals diferents amb la mateixa adreça de *MAC*, evidenciant aquest tipus d'atac (vegeu un article interessant a http://www.blackploit.com/2010/03/suplantar-direccion-ip-y-mac-spoofing.html).

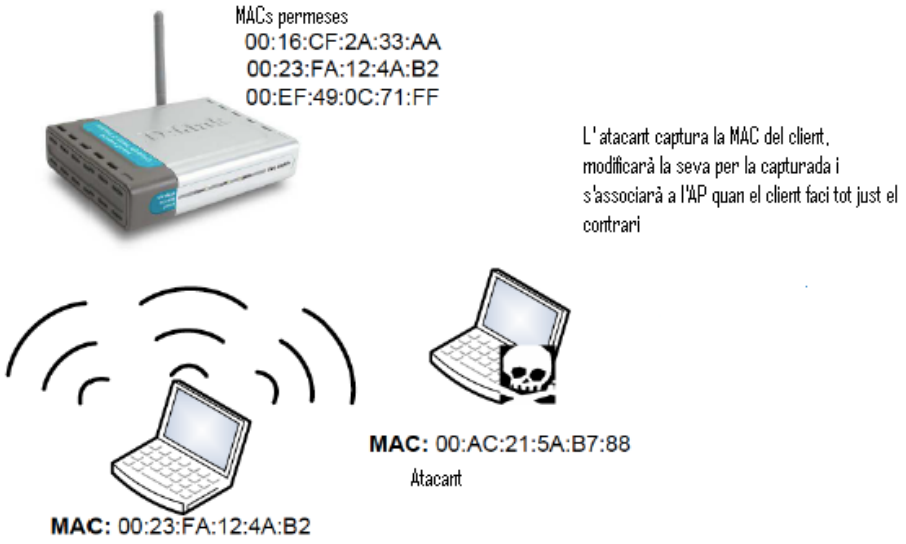

Figura 4.8 Atac de suplantació de MAC

4.6.3 Evil twin/Honeypot

Aquest tipus d'atacs consisteixen en realitzar un *phising* d' un *hot-spot*, és a dir, en inserir un punt d'accés que mostra a l' usuari la mateixa interfície que mostraria un *hot-spot* (punts d'accés a Internet públic que mitjançant un portal permeten l' accés a serveis diversos, com per exemple els existents en els aeroports per accedir a Internet pagant). Com a conseqüència d'això, el client no notarà diferència entre el punt d'accés legal i l' inserit, i procedirà a fer ús d'aquest últim. El negoci per a l' atacant prové de que els *hot-spots* sol·liciten el

client un usuari i una clau per accedir al servei o un pagament mitjançant targeta de crèdit, dades que l' atacant podrà capturar per al posterior ús fraudulent. L' *Evil twin* té un abast més ambiciós, busca aconseguir més informació confidencial. Redirigeix a l' usuari a pàgines web perilloses, on és atacat per *malware*. Hi ha pàgines web on només amb moure el ratolí, descarregarem *spyware*.

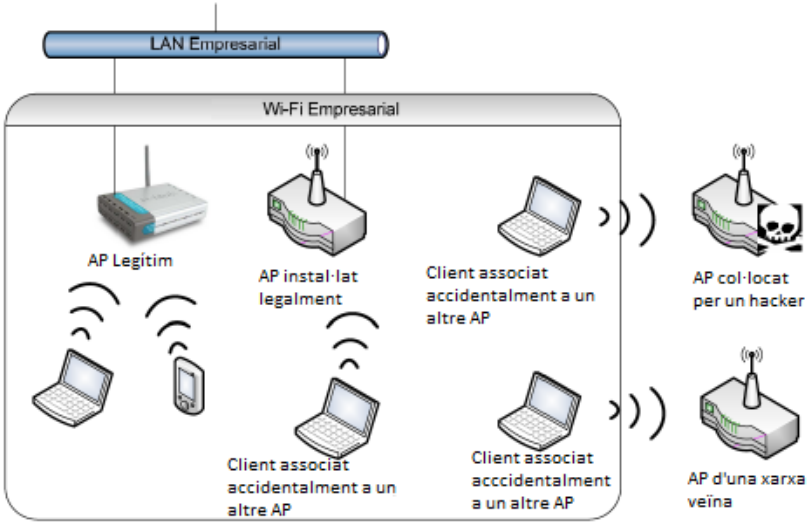

Figura 4.9 Atac Evil twin/honeypot

4.6.4 Man-in-the-middle

Aquest tipus d'atacs és aquell on l'atacant es posiciona entre el client i el servei que ha d' utilitzar. Així en una xarxa *Wi-Fi*, aquest atac consistiria en que el client es connecta al sistema de l'atacant, gràcies a algun engany per part d'aquest, i el sistema de l'atacant al mateix temps reenvia les dades al punt d'accés legal. D'aquesta forma el client no s'adonarà que no està connectat a la xarxa directament, doncs, tot sembla funcionar perfectament, però l'atacant té accés a totes les dades del client, doncs passen pel seu sistema. El major perill d'aquest tipus d'atacs radica en que l' intrús pot variar la informació que envia el client, substituint-la per aquelles dades que per ell siguin més interessants, no adonant-se d'això ni el client, ni la xarxa ni els servidors en cas de no existir sistemes de seguretat com *WIPS*, *IDS*, *IPS*, *NAC*...

Figura 4.10 Atac man-in-the-middle

4.6.5 Wi-Phising

Els *hots-pots*, punts d'accés *Wi-Fi* públics, presenten sovint força debilitats en el camp de la seguretat, ja que els proveïdors no tenen especial atenció en protegir la informació que circula en aquestes xarxes. Per aquest motiu, serà l' usuari qui haurà de procurar-se les seves pròpies mesures de seguretat.

Un dels atacs més freqüents sobre aquest tipus de xarxes és el *Wi-Phising*. Un usuari quan desitja connectar-se a Internet des d' un lloc públic deu, en primer lloc, comprovar els punts d'accés que li ofereixen connexió. Un atacant, utilitzant enginyeria social, pot col·locar un AP amb un *SSID* que transmeti confiança als possibles clients víctima. Un cop un usuari decideixi connectar-se a un AP, col·locat per l'atacant, tota la informació que circuli per la xarxa serà fàcilment compromesa. Molts punts d'accés públics presenten un menú de benvinguda, que pot ser simulat per un *hacker* i totalment creïble per a un usuari que només desitja connectar-se temporalment per consultar el correu electrònic, consultar *Twitter* o simplement connectar-se al correu electrònic.

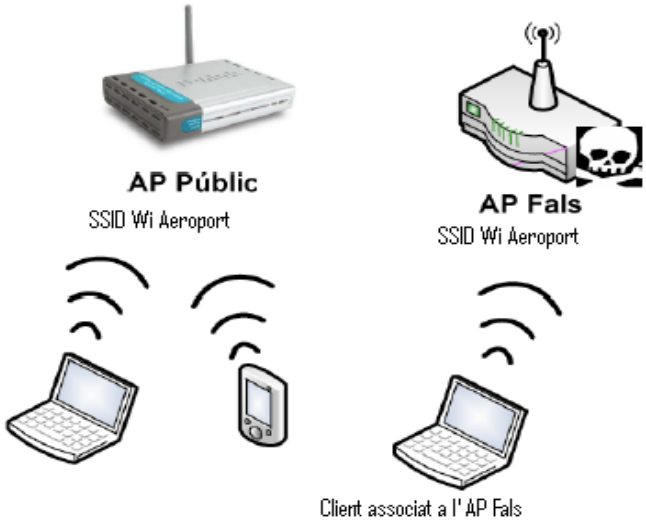

Figura 4.11 Atac Wi-Phising

Abans de permetre la connexió pot ser que l'atacant, mitjançant el menú, intenti obtenir algun tipus d' informació confidencial que sigui facilitada pels usuaris més confiats, com claus d'accés, números d' identitat, comptes bancàries, números de targetes de crèdit...Tot això es refereix a la informació que l'atacant pot robar mentre roman activa la connexió al punt d'accés, però un atacant amb més paciència i que no desitgi bombardejar l'usuari amb sol·licituds d' informació confidencial, pot introduir en la màquina de l'usuari *malware* de tipus virus, *spyware*, troians o *keyloggers*, amb els que podria acabar obtenint la mateixa informació en moments on l'usuari es sentis més confiat.

4.6.6 Segrest de sessió

Aquest tipus d'atac es basa en desautenticar a un usuari que està associat a la xarxa i reemplaçar-lo. El mode d'operació comença detectant i seleccionant la xarxa objectiu i monitoritzant-la per a obtenir informació com l' ESSID, adreces MAC, IP, etcètera. Després es realitza un atac DoS contra el client seleccionat per a ser suplantat, aconseguint així que sigui desautenticat. Amb la informació que havia obtingut, l' atacant procedeix a connectar-se a la xarxa suplantant l' usuari expulsat. El legítim intentarà connectar-se, però l' AP no li ho permetrà, doncs ja existeix un client amb les seves característiques connectat. Evidentment aquest atac es realitzarà quan l' AP utilitzi mecanismes o llistes d' autenticació.

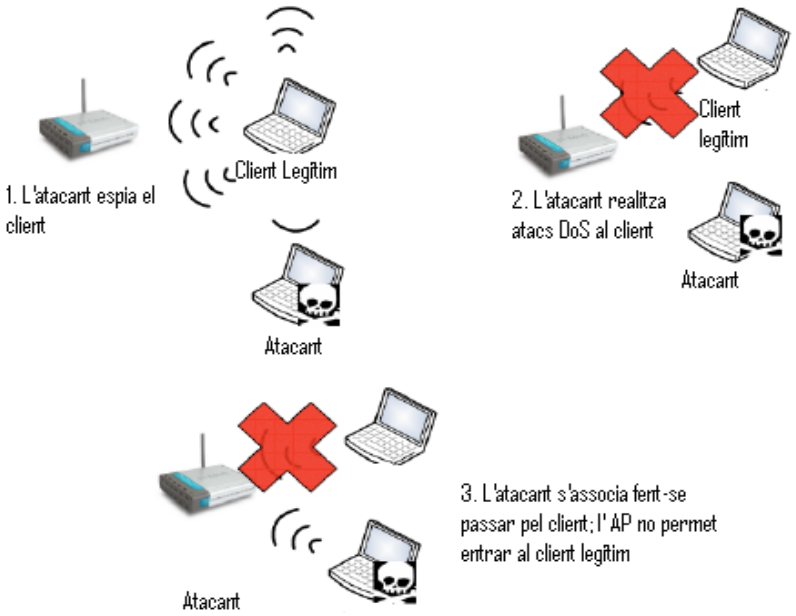

Figura 4.12 Atac de segrest de sessió

Un cop a dins la xarxa, l' atacant ha d'actuar ràpidament per evitar sospites, doncs el client que no s'ha pogut connectar notarà que alguna cosa no rutlla i

pot donar senyals al proveïdor de serveis o inclús a les autoritats. Un cop l'atacant ja ha fet la seva feina, normalment, marxarà per deixar connectar de nou el client legítim. En ser un atac que habitualment dura molt poc, resulta molt complicat per a l'administrador de la xarxa detectar l'atac, sobretot si no té eines específiques com les que poden presentar els *switchos* WLAN (control de ports, d'accés a la xarxa...).

4.6.7 Atacs d' intrusió

Atacs de falsificació d' identitats que ja hem vist, com els de *MAC Spoofing*, *Wi-Phising* o *Man-In-The-Middle* son també atacs d' intrusió, però en aquesta categoria es descriuen atacs, que exploten altre tipus de vulnerabilitats.

