Seguretat en xarxes

WPAN i WLAN

Lluís Toro Puig

TFC - Eng. Tècnica Telecomunicacions

UOC

Índex

1. Introducció

L'objectiu d'aquest treball és exposar les falles de seguretat dels protocols més estesos en les xarxes WPAN i WLAN. Per fer-ho, repassarem les solucions que estàndards i fabricants han atorgat a les diferents tecnologies, veurem les falles que s'han anat alliberant i comentarem les contramesures existents per fer-les front.

Introduirem breument el concepte *WPAN*, els estàndards que hi podrem trobar sota aquesta classificació, les seves aplicacions i en quins dispositius incorporen aquesta tecnologia.

Entrarem en detall en *RFID* comentant les seves característiques, components, freqüències de treball, I*SOs* que hi participen de la seva estandardització i codificacions admeses per *EPC*. Amb aquest precedents llistarem els requisits de seguretat que es demanen per a *RFID* i analitzarem tan els tipus d'atacs que poden trencar els sistemes de seguretat com les seves contramesures. Com que *RFID* ve molt lligat a temes d'identificació inclourem un apartat on destacarem els drets a privacitat dels usuaris recollits en la LOPD.

De la mateixa manera, analitzarem la tecnologia *Bluetooth*, les seves classes i, amb més deteniment, les seves versions i la pila de protocols que incorpora. Esmentarem els seus sistemes de seguretat i després mirarem de trencar-los amb diversos mètodes i eines. Acabarem aquest apartat amb contramesures per mantenir segurs els nostres dispositius *Bluetooth*.

En el darrer apartat WLAN exposarem l'estàndard 802.11 i les seves versions. Veurem com els primers intents d'oferir seguretat a les xarxes Wi-Fi no van ser gaires fructífers i seguirem l'evolució de los noves propostes que van sorgir. Finalitzarem amb l'exposició fil per randa d'un cas pràctic d'atac sobre una xarxa xifrada amb WPA2.

Afegirem un petit apartat on relacionarem els costos d'atacar aquestes diverses tecnologies, el hardware i el software necessari que necessitaríem per dur a terme una auditoria de seguretat a qualsevol empresa.

Finalment, després de tot el que haurem vist, exposarem les conclusions d'aquest treball sobre la seguretat en aquests entorn sense fils.

En els annexos podrem trobar alguns articles que hem considerat d'interès i que ens serviran per recolzar la motivació que ens ha portat a dur a terme aquest treball.

1.1 Motivació i objectius del projecte

Avui dia les xarxes sense fils de curt o mig abast, com ara les *WPAN* o *WLAN*, es troben arreu, són elements bàsics de la nostra quotidianitat tant per a usuaris com per a empreses i altres organitzacions. Això, entre d'altres factors, es deu a l'abaratiment de costos de producció d'aquestes tecnologies i a les avantatges que porten associades, sobretot a la mobilitat. Per tant, és innegable que aquestes tecnologies han vingut per quedar-se i cal tenir-les molt en compte, sobretot en temes de seguretat. ¿Per què? Aquestes tecnologies, per la seva naturalesa de curt abast requereixen proximitat i és casualment en aquestes tecnologies on hi dipositem enormes quantitats d'informació, molt cops personal o que faciliten l'accés a aquesta.

Per tant, l'objectiu principal d'aquest treball és exposar la feblesa d'aquestes tecnologies i advertir a usuaris, empreses i organitzacions dels perills que tenen si no se'n fa un ús correcte de les seves capacitats. Per això res millor que fer un repàs tant dels seus mètodes natius que, segons els fabricants, ens garanteixen seguretat, com dels mètodes i eines existents per trencar-la. Alhora, però, també oferirem solucions i recomanacions de bones pràctiques per oferir, no garantir, una mica més de seguretat.

Com ja s'ha esmentat, un dels apartats finals serà una aproximació als costos d'una hipotètica auditoria de seguretat, ja avancem que no són gens elevats, tot mirant d'atraure possibles mirades de petits i mitjans empresaris que els copsi el possible grau de vulnerabilitat de les seves xarxes corporatives vers els pocs recursos que es necessiten per comprometre-les.

2. Xarxes sense fils

Per xarxa sense fils entenem un seguit de connexions entre nodes sense cap tipus de connexió física o cables, sinó per ones electromagnètiques. Una de les seves avantatges, a part de l'evident mobilitat, és la reducció de costos al eliminar tota la infraestructura de cablejat. D'altra banda, com veurem en el desenvolupament d'aquest treball, requereix d'una seguretat més exigent i robusta per a evitar atacs i intrusions.

Tot i que la percepció general és que les xarxes sense fils formen part de les tecnologies més modernes, el cert és que existeixen des de fa més 15 anys. Certament, els seus primers usos eren molt específics i exclusius de certes industries i no fou dins a finals dels 90, amb la penetració d'Internet i més tard dels primers *smartphones* que no adquiriren aquesta popularitat.

Les xarxes sense fils les podem classificar, bàsicament, pel seu abast o rang d'acció:

- ***WPAN (Wireless Personal Area Network):*** Abast d'un pocs centímetres o metres, requereix que els dispositius estiguin molt a prop. L'estàndard més estès és *Bluetooth*.

- ***WLAN (Wireless Local Area Network):*** Poden donar cobertura a una llar, oficina o edifici. La majoria de gent associa a *WLAN* l'estàndard 802.11.

- ***WMAN (Wireless Metropolitan Area Network):*** Donen cobertura a tota una ciutat o area metropolitana. L'estàndard líder en aquest rang és *WiMax*.

- ***WWAN (Wireless Wide Area Network):*** Ofereixen cobertura a nivell estatal o continental. Parlem, generalment, de telefonia mòbil *GSM* o *UMTS*.

Molts cops s'associen aquests tipus de xarxa a l'estàndard més popular del seu rang, com relacionar la *WLAN* amb l'IEEE 802.11, però el cert és que en cada tipus de xarxa trobarem un ventall d'opcions com veurem al llarg d'aquest treball.

No hem d'oblidar, però, que tot i l'atribut *wireless*, les xarxes del tipus *WWAN* i *WMAN*, fins i tot també algunes *WLAN*, solen tenir una forta infraestructura de cablejat.

Per tant, en determinades ocasions les xarxes sense fils no són una solució per si soles, sinó un complement a les xarxes tradicionals.

Les xarxes sense fils es basen en ones de radio, un medi obert que permet la intercepció de dades per gent no autoritzada. En el disseny sense fils la capa física i d'enllaç, encarregades de la gestió de l'energia i d'evitar col·lisions entre paquets, han estat un mal de cap que ha deixat en segon pla la consideració de la seguretat.

3. Xarxes WPAN

L'estàndard més conegut dins les *WPAN* és el *Bluetooth* però és potser a les *WPAN* on trobarem més quantitat d'estàndards i extensions, com ara el *ZigBee* pensat per a domòtica o el *RFID* per emmagatzemar dades.

Generalment trobarem aquest tecnologia a mòbils, *PDAS*, impressores i altres dispositius de curt abast que requereixen connexions d'usuari a usuari. Entre les seves infinites aplicacions podem destacar el control i monitorització industrial, les targetes intel·ligents i domòtica.

Aquest tipus de xarxa té una cobertura molt reduïda i això, en certa manera, és una avantatge per a la seguretat dels dispositius que la fan servir. Veiem a continuació més detalladament els casos d'ISO 14443 i IEEE 802.15.

3.1 RFID i NFC

RFID (*Radio Frequency IDentification* o identificador per radiofreqüència) és una tecnologia especificada a ISO 14443 pensada per la identificació d'objectes mitjançant la informació que podem desar o recuperar d'uns dispositius anomenats "*tags RFID*". Són, bàsicament, petits dispositius que disposen d'antenes per la comunicació radio i poden ser adherits a qualsevol lloc o objecte.

Quan parlem d'un sistema RFID tendim a pensar només en els *tags*, però el cert és que un sistema complet RFID ha de contenir:

- ***Tags o etiquetes RFID***: Existeixen només de lectura que es personalitzen en el moment de la seva fabricació, lectura/escriptura, o anticol·lisió que permeten llegir un grup de tags amb només una lectura. ja que d'una altra manera només es poden llegir d'un en un. Actualment les etiquetes tenen un preu d'uns pocs cèntim d'euro i amb dimensions de 0.4mm2. Existeixen bàsicament dos tipus de *tags RFID*:

    - ***Tags actius***: Tenen la seva pròpia font d'alimentació que els hi permet emetre de forma contínua una senyal de radio. Aquests *tags* poden transmetre la senyal fins a varies desenes de metres i són més fiables que els passius, a més poden iniciar una sessió amb els lectors, però a diferència dels pasius, aquests solen ser

més grans, como ara la mida d'una moneda, costosos i la seva vida útil és "només" d'uns anys.

- ***Tags pasius***: No disposen de font d'alimentació, sinó que s'alimenten mitjançant el camp electromagnètic induït pel lector. Per tant, són dispositius molt petits, tant que poden ser inserits sota la pella, disposen d'una molt llarga vida útil ja que no se'ls s'hi esgota la bateria. A diferència dels actius, la seva lectura normalment s'ha de fet des d'una distància molt curta, de l'ordre d'uns pocs centímetres, tot i que sempre dependrà de la potència i sensibilitat del lector. A la següent figura podem veure alguns models de *tags* passius.

Figura 1: *Tags RFID* passius

- ***Lector***: És l'encarregat d'enviar senyals de radio cercant *tags* o etiquetes *RFID* properes. Quan una senyal és captada el lector transfereix les dades al subsistema de processament de dades.

- ***Subsistema de processament de dades o Middleware RFID***: És la part software de tota l'arquitectura, l'encarregat d'enviar les dades al sistema de gestió, per exemple d'una empresa. És, en certa manera, un encaminador entre les dades extretes pel lector i qualsevol altre software de gestió que hagi d'administrar les dades.

A la següent figura veiem un esquema del funcionament d'un sistema RFID.

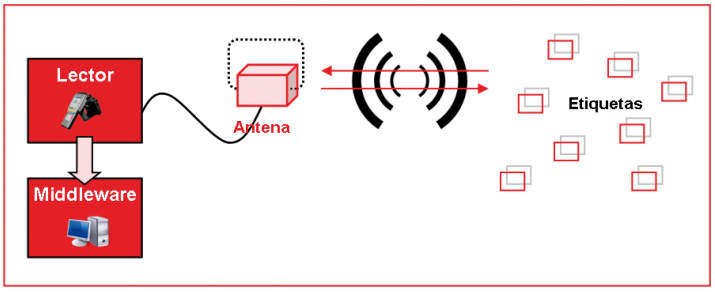


Figura 2. Esquema de funcionament de RFID

Si parlem de *RFID* hem d'esmentar l'organització *EPC Global*, que és l'organització encarregada d'assignar els diversos codis hexadecimal de 24 dígits *RFID* únics a entitats i empreses, anomenat *EPC (Electronic Product Code)*. Actualment ens trobem a la versió 1.6 d'*EPC* que admet els següents esquemes de codificació pels seus 96 bits depenent de la seva aplicació: *General Identifier (GID), Versió serialitzada del GS1 Global Trade Item Number (GTIN), GS1 Serial Shipping Container Code (SSCC), GS1 Global Location Number (GLN), GS1 Global Returnable Asset Identifier (GRAI), GS1 Global Individual Asset Identifier (GIAI)* i *Department Of Defense* (Departament de Defensa dels EEUU, DoD).

GS1 és una organització privada dedicada a la estandarditzación de normes i solucions globals per a millorar l'eficiència de les cadenes d'abastiment, la oferta i la demanda de tots els sectors a nivell mundial.

