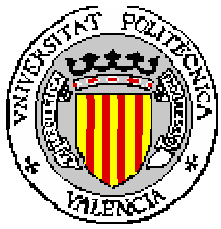
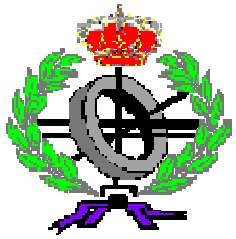
UNIVERSIDAD POLITÉCNICA DE VALENCIA

Escuela Técnica Superior de Ingeniería Informática





Seguridad WIFI. Agresiones posibles

PROYECTO FINAL DE CARRERA

Realizado por:

Miguel Iniesta Archidona

Dirigido por:

Juan Vicente Oltra Gutiérrez

Valencia, 24 de junio de 2010

Índice

1. Introducción

1.1 Resumen

En este trabajo se realiza una recopilación sobre distintos aspectos de la arquitectura para redes basada en la tecnología WiFi. Centrándose esta tanto en el campo de la seguridad en este tipo de redes como en las principales técnicas de hacking existentes para conseguir vulnerarla.

Esta recopilación comienza abordando los aspectos más generales de la propia arquitectura WiFi para los más inexpertos en la materia, a partir de ahí se centra en todos aquellos mecanismos y protocolos existentes para aumentar la seguridad de la misma, indicando cuales son los puntos fuertes y los puntos a mejorar en cada uno de ellos. Y finalmente intenta orientar sobre algunas técnicas de hacking wireless, pero no a modo de pasos a seguir para conseguir Internet de manera gratuita, sino con el objetivo de intentar hackear nuestra propia red y ver que nivel de seguridad tenemos frente a usuarios más avanzados.

Para esta recopilación se han empleado tanto conocimientos teóricos sobre la materia como experiencias y consejos de gran valor de muchos usuarios de este tipo de redes, cuyo fin no es ni más ni menos que orientar a las personas menos duchas en la materia. También se ha incluido algún estudio relacionado con la seguridad de las redes en la actualidad.

1.2 Motivación

El uso de redes WiFi, según diversos estudios, no hace más que aumentar con el paso de los años. Esto puede ser debido entre otras cosas a su facilidad de instalación frente al tipo de redes cableadas. También hemos de tener en cuenta que nos ofrecen una amplia movilidad comparada con la limitación que nos suponía anteriormente el tener que estar cerca de un cable de red si queríamos conseguir conexión a Internet o simplemente montar nuestra propia red local.

Sin embargo, no todo supuso ventajas con la aparición de esta nueva tecnología. La más importante y que a día de hoy sigue dando mucho que hablar es la seguridad. Se ha demostrado a lo largo de todo este tiempo que no hay una red WiFi 100% segura, todos los mecanismos o protocolos existentes tienen sus vulnerabilidades, si bien es posible lograr unos niveles de seguridad más que aceptables con las medidas de que dispones en la actualidad.

Es por eso que este trabajo busca precisamente orientarse hacia el campo de la seguridad, tratando de servir de base o guía a usuarios menos avanzados. Dado que este grupo de usuarios puede considerarse como la mayoría de la población, parece muy interesante y de gran valor todo lo que esta recopilación pueda aportar.

Por otra parte pueden ser interesantes varios aspectos teóricos que a lo largo del trabajo van apareciendo como introducción a estudiar diversas prevenciones o vulnerabilidades de las redes WiFi. Aunque no es la principal motivación de este.

La motivación se podría resumir como el intentar servir de ayuda a usuarios que tengan interés por tener una red segura más y no sepan por donde empezar o simplemente tengan curiosidad por ello.

1.3 Objetivos

Los objetivos que persigue este proyecto son, por tanto, introducir al lector en el mundo de las redes WiFi explicando las generalidades de las mismas, hacer un repaso de las debilidades y vulnerabilidades de los diversos protocolos y por último dar a conocer una serie de técnicas básicas orientadas al hacking wireless.

Podríamos dividirlo en tres partes claramente diferenciadas según los objetivos que persiguen:

- En una primera parte, se intenta dar a conocer las principales características de las redes WiFi, centrándonos en los aspectos más generales y relevantes para su comprensión.

- En una segunda parte, se tratan todos aquellos mecanismos y protocolos que nos ayudan en la materia de la seguridad de estas, centrándonos en cuales son las principales ventajas y desventajas que nos aporta cada uno de estos.

- Finalmente, a modo de orientación y no como guía, se explican una serie de técnicas de hacking wireless sobre el sistema operativo más extendido y el protocolo más utilizado en la actualidad. Se hace sobre estas premisas para que sirva a la mayor parte de los usuarios.

Con todo esto, como anteriormente hemos citado, lo que se persigue o se intenta conseguir es una completa recopilación de información acerca de la seguridad en redes inalámbricas y que esta pueda tener la utilidad de conseguir que una red sea más segura para los usuarios que así lo deseen.

1.4 Organización

La memoria de este proyecto se organiza de la siguiente manera:

En el capítulo 2, se explican las generalidades de una red WiFi con el objetivo de que el lector se familiarice con una serie de términos que serán utilizados a lo largo de todo el trabajo.

En el capítulo 3, se describen los principales protocolos de seguridad existentes y algunas medidas generales para evitar el acceso ajeno a una red WiFi.

En el capítulo 4, nos centramos en el protocolo de seguridad más extendido en redes WiFi, el protocolo WEP. Se explicará cada uno de los elementos de su arquitectura así como las debilidades que presenta y como puede ser vulnerado.

En el capítulo 5, se trata de analizar el protocolo se seguridad WPA, llamado a ir sustituyendo gradualmente al protocolo WEP. Incidiremos en las mejoras que este

aporta frente a su antecesor y en la necesidad de ir adaptando las redes WiFi a este protocolo.

Por último, en el capítulo 6, se recopilan las principales técnicas utilizadas para romper la seguridad de una red WiFi bajo Windows y con la seguridad del protocolo WEP, todo ello por ser los sistemas más extendidos en la actualidad.

2. Aspectos generales de una arquitectura WiFi

2.1 Introducción a Wi-Fi

Aunque hace bastante tiempo que existen las comunicaciones de red inalámbricas, existía un grave problema de incompatibilidades, ya que prácticamente cada fabricante usaba un estándar diferente.

Por este motivo, en 1999 varias empresas (las principales del sector de las comunicaciones y redes, como 3com, Airones Intersil, Lucent Technologies, Nokia y Symbol Technologies) crean la WECA (Wireless Ethernet Compability Aliance), actualmente Wi-Fi Alliance [1].

Esta asociación se encarga de certificar los diferentes estándares, así como su compatibilidad.

En el año 2000 certifica la interoperatividad (es decir, que puedan operar entre ellos) de equipos bajo la especificación IEEE 802.11b, a la que denomina Wi-Fi. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos.

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red Wi-Fi de una red Ethernet es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (Ethernet).

Esta denominación por extensión se utiliza para todas las especificaciones posteriores basadas en el estándar 802.11x de comunicaciones inalámbricas.

A los dispositivos certificados por la Wi-Fi Alliance se les permite usar este logotipo:

Con Wi-Fi se pueden crear redes de área local inalámbricas de alta velocidad siempre y cuando el equipo que se vaya a conectar no esté muy alejado del punto de acceso. En la práctica, Wi-Fi admite ordenadores portátiles, equipos de escritorio, asistentes digitales personales (PDA) o cualquier otro tipo de dispositivo de alta velocidad con propiedades de conexión también de alta velocidad (11 Mbps o superior) dentro de un radio de varias docenas de metros en ambientes cerrados (de 20 a 50 metros en general) o dentro de un radio de cientos de metros al aire libre.

Los proveedores de Wi-Fi están comenzando a cubrir áreas con una gran concentración de usuarios (como estaciones de trenes, aeropuertos y hoteles) con redes inalámbricas. Estas áreas se denominan "zonas locales de cobertura" [2].

2.2 Estándares existentes

El estándar 802.11 en realidad es el primer estándar y permite un ancho de banda de 1 a 2 Mbps. El estándar original se ha modificado para optimizar el ancho de banda (incluidos los estándares 802.11a, 802.11b y 802.11g, denominados estándares físicos 802.11) o para especificar componentes de mejor manera con el fin de garantizar mayor seguridad o compatibilidad. La tabla a continuación muestra las distintas modificaciones del estándar 802.11 y sus significados:

Nombre del estándar	**Nombre**	**Descripción**
802.11a	Wifi5	El estándar 802.11a (llamado WiFi 5) admite un ancho de banda superior (el rendimiento total máximo es de 54 Mbps aunque en la práctica es de 30 Mpbs). El estándar 802.11a provee ocho canales de radio en la banda de frecuencia de 5 GHz.
802.11b	WiFi	El estándar 802.11b es el más utilizado actualmente. Ofrece un rendimiento total máximo de 11 Mpbs (6 Mpbs en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto. Utiliza el rango de frecuencia de 2,4 GHz con tres canales de radio disponibles.
802.11c	Combinación del 802.11 y el 802.1d	El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos).
802.11d	Internacionalización	El estándar 802.11d es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
802.11e	Mejora de la calidad del servicio	El estándar 802.11e está destinado a mejorar la calidad del servicio en el nivel de la capa de enlace de datos. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo.
802.11f	Itinerancia	El 802.11f es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario

		itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.
802.11g		El estándar 802.11g ofrece un ancho de banda elevado (con un rendimiento total máximo de 54 Mbps pero de 30 Mpbs en la práctica) en el rango de frecuencia de 2,4 GHz. El estándar 802.11g es compatible con el estándar anterior, el 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.
802.11h		El estándar 802.11h tiene por objeto unir el estándar 802.11 con el estándar europeo (HiperLAN 2, de ahí la h de 802.11h) y cumplir con las regulaciones europeas relacionadas con el uso de las frecuencias y el rendimiento energético.
802.11i		El estándar 802.11i está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el AES (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.
802.11Ir		El estándar 802.11r se elaboró para que pueda usar señales infrarrojas. Este estándar se ha vuelto tecnológicamente obsoleto.
802.11j		El estándar 802.11j es para la regulación japonesa lo que el 802.11h es para la regulación europea.
802.11k		El 802.11k ayuda a gestionar las redes. El estándar IEEE 802.11k permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN, mejorando así su gestión.
802.11m		El estándar 802.11m ha sido propuesto para el mantenimiento de las redes inalámbricas.
802.11n		El estándar 802.11n trabaja tanto en la banda de 2.4GHz como en la de 5GHz, que es mucho más estable y segura, pero de momento mucho más cara de implementar. Además aumenta la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps.

También es importante mencionar la existencia de un estándar llamado "802.11b+". Éste es un estándar patentado que contiene mejoras con respecto al flujo de datos. Por otro lado, este estándar tiene algunas carencias de interoperabilidad debido a que no es un estándar IEEE [3].

2.3 Modos de funcionamiento

Existen varias clases de hardware que se pueden utilizar para implementar una red inalámbrica WiFi:

- Los adaptadores inalámbricos o controladores de la interfaz de red (en inglés wireless adaptaters o network interface controller, abreviado NIC) son tarjetas de red que cumplen con el estándar 802.11 que les permiten a un equipo conectarse a una red inalámbrica. Los adaptadores inalámbricos están disponibles en diversos formatos, como tarjetas PCI, tarjetas PCMCIA, adaptadores USB y tarjetas de memoria Flash. Una estación es cualquier dispositivo que tenga este tipo de tarjeta.

- Los puntos de acceso (abreviado PA y a veces denominados zonas locales de cobertura) pueden permitirles a las estaciones equipadas con WiFi cercanas acceder a una red conectada a la que el punto de acceso se conecta directamente.

El estándar 802.11 define dos modos operativos:

- El modo de infraestructura en el que los clientes de tecnología inalámbrica se conectan a un punto de acceso. Éste es por lo general el modo predeterminado para las tarjetas 802.11b.

- El modo ad-hoc en el que los clientes se conectan entre sí sin ningún punto de acceso.

2.3.1 Modo de infraestructura

En el modo de infraestructura, cada estación informática (abreviado EST) se conecta a un punto de acceso a través de un enlace inalámbrico. La configuración formada por el punto de acceso y las estaciones ubicadas dentro del área de cobertura se llama conjunto de servicio básico o BSS. Estos forman una célula. Cada BSS se identifica a través de un BSSID (identificador de BSS) que es un identificador de 6 bytes (48 bits). En el modo infraestructura el BSSID corresponde al punto de acceso de la dirección MAC.

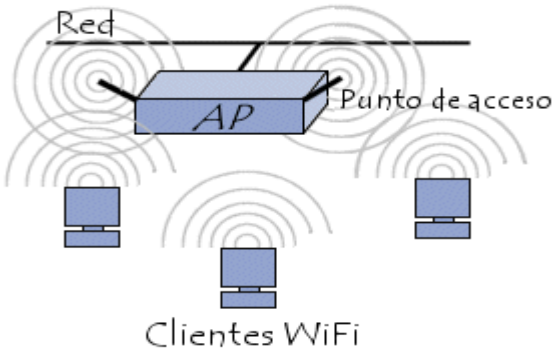


FIGURA 1. Modo infraestructura con un PA

Es posible vincular varios puntos de acceso juntos (o con más exactitud, varios BSS) con una conexión llamada sistema de distribución (o SD) para formar un conjunto de servicio extendido o ESS. El sistema de distribución también puede ser una red conectada, un cable entre dos puntos de acceso o incluso una red inalámbrica.

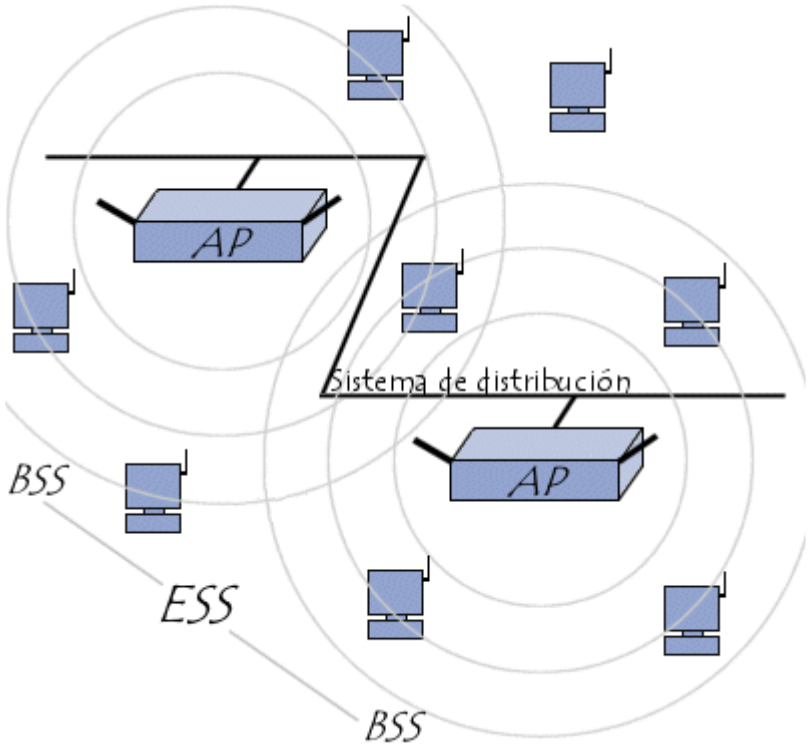


FIGURA 2. Modo infraestructura con varios PA

Un ESS se identifica a través de un ESSID (identificador del conjunto de servicio extendido), que es un identificador de 32 caracteres en formato ASCII que actúa como su nombre en la red. El ESSID, a menudo abreviado SSID, muestra el nombre de la red y de alguna manera representa una medida de seguridad de primer nivel ya que una estación debe saber el SSID para conectarse a la red extendida.

Cuando un usuario itinerante va desde un BSS a otro mientras se mueve dentro del ESS, el adaptador de la red inalámbrica de su equipo puede cambiarse de punto de acceso, según la calidad de la señal que reciba desde distintos puntos de acceso. Los puntos de acceso se comunican entre sí a través de un sistema de distribución con el fin de intercambiar información sobre las estaciones y, si es necesario, para transmitir datos desde estaciones móviles. Esta característica que permite a las estaciones moverse "de forma transparente" de un punto de acceso al otro se denomina itinerancia.

Comunicación con un punto de acceso

Cuando una estación se une a una célula, envía una solicitud de sondeo a cada canal. Esta solicitud contiene el ESSID que la célula está configurada para usar y también el volumen de tráfico que su adaptador inalámbrico puede admitir. Si no se establece ningún ESSID, la estación escucha a la red para encontrar un SSID.

Cada punto de acceso transmite una señal en intervalos regulares (diez veces por segundo aproximadamente). Esta señal, que se llama señalización, provee información de su BSSID, sus características y su ESSID, si corresponde. El ESSID se transmite automáticamente en forma predeterminada, pero se recomienda que si es posible se deshabilite esta opción.

Cuando se recibe una solicitud de sondeo, el punto de acceso verifica el ESSID y la solicitud del volumen de tráfico encontrado en la señalización. Si el ESSID dado concuerda con el del punto de acceso, éste envía una respuesta con datos de sincronización e información sobre su carga de tráfico. Así, la estación que recibe la respuesta puede verificar la calidad de la señal que envía el punto de acceso para determinar cuán lejos está. En términos generales, mientras más cerca un punto de acceso esté, más grande será su capacidad de transferencia de datos.

Por lo tanto, una estación dentro del rango de muchos puntos de acceso (que tengan el mismo SSID) puede elegir el punto que ofrezca la mejor proporción entre capacidad de carga de tráfico y carga de tráfico actual.

2.3.2 Modo ad-hoc

En el modo ad hoc los equipos cliente inalámbricos se conectan entre sí para formar una red punto a punto, es decir, una red en la que cada equipo actúa como cliente y como punto de acceso simultáneamente.

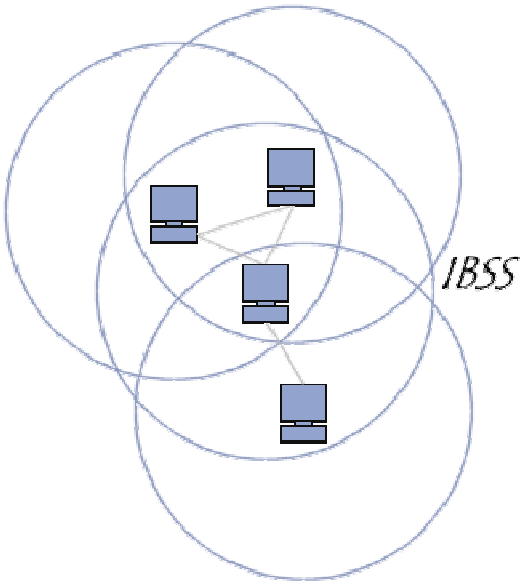


FIGURA 3. Modo ad-hoc

La configuración que forman las estaciones se llama conjunto de servicio básico independiente o IBSS.