Trencar claus WEP: el protocol *WEP* es basa en el xifrat RC4 per a codificar la informació amb la clau de xarxa. Aquesta clau pot estar formada per 64 o 128 bits, sent la part fonamental el vector d'inicialització, 24 bits semi aleatoris, que son transmesos en text pla. Un cop seleccionada la xarxa i el punt d'accés al que es vol realitzar l'atac, s'ha de capturar el tràfic que es transmet sobre aquesta xarxa. Degut a que el tràfic habitualment és molt baix, l'atacant pot fer que aquest augmenti realitzant altres atacs de manera conjunta, provocant desautenticacions dels clients i/o injectant tràfic en la xarxa que provoqui la generació de nous VIs, com la injecció de peticions ARP. Un cop capturat el tràfic suficient comença el procés de "cracking" de la contrasenya utilitzant la captura realitzada, amb el que s'obtindrà la clau WEP.

Trencar claus WPA: aquest tipus d'atac és semblant a l'anterior, en canvi, les diferències entre ambdós protocols fa que la metodologia d'atac sigui lleugerament diferent. Una de les principals diferències a l' hora de realitzar aquest atac és que no importa tant la quantitat de tràfic como passava anteriorment, el que realment importa és capturar un tipus de tràfic concret generat en el moment d' autenticació del client coneguda com a "*handshake*". Per tant, el començament de l'atac serà igual que en el cas anterior, seleccionant la xarxa, capturant tràfic i realitzant simplement un atac de denegació de servei sobre un client , ja que amb només un *handshake* serà possible desxifrar la clau. Addicionalment serà necessari disposar d'un diccionari que compari els seus valors amb aquest paquet. Degut a que la clau serà descoberta només en funció de que existeixi la mateixa entrada del diccionari, l'elecció i la qualitat del mateix és fonamental per a l' èxit de l' atac.

Atac a Cisco EAP – LEAP: la vulnerabilitat sobre el mètode d'autenticació *EAP-LEAP* desenvolupat per *CISCO* i la metodologia per llençar un atac *off-line* foren presentades el 2003.

Tot algorisme basat en claus o contrasenyes pot ser atacat amb la finalitat de descobrir la contrasenya d'accés. En aquest cas es realitza un atac de diccionari, és a dir, utilitzant un llistat de paraules clau. Existeixen eines que automatitzen i faciliten la realització d'atacs de diccionari sobre xarxes *Wi-Fi* protegides amb el mètode d'autentificació *EAP-LEAP*. Com aquest atac pot ser realitzat *off-line*, és possible capturar una quantitat de tràfic determinada i després atacar-la fins a descobrir la contrasenya.

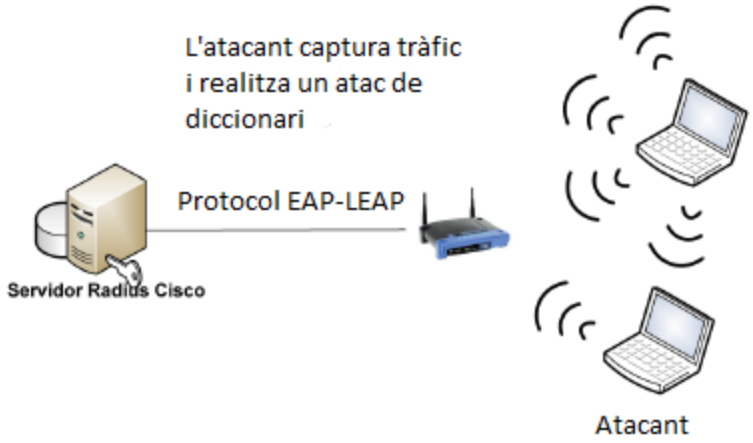

Figura 4.13. Atac EAP-LEAP

5. Solucions de seguretat *Wi-Fi*

5.1 Introducció

En l'apartat anterior hem abordat els principals aspectes inherents a la seguretat en les xarxes *Wi-Fi*: els protocols de seguretat *WEP/WPA/WPA2*, el mecanisme o procés d' autenticació de 802.1x i **les normes preventives d' ús d'aquestes xarxes**, que son un punt de partida per seguir enfortint la seguretat de les nostres xarxes. Partint d' aquestes tres mesures en certa manera "innates" i preventives, en aquest capítol 5, parlarem de mecanismes de seguretat addicionals existents en el mercat i ideals per a considerar-los sempre que despleguem una xarxa *Wi-Fi* en una corporació o companyia. Hem parlat sobre l' ús de **controladors**, entrarem en detall al següent punt, i afegirem les **sondes *WIPS***, **el concepte Network Control Access** (*NAC*) i altres solucions

alternatives com a determinants per fer front als problemes de seguretat de *Wi-Fi.* Val a dir que una manera òptima d'enfortir la seguretat de les xarxes 802.11b consisteix en integrar dins una mateixa *WLAN* sondes *WIPS* i solucions *NAC*: les primeres per evitar infiltracions de desconeguts o saturacions de servei i les segones, per controlar qui accedeix a la nostra xarxa. Fabricants d'aquest tipus de solucions en seguretat *Wi-Fi* son, per exemple: *Enterasys, Juniper, Cisco, McAfee, Symantec, Trendmicro*, entre d'altres i els preus del hardware i el disseny de les solucions son semblants; on tindrem o podem tenir diferències és en l'enginyeria o serveis professionals del proveïdor que pot ajudar-nos a implementar una o altre solució. Per aquest motiu, en el següent capítol, valorarem econòmicament i tècnica la solució *NAC* d' Enterasys, però és extensible a les altres, doncs, els objectius i manera de treballar son gairebé idèntiques.

Respecte a les sondes *WIPS*, detallarem quin és el seu objectiu, quines son les seves característiques i quins fabricants trobem al mercat. Tant *NAC* com WIPS no son solucions excloents l'una de l'altre sinó que es poden integrar en una mateixa *WLAN*.

Amb això, finalitzarà aquest treball que ha donat una visió global de les connexions sense fils actuals, ha particularitzat en les xarxes *Wi-Fi* de l'estàndard 82.11b i ha tractat algunes de les solucions més apropiades per a combatre els riscos, amenaces i vulnerabilitats que presenten les xarxes *Wi-Fi* actualment.

5.2 Controladors

A més a més de les normes bàsiques de protecció de xarxes *Wi-Fi*, l' ús d' **un controlador de punts d' accés,** no només facilita la gestió i manteniment d' una xarxa *Wi-Fi* sinó que pot servir tanmateix per augmentar la seva seguretat. Les possibilitats que proporciona un controlador dependran del fabricant i model, doncs no hi ha un estàndard, essent algunes de les importants, les que segueixen:

Firewall (tallafocs): és habitual que els controladors implementin funcions de firewall, que permetin controlar el tràfic que passa per la xarxa cablejada a la xarxa *Wi-Fi*, en base a adreces d' origen o destí, aplicacions, serveis, etc...El firewall és també un element important en la defensa davant atacs de denegació de servei (*DoS*).

Comunicació per túnel: si es disposa d'aquesta capacitat, el controlador crea un túnel amb cadascun dels punts d' accés. Dins aquest túnel (normalment és un encapsulat IP o SSL) es transmetrà el tràfic dels clients des del punt d' accés al controlador. Això permet que els clients *Wi-Fi*, potencialment insegurs, no tinguin accés a la xarxa directament, sinó que fa que tot el tràfic passi pel controlador que, segons les polítiques assignades en la funcionalitat de firewall que el propi controlador realitza, denegarà o permetrà l'accés a parts de la xarxa o a tota ella. La tunelització del tràfic també proporciona la possibilitat que els punts d' accés estiguin connectats a segments de xarxa diferents, ja que d'aquesta manera el tràfic dels clients sempre accedirà a la xarxa pel mateix punt d'aquesta, aquell al que estigui connectat el controlador. A més a més, si el túnel es realitza amb un protocol segur com SSL, la comunicació entre els punts d' accés i el controlador podrà fer-se a través de xarxes de tercers o inclús Internet, el que permetrà l' extensió de la xarxa sense fils a zones remotes travessant xarxes insegures sense exposar el tràfic propi.

Gestió per usuari: en conjunció amb un servidor d'autentificació, ja sigui intern al controlador o mitjançant un servidor RADIUS extern, serà possible assignar diferents accessos als usuaris en funció de les seves credencials, d' una manera més detallada i complexa que si el procés el dues a terme el punt d'accés. Així doncs, podran assignar-se a diferents xarxes, concedir-los accessos a diferents serveis, etcètera.

Gestió de l' ample de banda: El controlador podrà oferir una funcionalitat a partir de la qual regularà l'ample de banda disponible en funció de l' aplicació o l'usuari que desitgi fer ús d' ella. Així doncs, s'afavorirà el tràfic de veu sobre el de dades, evitant la saturació i bloqueig de la xarxa *Wi-Fi* per aplicacions abusives com descàrregues de fitxers o prioritzar el tràfic en favor d' uns o altres.

Localització espacial: un controlador pot oferir un servei de localització. En tenir control sobre els diferents punts d'accés que gestiona, pot monitoritzar els clients i la potència de recepció de tots aquests per cadascun dels punts d'accés que controla. Si el controlador té coneixement de la situació espaial dels punts d' accés, triangulant la posició respecte els diferents punts d'accés en base a la potència rebuda per aquests, podrà obtenir la ubicació del client. Tot i que aquesta posició pot no ser exacta, sí serà important a l'hora de localitzar equips, no només per a la seva pròpia gestió, sinó per trobar els atacants o intrusos d' una xarxa.

Limitació física en l'abast de la xarxa: tot i que la propagació del senyal de radiofreqüència no es pot acotar de forma efectiva en l'espai, un controlador amb servei de localització, podrà denegar l' accés a la xarxa a aquells equips

que es trobin fora dels límits del que s' ha establert com a zona de cobertura. Cal indicar que amb aquest mètode els clients de fora de la zona de cobertura de la xarxa seguiran rebent el senyal, i per tant podrien intentar altres mètodes d'atac a la xarxa si l' encriptació no és l'adequada, però no podran connectar-se a la mateixa. Aquesta funcionalitat és útil quan es vol donar cobertura *Wi-Fi* a un edifici però es desitja prevenir que els clients presents fora de l'edifici es pugui connectar com a intrusos, per una altra part, difícils de localitzar en estar ubicats en zones sobre les que no es té control físic.

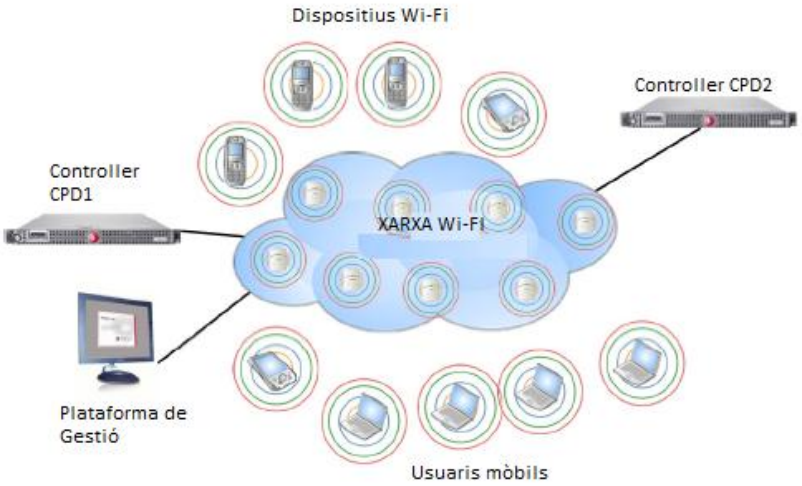

Figura 5.1 Xarxa Wi-Fi amb controladors de punts d'accés

5.3 Sondes WIPS

D'altra banda, una ***sonda WIPS*** (*Wireless Intrusion Prevention System*) és un conjunt d'equips de xarxa, que com el seu nom indica tenen com a objectiu prevenir i detectar intrusions en la xarxa *Wi-Fi*. És un sistema de prevenció d' intrusió sense fils; el seu homòleg en les xarxes cablejades son els sistemes *IDS/IPS*.