Gràcies a EPC, GS1 i a ISO s'han elaborat diverses especificacions per a RFID:

- ***ISO/IEC 11784-11785, ISO 10536, ISO 18000***: Privacitat i seguretat de les dades.

- ***ISO 14223/1***: Identificació d'animals i transponedors avançats i *interface* de radio.

- ***ISO 14443***: Sistemes de pagament electrònic i identificació personal. Els passaports que ja duen RFID es basen en aquest estàndard HF.

- ***ISO 15693:*** Estàndard HF per a targetes de crèdit o dèbit sense contacte.

- ***ISO18000-7***: Estàndard industrial UHF (per a *tags RFID* actius) que promou el *DoD* dels EEUU i la OTAN.

- ***ISO 18185***: Seguiment de contenidor a 433 MHz y 2.4GHz

- ***ISO/IEC 15961***: Defineix protocol de dades i interface de l'aplicació.

- ***ISO/IEC 15962***: Codificació de les dades i funcions de la memòria a *RFID*.

- ***ISO/IEC 15963***: Sistema de *tracking* i monitorització que afecta als *tags RFID*.

- ***ISO 19762-3***: Estableix com s'ha de dur a terme la identificació dels *RFID* en l'àmbit de la identificació automàtica i la captura de dades tècniques.

Tot i aquestes especificacions, són en darrer terme els governs i fabricants qui regulen les freqüències o implementen altres funcionalitats sobre els sistemes RFID. Aquesta manca d'estandardització més uniforme a nivell mundial, tot i l'esforç d'ISO i la universalitat dels codis EPC, són la font de problemes actuals pel que fa a la compatibilitat entre diversos dispositius RFID i la seva comunicació amb altres tecnologies. En la següent figura mostrem la implementació dels diversos estàndards RFID arreu del món, especificant les seves freqüències i potències màximes.

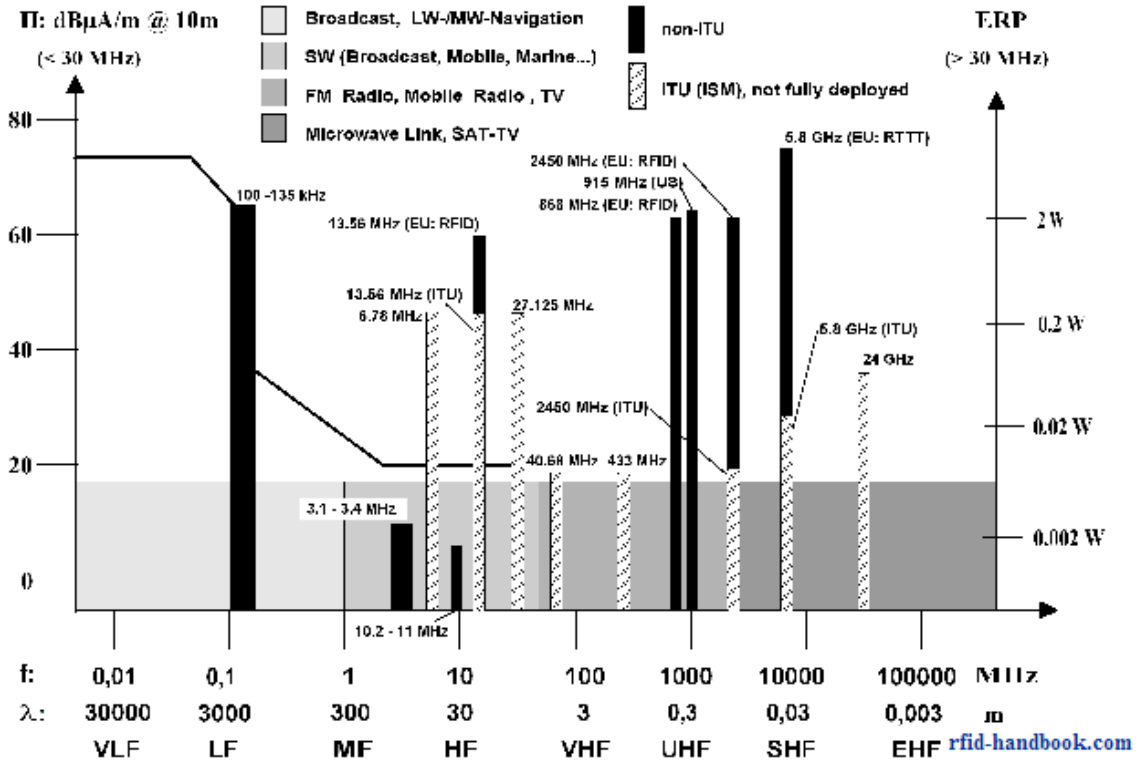


Figura 3. Espectre de la tecnologia RFID. Font rfid-handbook.de

També hem afegit en aquest apartat la tecnologia NFC, una extensió de RFID dedicada al traspàs de dades entre terminals propers i que ja incorporen molts telèfons mòbils, ja que es tracta d'una extensió de la ISO 14443 i que també inclou la ISO 18092 per als dispositius NFCIP-1. A diferència de RFID, que disposa d'un gran ventall d'aplicacions, NFC només opera en distàncies molt curtes, habitualment 4 cm, i quan es necessita més seguretat que la que ofereix RFID. Tot i salvant les distancies i les coses més específiques de cada protocol, part de les vulnerabilitats de RFID també las trobarem a NFC.

Les aplicacions d'aquestes dues tecnologies són força variades: permet a les botigues identificar els seus productes, ja sigui per passar per caixa, per gestionar l'estoc del magatzem o per activar una alarma de furt que, a més, ens avisarà quin producte ha estat extret. S'incorporen chips RFID a targetes de transport públic, de crèdit o al mateix mòbil per realitzar diversos pagaments, per a la identificació de mascotes amb xips subcutanis i també en competicions esportives per realitzar un seguiment més acurat del resultat, per exemple en carreres o maratons. Tot allò que calgui identificar es podrà fer mitjançant RFID.

3.1.1 Sistemes de seguretat

Els requeriments que fa la industria i usuaris sobre RFID són bàsicament els mateixos que per a la resta de tecnologies i fan referència als dos gran pilars de la seguretat: autenticació i privacitat.

- ***Autenticació d'etiqueta***: El requeriment de l'autenticació ha estat sempre bàsic per evitar el frau o la falsificació. Un *tag* que permeti autenticació podrà provar la seva identitat mitjançant eines criptogràfiques. A més, és una eina bàsica per evitar els atacs *d'eavesdropping*, com veurem en el següent apartat, ja que requereix una comunicació xifrada. *L'eavesdropping* és comú a totes les tecnologies sense fils i fa referència a l'escolta passiva de la informació que es transmet, tant si està xifrada com si no. D'una altra manera qualsevol atacant podria fàcilment demanar informació mostrant un nom fals d'un agent autoritzat. Si aquesta primera autenticació no es fa xifrada la víctima podria enviar tot tipus d'informació, encara que fos perfectament xifrada, directament a l'atacant.

- ***Autenticació del lector***: L'autenticació del lector és necessària per a aplicacions que necessiten accés a certes funcionalitats o informació restringides a la resta d'usuaris. L'autenticació del lector també és un requisit per evitar atacs *eavesdropping*, protegint la comunicació entre *tag* i lector.

- ***Confidencialitat (xifrat):*** Una comunicació xifrada entre *tag* i lector és bàsica per evitar atacs *d'eavesdropping*, que com ja estem veient és el punt feble de les tecnologies sense fils.

- ***Signatura***: Moltes aplicacions de RFID requereixen poder implementar la funció de signatura per oferir integritat a les dades i garantir que no ha estat modificada. Per exemple, un lector pot demanar a cert *tag* que signi certa informació quan l'enviï. Utilitzant aquesta signatura el lector podrà verificar que la informació rebuda l'ha generat un *tag* específic i que no ha estat modificada per tercers. Una industria que implementa la signatura, i és part crítica per aquesta, és la farmacèutica.

Els estàndards, però, no especifiquen quins protocols d'autenticació o algorismes de xifrat s'han d'utilitzar i, tot i aquest consens força general en els quatre punts bàsics de la seguretat a RFID, el cert és que existeixen tantes solucions possibles com proveïdors de *tags* existeixen en el món. Cadascú implementa els sistemes d'autenticació i privacitat que creuen més adient al seu producte. Alguns, com MIFARE, utilitzen protocols propietaris per a aquest objectiu.

És cert que, en general, l'ús que veiem en la nostra vida quotidiana del RFID es veu reduït a articles que comprem i que en certa manera és únicament una substitució del popular codi de barres. Però al no oblidar que una etiqueta RFID pot contenir més informació i que pot ésser llegida sense tenir visió directe o proximitat amb el lector.

3.1.2 Mètodes, eines i costos d'atac

Tot i aquest entorn de la tecnologia RFID sense gaire definició pels aspectes més tècnics de la seva seguretat, ja que els estàndards no esmenten cap sistema de seguretat específic, els atacs sobre els *tags* són quelcom més concret. Definirem els tipus d'atacs més estesos:

- ***Aïllament d'etiquetes***: És l'atac més bàsic que es pot realitzar sobre els *tags*. Quan aquests s'introdueixen a una gàbia de Faraday o es troben a prop d'un camp magnètic que interfereixi la seva senyal s'impedirà la comunicació entre el *tag* i el lector. Així, per exemple, quan hom desitja robar en una botiga un producte etiquetat amb RFID només li caldrà amagar l'article a una bossa mallada o recoberta d'algun material que no permeti el pas de les ones radio per sortir de la botiga sense activar cap alarma.

- ***Suplantació***: Aquest atac consisteix en l'enviament d'una informació falsa que el lector acceptarà com a vàlida. Per exemple, la substitució d'etiquetes entre dos articles, per tant del seu EPC, permetria obtenir un article pagant el preu de l'altre.

- ***Inserció***: Aquest atac permet d'inserir a la memòria de RFID codi executable on s'esperen dades. Aquestes comandes poden produir un atac de denegació de servei o la invalidació de lectors.

- ***Repetició***: Consisteix a enviar al lector una senyal reproduïda per un *tag* vàlid. Aquesta senyal s'haurà capturat mentre s'escoltava la comunicació. El lector acceptarà aquesta senyal repetida com a vàlida, permetent atacs del tipus *man-in-the-middle.*

- ***Clonació***: Mitjançant la escolta d'una comunicació entre lector i tag es poden extreure les dades del *tag* i sobreescriure-les en un altre per utilitzar-lo posteriorment.

- ***Denegació de Servei (DoS):*** Satura el sistema amb més dades de les que és capaç de processar. Existeix una variant, anomenada *RF Jamming*, on s'emet soroll a potencies elevades per tal d'anular la detecció dels *tags*.

- ***Desactivació d'etiquetes***: Quan induïm un for camp magnètic sobre les etiquetes aquest emet un pols electromagnètic que trencarà la part més dèbil de l'antena, deixant al *tag* inservible.

- ***Injecció SQL***: En els *tags* es poden incloure consultes SQL malignes que, un cop arriben al software de BDD o de gestió, modifiqui, insereixi o esborri elements de la BDD.

- ***Spoofing***: És un cas particular dels *tags* actius, semblant a la clonació. S'escriuen dades vàlides sobre un *tag* per tal de suplantar la informació original.

- ***Atacs Man-in-the-Middle (MIM):*** Mitjançant atacs com el de repetició podem arribar a un atac MIM. Es tracta, bàsicament, en vulnerar la confiança entre els *tags* i lectors, substituint alguna d'aquestes entitats.