Un IBSS es una red inalámbrica que tiene al menos dos estaciones y no usa ningún punto de acceso. Por eso, el IBSS crea una red temporal que le permite a la gente que esté en la misma sala intercambiar datos. Se identifica a través de un SSID de la misma manera en que lo hace un ESS en el modo infraestructura.

En una red ad hoc, el rango del BSS independiente está determinado por el rango de cada estación. Esto significa que si dos estaciones de la red están fuera del rango de la otra, no podrán comunicarse, ni siquiera cuando puedan "ver" otras estaciones. A diferencia del modo infraestructura, el modo ad hoc no tiene un sistema de distribución que pueda enviar tramas de datos desde una estación a la otra. Entonces, por definición, un IBSS es una red inalámbrica restringida.

2.4 Seguridad y fiabilidad

Las ondas de radio tienen en sí mismas la posibilidad de propagarse en todas las direcciones dentro de un rango relativamente amplio. Es por esto que es muy difícil mantener las transmisiones de radio dentro de un área limitada. La propagación radial también se da en tres dimensiones. Por lo tanto, las ondas pueden pasar de un piso a otro en un edificio (con un alto grado de atenuación).

La consecuencia principal de esta "propagación desmedida" de ondas radiales es que personas no autorizadas pueden escuchar la red, posiblemente más allá del confinamiento del edificio donde se ha establecido la red inalámbrica.

El problema grave es que se puede instalar una red inalámbrica muy fácilmente en una compañía sin que se entere el departamento de IT. Un empleado sólo tiene que conectar un punto de acceso con un puerto de datos para que todas las comunicaciones en la red sean "públicas" dentro del rango de transmisión del punto de acceso.

2.4.1 War-driving

Debido a lo fácil que es "escuchar" redes inalámbricas, algunas personas recorren la ciudad con un ordenador portátil (o PDA) compatible con la tecnología inalámbrica en busca de redes inalámbricas. Esta práctica se denomina war-driving (a veces se escribe wardriving o war-Xing). Software especializados en "war-driving" permiten hacer un mapa exacto de la ubicación de estos puntos de acceso abiertos con la ayuda de un sistema de posicionamiento global (GPS).

Estos mapas pueden revelar las redes inalámbricas inseguras que están disponibles y a veces permiten que las personas accedan a Internet. Se crearon diversos sitios Web para compartir esta información. De hecho, en 2002 unos estudiantes londinenses inventaron una especie de "lenguaje de signos" para mostrar dónde están las redes inalámbricas al indicar su presencia con símbolos dibujados con tiza en las veredas. Esto se denomina "warchalking". Dos semicírculos opuestos significa que el área está cubierta por una red abierta que provee acceso a Internet, un círculo indica la

presencia de una red inalámbrica abierta sin acceso a una red conectada y una W dentro de un círculo revela que es una red inalámbrica adecuadamente segura.

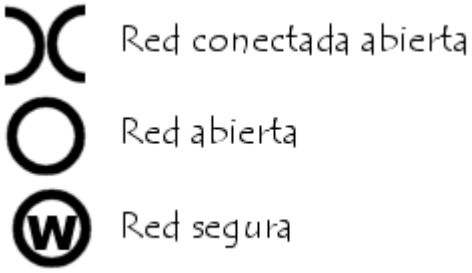


FIGURA 4. Warchalking

2.4.2 Riesgos de seguridad

Existen muchos riesgos que surgen de no asegurar una red inalámbrica de manera adecuada:

- La intercepción de datos es la práctica que consiste en escuchar las transmisiones de varios usuarios de una red inalámbrica.
- El crackeo es un intento de acceder a la red local o a Internet.
- La interferencia de transmisión significa enviar señales radiales para interferir con tráfico.
- Los ataques de denegación de servicio inutilizan la red al enviar solicitudes falsas.

Intercepción de datos

Una red inalámbrica es insegura de manera predeterminada. Esto significa que está abierta a todos y cualquier persona dentro del área de cobertura del punto de acceso puede potencialmente escuchar las comunicaciones que se envían en la red. En el caso de un individuo, la amenaza no es grande ya que los datos raramente son confidenciales, a menos que se trate de datos personales. Sin embargo, si se trata de una compañía, esto puede plantear un problema serio.

Intrusión de red

La instalación de un punto de acceso en una red local permite que cualquier estación acceda a la red conectada y también a Internet, si la red local está conectada a ella. Es por esto que una red inalámbrica insegura les ofrece a los hackers la puerta de acceso perfecta a la red interna de una compañía u organización.

Además de permitirle al hacker robar o destruir información de la red y de darle acceso a Internet gratuito, la red inalámbrica también puede inducirlo a llevar a cabo

ataques cibernéticos. Como no existe manera de identificar al hacker en una red, puede que se responsabilice del ataque a la compañía que instaló la red inalámbrica.

Interferencia radial

Las ondas radiales son muy sensibles a la interferencia. Por ello una señal se puede interferir fácilmente con una transmisión de radio que tenga una frecuencia cercana a la utilizada por la red inalámbrica. Hasta un simple horno microondas puede hacer que una red inalámbrica se vuelva completamente inoperable si se está usando dentro del rango del punto de acceso.

Denegación de servicio

El método de acceso a la red del estándar 802.11 se basa en el protocolo CSMA/CA, que consiste en esperar hasta que la red este libre antes de transmitir las tramas de datos. Una vez que se establece la conexión, una estación se debe vincular a un punto de acceso para poder enviarle paquetes. Debido a que los métodos para acceder a la red y asociarse a ella son conocidos, un hacker puede fácilmente enviar paquetes a una estación solicitándole que se desvincule de una red. El envío de información para afectar una red inalámbrica se conoce como ataque de denegación de servicio.

Asimismo, conectarse a redes inalámbricas consume energía. Incluso cuando los dispositivos inalámbricos periféricos tengan características de ahorro de energía, un hacker puede llegar a enviar suficientes datos cifrados a un equipo como para sobrecargarlo. Muchos periféricos portátiles, como los PDA y ordenadores portátiles, tienen una duración limitada de batería. Por lo tanto, un hacker puede llegar a provocar un consumo de energía excesivo que deje al dispositivo inutilizable durante un tiempo. Esto se denomina ataque de agotamiento de batería.

2.5 Ventajas y desventajas

Las redes Wi-Fi poseen una serie de ventajas, entre las cuales podemos destacar [4]:

- Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse desde distintos puntos dentro de un rango suficientemente amplio de espacio.

- Una vez configuradas, las redes Wi-Fi permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, no así en la tecnología por cable.

- La Wi-Fi Alliance asegura que la compatibilidad entre dispositivos con la marca Wi-Fi es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología Wi-Fi con una compatibilidad total. Esto no ocurre, por ejemplo, en móviles.

Pero como red inalámbrica, la tecnología Wi-Fi presenta los problemas intrínsecos de cualquier tecnología inalámbrica. Algunos de ellos son [4]:

- Una de las desventajas que tiene el sistema Wi-Fi es una menor velocidad en comparación a una conexión con cables, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear.

- La desventaja fundamental de estas redes existe en el campo de la seguridad. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta Wi-Fi en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella. Las claves de tipo WEP son relativamente fáciles de conseguir con este sistema. La alianza Wi-Fi arregló estos problemas sacando el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad. De todos modos muchas compañías no permiten a sus empleados tener una red inalámbrica. Este problema se agrava si consideramos que no se puede controlar el área de cobertura de una conexión, de manera que un receptor se puede conectar desde fuera de la zona de recepción prevista (Ej. desde fuera de una oficina, desde una vivienda colindante).

- Hay que señalar que esta tecnología no es compatible con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS, etc.

3. Mecanismos de seguridad en redes WiFi

3.1 Riesgos de las redes inalámbricas

La irrupción de la nueva tecnología de comunicación basada en redes inalámbricas ha proporcionado nuevas expectativas de futuro para el desarrollo de sistemas de comunicación, así como nuevos riesgos.

La flexibilidad y la movilidad que nos proporcionan las nuevas redes inalámbricas han hecho que la utilización de estas redes se haya disparado en el año 2002 siendo la mejor manera de realizar conectividad de datos en edificios sin necesidad de cablearlos.

Pero como todas las nuevas tecnologías en evolución, presenta unos riesgos debidos al optimismo inicial y en la adopción de la nueva tecnología sin observar los riesgos inherentes a la utilización de un medio de transmisión tan 'observable' como son las ondas de radio.

Aunque este apartado vaya dirigido a los aspectos de seguridad de la red inalámbrica, no podemos pasar por alto los elementos que componen la red inalámbrica.

Existen 4 tipos de redes inalámbricas, la basada en tecnología BlueTooth, la IrDa (Infrared Data Association), la HomeRF y la WECA (Wi-Fi). La primera de ellas no permite la transmisión de grandes cantidades de datos entre ordenadores de forma continua y la segunda tecnología, estándar utilizado por los dispositivos de ondas infrarrojas, debe permitir la visión directa entre los dos elementos comunicantes. Las tecnologías HomeRF y Wi-Fi están basadas en las especificaciones 802.11 (Ethernet Inalámbrica) y son las que utilizan actualmente las tarjetas de red inalámbricas.

La topología de estas redes consta de dos elementos clave, las estaciones cliente (STA) y lo puntos de acceso (AP). La comunicación puede realizarse directamente entre estaciones cliente o a través del AP. El intercambio de datos sólo es posible cuando existe una autentificación entre el STA y el AP y se produce la asociación entre ellos (un STA pertenece a un AP). Por defecto, el AP transmite señales de gestión periódicas, el STA las recibe e inicia la autentificación mediante el envío de una trama de autentificación. Una vez realizada esta, la estación cliente envía una trama asociada y el AP responde con otra.

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado nuevos riesgos de seguridad. La salida de estas ondas de radio ha proporcionado nuevos riesgos de seguridad. La salida de estas ondas de radio fuera del edificio donde está ubicada la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible a la empresa y a la seguridad informática de la misma.

Varios son los riesgos que derivan de este factor. Por ejemplo, se podría perpetrar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un punto de acceso ilegal más potente que capte las estaciones cliente en vez del punto de acceso legítimo, interceptando la red inalámbrica. También sería posible crear interferencias y una más que posible denegación de servicio con solo introducir un dispositivo que emita ondas de radio a una frecuencia de 2'4Ghz (frecuencia utilizada por las redes inalámbricas) [5].

La posibilidad de comunicarnos entre estaciones cliente directamente, sin pasar por el punto de acceso permitiría atacar directamente a una estación cliente, generando problemas si estas estación cliente ofrece servicios TCP/IP o comparte ficheros. Existe también la posibilidad de duplicar las direcciones IP o MAC de estaciones cliente legítimas.

Los puntos de acceso están expuestos a un ataque de Fuerza bruta para averiguar los passwords, por lo que una configuración incorrecta de los mismos facilitaría la irrupción en una red inalámbrica por parte de intrusos.

A pesar de los riesgos anteriormente expuestos, existen soluciones y mecanismos de seguridad para impedir que cualquiera con los materiales suficientes pueda introducirse en una red. Unos mecanismos son seguros, otros, fácilmente 'rompibles' por programas distribuidos gratuitamente por Internet.

3.2 Ataques generales a redes WiFi

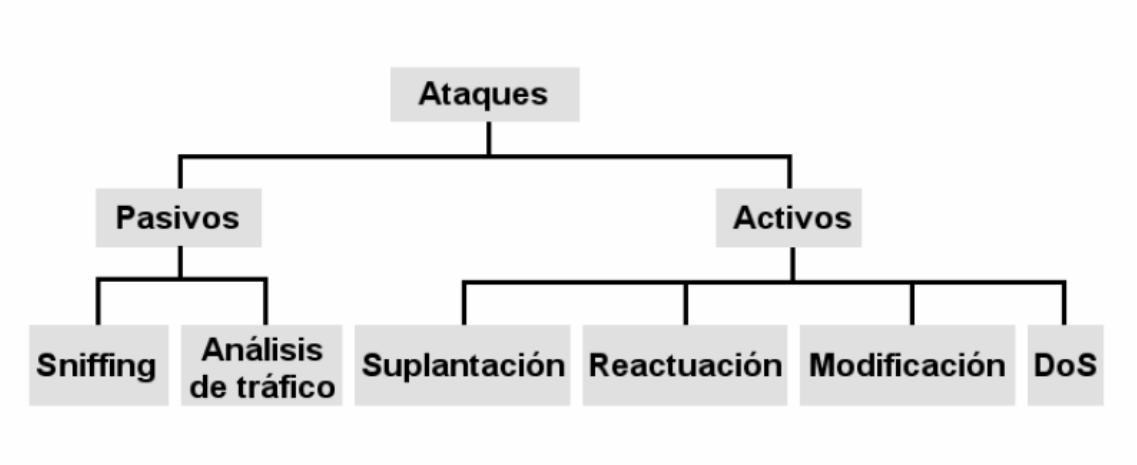


FIGURA 5. Ataques Wi-Fi

3.2.1 Ataques pasivos

Sniffing

- El tráfico de redes inalámbricas puede espiarse con mucha más facilidad que en una LAN.
- Basta con disponer de un portátil con una tarjeta inalámbrica.
- El tráfico que no haya sido cifrado, será accesible para el atacante y el cifrado con WEP también.

Análisis de tráfico

- El atacante obtiene información por el mero hecho de examinar el tráfico y sus patrones: a qué hora se encienden ciertos equipos, cuánto tráfico envían, durante cuánto tiempo, etc.

3.2.2 Ataques activos

Suplantación

- Mediante un sniffer para hacerse con varias direcciones MAC válidas.
- El análisis de tráfico le ayudará a saber a qué horas debe conectarse suplantando a un usuario u otro.
- Otra forma consiste en instalar puntos de acceso ilegítimos (rogue) para engañar a usuarios legítimos para que se conecten a este AP en lugar del autorizado.

Modificación

- El atacante borra, manipula, añade o reordena los mensajes transmitidos.

Reactuación

- Inyectar en la red paquetes interceptados utilizando un sniffer para repetir operaciones que habían sido realizadas por el usuario legítimo.

Denegación de servicio

- El atacante puede generar interferencias hasta que se produzcan tantos errores en la transmisión que la velocidad caiga a extremos inaceptables o la red deje de operar en absoluto.

- Otros ataques: inundar con solicitudes de autenticación, solicitudes de de autenticación de usuarios legítimos, tramas RTS/CTS para silenciar la red, etc.

3.3 Diseño recomendado

Se podrían hacer varias recomendaciones para diseñar una red inalámbrica e impedir lo máximo posible el ataque de cualquier intruso.

Como primera medida, se debe separar la red de la organización de un dominio público y otro privado. Los usuarios que proceden del dominio público (los usuarios de la red inalámbrica) pueden ser tratados como cualquier usuario de Internet (externo a la organización). Así mismo, instalar cortafuegos y mecanismos de autentificación entre la red inalámbrica y la red clásica, situando los puntos de acceso delante del cortafuegos y utilizando VPN a nivel de cortafuegos para la encriptación del tráfico en la red inalámbrica.

Los clientes de la red inalámbrica deben acceder a la red utilizando SSH, VPN o IPSec y mecanismos de autorización, autenticación y encriptación del tráfico (SSL). Lo ideal sería aplicar un nivel de seguridad distinto según que usuario accede a una determinada aplicación.

La utilización de VPNs nos impediría la movilidad de las estaciones cliente entre puntos de acceso, ya que estos últimos necesitarían intercambiar información sobre los usuarios conectados a ellos sin reiniciar la conexión o la aplicación en curso, cosa no soportada cuando utilizamos VPN.

Como contradicción, es recordable no utilizar excesivas normas de seguridad porque podría reducir la rapidez y la utilidad de la red inalámbrica. La conectividad entre estaciones cliente y PA es FCFS (First Come, First Served), es decir, la primera estación cliente que accede es la primera en ser servida, además el ancho de banda es compartido, motivo por el cual nos tenemos que asegurar un número adecuado de puntos de acceso para atender a los usuarios.

También se podrían adoptar medidas extraordinarias para impedir la intrusión. Como utilizar receivers (Signal Leakage Detection System) situados a lo largo del perímetro del edificio para detectar señales anómalas hacia el edificio además de utilizar estaciones de monitorización pasivas para detectar direcciones MAC no registradas o clonadas y el aumento de tramas de reautentificación.

Por último, también podrían ser adoptadas medidas físicas en la construcción del edificio o en la utilización de ciertos materiales atenuantes en el perímetro exterior del edificio, debilitando lo máximo posible las señales emitidas hacia el exterior. Algunas de estas recomendaciones podrían ser, aún a riesgo de resultar extremadas [5]:

- Utilizar cobertura metálica en las paredes exteriores.
- Vidrio aislante térmico (atenúa las señales de radiofrecuencia).
- Persianas venecianas de metal, en vez de plásticas.
- Poner dispositivos WLAN lejos de las paredes exteriores.
- Revestir los closets (rosetas) de la red con un revestimiento de aluminio.
- Utilizar pintura metálica.
- Limitar el poder de una señal cambiando la atenuación del transmisor.

3.4 Protocolos de seguridad

3.4.1 Mecanismos de seguridad

La emisión de señales de radiofrecuencia a través del espacio, pudiendo ser recibidas por cualquier equipo receptor que se encuentre en el área de cobertura, supone un problema de seguridad añadido que no se había producido hasta el momento en entornos de cableado estructurado.

Hasta el momento, los fabricantes de equipos Wireless LAN, han implementado mecanismos basados en el estándar 802.11 para dotar de un mínimo de seguridad a las comunicaciones entre los usuarios y los puntos de acceso [6]:

WEP

WEP (Wired Equivalent Protocol). Mecanismo estándar de cifrado de datos en el que la tarjeta WLAN cifra el cuerpo y el CRC (chequeo de integridad) de la trama, antes de ser transmitido. Utiliza el algoritmo RC4 con claves de 64 ó 128 bits. Para ello hace uso del llamado vector de inicialización que, con una longitud de 24 bits, es generado de manera aleatoria y concatenado con la llave generada a partir de una passphrase estática. De este modo la longitud real de las claves es de 40 y 104 bits.

WEP se considera un sistema poco seguro y ha sido roto de varias maneras: mediante ataques de fuerza bruta con o sin diccionario, por ataques inductivos o debilidades en la implementación del algoritmo RC4 (hay estudios que proponen mecanismos para obtener las claves recolectando de 5 a 10 millones de paquetes cifrados).

Existe software de libre acceso, y de uso sencillo, para la explotación de las debilidades en los mecanismos anteriores, que una vez descargado e instalado permiten conseguir acceso a multitud de redes inalámbricas y realizar ataques específicos contra clientes o acceder a otras redes y servicios accesibles a través de la red Wireless LAN.

CNAC

CNAC (Closed Network Access Control). Utiliza el nombre SSID (Server Set ID) de la red como contraseña para acceder a la red. Este nombre es fácil de conseguir ya que es enviado por los clientes al asociarse o autenticarse en el punto de acceso.