Un sistema *WIPS* sempre es composa de tres parts lògiques: els sensors que recolliran les dades de la xarxa, el servidor que recollirà les dades dels diferents sensors, els analitzarà i els relacionarà, i la consola que utilitzarà el personal encarregat de la seguretat de la xarxa per accedir a les dades i visualitzar les alarmes. Aquests tres blocs lògics no sempre estaran separats físicament, doncs és habitual que el servidor implementi un servidor WEB que sigui utilitzat per accedir a les seves dades i configuracions a través d' un navegador. No sempre un sistema *WIPS* és independent, en alguns sistemes aquesta funcionalitat està inclosa en el controlador, que farà les funcions de servidor, i en conjunció amb

els punts d' accés, es faran les funcions dels sensors, podent dur a terme part de les funcionalitats que realitzaria un *WIPS* dedicat.

Figura 5.2 Alguns dispositius WIPS

Un sistema *WIPS* monitoritza l' espectre radioelèctric de la xarxa *Wi-Fi* amb l' objectiu de detectar atacs o vulnerabilitats de diferents tipus, com poden ser:

Punts d'accés infiltrats: com hem vist, un dels atacs més efectius sol ser la infiltració d' un punt d'accés, que pot associar clients de la xarxa, obtenint per tant les seves dades, que es transmetran creient estar connectats a la xarxa legal. També, en cas de connectar-lo a la xarxa cablejada, pot ser un punt d'entrada a la xarxa de qualsevol intrús, que podrà accedir a distància i per tant serà difícil de localitzar.

Els WIPS poden detectar aquests punts d'accés infiltrats, emprant tècniques simples com el comptatge dels punts d' accés que detecta, fins a d'altres més complexes que impliquen relacionar l'adreça MAC de cada punt d' accés amb la potència que d' ells rep. En cas que es rebi informació de la mateixa *MAC* amb una potència diferent, significaria que o bé s' ha canviat de localització el punt d'accés, cosa que pot ser habitual, o que un nou punt d'accés, en una localització diferent, ha intentat suplantar l' equip legal. Un cop detectat l'equip infiltrat, el *WIPS* ho notificaria a l' administrador de la xarxa, i en alguns sistemes permetrà habilitar contramesures que bloquegin el punt d'accés infiltrat, per exemple, suplantant la seva adreça (*MAC spoofing*) o interferint-los.

Punts d' accés mal configurats: pot detectar converses entre els punts d'accés i els clients, sobretot en el moment de l'associació i negociació de l' encriptació a

utilitzar, detectant paràmetres i configuracions errònies. Però, inclús, mitjançant la informació emesa en els paquets de *beacon* pot avisar d' errades en la configuració dels punts d'accés.

Clients mal configurats: un client els accessos del qual siguin denegats de forma repetitiva, serà detectat com un error de configuració del client, o dependent del cas, com l' intent de connexió d' algú, que especialment en els casos en que intenti esbrinar les claus de xarxa mitjançant mètodes de força bruta, provocarà molts intents de connexió denegats per la xarxa.

Connexions no autoritzades: si en un sistema *WIPS* disposem d' una llista de clients autoritzats, podrem detectar la connexió de clients tant permesos com no, si son únicament intents de connexió repetitius.
Xarxes 'ad-hoc': aquestes xarxes poden ser altres fonts de vulnerabilitat: creades involuntàriament per un error de configuració, un troià, etc...poden crear forats de seguretat que tindran conseqüències importants. Els sistemes *WIPS*, mitjançant la monitorització dels canals *Wi-Fi*, podran detectar aquest tipus de xarxes i associacions, podent indicar així mateix l'equip que crea la xarxa i que està originant la vulnerabilitat.

Altres atacs com *MAC spoofing*, *evil twin/honeypot* i *man-in-the-middle*, vistos en el capítol anterior, son també resolts per aquests sistemes d' ondes de detecció d' intrusos inal·làmbrics.

Entre les característiques principals de les sondes *WIPS* destaquen:

- Detecció d' intrusos en temps real, des de qualsevol origen no autoritzat en xarxes 802.11.
- Avaluació de les vulnerabilitats per identificar punts febles de la xarxa com problemes de configuració en dispositius i implementacions de xifrat de baixa seguretat.
- Localització precisa i ràpida de qualsevol dispositiu en la xarxa.
- Aplicació de polítiques amb notificació instantània i resposta basada en les infraccions.
- Resposta ràpida a atacs; els administrador de seguretat poden acabar la connexió sense fils de dispositius no autoritzats, fent-los fora.
- Gestió centralitzada (com hem comentat): interfícies de gestió fàcils d'0 usar i personalitzar per diferents nivells d' usuari.

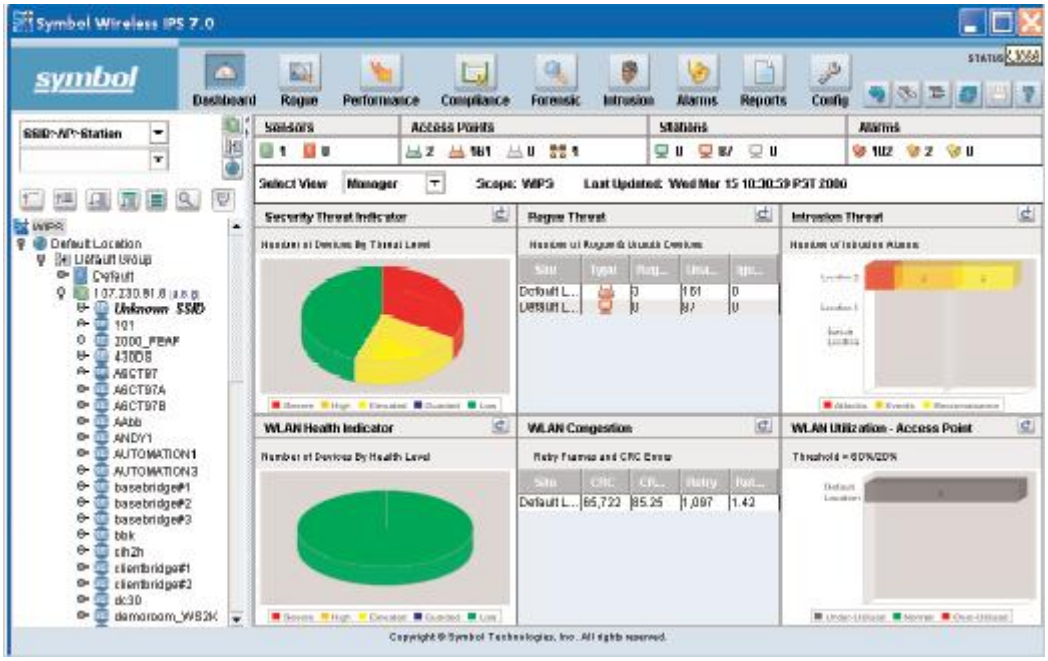

Figura 5.3 Panell de control d' un sistema basat en WIPS

Hi ha molts fabricants d'aquest tipus de sondes: *Motorola*, *Cisco*, *Enterasys*, *Aruba*, *AirTight*, etcètera.

5.4 Network Access Control

Com hem comentat en la introducció d'aquest capítol, el control d'accés a la xarxa, de l'anglès *Network Access Control*, i, en endavant, *NAC*, és una capa de seguretat addicional ideal per a les xarxes *LAN*, ja siguin *Ethernet* o *WLAN*. *NAC* és un conjunt de solucions encarregades d'assegurar i controlar qui accedeix a la nostra xarxa, en el nostre cas, sense fils.

Les solucions de *NAC* permeten únicament als dispositius autoritzats accedir i operar en una xarxa cablejada o sense fils. Si és aplicat de forma correcte, *NAC* pot millorar el perfil de seguretat d' una xarxa i reduir els riscos als que s'enfronten les empreses. Els distints punts de vista de *NAC* han creat un important i controvertit debat en tota la industria de seguretat *IT* des dels inicis del seu naixement. Els beneficis son clars, tot i que encara, segons el nostre parer, no s' ha estès globalment. Son solucions en general, cares, com veurem més endavant, i poden requerir, sobretot als seus inicis, d'una re-arquitectura de la xarxa important i un anàlisi llarg i costós en el temps. Actualment, han madurat força a nivell d'infraestructura, si bé, com dèiem, son encara de cost elevat.

Qualsevol solució *NAC* basada en agent requereix un projecte de descobriment de la xarxa abans del desplegament (monitorització i identificació dels equips que es connecten a la mateixa) per a obtenir l' inventari global de tots els dispositius que fins ara es connecten i tenen permís per a connectar-se a la nostra xarxa. Després vindrà el moment de definir un protocol d'actuació quan un nou equip es punxi a la xarxa acceptant-lo si compleix una sèrie de requisits o expulsant-lo si no és així. Normalment, s'estableixen patrons de descobriment lents, doncs, a la xarxa poden estar connectats dispositius de tot tipus: telèfons IP de marques i models diferents, equips portàtils de marques i models diferents que presenten diferents característiques físiques, vídeo càmeres de control de seguretat amb altres característiques, impressores de marques i models diferents, detectors digitals d' empremtes, màquines virtuals, equips d'alimentació ininterrompuda, equips PC d'altres marques i altres models, etcètera, etcètera. De manera, que en una primera fase d' identificació, necessitarem bones dosis de paciència i moltes hores d' esforç. Per què? Perquè pot succeir, per exemple, que *NAC* no detecti o presenti problemes per a detectar determinats dispositius perquè estan obsolets, perquè els desconeix, perquè no sabem com definir-los, etc. En aquest cas, els afegirem de forma manual si és que han de formar part del nostre inventari i son equips legals de la nostra xarxa. Així doncs, *NAC*, en un primer moment i molt probablement, requerirà importants intervencions humanes. Un cop descobert tot allò que està punxat a la nostra xarxa, i identificat el nostre inventari, haurem de definir un protocol de detecció automàtica per a saber què fer quan un dispositiu es punxi voluntàriament o involuntària a la nostra xarxa. Si compleix amb uns requisits en concret, donarem accés, en cas contrari, no. Aquests requisits poden ser: si té una adreça *MAC* que comença per *XXXX* fent referència al nostre fabricant de telèfons IP, per exemple, si un equip amb un nom concret està definit al nostre directori i existeix, si aquell equip té instal·lat un certificat de seguretat concret, etcètera. Malgrat aquestes costoses tasques d'anàlisi, podem aplicar una solució *NAC* completa i en temps real, doncs, son cada vegada més les grans corporacions que aposten per enfortir la seva seguretat amb solucions com aquesta. Es pot assegurar que tots els dispositius connectats a la xarxa son autoritzats durant to el cicle d' ús de la mateixa.

5.4.1 Visibilitat – El punt de partida per al desplegament de NAC

La visibilitat i el descobriment d'un dispositiu en temps real, no durant la fase prèvia de monitorització del parc, sinó, en temps real, son la base per al procés

NAC, elimina un dels punts principals d' atac i permet la cobertura de NAC per a tota la infraestructura de la xarxa. Si una solució NAC no pot identificar tots els dispositius connectats a la xarxa en temps real, és probable que la nostra seguretat en la nostra xarxa es vegi decrementada.