Com diu la Agencia Espanyola de Protecció de Dades al respecte, la possibilitat d'aquests atacs es deu a la maduresa d'aquesta tecnologia, que permet obtenir lectors i gravadors a un preu força assequible. A més, l'augment de les mesures de la memòria i processament dels *tags* és quelcom que la industria demanda per tal d'incorporar mecanismes de seguretat i xifrat més sofisticats.

Més enllà dels atacs a la seguretat de les etiquetes, aconseguir dades d'una d'elles implica un greuge a la privacitat personal. En 2006 la Comissió Europea va dur a terme una consulta pública sobre RFID i els punts que més preocupaven a la opinió pública varen ser els següents:

- ***Accés il·lícit a les etiquetes***: Aquestes poden contenir informació personal, així com nom, data de naixement, direccions, dades fiscals, sanitàries, etc.

- ***Tracking de persones***: Una persona portadora d'un *tag* RFID amb les seves dades pot ser observada i classificada a partir de les seves accions, gustos, compres i altres aspectes reservats i privats.

- ***Us de les dades per l'anàlisi:*** Les dades recavades pel *tracking* privat i personal es podrien incloure en bases de dades per a mostrejar les preferències de clients o consumidors. Això no seria quelcom dolent, si no fos perquè les dades han estat recavades des d'unes fonts d'informació personals i privades que no hem cedit voluntàriament.

Actualment l'eina més estesa per a realitzar lectura/escriptura sobre *tags* és *RF-Dump*, alliberada sota llicència GPL i multiplataforma, dissenyada per *Boris Wolf* i *Lukas Grunwald*. Ha estat inclosa en les darreres versiones de GNU/Linux BackTrack, una distribució per a auditories de seguretat. Detecta i opera per a quasi tots els tipus d'etiquetes disponibles actualment al mercat, amb total compatibilitat amb l'ISO/IEC 14443 A i B, permet realitzar atacs de força bruta o mitjançant diccionari fent ús de les claus per defecte habituals. A la seva pàgina web el podem descarregar de forma gratuïta, també trobarem imatges per carregar a *VMWare*. Els fundadors de *RF-Dump* han creat l'empresa *NeoCatena Networks*, especialitzada en la seguretat dels sistemes *RFID*.

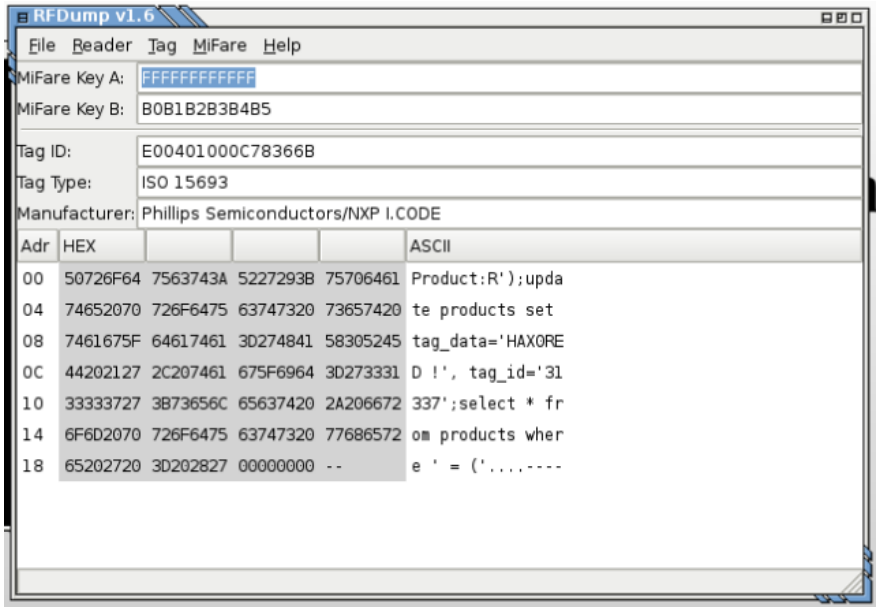


Figura 4. RF-Dump

Per realitzar una auditoria a sistemes *RFID* no requereix un equip força costós. Ja hem esmentat un software de franc amb llicència *GPL*, *RF-Dump*. Necessitarem també un lector. A la xarxa trobarem webs com *Cooking-hacks* on trobarem kits amb lectors i etiquetes que treballen en modes de d'escriptura i lectura per menys de 100 €. Són lectors que funcionen connectats a un portàtil mitjançant USB. Existeixen altres lectors autònoms, semblants als datàfons de les botigues, però el preu ja es pot disparar fins a 2000 €. Pel que fa a les etiquetes, les grans corporacions les compren a granel, si sol·liciten un miler de milions d'etiquetes les poden arribar a pagar a 0.05$ la unitat.

3.1.3 Contramesures

La desconfiança que RFID genera, a la xarxa trobarem centenar de milers d'articles que en fan referència, algunes organitzacions i experts han ofert solucions i recomanacions d'us que mitiguen o redueixen el risc de patir atacs sobre RFID. El curiós del cas RFID és que alguns dels mateixos atacs que hem definit en l'apartat anterior són, alhora, part de la solució i proveeixen seguretat en certs casos.

- ***Watchdog***: Trobarem etiquetes anomenades *watchdog* (gos guardià) que notifiquen els intents de lectura/escriptura en una àrea sobre etiquetes RFID.

- ***Aïllament***: Existeixen dispositius que no permeten la propagació o penetració de les ones radio mitjançant el principi de gàbia de Faraday. Així, quan volem que la etiqueta

sigui llegida només l'haurem de treure de la seva gàbia. Alguns exemples són les carteres amb cobertura metàl·lica

Figura 5. Cartera metàl·lica i bossa "jamming" de RSA

- ***Jamming tags***: Existeix un invent patentat, però encara no comercialitzat, per la companyia RSA anomenat "*jamming tags*". Es tracta d'una bossa amb una etiqueta *RFID* que produeix una senyal que inhabilita els lectors, ja que no disposen de prous recursos per a tractar la gran quantitat de dades que la etiqueta envia, produint una denegació de servei i impedint de llegir la informació del *tag RFID* que s'inclou dins la bossa. És, en definitiva, un sol *tag* que aparenta ser milers. S'han realitzat proves d'aquest invent a la industria farmacèutica i el cert és que no ha estat tan reeixit com s'esperaven, sobretot pel fet que mentre s'aplica aquest mètode de seguretat el *tag* queda inhabilitat pel seu ús i impedeix de treballar amb altres *tags* propers.

- ***Comanda KILL***: Es recomana la inutilització física de la etiqueta o mitjançant l'activació de la comanda KILL, que inclou la memòria del *tag*, que deixarà la inservible. Així es limita l'ús i un cop s'ha fet servir es garanteix la privacitat de l'usuari. Per exemple, activant la comanda KILL quan un producte passa per caixa i es cobra l'etiqueta deixaria de funcionar.

- ***Zona segura***: Trobarem dispositius anomenats *firewalls RFID* que, d'una forma semblant a la bossa de RSA, actuen com inhibidors de freqüència. Molts d'aquests dispositius són plaques impreses que requereixen d'alimentació externa per produir una senyal que abasteixi una area raonable.

- ***Reanomenat i temporització***: Les etiquetes *RFID* podrien contenir un conjunt de pseudònims generats de forma pseudo-aleatòria, de tal manera que cada cop que un

lector mira de llegir informació d'un *tag* aquest respon amb un nom diferent. Per mirar de suplantar la etiqueta l'atacant hauria de conèixer tots els pseudònims possibles. Igualment, es podrien extreure utilitzant un lector que permetés realitzar moltes consultes ràpidament per mirar d'extreure tots els possibles noms. Per a evitar aquest atac s'augmenta el temps de resposta del lector davant d'una seqüència ràpida de demandes per part d'un lector.

- ***Reducció d'informació a etiquetes***: S'aconsella no introduir dades sensibles a les etiquetes, sobretot de caràcter personal. De la mateixa manera s'aconsella que un codi EPC contingui el mínim d'informació possible i les dades dels productes o persones es mantinguin desades en una BDD central, minimitzant el risc d'extracció o reescriptura d'informació de les etiquetes.

Actualment, amb l'escassa memòria i capacitat de processament dels *tags* és molt costos implementar solucions basades en criptografia. Per tant, la majoria del món RFID està d'acord respecte al problema de la seguretat, de la privacitat en particular, i creuen que la solució definitiva respecte a aquest problema no ha de venir de la vessant tecnològica, sinó de la definició d'unes politiques que estableixin clarament l'ús i el tipus d'informació que es poden incloure en un RFID i que el consumidor n'estigui informat.

3.1.4 LOPD i RFID

Un usuari mes o menys versat en temes de privacitat i que ara es trobes en possessió d'una etiqueta ja s'hauria plantejat preguntes com:

- Conté el meu nom o altres dades personals sensibles?

- Qui té accés a aquestes dades?

- Des d'on es pot arribar a llegir el meu *tag*?

- Quina és la seguretat que incorpora?

- On es troben els lectors?

- Que fan amb aquestes dades?

La AEPD ha publicat informes divulgatius sobre RFDI on s'esmenten les eines legals que deriven de l'aplicació de la LOPD i que regulen l'ús dels *tags* RFID. Aquest informe ens diu que quan estiguem en un entorn on:

- Les etiquetes serveixin per a recopilar informació vinculada amb dades personals. Per exemple, una determinada compra.

- Les etiquetes emmagatzemin informació personal.

- Quan les etiquetes tinguin la finalitat de rastrejar informació dels usuaris en absència d'altres identificador. Per exemple, si un comerç escaneja els *tags* d'un client amb la finalitat de generar un perfil de consumidor.

L'usuari final tindrà dret, entre altres, a conèixer de forma clara la finalitat de les etiquetes i quins productes en porten incorporades, conèixer si aquestes estan actives o no, la seva localització en el producte, si serviran per monitoritzar, si existeixen lectors propers, els mètodes que inhabilitin realment les etiquetes o com extreure-les. A més, els productors d'aquestes etiquetes hauran de realitzar un estudi que avali la idoneïtat de l'ús de les etiquetes *RFID* i no altres alternatives, adoptar mesures que preveuen la cancel·lació de les dades obtingudes, així com garantir la seguretat dels elements hardware i software que hi participin en el seu sistema *RFID*, respectant la LOPD.

Tot i la llei, no només la LOPD, sinó les actes europees i altres tractats amb països no comunitaris que vetllen per la protecció de les dades, a Internet podem trobar personalitats com *Richard Stallman*, creador de la *Free Software Foundation*, que s'han pronunciat contra *RFID*. També desenes de grups *anti-RFID* molt crítics amb la implantació d'aquesta tecnologia, com ara l'alemany *FoeBuD* que realitza campanyes alertant dels perills pels consumidors i dels beneficis que aquesta tecnologia pot oferir al "*Big Brother*".

Figura 6. Logo de la campanya anti-RFID de FoeBuD

3.2 Bluetooth i ZigBee

L'origen del nom *Bluetooth* s'atribueix a un rei danès i noruec, *Harald Blatand*, de la seva traducció anglesa (dents blaves), que fou conegut per les seves habilitats de comunicació i capacitat d'unificació de diverses tribus noruegues i daneses.