ACL

ACL (Access Control List). Permite utilizar una lista de MACs de las tarjetas de los clientes para limitar el acceso a la red. No supone una medida de seguridad efectiva ya que es muy sencillo utilizar un sniffer para localizar alguna MAC con acceso y emplearla en nuestra tarjeta. Puede localizarse la MAC del punto de acceso y deshabilitar un equipo o toda la red enviando ciertas tramas de des-asociación a un cliente o a la dirección de broadcast.

OSA

OSA (Open System Authentication). Mecanismo de autenticación definido por el estándar 802.11 que utiliza una clave secreta conocida por el cliente y el punto de acceso. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aún activando WEP, por lo tanto es un mecanismo poco fiable.

3.4.2 802.11i

Como consecuencia de las debilidades que presenta el protocolo WEP, nació el comité 802.11i. Este comité se centra en desarrollar un estándar que defina el cifrado y la autenticación para complementar y mejorar el protocolo WEP.

La especificación 802.11i puede ser dividida en dos capas; en la capa inferior se encuentran los algoritmos de cifrado como TKIP (Temporal Key Integrity Protocol), basado en RC4 y CCMP (Counter mode with CBC-MAC Protocol) basado en AES [6].

TKIP

TKIP. Ha sido diseñado para solucionar las debilidades del algoritmo WEP manteniendo compatibilidad hacia atrás. Utiliza un vector de inicialización de 48 bits y un contador de secuencia para descartar los paquetes fragmentados que llegan

CCMP

CCMP. Es un método de cifrado basado en el AES (Advanced Encryption Standard). AES puede ser implementado utilizando diferentes algoritmos. El modo escogido para 802.11 es CCM (Counter mode with CBC-MAC). Counter mode para la privacidad de datos y CBC-MAC para la integridad y autenticación. De manera general AES es un algoritmo simétrico e iterativo que utiliza la misma clave para cifrar y descifrar bloques de 128 bits. Al contrario que TKIP, CCMP es obligatorio para 802.11 según especificaciones de 802.11i.

3.4.3 802.1X / EAP

Por encima de estos algoritmos se encuentra 802.1x, que es un protocolo de autenticación desarrollado por un grupo diferente dentro de IEEE y utilizado desde hace tiempo en otros entornos para autenticación por puerto [6].

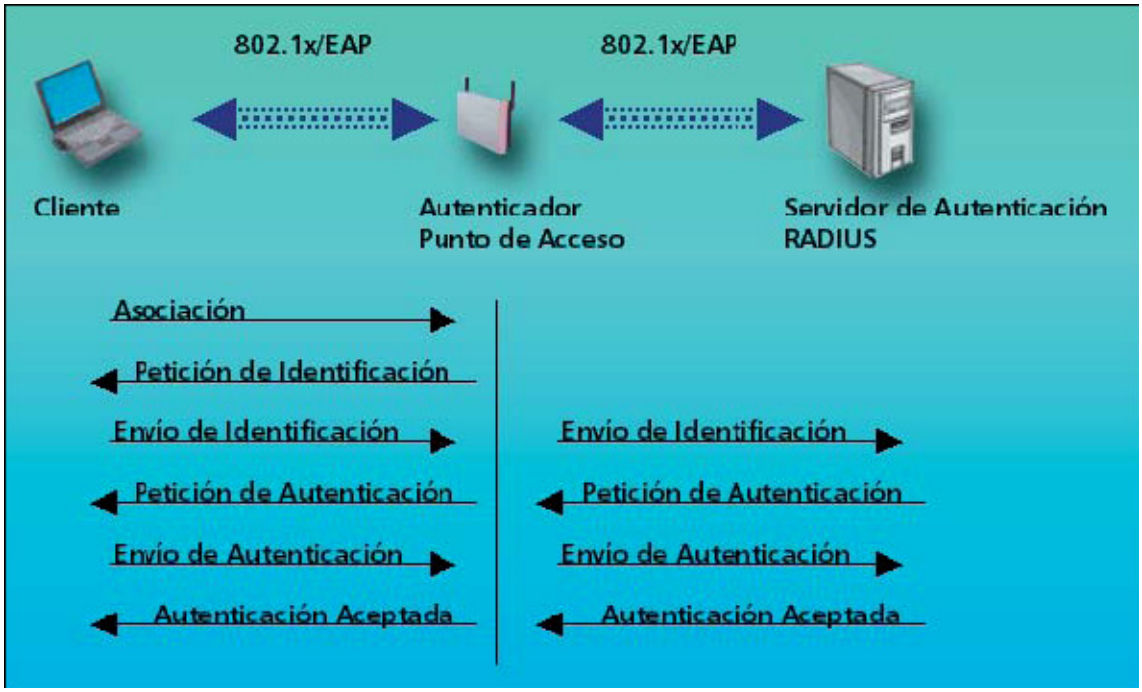


FIGURA 6. 802.1X / EAP

802.11x es un protocolo estándar de autenticación en red, basado en puerto, que se aplica tanto a redes tradicionales como inalámbricas. Proporciona los elementos necesarios para la autenticación de usuario y la distribución de las claves, que serán utilizadas por los algoritmos de cifrado.

En el caso de redes tradicionales se implementa en los switches de acceso. Se utiliza para restringir el acceso a los servicios de una red, hasta ser autenticado en la misma, en combinación con protocolos de capas superiores.

Introduce tres roles en escena: el cliente que accede a la red, el autenticador que realiza el proceso de autenticación –habitualmente el punto de acceso–, y el servidor de autenticación que mantiene un repositorio de usuarios, habitualmente un servidor Radius.

Un cliente que quiere validarse en la red, para hacer uso de sus recursos, establece una comunicación 802.1x con el punto de acceso y éste le solicita identificación. El cliente envía un paquete con la identificación que es reencaminado por el punto de acceso hacia el servidor de autenticación. El tráfico se envía por un canal seguro utilizando un protocolo de autenticación de capa superior, alguna variante de EAP (Extensible Authentication Protocol). Si la autenticación es correcta, el servidor de autenticación envía un mensaje de aceptación al punto de acceso, y éste permitirá el acceso del cliente a la red.

Como parte del proceso de autenticación se generan las claves que serán utilizadas posteriormente por los algoritmos de cifrado. 802.1x se encarga del paso de claves a las capas inferiores, tanto para el cliente como para el punto de acceso.

Con 802.1x en dispositivos Wireless LAN se utilizan dos claves diferentes; una clave de grupo que compartirán todos los clientes del punto de acceso, y que se utiliza para tráfico multicast, y una clave de sesión, que será utilizada para comunicación entre un cliente y el punto de acceso.

3.4.4 Protocolos de autenticación de capa superior

Los protocolos de autenticación para capas superiores no se especifican en el estándar 802.11i aunque son parte integrante de la mayoría de las implementaciones. Estos protocolos operan en capas altas del modelo de red OSI y por lo tanto se encuentran fuera del alcance de 802.11i, que se centra en las capas física y MAC.

Hay varios protocolos que se utilizan en la actualidad para proporcionar intercambio de credenciales de autenticación entre el cliente y el servidor de autenticación, generando las claves de sesión que se utilizarán entre el cliente y el punto de acceso.

Los protocolos de autenticación de capa superior trabajan en conjunción con 802.1x definiendo los mecanismos de comunicación segura para la autenticación, mientras que 802.1x se encarga de dirigir el tráfico de intercambio hasta el servidor de autenticación.

Algunos de los protocolos más utilizados son [6]:

EAP-TLS

EAP-TLS (Extensible Authentication Protocol with Transport Layer Security).

De las primeras versiones de EAP e incluido de manera nativa en Windows XP, está basado en certificados digitales. Requiere instalar un certificado digital en cada uno de los clientes además del certificado del servidor de autenticación, por lo que es necesario contar con una infraestructura PKI. En el proceso de generación de claves se realizan intercambios de credenciales y datos aleatorios. Una vez completado el proceso, el servidor de autenticación envía las claves de cifrado al punto de acceso, éste inicia un diálogo con el cliente para finalizar enviando las claves de cifrado a la capa MAC.

EAP-TTLS

EAP-TTLS (Extensible Authentication Protocol with Tunneled Transport Layer Security).

También es un estándar del IETF. Su funcionamiento es similar a PEAP; no necesita que ambas partes estén certificadas. Solo se requiere certificado en el servidor de autenticación. En el intercambio de mensajes inicial se utiliza un ID de usuario y una clave; una vez realizada la autenticación inicial se crea un túnel seguro.

PEAP

PEAP (Protected Extensible Authentication Protocol).

Es un estándar del IETF basado en contraseña secreta. Requiere un certificado en el servidor de autenticación. Este certificado se envía al cliente, el cual genera una clave de cifrado maestra y la devuelve cifrada utilizando la clave pública del servidor de autenticación. Una vez que ambos extremos conocen la clave maestra, se establece un túnel entre ellos realizándose la autenticación del cliente a través de una contraseña secreta.

LEAP

LEAP (Lightweight Extensible Authentication Protocol).

Es un protocolo propietario. Se autentica tanto al cliente como al servidor de autenticación, habitualmente un servidor Radius. Utiliza claves privadas compartidas para construir los mensajes intercambiados. También permite utilizar claves WEP dinámicas por usuario o sesión.

EAP-MD5

EAP-MD5 (Extensible Authentication Protocol with Message Digest).

Se trata de un método de autenticación por desafío. Es el más sencillo pero menos fiable que los anteriores.

3.4.5 WPA

WPA (Wired Protected Access) es una solución de seguridad inalámbrica (WiFi) ofrecida por WiFi Alliance para solucionar las carencias de WEP.

El soporte a WPA, por parte de los fabricantes, será obligatorio para disponer del logo Wi-Fi, tanto para nuevos productos como para actualizaciones de software en los productos actuales.

WPA es compatible con las especificaciones actuales de 802.11i. En realidad WPA es un subconjunto de 802.11i, tomando ciertas piezas ya disponibles para su implementación en el mercado, como son 802.11x y TKIP. La implementación de estos nuevos mecanismos de autenticación y cifrado es posible mediante actualizaciones de software en la mayoría de dispositivos existentes en el mercado.
En entornos empresariales WPA se utiliza junto con servidores de autenticación, como Radius, para proporcionar gestión centralizada de usuarios.

En entornos domésticos o de pequeñas oficinas, donde no hay servidores de autenticación, WPA funciona en modo PKS (Pre-Shared Key), permitiendo a los usuarios configurar las claves manualmente en el punto de acceso y en los clientes. Con este simple método se limita el acceso a clientes que no posean la clave correcta, además de proporcionar la clave automáticamente al algoritmo criptográfico TKIP.

El cifrado es idéntico al que utiliza WPA con 802.11x, salvo en el hecho de que emplea una clave preconfigurada en vez de credenciales de usuario.

3.5 Políticas de seguridad

3.5.1 Consideraciones previas

Los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio. Las ondas de radio -en principio- pueden viajar más allá de las paredes y filtrarse en habitaciones/casas/oficinas contiguas o llegar hasta la calle.

Si nuestra instalación está abierta, una persona con el equipo adecuado y conocimientos básicos podría no sólo utilizar nuestra conexión a Internet, sino también acceder a nuestra red interna o a nuestro equipo -donde podríamos tener carpetas compartidas- o analizar toda la información que viaja por nuestra red -mediante sniffers- y obtener así contraseñas de nuestras cuentas de correo, el contenido de nuestras conversaciones por MSN, etc.

Si la infiltración no autorizada en redes inalámbricas de por sí ya es grave en una instalación residencial (en casa), mucho más peligroso es en una instalación corporativa.

3.5.2 Estrategias de seguridad

Más que hablar de la gran regla de la seguridad podemos hablar de una serie de estrategias que, aunque no definitivas de forma individual, en su conjunto pueden mantener nuestra red oculta o protegida de ojos ajenos [7].

Ítem	**Complejidad**
1. Cambiar la contraseña por defecto	Baja
2. Usar encriptación WEP/WPA	Alta
3. Cambiar el SSID por defecto	Baja
4. Desactivar el broadcasting SSID	Media
5. Activar el filtrado de direcciones MAC	Alta
6. Establecer el nº máximo de dispositivos que pueden conectarse	Media
7. Desactivar el DHCP	Alta
8. Desconectar el AP cuando no lo usemos	Baja
9. Cambiar las claves WEP regularmente	Media

1. Cambiar la contraseña por defecto

Todos los fabricantes establecen un password por defecto de acceso a la administración del Punto de Acceso.

Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible que el observador la conozca.

2. Usar encriptación WEP/WPA

Activar en el Punto de Acceso la encriptación WEP. Mejor de 128 bits que de 64 bits (cuanto mayor sea el número de bits mejor).

Los Puntos de Acceso más recientes permiten escribir una frase a partir de la cual se generan automáticamente las claves. Es importante intercalar mayúsculas con minúsculas y números, evitar utilizar palabras incluidas en el diccionario y secuencias contiguas en el teclado (como "qwerty", "fghjk" o "12345").

También deberemos establecer en la configuración WEP la clave que se utilizará de las cuatro generadas (Key 1, Key 2, Key 3 o Key 4).

Después de configurar el AP tendremos que configurar los accesorios o dispositivos Wi-Fi de nuestra red. En éstos tendremos que marcar la misma clave WEP que hemos establecido para el AP y la misma clave a utilizar (Key 1, Key 2, Key 3 o Key 4).

Algunos Puntos de Acceso soportan también encriptación WPA (Wi-Fi Protected Access), encriptación dinámica y más segura que WEP.

Si activamos WPA en el Punto de Acceso, tanto los accesorios y dispositivos WLAN de nuestra red como de nuestro sistema operativo deberán soportarlo.

3. Cambiar el SSID por defecto

Suele ser algo del estilo a "default", "wireless", "101", "linksys" o "SSID".

En vez de "MiAP", "APManolo" o el nombre de la empresa es preferible escoger algo menos atractivo para el observador, como puede ser "Broken", "Down" o "Desconectado".

Si no llamamos la atención del observador hay menos posibilidades de que éste intente entrar en nuestra red.

4. Desactivar el broadcasting SSID

El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual.

Al desactivarlo tendremos que introducir manualmente el SSID en la configuración de cada nuevo equipo que queramos conectar.

Por tanto si el observador no conoce el SSID le resultará más difícil conectarse a nuestra red.

5. Activar el filtrado de direcciones MAC

Activar en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente tengamos funcionando. Al activar el filtrado MAC dejaremos que sólo los dispositivos con las direcciones MAC especificadas se conecten a nuestra red Wi-Fi.

Por un lado es posible conocer las direcciones MAC de los equipos que se conectan a la red con tan sólo "escuchar" con el programa adecuado, ya que las direcciones MAC se transmiten "en abierto", sin encriptar, entre el Punto de Acceso y el equipo.

Sin embargo, aunque en teoría las direcciones MAC son únicas a cada dispositivo de red y no pueden modificarse, hay comandos o programas que permiten simular temporalmente por software una nueva dirección MAC para una tarjeta de red.

6. Establecer el nº máximo de dispositivos que pueden conectarse

Si el AP lo permite, establecer el número máximo de dispositivos que pueden conectarse al mismo tiempo al Punto de Acceso.

7. Desactivar el DHCP

Desactivar DHCP en el router ADSL y en el AP.

En la configuración de los dispositivos/accesorios Wi-Fi tendremos que introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y el DNS primario y secundario.

Si el observador conoce "el formato" y el rango de IP’s que usamos en nuestra red, no habremos conseguido nada con este punto.

8. Desconectar el AP cuando no lo usemos

Desconectar el Punto de Acceso de la alimentación cuando no lo estemos usando o no vayamos a hacerlo durante una temporada. El AP almacena la configuración y no necesitamos introducirla de nuevo cada vez que lo conectemos.

9. Cambiar las claves WEP regularmente

Por ejemplo semanalmente o cada 2 ó 3 semanas.

Existen aplicaciones capaces de obtener la clave WEP de nuestra red Wi-Fi analizando los datos transmitidos por la misma. Pueden ser necesarios entre 1 y 4 Gb de datos para romper una clave WEP, dependiendo de la complejidad de las claves.

Cuando lleguemos a este caudal de información transmitida es recomendable cambiar las claves.

4. Debilidades y vulnerabilidad del protocolo WEP

4.1 Características y funcionamiento

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior [9].

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

WEP (Wired Equivalent Privacy, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN.

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.

El algoritmo de encriptación utilizado es RC4 con claves (seed), según el estándar, de 64 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 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.

El algoritmo de encriptación de WEP es el siguiente:

1. Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, Integrity Check Value).

2. Se concatena la clave secreta a continuación del IV formado el seed.

3. El PRNG (Pseudo-Random Number Generator) de RC4 genera una secuencia de caracteres pseudoaleatorios (keystream), a partir del seed, de la misma longitud que los bits obtenidos en el punto 1.

4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.

5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (frame body) de la trama IEEE 802.11.

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el seed y con ello podrá generar el keystream. Realizando el XOR entre los datos recibidos y el keystream se obtendrá el mensaje sin cifrar (datos y CRC-32). A continuación se comprobara que el CRC-32 es correcto.

4.2 El cifrado WEP

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 cifrados utilizando esta clave compartida.

El estándar 802.11 no especifica cómo se establece la clave secreta, pero permite que la existencia una tabla que asocie una clave exclusiva con cada estación. En la práctica general, sin embargo, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado.

Para proteger el texto cifrado 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) que se añade al final de cada trama a transmitir [8].

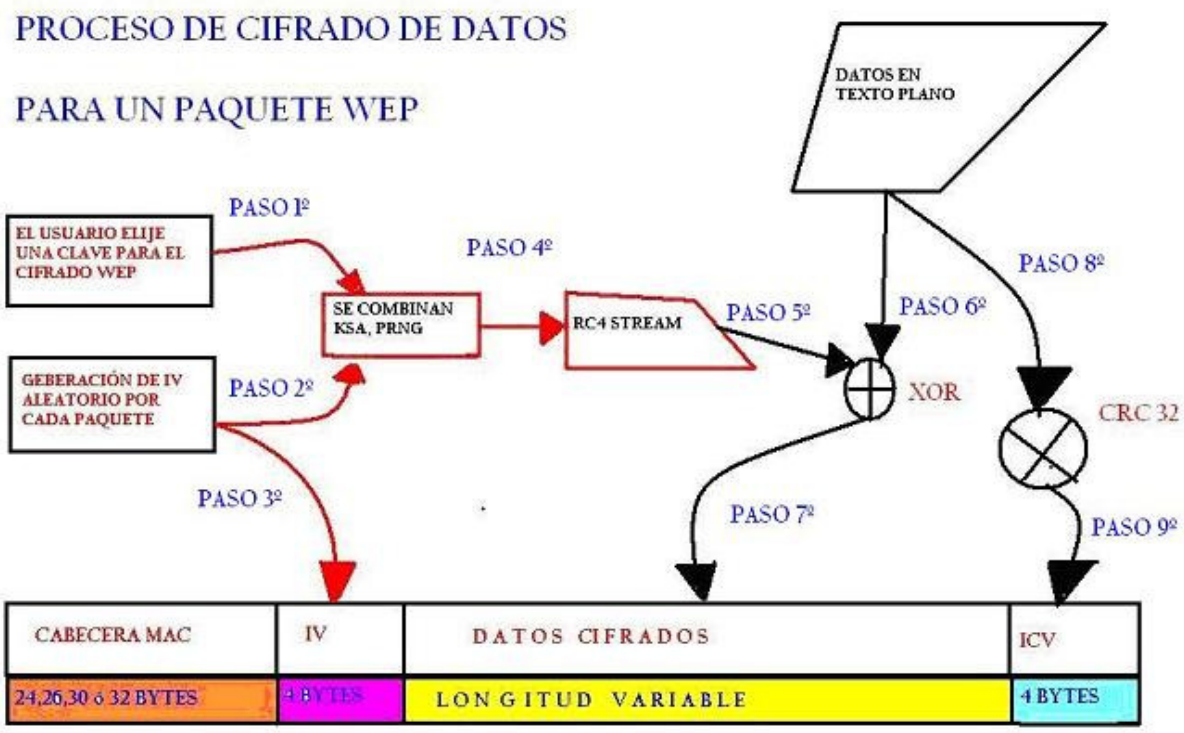


FIGURA 7. Cifrado de datos (WEP).