5.4.2 Auditoria i compliment

Els perfils dels dispositius proporcionen informació contextual sobre cada dispositiu de xarxa, incloent informació d' usuari i funcionament del hardware i el software. Basat en aquesta amplia auditoria de la informació, un administrador d' IT pot determinar els dispositius que estan autoritzats a accedir a la xarxa segons la política de l' organització. Paral·lelament, aquesta auditoria de la informació permet als administradors identificar els dispositius no autoritzats abans de l'activació dels processos NAC.

5.4.3 Garantia d' una completa cobertura de xarxa

Una solució NAC ha d'operar en temps real. Cada dispositiu ha de ser detectat i inclòs en el procés de NAC. Sense la detecció en temps real, un dispositiu i/o un usuari poden actuar de manera maliciosa o fraudulenta en la xarxa.

El mecanisme utilitzat de quarantena no ha de dependre de la infraestructura IT subjacent. Questions de política interna entre els diferents departaments d' una gran empresa evitaran que una solució NAC que depèn de la infraestructura d' IT s'escali a través de tota la xarxa. A més a més, qualsevol canvi de configuració en la xarxa d' un banc o una empresa de serveis financers mai no serà autoritzat. L'experiència d' usuari per als dispositius compatibles i gestionats ha de ser el més transparent possible. Un usuari de dispositius compatibles i gestionats deu passar pel procés de *NAC* sense saber ni tant sols que el dispositiu va ser avaluat per la solució *NAC*. Els desplegament de la solució ha d' incloure tots els possibles segments de la nostra xarxa per a que el resultat sigui òptim.

5.4.4 Arquitectura d' una xarxa amb NAC

Sense particularitzar en cap marca en concret, podem dir que una solució *NAC* presenta fonamentalment 4 components:

NAC Gateway: actua com a Proxy ràdius a la xarxa i realitza tasques d' avaluació; en funció dels seus resultats, enviarà les corresponents ordres als *switchos* de la xarxa per a realitzar canvis de polítiques d' accés als usuaris.

Quan s' utilitzen a les xarxes únicament NAC Gateways, diem que la implementació és en mode *Out-of-band*.

NAC Controller: s' utilitzen quan els *switchos* d'accés de la xarxa no suporten autenticació ni RFC-3580 (RADIUS, *Remote Authentication Dial In User Service*). Permeten la possibilitat de "*multiautenticar*" un número determinat d' usuaris o dispositius del nivell d'accés en un port físic, cosa que permet aplicar polítiques de xarxa de la mateixa manera que utilitzant *switchos* d' accés específics. Quan s'utilitzen controladors NAC a la xarxa, diem que la implementació és en mode *in-band*.

Agent NAC: Es tracta d' una aplicació que s' instal·la en els equips dels usuaris i que consulta l'estat del sistema accedint a les claus de registre de l'equip, a l'estat de l'aplicació i als processos en execució. El NAC *gateway* realitza consultes periòdiques a l'agent per demanar-li l'estat de configuració i seguretat del sistema.

NAC Manager: és l'aplicació de gestió per configurar, monitoritzar i administrar la solució NAC.

Les solucions NAC, en general, admeten diferents escenaris, fonamentalment en funció de dos requeriments que es demanen als *switchos* d'accés de la xarxa; autentificació i l'estàndard RFC3580. Així doncs, una arquitectura de xarxa amb NAC pot ser la que mostra la següent figura.

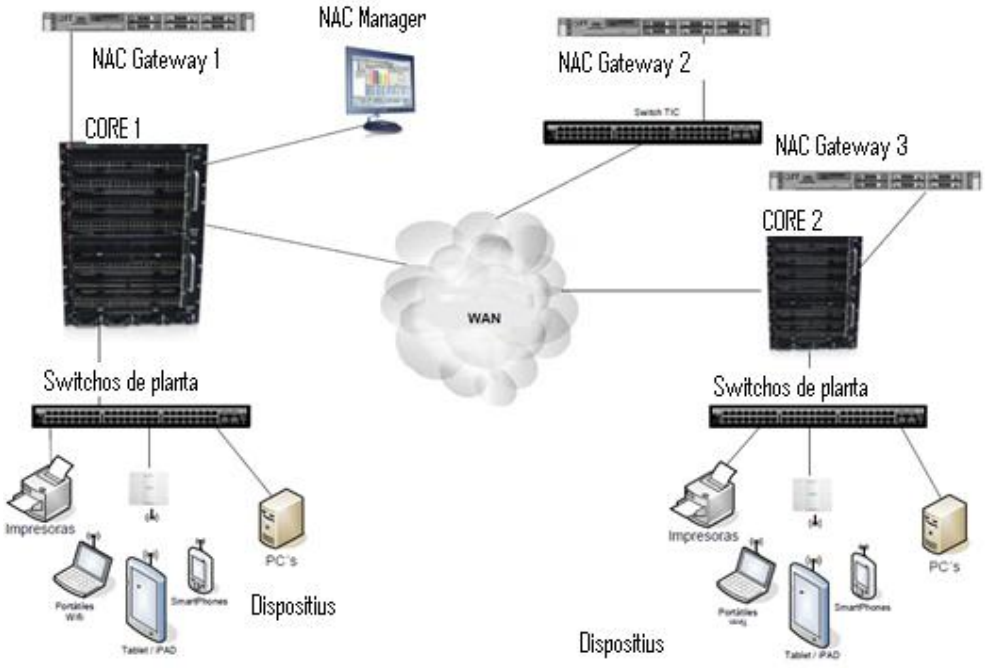

Figura 5.4 Arquitectura de dues seus per una xarxa Wi-Fi amb seguretat NAC

6. Cas pràctic

6.1 Introducció

En els capítols anteriors hem parlat abastament de les principals mesures que cal prendre per part de l' usuari per a protegir les seves dades (normes bàsiques), dels mecanismes de seguretat que proporciona *Wi-Fi* i d' algunes solucions que enforteixen la seguretat de les nostres xarxes sense fils. Però, com podem saber a què estem sotmesos? Com poden comprometre la seguretat de la nostra xarxa *Wi-Fi*? Doncs bé, existeixen al mercat infinitat d' eines per a detectar i analitzar xarxes *Wi-Fi*, tant d' us comercial com gratuït, i que es poden utilitzar en una gran varietat de plataformes Windows, iOS, Linux, Android...el que posa de manifest l'interès en la seguretat en aquest tipus de xarxes. En l' annex d'aquest treball veureu alguns exemples d'atacs.

Es poden classificar en diferents categories. Per exemple, n'hi ha d' especialitzades en trobar punts d'accés i analitzar els paquets *Wi-Fi* capturats com els analitzadors de tràfic; si el que es vol és monitoritzar el tràfic escollirem una sonda *WIPS*, etcètera. Algunes d'elles son, per categories: ***1. Capturadors de paquets Wi-Fi***: Aircrack-ng Suite, ettercap, libcap, CACE AAirPcap, Prism2Dump, tcpdump; ***2. Analitzadors de tràfic Wi-Fi***: AirMagnet *Wi-Fi* Analyzer, CACE *Wi-Fi* Pilot, BVS YellowJacket BAG, Kismet, NetScout Sniffer Portable, Ufasoft Snif, Fluke Networks OtiView, WidPackets OmniPeeks, WireShark, MetaGeek Eye, Cambridge vxSniffer, Javvin Network Packet Analyzer, Motorola AirDefense Mobile; ***3. Analitzadors de tràfic i QoS de VoWI-FI:*** AirMagnet VoFi Analyzer, VeriWave VoIP QoS Service Assurance Test, WildPackets OmniPeek; ***4. Sistemes de prevenció i detecció d' intrusos***: AirMagnet Enterprise, AirMobile Server, AirPatrol WLS, Aruba Networks, Enterasys HiPath Wireless Mgt Suite, Cisco Adaptative WIPS, Motorola AirDefense Enterprise; ***5. Eines de planificació predictiva Wi-Fi:*** Aerohive Online *Wi-Fi* Planner, Motorola LAN PLAnner, Psiber RF3D, Ruckus Wireless, AirMagnet Planner; ***6. Eines de mapeig de cobertura***: BVS Hive, Ekahau Wireless Site Survey Standard, Helium Networks Wireless Recon, Meraki Cloud *Wi-Fi* Mapper, TamoGraph Site Survey, VeriWave WaveDeploy; ***7. Escàners de vulenrabilitat i eines d'avaluació***: Airpwn, AP Hopper, Autoscan, Nessus, Nmpa-Zenmap, WiCrwal, *Wi-Fi*Denum, *Wi-Fi*Zioo, *Wi-Fi* Scanner, Security Auditor's Research Assitant, MDK3, Karma, Motorola AirDefense Wireless VA Module....

6.2 Auditoria de Seguretat d' una xarxa *Wi-Fi*

6.2.1 Objectiu

Un client ens demana una auditoria de seguretat dels seus llocs de treball mòbils per a determinar en quin punt es troba compromesa la seguretat de les seves dades, doncs recentment ha desplegat *Wi-Fi* a les seves oficines.

Realitzarem les proves de forma presencial, a casa el client, sense tenir cap coneixement del seu entorn o infraestructura de xarxa existent. Aquesta metodologia, anomenada Caixa Negra, permet avaluar el nivell de risc del sistema davant atacs dirigits contra la organització, per part d' usuaris o agents no associats amb el nostre client. Es realitzaran diverses proves tècniques amb l'objectiu d'avaluar el nivell de seguretat de la infraestructura tecnològica que suporta la xarxa *Wi-Fi*, així com la identificació de debilitats estructurals en la maqueta de lloc de treball portàtil, des de la que es realitzen les connexions a la xarxa interna i a la infraestructura de la organització. Totes les proves es realitzaran sense cap informació d'usuaris i claus d'accés. La verificació de l'entorn es realitza en base a metodologies de seguretat específiques ja siguin definides per algunes entitats globals o bé fent us de metodologies lliures i reconegudes a nivell internacional com, per exemple, OSSTMM (*Open Source Security Testing Methodology*) i OWASP *(Open Web Application Security Project)*.

6.2.2 Abast

Dins el marc de treball creat en la col·laboració tècnica entre el client i nosaltres, es procedirà a realitzar un anàlisi de seguretat exhaustiu de l' entorn de lloc de treball mòbil, incloent-hi en l'abast els següents elements relacionats directament amb l'accés a la informació des del terminal d' usuari: terminal d'usuari portàtil, xarxa sense fils oberta als col·laboradors de la firma i el portal web de mobilitat, des del que els usuaris, estiguin on estiguin es poden connectar. S'examinaran aquells elements tecnològics involucrats en l'accés de la informació, a fi i efecte de verificar els controls de seguretat existents en el lloc de treball, identificant possibles errors de seguretat que puguin afectar a la disponibilitat, integritat i confidencialitat de la informació en tots els seus estats (transmissió, tractament o emmagatzematge). L' objectiu d'aquesta revisió és permetre identificar aquelles deficiències tecnològiques que poden suposar un risc de seguretat per a la xarxa del nostre client o puguin permetre la fuita d'informació (això, concretament ho tracten les solucions de *Data Loss-Leak Prevention* i és tot un món!), definint contramesures per a enfortir les defenses actuals i millorar els nivells de maduresa en els processos de resposta en front

d' incidents de seguretat. Per fer un bon anàlisi i obtenir conclusions, utilitzarem algunes de les eines anomenades anteriorment i de les que veurem algunes mostres en l' annex d'aquest treball; a més a més, emprarem un usuari anònim, sense necessitar cap credencial concreta del client.

Les tasques d'anàlisi les resumirem en tres fases perfectament diferenciades: **anàlisi de la viabilitat** on s' identifiquen els actius i tots aquells mètodes o passarel·les que es puguin utilitzar per accedir als recursos interns de l' organització; **validació a nivell de seguretat** que és la recerca de deficiències en els controls de seguretat implementats que puguin ser vulnerats per fer-se amb el control de la informació sensible o bé afectar la disponibilitat i/o integritat de les dades allotjades a l'organització; ***identificació de contramesures*** que proposa les mesures correctives per arreglar les deficiències detectades.

Després d' un numero concret de jornades fent l'estudi, determinem les següents conclusions.

6.2.3 Conclusions

Hem suposat, dins aquest treball, unes conclusions amb l' objectiu de recomanar el nostre client la implementació d'una solució robusta d seguretat com és NAC. Òbviament, es poden concloure més mesures, que van des de les normes bàsiques d'ús fins a l' ús de sondes WIPS, túnels VPN (IPSEC-SSL), protecció amb contrasenya de BIOS, etcètera.

Després de l'anàlisi de les evidencies obtingudes de les proves tècniques de seguretat i en base a la cripticitat de les vulnerabilitats detectades, podem exposar un indicador de risc dels diferents entorns analitzats, d'acord, per exemple, amb el sistema d' avaluació de la taula següent.

Entorn	***Nivell de risc***	***Impacte***
Xarxa sense fils	BAIX	Tot i que pot existir el risc que robin informació de l'empresa per part d'altres usuaris, per a realitzar aquest atac cal una compte d'usuari vàlida.
Portàtil	MIG	S' han identificat riscos derivats de la configuració del lloc de treball; alguns possibles atacs son la presa de credencials i l' accés extern a l' organització.

Portal de mobilitat	MÍNIM	No s' identifiquen debilitats en el portal, pel que la seguretat de la passarel·la depèn de la política d' usuaris i contrasenyes de l' organització.

Figura 6.1 Anàlisi de resultats d'auditoria

De forma resumida, i d'acord amb la taula 6.1, les principals debilitats identificades en el transcurs d' aquesta auditoria son les següents:

► ***Protecció d' arranc:*** cal protegir l' arranc dels equips portàtils, doncs amb un dispositiu *USB* o un disc dur extern podrien arribar a accedir a tota la informació, inclús, contrasenyes xifrades.

► ***Xifrat de contrasenyes locals:*** la configuració actual dels equips del client no protegeix l' algoritme criptogràfic utilitzat per guardar la clau de l'administrador local dels equips.

► ***Catxé de credencials:*** el sistema permet emmagatzemar les claus de domini emprades pels usuaris pel que es podrà capturar claus xifrades d' usuaris de domini.

► ***Polítiques de seguretat insuficients:*** la parametrització de seguretat de l' equip portàtil ha de ser suficientment robusta i pel que es veu a les directrius i polítiques de seguretat de l'empresa, no ho és.

► ***Debilitats de la xarxa sense fils:*** no s'apliquen gran part de les normes bàsiques d' ús d' una xarxa sense fils; com poden ser fortalesa i complexitat en la contrasenya d'usuari, canviar les configuracions per defecte dels punts d'accés i canviar l' SSID actual per un no tan intuïtiu (si pot ser, amagar-lo).

► ***Xifrat de disc:*** no s' ha detectat la presència de cap eina de xifrat de la informació, que limiti el risc de fuites d'informació davant el robatori de l'equip. Eines com *Bitlocker* de Microsoft podrien ser la solució.

6.2.4 Principals accions recomanades

Associat a les debilitats observades i descrites anteriorment, suggerim les següents línies d'actuació que el nostre client ha de dur a terme per a minimitzar els riscos identificats durant el desenvolupament d'aquest anàlisi:

► ***Protecció d' arranc***: establir una clau d'accés a la BIOS i restringir l' arranc del sistema des de dispositius externs.

► ***Xifrat de disc:*** desplegar una solució de xifrat de disc, com *Bitlocker* de Microsoft.

► ***Polítiques de seguretat:*** definir una guia adequada de polítiques de seguretat per a l`ús dels equips portàtils i dur-la a terme com a línia base o codi de conducta telemàtica.

► ***Control d'accés a la xarxa:*** donada la quantitat de dispositius connectats a la xarxa (equips portàtils, desktops, equips virtuals, impressores, telèfons IP, detectors d'empremtes...) és convenient desplegar una solució NAC per controlar degudament qui accedeix a la xarxa del client i qui no.

6.3 Proposta Network Control Access (NAC)

A continuació, quantificarem una solució *NAC* actual per a que ens fem una idea de què i quant estem parlant, en temps i en diners. Proporcionarem al nostre client els mecanismes adients d' accés segur a la xarxa i qualitat de servei orientats al client, de forma que sigui possible establir polítiques d'accés a la xarxa als diferents usuaris i dispositius en un mateix port de xarxa en funció de la identificació prèvia de l'usuari i el dispositiu.

Aquesta proposta es divideix en dos blocs. En primer lloc, establirem un pla de desplegament i implantació de la solució *NAC* d' *Enterasys*, partint de la situació que hem conclòs en el punt anterior. I, en segon lloc, farem una aproximació econòmica de què suposa una solució d'aquest tipus. Hem seleccionat *Enterasys*, d' igual forma que podríem haver escollit altres com *McAfee, Cisco, Juniper o Sophos*. Segons els analistes *Forrester* y *Gartner*, *Enterasys* no és la millor solució (*Cisco* i *Juniper* estan per davant), però està ben situada en els seus quadrants màgics i per tant, apostem per ella. Veiem la figura 6.2 on es posicionen totes elles:

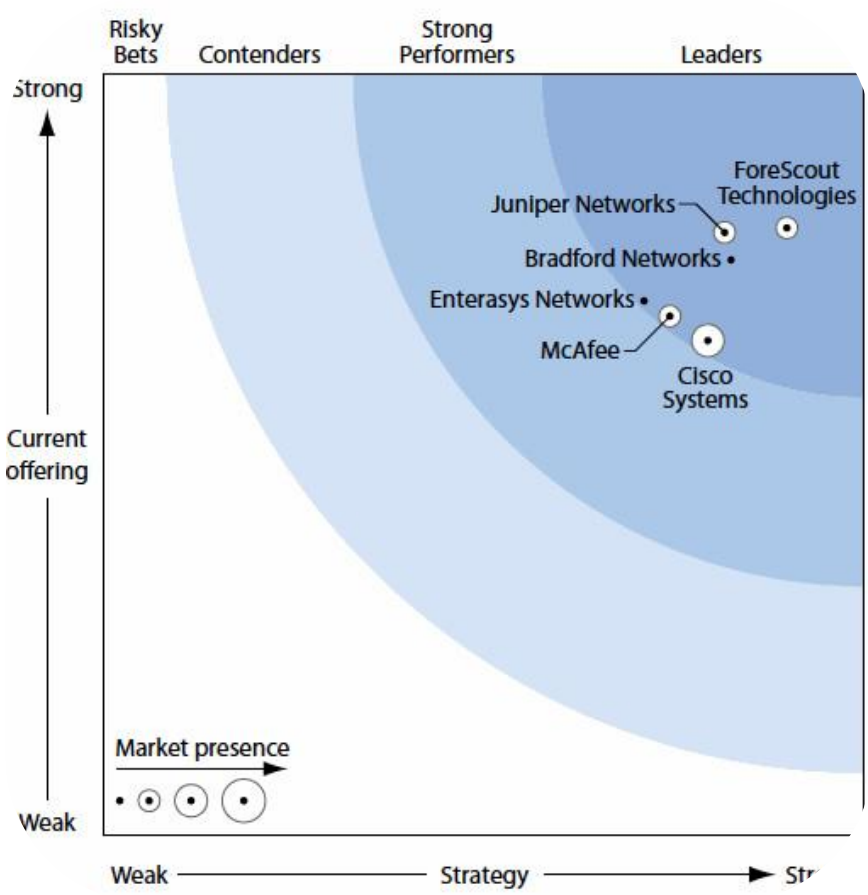

Figura 6.2 Quadrant Magic Gartner NAC Solutions

Els objectius generals d'una proposta com aquesta han de ser:

Control de tràfic en tots i cadascun dels punts de la xarxa (LAN i WLAN): Control d'accés dels usuaris als serveis i recursos de xarxa, prèvia autentificació des de qualsevol lloc. Eliminació de virus i tràfic no desitjats.
Mobilitat total d'usuaris i dispositius: supressió de tasques d'operació assignant dinàmicament els entorns de connectivitat.
Traçabilitat: Coneixement en temps real de la ubicació física dels usuaris, manteniment històric de les seves activitats.
Xarxa orientada a serveis: operativa segura de nous serveis sobre la xarxa (telefonia IP, vídeo, virtualització, etcètera).

6.3.1 Solució NAC d' Enterasys

Enterasys NAC neix com a concepte per a protegir la xarxa en l' accés. Integrat en un conjunt de fabricants que formen el *TNG* ("*Trusted Network Group*") i al qual pertanyen fabricants tan importants com *Microsoft*, *Enterasys* forma part d' un marc d' interoperabilitat de diferents fabricants amb el propi sistema operatiu

simplificant el desplegament i assegurant el correcte funcionament de tot el conjunt del sistema. *Enterasys NAC* es caracteritza per haver desenvolupat un producte que és independent del fabricant de xarxa que tinguem, únicament haurem de preocupar-nos que aquest fabricant compleixi amb els estàndards.

Aquesta solució s' implementa sobre una plataforma que permet l' autenticació, autorització i auditoria de fluxos de tràfic individuals, permetent un control granular d' usuaris, dispositius i aplicacions. Per tant, va molt més enllà que una solució Ràdius tradicional, que "tan sols" valida i autentica usuaris; amb *NAC* validem tots els dispositius IP que connectem, els validem i controlem les seves peticions. La solució NAC, per sobre d' una solució Ràdius convencional, proveeix d' una major intel·ligència el sistema de control d' accés a la xarxa basat en polítiques, utilitzant dos principis fonamentals:

AUTENTIFICACIÓ: aquesta fase garanteix que només usuaris o dispositius amb una identitat vàlida puguin accedir a la xarxa.

AVALUACIÓ: només aquells dispositius que compleixin amb els requeriments mínims de seguretat establerts per la organització, per tant, per nosaltres, podran accedir a la xarxa. Aquests requeriments poden ser, per exemple: l' antivirus corporatiu existent i actualitzat; aplicacions instal·lades i en execució (que estiguin permeses); nivells d'actualització del sistema operatiu (partxes)...

6.3.2 Implementació de la solució NAC a la xarxa sense fils

Per a la xarxa cablejada usarem autenticació 802.1x i/o adreces MAC per a autentificar els dispositius Ethernet com impressores, telèfons IP, equips *desktop* i altres dispositius susceptibles de connectar-se a la xarxa emprant cablejat Ethernet. Per que fa als dispositius mòbils, usarem principalment, certificats digitals per autentificar-se. Detallem-ho a continuació.

La infraestructura *Wi-Fi* és la que concentrarà la majoria dels accessos dels usuaris amb diferents dispositius mòbils, al ser el més favorable per a solucions *BYOD* (*Bring Your Own Device*). Aquest fet facilitarà que si el nostre client compta amb equips corporatius com tauletes (*tablets*) o dispositius que son propietat de l'usuari final, podrem incloure'ls en el nostre control quan accedeixin amb ells a l'entorn corporatiu. A l' *SSID* corporatiu, es desitja que només es puguin connectar equips corporatius usats per usuaris corporatius, és a dir, tant l'equip o dispositiu que es connecta com l'usuari han de ser coneguts i autoritzats al mateix temps per a poder entrar a la xarxa *Wi-Fi* del client.