Bluetooth és una especificació industrial, creada per *Jaap Haartsen* i *Mattisson Sven* mentre la desenvolupaven a Ericsson l'any 1994, pensada per a la transferència de veu i dades mitjançant radiofreqüència com a substitució del cable. Les especificacions varen ser presentades i formalitzades per un grup d'empreses, el *Bluetooth Special Interest Group (SIG)*, inicialment *Ericsson, IBM, Intel, Toshiba* i *Nokia*, però que actualment està format per més de 14000 entitats. Treballa a la banda ISM (*Industrial, Scientific and Medical*) de 2,4 GHz. Trobarem aquesta tecnologia implementada en una gran quantitat de dispositius que ens són familiars: mòbils, ordinadors, *PDAs*, *tablets*, impressores, càmeres digital...

La tecnologia *Bluetooth* té un baix cost, com baixa és la seva cobertura i el seu consum energètic. Aquests paràmetres de consum i cobertura o d'ampla de banda ens serveixen per categoritzar les diverses classes i versions d'aquest estàndard.

Classe	Potencia màx (mW)	Potència màx. (dBm)	Cobertura
Classe 1	100 mW	20 dBm	100 metres
Classe 2	2,5 mW	4 dBm	10 metres
Classe 3	1 mW	0 dBm	1 metre

Taula 1. Classes de Bluetooth

Versió	Ampla de banda
1.2	1 Mbit/s
2.0 + EDR	3 Mbit/s
3.0 + HS	24 Mbit/s
4.0	24 Mbit/s

Taula 2. Versions de Bluetooth

Bluetooth treballa mitjançant salts de freqüència d'1MHz en la banda entre 2.4 i 2.48 GHz, cosa que li confereix seguretat al no trobar-se sempre al mateix canal. Originàriament només acceptava l'esquema de modulació GFSK (*Gaussian frequency-*

shift keying), fins l'arribada de la versió 2.0+EDR (*Enhanced Data Rate*) que admetia π/4-DQPSK i 8DPSK i permetia comunicar-se amb altres aparells compatibles. *Bluetooth* és un protocol basat en paquets amb una estructura de màster-esclau on cada node màster pot comunicar-se fins amb set nodes esclaus alhora, donant lloc a una "*piconet*". Els dispositius *Bluetooth* poden canviar-se els rols i el que era esclau pot esdevenir màster per crear una nova xarxa. Els dispositius que poden actuar com a màster i esclau alhora poden connectar dues "*piconet*" creant una nova estructura de xarxa anomenada "*scatternet*".

A l'estàndard trobarem la definició de fins a 32 perfils de treball diferent per a *Bluetooth*, cadascun associat a un tipus d'aplicació o servei: audio, vídeo, telefonia, missatgeria, mans lliures, accés a la SIM, sincronització...

De la mateixa manera introduïm aquí el protocol *ZigBee*, que incorpora el mateix estàndard 802.15.4 per a les capes física i d'enllaç, però incorpora les seves capes pròpies de transport, seguretat i aplicacions. És indicat per a aplicacions que requereixen seguretat amb una baixa taxa de dades i un baix consum, com ara la domòtica o sensors. Les principals diferències amb *Bluetooth* són:

- Bluetooth s'ha destinat a la mobilitat de l'usuari, mentre que ZigBee està destinat per l'automatització a gran escala i control remot.

- Una xarxa *ZigBee* pot assolir fins a 65535 nodes en 255 subxarxes, enlloc dels 8 nodes d'una *piconet*.

- Menys consum energètic ja que no transmet dades contínuament.

- Velocitat de fins a 250 kbps, suficient pel tipus d'aplicació al que està destinat.

3.2.1 Evolució de Bluetooth

Fem un breu repàs a les característiques de les diverses versions per les que ha evolucionat Bluetooth:

- Bluetooth v1.0 i v1.0B: Aquestes primeres versions encara tenien molts problemes, els diferents fabricants tenien dificultats per fer que els seus dispositius foren

compatibles. En aquestes versions s'especificava els components hardware obligatoris per la implementació de Bluetooth.

- Bluetooth v1.1: Ratificat per la IEEE com l'estàndard 802.15.1-2002. Molts dels errors anteriors varen ser solucionats, s'afegia suport per a canals no xifrats i en l'apartat hardware s'incloïa un RSSI per a mesurar la potencia de la senyal rebuda.

- Bluetooth v1.2: Aquesta versió la van fer compatible amb 1.1. S'implementava una connexió i descobriment de terminals més ràpid, es millorava la resistència a interferències de radio, també els algorismes per la transmissió i codificació de la veu. S'introduïen mètodes de control de flux i modes de retransmissió per a L2CAP, element que definirem en 3.2.2. Tot això es va incloure en 802.15.1-2005.

- Bluetooth v2.0 + EDR: De nou, es mantenia la compatibilitat amb versions anteriors. La principal diferència és la introducció de la tecnologia EDR *(Enhanced Data Rate)* que redueix el consum i millora el rati de transferència de dades, amb una velocitat teòrica de 3 Mbit/s tot i que a la pràctica s'ha arribat a 2,1 Mbit/s. EDR implementava una combinació de les modulacions GFSK i PSK, amb les variants π/4-DQPSK i 8DPSK. Existeix també la versió 2.0 sense EDR però disposa de menys velocitat.

- Bluetooth v2.1 + EDR: Completament compatible amb la 1.2 i superiors. Implementava el *Secure Simple Pairing* (SSP) que permet enllaçar mitjançant un canal segur dos dispositius. També s'afegien altres millores en el filtratge de dispositius abans d'una connexió i un mode de treball de baix consum.

- Bluetooth v3.0 + HS: Suporta una velocitat teòrica de 24 Mbit/s. De fet, l'enllaç Bluetooth s'utilitza per la negociació i establiment de la connexió, però la portadora del tràfic està a la mateixa banda que especifica 802.11. El sufix HS fa referència a aquest canal *High Speed*.

- Bluetooth v4.0: Inclou les especificacions clàssiques de Bluetooth, les d'alta velocitat i els protocols que integren la modalitat *Low Energy*. S'implementa una nova pila per la modalitat de baix consum. El hardware esdevé d'un cost reduït, també el seu consum i mida, permetent d'integrar-lo en equips compactes i lleugers. Ofereix serveis i perfils xifrats sota AES, un algorisme de xifrat simètric que utilitza un sistema de xifrat per

blocs de substitució i permutació del que el govern d'Estats Units va promoure la seva estandardització.

3.2.2 Protocols Bluetooth

En paraules de *William Stallings* en el seu llibre "*Wireless communications & networks": "Bluetooth es defineix com una arquitectura de capes de protocols que consta de protocols de nucli, de reemplaçament de cables, de telefonia i els protocols adoptats o heretats".*

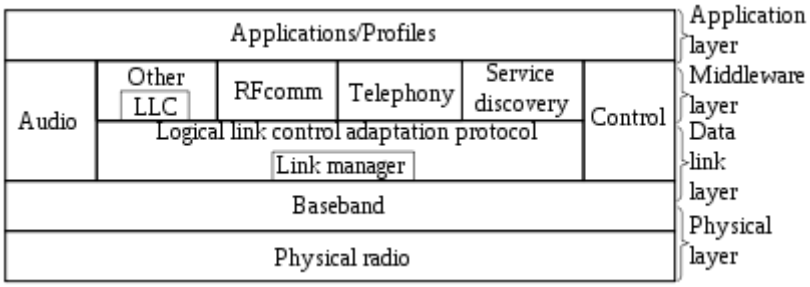


Figura 7. Pila de protocols Bluetooth

A la figura anterior es mostra la pila de protocols Bluetooth que just ara definirem. Cal recordar que els únics que són d'ús estrictament obligatori són LMP, L2CAP i SDP:

- ***Link Management Protocol (LMP):*** S'utilitza per la gestió de l'enllaç radio entre dos dispositius.

- ***A/V Remote Control Profile (AVRCP):*** Normalment utilitzat en el sistema de navegació dels cotxes per controlar *l'streaming* d'audio.

- ***Logical Link Control and Adaptation Protocol (L2CAP):*** Multiplexa diverses connexions lògiques entre dos dispositius, fent servir protocols de nivells més alts. Realitza la segmentació, recupera l'estructura original dels paquets rebuts i gestiona el QoS, la qualitat del servei, per als protocols de la capa superior.

- ***Service Discovery Protocol SDP:*** Ajuda a descobrir serveis suportats per altres dispositius i negocia els paràmetres per realitzar la connexió.

- ***Radio Frequency Communications (RFCOMM):*** Es tracta d'un protocol de reemplaçament de cable que virtualitza un port serial.

- Bluetooth Network Encapsulation (BNEP): Transfereix una altra pila de protocol via L2CAP, com ara una pila IP. És a dir, permet transportar paquets de control i dades per oferir connectivitat a altres xarxes, fet que permet connectar dispositius Bluetooth a xarxes com ara IPv4 i IPv6.

- Audio/Video Control Transport Protocol (AVCTP): Utilitzat per comandaments a distància.

- Audio/Video Distribution Transport Protocol (AVDTP): Transferència *streaming* d'audio/vídeo a altres dispositius.

- Telephony Control Protocol – Binary (TCS BIN): Realitza el control i la senyalització d'una trucada entre dos dispositius.

Pel que fa als protocols adoptats són aquells que han desenvolupat altres organitzacions, no SIG, i s'han incorporat a la pila de protocols Bluetooth, com ara PPP, TCP/IP/UDP, OBEX o WAE/WAP.

3.2.3 Sistemes de seguretat

Hem vist en certs punts com Bluetooth, a diferència de RFID, defineix l'ús de certs algorismes com *l'AES* o mecanismes de seguretat com el *pairing*. Fins a la versió 2.1 el xifrat no era quelcom requerit i podia apagar-se en qualsevol moment. El mètode de xifrat d'aquesta versió es demostrà del tot ineficaç ja que les claus podien ser descobertes a través d'atacs XOR en 24 hores, el que atribuïa a totes les claus un període de vida de, només, un dia.

Bluetooth implementa mètodes per garantir la confidencialitat, autenticitat i la distribució de claus amb un algorisme personalitzar basat en l'algorisme de xifrat de bloc SAFER+. La generació de claus Bluetooth es deriva del PIN que els usuaris han d'introduir en els dispositius que s'enllaçaran. Aquest procés pot variar si un dels dispositius disposa d'un PIN prefixat pel fabricant, com són els auriculars Bluetooth. Durant el procés de *pairing* o emparellat la clau d'inicialització o màster es crea mitjançant l'algorisme E22. L'algorisme E0 s'utilitza pel xifrat dels paquets, garantint la confidencialitat, basat en una clau compartida, la mateixa clau màster que acabem d'esmentar, genera prèviament a l'establiment de l'enllaç.

A Setembre de 2008 la *National Institute of Standards and Technology* (NIST) va publicar una guia que servia com a referència sobre la seguretat de Bluetooth i dels mètodes que calien aplicar per millorar-la. Aquest informe que deixarem a la bibiografia permet a usuaris i organitzacions avaluar, mitjançant *checklists*, guies i recomanacions per mantenir assegurats les nostres *piconets*.

3.2.4 Eines i mètodes d'atac

Bluetooth ha sigut sempre susceptible a diversos tipus d'atacs: *DoS*, *eavesdropping*, *man-in-the-middle*, modificació de missatges i fins i tot a l'apropiació il·legítima de recursos. Si repassem la història dels atacs a Bluetooth hauríem d'escriure uns quants volums. Per citar un parell d'exemples, a 2005 la policia de *Cambridgeshire*, a Anglaterra, es va adonar com els lladres realitzaven escanejos de cotxes tot cercant dispositius amb Bluetooth activat al seu interior, com ara mòbils, PDAs o ordinadors portàtils. En Octubre de 2007 a la conferència de seguretat *Hack.lu* a Luxemburg uns ponents varen mostrar i alliberar un mètode que permetia accedir remotament a una consola root en els models de Mac OS X v10.3.9 and v10.4.