4.2.1 Tipos

A) El ICV es el CRC de los datos a transmitir sin cifrar y se añade al final de los datos cifrados:

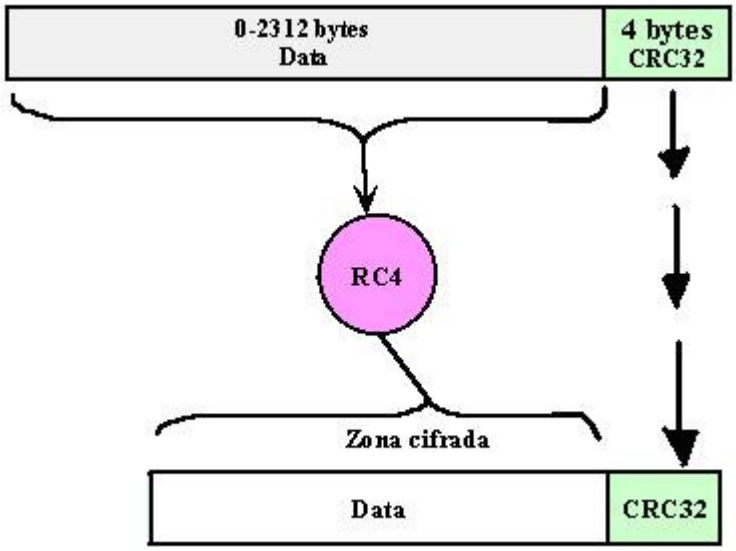


FIGURA 8. Cifrado WEP Tipo A.

B) El ICV es el CRC32 de los datos a transmitir sin cifrar al que se le aplica el algoritmo RC4 y que se añade al final de de los datos cifrados:

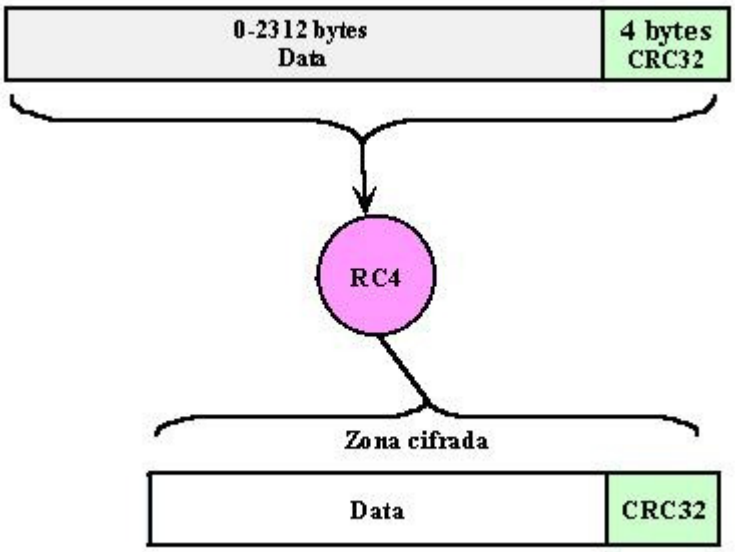


FIGURA 9. Cifrado WEP Tipo B.

C) El ICV es el CRC32 de los datos a transmitir sin cifrar al que se le aplica un keystream resultante del algoritmo RC4 y que se añade al final de los datos cifrados.

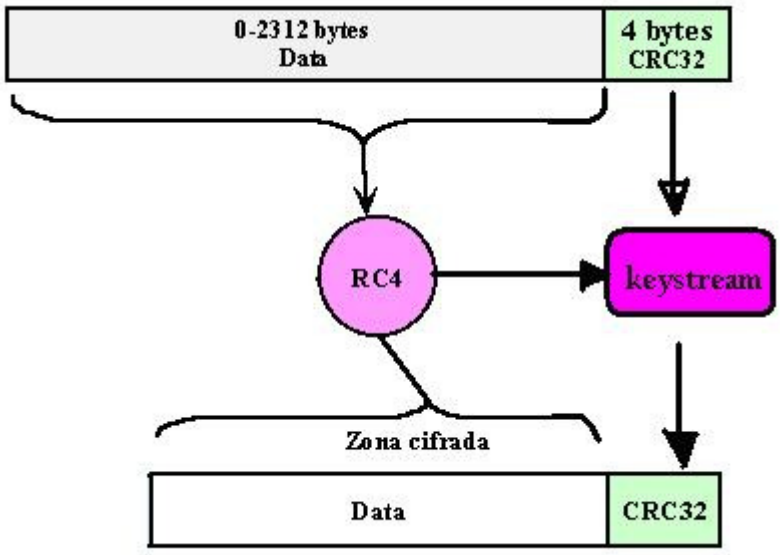


FIGURA 10. Cifrado WEP Tipo C.

4.2.2 Algoritmo RC4

Bajo el nombre de WEP se esconde en realidad el algoritmo de cifrado de clave simétrica RC4 [12].

RC4 es un algoritmo de cifrado de flujo. Fue diseñado por Ron Rivest de la RSA Security en el año 1987; su nombre completo es Rivest Cipher 4, teniendo el acrónimo RC un significado alternativo al de Ron's Code utilizado para los algoritmos de cifrado RC2, RC5 y RC6 [10].

Los cifrados de flujo funcionan expandiendo una clave secreta (en el caso de WEP, un vector de inicialización (IV) público y una clave secreta) en una clave arbitrariamente larga de bits pseudo aleatorios (el keystream).

El algoritmo de criptografía RC4 fue diseñado por Ron Rivest de la RSA Security en el año 1987; su nombre completo es Rivest Cipher 4, teniendo el acrónimo RC un significado alternativo al de Ron's Code utilizado para los algoritmos de cifrado RC2, RC5 y RC6 [10].

Inicialmente el algoritmo era un secreto registrado, pero en septiembre de 1994 una descripción del algoritmo fue posteada anónimamente en una lista de correo de Cypherpunks. En seguida pasó al grupo de correo sci.crypt y de ahí fue publicado en numerosos sitios de Internet. Debido al conocimiento del algoritmo, éste dejó de ser un secreto registrado. Sin embargo RC4 aún es una marca registrada.
RC4 es parte de los protocolos de cifrado más comunes como WEP, WPA para tarjetas wireless y TLS.

RC4 genera un flujo pseudoaleatorio de bits (un keystream) que se combina con el texto plano usando la función XOR.

Es un cifrado simétrico (ambos extremos poseen la misma clave para cifrar y descifrar el mensaje) y genera el mismo número de bytes cifrados que los existentes en el texto plano.

Por eso se llama de "flujo", el tamaño del texto cifrado es idéntico al tamaño del texto resultante del cifrado, esto no ocurre con otros tipos de cifrado como pueden ser los de bloques.

El motivo de utilizar RC4 en WEP es por su simplicidad de cálculo en los procesos, si las redes inalámbricas ya tienen que competir con los esfuerzos de una transmisión rápida, colisiones, acceso compartido al medio, etc. si le añadimos un algoritmo de cifrado que ocupe mucho tiempo en calcularse o que genere un tamaño de texto cifrado mucho mas grande, la comunicación sería muy lenta [8].

4.3 Seguridad en WiFi con WEP

Todo el tráfico que transcurre por una red es accesible a un posible atacante, por tanto es necesario garantizar unos servicios de seguridad:

- Autenticación: Identificación con un grado aceptable de confianza de los usuarios autorizados.

- Confidencialidad: La información debe ser accesible únicamente a las personas autorizadas.

- Integridad: La información debe mantenerse completa y libre de manipulaciones fortuitas o deliberadas, de manera que siempre se pueda confiar en ella

Sin embargo, el protocolo de seguridad WEP no consigue ofrecer ninguno de estos servicios.

4.3.1 Autenticación

El proceso de autenticación precede al de envío de datos, antes de poder enviar información por la red debemos estar autenticados y asociados…

Si usamos WEP como cifrado en modo seguro (esto es, cifrado + clave compartida) el proceso de autenticación es así:

- Cuando una estación trata de conectarse con un punto de acceso, éste le envía 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.

En el caso de que usemos WEP en modo abierto, (sin el uso de claves compartidas) podremos autenticarnos (no asociarnos), no podremos enviar datos puesto que desconocemos la clave wep y lo que recibamos tampoco "lo entenderemos" puesto que está cifrado.

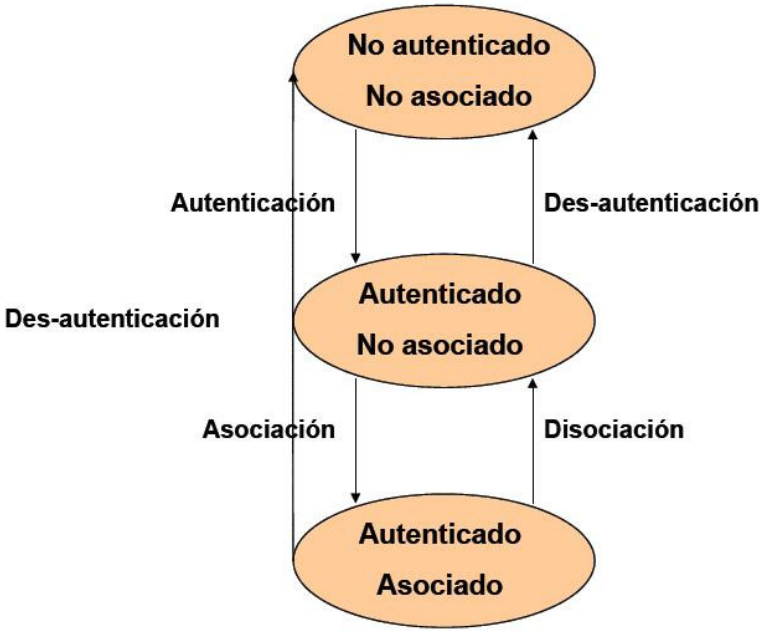


FIGURA 11. Estados de un Cliente

4.3.2 Confidencialidad

WEP usa el algoritmo de cifrado RC4 para la confidencialidad.

El cifrado RC4 presenta debilidades. La clave de sesión compartida por todas las estaciones es estática. Esto significa que para implementar un gran número de estaciones WiFi, es necesario configurarlas utilizando la misma clave de sesión, teniendo como consecuencia que el conocimiento de la clave basta para descifrar la comunicación.

Además, 24 bits de la clave sirven únicamente para la inicialización, lo que significa que sólo 40 bits de la clave de 64 bits sirven realmente para cifrar y 104 bits para la clave de 128 bits. En el caso de una clave de 40 bits, un ataque por fuerza bruta (intentando todas las combinaciones posibles de la clave) puede rápidamente llevar al hacker a encontrar la clave de sesión. [11]

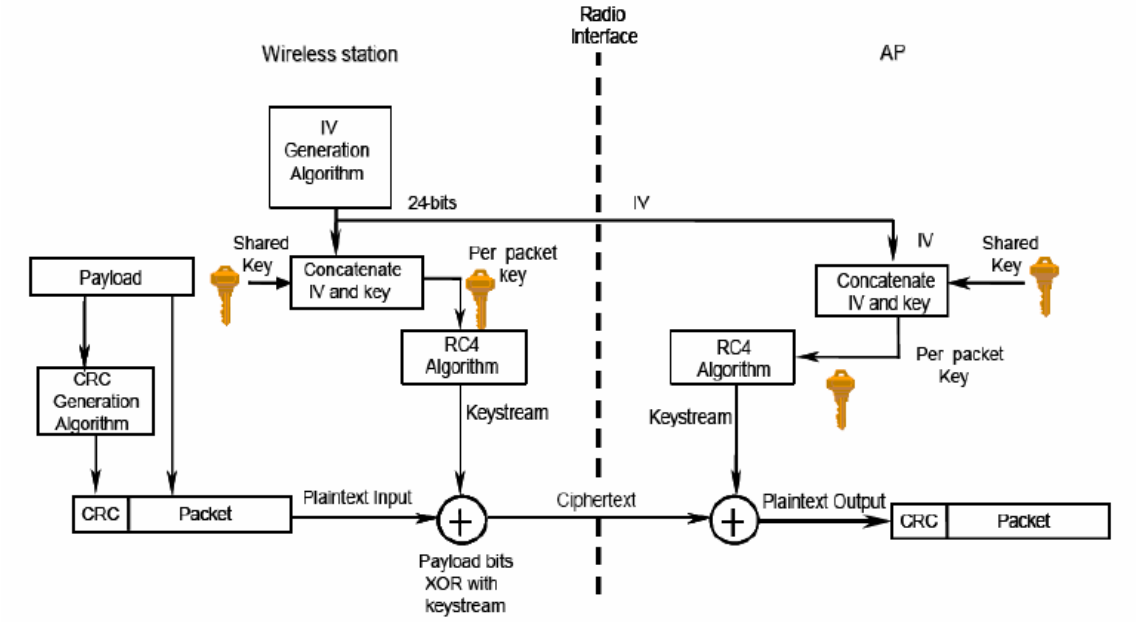


FIGURA 12. Confidencialidad en WEP.

4.3.3 Integridad

En cuanto a la integridad de los datos, WEP utiliza el algoritmo de comprobación de integridad CRC32.

Este algoritmo permite la modificación de la cadena de verificación del paquete a comparar a la cadena final producto de los datos recibidos, lo que permite a un hacker hacer pasar sus informaciones como informaciones válidas [11].

4.4 Vulnerabilidades WEP

Uso de claves estáticas

- No existe ningún mecanismo de gestión de claves.
- Se comparten entre numerosos usuarios por tiempo ilimitado.
- Se genera mucho tráfico, lo que permite su análisis.

El vector de inicialización (IV) se envía en claro

- El IV posee 24 bits: demasiado corto.
- Si se repite el IV (es típico inicializarlo a 0 con cada conexión), se produce la misma secuencia cifrante.
- Conocida ésta, se puede descifrar el tráfico cifrado con ella.

El IV forma parte de la clave WEP

- Además RC4 posee una debilidad en su planificación de claves.
- Permite realizar un ataque que recupera la clave.

No existe control criptográfico de la integridad

- CRC se diseñó para detectar errores fortuitos.
- Existe un ataque en el que se descifra un paquete cambiando su CRC y anotando cuándo es rechazado por el AP.
- Se pueden cambiar a ciegas algunos bits del paquete y a pesar de todo se obtiene el mismo CRC.
- Se puede cambiar la dirección de destino.

Configuración predeterminada débil

- Los valores por defecto de los fabricantes suelen excluir la seguridad para facilitar el despliegue.

Autenticación de la estación, no del usuario

- Se autentica la máquina, no el individuo que está sentado a la máquina.

Autenticación unidireccional

- El cliente no autentica al AP, sólo el AP autentica al cliente.
- Posibilidad de un ataque man-in-the-middle (MitM), ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado (wikipedia.org).

4.5 Alternativas a WEP

Las vulnerabilidades explicadas de WEP son motivos más que suficientes para utilizar otros mecanismos de seguridad en redes WLAN.

Aunque no forma parte del estándar, los fabricantes de productos Wi-Fi decidieron ofrecer la posibilidad de utilizar claves del doble de longitud (de 64 bits a 128 bits). WEP utilizado con claves de 128 bits es lo que se conoce generalmente como WEP2. Sin embargo, debemos observar que la longitud del vector de inicialización sigue siendo de 24 bits (las tramas IEEE 802.11 no contemplan un mayor número de bits para enviar el IV), por lo que lo único que se ha aumentado es la clave secreta (de 40 bits a 104 bits). Debido a que la longitud del IV y su forma de utilizarlo no varían, las debilidades del IV pueden seguir siendo aprovechadas de la misma manera. WEP2 no resuelve los problemas de WEP.

Otra variante de WEP utilizada en algunas implementaciones es WEP dinámico. En este caso se busca incorporar mecanismos de distribución automática de claves y de autentificación de usuarios mediante 802.1x/EAP/RADIUS. Requiere un servidor de

autentificación (RADIUS normalmente) funcionando en la red. En el caso de que la misma clave (clave secreta + WEP) no se utilice en más de una trama, este mecanismo sería suficiente para compensar las principales debilidades de WEP.

Sin embargo, la solución preferida por las empresas como alternativa a WEP ha sido la utilización de VPNs, de la misma manera que se haría si los usuarios estuviesen conectados remotamente a la oficina. La tecnología de VPNs está suficiente probada y se considera segura, aunque no ha sido diseñada específicamente para redes WLAN. Tiene como inconveniente la falta de interoperatibilidad entre dispositivos de distintos fabricantes.

Los mecanismos diseñados específicamente para redes WLAN para ser los sucesores de WEP son WPA y WPA2 (IEEE 802.11i) [9].