En el disseny de *NAC* serà necessari incloure controladors *Wi-Fi*, explicats en l'apartat 5.2 d'aquest treball, que en conjunció amb el servidor d' autentificació Ràdius facilitaran la gestió dels usuaris i dispositius que es vulguin connectar a la xarxa. Farem que el servidor d'autenticació primari sigui el *NAC Gateway* i secundari el servidor *Ràdius* de la companyia (un controlador de domini, DC, per exemple, amb aquella funció o rol). El *NAC Gateway* realitzarà dues accions: la primera, passar al servidor *Ràdius* la petició de validació de forma transparent; la segona, serà avaluar el dispositiu que pretén connectar-se a través de la xarxa sense fils, ja sigui amb un agent instal·lat o sense ell, per a verificar efectivament, si el dispositiu compleix amb els requeriments mínims de seguretat establerts pel client. El resultat d' aquesta avaluació condicionarà l'accés del dispositiu: si passa, el dispositiu accedirà a la xarxa amb la política de seguretat establerta per l'usuari i si no passa, pot ser retingut en una *VLAN* de quarantena establerta pel controlador *Wi-Fi* per a que sigui tractat a part.

Donat que el client pot tenir un gran numero de dispositius a connectar-se, s'establirà una distribució de grups en base al mètode d'autenticació proposat:

Portàtils: es connectaran utilitzant un certificat digital d' igual forma que fan contra la xarxa cablejada. L' usuari serà validat pel nom d'usuari del domini Windows (per exemple).

Tablets: emprarem un certificat digital instal·lat utilitzant el mètode EAP-TLS. Els tablets sense aquest certificat digital no seran autoritzats.

Smartphones: s' utilitzarà un certificat digital instal·lat en l' *smartphone*. D' igual manera que amb els tablets, els smartphones sense aquest certificat digital no seran autoritzats a la xarxa.
La distribució dels certificats digitals als dispositius mòbils així com la configuració de les diferents opcions EAP en cada cas, es pot realitzar mitjançant sistemes de gestió d'equips, com *System Center Configuration Manager* de Microsoft o mitjançant el software d' autoconfiguració EAP i de certificats ClouPath que poden integrar-se amb la plataforma NAC utilitzada.

Addicionalment, a tots els dispositius que es connectin a la xarxa *Wi-Fi*, és possible configurar un perfil de dispositiu. El perfil del dispositiu pot incloure els resultats de l'escaneig del software del dispositiu: un *DHCP fingerprint*, una adreça MAC, el sistema operatiu, usuari i localització física entre d' altres, permetent que si qualsevol d'aquests valors canvia, puguem denegar l'accés al dispositiu.

Cada *NAC Gateway* podrà suportar un número concret de connexions en funció del número de dispositius que disposi el nostre client i el número de controladors que vulguem posar a la xarxa. Si volem alta disponibilitat, en necessitarem més per a que la càrrega sigui suportada en cas de desastre o caiguda d'algun dels *gateways*. Per exemple, podem oferir 3 *NAC Gateways* cadascun dels quals suporta 3.000 connexions concurrents, de manera que suportarem en total prop de 9.000 dispositius alhora.

Figura 6.3 Enterasys NAC-A-20 (3000)

En cas de caiguda d' un equip, la solució arribaria a suportar 6.000 equips, suficient per a garantir el 100% del parc (si té prop de 2.000 dispositius, per exemple). La configuració en redundància estableix un repartiment de les connexions dels usuaris de xarxa, de forma que cada switch Ethernet o controlador *Wi-Fi* disposarà d' un NAC primari i un altre secundari configurat, realitzant un repartiment de la càrrega de tràfic d'autentificació de forma homogènia. El principal avantatge que aporta aquesta configuració és poder disposar de diferents *NAC Gateways* repartits geogràficament, és a dir, no és necessari que estiguin els tres equips al mateix CPD.

6.3.3 Valoració Econòmica

Informació obtinguda de diferents web que ofereixen preus per aquests dispositius:*www.preciomania.com*;*www.costcentral.com*;*www.pcsuperstore.com, www.tpoinformatica.com...*

I les webs d' *Enterasys*: *www.enterasys.com/company/literature/nac-ds.pdf*

Descripció equipament NAC Enterasys	Quantitat	Venda unitat (€)	Total (€)
NAC Gateway NAC-A-20	3	13.000,00 €	39.000,00 €
NAC assesment, agent and Network based for NAC-A-20	3	5.000,00 €	15.000,00 €
Extensions de garantia i reposició d'equips NBD	3	2.500,00 €	7.500,00 €
Serveis d'enginyeria	1	20.000,00 €	20.000,00 €
TOTAL	-	40.500,00 €	**81.500,00 €**

Figura 6.4 Valoració econòmica de la solució NAC d' Enterasys

Altres marques com *Cisco* o *Juniper Networks* tenen uns preus semblants i les solucions son pràcticament idèntiques (excepte en els serveis professionals, és

clar). Per tant, *NAC* és una alternativa viable per a enfortir la seguretat de les nostres xarxes sense fils, tot i que el seu cost, òbviament, és elevat.

7. Annex

7.1 Introducció

Normalment, qui intenta connectar-se a xarxes protegides esgota tots els recursos possibles, que poden ser les següents webs entre d'altres:

Quewifi: http://www.quewifi.es/, localitza accessos *Wi-Fi* arreu del món.
FonMaps: http://www.fon.com/es/, fent-te membre i adquirint un punt d'accés de *FonMaps* podràs compartir la teva *Wi-Fi* amb la resta d'usuaris i accedir a les seves xarxes allà on et trobis i hi hagi disponibilitat.
WeFi: http://wefi.softonic.com/, és un rastrejador *Wi-Fi* que ajuda a trobar i avaluar xarxes *Wi-Fi*. Altre semblants son: *OutSSIDer*, *Boingo*...
HotSpotr: http://hotspotr.com/wifi, mostra on hi ha *hotspots* (punts d'accés) gratuïts arreu del món.
JiWire: http://v4.jiwire.com/search-hotspot-locations.htm localitza xarxes Wi-Fi's de pagament i gratuïtes.

*Figura 7.1 Resultat búsqueda **JiWire** a Barcelona*

Quan s'escanegen les xarxes Wi-Fi d'una zona, poden apareixer moltes o poques en funció d' on ens trobem o on estem buscant.

Figura 7.2 Resultat escaneig amb un rastrejador Wi-Fi

Hi ha més d' un 40% de xarxes poc protegides esperant que algú vulneri la seva seguretat. Per augmentar les possibilitats de trobar-ne una, els hackers acostumen a:

Moure's cap a zones residencials: les xarxes domèstiques solen estar menys protegides.
Busquen una alta concentració de noms de xarxes genèriques (p.e. *WLAN_XXX*).
Utilitzen un escàner de xarxes *Wi-Fi* millor que el que ve per defecte amb alguns sistemes operatius. Alguns d'aquests escàners, els veiem en el següent punt.
Es situen en llocs còmodes i oberts, com el banc d'una plaça.

7.2 Detecció de Wi-Fis

El més habitual és buscar xarxes *Wi-Fi* amb els assistents de connexió de Windows o els proporcionats pels fabricants. Malgrat la seva rapidesa, aquests programes son força primitius limitant-se a mostrar les connexions trobades durant l'escaneig. No refresquen automàticament el llistat de punts d' accés i proporcionen poca informació sobre les xarxes.

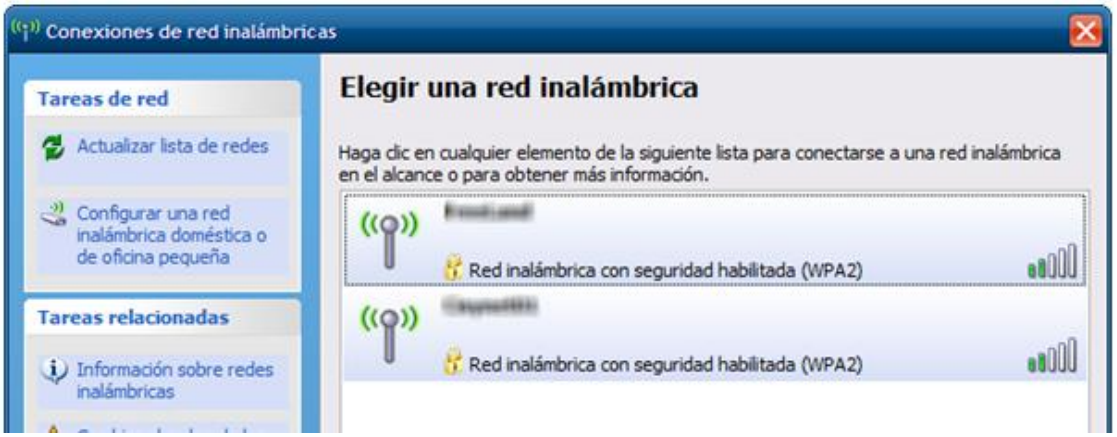

Figura 7.3 Búsqueda de Wi-Fis amb software natiu

Hi ha escàners *Wi-Fi* alternatius, gratuïts i prou potents com per ajudar a seguir un punt d'accés interessant. Alguns recopilen dades en el temps per generar gràfiques de potència del senyal, i d' altres tenen indicadors acústics de potència del senyal, com si fos un "detector de metalls" per a xarxes de lliure accés. Algunes d'elles son: ***Xirrus Wi-Fi Inspector, Easy WiFi Radar, NetStumbler, Vistumbler, InSSIDer, OutSSIDer*** (molt pràctica!)***, WirelessNetViewer...***