Donem un cop d'ull algunes de les eines que ens permetran d'explotar les vulnerabilitats de Bluetooth:

- ***Blooover***: És una aplicació per a mòbils que corre sota J2ME. Ens permet de fer auditories de seguretat sobre dispositius Bluetooth testejant vulnerabilitats conegudes i atacs *BlueSnarf* o *BlueBug*. La darrera versió d'aquest software és altament nociu ja que pot inhabilitar el mòbil víctima, denegant permisos per escriure SMS o fer trucades.

- ***BTCrack***: Va ser publicada al congrés *hacker* 23C3 a Alemanya. Ofereix una interface gràfica per a realitzar atacs passius d'escolta, aprofitant *l'eavesdropping* tot mirant de capturar missatges en el procés de *pairing* per tal de descobrir la clau mestra.

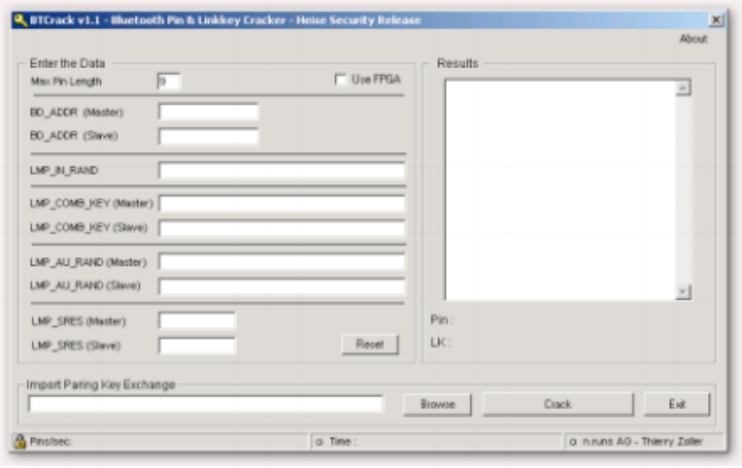


Figura 8: BTCrack

De nou, moltes d'aquestes eines tornen a estar de franc a la distribució de Linux *BackTrack.*

La fama de la inseguretat de Bluetooth ha fet que molts dels mètodes d'atac específics d'aquesta tecnologia s'han guanyat a pols el prefix "blue". Veiem alguns exemples:

- ***BlueSnarf i BlueSnarf++:***: Permet a un usuari extreure dades del dispositiu atacat, com ara fotografies, dades de l'agenda del mòbil o el calendari. Els dispositius que poden ser potencials víctimes d'aquest atac solen tenir una incorrecte implementació d'OBEX (un protocol d'intercanvi de dades que Bluetooth ha implementat). La versió BlueSnarf++ és senzillament una millora del primer que ataca a altres vulnerabilitats d'OBEX.

- ***BlueBug***: Permet d'assolir control remot total d'un dispositiu, mòbils normalment, que utilitzi el protocol RFCOMM dins la pila Bluetooth. La vulnerabilitat es troba en el canal 17 de RFCOMM, que ofereix una porta d'entrada al dispositiu.

- ***BlueJacking***: A diferència dels anterior atacs, aquest no és purament un atac sobre l'arquitectura Bluetooth, sinó sobre l'aplicació de *vCards* que tenen determinats models. Aquesta aplicació permet compartir certa informació personal, com la que oferiríem en una targeta de presentació, però en aquest cas de forma electrònica. La seva finalitat tampoc és la de fer-se amb el control de terminal o extreure dades personals. Aquesta vulnerabilitat permet enviar missatges -via Bluetooth- a l'usuari infectat sense que ell

accepti cap connexió. La impressió de l'usuari infectat que comença a rebre missatges anònims és que s'ha contagiat d'algun virus o que algú l'està acusant.

-***HeloMoto***: Es tracta d'una combinació dels atacs *BlueSnarf* i *BlueBug* sobre una incorrecte implementació de Motorola, que és qui dina el nom a l'atac, sobre altres agents Bluetooth de confiança.

-***BlueSmack***: És el típic atac de denegació de servei, quelcom similar al ping de la mort que assolava IP fa uns anys. La víctima rep un "echo request" d'uns 600 bytes i generalment, tot i el *buffer* per a reservar-lo, no té prous recursos per tractar-lo i el dispositiu acaba per blocar-se.

- ***Blue MAC Spoofing***: Bluetooth estableix diversos nivells de confiança que es basen en guardar informació xifrada de l'adreça MAC d'altres dispositius amb els que ja han interactuat prèviament. Si un atacant és capaç d'esbrinar la MAC d'un dispositiu que ja s'admet com autoritzat guanyarà accés al terminal víctima suplantant la identitat del primer.

- ***CarWhisperer, Headset Hijacking...:*** En realitat diversos mètodes diferents per a diferents tipus de dispositius: el mans lliure d'un cotxe, uns auricular sense fils, portàtils... Però la finalitat és la mateixa: punxar la comunicació d'aquests dispositius i crear un canal d'audio entre aquests dispositius i l'atacant. Succeeix que, normalment, aquests dispositius duen una clau per defecte incorporada de fàbrica que no es pot modificar. Quan aquesta clau es coneix ja es pot establir la comunicació amb el dispositiu. Existeixen aplicacions que duen el mateix nom. *Car Whisperer*, a més d'aplicació, fou una campanya promoguda pel grup *Trifinite* amb la finalitat de conscienciar als fabricants de dispositius Bluetooth del perill de les claus predefinides.

A la bibliografia deixem un enllaç on trobarem de forma detallada el procés per esbrinar o trencar el PIN en una comunicació Bluetooth. Per la seva extensió no hem cregut oportú afegir-ho en aquest espai.

3.2.5 Contramesures

Acabem de veure com Bluetooth no és precisament quelcom segur, ni de llarg la millor opció per transmetre o guardar dades sensibles en determinats dispositius. De totes maneres, encara no està tot perdut.

En algunes de les vulnerabilitats esmentades, com el cas de *BlueSnarf* i *BlueBug*, s'ha aclarit que responen a una incorrecte implementació per part dels fabricants. Això en certa manera és bo, ja que té solució, però d'altra banda estem exposats a ser atacs fins que el nostres fabricant ens faciliti una actualització del firmware. En aquests casos la majoria de terminals vulnerables eren Nokia i Ericsson. De la mateixa manera haurem d'esperar una actualització software de Motorola per fer front a l'atac *HeloMoto*. Aquestes vulnerabilitats ja són residuals en terminals antics.

D'altra banda, per la resta de vulnerabilitats i per la seguretat en general, es recomana seguir unes bones pràctiques com ara apagar el Bluetooth mentre no en fem us. Si l'hem d'activar mirem de configurar-lo en mode ocult per evitar ser descoberts per altres dispositius. Si és possible caldrà xifrar les connexions sempre que el dispositiu ens ho permeti. Hem d'evitar que el nom del terminal, tot i estar ocult, doni informació del model de dispositiu i canviar el que se'ns facilitarà per defecte. No haurem d'acceptar connexions Bluetooth si no sabem d'on provenen i verificarem periòdicament la llista de terminals de confiança que hem associat. A més, mirarem sempre d'utilitzar una clau o PIN el més llarg possible, per exemple durant el procés de *pairing*, per evitar atacs de força bruta. Aplicant aquestes regles no serem invulnerables però farem que l'atacant es plantegi abandonar si li posem les coses difícils.

4. Xarxes WLAN

Les xarxes d'àrea local sense fils o WLAN són un sistema de comunicació molt utilitzat com alternativa o complement a les xarxes d'àrea local o LAN. Aquesta tecnologia basada en radiofreqüència permet als usuaris una major mobilitat. Aquestes xarxes han adquirit força rellevància tant en el món empresarial, com ara en magatzems o manufactura, així com a la llar.

Podem classificar les xarxes WLAN per la seva topologia, bàsicament en tres grups:

- ***P2P o ad-hoc:*** És el tipus de xarxa més bàsic, format per dos ordinadors que es comuniquen entre sí a través d'ones radio. Es tracta d'una comunicació directa entre aquests dos dispositius sense cap node intermedi que gestioni la connexió.

- ***Bridge:*** Un bridge o pont s'utilitza per enllaçar dos tipus de xarxes diferents, com ara una WLAN i una LAN. És la connexió més habituals a les llars, on un únic punt d'accés dona pas a la LAN de la casa o WAN del proveïdor.

- ***Wireless distribution system (WDS):*** L'abast dels punts d'accés sense fils és limitat. Sí volem ampliar la cobertura caldrà distribuir més punts d'accés en la superfície que volem cobrir. WDS permet expandir una xarxa WLAN mitjançant la connexió de diversos punts d'accés sense fils, és a dir, sense connectar-los entre ells amb fils. Trobarem WDS a grans empreses, universitats o altres espais públics de gran superfície.

Disposem d'un estàndard que és el paradigma de les WLAN, ens permet de crear xarxes amb les topologies ja esmentades i també incorpora altres característiques per xifrar i autenticar les comunicacions. Es tracta de l'IEEE 802.11, que disposa de diverses extensions i versions diferenciades per les seves velocitats, cobertures i sistemes de modulació.

4.1 IEEE 802.11

IEE 802.11 és un conjunt d'estàndards que implementen les funcions necessàries per crear xarxes WLAN entre ordinadors en les bandes freqüencials de 2.4, 3.6 i 5 GHz. La tecnologia 802.11 neix l'any 1985 aprofitant que la Comissió Federal de Comunicacions dels EEUU allibera la banda de freqüències ISM per a us lliure, sense llicències. Vic

Hayes, qui va presidir el grup IEEE 802.11 durant 10 anys, per això l'anomenen el "pare del WiFi", es va involucrar en el disseny inicial de 802.11b i 802.11a. Finalment, a 1999 es va crear la Wi-Fi Alliance, una associació de grans empreses com ara 3com, Lucent, Nokia o Symbol que cercaven una tecnologia sense fils per implementar en els seus productes i que aquestos fossin compatibles. Va ser el impuls de la Wi-Fi Alliance el que va afavorir l'extensió de la tecnologia sense fils i l'any 2002 aquesta associació d'empreses ja tenia prop de 150 membres. Tot i aquesta compatibilitat el cert és que cada país implementa la capa física de formes diferents, adequant-la a les necessitats o disponibilitats de l'espectre. Per exemple, al Japó a la versió 802.11b s'afegeix un darrer canal, el 14, a 12 MHz del canal 13, encara que l'espai habitual entre canals és de 5 MHz.

La norma 802.11 especifica equivalències en les capes física i d'enllaç amb l'estàndard 802.3 (Ethernet). Per exemple, tots dos estàndards utilitzen adreces MAC i, per tant, aquestes dues normes disposen de serveis compatibles.

4.1.1 Versions 802.11

Al llarg dels anys s'han desenvolupat diverses versions de l'estàndard 802.11 tot cercant nous rangs de cobertura, la millora del rendiment i la velocitat. És a partir de la versió base, 802.11-1997 (legacy), que s'han anat desenvolupant la resta.

Els estàndards 802.11b, 802.11g i 802.11n gaudeixen d'una gran acceptació internacional ja que la seva banda de treball a 2.4 GHz està disponible gairebé arreu del món. Les seves velocitats arriben fins a 11 Mbps, 54 Mbps i 300 Mbps respectivament.

Actualment també trobarem a l'abast la versió 802.11a, coneguda com a WiFi 5, ja que corre en els 5 GHz. Aquesta freqüència fa que aquesta versió gaudeixi d'uns canals relativament nets, sense gaires sorolls ni interferències. D'altra banda, al ser una freqüència major el seu abast de cobertura es redueix.