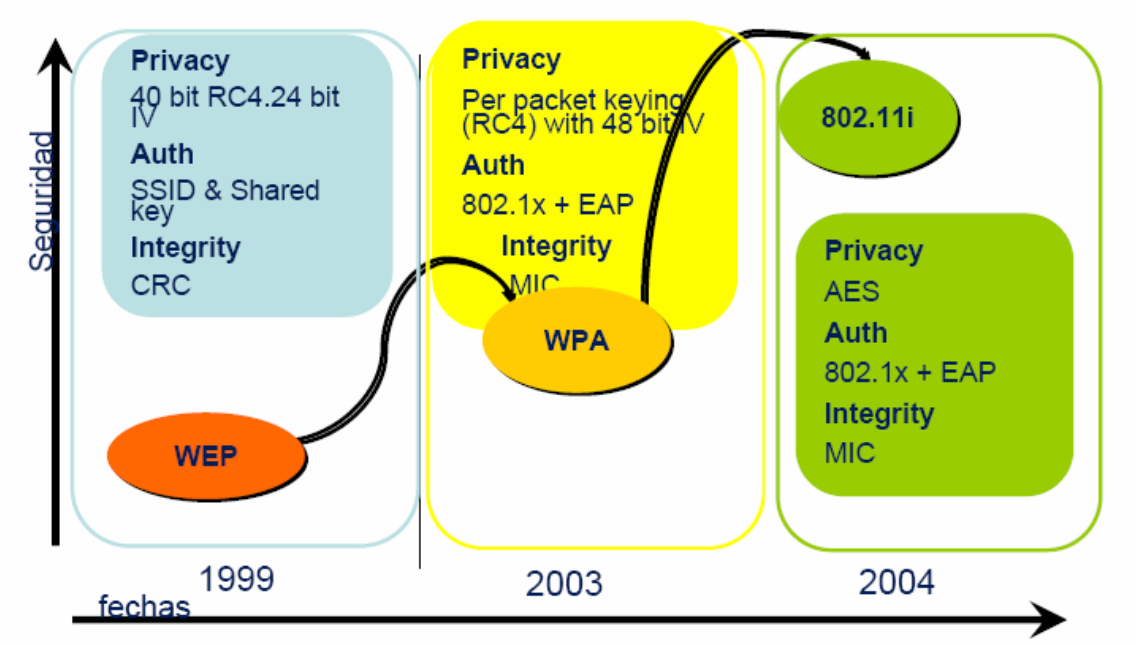


FIGURA 13. Mejoras del protocolo WEP.

5. El protocolo WPA

5.1 Introducción

WPA fue creado por la Wi-Fi Alliance, dueños de la marca Wi-Fi, certificadores de dispositivos que llevan esa marca.

WPA fue diseñado para usarse en servidores de autenticación IEEE 802.11X, el cual distribuye diferentes claves para cada usuario (aunque puede ser utilizado de forma menos segura y darle a cada usuario la misma clave) [13].

En tanto la Wi-Fi Alliance anticipó el WPA2 basada en el borrador final del estándar 802.11i.

La Wi-Fi Alliance desarrolló el protocolo Wi-Fi Protected Access con los objetivos de encontrar un sustituto del protocolo WEP ante la revelación de su debilidad ante ataques pasivos y por la conveniencia de autentificar a los usuarios en lugar de a los dispositivos, tal como hace el protocolo WEP, hasta la aparición definitiva del protocolo 802.11i.

La Wi-Fi Alliance declaró que los dispositivos que implementaran WPA serían compatibles con el futuro 802.11i, con el fin de evitar el temor de los usuarios de tener que renovar su equipamiento para adaptar el nuevo estándar. WPA es una parte del borrador del 802.11i, tomando la autentificación mediante el protocolo 802.1x y la encriptación TKIP. Otros avances del 802.11i, como la asociación segura, no son posibles mediante el protocolo WPA.

WPA es la abreviatura de Wifi Protect Access, y consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP. También se le conoce con el nombre de TSN (Transition Security Network).

WPA utiliza TKIP TKIP (Temporal Key Integrity Protocol) [14] para la gestión de las claves dinámicas mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización. En general WPA es TKIP con 802.1X. Por lo demás WPA funciona de una manera parecida a WEP pero utilizando claves dinámicas, utiliza el algoritmo RC4 para generar un flujo de bits que se utilizan para cifrar con XOR y su vector de inicialización (IV) es de 48 bits. La modificación dinámica de claves puede hacer imposible utilizar el mismo sistema que con WEP para abrir una red inalámbrica con seguridad WPA.

Además WPA puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital u otro sistema o simplemente utilizar una contraseña compartida para identificarse.

5.2 Características

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA incluye las siguientes tecnologías:

- IEEE 802.1X. Estándar del IEEE de 2001 [16] para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP [17]y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service) [18]. Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

- EAP. EAP, definido en la RFC 2284 [17], es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol) [19], aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN) [16].

- TKIP (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama [15].

- MIC (Message Integrity Code) o Michael. Código que verifica la integridad de los datos de las tramas [15].

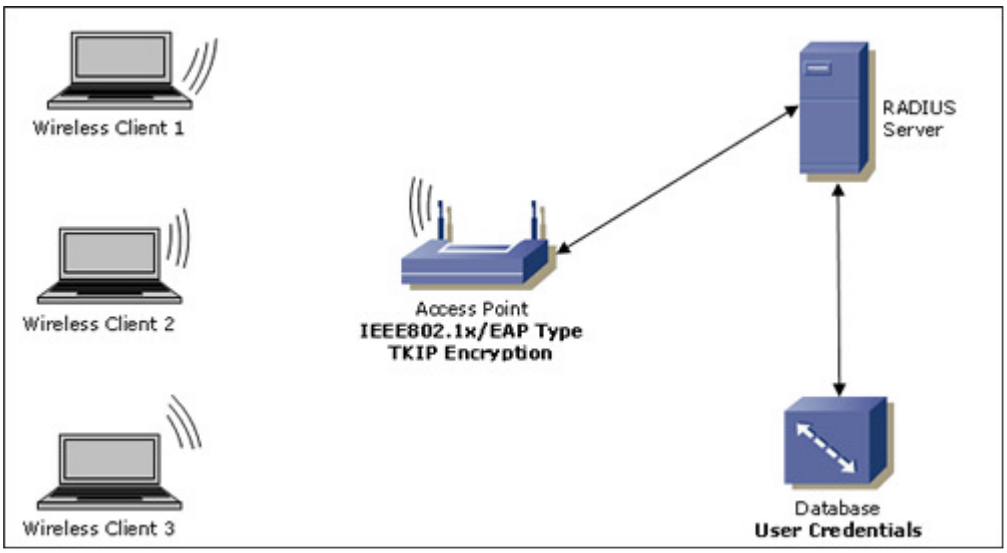


FIGURA 14. Encriptación WPA.

5.3 Mejoras de WPA respecto a WEP

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (replay).

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

5.4 Modos de funcionamiento

El estándar IEEE 802.11i define dos modos operativos:

- WPA-Personal: Este modo permite la implementación de una infraestructura segura basada en WPA sin tener que utilizar un servidor de autenticación. WPA Personal se basa en el uso de una clave compartida, llamada PSK que significa clave precompartida, que se almacena en el punto de acceso y en los dispositivos cliente. A diferencia del WEP, no se necesita ingresar una clave de longitud predefinida. El WPA le permite al usuario ingresar una frase de contraseña. Después, un algoritmo condensador la convierte en PSK [20].

- WPA-Empresarial: Este modo requiere de una infraestructura de autenticación 802.1x con un servidor de autenticación, generalmente un servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota, y un controlador de red (el punto de acceso) [20].

5.4.1 Modo personal / PSK

WPA-PSK

Es el sistema más simple de control de acceso tras WEP, a efectos prácticos tiene la misma dificultad de configuración que WEP, una clave común compartida, sin embargo, la gestión dinámica de claves aumenta notoriamente su nivel de seguridad. PSK se corresponde con las iniciales de PreShared Key y viene a significar clave

compartida previamente, es decir, a efectos del cliente basa su seguridad en una contraseña compartida.

WPA-PSK usa una clave de acceso de una longitud entre 8 y 63 caracteres, que es la clave compartida. Al igual que ocurría con WEP, esta clave hay que introducirla en cada una de las estaciones y puntos de acceso de la red inalámbrica. Cualquier estación que se identifique con esta contraseña, tiene acceso a la red.

Las características de WPA-PSK lo definen como el sistema, actualmente, más adecuado para redes de pequeñas oficinas o domésticas, la configuración es muy simple, la seguridad es aceptable y no necesita ningún componente adicional.

Autenticación PSK

- Clave compartida previamente.
- Se introduce la contraseña en cada estación para acceder a la red.
- Son de 8 a 63 caracteres (pasphrase) o una cadena de 256 bits.
- Clave para iniciar la autenticación, no para el cifrado.
- Usuarios domésticos o pequeñas redes:
    * Configuración simple.
    * Seguridad aceptable.
    * Sin componentes adicionales: Servidor.

Debilidades de WPA-PSK

La principal debilidad de WPA-PSK es la clave compartida entre estaciones. Cuando un sistema basa su seguridad en un contraseña siempre es susceptible de sufrir un ataque de fuera bruta, es decir ir comprobando contraseñas, aunque dada la longitud de la contraseña y si está bien elegida no debería plantear mayores problemas. Debemos pensar que hay un momento de debilidad cuando la estación establece el diálogo de autenticación. Este diálogo va cifrado con las claves compartidas, y si se entienden entonces se garantiza el acceso y se inicia el uso de claves dinámicas. La debilidad consiste en que conocemos el contenido del paquete de autenticación y conocemos su valor cifrado. Ahora lo que queda es, mediante un proceso de ataque de diccionario o de fuerza bruta, intentar determinar la contraseña.

5.4.2 Modo empresarial / 802.1X

WPA empresarial

En redes corporativas resultan imprescindibles otros mecanismos de control de acceso más versátiles y fáciles de mantener como por ejemplo los usuarios de un sistema identificados con nombre/contraseña o la posesión de un certificado digital. Evidentemente el hardware de un punto de acceso no tiene la capacidad para almacenar y procesar toda esta información por lo que es necesario recurrir a otros elementos de la red cableada para que comprueben unas credenciales. Ahora bien, parece complicado que un cliente se pueda validar ante un componente de la red por cable si todavía no tenemos acceso a la red. En este punto es donde entra en juego el IEEE 802.1X, que describiremos a continuación, para permitir el tráfico de validación entre un cliente y una máquina de la de local. Una vez que se ha validado a un cliente es cuando WPA inicia TKIP para utilizar claves dinámicas.

Los clientes WPA tienen que estar configurados para utilizar un sistema concreto de validación que es completamente independiente del punto de acceso. Los sistemas de validación WPA pueden ser, entre otros, EAP o Radius.

Autenticación 802.1X

- También implementado en redes cableadas.
- Adecuado para empresas.
- Requiere servidor configurado (RADIUS).
- Se basa en puertos: Un puerto por cliente.
- Para el control de admisión utiliza EAP (Extensible Authentication Protocol), hace posible la comunicación entre clientes (solicitantes) y servidores de autenticación (Ej. RADIUS).

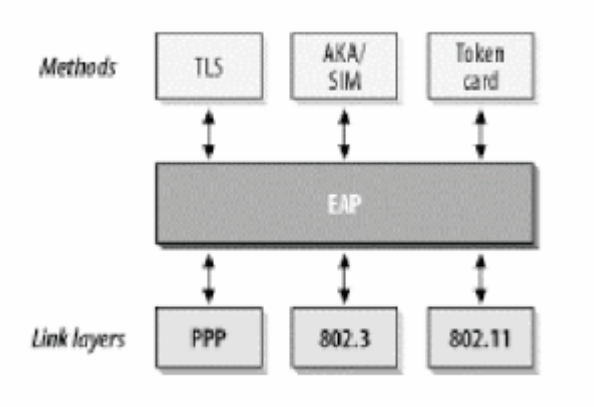


FIGURA 15. Capas y métodos del protocolo EAP.

Componentes:

- Suplicante: estación inalámbrica que quiere acceder a la red (Estación).
- Autenticador: realiza el control de acceso, habilita el puerto tras la autenticación (Punto de acceso).
- Servidor de autenticación: comprueba si el cliente esta autorizado para acceder a la red. Servidor AAA (Authentication, Authorization, Accounting) como RADIUS (Remote Authentication Dial In User Service).

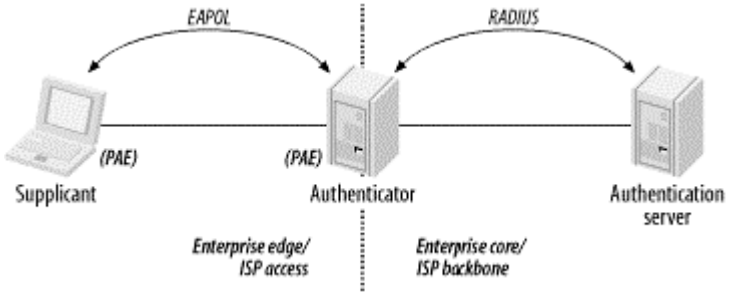


FIGURA 16. Componentes en autenticación 802.1X

Puertos:

Cada puerto físico, dos puertos lógicos:

- PAE (Port Access Entity) de autenticación abierta siempre y permite el paso de procesos de autenticación.
- PAE de servicio sólo se abre tras una autenticación exitosa por un tiempo limitado (3600 segundos por defecto).

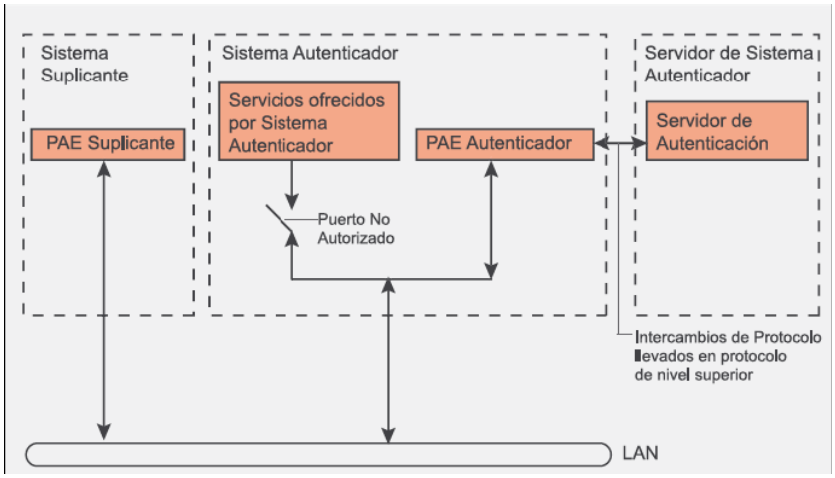


FIGURA 17. Puertos en autenticación 802.1X

Pasos:

- Intercambio tramas gestión 802.11 entre STA (estación) y AP (punto de acceso):

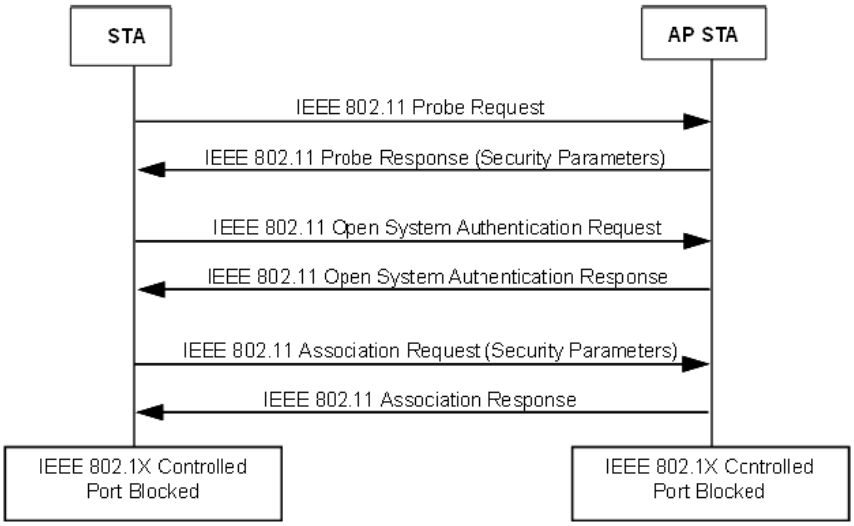


FIGURA 18. Intercambio de tramas (STA-AP).

- Tras la asociación de la STA, autenticación 802.1x:

  - El AP pide datos de identidad del cliente.
  - Respuesta del cliente con el método de autenticación preferido.
  - Intercambio mensajes entre el cliente y el servidor de autenticación para generar una clave maestra común (MK).
  - Al final, el servidor de autenticación envía al AP un mensaje Radius Accept, con la MK y un mensaje final EAP Success para el cliente.

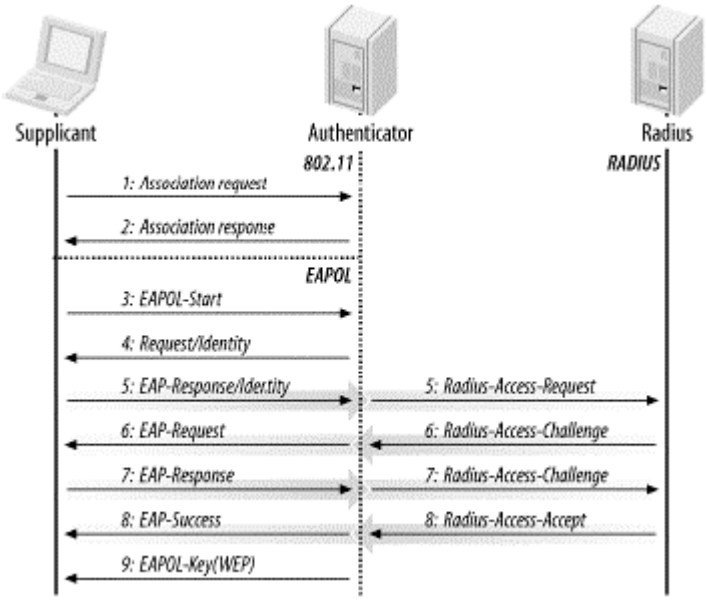


FIGURA 19. Autenticación 802.1X

5.5 Generación e intercambio de llaves

Partimos de la PMK (Pairwise Master Key):

- Para PSK (generada desde una passphrase (de 8 a 63 caracteres) o una cadena de 256-bit), PMK = PSK.
- Para 802.1X, PMK es derivada de la MK de autenticación.
- No se usa nunca para la encriptación o la comprobación de integridad.
- Generar una clave de encriptación temporal de sesión: PTK (Pairwise Transient Key).

Derivación de la clave: dos handshake

- 4-Way Handshake: derivación de la PTK (Pairwise Transient Key) y GTK (Group Transiet Key).
- Group Key handshake: renovación de GTK.

La PTK se deriva de la PMK, MAC del AP, MAC del cliente y dos nº aleatorios (ANonce y SNonce, generados por el autenticador y el suplicante).

De la longitud de la PTK depende el protocolo de encriptación: 512 bits para TKIP y 384 bits para CCMP. Son varias claves temporales dedicadas:

- KCK (Key Confirmation Key 128 bits): Clave para la autenticación de mensajes (MIC) durante el 4-Way Handshake y el Group Key Handshake.
- KEK (Key Encryption Key 128 bits): Clave para asegurar la confidencialidad de los datos durante el 4-Way Handshake y el Group Key Handshake.
- TK (Temporary Key 128 bits): Clave para encriptación de datos (usada por TKIP o CCMP).
- TMK (Temporary MIC Key – 2x64 bits): Clave para la autenticación de datos (usada sólo por Michael con TKIP). Se usa una clave dedicada para cada lado de la comunicación.

El tráfico multicast se protege con otra clave: GTK (Group Transient Key), generada de la clave maestra GMK (Group Master Key), MAC del AP y un nº aleatorio GNonce.

La longitud del GTK depende del protocolo de encriptación, 256 bits para TKIP y 128 bits para CCMP. Se divide en claves temporales dedicadas:

- GEK (Group Encryption Key): Clave para encriptación de datos (usada por CCMP para la autenticación y para la encriptación, y por TKIP).
- GIK (Group Integrity Key): Clave para la autenticación de datos (usada solamente por Michael con TKIP).

4-Way-Handshake:

- Confirmar que el cliente conoce la PMK.
- Derivar una PTK nueva.
- Instalar claves de encriptación e integridad.
- Encriptar el transporte de la GTK.
- Confirmar la selección de la suite de cifrado.

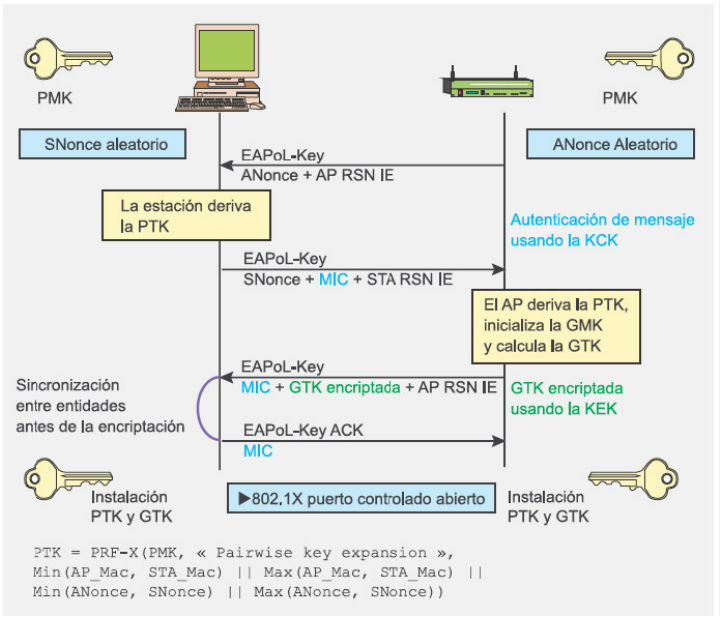


FIGURA 20. 4-Way-handshake.

Group Key Handshake:

- Disasociación de una estación o para renovar la GTK, a petición del cliente.

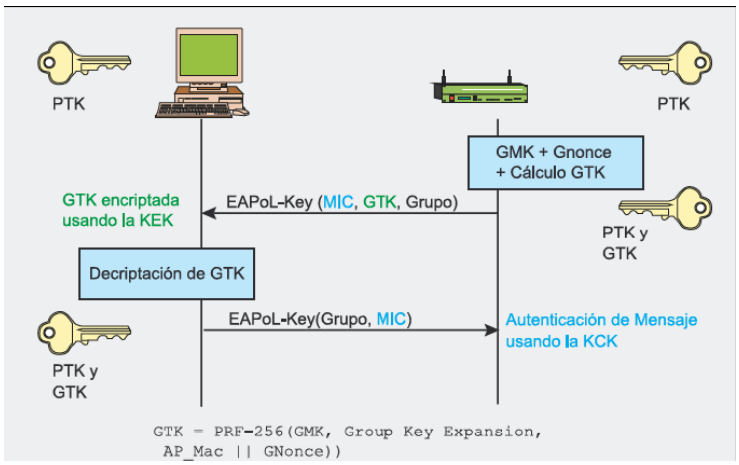


FIGURA 21. Group Key Handshake.

También existe un STAkey Handshake. Generación de una clave, STAkey, por el punto de acceso para conexiones ad-hoc.

5.6 Seguridad de WPA

Una vez analizadas lo inseguras que son las redes inalámbricas con cifrado WEP y facilidad con que se pueden recuperar claves WEP mediante técnicas de reinyección de tráfico, desautentificación, autentificación falsa y captura de datos, se nos plantea el reto de comprobar la seguridad de las redes WPA.

Las redes con seguridad WPA siguen siendo inseguras (aunque ya no tanto según se configuren), pero según su configuración realmente podemos estar bastante tranquilos.

Hay varias formas de seguridad vía WPA, pero las mas habituales a nivel de usuario utilizadas por la mayoría de nuestras redes domesticas son del tipo WPA-PSK, sin entrar en servidores RADIUS (utilizados en el modo empresarial de WPA). La configuración mediante encriptación WEP no depende de una buena configuración, simplemente son inseguras. Las WPA-PSK pueden ser muy seguras, pero siempre que estén bien configuradas [21].

Como explicamos anteriormente, este tipo de protección difiere de las WEP en que la clave es dinámica, es decir, que cambia cada cierto tiempo y es específica para cada terminal.

5.7 WPA2

El 802.11i se ratificó el 24 de junio de 2004 para abordar el problema de la seguridad en redes inalámbricas. Se basa en el algoritmo de cifrado TKIP, como el WPE, pero también admite el AES (Estándar de cifrado avanzado) que es mucho más seguro [20].

WiFi Alliance creó una nueva certificación, denominada WPA2, para dispositivos que admiten el estándar 802.11i (como ordenadores portátiles, PDA, tarjetas de red, etc.).

WPA2 incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requiere un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no pueden incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC.

A diferencia del WPA, el WPA2 puede asegurar tanto redes inalámbricas en modo infraestructura como también redes en modo "ad-hoc".

5.8 Situación del mercado

Uso del WiFi

Según el "Informe Wifi 2008" del "Observatorio Wireless del Grupo Gowex" [22], la mitad de los internautas españoles se conectan a Internet mediante WiFi.

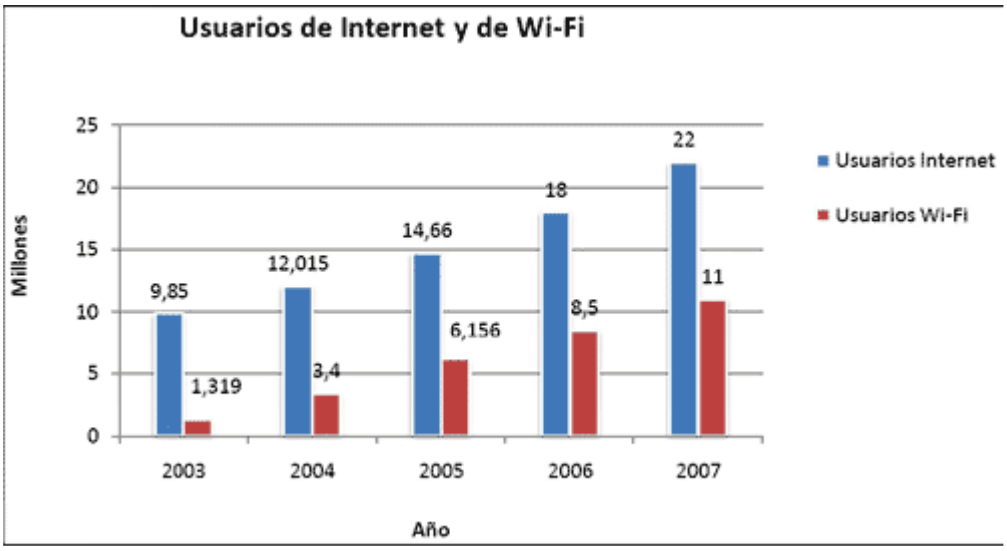


FIGURA 22. Usuarios de Internet y de Wi-Fi.

Según el "Estudio sobre la situación de seguridad y buenas prácticas en dispositivos móviles y redes inalámbricas" publicado por el "Inteco" [23], solo el 30% de los usuarios han protegido su red WiFi con encriptación WPA u otro sistema, mientras que casi un 50% de los usuarios sigue utilizando WEP o desconoce la encriptación de su punto de acceso inalámbrico.

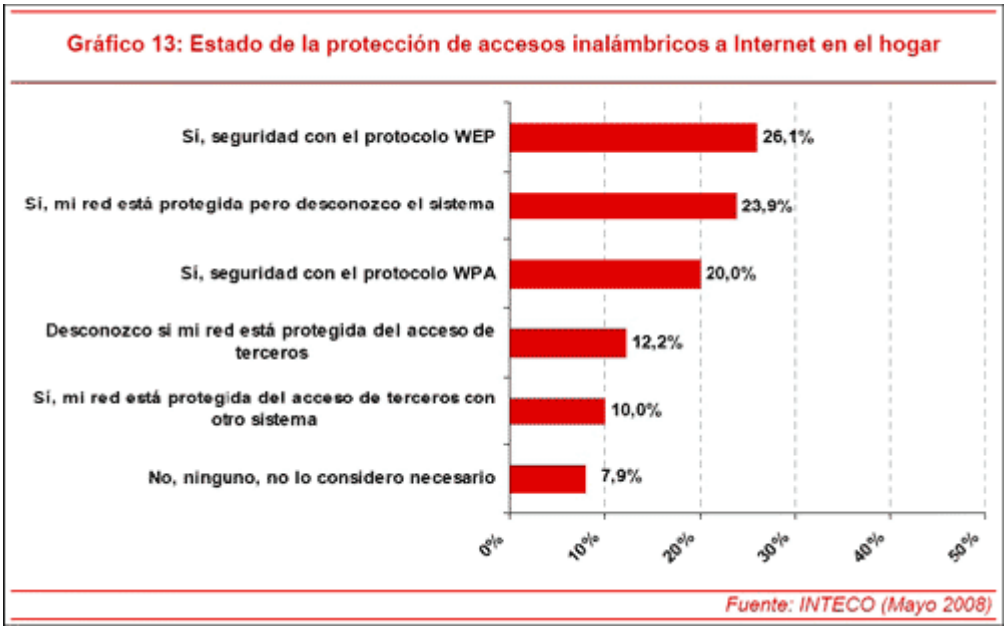


FIGURA 23. Protección Wi-Fi doméstica.

Informe

Durante la tarde del lunes 8 de diciembre de 2008, "bandaancha.eu" [24] realizó un recorrido de 15 Km. por algunas de las principales calles de la ciudad de Alicante con el objetivo de recoger una muestra lo suficientemente representativa de las redes WiFi activas en un núcleo urbano. Seleccionaron esta ciudad por la proximidad al lugar de residencia del autor del estudio, no obstante afirman que cualquier otra capital de provincia del estado español hubiese resultado igualmente útil para el propósito de este estudio, ya que los operadores proporcionan el mismo equipamiento a sus clientes independientemente de su ubicación.

Resultados

A partir del nombre de la red (SSID) se dedujo el proveedor de Internet que da servicio al punto de acceso. Se descartaron del estudio los puntos de acceso en los que el SSID había sido modificado por el usuario. Los resultados fueron los siguientes:

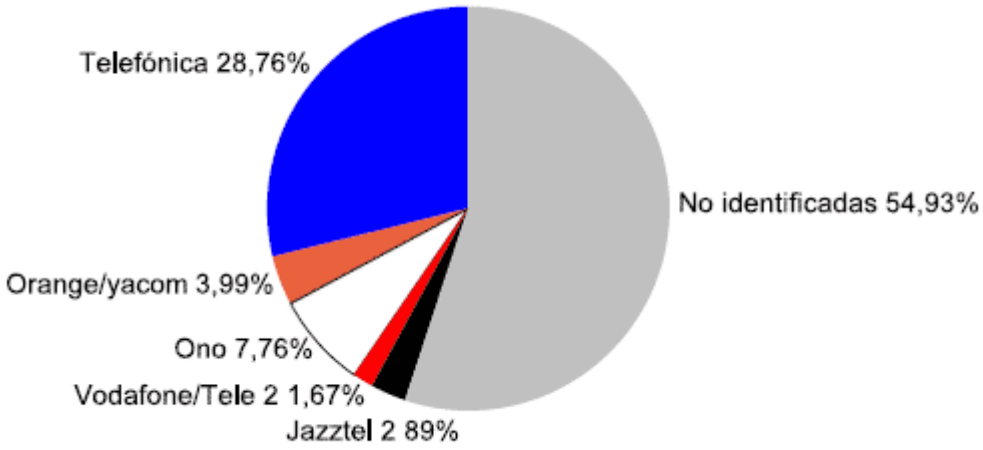


FIGURA 24. ISP's detectados durante el estudio.

De las 3.326 redes detectadas, 2.011 utilizan WEP, mientras que 632 permanecen desprotegidas. Solo 683 están protegidas con WPA:

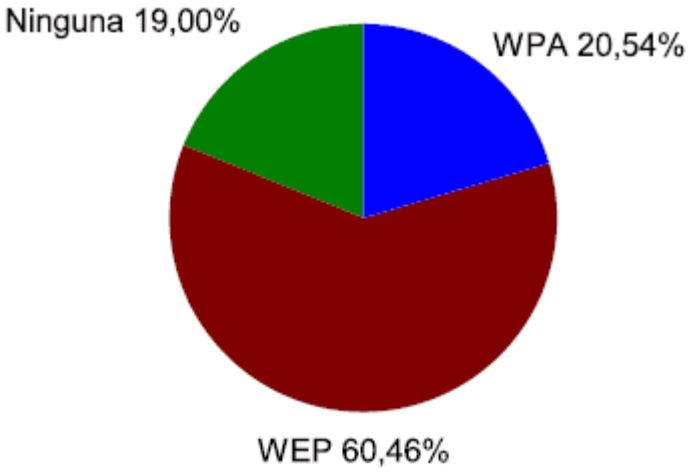


FIGURA 25. Nivel de seguridad en los SSID.

Cabe destacar que de las 923 redes de Telefónica que se detectaron, 880 permanecían con la configuración original establecida por la operadora: identificador WLAN_XX, encriptación WEP y patrón de clave alfanumérico.

Por otra parte, Vodafone/Tele2 resultó ser la operadora con mayor porcentaje de puntos de acceso protegidos por WPA (cerca de un 97%).

Conclusión

De este estudio podemos extraer una conclusión que dice más bien poco de la situación del mercado en nuestro país con respecto a la seguridad WiFi: un 93% de los routers WiFi del principal ISP (Telefónica) continúan con la configuración original establecida por la operadora. En este caso, además de ser vulnerables debido al uso de WEP, las claves son parcialmente predecibles debido al uso de patrones.

6. Técnicas hacking wireless

6.1 Introducción

El hacking no consiste precisamente en seguir los pasos como se de una receta de cocina se tratase. Consiste en conocer teóricamente las técnicas de ataque y fundamentos básicos del entorno, esto es lo que posibilita desarrollar nuevas herramientas de seguridad, combinar diferentes técnicas de ataque para aumentar la efectividad, desarrollar estrategias de ataque, etc.

El objetivo de este apartado es dar una visión general sobre las distintas herramientas, técnicas y estrategias utilizadas en el hacking wireless.

Por hacking wireless entendemos acceder a la red WLAN de otro usuario y utilizar su ancho de banda para conectarse a Internet, en otras palabras, conectarnos a Internet gratuitamente.

Aunque a priori no es condición necesaria para acceder a una red ajena el tener conocimientos teóricos sobre redes, si que es aconsejable el tener una serie de conocimientos previos sobre:

- El modelo de capas OSI.
- El protocolo TCP/IP.
- Los diferentes estándares IEEE 802.11.
- Topología básica de redes.

6.2 Hardware 802.11

Equipo necesario

La monitorización de redes consiste en detectar las redes inalámbricas cuyas ondas llegan a nuestro captador de señal.

Para este fin necesitaremos una tarjeta de red inalámbrica WNIC (Wireless Network Interface Card, estas tarjetas también reciben el nombre de adaptadores inalámbricos (AI's). Por otra parte nos será necesario un software para detectar AP's (Access Points o puntos de acceso).

A la hora de escoger una tarjeta inalámbrica deberemos tener en cuenta:

- El chipset: es el chip de la tarjeta.
- Nivel de potencia de salida y posibilidad de ajustarlo.
- Sensibilidad en la recepción.
- Conectores para antenas externas
- Soporte de algoritmos de encriptación mejorados.
- Compatibilidad con el sistema operativo.

FIGURA 26. Tarjeta wireless PCI.

Detección a larga distancia

El proceso de monitorización de redes se puede implementar con un portátil para poder salir de casa e ir en busca de redes en un centro comercial, otros edificios, etc.

Es aquí donde surge el conocido término wardriving: ir en busca de redes con un coche, así también está el warcycling (ir en su búsqueda en bici), o el warwalking (dando un paseo).

Si por el contrario lo que deseamos es captar redes desde nuestra propia casa, podemos aumentar nuestra potencia de detección. Así sin movernos de casa, detectaremos redes a largas distancias.

Para aumentar la potencia de detección deberemos disponer de una antena apropiada. Lo que hará esta antena será dirigir la señal aumenta su calidad. Desde la perspectiva del atacante:

- La distancia supone ocultación física y alejamiento.
- Es esencial para ataques sobre la capa física, de denegación de servicios (DoS) y ataques man-in-the-middle (de intermediario).

Como aspectos teóricos a tener en cuenta a la hora de elegir una antena debemos saber que:

- La ganancia de una antena es la amplificación de potencia. Se expresa en dBi y es pasiva, ya que la antena como hemos dicho no añade en realidad potencia, sino que enfoca las ondas radiadas para conseguir un haz más estrecho (apunta).
- El ancho de haz determina la zona de cobertura de la antena.

FIGURA 27. Antena wireless omnidireccional.

6.3 Software para detectar AP's

Existen varios métodos para detectar APs:

- Monitorización activa (barrido activo): Consiste en que el AI envía un paquete sonda o baliza (beacon frame) y en caso de existir un AP al que le llegue la señal, contestará con marco de respuesta sonda (request frame) que contiene los datos de la red.
- Monitorización pasiva: Implica la escucha del AI en busca de marcos baliza que emiten los AP's.

Teniendo en cuenta que los usuarios de otros sistema operativos (OS) que no sean Windows suelen tener unos conocimientos medios de informática avanzados, no centraremos en programas para Windows.

El más conocido es el Net Stumbler, es un programa de código cerrado que monitoriza las redes de forma activa.

6.4 Modo monitor o RFMON

Consiste en poner nuestra tarjeta wireless en escucha para poder captar los paquetes que transmiten otras redes wireless sin estar asociados a ellas.

Cuando se pone la tarjeta en este modo se suelen hablar de ponerla en modo monitorización o monitor [25].

Este modo permite la captura de los paquetes de una red wireless (que van por el aire en ondas de radio) sin estar asociados a la red.

Este modo monitor se conoce de forma técnica como modo RFMON y no ha de confundirse con el modo promiscuo de las tarjetas de red ethernet.

Este modo es vital para poder realizar cualquier técnica de auditoria inalámbrica, por ejemplo, para romper el cifrado WEP es necesario recoger un gran número de paquetes con IV's débiles.

Para poner una tarjeta en modo monitor es importante tener en cuenta los controladores. En Linux son las Linux Wireless Extensions los más utilizados para la configuración de adaptadores inalámbricos.

Cuando queremos hacer esto en Windows nuestras posibilidades se limitan, sobre todo por la falta de modelos compatibles con los controladores. En Windows se utiliza el controlador de Airopeek de la compañía WildPackets.

6.5 Sniffers y WEP crackers

Sniffers

Los sniffers (también denominados analizadores de protocolos o "husmeadores") son programas utilizados para realizar técnicas de sniffing.

El sniffing de paquetes es la práctica de capturar datos de red que no están destinados a tu máquina, generalmente con el propósito de ver tráfico confidencial (contraseñas, datos...).

Para esnifar ("olfatear") es necesario entender como transmiten los paquetes las máquinas en una red.

Una vez configurada la tarjeta en modo monitor, trataremos de capturar los paquetes de otras redes o la propia (auditoria de seguridad) con el objetivo de saltarnos sus medidas de seguridad y asociarnos a la red (ancho de banda, datos confidenciales).

Aquí entran en juego factores de lo bien que esté configurada la red o no. Términos previos:

SSID (Service Set IDentifier). El SSID es un código de 32 caracteres alfanuméricos que llevan los paquetes de una WLAN para identificarlos como parte de esa red. Por lo tanto todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo ESSID. Las redes cuya infraestructura incorpora un punto de acceso, utilizan el ESSID (E de extendido). Sin embargo nos podemos referir a este como SSID en términos generales. A menudo al ESSID se le conoce como nombre de la red.

El ESSID de la red ficticia del vecino está por defecto en emisión pública, cualquier usuario usando un stumbler podría detectar esta ESSID (nombre de red) y sabiendo que el ESSID actúa como la relación entre la estación cliente (nuestra máquina) y el AP, ya tenemos el nombre de red, que será vital para asociarse a la red a la que "atacamos".

Es por esto que una medida fundamental de seguridad es desactivar la emisión pública del ESSID (broadcasting), y sino es posible, al menos ocultarlo para que un atacante inexperto no pueda continuar en su intento.

WEP crackers

WEP es el sistema de cifrado incluido en redes estándar 802.11 de los paquetes que se transmiten en una red wireless.

Como hemos podido observar en apartados anteriores es el protocolo de seguridad más extendido con un amplio margen sobre los demás, es por eso por lo que nos centraremos en las técnicas de ataque sobre este protocolo.

WEP cifra y comprime los datos enviados por ondas de radio. Sin embargo, WEP no es precisamente el sistema de encriptación más potente del mercado. Incluso aunque esté habilitado nuestra red sigue siendo insegura.

Es "rompible" con los denominados WEP crackers.

El cifrado WEP, como vimos, no es otro que el algoritmo de encriptación RC4 (Algoritmo de cifrado de flujo, es decir que funciona expandiendo una clave secreta o "seed" la cual es un generador de números pseudoaleatoria).

Siguiendo las principales vulnerabilidades que afectan a este algoritmo proporcionado por RSA Security es posible reducir su potencia de 128 bits de cifrado a 24 bits. Lo que conlleva una disminución importante de la seguridad (de 2^104-1 a 2^24-1)

Además se usa un vector de inicialización (conocido como IV de 24 bits) el cual se añade a la seed mencionada antes, y cambia para cada trama. El receptor usa el mismo IV para chequear la integridad del mensaje.

Los IVS son públicos (no cifrados, en texto plano, o sea legibles), y aparecen en los paquetes transmitidos por la red. Estos varían, el problema es que la máquina suele reutilizar IVS y un intruso podría hacer con duplicados, montar una tabla y conocer el texto de un mensaje. Para ello ha de servirse el intruso de un bolígrafo, papel y mucha paciencia para interpretar el flujo. Pero esto nos llevaría demasiado tiempo, así que se ha automatizado el proceso.

Esto es en esencia lo que hace un WEP cracker. Tras capturar una serie de paquetes, en el orden de 1 millón para romper un cifrado de 128 bits, estos programas rompen la clave WEP de forma pasiva, analizando los IVs débiles o repetidos.

El WPA es mucho más seguro, pero este sistema no es funcional en algunos host AP's (routers) que funcionan con estándares IEEE 802.11 antiguos.

6.6 WEP cracker en Windows

Una vez tenemos los drivers de WildPackets instalados para trabajar con nuestra tarjeta wireless en modo monitor bajo Windows, es el momento de utilizar un Wep Cracker para averiguar el cifrado Wep.

El Wep Cracker más recomendado para Windows es el Aircrack, muy fácil de utilizar e intuitivo. Y además porque incluye el Airodump, un programa para capturar paquetes, también muy fácil de utilizar [26].

Capturando paquetes y averiguando el cifrado

Esta tarea la realizaremos en 2 fases:

- Primero capturaremos paquetes con Airodump.
- Segundo, una vez con suficientes paquetes válidos, averiguaremos el cifrado.

Antes de empezar a explicar el proceso debemos de tener muy claro que esto es ilegal (capturar paquetes) y solamente es justificable para realizar una auditoria informática de nuestra propia red y comprobar el estado de seguridad de la misma.

Una vez tengamos el Aircrack con el Airodump extraído, y nuestra tarjeta con los drivers compatibles instalados, ya lo tenemos todo para empezar a esnifar la red.

Así que ejecutaremos el Airodump.exe, una vez abierto detectará todas las tarjetas habilitadas en el sistema de forma automática, aquí introduciremos el número que hay a la izquierda de la tarjeta inalámbrica.

El primer paso es seleccionar el tipo de interfaz de la red, (Atheros, Aironet / Orinoco Realtek), esto dependerá de cada uno, del driver y de la tarjeta que tengamos.

El siguiente paso será elegir el canal. Si ponemos cero, dará por entendido que no queremos filtrar ningún canal y los esnifará todos, esto es útil si no sabemos el canal de la red que queremos esnifar.

A continuación introduciremos el nombre del archivo donde guardará los paquetes, no hará falta poner ninguna extensión, ya que automáticamente la creará.

Hay una opción que sirve para filtrar MAC's, es decir el programas solo aceptara los paquetes de la MAC que escribas, el formato debe ser 00:00:00:00:00, es decir hay que añadir los dos puntos ":". Para no filtrar ninguna y procesar todos los paquetes de todas las MAC's, bastará con escribir una "p".

Por ultimo si todo ha ido bien empezará a capturar paquetes. Dependiendo de la cantidad de trafico que haya, podremos tardar más tiempo o menos (a mayor cantidad de trafico mas IV's nos llegarán).

Más o menos con un millón de IV's es suficiente para una llave de 128 bits (104 bits reales) para una de 64 pues la mitad, es recomendable por si acaso que no paremos de capturar.

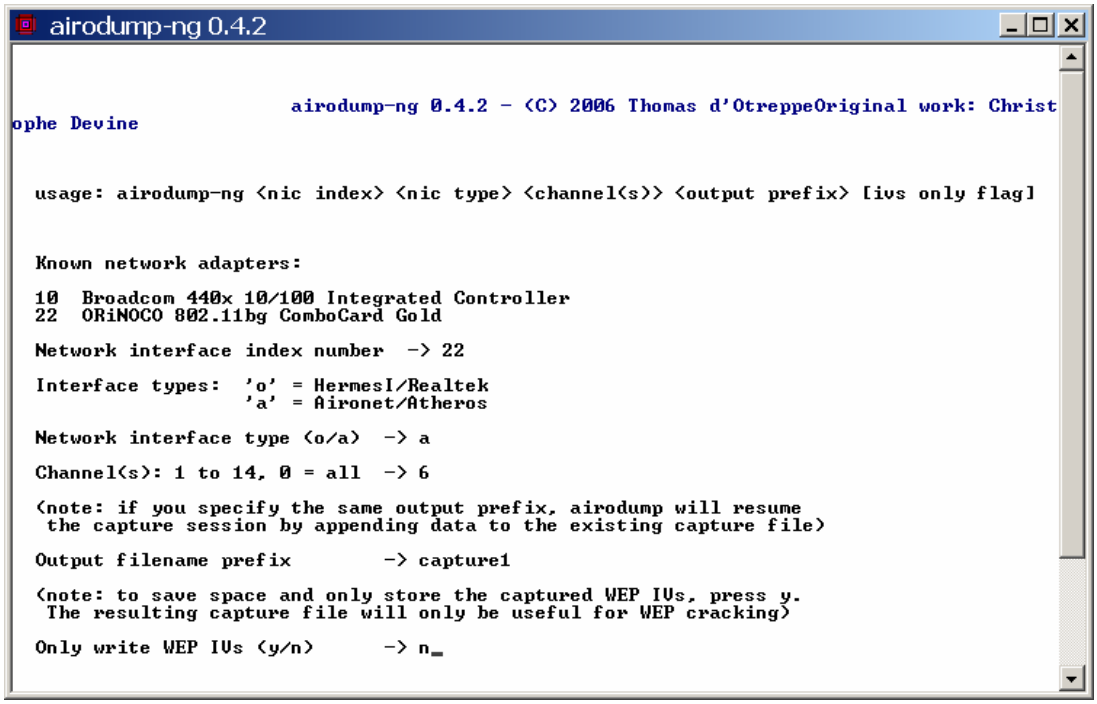


FIGURA 28. Airodump bajo Windows.

Si vemos que capturamos muy poco o si simplemente no interceptamos ningún IV's, podría ser por uno de los siguientes motivos:

- La red que estamos esnifando utiliza WPA en lugar de WEP.
- Nos encontramos demasiado alejados de la red y sólo recibimos los Beacon Frames.
- Nuestra tarjeta no es compatible con el 802.11g, y el AP sólo emite en 802.11g.
- Nuestro driver puede que esté mal instalado.

Crackeando con Aircrack

Aircrack también resulta muy fácil de utilizar. A continuación explicaremos para que sirven las distintas opciones:

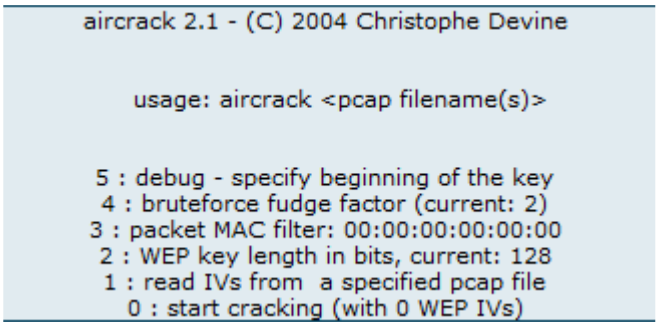


FIGURA 29. Aircrack versión línea de comandos.

Opción 5: sirve para especificar tú una llave y ver cuanto tarda en crackearla.

Opción 4: sirve para aumentar la cantidad de llaves a probar. Es decir si con 5000 llaves no encuentra la clave acertada, aumentamos el número (por defecto 2) y así conseguiremos que pruebe más llaves posibles.

Opción 3: es un filtro de paquetes que solo acepta los de la MAC introducida.

Opción 2: Sirve para especificar la longitud de la llave. Por defecto es 128 (lo mas común). Si no sabemos si será de 128 o de 64, lo dejaremos como está por defecto (128 bits) y si es de 64 bits la sacará de todas formas.

Opción 1: lee los paquetes válidos (IV's) del archivo donde guardamos los paquetes que anteriormente capturamos con Airodump y los enumera. Solo hay que introducir el nombre del archivo (este debe estar en la misma carpeta y hay que incluir la extensión, normalmente .cap)

Opción 0: empieza a crackear.

Cuando acabe nos saldrá un mensaje de KEY FOUND, y ya tenemos la clave.

Conectarnos o asociarnos a la red

Una vez tenemos la clave (es importante volver a instalar los drivers anteriores de la tarjeta), intentaremos conectarnos o asociarnos a la red. Para ello lo primero que haremos será activar DHCP en nuestra tarjeta (para que el router nos de una IP automáticamente).

En la herramienta de Windows para conectarnos a una red wireless, cuando sale una imagen de un candado ("Esta red tiene seguridad habilitada") significa que tiene el cifrado activo, y por lo tanto necesitas una clave, la que antes conseguimos.

Cuando no sabemos la clave pero nos sale al conectarnos un mensaje de "Conectividad Nula o Limitada", seguramente sea por uno de estos motivos:

- Porque la llave WEP que introducimos no es la acertada (no recibiremos ningún paquete).

- O también puede ser porque el router tiene desactivado el DHCP, es decir los clientes deben configurar su IP, su máscara y su puerta de enlace, y por lo tanto deben saber en que subred se encuentra configurada la conexión, así como la puerta de enlace (los más usuales son del tipo 192.168.xxx.xxx).

Para averiguar la puerta de enlace, por ejemplo y más datos deberemos volver a instalar los drivers de WildPackets y monitorizar un poco de tráfico y con un analizador de paquetes (Airopeek, por ejemplo), averiguarlos.

Una vez sabiendo la puerta de enlace, ya podemos configurar nuestra IP y la puerta de enlace, (la mascara de subred casi siempre es 255.255.255.0).

Una vez configurada la puerta de enlace y todo lo demás, si la red no tiene ningún tipo de seguridad en capas mas altas (Ipsec, SSH) que casi seguro si es una red domestica no tendrá, ya deberíamos de poder tener conexión a Internet.

Si la red tiene un filtro para MAC's (ACL), es decir solo acepta la lista de MACs configurada en el router, la cosa también se soluciona muy fácilmente, por ejemplo el Net Stumbler nos dice la BSSID, es decir la MAC del AP (el router, normalmente), cambiando la MAC de nuestra tarjeta inalámbrica, podremos entrar a la red sin problemas con el ACL.

Una vez dentro si conseguimos entrar al router podríamos añadir a la tabla de MACs una MAC un tanto rarilla (para que el administrador no sospechase). Y así no tener que utilizar la misma que el AP.

Y este sería el proceso para hackear una red wireless y conseguir acceso gratuito a Internet.

6.7 Ataque por fuerza bruta a WEP

Otra opción para descifrar la clave WEP de una red wireless es realizar un ataque por fuerza bruta contra un único paquete de datos capturado, cifrado mediante WEP.

Para conseguir paquetes de datos de una red wireless es necesario seguir los pasos que hemos descrito anteriormente, es decir, poner la tarjeta en modo monitor, y realizar una captura de paquetes IV.

Atacar mediante fuerza pura (probar todas las combinaciones posibles) solamente es viable contra clave WEP de 40 bits. Incluso en un tamaño tan pequeño como este podríamos hablar de 50 días de trabajo de un Pentium III.

A pesar de ello, podemos servirnos de diccionarios para aumentar la viabilidad y efectividad de este ataque, pudiendo realizar un ataque potencialmente peligroso a claves WEP de 128 bits e incluso de mayor tamaño. Por eso recomendable no subestimar este tipo de ataque.

Si tenemos en cuenta las vulnerabilidades de este cifrado, que no es otro que RC4. Podríamos llegar a reducir la potencia del cifrado de encriptación. Esto reduciría el tiempo de ataque por fuerza bruta a unos 35 segundos en un Pentium III a 500MHz y a 90 segundos en una máquina Pentium II a 233MHz [27]. Es decir, bastarían unos segundos para descifrar la clave WEP con los microprocesadores más actuales.

Para romper estos cifrados se utiliza unas herramientas conocidas como Wep_tools y Dwepcrack (Linux).

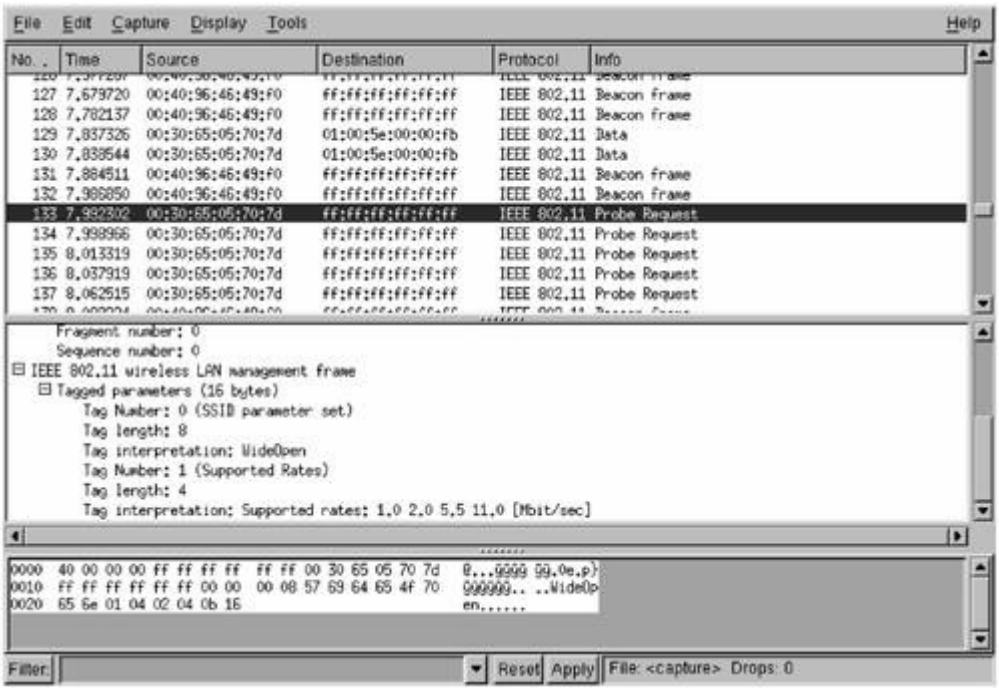


FIGURA 30. Dwepcrack bajo Linux.

También podemos probar a realizar un ataque de diccionario contra un único paquete de datos o contra volcados de tráfico de tamaño limitado (no 24 Gb) usando WepAttack.

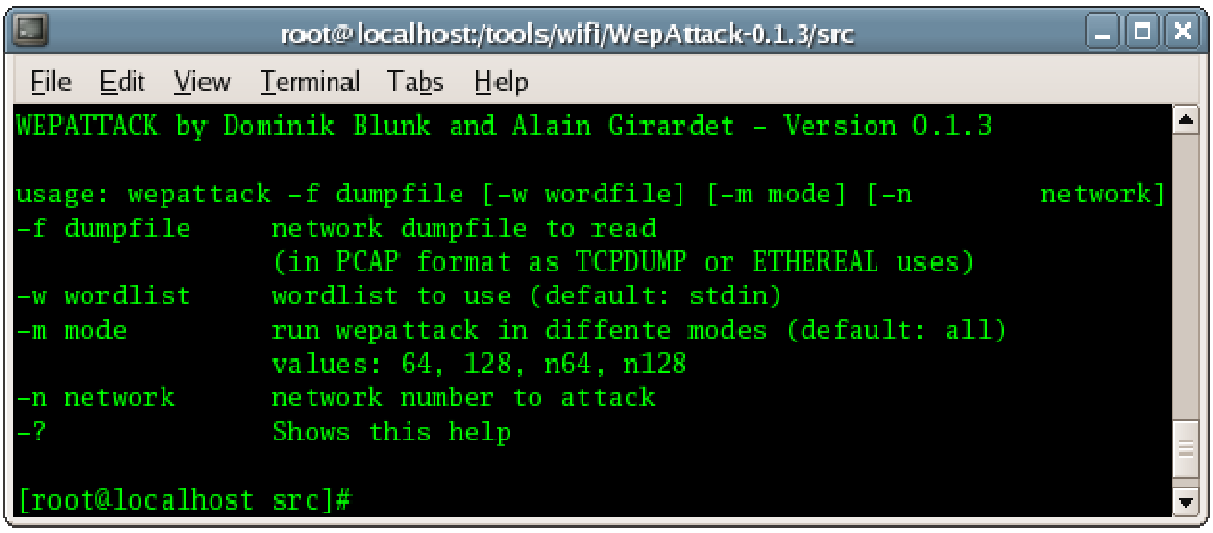


FIGURA 31. WepAttack bajo Linux.

6.8 Sacar la clave WEP en Windows

Si tenemos acceso físico a una de las máquinas de la red (con sistema operativo Windows) podremos extraer la clave WEP, ahorrándonos tiempo de trabajo.

Para ello podemos usar el programa WZCOOK incluido en la última versión de Aircrack. Este programa es experimental, así que puede o no funcionar dependiendo del nivel de nuestro Service Pack (SP) [28].

Este programa utiliza la utilidad de configuración rápida de Windows XP llamada Wireless Zero Configuration tools (servicio de Windows XP) para recuperar la clave WEP. Así que simplemente ejecutando esta utilidad te aparece la clave WEP de la red inalámbrica del sistema, sin más, por lo que cualquier persona que acceda a un ordenador que se encuentre dentro de una red inalámbrica y ejecute este programa podrá obtener la clave WEP [29].

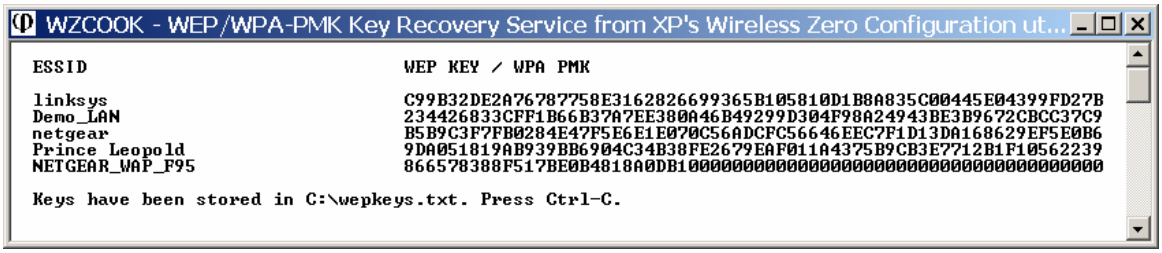


FIGURA 32. Wzcook.

6.9 Obstáculos en el ataque

A la hora de realizar los tipos de ataque explicados podemos encontrarnos algunas barreras que se despliegan como medidas básicas e insuficientes de seguridad, con la intención de desanimar a los atacantes. Un atacante avanzado habitualmente no suele ser peligroso. Las medidas que comentaremos a continuación son las más comunes, no por esto las únicas:

Broadcast del ESSID desactivado: Al desactivar el BROADCAST del ESSID el AP deja de emitir marcos baliza (beacon frames) y la red aparece como no en uso. Un programa que haga barrido activo no la detectará y sin embargo si lo conseguiremos mediante un barrido pasivo, ya que los paquetes siguen en el aire. Como ya hemos dicho el ESSID es el nombre de red y es vital para poder asociarnos a ella, en este caso no podremos visualizarlo y aunque logremos romper el WEP no tendremos nada que hacer.

La solución es que cuando está desactivado (el ESSID se envía en marcos de respuesta -request frames-), el ESSID sigue enviándose en paquetes de petición de asociación y reasociación. Entonces deberemos esperar con un "husmeador" activado a que un usuario se conecte a la red (ese paquete contendrá el nombre de la red).
Pero si no queremos realizar esta espera, existen utilidades para realizar un ataque "DoS" como Air-jack toolkit que, entre otras, lleva una aplicación llamada essid_jack,

cuya función concreta es provocar que los clientes se tengan que reasociar al punto de acceso y así capturar el paquete de asociación que contiene el ESSID. Pero esto ya entra en un nivel alto para usuarios avanzados.

Filtrado de direcciones MAC (ACL): Esta medida consiste en permitir solamente la conexión a cierto equipos atendiendo a su MAC. Sin embargo es posible cambiar la dirección MAC de nuestra tarjeta utilizando software específico, de este modo suplantaríamos la identidad de una de las máquinas de confianza (trusted). Esta técnica se conoce como MAC spoofing. Para saber que MAC deberemos emular, utilizaremos un husmeador (el más idóneo es Kismet) [30].

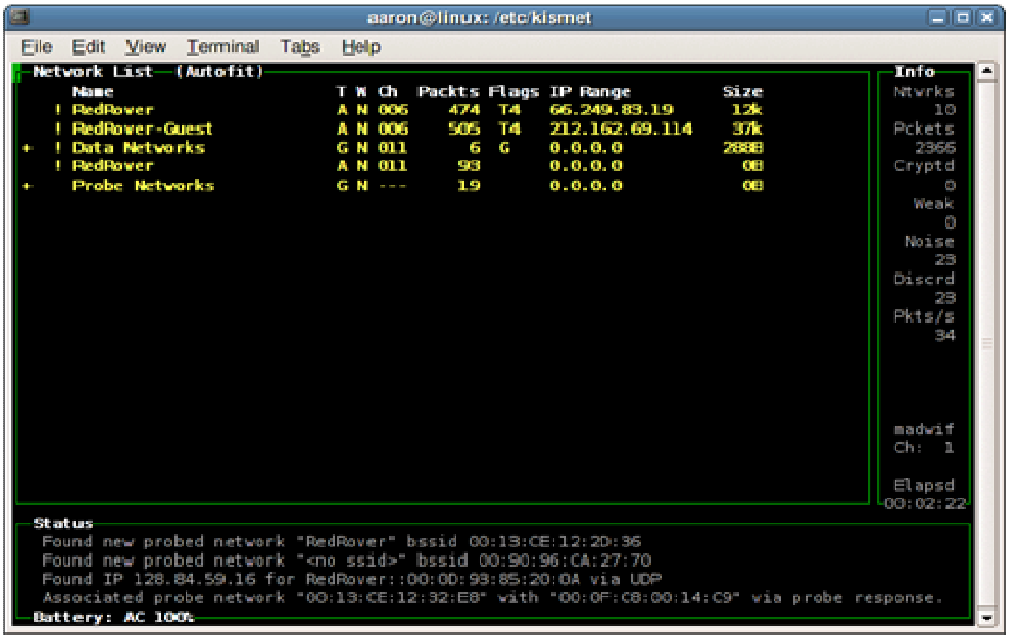


FIGURA 33. Kismet.

7. Conclusiones

Con la tecnología inalámbrica aplicada al mundo de las redes de ordenadores se nos abre todo un mundo de posibilidades de conexión, dejando a un lado la utilización del cableado clásico, proporcionando una flexibilidad y comodidad sin precedentes en la conectividad entre ordenadores.

Sin embargo, esta tecnología también presenta inconvenientes. Y precisamente tiene como mayor inconveniente la principal de sus ventajas, el acceso al medio compartido de cualquiera con el material y los métodos adecuados, es decir, que mediante el uso de las técnicas apropiadas cualquier intruso puede acceder a nuestra red en un momento dado.

Este hecho proporciona un elevado riesgo de seguridad que tendremos que tener presente a la hora de decantarnos por utilizar este tipo de tecnología para construir una red de ordenadores. Este riesgo siempre va a existir y además crecerá en igual medida (o más rápido) que las soluciones aportadas para intentar subsanar estos riesgos.

Por lo tanto, es recomendable utilizar una política de seguridad lo más homogénea posible y sin fisuras, que trate de corregir todos aquellos aspectos que comporten riesgo. Pero también deberemos tener en cuenta que esta política que elijamos no comprometa la rapidez de la red y que siga manteniendo todas las virtudes y ventajas de las redes inalámbricas.

Entrando a evaluar las distintas políticas de seguridad que tenemos a nuestro alcance, es inevitable centrarnos en el campo de los protocolos de seguridad. Un protocolo de seguridad define las reglas que gobiernan las comunicaciones entre ordenadores, diseñadas para que el sistema pueda soportar ataques de carácter malicioso. Disponemos de varios de estos protocolos para proteger una red inalámbrica.

El más extendido es sin duda el protocolo WEP, protocolo utilizado por defecto en la principal compañía de telefonía de nuestro país. Sin embargo, este protocolo es fácilmente vulnerable, incluso para atacantes de perfil bajo en conocimientos de hacking.

Este dato unido al cada vez más creciente uso de redes WiFi, nos debe llevar sin duda a la reflexión sobre el estado de la seguridad de nuestras redes.

Es por ello por lo que no deberíamos dejar de lado el aspecto de la seguridad de nuestra red una vez instalada por el proveedor que hayamos elegido. Es necesario avanzar en este aspecto si no queremos ser víctima de los ataques de algún intruso. En este sentido lo más recomendable sería actualizar nuestro protocolo de seguridad de WEP a WPA.

Ningún protocolo es totalmente seguro, pero con este cambio nos garantizaríamos un nivel de seguridad mucho más fiable y un acceso por parte de terceros al alcance sólo de los más expertos en la materia. Además existen una serie de estrategias asociadas a este protocolo que de llevarlas a cabo lo harían muy aceptablemente fiable, casi infranqueable.

Por último, siempre nos queda intentar ponernos al otro lado e intentar acceder a nuestra propia red como si de un intruso nos tratáramos, utilizando técnicas de hacking y viendo realmente en que medida nuestra red es o deja de ser segura.

Agradecimientos

A la Universidad Politécnica de Valencia por la formación recibida y por poner todos los medios de los que dispone a mi servicio.

Al director del proyecto Juan Vicente Oltra Gutiérrez por el seguimiento que ha realizado en el desarrollo de este proyecto y por prestarme ayuda en cada una de las dudas que me han ido surgiendo.

Glosario

Access Point: (Punto de Acceso o AP). Es el dispositivo que hace de puente entre la red cableada y la red inalámbrica. Podemos pensar que es, de alguna manera, la antena a la que nos conectaremos.

Accesorio Wi-Fi: Es el accesorio adicional que usaremos para incorporar el estándar 802.11 a nuestro equipo (PDA, ordenador portátil o de sobremesa), en caso de no tener Wi-Fi integrado. Estos accesorios pueden encontrarse en formato de tarjetas PCMCIA (para portátil), PCI y USB (para ordenadores de sobremesa).

Bridge: Une dos redes de área local cableadas en localizaciones diferentes usando una conexión inalámbrica de alta velocidad. Mantiene una conexión permanente entre las redes cableadas que pueden estar separadas por una carretera, campo, parking o cualquier espacio abierto.

DHCP: Tecnología utilizada en redes que permite que los equipos que se conecten a una red (con DHCP activado) auto-configuren los datos dirección IP, máscara de subred, puerta de enlace y servidores DNS, de forma que no haya que introducir estos datos manualmente. Por defecto la mayoría de los routers ADSL y los Puntos de Acceso tienen DHCP activado.

Dirección IP: (IP Address). Una dirección IP es una serie de números que identifica a nuestro equipo dentro de una red.
Distinguimos entre **IP pública** (Ej. 80.20.140.56), cuando es la dirección que nos identifica en Internet (por ejemplo la IP de tu router ADSL en Internet) e **IP privada** (Ej. 192.168.0.2), que es la dirección que identifica a un equipo dentro de una red local (LAN).

Dirección MAC: (MAC Address – Media Access Control). Es el código único de identificación que tienen todas las tarjetas de red. Nuestro accesorio Wi-Fi, nuestro equipo portátil, PC de sobremesa o nuestro PDA con Wi-Fi integrado, al ser un dispositivo de red, también tendrá una dirección MAC única.
Las direcciones MAC son **únicas** (ningún dispositivo de red tiene dos direcciones MAC iguales) y **permanentes** (ya que vienen preestablecidas de fábrica y no pueden modificarse).

Firewall: Un dispositivo que hace que una red o un PC esté mas seguro limitando y previniendo accesos del mundo exterior. Una vez que un ordenador está permanentemente conectado a Internet un firewall es esencial.

Hot Spot: Una conexión Wi-Fi pública que podemos usar para navegar por Internet.

IEEE: La abreviatura de Institute of Electrical and Electronic Engineers, pronunciada i-e-cubo. Fundada en 1884 como AIEE; la IEEE se formalizó en 1963 cuando la AIEE se fusionó con la IRE. IEEE es una organización compuesta por ingenieros, científicos y

estudiantes. LA IEEE es muy conocida por el desarrollo de estándares para la industria de la electrónica y la computación. En particular, el estándar IEEE 802 para redes de área local es seguido masivamente.

Infraestructura: Modo de conexión en una red wireless que define que nuestro equipo (PDA, portátil u ordenador de sobremesa) se conectará a un Punto de Acceso. El modo de conexión deberá de especificarse en la configuración de nuestro equipo o del accesorio Wi-Fi.

Máscara de subred: (Subnet Address). Cifra de 32 bits que específica los bits de una dirección IP que corresponde a una red y a una subred. Normalmente será del tipo 255.255.255.0

Puerta de enlace: (Gateway). Es la dirección IP privada de nuestro router.

Roaming: En las redes inalámbricas, el término roaming se refiere a la posibilidad de moverse desde el área de cobertura de un AP (Access Point) a otro sin interrupción en el servicio o perder la conectividad.

Servidores DNS: (DNS Server). Las páginas web también tienen su dirección IP pública y es a través de ésta dirección como en realidad nos conectamos a ellas. Pero es más sencillo memorizar o escribir el nombre del dominio (www.google.es) que su dirección IP (216.239.59.104). Para no memorizar las direcciones IP tenemos los servidores DNS. Un servidor DNS es un servidor en donde están almacenadas las correlaciones entre nombres de dominio y direcciones IP.

SSID: (Service Set Identification). Nombre con el que se identifica a una red Wi-Fi. Este identificador viene establecido de fábrica pero puede modificarse a través del panel de administración del Punto de Acceso.

USB: Un sistema de expansión barato y fácil de usar que está muy implementado en los equipos de sobremesa y portátiles. USB permite conectar rápidamente nuevos dispositivos al ordenador.

WEP: WEP es la abreviatura de Wired Equivalent Privacy, un protocolo de seguridad para redes de área local inalámbricas definido en e el estándar 802.11 b. WEP se diseña para proveer el mismo nivel de seguridad que se obtiene en redes locales cableadas.

Wi-Fi: Organización que certifica la interoperabilidad de dispositivos 802.11 como un estándar compatible y global de redes WLAN.

WLAN: LAN inalámbrica.

WPA: Wi-Fi Protected Access es un nuevo estándar diseñado que aparece en escena para optimizar la seguridad de redes inalámbricas. El nuevo estándar, está dirigido a clientes corporativos que quieren optimizar la seguridad. WPA reemplazará el estándar actual (WEP) Wired Equivalent Privacy. WEP utiliza claves fijas de encriptación. WPA utiliza usa el protocolo TKIP (Temporal Key Integrity Protocol), que genera nuevas claves cada 10 K de datos transmitidos en la red, haciendo la red bastante mas segura.

Referencias

[1] Josito (2007). http://www.configurarequipos.com/doc538.html Córdoba. 26/01/2010

[2] Wikitel (2009). http://www.wikitel.info/wiki/WiFi Barcelona. 26/01/2010

[3] Kioskea (2008). http://es.kioskea.net/contents/wifi/wifiintro.php3 26/01/2010

[4] Wikipedia (2010). http://es.wikipedia.org/wiki/Wi-Fi 26/01/2010

[5] elhacker (2010) http://www.elhacker.net/Textos1.htm

[6] José López García (2004) https://infonet.siemens.es/Newsletter_I&C/newsletter_eVoluciona_n7/pdf/SIC_58_SIEMENS.pdf 01/02/2004

[7] José Julio Ruiz (2004) http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridad_en_redes_inalambricas_WiFi.shtml Madrid. 24/08/2004

[8] Vic_Thor (2005) http://www.wadalbertia.org/foro/viewtopic.php?t=5589 28/01/2005

[9] Saulo Barajas (2004) http://www.saulo.net/pub/inv/SegWiFi-art.htm Madrid. 01/06/2004

[10] Wikipedia (2010) http://es.wikipedia.org/wiki/RC4 02/03/2010

[11] manombolo (2008) http://es.kioskea.net/faq/56-wifi-curso-de-introduccion 04/08/2008

[12] Unravel (2005) http://foro.elhacker.net/hacking_wireless/vulnerabilidades_del_cifrado_wep-t54992.0.html 25/01/2005

[13] Alegsa (2010) http://www.alegsa.com.ar/Dic/wpa.php

[14]  mixtron (2007) http://kdocs.wordpress.com/2007/02/12/diferencia-entre-wep-y-wpa/ 12/02/2007

[15]  Wireless Fidelity Alliance (2010) http://www.wi-fi.org

[16]  "Port-Based Network Access Control", IEEE Std 802.1X-2001, junio de 2001.

[17]  L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, marzo de 1998.

[18]  C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, junio de 2000.

[19]  W. Simpson, "The Point-to-Point Protocol (PPP)", RFC 1661, julio de 1994.

[20]  Kioskea (2008) http://es.kioskea.net/contents/wifi/wifi-wpa2.php3 16/10/2008

[21]  Elhacker (2010) http://hwagm.elhacker.net/wpa/wpa.htm

[22]  Iber-x (2008) http://www.iber-x.com/observatorio.php

[23]  Inteco (2008) http://www.inteco.es/

[24]  Bandaancha (2008) http://bandaancha.eu/

[25]  elhacker (2005) http://foro.elhacker.net/hacking_wireless/sniffer_para_mirar_el_trafico_de_una_wireless-t64149.0.html 31/03/2005

[26]  elhacker (2005) http://foro.elhacker.net/wireless_en_windows/texto_sobre_inseguridad_en_redes_80211-t64705.0.html 03/04/2005

[27]  elhacker (2005) http://foro.elhacker.net/hacking_wireless/hack_wep_con_centrino-t64471.0.html 02/04/2005

[28]  elhacker (2005) http://foro.elhacker.net/hacking_wireless/mas_wifi-t56008.0.html;msg281743 12/03/2005

[29]  elhacker (2005) http://foro.elhacker.net/hacking_wireless/manual_aircrack_para_windows_xp-t61344.0.html 11/03/2005

[30]  elhacker (2005) http://foro.elhacker.net/hacking_basico/cambio_direccion_mac-t63350.0.html 25/03/2005