Figura 7.4 Xirrus Wi-Fi Inspector

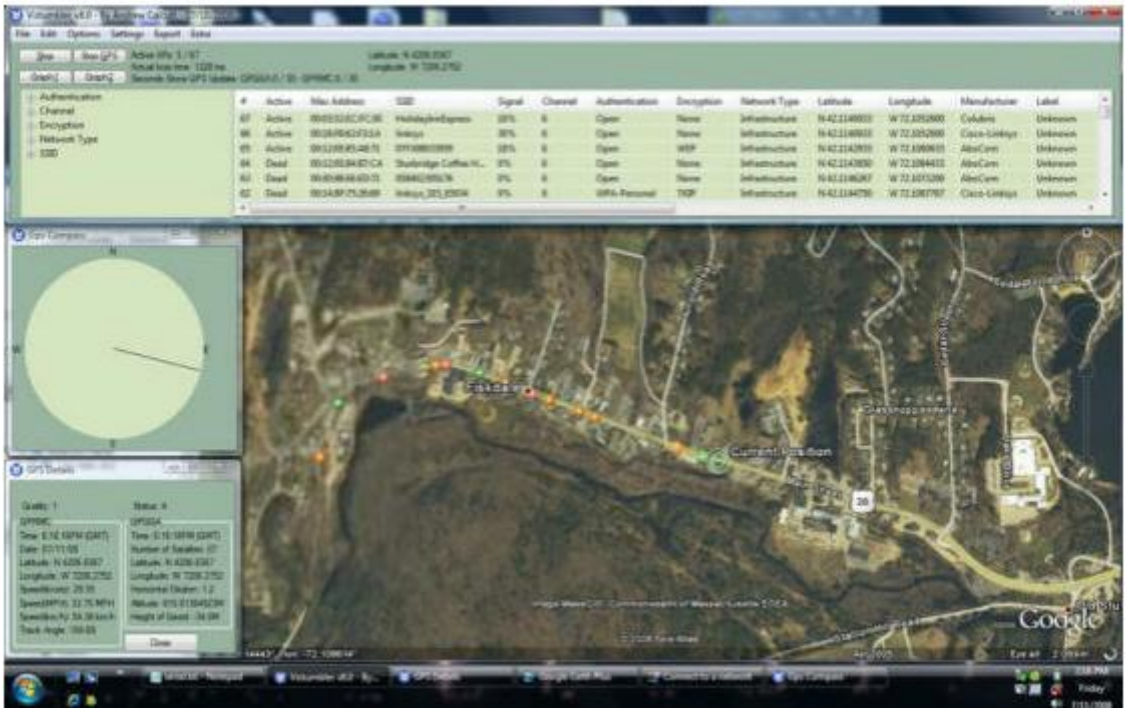

Figura 7.5 Netstumbler i Vistumbler

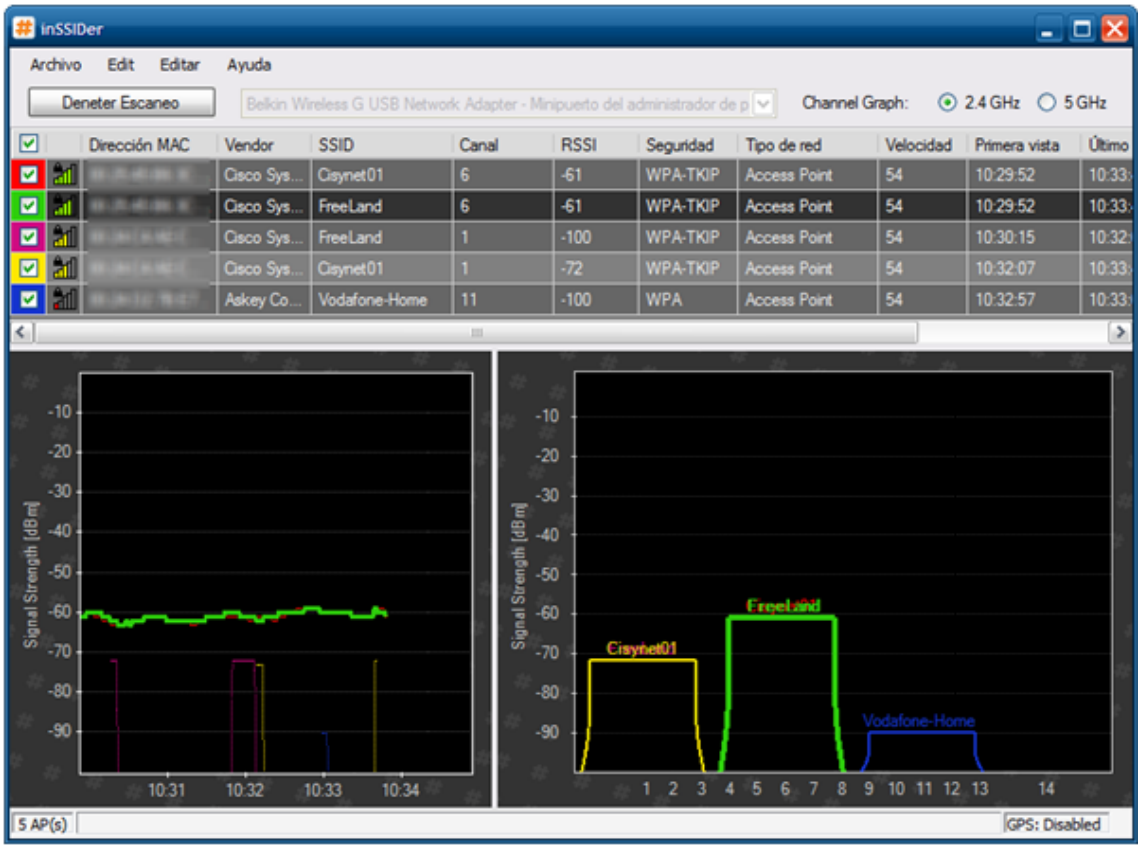

Figura 7.6 InSSIDer

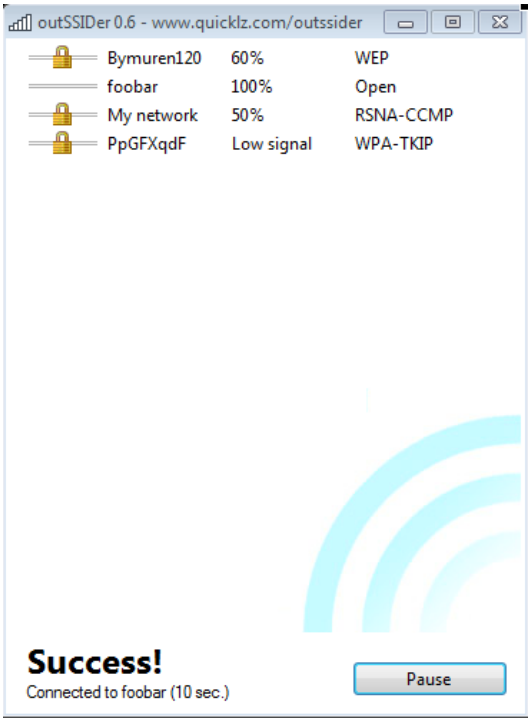

Figura 7.7 OutSSIDer

OutSSIDer busca contínuament xarxes obertes al nostre voltant i es connecta a la més estable.

7.3 Obtenció de claus Wi-Fi

Com hem dit, hi ha molts programes que auditen vulnerabilitats conegudes de *routers* de totes les marques, permetent calcular claus *WPA* a l' instant. Alguns son:

- ***Wifipass*** (Android) - Per routers de *Movistar* i *Jazztel* (WLAN_XXX, Jazztell_XXX).
- ***WiFi Auditor*** (Windows, Mac, Linux) - No molt en ús, però funciona igual de be que Wifipass.
- **Easy WiFi** (Android) – Per *Livebox* d' Orange.
- ***WLANAudit*** (Android) - Eficaç amb rotuers *Zyxel* i *Comtrend*.
- ***WLAN_XXX Decrypter*** (Android).
- ***HHG5XX WEP scanner*** (Android) – Només per a un model concret de punt d'accés de Huawei.
- ***AirCrack*** (Windows, Linux) – Des de la versió 0.9, es poden desxifrar claus *WEP* en poc temps. Al punt següent, fem una demostració.

- ***Reaver*** (Linux) - Aprofita una vulnerabilitat per obtenir la clau WPA. Pot trigar unes hores.
- ***Wifiway*** *(LiveCD)* – Amb moltes eines d'auditoria *Wi-Fi* i força popular.
- ***Beini*** *(LiveCD)* – Un altre *LiveCD* que injecta paquets per aconseguir claus *Wi-Fi.*

Cal destacar que els *exploits* que s' utilitzen per accedir a les xarxes no suposen cap perill ni pel *router* ni tampoc per als demés ordinadors en xarxa; no fan malbé cap programa ni dispositiu.

7.4 Atacs WPA amb Aircrack-ng (Windows)

Partint de la base que: *"Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools. In fact, Aircrack-ng is a set of tools for auditing wireless networks."*

Ens hem instal·lat el software al nostre equip per procedir a l'obtenció de claus *WEP* o *WPA*. Les figures 7.8, 7.9, 7.10 i 7.11 ens mostren com hem actuat per obtenir el password de la Wi-Fi on estem connectats, en aquest cas la d'SSID, *Yacom056156*.

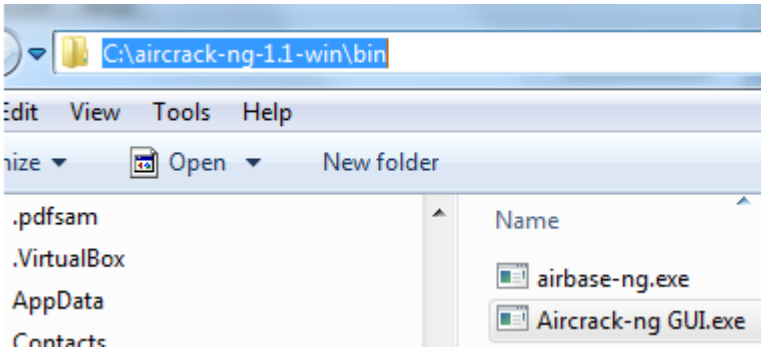

Figura 7.8 Execució de Aircrack-ng

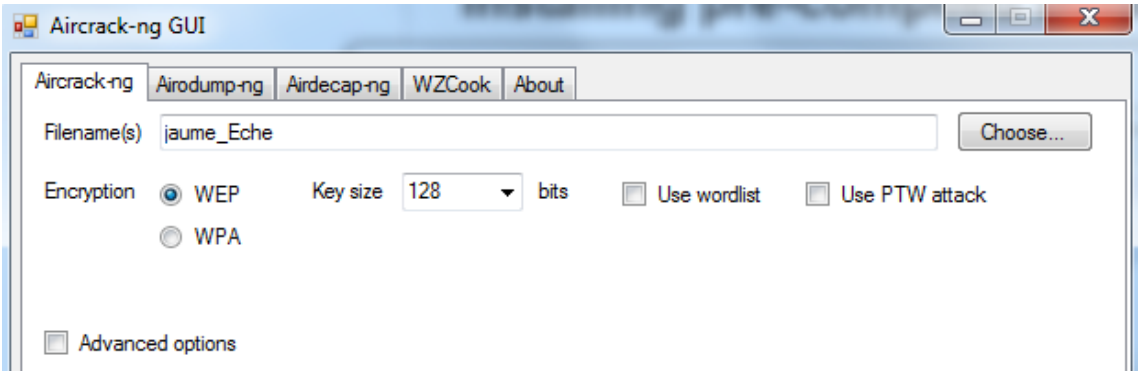

Figura 7.9 Aircrack-ng GUI

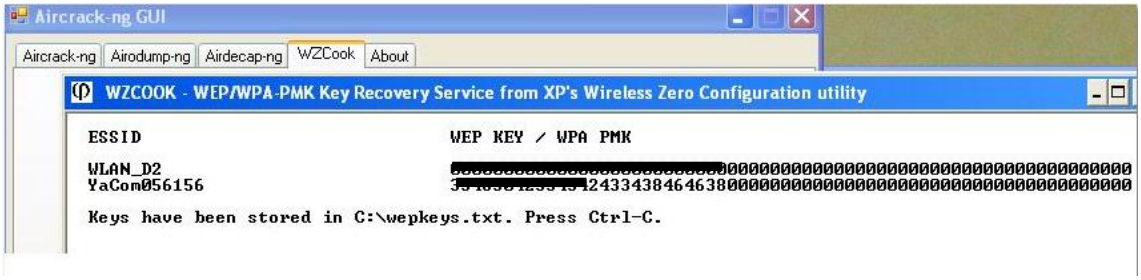

Figura 7.10 Obtenció de claus

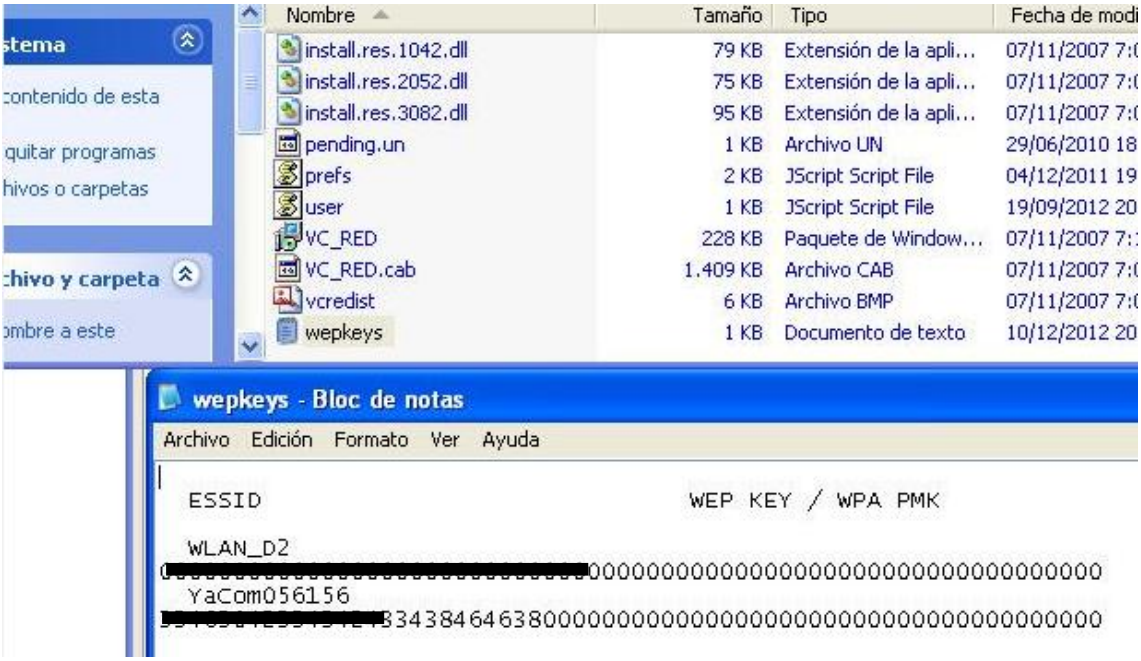

Figura 7.11 Fitxer wepkeys obtingut

7.5 Atacs WPA2-PSK amb BackTrack 5 (Linux)

Tot seguit mostrarem un exemple d' atac a *WPA2-PSK*, és a dir, amb clau pre-compartida. En aquest exemple treballarem sota la distribució *BackTrack* 5 de 64 bits. El primer pas serà configurar la nostra targeta per canviar-la a estat "monitor", només les targetes amb *chipset Atheros* i Prisma ho permeten, per tal d' escoltar tot el tràfic *Wi-Fi* proper. La nostra targeta *wireless* s' identifica al sistema operatiu com "wlan0". Configurem el mode monitor amb la comanda:

$ iwconfig wlan0 mode monitor

Si no s' especifica cap canal d' operació la targeta actuarà per defecte mitjançant salts de freqüència. En cas de voler configurar el mode monitor amb un canal concret l' ordre serà:

$ iwconfig wlan0 mode monitor channel 6

Hem obtingut l' objectiu mitjançant l' aplicació *Kismet*, que ens permet visualitzar les xarxes que ens envolten, així com les adreces MAC dels AP i dels clients associats, també els mètodes de xifrat i d' autenticació.

El següent pas serà desar tota la informació relacionada amb el punt d' accés atacat. Les eines ens proporcionen la informació necessària, en aquest cas només necessitarem la *MAC* de l' *AP* i el canal. Farem servir *airodump-ng* de la següent manera:

$ airodump-ng –c 6 –bssid 00:18:39:83:0E:6D –w psk wlan0

La opció *-c* defineix el canal, *bssid* la MAC de l' AP, *-w* escriu un nou arxiu anomenat *psk* amb cap d' extensió i que haurem de tractar més endavant. El darrer paràmetre fa referència a la targeta que utilitzarem en cas que tinguem més d' una. La següent imatge ens mostra el resultat d' aquesta execució.

Figura 7.12 Resultat airodump-ng

Ara ja estem capturant i desant paquets a l' arxiu *psk.cap*. En el cas d' atacar a *WPA2* caldrà escoltar el procés de negociació *handshake-4* per obtenir, entre d' altres paràmetres, la clau xifrada. Sense aquest pas de detecció de *handshake* aquest atac és inviable. Per detectar un *handshake* caldrà esperar que un nou client s' associï al punt d' accés o forçar la desconnexió d' un client ja connectat mitjançant l'eina de reenviament de paquets *aireplay-ng*. La comanda és:

$ aireplay-ng -0 1 –a 00:18:39:83:0E:6D –c 00:13:E8:7B:51:13 wlan0

L' opció *-0* indica que és un reenviament de deautenticació; el nombre *1* indica els intents fets; el paràmetre *–a* introdueix la MAC de l' AP i *–c* la de qualsevol client associat, com es mostren a la captura anterior; de nou, caldrà especificar l' interfície que utilitzarem, *wlan0*.

Figura 7.13 Resultat aireplay-ng

Enviats els paquets de reautenticació i capturat el procés de negociació ja podrem iniciar l' atac sobre les dades obtingudes. Aquí és on rau la veritable dificultat de *WPA2* ja que l"atac sobre els sistemes de xifrat *TKIP o AES*, a diferència del *WEP* basat en *RC4*, s"ha de realitzar mitjançant força bruta. És habitual l"ús de diccionaris predefinits per tal de reduir el temps de processament i acotar les opcions. Es pot utilitzar eines com *crunch* per generar

els nostres diccionaris amb paràmetres personalitzats. L"eina que utilitzarem per aquest darrer pas és *aircrack-ng*:

$ aircrack-ng –w dictionary.txt –b 00:18:39:83:0E:6D psk.cap

On *–w* selecciona el diccionari; *-b* la MAC de l' AP i el darrer paràmetre és l' arxiu *.cap* que hem generat amb *airodump-ng* amb tots els paquets recaptats. Si hem tingut èxit amb l' atac ens apareixerà una pantalla com la següent on se' ns mostrarà la clau.

Figura 7.14 Resultat aircrack-ng

Aircrack-ng ens proporciona unes taxes que ronden les 1000 claus per segon. Com ja hem esmentat, eines com *pyrit* que utilitzen la capacitat de processament de les noves *GPU*, és a dir, de les targetes gràfiques, aconsegueix multiplicar la velocitat de les proves. A la xarxa podem veure exemples d'atac que assoleixen un rati de fins a 5.000 claus/seg.

Imaginem que disposem d'una informació que ens indica que la clau té una longitud de 10 caràcters alfanumèrics. Suposem un diccionari que ha generat totes les combinacions possibles de 26 lletres en majúscules i minúscules, és a dir 52 caràcters i, a més, els 10 caràcters numèrics, un total de 62 elements agafats de 10 en 10; 62^{10}= 839.299.365.868.340.224 possibles claus. Si com en el millor dels casos, podem assolir una capacitat de processament de 5.000 claus/seg trigaríem poc més de cinc milions d'anys en testejar totes les possibles combinacions.

8. Referències web consultades

Infrarrojos

http://www.monografias.com/trabajos-pdf4/comunicaciones-infrarrojas/comunicaciones-infrarrojas.pdf

http://www.izt.uam.mx/newpage/contactos/anterior/n47ne/infra.pdf

Bluetooth

http://www.bluetooth.com/Pages/Bluetooth-Home.aspx

ZigBee

http://www.seccperu.org/files/ZigBee.pdf

Pàgina de RTC-The magazine of record for the embedded computing industry: Using ZigBee Wireless Networking to Develop Commercial Products

http://www.rtcmagazine.com/home/article.php?id=100656

WiMAX

http://www.bandaancha.es/Informacion/Tecnologias/TecnologiasInalambricas/Paginas/WiMAX.aspx

http://netacad.uv.es

http://www.wimaxforum.org

http://www.intel.com

http://www.wikipedia.org

http://www.radiooptica.com

http://www.adslayuda.com

http://www.tuxteno.com

WIPS

http://www.motorola.com/web/Business/Services/Advanced%20Services/Wireless%20IPS%20Advanced%20Services/_Documents/Static%20Files/Spanish%20Datasheet_WIPS_SP.pdf

http://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system

http://www.airtightnetworks.com/home/solutions/wireless-intrusion-prevention.html

http://www.airtightnetworks.com/fileadmin/pdf/datasheet/AirTight-WIPS-Datasheet.pdf

http://www.cisco.com/en/US/docs/wireless/technology/wips/deployment/guide/wipsdep.html#wp136114

http://revistaie.ase.ro/content/47/23Timofte.pdf

http://www.digitalairwireless.com/outdoor/point-to-point-wireless.html
http://go.airtightnetworks.com/AirTight-Product-Demos.html

Seguretat Wi-Fi:

Observatorio tecnológico del ministerio de educación, cultura y deporte
http://recursostic.educacion.es/observatorio/web/es/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi?start=7
Departamento de Tratamiento de la Información y Codificación del CSIC
www.iec.csic.es
Red Temática de Criptografía y Seguridad de la Información de la Universidad Politécnica de Madrid: *www.criptored.upm.es*
Seguridad Wireless: *http://www.seguridadwireless.net/*
http://foro.seguridadwireless.net/puntos-de-acceso-routers-switchs-y-bridges/
http://www.aircrack-ng.org/doku.php
http://foro.seguridadwireless.net/noticias-wireless/
http://www.cypsela.es/especiales/pdf206/confidencialidad.pdf
Protocols de seguretat *WEP/WPA/WPAv2*:
http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml#ixzz2FaGEwca3
http://ocw.uoc.edu/computer-science-technology-and-multimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01771.pdf
http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf
http://es.wikipedia.org/wiki/Comprobaci%C3%B3n_de_redundancia_c%C3%ADclica
http://standards.ieee.org/getieee802/download/802.11i-2004.pdf
http://www.belt.es/noticiasmdb/home2_noticias.asp?id=13250
Vikipèdia: *es.wikipedia.org/wiki/Wi-Fi*
Instituto Nacional de las Tecnologías de la Comunicación: *cert.inteco.es*

Alres web interessants

"El Hacker":
http://www.elhacker.net/manual_hacking_wireless.html

"El taller de redes WIFI de Vic_THOR":
http://www.hackxcrack.com/phpBB2/viewtopic.php?t=21310

"Manual de sniffers de LorD_Darkness"
http://ccia.ei.uvigo.es/docencia/SSI/SniffersPDF.pdf

"Manual de redes wireless de Vicent Alapont":

http://ns2.elhacker.net/timofonica/facu/seguridad_en_redes_inalambricas_by_vicent_alapont.zip

"Taller práctico de intrusión en redes locales de Gospel"
http://foro.elhacker.net/hacking_avanzado/taller_practico_de_intrusion_en_redes_locales-t45618.0.html

NAC:

http://www.enterasys.com/company/literature/nac-ds.pdf
http://www.opus1.com/nac/#NAC
http://www.infoworld.com/article/05/09/05/36FEbattlesecurity_1.html
Implementing NAP and NAC Security Technologies. Daniel V. Hoffman
Network Security Technologies and Solutions. Yusuf Bhaiji
http://www.interop.com/newyork/eventhighlights/interoplabs/
http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1228704,00.html
http://en.wikipedia.org/wiki/Network_Admission_Control
http://sslvpn.breakawaymg.com/eps/NAC.phpRedes&Telecom
http://en.wikipedia.org/wiki/Access_Control
http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html
Microsoft NAP
http://www.microsoft.com/technet/network/nap/default.mspx
http://en.wikipedia.org/wiki/Access_Control
http://www.germinus.com/sala_prensa/articulos/SIC73_096-100.pdf
https://www.trustedcomputinggroup.org/groups/network/
http://www.trustedcomputinggroup.org/solutions/network_access_and_identity
http://en.wikipedia.org/wiki/802.1X
http://netpass.sourceforge.net/
http://www.freenac.net/
http://www.packetfence.org/

Aquest TFC està dedicat especialment a l' Anna. Sense ella, no hagués arribat on estic. Gràcies.