L'any 2009 l'IEEE va ratificar l'estàndard 802.11n que pot treballar tant en 2.4 com en 5 GHz, arribant a velocitats de fins a 600 Mbps i compatible amb la resta de versions esmentades anteriorment. Actualment els proveïdors d'Internet ja ofereixen encaminadors amb 802.11n per al mercat domèstic.

S'espera que el futur del Wi-Fi derivi cap a l'estàndard 802.11ac que disposarà de velocitats de fins a 1Gb/s.

Afegirem una taula resum on podrem veure en detall les característiques de cada versió:

802.11 protocols	Data alliberament	Freq. (GHz)	Ample de banda (MHz)	Velocitats (Mbit/s)	Modulació	Cobertura interiors (m)	Cobertura exteriors (m)
legacy	jun-97	2.4	20	1, 2	DSSS,FHSS	20	100
a	sep-99	5	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM	35	120
		3.7				—	5
b	sep-99	2.4	20	1, 2, 5.5, 11	DSSS	35	140
g	jun-03	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM,DSSS	38	140
n	oct-09	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	OFDM	70	250
			40	15, 30, 45, 60, 90, 120, 135, 150		70	250
ac (esborrany)	Nov. 2011	5	20	fins a 87.6			
			40	fins a 200			
			80	fins a 433.3			
			160	fins a 866.7			

Taula 3: Versions 802.11

4.1.2 Sistemes de seguretat

Un nombre molt elevat de xarxes Wi-Fi són instal·lades sense tenir en consideració la seguretat, amb punts d'accés oberts o amb les contrasenyes que el fabricant o proveïdor proporciona per defecte. 802.11 incorpora un ventall de sistemes que permeten autenticar als usuaris i xifrar les dades:

- ***Ocultació de punt d'accés:*** Podem ocultar la publicació del nom del nostre punt d'accés. Només la gent que conegui el nom i els paràmetres correctes de la connexió podrà accedir-hi.

- ***Filtre MAC:*** A nivell d'enllaç podem definir en el nostre punt d'accés quines MAC tenen permís per accedir a la nostre xarxa.

- ***Wired Equivalent Privacy (WEP):*** Presentat l'any 1999 aquest sistema de xifrat pretenia proporcionar una confidencialitat comparable a la d'una xarxa tradicional amb fils. Proporciona un xifrat basat en l'algorisme RC4 mitjançant claus de 64 (clau de 40 bits més 24 bits de vector d'inici IV) o 128 bits (clau de 104 bits més 24 bits de vector d'inici IV). La llavor formada per clau i vector IV servirà per generar una seqüència més llarga de nombres pseudo-aleatoris que mitjançant una XOR xifraran el missatge en clar.

WEP permet connectar client i punt d'accés (AP) sense autenticació o mitjançat una clau compartida que el propi sistema WEP utilitza per a que el client respongui a un repte xifrant un missatge model que envia l'AP.

- **Wi-Fi Protected Access (*WPA):*** Creat per corregir les deficiències de WEP. En primer terme es va pensar per la utilització conjunta amb servidors d'autenticacions, como ara RADIUS, que distribueixen les claus entre els usuaris. Com en l'ús domèstic no és habitual disposar d'aquests servidors s'afegeix un mode anomenat clau precompartida o PSK (Pre-Shared Key). En aquest darrer mode els diversos actors entre una comunicació han intercanviat prèviament la clau a través d'una canal segur. WPA segueix utilitzant el sistema RC4 amb una clau de 128 bits i un vector IV de 48 bits. WPA incorpora el Protocol d'Integració de Clau Temporal (TKIP) que canvia les claus a mida que el sistema va funcionant. Això ens evita ser atacats mitjançant la recuperació estadística de claus als que WEP era vulnerable.

- *WPA2:* Mentre que WPA es pot considerar com a sistema de migració mentre es cercava una millora a WEP, podem dir que WPA2 és la versió certificada de l'estàndard de la IEEE basada en 802.11i. A la versió de clau pre-compartida se la coneix com a WPA2-Personal i a la versió amb autenticació definida a 802.1x/EAP com a WPA2-Enterprise. Amb l'alliberament de WPA2 els fabricants de la Wi-Fi Alliance varen començar a produir dispositius més potents capaços d'implementar l'algorisme AES (Advanced Encryption Standard) per tal d'assolir els requeriments de l'Administració americana.

4.1.3 Eines i mètodes d'atac

Moltes de les mesures de seguretat previstes per la Wi-Fi Alliance s'han anat demostrant ineficaces. Els models més senzills com l'ocultació del punt d'accés o el filtre de MAC són fàcilment explotables. En el primer cas només ens caldrà una targeta de xarxa capaç d'"escoltar" el medi, l'aire. Aquestes targetes operen en un mode anomenat "promiscu" o "monitor" que permet la recaptació de paquets tot i que elles no siguin les destinatàries legítimes. A més, permeten treballar en tots els canals Wi-Fi mitjançant salts en les freqüències. Aquestes paquets capturats duen informació com ara nom de la xarxa, MAC d'origen i destí. Tot i que la direcció MAC ha estat gravada a foc a les NIC, o targetes de xarxa, i no es poden modificar, a través del nostre sistema operatiu podem canviar la nostra MAC a nivell de software per tal de suplantar la identitat d'un altre ordinador a nivell d'enllaç.

El cas més flagrant és el de WEP, instaurant a 1999 sota un sistema de xifrat RC4 que ja s'havia demostrat vulnerable l'any 1995. L'any 2001 Scott Fluhrer, Itsik Mantin i Adi Shamir varen publicar un article on mostraven dues vulnerabilitats sobre WEP: debilitat de no-variació, que més tard es solucionarà amb TKIP, i vectors IV coneguts. Tots dos mètodes es basen en el fet que, per a certs valors de la clau, és possible que els bits en els bytes inicials del flux només depenguin d'uns pocs bits de la clau de xifrat, permetent un atac estadístic. Per dur a terme un atac sota aquest mètode cal un temps i una quantitat de tràfic considerable. David Hulton va idear un mètode optimitzat que permetia realitzar el mateix atacs amb menor quantitat de tràfic i, per tant, invertint menys temps. Més tard, amb la incorporació del mètode d'injecció de paquets, es va aconseguir millorar les fites anteriors reduint el temps d'un atac WEP a 10 minuts. Tot i

així varen existir intents de perpetuar WEP amb petites millores com ara WEP dinàmic, que afegia temporalitat a la clau, WEP2, que augmentava el nombre de bits de la clau o WEP Plus, que evitava l'ús de vectors IV dèbils. D'ençà que WEP es va demostrar del tot vulnerable va quedar relegat a un ús domèstic i ara només el trobem a les implementacions dels firmwares del encaminadors sense fils com a vestigi del que un dia va ser 802.11.

Pel que fa a WPA/WPA2, s'ha demostrat força vulnerable en el procés d'establiment de connexió o handshake entre AP i client, és a dir, en la seva configuració de clau pre-compartida (PSK), tant en AES com TKIP. Com que el procés vulnerable és la negociació, l'atac és el mateix tant per WPA com per WPA2. Aquesta és la única falla destacable, els desenvolupadors d'aplicacions que existeixen per explotar WPA/WPA2 recomanen no intentar un atac si no és sota PSK. Part de la dificultat afegida a WPA/WPA2 rau en la temporalitat de la clau, que no és estàtica com ara WEP, i en l'ús de diccionaris per explotar-la, que pot arribar a incrementar el temps d'atac d'una forma notable. L'eina més efectiva per realitzar l'atac de força bruta mitjançant diccionaris és *pyrit*, capaç d'utilitzar tota la capacitat de processament de la GPU o d'un processador multinucli.

WEP ha presentat tantes vulnerabilitats que s'han desenvolupats diversos mètodes que permeten explotar-les i treure en clar la clau d'accés o deduir el missatge en clar. WPA n'ha heretat algunes de les deficiències de WEP. Els mètodes més estesos per explotar aquests dos sistemes venen incorporats a la suite aircrack-ng:

- ***Deautenticació***: La finalitat d'aquest atac és generar paquets de deautenticació per forçar al client a identificar-se de nou i així poder capturar les dades que s'intercanvien en el procés d'establiment o handshake de WPA i WPA2.

- ***Falsa autenticació:*** Permet realitzar els dos tipus d'autenticació WEP, obert o amb clau pre-compartida, i associar-se amb el punt d'accés. És útil quan necessitem una direcció MAC associada per utilitzar-la en algun dels altres atacs i no trobem cap client actiu.

- ***Reenviament de paquets:*** Ens permet escollir el paquet a reenviar. Aquest mètode ens permet obtenir paquets per dues vies. La primera és capturant-los. La segona és fent

servir un arxiu cap que contingui paquets mostres que hem obtingut anteriorment o que hem generat amb software com ara packetforge-ng.

- ***Enverinament ARP:*** Permet generar sol·licitud ARP, un protocol que permet esbrinar la direcció MAC donada una IP, com a client legítim amb la finalitat d'incrementar el tràfic que en altres condicions requeririen més temps d'assolir. La generació de nous paquets és la forma més efectiva de generar nous vectors IV.

- ***Chop-chop:*** Aquest atac és basa en la integritat implementada mitjançant el CRC-32 de la trama 802.11. L'atacant modifica un bit del paquets i el torna a injectar al medi. Depenent de la resposta del punt d'accés, si el descarta o si l'accepta, l'atacant podrà deduir el valor del text en clar abans de ser xifrat pel XOR. És per això que es diu que aquest mètode retorna el text en clar sense necessitat de conèixer la clau.

- ***Atac de fragmentació:*** Semblant a chop-chop, no recupera la clau WEP, si no que mitjançant diversos reenviaments de paquets va recopilant informació que servirà per deduir el text en clar.

La suite aircrack-ng conté bàsicament tres programes bàsics que permeten explotar WEP i WPA/WPA2:

- ***Airodump-ng***: Permet escoltar i desar en un fitxer .cap els paquets que la targeta de xarxa sense fils escolta en mode monitor. Permet especificar quines MAC o canals vol escoltar i desar.

- ***Aireplay-ng:*** És l'encarregat del reenviament de paquets, ens permetrà generar més tràfic per què ho pugui escoltar airodump-ng.

- ***Aircrack-ng:*** Rep el mateix nom que la suite genèrica. La seva tasca és el tractament del fitxer .cap que hem generat amb airodump-ng per tal de desxifrar la clau WEP o WPA/WPA2.

Existeixen altres utilitats com la ja esmentada packetforge-ng que permet generar paquets a nivell d'enllaç, xarxa o transport introduint els camps desitjats o a partir d'un paquet model. També cal esmentar una eina de gran utilitat com ara Kismet, que ens proporciona una gran quantitat d'informació de les xarxes que és capaç de detectar la

nostra NIC en mode promiscu, com ara MAC de punts d'accés, MACs de clients associats, IPs, potència del senyal, taxa de dades i tipus de xifrat.

Totes aquestes aplicacions i més estan incloses a BackTrack, com les ja esmentades a RFID i Bluetooth, la distribució GNU/Linux especialitzada en auditories de seguretat. Tot i així, pel que fa a 802.11, disposem d'altres versions GNU/Linux més lleugeres i especialitzades exclusivament en la tecnologia Wi-Fi, com ara Wifiway o Wifislax.

Un darrer cas digne d'estudi són els routers que els principals proveïdors de serveis ofereixen als seus clients. Aquests operadors, amb una extensa quota de mercat, incorporen claus per defecte que han estat generades mitjançant un senzill algorisme que rep com a entrada el nom de la xarxa i l'adreça MAC del punt d'accés. Existeixen aplicacions molt lleugeres executables a smartphones amb Wi-Fi que permeten recaptar aquests dos paràmetres i generar la mateixa clau que el dispositiu du configurada per defecte.

4.1.4 Contramesures

Tot i que el panorama Wi-Fi sembla tan desolador com RFID i Bluetooth el cert és que no està tot perdut. Molts dels atacs esmentats tenen patrons de comportament, com ara un reenviament molt ràpid de paquets erronis o paquets molt petits. Els fabricants han estudiat aquestes característiques i han implementat en el seu firmware mecanismes de detecció i de la majoria d'aquests atacs coneguts. Algunes mesures poden ser la desconnexió d'un client o ometre paquets si aquets emet dos paquets erronis en menys de 60 ms. o reduir la vida de la clau pseudo-aleatòria a 2 minuts.

Òbviament, es descarta l'ús de WEP en qualsevol de les seves modalitats. Tot i que fa uns anys la migració a WPA i, sobretot, a WPA2 era impossible per la incompatibilitat amb alguns dispositius antics, avui dia no existeix cap excusa que ens obligui a l'ús de WEP.

Mentre que en l'entorn domèstic es recomana utilitzar WPA2 amb una clau llarga que contingui caràcters especials, en entorns empresarials s'ha demostrat que el més adequat són solucions del tipus servidors RADIUS o Active Directory, elements de confiança, interns i segurs que gestionen les claus dels usuaris.

Altres opcions que permeten un accés de forma més segura les trobarem si escalem per la pila OSI, com ara les VPN a nivell de xarxa. També ens serà d'utilitat disposar de registres o logs que pot generar el punt d'accés per tenir sota control els intents d'accés no autoritzats.

4.1.5 Cas pràctic: WPA2-PSK

Tot seguit mostrarem un exemple d'atac vers WPA2-PSK, és a dir, amb clau precompartida. En aquest exemple treballarem sota la darrera distribució BackTrack 5 de 64 bits. El primer pas serà configurar la nostra targeta per canviar-la a estat "monitor", només les targes amb chipset Atheros i Prisma ho permeten, per tal d'escoltar tot el tràfic Wi-Fi proper. La nostra tarja 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 tarja actuarà per defecte mitjançant salts de freqüència. En cas de voler configurar el mode monitor amb un canal concret l'ordre serà:

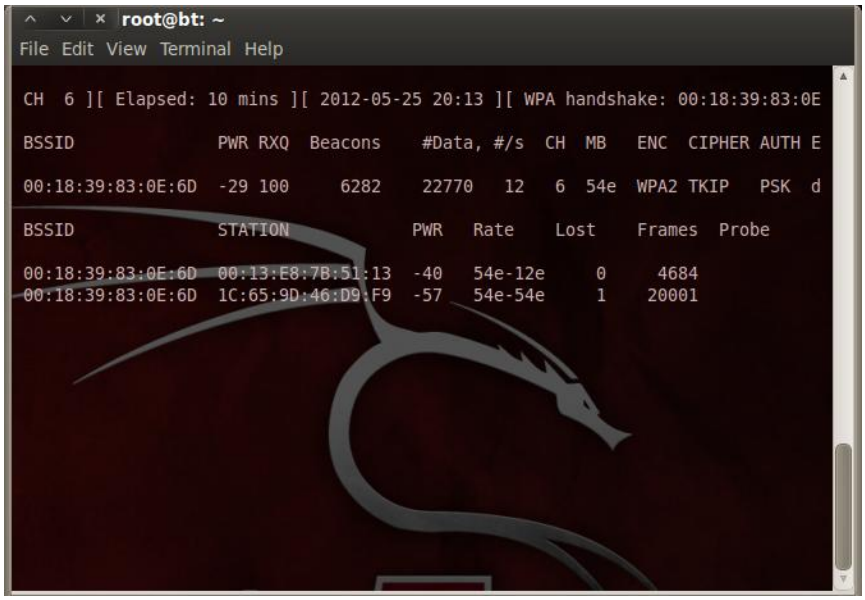
$ iwconfig wlan0 mode monitor channel 6

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 el mètode d xifrat i 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 del 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

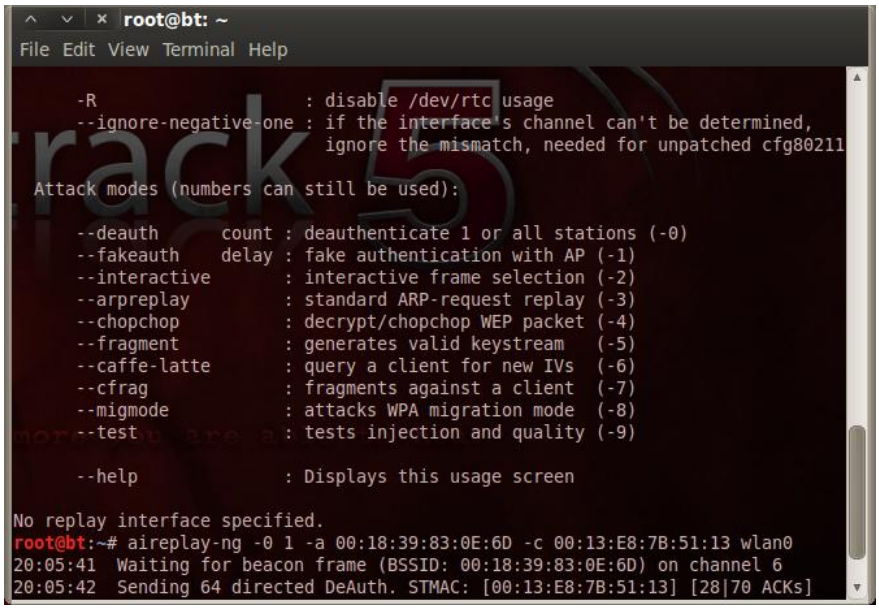
La opció -c defineix el canal, bssid la MAC del AP, -w escriu un nou arxiu anomenat psk amb extensió cap que haurem de tractar més endavant. El darrer paràmetre fa referència a quina de les nostres targes utilitzarem en cas que tinguem més d'una. La següent imatge ens mostra l'aspecte d'aquesta execució.



Ara ja estem agafant 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 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. 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'interface que utilitzarem, wlan0.

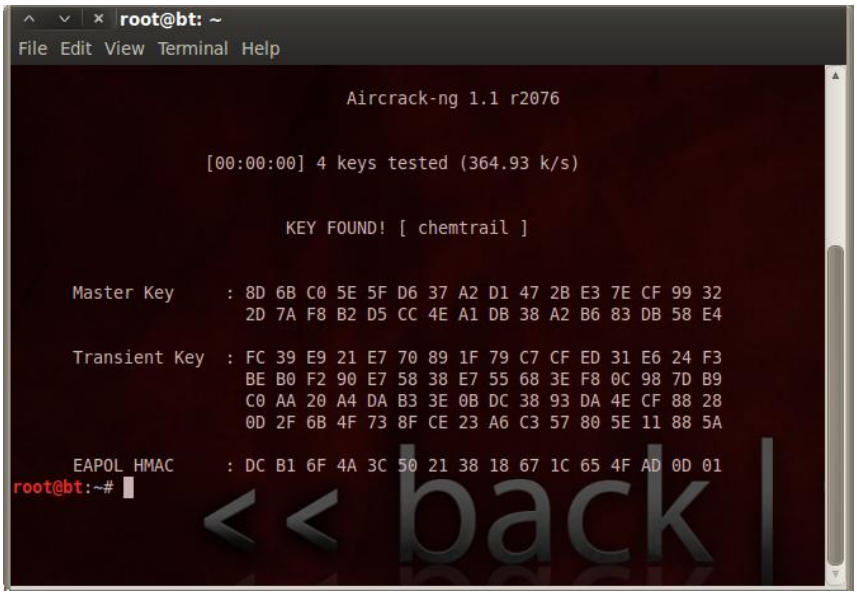


Enviats els paquets de reautenticació i captat el procés de negociació ja podrem iniciar l'atac sobre les dades obtingudes. Aquí és on rau la veritable dificultat de WPA2 ja que l'atac sobre els sistemes de xifrat TKIP o AES, a diferència del WEP basat en RC4, s'ha de realitzar mitjançant força bruta. 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 de la següent manera:

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

On –w selecciona el diccionari, es pot fer mitjançant la ruta completa del sistema, -b el MAC de l'AP i el darrer terme 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.



Aircrack-ng ens proporciona en el nostre cas unes taxes que ronden les 1000 claus/s. 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 5000 claus/s.

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 $62^{10} = 839.299.365.868.340.224$ possibles claus. Si ,com en el millor dels casos, podem assolir una capacitat de processament de 5000 claus/s trigaríem poc més de cinc milions d'anys en testejar totes les possibles combinacions.

5. Estudi de costos

Fins aquí ja hem realitzar un estudi general de la seguretat en les tecnologies RFID, Bluetooth i Wi-Fi. Les eines, software i hardware, que caldrien per realitzar una auditoria en aquestes tres tecnologies són:

- Portàtil o ordinador de sobretaula: ~700 €
- Kit lectura/escriptura RFID: ~70 €
    - Exemple: RFID 125 KHz Arduino Pack: 67 € a Cooking Hacks

En el cas que el nostre equip portàtil o sobretaula no estigui equipat amb targetes Bluetooth o Wi-Fi:

- Clau USB Bluetooth: ~10 €
    - Exemple: Belkin Bluetooth Adapter 2.1 EDR per 13 € a Life
- Clau USB o targeta PCI Wi-FI amb xip Atheros o Prisma: ~20 €
    - Exemple: D-Link AirPlus G DWL-G510 per 18,56 € a Life

A més, destaquem que totes les eines que hem anat esmentat al llarg del treball es troben sota llicència GNU o GPL i es poden descarregar de franc. Cal tornar a esmentar la importància de la distribució GNU/Linux BackTrack 5.0 ja que incorpora una gran ventall d'eines especialitzades en l'auditoria de seguretat, no només en les tecnologies que hem tractat. Per tant, per menys de 1000 € podem tenir tots els components necessaris per començar a realitzar tasques d'auditoria.

6. Conclusions

Al llarg d'aquest treball hem pogut veure quines solucions de seguretat s'han implementat en les diverses tecnologies.

En primer lloc hem vist les RFID amb els sistemes de seguretat poc definits. La tecnologia RFID, per la seva naturalesa presenta un gran discurs en relació amb la privacitat dels seus usuaris i l'ús que en fan altres actors de la informació. Tot i que, com s'ha vist, RFID presenta algunes falles de seguretat, el cert és que s'han presentat solucions i propostes per a canviar els estàndards, com ara la comanda KILL, que obren un camí cap a un ús més segur i responsable d'aquesta tecnologia.

Seguidament hem vist com Bluetooth ha esdevingut vulnerable sobretot per males implementacions dels fabricants. Algunes de les causes de la passivitat d'aquestos és que Bluetooth ja es presentava com un protocol robust al incorporar sistemes de seguretat en el seu estàndard.

Finalment, el cas de Wi-Fi ens ha mostrat com els primers intents de xifrat mitjançant WEP ràpidament es van demostrar ineficaços. Des dels inicis Wi-Fi ha estat fiable, però gràcies a solucions d'altres nivells, algunes només disponibles en el món empresarial como ara els servidors RADIUS o l'ús de VPNs. No ha estat fins l'arribada de WPA2 que aquesta tecnologia ha arribat a ser segura per si mateixa. En el cas pràctic hem vist com actualment el temps necessari per realitzar un atac de força bruta és inviable en termes de temps.

En tots els casos, també en altres protocols i estàndards, la seguretat és un aspecte que sempre s'ha millorat un cop els protocols es posen en mans de gent d'arreu. Per tant, en general, la sensació que hom se'n pot endur si repassa l'evolució d'aquests protocols és que la seguretat és un dels aspectes menys cuidats quan neix una nova tecnologia.

7. Bibliografia

Wikipedia. "Red inalámbrica". [article en línia]. <http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica>

Wikipedia. "WPAN". [article en línia]. <http://es.wikipedia.org/wiki/WPAN>

Wikipedia. "ISO 14443". [article en línia]. <http://es.wikipedia.org/wiki/ISO_14443>

Wikipedia. "NFC". [article en línia]. < http://en.wikipedia.org/wiki/Near_field_communication>

Wikipedia. "ZigBee". [article en línia]. < http://en.wikipedia.org/wiki/ZigBee>

L. Garfinkel, Simson. (2005, 5 de October). "RFID Security and Privacy". [document PDF]. <http://simson.net/ref/2005/rfid-oecd.pdf>

AEPD (2010, de Maig). "Guía sobre seguridad y privacidad de la tecnología RFID". [document PDF]. <https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/julio/Guia_RFID.pdf>

Atmel. "Understanding the Requirements of ISO/IEC 14443 for Type B Proximity Contactless Identification Cards". [document PDF]. <http://www.atmel.com/Images/doc2056.pdf>

Wikipedia. "Código Electrónico de Producto". [article en línia]. <http://es.wikipedia.org/wiki/C%C3%B3digo_electr%C3%B3nico_de_producto>

GS1. "GS1 EPC Tag Data Standard 1.6". [document PDF]. <http://www.gs1.org/gsmp/kc/epcglobal/tds/tds_1_6-RatifiedStd-20110922.pdf>

Wikipedia. "Radio-frequency identification". [article en línia]. <http://en.wikipedia.org/wiki/Radio-frequency_identification>

Bridge-Project. "White Paper - RFID Tag Security". [document PDF]. <http://www.bridge-project.eu/data/File/BridgesecuritypaperDL_9.pdf>

Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, Ted Phillips. (2007, de Abril). National Institute of Standards and Technology. "Guidelines for Securing Radio Frequency Identification (RFID) Systems". [document PDF]. <http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf>

Heiko Knospe, Hartmut Pohl. Hochschule Bonn-Rhein-Sieg. "RFID Security". [document PDF]. <http://www.inf.h-brs.de/informatikmedia/Downloads/Personen/pohl/Aufsaetze/Pohl_Knospe_RFID_Security_050126.pdf>

RFDump. "What is RFDump". [article en línia]. <http://www.rfdump.org/about.shtml>

Cooking hacks. "ARDUINO RFID PACK". [botiga on-line]. <http://www.cooking-hacks.com/index.php/arduino-rfid-pack.html>

Wikipedia. "Bluetooth". [article en línia]. <http://es.wikipedia.org/wiki/Bluetooth>

Wikipedia [ENG]. "Bluetooth". [article en línia]. <http://en.wikipedia.org/wiki/Bluetooth>

Wikipedia [ENG]. "Bluetooth profiles". [article en línia]. <http://en.wikipedia.org/wiki/Bluetooth_profile>

Wikipedia. "802,15". [article en línia]. <http://es.wikipedia.org/wiki/IEEE_802.15>

Wikipedia [ENG]. "E0" (cipher). [article en línia]. <http://en.wikipedia.org/wiki/E0_(cipher)>

Becker, Andrea. (2007, 16 de Abril). Bluetooth Security and Hacks. "Bluetooth Security". [document PDF]. <http://gsyc.es/~anto/ubicuos2/bluetooth_security_and_hacks.pdf>

Karen Scarfone, John Padgette. (2008, de Setembre). National Institute of Standards and Technology. "Guide to Bluetooth Security". [document PDF]. <http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf>

Moreno Tablado, Alberto. (2006, de Juny). Seguridad Mobile. "Seguridad en Bluetooth". [document PDF]. <http://www.seguridadmobile.com/Files/PFC.Seguridad.en.Bluetooth.pdf>

Yaniv Shaked, Avishai Wool. (2005, 5 de Febrer)." Cracking the Bluetooth PIN". [article en línia]. <http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05>

Wikipedia [ENG]. "Wireless LAN". [article en línia]. <http://en.wikipedia.org/wiki/Wireless_LAN>

Wikipedia. " Red de área local inalámbrica". [article en línia]. <http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local_inal%C3%A1mbrica>

Wikipedia. " IEEE 802.11". [article en línia]. <http://es.wikipedia.org/wiki/IEEE_802.11>

Wikipedia [ENG]. " IEEE 802.11". [article en línia]. <http://en.wikipedia.org/wiki/IEEE_802.11>

Wikipedia. " Wi-Fi". [article en línia]. <http://es.wikipedia.org/wiki/Wi-Fi>

Wikipedia. " Wired Equivalent Privacy". [article en línia]. <http://es.wikipedia.org/wiki/WEP>

Wikipedia. " Wi-Fi Protected Access". [article en línia]. <http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access>

Nikita Borisov, Ian Goldberg i David Wagner. " Security of the WEP algorithm". [article en línia]. <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

Guillaume Lehembre. (2006) Hakin9. " Seguridad Wi-Fi – WEP, WPA y WPA2". [document PDF]. <http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf>

Joshua Wright.(2008) Inguardians.com " Understanding the WPA/WPA2 break". [document PDF]. < http://www.willhackforsushi.com/presentations/TKIP_Attack_Webcast_2008-11-17.pdf>

Glenn Fleishman.(2008, 7 de Novembre) Arstechnica.com " Battered, but not broken: understanding the WPA crack". [article en línea]. <http://arstechnica.com/security/2008/11/wpa-cracked/>

Aircrack-ng.org.(2009, 14 d'Agost) "Aireplay-ng". [article en línea]. <http://www.aircrack-ng.org/doku.php?id=es:aireplay-ng>

Aircrack-ng.org.(2007, 16 de Maig) "Tutorial: Como crackear WPA/WPA2". [article en línea]. <http://www.aircrack-ng.org/doku.php?id=es:cracking_wpa&s[]=wpa2>

Pyrit. "Pyrit". [article en línea]. < http://code.google.com/p/pyrit/>

8. Annexos

8.1 A Hacker's Guide To RFID

Of all the things that radio frequency identification technology was supposed to do for retailers--simplifying inventory management and supply chain issues, for instance--creating a new type of theft wasn't one of them. But that is exactly what could happen, and a German information security consultant can prove it. Consider the following scenario.

A would-be scofflaw heads into a grocery store where all the products have RFID tags on them. Rather than paying $7 for a bottle of shampoo, he'd rather pay $3. To make that happen, he whips out a PDA equipped with an RFID reader and scans the tag on the shampoo. He replaces that information with data from the tag on a $3 carton of milk and uploads it to the shampoo bottle tag. When he reaches the check-out stand--which just happens to be automated--he gets charged $3 instead of $7, with the store's computer systems none the wiser.

Lukas Grunwald, the German consultant, says this is not only possible, he's done it. That is, he's changed the information on the RFID tag. He didn't actually steal anything. To prove his point and let others learn about RFID tag security, he's created a free software program called RFDump that is the result of a few years of research into RFID. He presented his findings and announced the release of the software at the Black Hat Security Briefings conference in Las Vegas today.

"There is a huge danger to customers using this technology, if they don't think about security," Grunwald says.

This kind of disclosure--complete with a software release that could potentially be misused--is not unusual for Black Hat, a gathering where IT security pros talk frankly about the latest in computer security problems and how to solve them. But don't put your Luddite hat back on just yet.

Companies like Wal-Mart Stores (nyse: WMT - news - people) andTarget (nyse: TGT - news - people) are slowly embracing RFID as the next great boost to their supply chains. But they, like most companies, aren't yet tagging individual items, which is what Grunwald hacked at a store belonging to the Metro retail chain. Instead, they are putting

RFID tags only on large cases and shipping pallets until the cost of item-level tagging comes down. A Wal-Mart spokesman says there is no price information on its pallet tags.

Albrecht Truchsess, a spokesman for Metro, says the company is now creating item-level tags for three products: cream cheese from Kraft Foods (nyse: KFT - news - people), Pantene Shampoo from Procter & Gamble (nyse: PG - news - people) and razor blades from Gillette(nyse: G - news - people). He also says that since the tags are being tested only at Metro's Future Store, a demonstration project bringing together several new retail technologies, their security isn't strong by design.

"What we're doing in the Future Store is using the RFID tags for smart-shelf applications," says Truchsess, referring to shelves that track what has been placed on them. "And the sort of tags we're using are very basic. It's really just a test right now."

Metro expects it will take ten years or more before all store items have their own RFID tags on a regular basis. "The ones we're using now cost about 30 or 40 cents each," says Truchsess. "More secure tags are too expensive right now."

Pete Abell, an RFID consultant at Boston-based EPCGroup, says that as stores adopt the technology beyond the test phase, any shopper who brought his own RFID reader into a store would likely be detected. Secondly, he says, tags on products would be programmed to respond only to authorized readers. Finally, he says, the industry is working on stronger encryption than what is available now. "Currently there's only 8-bit encryption available, and that is pretty easy to get around," he says. "And in this case I doubt even that was in place."

Arik Hesseldahl. (2004, 29 de Juliol), Forbes," A Hacker's Guide To RFID". [article on-line] <http://www.forbes.com/2004/07/29/cx_ah_0729rfid.html>

8.2 Phone pirates in seek and steal mission

MOBILE phone technology is being used by thieves to seek out and steal laptops locked in cars in Cambridgeshire.

Up-to-date mobiles often have Bluetooth technology, which allows other compatible devices, including laptops, to link up and exchange information, and log on to the internet. But thieves in Cambridge have cottoned on to an alternative use for the function, using it as a scanner which will let them know if another Bluetooth device is locked in a car boot.

Det Sgt Al Funge, from Cambridge's crime investigation unit, said: "There have been a number of instances of this new technology being used to identify cars which have valuable electronics, including laptops, inside.

"The thieves are taking advantage of a relatively new technology, and people need to be aware that this is going on. We would urge people not to leave laptops, or anything of value, in their cars, and always de-activate these wireless connections when you're not using a laptop - otherwise you're making life easy for the thieves."

Last month a spate of thefts from cars were put down to thieves using their phones to find laptops after three laptops were stolen from cars parked in neighbouring bays at the Holiday Inn, in Cambridge Road, Impington.

Police in Royston have mirrored the warning, after picking up on new crime trends in the area. Superintendent Adrian Walter said: "The car industry has done a lot of work in recent years to make vehicles theft proof, including building in stereos and we're glad to say the majority of people seem to be taking our advice and keeping valuables out of sight.

"However, we must not be complacent and by following simple crime prevention methods we can all help to keep vehicle crime down in the area." The call for caution follows the latest in a string of thefts from cars in Royston.

At about 8.20am last Wednesday, a Sony TR 1MP laptop was taken from an Audi A6 estate parked in Tesco car park off old North Road. Anyone with any information can call police on (01992) 533002 or Crimestoppers on 0800 555 111.

Cambridge Evening News. (2005, 27 d'Agost). "Phone pirates in seek and steal mission". [article on-line].
<http://web.archive.org/web/20070717035938/http://www.cambridge-news.co.uk/news/region_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf>