UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

INGENIERÍA EN COMPUTACIÓN

"SEGURIDAD EN LAS REDES INALAMBRICAS"

Tesis presentada para la obtención del título de Ingeniero en Computación.

AUTOR: Yazmin Teoyotl Calderón

TUTOR: Profra. Silvia Vega Muytoy

Febrero de 2013

AGRADECIMIENTOS

A mis Padres.

Por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo a través del tiempo.
Todo este trabajo ha sido posible gracias a ellos.

A mis familiares.

A mi hermano Jos por sus regaños y sus consejos pero sobre todo por su apoyo y comprensión en momentos difíciles.
A mis abuelos por estar siempre cerca de mí, apoyándome a lo largo de mi vida.
Y a todos aquellos que participaron directa o indirectamente en la elaboración de esta tesis.

A mis amigos.

Que me apoyaron mutuamente a lo largo de toda mi formación profesional, a todos aquellos que se preocuparon por mí y que me han estado conmigo. Pero sobre todo gracias a todos aquellos que contribuyeron conmigo para realizar este trabajo, a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

A mis maestros.

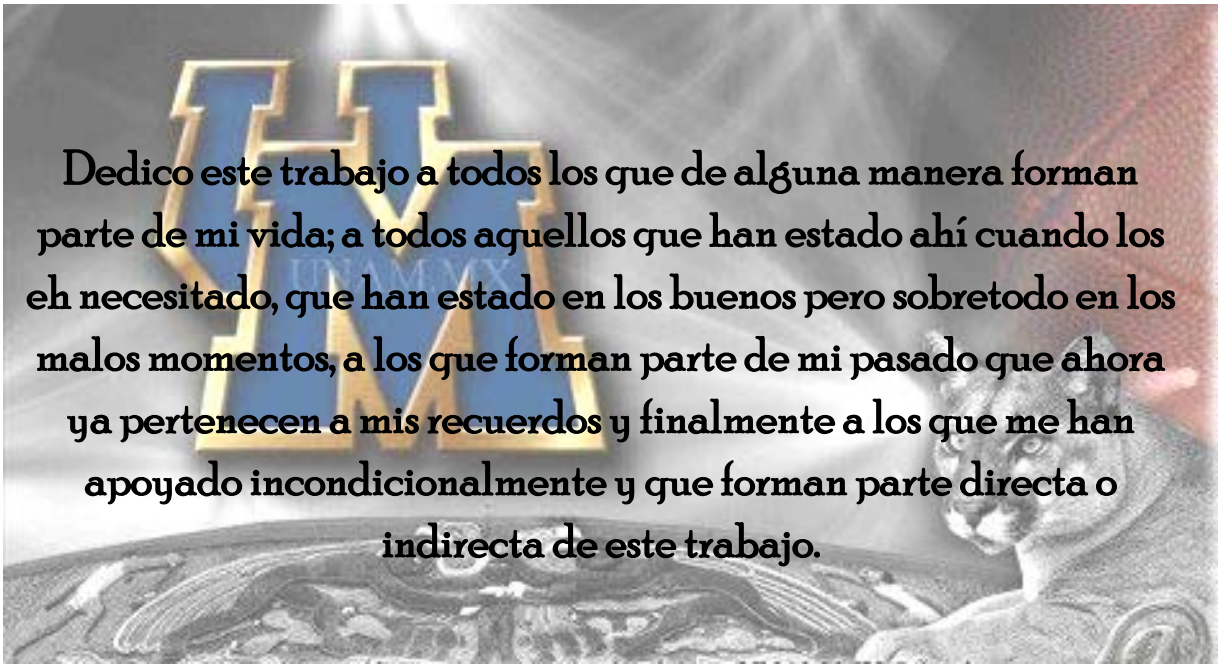
Que tuve a lo largo de este camino, Gracias por compartir conmigo su sabiduría y sus conocimientos, por su gran apoyo, dedicación y motivación para la culminación de mis estudios.

A ti

Por qué poco a poco te fuiste adentrando en mi vida, por ser esa persona que me escucha y me da consejos, por enseñarme tantas cosas y compartir conmigo tus conocimientos.

¡GRACIAS A TODOS USTEDES!

DEDICATORIA



ÍNDICE

CAPÍTULO 2:WEP Y WPA

CAPÍTULO 3: WPA2 (IEEE 802.11i)

OBJETIVOS

OBJETIVOS GENERALES

- El presente trabajo tiene como objetivo comprender los conceptos básicos de seguridad informática
- Describir los principales problemas de seguridad informática con los que se enfrentas los usuarios de computadoras.
- Conocer varios conceptos que nos ayuden a entender más acerca de este tema
- Conocer los factores de riegos
- Conocer los mecanismos de seguridad informática existentes.
- Concientizar sobre los riesgos a los que las organizaciones y usuarios de computadoras se enfrentan en materia de seguridad de la información
- Y por último ampliar o enriquecer los conocimientos acerca de la seguridad informática.

OBJETIVOS DEL TEMA

La seguridad informática se resume, por lo general, en cinco objetivos principales:

- **Integridad**: garantizar que los datos sean los que se supone que son
- **Confidencialidad**: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.
- **Disponibilidad**: garantizar el correcto funcionamiento de los sistemas de información.
- **Evitar el rechazo**: garantizar de que no pueda negar una operación realizada.
- **Autenticación**: asegurar que sólo los individuos autorizados tengan acceso a los recursos.

INTRODUCCIÓN

Todos los inventos y descubrimientos que se han registrado a través de nuestra historia, son el resultado de los estudios e investigaciones de un gran número de científicos, efectuados a lo largo de muchos siglos, encontrándose en este contexto el sistema computacional y con ello la computadora como herramienta importante.

Se puede considerar que la computación es la disciplina que busca establecer una base científica para resolver problemas mediante el uso y manejo de dispositivos electrónicos y sistemas computacionales, esto es, todo un conjunto de conocimientos científicos y tecnológicos (bases teóricas, métodos, metodologías, técnicas, y tecnologías) que hacen posible el procesamiento automático de los datos mediante el uso y manejo de computadoras, para producir información útil y significativa para el usuario. En otras palabras, la computación e informática son las ciencias del tratamiento automático de la información mediante una computadora (llamada también ordenador o computador).

Así, como herramienta tecnológica, se puede decir que una computadora es un sistema digital capaz de procesar datos a partir de un grupo de instrucciones denominado programa. La estructura básica de una computadora incluye microprocesador (CPU), memoria y dispositivos de entrada/salida (E/S), junto a los buses que permiten la comunicación entre ellos. La característica principal que la distingue de otros dispositivos similares, es que puede realizar tareas muy diversas, cargando distintos programas en la memoria para que los ejecute el procesador.

Con el avance de la tecnología se crea todo un conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más ordenadores o computadoras, dando lugar a lo que comúnmente se denomina "red". Al igual que en el sistema computacional normal, una red se encuentra

integrada por un software y un hardware; el primero consiste en programas informáticos que establecen protocolos o normas, para que las computadoras se comuniquen entre sí, y el segundo está formado por los componentes que unen a las computadoras.

Los usuarios de una red pueden compartir ficheros, impresoras y otros recursos, enviar mensajes electrónicos y ejecutar programas en otras computadoras.

El embrión de internet fue concebido a finales de los años 60's, se llamaba ARPANET y su misión era conectar los ordenadores de diferentes instituciones militares, a fin de que las comunicaciones no se interrumpieran si algunas de estas instituciones eran destruidas, para lo que se crearon unos protocolos (normas para enviar información) que permiten ser interpretados por todas las computadoras, independientemente del sistema operativo. Estas normas se conocen con el nombre TCP/IP.

La seguridad es un aspecto que cobra especial relevancia cuando se habla 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 ajeno a la dependencia de la empresa podría acceder a la red con solo ubicarse dentro del área delimitada por la señal. Pol lo que en caso de un atague pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibilitaran una identificación posterior.

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

Conscientes de este problema, el IEEE[1] publicó un mecanismo opcional de seguridad denominado WEP[2], en la norma de redes inalámbricas 802.11. Pero WEP, desplegado en numerosas redes WLAN, ha sido roto de distintas formas, lo que lo ha convertido en una protección inservible.
Para solucionar sus deficiencias, el IEEE comenzó el desarrollo de una nueva norma de seguridad conocida como 802.11i, que permitiera dotar de suficiente seguridad a las redes WLAN[3].

El problema de 802.11i radica en su demora para ver la luz. Algunas empresas, en vista de que WEP era insuficiente y de que no existían alternativas estandarizadas mejores, decidieron utilizar otro tipo de tecnologías, como son las VPNs[4], para asegurar los extremos de la comunicación. La idea de proteger los datos de usuarios remotos, conectados desde Internet a la red corporativa se extendió, en algunos entornos, a las redes WLAN. Ambos canales de transmisión deben considerarse inseguros, pero la tecnología VPN es quizás demasiado costosa en recursos para su implementación en redes WLAN.

No ajena a las necesidades de los usuarios, la asociación de empresas Wi-Fi[5] decidió lanzar un mecanismo de seguridad intermedio de transición hasta que estuviese disponible el 802.11i, tomando aquellos aspectos que estaban suficientemente avanzados en desarrollo de la norma. El resultado, fue WPA[6].

Este trabajo está compuesto por cuatro grandes capítulos:

Capítulo 1: La red inalámbrica y sus inseguridades

Este capítulo nos da una breve explicación de lo que son las redes inalámbricas, los tipos de redes inalámbricas que existen, características, aplicaciones, ventajas y desventajas, principales vulnerabilidades a las que se enfrentan,

[1] IEEE : Instituto de Ingenieros Eléctricos y Electrónicos. http://www.ieee.org
[2] WEP: Wired Equivalent Privacy, protocolo de encriptación por defecto para redes 802.11
[3] WLAN : Wireless local área network, red de área local inalámbrica.
[4] VPNs: de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada.
[5] WiFi: es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.
[6] WPA: Wireless Protected Access, implementación de una versión temprana del estándar 802.11i, basada en el protocolo de encriptación TKIP.

mecanismos de seguridad, y terminamos el capítulo con algunas recomendaciones para tener una mejor seguridad en nuestra red.

Capítulo 2:WEP y WPA

En este capítulo analizaremos dos protocolos el WEP y WPA.
En la primera parte empezamos con la definición del protocolo WEP, se hace mención brevemente de su historia, se explican algunas de sus características (como lo son el tipo de estándar en el que se basa, cifrado, autentificación y algoritmos), vulnerabilidades, se explica el procedimiento para obtener la clave de seguridad de una red mediante el uso del programa Aircrack, finalmente terminaremos con las vulnerabilidades de este protocolo.

Para la segunda parte tendremos la definición de WPA, características y su funcionamiento, vulnerabilidades y finalmente cerraremos el capítulo con las mejoras que tiene WPA respecto a WEP.

Capítulo 3: WPA2 (IEEE 802.11i)

En este capítulo daremos la definición de WPA2, características, funcionamiento y cerraremos con sus vulnerabilidades.

Capítulo 4: Recomendaciones para conseguir una red inalámbrica más segura

Terminamos con este capítulo en el cual veremos algunas recomendaciones para conseguir una red inalámbrica más segura, definiremos warchalking y wardriving, definiremos lo que es un mecanismo de seguridad y presentaremos cinco métodos para garantizar una mejor seguridad analizando para ello sus ventajas y desventajas.

Capítulo 1: LA RED INALÁMBRICA Y SUS INSEGURIDADES

No fue sino hasta 1971 cuando un grupo de investigadores bajo la dirección de Norman Abramson de la Universidad de Hawaii, crearon el primer sistema de conmutación de paquetes mediante una red de comunicación por radio, dicha red se llamó ALOHA. Ésta es la primera red de área local inalámbrica (WLAN), estaba formada por 7 computadoras situadas en distintas islas que se podían comunicar con un ordenador central, al cual pedían que realizara cálculos. Uno de los primeros problemas que tuvieron y tiene todo nuevo tipo de red inventada fue el control de acceso al medio (MAC), es decir, el protocolo a seguir para evitar que las distintas estaciones solapen sus mensajes entre sí. En un principio se solucionó haciendo que la estación central emitiera una señal intermitente en una frecuencia distinta a la del resto de computadoras, mientras estuviera libre, de tal forma que, cuando una de las otras estaciones se disponía a transmitir, antes "escuchaba" y se cercioraba de que la central estaba emitiendo dicha señal para entonces enviar su mensaje, esto se conoce como CSMA[7] (Carrier Sense Multiple Access).

Un año después, Aloha se conectó mediante ARPANET al continente americano. ARPANET es una red de computadoras creada por el Departamento de Defensa de los EEUU, como medio de comunicación para los diferentes organismos del país.[8]

1.1 RED INALÁMBRICA

El término red inalámbrica *(Wireless network)* es un término que se utiliza para designar la conexión de nodos, sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos y con las redes inalámbricas un usuario puede

[7] CSMA: se entiende por Acceso Múltiple por Detección de Portadora (Carrier Sense Multiple Access) el escuchar el medio para saber si existe presencia de portadora en los momentos en los que se ocupa el canal.

[8] **Historia de las redes inalámbricas**
http://histinf.blogs.upv.es/2010/12/02/historia-de-las-redes-inalambricas/
*Fecha de consulta: 22 de Noviembre de 2011

mantenerse conectado, cuando se desplaza dentro de una determinada área geográfica.

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo), en lugar de cableado estándar. Hay muchas tecnologías diferentes que se diferencian por la frecuencia de transmisión que utilizan, el alcance y la velocidad de sus transmisiones.

Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, ya se encuentren a unos metros de distancia, ya varios kilómetros. Asimismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente, como pasa con las redes cableadas

Por otro lado, existen algunas cuestiones relacionadas con la regulación legal del espectro electromagnético, porque las ondas electromagnéticas se transmiten a través de muchos dispositivos (de uso militar, científico y de aficionados), que son propensos a las interferencias. Por esta razón, todos los países necesitan regulaciones que definan los rangos de frecuencia y la potencia de transmisión que se permite a cada categoría de uso.

Además, las ondas hertzianas no se confinan fácilmente a una superficie geográfica restringida, por lo que un hacker puede con facilidad escuchar una red, si los datos que se transmiten no están codificados. Por lo tanto, se deben tomar medidas para garantizar la privacidad de los datos que se transmiten a través de redes inalámbricas.

Conceptos Básicos

La naturaleza de las redes Wireless hace que cualquier persona pueda tener acceso a los datos que son enviados, debido a que estos utilizan como medio de transmisión el aire (ondas electromagnéticas). Esto plantea un problema añadido con respecto al cable, pues para tener acceso a los datos transmitidos por cable, se ha de tener acceso al mismo o a los dispositivos asociados. Para las redes Wireless no es necesario, basta con que la señal viaje hasta nosotros. Por tanto, teniendo en cuenta esta perspectiva se han de implementar los mecanismos necesarios para mantener el nivel de seguridad que se requieren en muchos proyectos.
La revisión 802.11b del estándar original tiene una velocidad máxima de transmisión de 11 Mbps. El estándar 802.11b utiliza la frecuencia 2.4 Ghz que es

la misma que utilizan otros dispositivos móviles, como GPS, Bluetooth, etc. Esto puede incidir, para mal, en la calidad de la señal. Las interferencias hacen que se reduzca la velocidad, 802.11g tiene la ventaja de poder coexistir con los estándares 802.11a y 802.11b, esto debido a que puede operar con las Tecnologías RF DSSS[9] y OFDM.

Sin embargo, si se utiliza para implementar usuarios que trabajen con el estándar 802.11b, el rendimiento de la celda inalámbrica se verá afectado por ellos, permitiendo sólo una velocidad de transmisión de 22 Mbps. Esta degradación se debe a que los clientes 802.11b no comprenden OFDM.
El estándar 801.11i está dirigido abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integras – Seguras – Temporales), y AES (*Estándar de Cifrado Avanzado*), que se implementa en WPA2[10].

Se debe tener en cuenta que a mayor distancia entre el emisor y el receptor menor velocidad de transmisión. Otro problema que se puede plantear son los elementos intermedios que pueden interferir en la señal, como pueden ser paredes, campos magnéticos o electrónicos. Un aspecto más y que puede producir reducción de la transmisión es la saturación del espectro debido al número de usuarios.

Por último, se puede comentar que existen dos tipos de antenas, omnidireccionales y direccionales. En las primeras, la emisión de la onda se produce en todas las direcciones a discreción, útil para entornos abiertos donde la ubicación de las estaciones no está definida o es susceptible de ocupar cualquier situación física. El segundo tipo dirige la señal a un punto determinado fuera del mismo la señal no es "audible". Ideal para conectar dos puntos.

En 2004 se comenzó a trabajar en una nueva revisión, el 802.11n. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y unas 40 veces más rápida que una red bajo el estándar 802.11b. Este estándar se viene implementando desde 2008, 802.11n puede trabajar en dos bandas de

[9] RF DSSS: Radio frecuencia que funciona transmitiendo simultáneamente por varias frecuencias diferentes
[10] WPA2: Es una versión mejorada de WAP, basado en el estándar 802.11i.

frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

ESSID/SSID

Toda red Wireless tiene un ESSID (Extended Service Set Identifier, Servicio Extendido de identificación) que la identifica. Este consta de como máximo 32 caracteres. Es necesario conocer el ESSID del AP para poder formar parte de la red, es decir, el ESSID debe ser el mismo tanto en el AP como en el dispositivo móvil (cliente).

Existen algunas variantes principales del SSID. Las redes ad-hoc, que consisten en máquinas cliente sin un punto de acceso, utilizan el BSSID (Basic Service Set IDentifier); mientras que en las redes en infraestructura que incorporan un punto de acceso, se utiliza el ESSID.
Se puede referir a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como nombre de la red.

BSSID

Dirección MAC del punto de acceso. Éstas las emplean las tarjetas wireless para identificar y asociarse a redes inalámbricas.

Beacon Frames

Los Puntos de Acceso mandan continuamente "anuncios" de la red, para que los clientes móviles puedan detectar su presencia y conectarse a la red wireless. Estos anuncios son conocidos como "Beacon Frames". Esta propiedad puede ser deshabilitada en la mayoría de los AP actuales.

OSA (*Open System Authentication*)

Es un proceso de autenticación nulo, las tramas se envían en texto plano aun teniendo activado cualquier cifrado.

SKA (*Shared Key Authentication*)

Este método utiliza una clave compartida entre el Punto de Acceso y el cliente. El cliente envía un Authentication Request, mientras que el Punto de Acceso responde con un Authentication Challenge.

El cliente a su vez, responde con un Authentication Response (cifrado) y finalmente el Punto de Acceso responde con Authentication Result. Es dentro del SKA donde se pueden utilizar los diferentes sistemas de cifrados existente para redes Wireless.

WEP (*Wired Equivalent Privacy*)

Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits o de 128 bits. No se mencionará otra vez por ser inseguro.

WPA (Wired Protected Access)

Es un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias del sistema previo WEP. Se han encontrado varias debilidades en el algoritmo WEP, como la reutilización del vector de inicialización, del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros. Nació para paliar las deficiencias de seguridad de WEP. Implementa el estándar 802.11i.

WPA2 (Wired Protected Access 2)

Sistema de cifrado creado a partir del WPA, que corrige vulnerabilidades del anterior. WPA y WPA2 se diferencian poco conceptualmente y difieren principalmente en el algoritmo de cifrado que emplean. Mientras WPA basa el cifrado de las comunicaciones en el uso del algoritmo TKIP[11] (Temporary Key Integrity Protocol), que está basado en RC4 al igual que WEP, WPA2 utiliza CCMP[12] (Counter-mode/CBC-MAC Protocol), basado en AES (Advanced Encrytion System).

La segunda diferencia notable se encuentra en el algoritmo utilizado para controlar la integridad del mensaje. Mientras WPA usa una versión menos elaborada para la generación del código MIC (Message Integrity Code), o código "Michael", WPA2 implementa una versión mejorada de MIC.

[11]TKIP incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos.
[12]CCMP: es una encriptación de protocolo designada por productos Wireless LAN para la implementación del estándar IEEE 802.11i.

1.2 TOPOLOGÍAS DE UNA RED INALÁMBRICA

La topología de una red es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (e.g. computadoras, impresoras, servidores, hubs, switches, enrutadores, etc.) se interconectan entre sí sobre un medio de comunicación.

a) Topología física: Se refiere al diseño actual del medio de transmisión de la red.
b) Topología lógica: Se refiere a la trayectoria lógica que una señal a su paso por los nodos de la red.

Existen varias topologías de red básicas (ducto, estrella, anillo y malla), pero también existen redes híbridas que combinan una o más de las topologías anteriores en una misma red.

1.2.1 Modo Ad-Hoc

Esta topología se caracteriza porque no hay Punto de Acceso (AP), las estaciones se comunican directamente entre sí (peer-to-peer), de esta manera el área de cobertura está limitada por el alcance de cada estación individual; como se aprecia en la Imagen 1.1.
La naturaleza descentralizada de las redes ad hoc, hace de ellas las más adecuadas en aquellas situaciones en las que no puede confiarse en un nodo central y mejora su escalabilidad comparada con las redes inalámbricas tradicionales, desde el punto de vista teórico y práctico.

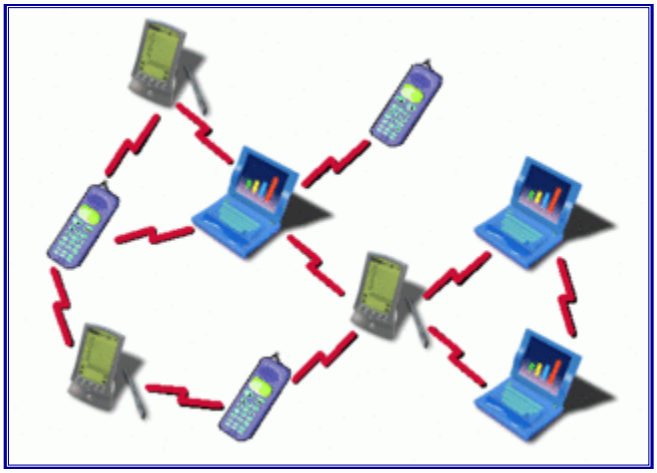


Imagen 1.1 Topología Ad-Hoc
No hay un punto de acceso determinado, y todos los equipos se comunican entre sí.

1.2.2 Modo Infraestructura

En el modo infraestructura se dispone como mínimo de un Punto de Acceso (AP) y las estaciones Wireless no se pueden comunicar directamente, todos los datos deben pasar a través del AP. Todas las estaciones deben ser capaces de ver y establecer conexión con el AP, como se aprecia en la Imagen 1.2.

La mayoría de las redes inalámbricas se pueden encontrar en las empresas utilizan el Modo Infraestructura con 1 ó más puntos de acceso. El AP actúa como un Hub en una red cableada y redistribuye los datos hacia todas las estaciones.

Si el punto de acceso se conecta a una red cableada, los clientes inalámbricos pueden acceder a la red fija a través del punto de acceso. Para interconectar muchos puntos de acceso y clientes inalámbricos, todos deben configurarse con el mismo SSID.

Es importante resaltar que, a diferencia del modo ad-hoc, los equipos inalámbricos no hablan directamente entre sí, sino que lo hacen a través de la unidad base, lo que ofrece más seguridad (gracias a la gestión ofrecida por la unidad base) y conectividad con los terminales situados en la red con cables.

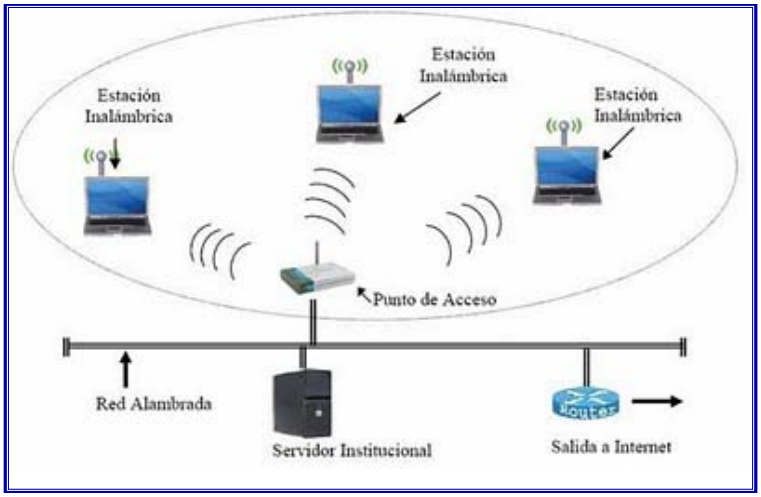


Imagen 1.2 Topología Infraestructura

En esta topología debe existir forzosamente un punto de acceso y todos los equipos se conectan a través de él.

1.2.3 Redes Mesh

Las redes inalámbricas Mesh, redes acopladas o redes de malla inalámbricas de infraestructura, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas: la topología Ad-hoc y la topología Infraestructura. Básicamente son redes con topología de infraestructura que permiten unirse a la red a dispositivos, que estan fuera del rango de cobertura de los puntos de acceso, como se aprecia en la Imagen 1.3. Por tanto, se utiliza una topología en malla (de ahí que se denominen redes acopladas) por la que los mensajes son transmitidos directamente entre las estaciones, aunque éstas no estén gestionadas por el mismo Punto de Acceso.

Imagen 1.3 Topología Red Mesh
Esta topología no es más que una mezcla de las topologías Ad-hoc e Infraestructura

1.3 CATEGORÍAS DE REDES INALÁMBRICAS

Por lo general, las redes inalámbricas se clasifican en varias categorías, de acuerdo al área geográfica desde la que el usuario se conecta a la red (*denominada área de cobertura*), como se puede apreciar en la Imagen 1.4.

En este tipo de red de cobertura personal, existen tecnologías basadas en HomeRF[13], Bluetooth (protocolo que sigue la especificación IEEE 802.15.1), ZigBee (basado en la especificación IEEE 802.15.4 y utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo

[13] HomeRF: estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central.

consumo), RFID (sistema remoto de almacenamiento y recuperación de datos) con el propósito de transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

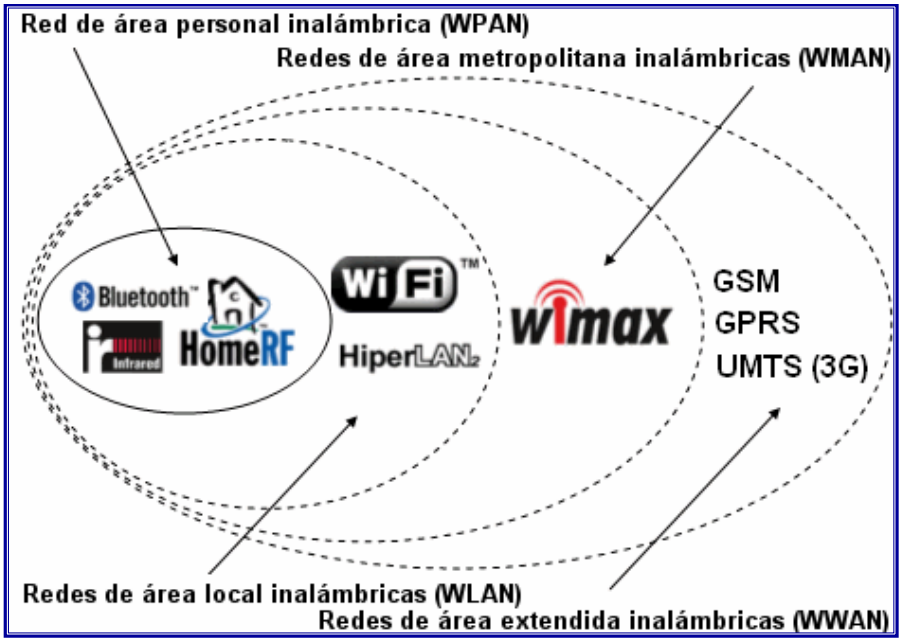


Imagen 1.4 Wireless Personal Área Network
Denominación de una red a partir del área de cobertura.

Una red inalámbrica es aquella que permite a sus usuarios conectarse a una red local o a Internet sin estar conectado físicamente; sus datos (paquetes de información) se transmiten por el aire.

Al montar una red inalámbrica, hay que contar con una Computadora que sea un "Punto de Acceso" y las demás computadoras serán "dispositivos de control", toda esta infraestructura puede variar dependiendo qué tipo de red que se requiere montar en tamaño y en la distancias de alcance de la misma.

1.3.1 De larga distancia.

Éstas redes son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps.

Tipos de redes de larga distancia:

Redes de conmutación de paquetes (públicas y privadas):

La Red Pública De Conmutación De Paquetes Por Radio no tiene problemas de pérdida de señal, debido a que su arquitectura está diseñada para soportar paquetes de datos, en lugar de comunicaciones de voz.

Las redes privadas de conmutación de paquetes utilizan la misma tecnología que las públicas, pero bajo bandas de radio frecuencia restringida por la propia organización de sus sistemas de cómputo.

En las redes de área local se pueden encontrar tecnologías inalámbricas basadas en HIPERLAN (*High Performance Radio LAN*), un estándar del grupo ETSI, o tecnologías basadas en Wi-Fi, que siguen el estándar IEEE 802.11 con diferentes variantes.

Para redes de área metropolitana se encuentran tecnologías basadas en WiMAX (*Worldwide Interoperability for Microwave Access, es decir, Interoperabilidad Mundial para Acceso con Microondas*), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMAX es un protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda. También se pueden encontrar otros sistemas de comunicación como LMDS (*Local Multipoint Distribution Service*).

Una WWAN difiere de una WLAN (*wireless local área network*) en que usa tecnologías de red celular de comunicaciones móviles como WiMAX (aunque se aplica mejor a Redes WMAN), UMTS (*Universal Mobile Telecommunications System*), GPRS, EDGE, CDMA2000, GSM, CDPD, Mobitex, HSPA y 3G para transferir los datos. También incluye LMDS y Wi-Fi autónoma para conectar a internet; como se observa en la Imagen 1.5

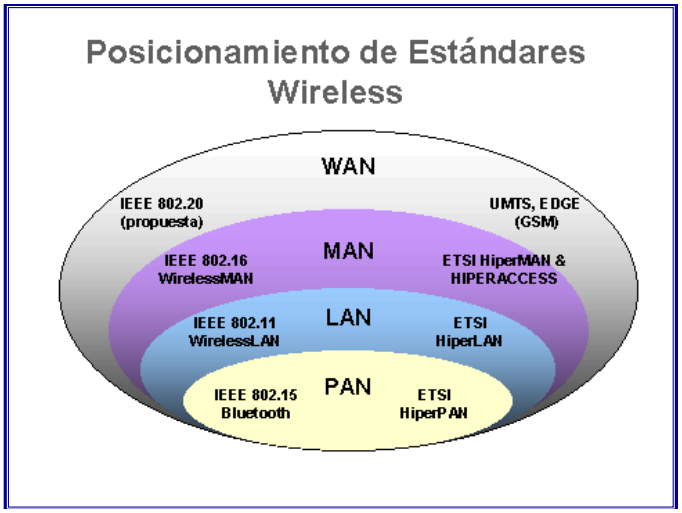


Imagen 1.5 Posicionamiento de Estándares Wireless

1.3.2 De corta distancia.

Éstas son utilizadas principalmente en redes corporativas, cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre sí, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

1.4 CARACTERÍSTICAS DE LAS REDES INALÁMBRICAS

Según el rango de frecuencias utilizado para transmitir, el medio de transmisión pueden ser las ondas de radio, las microondas terrestres o por satélite, y los infrarrojos, por ejemplo. Dependiendo del medio, la red inalámbrica tendrá unas características u otras:

- **Ondas de radio:** las ondas electromagnéticas son omnidireccionales, así que no son necesarias las antenas parabólicas. La transmisión no es sensible a las atenuaciones producidas por la lluvia, ya que se opera en frecuencias no demasiado elevadas. En este rango se encuentran las bandas desde la ELF que va de 3 a 30 Hz, hasta la banda UHF que va de los 300 a los 3000 MHz, es decir, comprende el espectro radioeléctrico de 30 ~ 3000000000 Hz.

- **Microondas terrestres:** se utilizan antenas parabólicas con un diámetro aproximado de unos tres metros. Tienen una cobertura de kilómetros, pero con el inconveniente de que el emisor y el receptor deben estar perfectamente alineados; por eso se acostumbran utilizarlas en enlaces

punto a punto en distancias cortas. En este caso, la atenuación producida por la lluvia es más importante, ya que se opera a una frecuencia más elevada. Las microondas comprenden las frecuencias desde 1 hasta 300 GHz.

- **Microondas por satélite:** se hacen enlaces entre dos o más estaciones terrestres que se denominan estaciones base. El satélite recibe la señal (denominada señal ascendente) en una banda de frecuencia, la amplifica y la retransmite en otra banda (señal descendente). Cada satélite opera en unas bandas concretas. Las fronteras frecuenciales de las microondas, tanto terrestres como por satélite, con los infrarrojos y las ondas de radio de alta frecuencia se mezclan bastante, así que puede haber interferencias con las comunicaciones en determinadas frecuencias.
- **Infrarrojos:** se enlazan transmisores y receptores que modulan la luz infrarroja no coherente. Deben estar alineados directamente o con una reflexión en una superficie. No pueden atravesar las paredes. Los infrarrojos van desde 300 GHz hasta 384 THz.

1.5 APLICACIONES DE LAS REDES INALÁMBRICAS

- Las bandas más importantes con aplicaciones inalámbricas, del rango de frecuencias que abarcan las ondas de radio, son la VLF (comunicaciones en navegación y submarinos), LF (radio AM de onda larga), MF (radio AM de onda media), HF (radio AM de onda corta), VHF (radio FM y TV), UHF (TV).

- Mediante las microondas terrestres, existen diferentes aplicaciones basadas en protocolos como Bluetooth o ZigBee para interconectar computadoras portátiles, PDAs, teléfonos u otros aparatos. También se utilizan las microondas para comunicaciones con radares (detección de velocidad u otras características de objetos remotos) y para la televisión digital terrestre.

- Las microondas por satélite se usan para la difusión de televisión por satélite, transmisión telefónica a larga distancia y en redes privadas, por ejemplo.

- Los infrarrojos tienen aplicaciones como la comunicación a corta distancia de las computadoras con sus periféricos. También se utilizan para mandos a distancia, ya que así no interfieren con otras señales electromagnéticas, por ejemplo la señal de televisión. Uno de los estándares más usados en estas comunicaciones es el IrDA (*Infrared Data Association*). Otros usos que tienen los infrarrojos son técnicas como la termografía, la cual permite determinar la temperatura de objetos a distancia.

1.6 VENTAJAS DE LAS REDES INALÁMBRICAS

Las principales ventajas que ofrecen las redes inalámbricas frente a las redes cableadas son las siguientes:

- **Movilidad.** La libertad de movimientos es uno de los beneficios más evidentes en las redes inalámbricas. Una computadora o cualquier otro dispositivo (por ejemplo, una PDA o una webcam) pueden situarse en cualquier punto dentro del área de cobertura de la red, sin tener que depender de la posibilidad de hacer llegar un cable hasta este sitio. Ya no es necesario estar atado a un cable para navegar en Internet, imprimir un documento o acceder a los recursos compartidos desde cualquier lugar de ella, hacer presentaciones en la sala de reuniones, acceder a archivos, etc., sin tener que tender cables a mitad de la sala o depender de la extensión del cable de red.

- **Desplazamiento.** Con una computadora portátil o PDA no sólo se puede acceder a Internet o a cualquier otro recurso de la red local, desde cualquier parte de la oficina o de la casa, sino que se puede desplazar sin perder la comunicación. Esto no sólo da cierta comodidad, sino que facilita el trabajo en determinadas tareas como, por ejemplo, la de aquellos empleados cuyo trabajo les lleva a moverse por todo el edificio.

- **Flexibilidad.** Las redes inalámbricas no sólo permiten estar conectados mientras hay desplazamiento con una computadora portátil, sino que también permite colocar una computadora de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio de configuración de la red. A veces, extender una red cableada no es una tarea fácil ni barata. En muchas ocasiones se acaba colocando peligrosos cables en el suelo para

evitar poner contactos de red más cercanos: las redes inalámbricas evitan todos estos problemas. Resulta también especialmente indicado para aquellos lugares en los que se necesitan accesos esporádicos. Si en un momento dado existe la necesidad de que varias personas se conecten en la red en la sala de reuniones, la conexión inalámbrica evita llenar el suelo de cables. En sitios donde pueda haber invitados que necesiten conexión a Internet (centros de formación, hoteles, cafés, entornos de negocio o empresariales), las redes inalámbricas suponen una alternativa mucho más viable que las redes cableadas.

- **Ahorro de costos.** Diseñar o instalar una red cableada puede llegar a alcanzar un alto costó no solamente económico, sino en tiempo y molestias. En entornos domésticos y en determinados entornos empresariales donde no se dispone de una red cableada, porque su instalación presenta problemas, la disposición de una red inalámbrica permite ahorrar costos al permitir compartir recursos: acceso a Internet, impresoras, etc.

- **Escalabilidad.** Se le llama escalabilidad a la facilidad de expandir la red, después de su instalación inicial. Conectar una nueva computadora cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta y listo. Con las redes cableadas esto mismo requiere instalar un nuevo cableado o, lo que es peor, esperar hasta que el nuevo cableado quede instalado.

1.7 DESVENTAJAS DE LAS REDES INALÁMBRICAS

Evidentemente, como todo en la vida no todo son ventajas, las redes inalámbricas también tienen unos puntos negativos en comparación con las redes de cable. Los principales inconvenientes de las redes inalámbricas son los siguientes:

- **Menor ancho de banda**. Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas Wi-Fi lo hacen a 11 Mbps. Es cierto que existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los

comienzos de su comercialización y tiene un precio superior al de los actuales equipos Wi-Fi.

- **Mayor inversión inicial**. Para la mayoría de las configuraciones de la red local, el costo de los equipos de red inalámbricos es superior al de los equipos de red cableada.

- **Seguridad.** Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Esto fundamentalmente es una ventaja, pero se convierte en una desventaja cuando se piensa que cualquier persona con una computadora portátil sólo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura no está definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan las redes Wi-Fi no es de lo más confiables. A pesar de esto, también es cierto que ofrece una seguridad válida para la inmensa mayoría de las aplicaciones, pues ya se dispone de un nuevo sistema de seguridad (WPA) que hace a Wi-Fi mucho más seguro.

- **Interferencias.** Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda de 2,4 GHz. Esta banda de frecuencias no requiere licencia administrativa para ser utilizada, por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes Wi-Fi funcionan en la misma banda de frecuencias incluida la de los vecinos. Este hecho hace que no se tenga la garantía del entorno radioelectrónico esté completamente limpio para que la red inalámbrica funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de la red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

- **Incertidumbre tecnológica**. La tecnología que actualmente se está instalando va adquiriendo una mayor popularidad; ejemplo de ello es la conocida como Wi-Fi (IEEE 802.11B). Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles

de seguridad. Es posible que cuando se popularice esta nueva tecnología, se deje de aplicar la actual o, simplemente se le deje de impulsar. Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades del cliente y, aunque existe una incógnita, los fabricantes no querrán perder el tirón que ha supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales. La historia ha dado muchos ejemplos similares.

1.8 ALGUNAS VULNERABILIDADES DE LAS REDES INALÁMBRICAS

El acceso sin necesidad de cables, razón que hace tan populares a las redes inalámbricas, es a la vez, el problema más grande de este tipo de redes en cuanto a seguridad se refiere. Cualquier equipo que se encuentre a 100 metros, o menos de un punto de acceso, podría tener acceso a la red inalámbrica.

Lo grave de esta situación es que muchos administradores de redes parecen no haberse dado cuenta de las implicaciones negativas de poseer puntos de acceso inalámbrico en la red de una empresa. Es muy común encontrar redes en las que el acceso a internet se protege adecuadamente con un firewall bien configurado, pero al interior de la red existen puntos de acceso inalámbrico totalmente desprotegidos e irradiando señal hacia el exterior del edificio. Cualquier persona que desde el exterior capte la señal del punto de acceso tendrá acceso a la red de la compañía, con la posibilidad de navegar gratis en la internet, emplear la red de la compañía como punto de ataque hacia otras redes y luego desconectarse para no ser detectado, robar software y/o información, introducir virus o software maligno, entre muchas otras cosas.

Un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que vulnera, por completo, la seguridad informática de la compañía. La mala configuración de un acceso inalámbrico es, desgraciadamente un hecho muy común.

Existen dos prácticas bien conocidas para localizar redes inalámbricas:

- El **warchalking,** que consiste en caminar por la calle con una computadora portátil dotado, de una tarjeta WLAN, buscando la señal de puntos de acceso. Cuando se encuentra un punto se pinta con tiza un

símbolo especial, como los que se aprecian en la Imagen 1.6; en la acera o en un muro, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no. De este modo, otras personas pueden conocer la localización de la red.

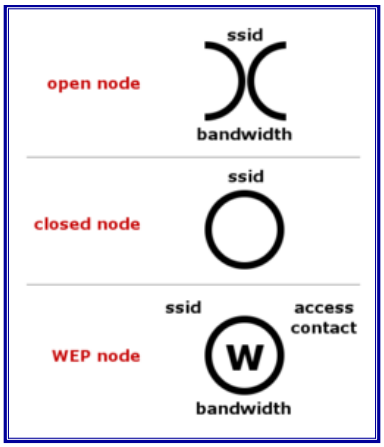


Imagen 1.6 Simbología del Warchalking[14]

- El **wardriving,** propio para localizar puntos de acceso inalámbrico desde un automóvil y para este fin, se necesita de un computador portátil con una tarjeta WLAN, una antena adecuada (que se puede elaborar fácilmente con una lata de conservas o de papas fritas, un GPS para localizar los puntos de acceso en un mapa y software para detección de redes inalámbricas, que se consigue libremente en el internet.

Una vez localizada una red inalámbrica, una persona podría llevar a cabo dos tipos de ataques:

- Ingresar a la red y hacer uso ilegítimo de sus recursos.
- Configurar un punto de acceso propio, orientando la antena de tal modo que las computadoras, que son clientes legítimos de la red atacada, se conecten a la red del atacante. Una vez hecho esto, el atacante podría robar la información de dichas computadoras, instalarles software maligno o dañar la información.

[14] Imagen, tomada de: http://warchalking-indaiatuba.blogspot.mx/
*Fecha de consulta: 29 de Diciembre de 2011

1.9 SEGURIDAD EN LAS REDES INALÁMBRICAS

Estas redes se caracterizan por no tener implementado ningún sistema de autenticación o cifrado. Las comunicaciones entre los terminales y los AP viajan en texto plano y no se solicita ningún dato para acceder a ellas.

Para lograr algo de seguridad en este tipo de redes se puede implementar:

- **Filtrado por MAC o IP:** permitir el acceso sólo a aquellas terminales que hayan sido previamente configuradas en el AP mediante ACL[15].
- **Bloquear Beacon Frames:** bloquear el envío de Beacon Frames para evitar que se conozca el ESSID

Estas medidas tienen en común que intentan limitar el acceso no autorizado al sistema, pero no impiden que alguien pueda espiar las comunicaciones que se realizan entre los dispositivos y terminales.
Se podría decir que la primera medida de seguridad que se implementó en redes wireless fueron las Listas de Control de Acceso (ACL – *Access Control List*) basadas en MAC. Sólo se crea una lista con las direcciones MAC de los equipos a los que se permite el acceso a la red. Hoy en día, se sabe que es relativamente sencillo cambiar la dirección MAC de una tarjeta por otra que sea válida, la cual puede ser obtenida con un Sniffer[16].

Por mucho tiempo se ha aconsejado ocultar el ESSID de una red, de esta forma se hace "invisible" a posibles intrusos, sin embargo en la mayoría de los dispositivos actuales tienen como opción la búsqueda de "redes ocultas", lo cual permite ver las redes con el ESSID deshabilitado. Además un posible atacante bien podría utilizar un Snifer para capturar alguna conexión de red y poder conseguir el ESSID, a través de las tramas PROBE REQUEST o PROBE RESPONSE[17].

Con esto se pueden sacar dos conclusiones: la primera (que definitivamente no es recomendable en ningún caso), utilizar redes abiertas cuando se maneja información importante o sensible, ya que puede ser capturada de alguna forma.

---

[15] ACL. Access Control List, Listas de Control de acceso
[16] Sniffer: un analizador de paquetes, es un programa de captura de las tramas de una red de computadoras
[17] Seguridad en redes inalámbricas.
http://documentos.shellsec.net/otros/SeguridadWireless.pdf
*Fecha de consulta: 15 de Diciembre de 2011

La segunda, implementar diferentes medidas de seguridad para evitar en lo posible las amenazas latentes, (ocultar el ESSID quizás no sea una medida que de mucha seguridad, pero es algo que puede ayudar cuando se mezcla con un plan de medidas adicionales).

1.10 INSEGURIDADES EN LAS REDES INALÁMBRICAS

Las inseguridades de las redes inalámbricas radican en:

- Configuración del propio "servidor" (puntos de accesos).
- La "escucha" (pinchar la comunicación del envió de paquetes).
- "Portadoras" o pisarnos nuestro radio de onda (NO MUY COMÚN), mandan paquetes al aire, pero esta posibilidad es real.
- El sistema de encriptación (WEP, Wirelles Equivalent Privacy , el más usado es de 128 Bits, pero depende del uso que se le dé a la red.

1.11 CONSEJOS DE SEGURIDAD

1. Cambiar las claves por defecto, cuando se instale el software del Punto De Acceso.
2. Control de acceso seguro con autentificación bidireccional.
3. Control y filtrado de direcciones MAC e identificadores de red, para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.
4. Configuración WEP (muy importante). La seguridad del cifrado de paquetes que se transmiten es fundamental en las redes inalámbricas, la codificación puede ser más o menos segura dependiendo del tamaño de la clave creada y su nivel, la más recomendable es de 128 Bits.
5. Crear varias claves WEP que varíen cada día, para el punto de acceso y los clientes.
6. Utilizar opciones no compatibles, si la red es de una misma marca se puede escoger esta opción para tener un punto más de seguridad, esto hará que un posible intruso tenga que trabajar con un modelo compatible al nuestro.
7. Radio de transmisión o extensión de cobertura: este punto no es muy común en todos los modelos, resulta más caro, pero sí se puede controlar el radio de transmisión al círculo de nuestra red; se puede conseguir podemos conseguir un nivel de seguridad muy alto y bastante útil.

En los últimos años las redes de área local inalámbricas (WLAN, Wireless Local Área Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas.

Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar. Con las WLANs la red, por sí misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las empresas donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbit/s, o superiores.

Pero no solamente encuentran aplicación en las empresas, sino que su extensión a ambientes públicos, en áreas metropolitanas, como medio de acceso a Internet o para cubrir zonas de alta densidad de usuarios (hot spots) en las próximas redes de tercera generación (3G) se ven como las aplicaciones de más interés durante los próximos años.

Muchos de los fabricantes de computadoras y equipos de comunicaciones como son los PDAs (Personal Digital Assistants), módems, terminales de punto de venta y otros dispositivos están introduciendo aplicaciones soportadas en las comunicaciones inalámbricas.

Las nuevas posibilidades que ofrecen las WLANs son: permitir una fácil incorporación de nuevos usuarios a la red, ofrecer una alternativa de bajo costo a los sistemas cableados, además de la posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red.

Capítulo 2: WEP Y WPA

2.1 ¿QUÉ ES WEP (WIRED EQUIVALENT PRIVACY)?

WEP (Wired Equivalent Privacy, privacidad equivalente al cable) es un algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Fue el primer protocolo de encriptación introducido en el primer estándar IEEE 802.11 allá por 1999. Está basado en el algoritmo de encriptación RC4[18], con una clave secreta de 40 ó 104 bits, combinada con un *Vector de Inicialización* (IV) de 24 bits para encriptar el mensaje de texto *M* y su checksum – el ICV (*Integrity Check Value*). El mensaje encriptado *C* se determinaba utilizando la siguiente fórmula y como se observa en la Imagen 2.1:

$$C = [\, M \,||\, \mathrm{ICV}(M) \,] + [\, \mathrm{RC4}(K \,||\, \mathrm{IV}) \,]$$

Donde || es un operador de concatenación y + es un operador XOR.

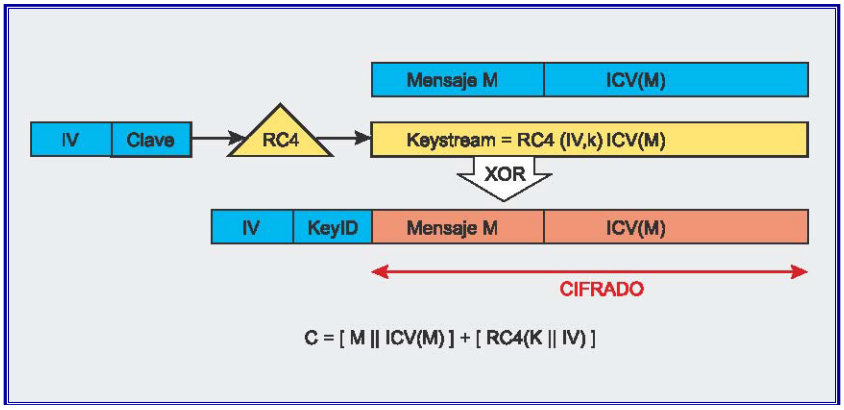


Imagen 2.1 Protocolo de encriptación WEP[19]
Proceso de encriptado de un mensaje

El vector de inicialización es la clave de la seguridad WEP, así que para mantener un nivel decente de seguridad y minimizar la difusión, el IV debe ser aplicado a cada paquete, para que los paquetes subsiguientes estén encriptados con claves diferentes. Desafortunadamente para la seguridad WEP, el IV es

[18] RC4: es un sistema de cifrado de flujo, quizás el más utilizado y se usa en algunos de los protocolos.
[19] Imagen tomada de : Seguridad Wi-Fi – *WEP*, WPA y WPA2
http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf
*Fecha de consulta: 28 de Noviembre de 2011

transmitido en texto simple, y el estándar 802.11 no obliga a la incrementación del IV, dejando esta medida de seguridad como opción posible para una terminal inalámbrica particular (punto de acceso o tarjeta inalámbrica)[20].

Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN. El WEP entonces, es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas. En ningún caso es compatible con IPSec[21].

2.1.1 Breve historia de WEP

El protocolo WEP no fue creado por expertos en seguridad o criptografía, así que pronto se demostró que era vulnerable ante los problemas RC4 descritos por David Wagner cuatro años antes. En 2001, Scott Fluhrer, Itsik Mantin y Adi Shamir (FMS para abreviar) publicaron su famoso artículo sobre WEP, mostrando dos vulnerabilidades en el algoritmo de encriptación: debilidades de no-variación y ataques IV conocidos. Ambos ataques se basan en el hecho de que para ciertos valores de clave es posible que los bits en los bytes iniciales del flujo de clave dependan de tan sólo unos pocos bits de la clave de encriptación (aunque normalmente cada bit de un flujo de clave tiene una posibilidad del 50% de ser diferente del anterior). Como la clave de encriptación está compuesta concatenando la clave secreta con el IV, ciertos valores de IV muestran claves débiles[22].

2.2 CARACTERÍSTICAS Y FUNCIONAMIENTO

2.2.1 Estándar

El estándar IEEE 802.11 proporciona mecanismos de seguridad mediante procesos de autenticación y cifrado. En el modo de red Ad Hoc o conjunto de servicios avanzados, la autenticación puede realizarse con un sistema abierto o

[20] Seguridad Wi-Fi – *WEP*, WPA y WPA2
http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf
*Fecha de consulta: 28 de Noviembre de 2011

[21] **IPSec:** (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

[22] Seguridad Wi-Fi – *WEP*, WPA y WPA2
http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf
*Fecha de consulta: 28 de Noviembre de 2011

clave compartida. Una estación de red que reciba una solicitud puede conceder la autorización a cualquier estación, o sólo a aquellas que estén incluidas en una lista predefinida. Y en un sistema de clave compartida sólo aquellas estaciones que posean una llave cifrada serán autenticadas.

El estándar 802.11 especifica una capacidad opcional de cifrado denominada WEP; su intención es la de establecer un nivel de seguridad similar al de las redes cableadas. WEP emplea el algoritmo RC4 de RSA Data Security, y es utilizado para cifrar las transmisiones realizadas a través del aire.

Aunque los sistemas WLAN pueden resistir las escuchas ilegales pasivas, la única forma efectiva de prevenir que alguien pueda comprometer los datos transmitidos consiste en utilizar mecanismos de cifrado. El propósito de WEP es garantizar que los sistemas WLAN dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio. Un propósito secundario de WEP es el de evitar que usuarios no autorizados puedan acceder a las redes WLAN (es decir, proporcionar autenticación). Este propósito secundario no está enunciado de manera explícita en el estándar 802.11, pero se considera una importante característica del algoritmo WEP[23].

WEP es un elemento crítico para garantizar la confidencialidad e integridad de los datos en los sistemas WLAN basados en el estándar 802.11, así como para proporcionar control de acceso mediante mecanismos de autenticación. Consecuentemente, la mayor parte de los productos WLAN compatibles con 802.11 soportan WEP como característica estándar opcional.

2.2.2 Cifrado

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida. El estándar 802.11 no especifica cómo se establece la clave secreta, pero permite que haya una tabla que asocie una clave exclusiva con cada estación. En la práctica

[23] 802.11 standards: 802.11b,802.11a, 802.11g: Which one isright for you?
http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm
*Fecha de consulta: 2 de Febrero de 2012

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). Dicho valor de comprobación de integridad se concatena con el texto en claro. El valor de comprobación de integridad es, de hecho, una especie de huella digital del texto en claro. El valor ICV se añade al texto cifrado y se envía al receptor junto con el vector de inicialización. El receptor combina el texto cifrado con el flujo de clave para recuperar el texto en claro. Al aplicar el algoritmo de integridad al texto en claro y comparar la salida con el vector ICV recibido, se puede verificar que el proceso de descifrado ha sido correcto o que los datos han sido corrompidos. Si los dos valores de ICV son idénticos, el mensaje será autenticado; en otras palabras, las huellas digitales coinciden.

2.2.3 Autenticación

WEP proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN, y una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red. De los dos niveles, la autenticación mediante clave compartida es el modo seguro, pues en él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN. Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio que constituye el *desafío (challenge)*. La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando la misma clave compartida y compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red. Si la estación no dispone de una clave, o si envía una respuesta incorrecta, el punto de acceso la rechaza, evitando que la estación acceda a la red.

La autenticación mediante clave compartida funciona sólo si está habilitado el cifrado WEP. Si no está habilitado, el sistema revertirá de manera predeterminada al modo de sistema abierto (inseguro), permitiendo en la práctica que cualquier estación que esté situada dentro del rango de cobertura

de un punto de acceso pueda conectarse a la red. Esto crea una ventana para que un intruso penetre en el sistema, después de lo cual podrá enviar, recibir, alterar o falsificar mensajes.
Es bueno asegurarse de que WEP está habilitado siempre que se requiera un mecanismo de autenticación seguro. Incluso, aunque esté habilitada la autenticación mediante clave compartida, todas las estaciones inalámbricas de un sistema WLAN pueden tener la misma clave compartida, dependiendo de cómo se haya instalado el sistema. En tales redes, no es posible realizar una autenticación individualizada; todos los usuarios, incluyendo los no autorizados, que dispongan de la clave compartida podrán acceder a la red. Esta debilidad puede tener como resultado accesos no autorizados, especialmente si el sistema incluye un gran número de usuarios. Cuantos más usuarios haya, mayor será la probabilidad de que la clave compartida pueda caer en manos inadecuadas.

2.2.4 Características Generales

Según el estándar, WEP debe 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.

2.2.5 Algoritmos

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 se sabe 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. Obserbar que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación de WEP, Imagen 2.2

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. 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.

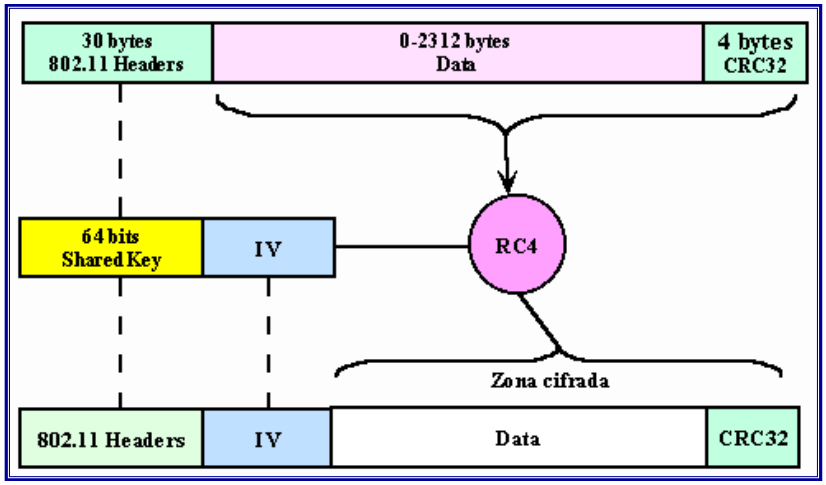


Imagen 2.2. Algoritmo de Encriptación WEP[24]

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

[24] Imagen tomada de: Protocolo de seguridad Wep
http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml
*Fecha de consulta: 10 de Enero de 2012

keystream se obtendrá el mensaje sin cifrar (datos y CRC-32), luego se comprueba que el CRC-32 es correcto[25].

Algoritmo de encriptación RC4

Es un algoritmo de Cifrador de flujo (no de bloques), creado en 1987 por Ronald Rivest (la R de RSA - Secreto Comercial de RSA Data Security). Fue publicado el 13 de Septiembre de 1994 usando remailers anónimos en un grupo de news: sci.crypt. Es usado por diversos programas comerciales como Netscape y Lotus Notes.

Funciona a partir de una clave de 1 a 256 bytes (8 a1024 bits), inicializando una tabla de estados. Esta tabla se usa para generar una lista de bytes pseudo-aleatorios, los cuales se combinan mediante la función XOR con el texto en claro; el resultado es el texto cifrado[26].

2.3 VULNERABILIDADES

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. Recordar que el IV es la parte variable de la clave (*seed*) para impedir que un posible atacante recopile suficiente información cifrada con una misma clave.

Sin embargo, el estándar 802.11 no especifica cómo manejar el IV; se indica que debería cambiarse en cada trama para mejorar la privacidad, pero no obliga a ello. Y queda abierta a los fabricantes la cuestión de cómo variar el IV en sus productos. La consecuencia de esto es que buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada trama, lo cual ocasiona que las primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente, más aún, si se tiene en cuenta que cada estación utiliza la misma clave secreta, por lo que las tramas con igual clave se multiplican en el medio.

---

[25] Protocolo de seguridad Wep
http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml
*Fecha de consulta: 10 de Enero de 2012

[26] Wi-Fi. (Cómo construir una red inalámbrica).
Carballar, José A.
2ª ed., México, Ed. Alfaomega Grupo editor, 2005

Por otro lado, el número de IVs diferentes no es demasiado elevado (2^24=16 millones aprox.), por lo que terminarán repitiéndose en cuestión de minutos u horas: el tiempo será menor cuanto mayor sea la carga de la red. Lo ideal sería que el IV no se repitiese nunca, pero, esto es imposible en WEP. La cantidad de veces que se repite un mismo IV dependerá de la implementación elegida para variar el IV por el fabricante (secuencial, aleatoria, etc.) y de la carga de la red. Observar que es trivial saber si dos tramas han sido cifradas con la misma clave, puesto que el IV se envía sin cifrar y la clave secreta es estática.

WEP no incluye autentificación de usuarios, lo más que incluye es la autentificación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). El sistema de autentificación descrito es tan débil que el mejor consejo sería no utilizarlo, para no ofrecer información extra a un posible atacante. En este caso se tendría una *autentificación de sistema abierto*, es decir, sin autentificación.

Entre la larga lista de problemas de seguridad de WEP, se encuentra también la ausencia de mecanismos de protección contra mensajes repetidos (*replay*). Esto permite que se capture un mensaje y se introduzca en la red en un momento posterior. El paquete podría ser, por ejemplo, el que contiene la contraseña de un usuario para utilizar un determinado servicio.

Todos los problemas comentados unidos a las características propias de WEP, como es la distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica.

2.3.1 Crackeado de la clave WEP utilizando Aircrack

El crackeado[27] de WEP puede ser demostrado con facilidad utilizando herramientas como Aircrack (creado por el investigador francés en temas de seguridad, Christophe Devine).

[27] **Crackeado:** Cuando se extrae una clave generalmente realizado con un crack que es un programa que se emplea para extraer claves, contraseñas o passwords encriptados

¿Qué es Aircrack?

Es un programa crackeador de claves WEP 802.11 y claves WPA-PSK que es capaz de recuperar las claves una vez que haya conseguido suficientes paquetes de datos.

Consiste en un analizador de paquetes de redes, un crackeador de redes WEP y WPA/WPA2-PSK y otro conjunto de herramientas de auditoría inalámbrica.

La suite está diseñada para trabajar con una distribución Linux, aunque también existe una versión para Windows que no es muy estable debido a conflictos con drivers.

Esta suite está diseñada para trabajar con tarjetas inalámbricas con circuitos integrados Atheros y con algunas con circuitos Railink sin necesidad de configurarlas. También se ha logrado usar la suite en otros circuitos, con configuraciones especiales en Linux[28].

Aircrack contiene tres utilidades principales, usadas en las tres fases del ataque necesario para recuperar la clave:

- **Airodump:** herramienta de sniffing utilizada para descubrir las redes que tienen activado WEP
- **Aireplay:** herramienta de inyección para incrementar el tráfico
- **Aircrack:** crackeador de claves WEP que utiliza los IVs únicos recogidos.

En la actualidad, Aireplay sólo soporta la inyección en algunos chipsets wireless y el soporte para la inyección, en modo monitor, requiere los últimos drivers parcheados.

[28] **aircrack**
http://www.aircrack.es/
*Fecha de consulta: 10 de Enero de 2012

Como utilizar Aircrack (Programa basado en Linux) –Manual Ilustrado

Paso.-1

Ir al botón de inicio, en la parte inferior de lado izquierdo, dar clic, de inmediato se despliega el menú y entonces dar clic en WIFIWAY-CHIPSET-CHIPS RTL.... finalmente oprimimos ENTER.

Paso.-2

Dar de alta el dispositivo alfa; para ello dar un clic en el botón INSTALL_8387.SH, hasta que en la parte inferior se pinte o habilite el botón SIGUIENTE

Paso.-3

Dar un clic en UTILIZAR EL DRIVER R8187 ALTA POTENCIA y esperar hasta que este habilitado el botón siguiente

Paso.-4

Una vez cargado el driver de la antena alfa, como se muestra en la pantalla, ahora se tiene que habilitar el modo monitor para el dispositivo seleccionando WLAN0 y dar clic en activar.

Paso.-5

Enseguida aparece una ventana en la cual se selección la WLAN0 y se da un clic en aplicar para visualizar la siguiente ventana.

Paso.-6

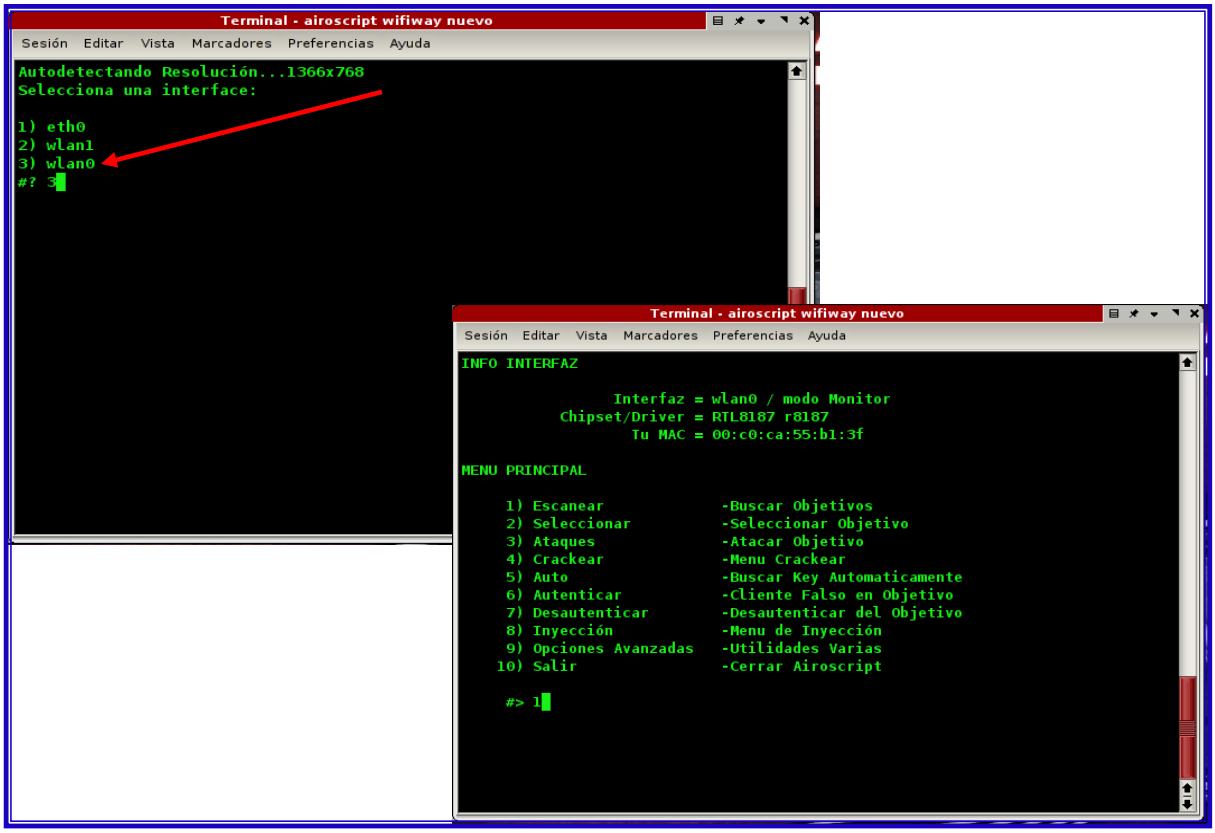
En la siguiente ventana se aprecia la habilitación de la consola en modo monitor y muestra cuando la tarjeta inalámbrica ya esta activada.

Paso.-7

Ahora se empezara a trabajar con el siguiente programa: aeroscript wifiway, entonces los pasos para utilizarlo son: INICIO-WIFIWAY-SUITE AIRCRAK+G- AEROSCRIPT WIFIWAY y se oprime enter o se da clic.

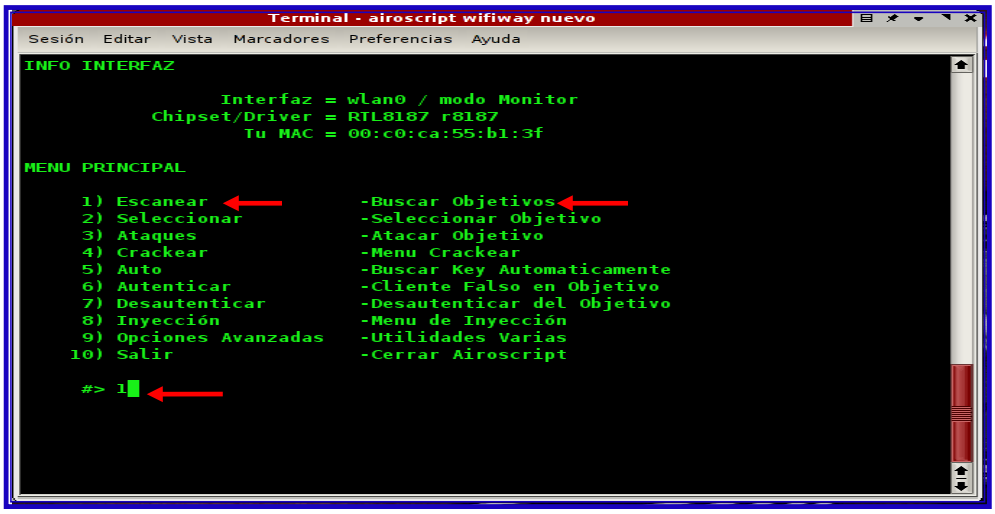
Paso.-8

En la siguiente ventana se elegirá la tarjeta WLAN0, la opción número 3, y se oprime la tecla enter, entonces se visualiza la ventana siguiente:

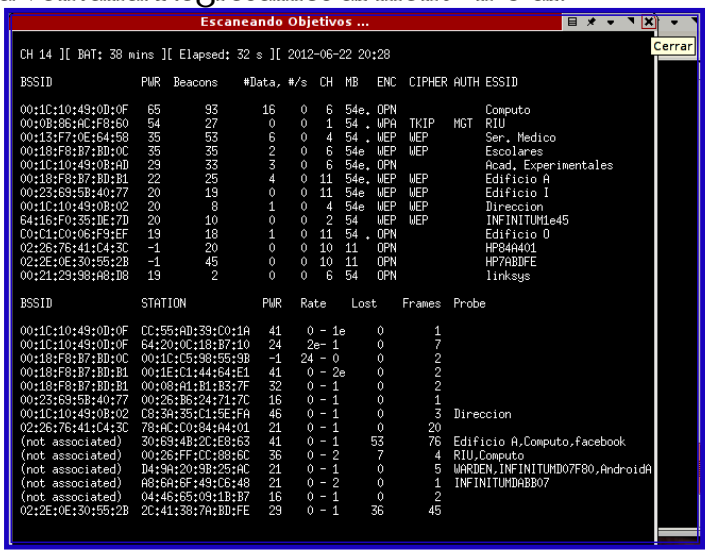


Pasó.- 9

A continuación, como se aprecia en la siguiente imagen se seleccionará la opción 1 que es escanear y oprimimos enter.

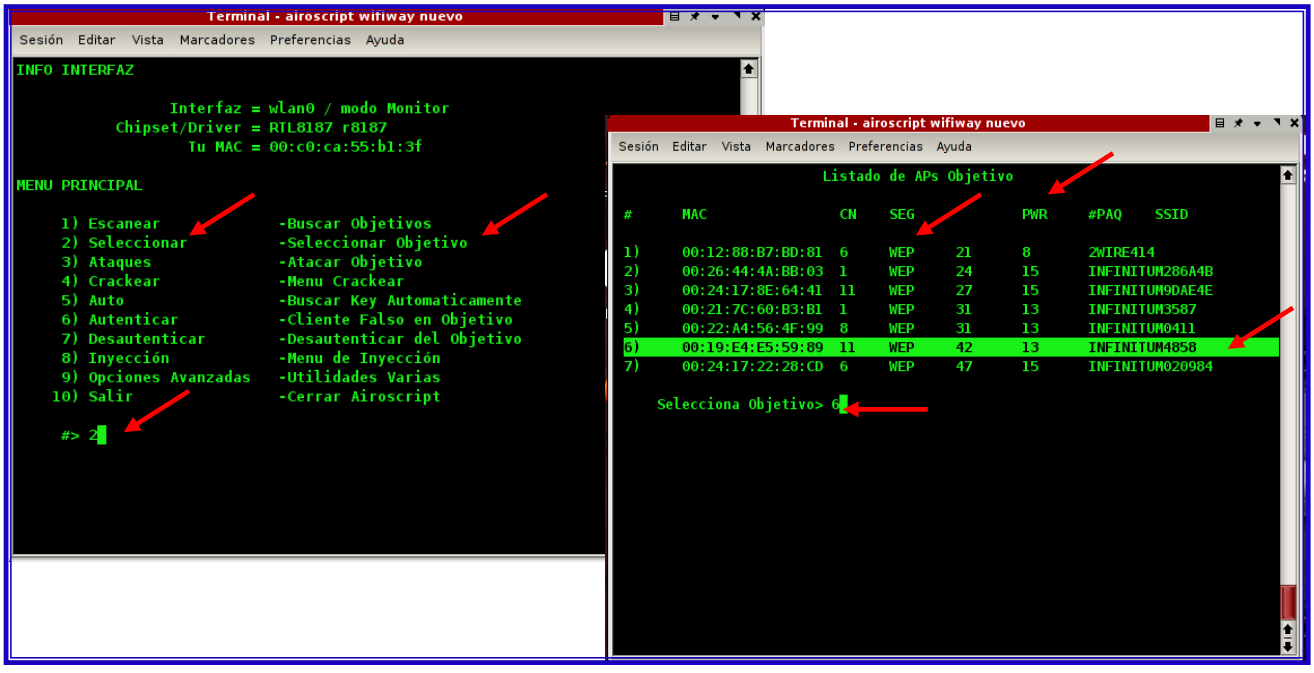


La siguiente ventana muestra las redes que se encuentran al alcance; para saber cuál queremos elegir y craguear. Debemos esperar de 30segundos a 1 minuto y cerraremos la ventana. Regresamos al menú inicial.



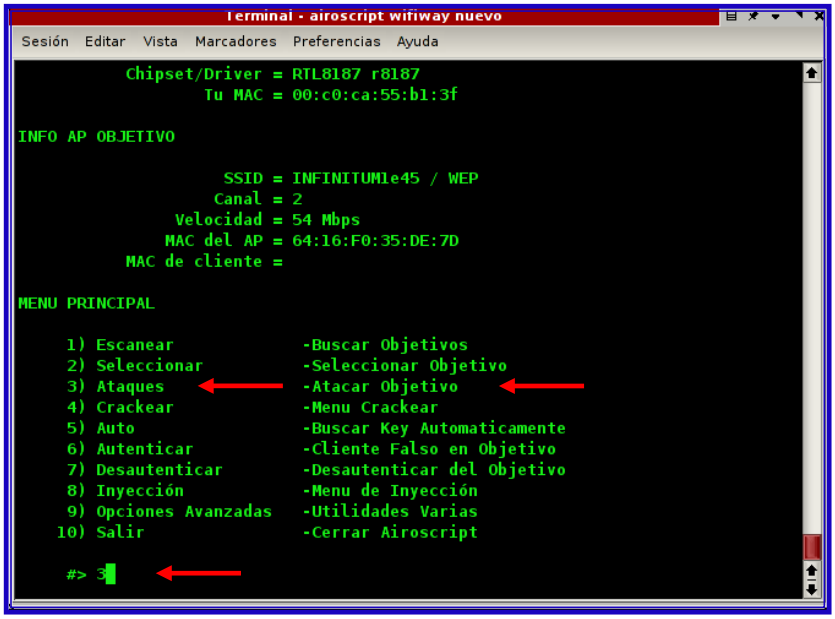
Paso.-10

A continuación, seleccionamos la opción 2 SELECCIONAR OBJETIVO, la red que se desea hackear, y oprimimos enter. Nos muestra entonces la red o redes que deseamos hackear (en este caso es la número 6) y se oprime enter. La red que se seleccione en cada caso será diferente pues será la que tú desees, recordando que solamente deben ser las de tipo WEB y en PWR que es la potencia de señal que tiene o bien la más cercana.

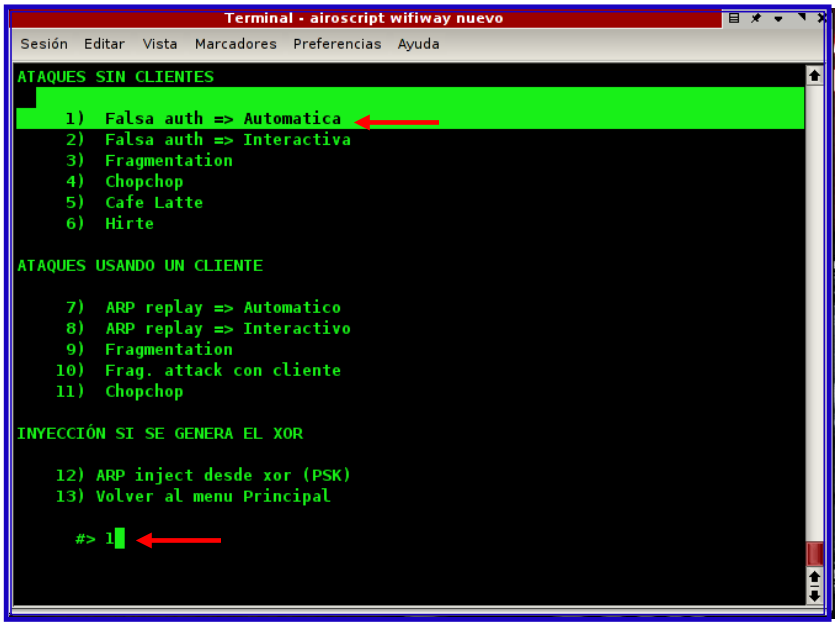


Paso.-11

Una vez seleccionada la red a hackear, se regresa al menú inicial, donde a continuación se seleccionara la opción 3. Se oprime la tecla enter.



La siguiente ventana muestra otro menú. Donde se selecciona la opción 1 y se oprime la tecla enter.

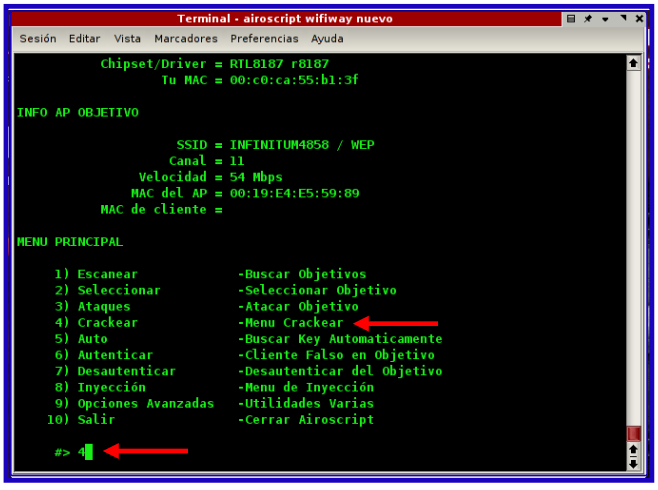


En las siguientes ventanas se aprecia el proceso de hackear la red; deben aparecer tres ventanas: de una con letras rojas, otra con letras blancas, y la última con letras verdes. Si no aparecen las tres ventanas, el proceso está mal realizado. Entonces se tendrá que volver a realizarlo desde el paso 7.

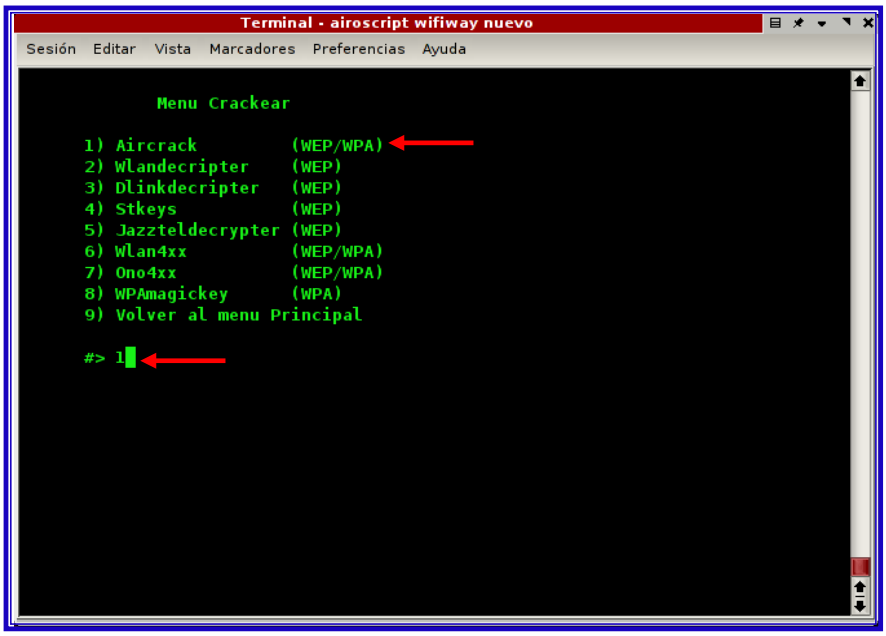
En la ventana con letras blancas se debera esperar a que se acumulen como mínimo 50000 paquetes #DATA. Para asegurar el correcto hackeo o crakeo de la red es recomendable esperar de 100000 hasta 150000 mil paquetes; en algunas ocasiones llega a dar la clave exacta con 50000, pero no en todos los casos. Al completar los paquetes ya deseados, se tendrán que cerrar las tres ventanas dando un clic en cada esquina superior en donde se encuentra la X.

Paso.-12

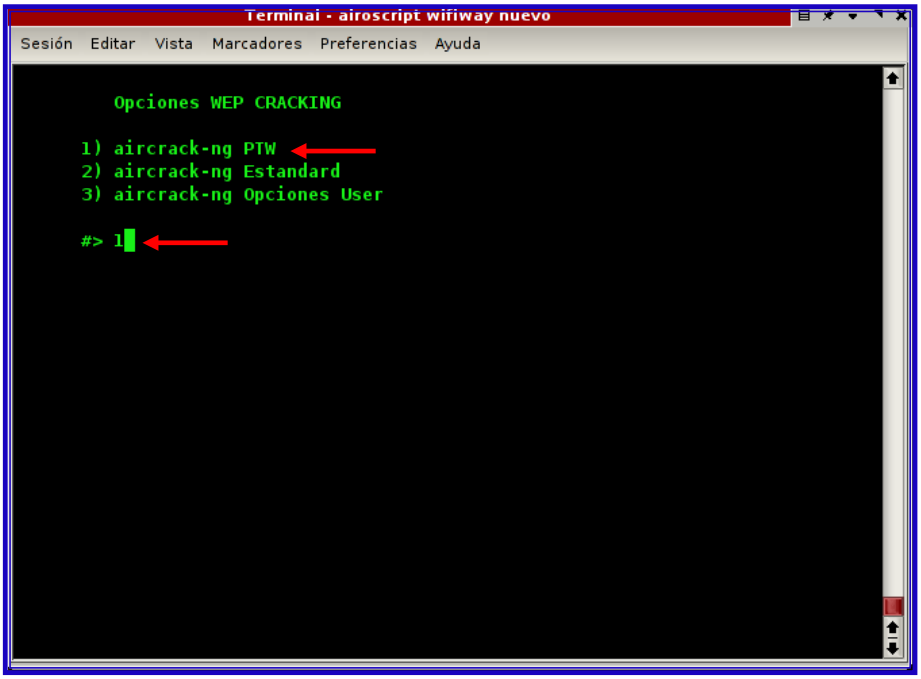
Por último, regresar al menú inicial, Después de haber cerrado las tres ventanas y completado los paquetes deseados, seleccionamos la opción 4 CRACKEAR y enter.



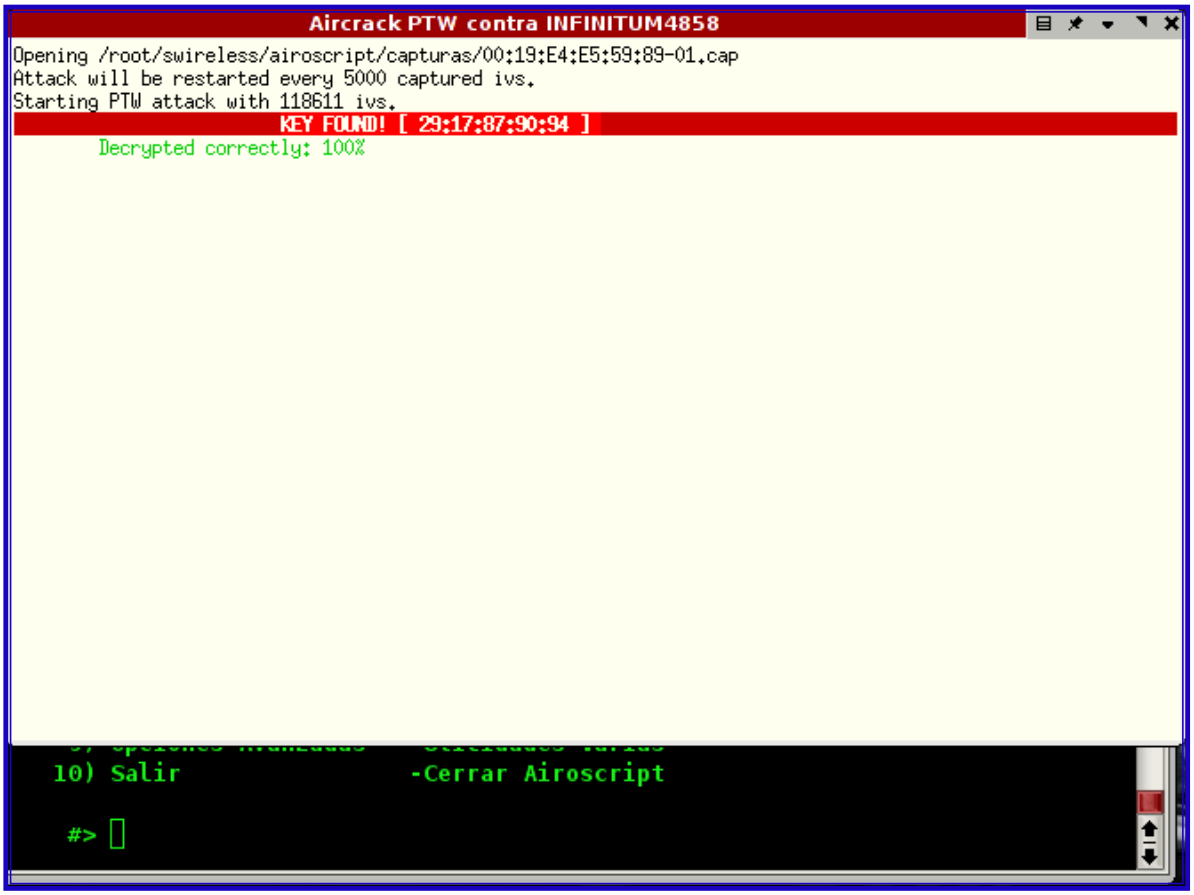
Se despliega otra ventana con menú, se selecciona la opción 1 AIRCRACK y oprimimos enter.



Se despliega nuevamente otra ventana con menú, se selecciona la opción 1 AIRCRACK-mg PTW y oprimimos enter.



Por último aparece otra ventana, la cual nos muestra la calve de la red hackeada, sólo bastara con apuntarla para entonces agregarla en donde se pide la clave de red para poder conectarse.



2.4 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 a 128 bits). WEP utilizado con claves de 128 bits es lo que se conoce generalmente como *WEP2*. Sin embargo, se debe 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), pues lo único que se ha aumentado es la clave secreta (de 40 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, además WEP2 no resuelve los problemas de WEP.

Otra variante de WEP utilizada en algunas implementaciones es *WEP dinámico*, con el cual se busca incorporar mecanismos de distribución automática de claves y de autentificación de usuarios mediante 802.1x/EAP[29]/RADIUS, por lo que se 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.

2.5 ¿QUÉ ES WPA?

Su nombre proviene del acrónimo WPA, es decir, *Wireless Protected Access* (acceso inalámbrico protegido) y tiene su origen en los problemas detectados en el anterior sistema de seguridad creado para las redes inalámbricas. La idea era crear un sistema de seguridad que hiciera de puente entre WEP y el 802.11i (WPA2), el cual estaba por llegar. Para ello utiliza el protocolo TKIP (Temporal Key Integrity Protocol) y mecanismos 802.1x.

La combinación de estos dos sistemas proporciona una encriptación dinámica y un proceso de autentificación mutuo. Así pues, WPA involucra dos aspectos: un sistema de encriptación mediante TKIP[30] y un proceso de autentificación mediante 802.1x. El proceso de encriptación es similar al realizado en WEP, pero con varias diferencias.

Para empezar, si bien TKIP usa el algoritmo RC4 proporcionado por *RSA Security* para encriptar el cuerpo del frame así como el CRC antes de la

[29] **EAP**: Protocolo de autentificación extensible para llevar a cabo tareas autorización, autentificación y contabilidad
[30] TKIP: (***T**emporal **K**ey **I**ntegrity **P**rotocol)* incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbrico.

transmisión, en este caso se utilizan IV de 48 bits, lo que reduce significativamente la reutilización y por tanto la posibilidad de que un hacker recoja suficiente información para romper la encriptación.
Por otro lado y a diferencia de WEP, WPA automáticamente genera nuevas llaves de encriptación únicas para cada uno de los clientes, lo que evita que la misma clave se utilice durante semanas, meses o incluso años, como pasaba con WEP. Por último, WPA implementa lo que se conoce como MIC o *message integrity code*, es decir, código de integridad del mensaje.

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.

2.6 CARACTERÍSTICAS Y FUNCIONAMIENTO

El funcionamiento del WPA incluye las siguientes tecnologías:

- **IEEE 802.1X**. Estándar del IEEE para proporcionar un control de acceso en redes basadas en puertos, concepto, 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 cuales tratarán entonces de conectarse a un puerto del punto de acceso, el cual mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (*Authentication Authorization Accounting*) como puede ser RADIUS (*Remote Authentication Dial-In User Service*). Si la autorización es positiva, entonces el punto de acceso abre el puerto, aunque 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, 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*), 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*).

- **TKIP** (*Temporal Key Integrity Protocol*). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.
- **MIC** (*Message Integrity Code*) o Michael. Código que verifica la integridad de los datos de las tramas

2.7 MODOS DE FUNCIONAMIENTO DE WPA

WPA puede funcionar en dos modos:

- **Con servidor AAA, RADIUS, normalmente**. Este es el modo indicado para las empresas y requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.
- **Con clave inicial compartida (PSK).** Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

2.8 VULNERABILIDADES

Sin embargo WPA no está exento de problemas. Y entre los más importantes destacan los DoS o ataques de denegación de servicio. Si alguien envía dos paquetes consecutivos en el mismo intervalo de tiempo usando una clave incorrecta, el punto de acceso elimina todas las conexiones de los usuarios durante un minuto. Este mecanismo de defensa utilizado para evitar accesos no autorizados a la red puede ser un grave problema. Aunque se han descubierto algunas pequeñas debilidades en WPA desde su lanzamiento, ninguna de ellas es peligrosa si se siguen unas mínimas recomendaciones de seguridad. La vulnerabilidad más práctica es el ataque contra la clave PSK de WPA. La PSK proporciona una alternativa a la generación de 802.1X PMK usando un servidor de autenticación.

La PSK es una cadena de 256 bits o una frase de 8 a 63 caracteres, usada para generar una cadena, utilizando un algoritmo conocido: PSK = PMK = PBKDF2(frase, SSID, SSID length, 4096, 256), donde PBKDF2 es un método utilizado en PKCS#5, 4096 es el número de hashes y 256 la longitud del resultado. La PTK es derivada de la PMK, utilizando el *4-Way Handshake* y

toda la información utilizada para calcular su valor se transmite en formato de texto.
La fuerza de PTK radica en el valor de PMK, que para PSK significa exactamente la solidez de la frase. Como indica Robert Moskowitz, el segundo mensaje del *4-Way Handshake* podría verse sometido a ataques de diccionario o ataques offline de fuerza bruta. La utilidad *cowpatty* se creó para aprovechar este error, y su código fuente fue usado y mejorado por Christophe Devine en Aircrack para permitir este tipo de ataques sobre WPA. El diseño del protocolo (4096 para cada intento de frase) significa que el método de la fuerza bruta es muy lento (unos centenares de frases por segundo con el último procesador simple). La PMK no puede ser pre-calculada (y guardada en tablas), porque la frase de acceso está codificada adicionalmente según la ESSID.

2.9 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.

En resumen...

Las redes Wi-Fi son prácticas y cada vez más habituales. Pero deben protegerse. Lo normal es hacerlo mediante WEP o WPA, que cifran la información de la red inalámbrica. No es igual un sistema que otro. Ve en qué se diferencian y cuál conviene más usar.

Pero ... ¿Es mejor el WEP o el WPA?
La respuesta corta: es MUCHO más seguro el WPA.

WEP (Wired Equivalent Privacy)
WEP fue el primer estándar de seguridad para redes Wi-Fi. Hoy está superado. NO debes usar WEP para proteger tu red inalámbrica si tienes alternativa. Su protección es demasiado débil. Se puede crackear un cifrado WEP en pocos minutos usando las herramientas adecuadas.

WPA (Wi-Fi Protected Access)
Surgió para corregir las limitaciones del WEP. Introdujo mejoras de seguridad como el TKIP (*Temporal Key Integrity Protocol*), que varía por sí solo la contraseña Wi-Fi cada cierto tiempo.

Su variante más normal es la WPA-Personal. Usa el sistema PSK, o de clave precompartida. En él, todos los usuarios de la red inalámbrica tienen una misma contraseña Wi-Fi, que el propio usuario define. Ve más abajo cómo elegir una clave fuerte.

También hay una versión WPA empresarial (*WPA-Enterprise*). Ofrece seguridad adicional al obligar al usuario a identificarse con un nombre y contraseña en sistemas de autentificación especiales, como RADIUS o 802.1X.

Capítulo 3: WPA 2

Una vez finalizado el nuevo estándar 802.11ie se crea el WPA2 basado en éste. WPA se podría considerar de «migración», mientras que WPA2 es la versión certificada del estándar de la IEEE. El estándar 802.11i fue ratificado en junio de 2004.

La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

Los fabricantes comenzaron a producir la nueva generación de puntos de acceso apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 le dan a los gerentes de TI la seguridad de que la tecnología cumple con estándares de interoperatividad", declaró Frank Hazlik Managing, Director de la Wi-Fi Alliance. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES, es importante resaltar que los productos certificados para WPA siguen siendo seguros, de acuerdo a lo establecido en el estándar 802.11i.

802.11i es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Wi-Fi está haciendo una implementación completa del estándar en la especificación WPA2.

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. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante, puesto que significa que dispositivos antiguos sin suficientes capacidades de proces,o no podrán 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.

3.1 CARACTERÍSTICAS Y FUNCIONAMIENTO

Estándar WPA2

La función principal del protocolo 802.11x es encapsular los protocolos de autenticación, sobre los protocolos de la capa de enlace de datos (capa 2 del modelo OSI) que describe el modo de autenticación basado en EAP (*Extensible Authentication Protocol*).

Define tres elementos:

- **Solicitante o suplicante:** Es el elemento que solicita la autenticación. Generalmente el Cliente.
- **Autenticador:** Elemento al que se conectará el suplicante. Pasa la información al servidor de autenticación, generalmente el Punto de Acceso.
- **Servidor de autenticación:** Elemento que evalúa la autenticación del suplicante enviando una respuesta al autenticador. En este caso será un servidor RADIUS.

EAP[31] puede transportar diferentes protocolos de autenticación, como se puede observar en la Imagen 3.1, como TLS (*Transport Layer Security*), TTLS (*Tunnel Transport Layer Security*), MD5 (*Message Digest 5*), PEAP (*Protected EAP*), LEAP (*Lightweight EAP*), etc.

EAP-TLS está basado en el uso de certificados digitales X.509 para la autenticación del cliente y del servidor. En el protocolo TTLS, sólo se autentica el cliente. El mayor inconveniente de EAP-TLS es que tanto el servidor de autenticación como los clientes han de poseer su propio certificado digital, y la distribución entre un gran número de clientes puede ser costosa y difícil. Por este motivo se creó PEAP y EAP que sólo requieren certificados en el servidor.

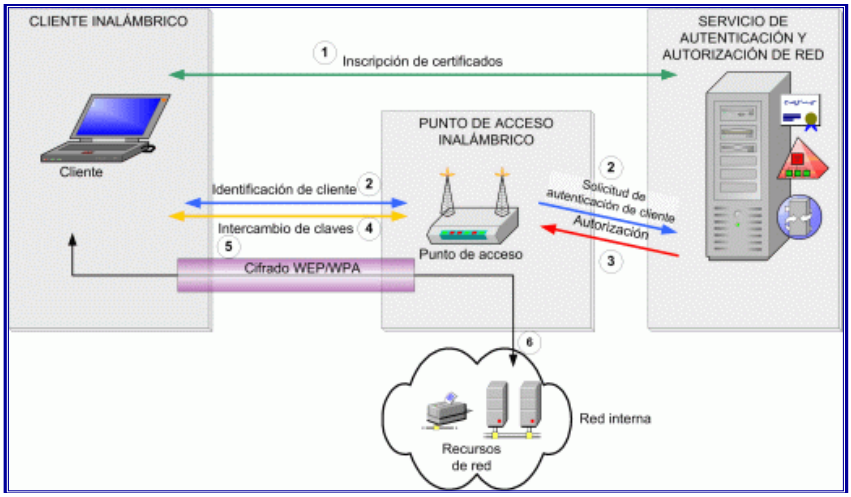


Imagen 3.1 Proceso de un EAP

[31] EAP: que es una estructura de soporte, no un mecanismo específico de autenticación

EAP-TTLS añade a las características de seguridad de EAP-TLS un canal de comunicación seguro para intercambiar credenciales con el usuario, incrementando la seguridad contra ataques de Sniffing. Por otro lado, elimina la necesidad de contar con certificados en todos los clientes.

Definición de los tipos de mensajes de intercambio:

- **Request:** Petición desde el Punto de Acceso al cliente
- **Response:** Mensaje del cliente al Punto de Acceso
- **Success:** Autorización del acceso
- **Failure:** Denegación del acceso.

El transporte de los mensajes se realiza a través del protocolo EALPOL (EAL over LAN), protocolo desarrollado para entornos Ethernet. En dicho protocolo se pueden encontrar cinco tipos de mensajes:

- **Start:** El cliente envía, a la dirección MAC multicast, a la espera de que el Punto de Acceso responda.
- **Key:** Una vez obtenido el acceso, el Punto de Acceso usa este mensaje para enviar las claves al cliente.
- **Packet:** Los mensaje EAL que son transmitidos se encapsulan en este mensaje EALPOL
- **Logoff:** Mensaje de desconexión enviado por el cliente
- **Encapsulated-ASF-Alert**: No utilizado en la actualidad.

El funcionamiento estándar de 802.11x se enfoca en la denegación de todo tráfico que no sea hacia el servidor de autenticación, hasta que el cliente no se haya autenticado. El autenticador crea un puerto por cliente creando 2 posibilidades: uno autorizado, el otro no, éste último lo mantiene cerrado hasta que el servidor de autenticación le comunique que el cliente tiene acceso.
Cuando el solicitante pasa a estar activo, selecciona y se asocia a un AP, el autenticador (que está en el AP) al detectar la asociación del cliente le habilita un puerto, permitiendo sólo tráfico 802.1x, el resto lo bloquea.

El cliente envía un mensaje "EAP Start", el autenticador responde con mensaje "EAP Request Identity" para obtener la identidad del cliente, la respuesta del solicitante "EAP Response" contiene su identificador y es retrasmitido por el autenticador hacia el servidor de autenticación. A partir de este momento el solicitante y el servidor de autenticación se comunicarán directamente.

3.2 MODOS DE FUNCIONAMIENTO DE WPA2

WPA2 tiene dos modos de funcionamiento:

- WPA2-ENTERPRISE: basado en el protocolo 802.1x explicado anteriormente, que utiliza los tres elementos ya descritos (suplicante, autenticador, servidor de autenticación).
- WPA2-PSK (*Pre-Share Key*): Pensado para entornos personales, evita el uso de dispositivos externos de autenticación. Se han descrito ataques *off-line* contra los mismos basado en ataques de diccionarios o contraseñas débiles.

Tanto el servidor de autenticación como el suplicante generan dos claves aleatorias denominadas PMK (*Pairwise Master Key*) durante la fase de autorización y autenticación de 802.1x. Una vez finalizada la fase de autenticación, el servidor de autenticación y el cliente tienen PMK idénticas, pero el Punto de Acceso no, por lo tanto a través del uso de RADIUS copia la clave del servidor de autenticación al Punto de Acceso. El protocolo no especifica el método de envío de la clave entre ambos dispositivos.

Llegados hasta este punto aún no se permite la comunicación si no que deben generar nuevas claves, en función de la PMK, para ser usadas en relación al cifrado y a la integridad, formando un grupo de cuatro claves llamado PTK (*Pairwise Transient Key*) con una longitud de 512 bits.

Para asegurar el tráfico broadcast, se crea claves de grupos de 256 bits llamadas GMK (*Group Master Key*) usado para crear la GEK (*Group Encryption Key*) y la GIK (*Group Integrity Key*) de 128 bits de longitud cada una. Las cuatro claves forman GTK (*Group Transient Key*).
La última parte es demostrar que el Punto de Acceso tiene PMK idéntico; para ello lo valida el servidor de autenticación.
Este proceso se realiza cada vez que es asociado un cliente con un Punto de Acceso.

3.3 VULNERABILIDADES

Aunque se han descubierto algunas pequeñas debilidades en WPA/WPA2 desde su lanzamiento, ninguna de ellas es peligrosa si se siguen unas mínimas recomendaciones de seguridad. La vulnerabilidad más práctica es el ataque contra la clave PSK de WPA/WPA2.

Ya se ha comentado del proceso de asociación de un cliente a una red Wireless; si el AP está emitiendo *Beacon Frames,* el proceso se realiza en 2 fases, una de

autenticación que podrá ser abierta o con clave compartida y una segunda fase de asociación. En el supuesto caso de que el punto de acceso no esté emitiendo "Beacon frames" existe una Fase de Prueba inicial donde el cliente envía el ESSID de la red wireless a la que quiere conectarse, esperando que el punto de acceso responda y así iniciar las fases de Autenticación y Asociación.

Pues bien, conociendo todo el proceso o modo de funcionamiento que realiza WPA2 y el intercambio de números aleatorios que se llevan a cabo entre un cliente y el AP para la autenticación y asociación, un atacante que quiera vulnerar una red WPA2-PSK va a tratar de capturar ese intercambio de números, para que una vez conocidos éstos, junto con el SSID, las direcciones MAC del cliente y el punto de acceso de la red, obtener la frase o secreto compartido que se utilizó. Una vez que el atacante tenga la clave compartida se podrá conectar a la red.

3.3.1 Rogue AP y Rogue RADIOUS

Una de las aproximaciones más interesantes para el robo de información en redes WiFi es la de la suplantación del punto de acceso o uso de lo que se llama Rogue[32] APs. La idea de esta técnica de ataque es conseguir que la víctima se conecte al equipo del atacante, que funciona como un punto de acceso legítimo, para que sea éste el que redirija el tráfico; como lo podemos observar en la Imagen 3.2. Es una forma sencilla de realizar un ataque de Man In The Middle, ya que al estar el atacante realizando funciones de AP va a poder interceptar absolutamente todas las comunicaciones; aparte podría realizar ataques de tipo DoS, robar datos de los clientes conectados, datos de usuarios como contraseñas e incluso monitorizar las actividades de cada cliente. Este tipo de ataque se ha empleado mucho para el espionaje corporativo.

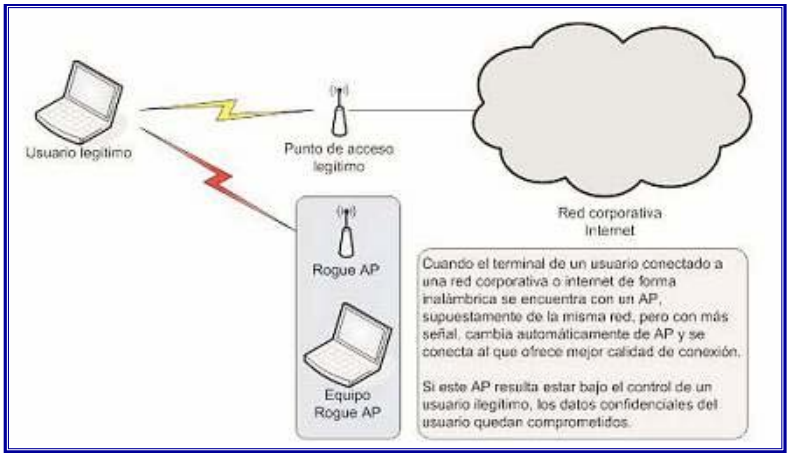


Imagen 3.2 Ataque RogueAP

[32] ROGUE: es un software que, simulando ser una aplicación anti-malware (o de seguridad), realiza justamente los efectos contrarios a éstas: instalar malware.

El Rogue AP puede hacerse con un AP modificado o incluso con un portátil, siempre y cuando éste tenga las aplicaciones necesarias, como son un servidor HTTP, DNS, DHCP y un Portal Cautivo para redireccionar el tráfico. También se podría hacer uso de AirSnarf para simplificar el proceso.
Para que el ataque tenga efectividad, es necesario que la suplantación de un AP legítimo sea lo más real posible, por lo que se debe recrear un entorno de red con las mismas características en el Rogue AP a las del AP legítimo, copiando para ello el BSSID, ESSID, las configuraciones de seguridad de la red y, por supuesto, la clave.
Como Rogue RADIOUS se conocen aquellos montajes que a parte del *Rogue AP* incorporan un servidor RADIOUS en el terminal de atacante. Para este caso se emplea un Servidor FreeRADIOUS configurado para responder a las peticiones que hagan los usuarios legítimos.

Para defender los sistemas de estos ataques nos encontramos con 2 frentes: defender el cliente y la infraestructura. El peligro al que se enfrenta un usuario de una terminal móvil es la asociación a un Rogue AP de forma voluntaria o no. Es conocido que sistemas como Windows Xp,Vista y 7 manejan las conexiones inalámbricas de forma automática, y esta es precisamente una característica muy apreciada por cualquier atacante, pues el sistema operativo se basa en la intensidad de la señal y el SSID para asociarse a un AP, siendo presa fácil para los Rogue AP.

En shmoo[33] se ha creado una herramienta para monitorizar las conexiones inalámbricas y detectar posibles ataques de este tipo, y es que en definitiva, quizás las mejores herramientas con las que se puede contar para prevenir cualquier amenaza informática son la monitorización constante de nuestros equipos y sistemas.

3.3.2 Fuerza Bruta

Este tipo de ataques son muy conocidos y no solamente en entornos inalámbricos. Básicamente se trata de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. La limitación principal para este tipo de ataques contra el protocolo WPA2 radica en la cantidad de tiempo que se puede emplear para poder encontrar la clave, teniendo en cuenta la velocidad de procesamiento que permite un procesador; por ese motivo se deben usar claves complejas y largas; de esa forma se subsanaría en gran medida un ataque por fuerza bruta. Sin embargo, con el uso actual de las GPU (*Graphics Processing Units*) los

[33] **SHMOO:** empresa encargada de crear herramientas que facilitan la seguridad en redes inalámbricas, reconocidos por ser los creadores de la herramienta airsnarf.

ataques de fuerza bruta se están convirtiendo en algo mucho más sencillo y efectivo de realizar.

3.3.3 Ataques de Fuerza Bruta usando GPUs

La potencia de las GPU[34]s, especialmente los últimos modelos, permite realizar un número ingente de operaciones por segundo, lo que pone en bandeja la realización de este tipo de ataques. Cifrar en 10.000 veces más rápida la ruptura de claves, comparando una GPU con una CPU convencional, es, según la información que manejan los expertos, una cifra razonable.

Este panorama abre un tanto forzadamente, la necesidad de que los usuarios y las empresas empiecen a considerar métodos alternativos para proteger sus activos de información. Aunque no son precisamente económicos, qué duda cabe que la mejor manera de evitar este tipo de ataques es dotar a la conectividad inalámbrica de doble autenticación bajo VPN. En este formato, además de emplear un *token* como segundo factor de autenticación, se confía el tráfico a una red privada virtual, lo que teóricamente impide la realización de ataques de este tipo.

A modo de ejemplo, Usando Pyrit se puede realizar ataques de fuerza bruta, haciendo uso de la GPU en contra del protocolo WPA/WPA2.
Haciendo uso de CUDA (herramienta creada por Nvidia) se abre la posibilidad de romper mediante fuerza bruta las claves que se usa en las conexiones Wiffi con encriptación WPA/WPA2. La capacidad de estas tarjetas gráficas combinadas con la posibilidad de usar configuraciones de múltiples de ellas en máquinas convencionales y el uso del lenguaje CUDA, creado específicamente para poder usar estas capacidades, dan como resultado una potencia de cálculo muy por encima de las CPUs en este tipo de tareas.

Como otro ejemplo se puede nombrar a ElcomSoft, quien ha desarrollado una aplicación llamada *Distributed Password Recovery*, que está orientada a revelar las contraseñas con las que están protegidos distintos tipos de documentos (PDF, ZIP, RAR, archivos de Office) e incluso las contraseñas de Windows, pero haciendo uso de la GPU.

3.3.4 Vulnerabilidad Hole 196

A pesar de que WPA2 es actualmente la forma de encriptación y autentificación más sofisticada y fuerte de todas las implementadas, estandarizadas y utilizadas hoy en

[34] **GPU**: unidad de procesamiento gráfico, es un coprocesador dedicado al procesamiento de gráficos.

día, AirTight Networks descubrió en 2010 una vulnerabilidad que llamaron Hole 196 (El apodo se refiere a la página del estándar IEEE 802.11, en el que está enterrada esta vulnerabilidad). Esta vulnerabilidad permite, básicamente, a cualquiera con acceso autorizado a la red Wi-Fi, desencriptar y robar información confidencial de cualquier otro que se encuentre conectado a la misma red inalámbrica, inyectar tráfico malicioso a la red y comprometer otros dispositivos autorizados, pero repito, siempre y cuando sea ya un usuario legítimo conectado a la red, es decir, que no se trata de una vulnerabilidad con la que se pueda realizar un ataque de fuerza bruta o algún otro tipo de ataque que permita la entrada no autorizada en la red, como podría ser un ataque al algoritmo de cifrado.

Kaustubh Phanse, investigador de AirTight afirma que no hay nada que se pueda hacer, al menos nada estándar que no sea crear una revisión del protocolo para solucionar o "parchar" la vulnerabilidad "Hole 196" y la describe como "una vulnerabilidad '*Zero Day*' que crea una ventana de oportunidad para la explotación". En la página 196 del estándar dice que los mensajes enviados con claves de grupo, es decir, las claves pensadas para comunicaciones broadcast no tienen protección contra Spoofing. Así, un atacante puede enviar un mensaje con una clave GTK con la IP que quiera.

La gracia del ataque es enviar un mensaje con una clave GTK, pero a una MAC dirigida en lugar de a una dirección MAC de broadcasting. Haciendo esto, sólo la víctima procesará ese paquete broadcast y, por tanto, salvo que la tabla de ARPs tenga la resolución de la MAC del Gateway estática, se producirá un envenenamiento de la IP que permitirá suplantar al router.

A partir de ese momento, cuando la víctima se comunique con el Gateway se utilizarán las claves PTK asociadas a esa IP, que el atacante amablemente entregará para hacer el MITM. Simple, pero funcional.

No rompe el sistema de autenticación de WPA/WPA-2 Enterprise, pero ayuda a hacer ataques MITM en esos entornos de forma oculta. La gracia es que el paquete va cifrado con la GTK y a una MAC que no es de broadcast lo que haría que hasta que no aparezcan soluciones IDS que inspeccionen todo el tráfico que vaya cifrado con claves GTK aunque no vaya a MAC de broadcast, el ataque no sea descubierto.

3.3.5 PSK

La vulnerabilidad más práctica es el ataque contra la clave PSK de WPA/WPA2. Como ya hemos dicho, la PSK proporciona una alternativa a la generación de 802.1X PMK usando un servidor de autenticación. Es una cadena de 256 bits o una frase de 8

a 63 caracteres, usada para generar una cadena utilizando un algoritmo conocido: PSK = PMK = PBKDF2(frase, SSID, SSID length, 4096, 256), donde PBKDF2 es un método utilizado en PKCS#5, 4096 es el número de hashes y 256 la longitud del resultado. La PTK es derivada de la PMK utilizando el *4-Way Handshake* y toda la información utilizada para calcular su valor se transmite en formato de texto.

La fuerza de PTK radica en el valor de PMK, que para PSK significa exactamente la solidez de la frase. Como indica Robert Moskowitz, el segundo mensaje del *4-Way Handshake* podría verse sometido a ataques de diccionario o ataques offline de fuerza bruta. La utilidad *cowpatty* se creó para aprovechar este error, y su código fuente fue usado y mejorado por Christophe Devine en Aircrack para permitir este tipo de ataques sobre WPA. El diseño del protocolo (4096 para cada intento de frase) significa que el método de la fuerza bruta es muy lento (unos centenares de frases por segundo con el último procesador simple). La PMK no puede ser pre-calculada (y guardada en tablas) porque la frase de acceso está codificada adicionalmente según la ESSID. Una buena frase que no esté en un diccionario (de unos 20 caracteres) debe ser escogida para protegerse eficazmente de esta debilidad.

En resumen ...

WPA2

Es el estándar más moderno para proteger redes inalámbricas y el que recomienda la *Wi-Fi Alliance*. Existe también una versión personal (*WPA2-Personal*) y empresarial (*WPA2-Enterprise*).

WPA2 es compatible con WPA, lo que significa que en tu red Wi-Fi puedes usar PCs o dispositivos (router, adaptadores de red...) que admitan uno u otro sistema.

WPA2 no es compatible, sin embargo, con sistemas WEP. No podrás juntar en una misma red Wi-Fi dispositivos que sólo admitan WEP con otros válidos para WPA2. Es por razones de seguridad.

Capítulo 4: RECOMENDACIONES PARA CONSEGUIR UNARED INALÁMBRICA MÁS SEGURA

Las redes Wi-fi son cada vez más utilizadas y todas las computadoras modernas están preparadas para trabajar con ellas sin dificultades.

Básicamente se trata de una red inalámbrica, es decir que no necesita cables. Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-fi es la seguridad.

Mientras que en las redes cableadas es más complicado conectarse de forma ilegítima ya que habría que conectarse físicamente mediante un cable; en las redes Wi-fi o inalámbricas (en las que la comunicación se realiza mediante ondas de radio), esta tarea es más sencilla.

Debido a esto hay que poner especial cuidado en protegerla de los posibles usos indebidos que los extraños puedan hacer de nuestra red Wi-fi. Las ondas de radio pueden viajar más allá de las paredes y filtrarse en habitaciones, casas u oficinas vecinas o llegar hasta la calle.

4.1 WARCHALKING Y WARDRIVING

El warchalking hace referencia a la utilización de un lenguaje de símbolos para reflejar visualmente la infraestructura de una red inalámbrica y las características de alguno de sus elementos. Estas señales se suelen colocar en las paredes de edificios situados en las zonas en las que existen redes inalámbricas para indicar su condición y facilitar el acceso a las mismas[35].

El wardriving se refiere a la acción de ir recorriendo una zona en busca de la existencia de redes wireless y conseguir acceder a ellas. Requiere de un software especial que capture las tramas broadcast que difunden los AP.

[35] ***Warchalking.***
http://www.warchalking.org
*Fecha de consulta:20 de Marzo de 2012

4.2 MECANISMOS DE SEGURIDAD

La seguridad WIFI abarca dos niveles. En el nivel más bajo se encuentran los mecanismos de cifrado de la información, y en el nivel superior los procesos de autenticación.

4.2.1 AUTENTICIDAD Y PRIVACIDAD

Al igual que en el resto de redes la seguridad para las redes wireless se concentra en el control y la privacidad de los accesos. Un control de accesos fuerte impide a los usuarios no autorizados comunicarse a través de los AP, que son los puntos finales que en la red Ethernet conectan a los clientes WLAN con la red. Por otra parte, la privacidad garantiza que sólo los usuarios a los que van destinados los datos trasmitidos los comprendan. Así, la privacidad de los datos transmitidos sólo queda protegida cuando los datos son encriptados con una clave que sólo puede ser utilizada por el receptor al que están destinados esos datos.

Por tanto, en cuanto a seguridad, las redes wireless incorporan dos servicios: de autenticación y privacidad.

AUTENTICIDAD

Los sistemas basados en 802.11 operan muy frecuentemente como sistemas abiertos, de manera que cualquier cliente inalámbrico puede asociarse a un punto de acceso si la configuración lo permite. También existen listas de control de accesos basadas en la dirección MAC, disponiendo en el AP de una lista con los clientes autorizados para rechazar a los que no lo están. También es posible permitir el acceso a cualquier nodo que se identifique y que proporcione el SSID (Service Set ID) correcto.

PRIVACIDAD

Por defecto, los datos se envían sin utilizar ningún cifrado. Si se utiliza la opción WEP los datos se encriptan antes de ser enviados utilizando claves compartidas, que pueden ser estáticas o dinámicas. Para realizar el cifrado se emplea la misma clave que se usa para la autenticación WEP. También se pueden utilizar otros mecanismos más potentes, como WPA o el nuevo estándar 802.11i.

4.3 GARANTIZANDO LA SEGURIDAD DE UNA RED INALÁMBRICA

Para poder considerar una red inalámbrica como segura, debería cumplir con los siguientes requisitos:

- Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.
- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Existen varios métodos para lograr la configuración segura de una red inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas.

4.3.1 Método 1: Filtrado de direcciones MAC

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

Ventajas y Desventajas

Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

- No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.

- El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.

- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales como AirJack[36] o WellenReiter[37], entre otros. De este modo, el atacante puede hacerse pasar por un cliente válido.

- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

4.3.2 Método 2: Wired Equivalent Privacy (WEP)

El algoritmo WEP[38] forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.
El algoritmo WEP cifra de la siguiente manera, y como se ve en la Imagen 4.1:

[36] **AirJack.**
http://802.11ninja.net/airjack/
*Fecha de consulta: 28 de Enero de 2012
[37] **Wellenreiter, WLAN Hacking.**
http://www.wellenreiter.net/
*Fecha de consulta: 29 de Enero de 2012
[38] ***Authentication and Privacy.*** **En ANSI / IEEE Standard 802.11, 1999 Edition.**
http://standards.ieee.org/getieee802/ download/802.11-1999.pdf , 59- 68 pp.
*Fecha de consulta: 14 de Febrero de 2012

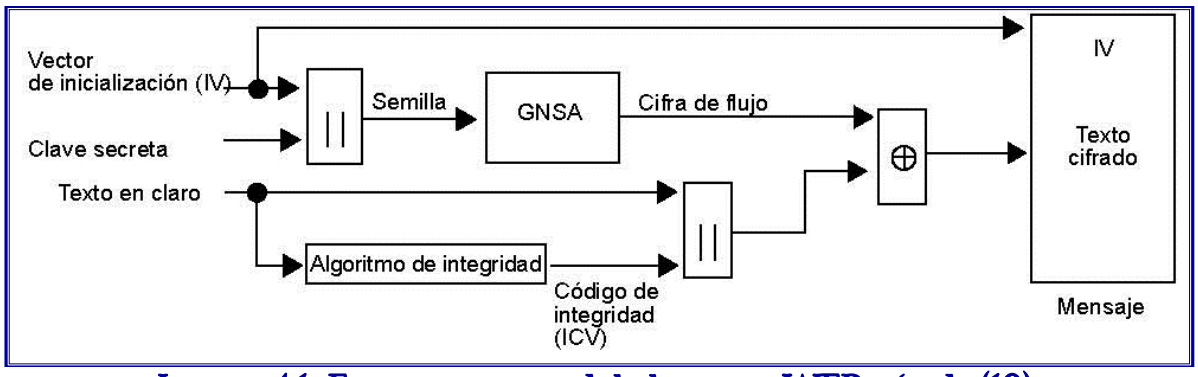


Imagen4.1 Funcionamiento del algoritmo WEP cifrado (10)

- A la trama en claro se le computa un código de integridad (Integrity Check Value, ICV) mediante el algoritmo CRC-32. Dicho ICV se concatena con la trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.
- Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.
- Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas en claro iguales producirían tramas cifradas similares.
- Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.
- La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números seudo-aleatorios. El generador RC4 es capaz de generar una secuencia seudo-aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.
- El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el ICV).
- Se hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada.
- El IV y la trama se transmiten juntos.
- En el receptor se lleva a cabo el proceso de descifrado como se ve en la Imagen 4.2:

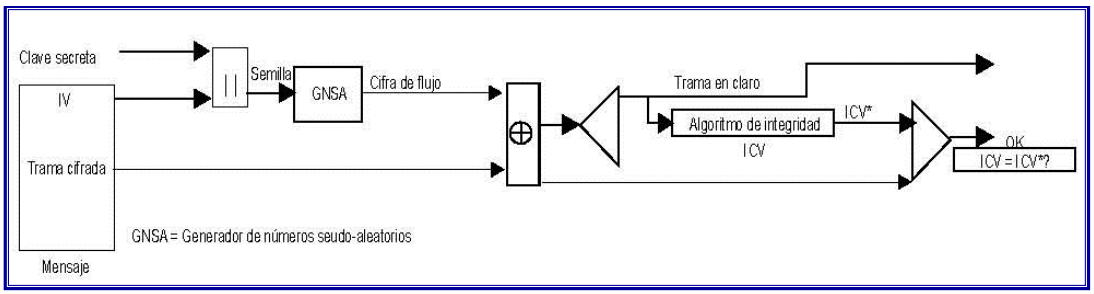


Imagen 4.2 Funcionamiento del algoritmo WEP en modalidad de descifrado

- Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.
- Un generador RC4 produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.
- Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrado, obteniéndose de esta manera la trama en claro y el ICV.
- A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.
- Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro en la manera que es empleado en la mayoría de aplicaciones:

- La mayoría de instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.

- El IV que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio de 2^{24} IV distintos. Esto no es problemático en una red casera con bajo tráfico, pero en una red que posea alto tráfico se puede agotar el espacio de los IV en más o menos 5 horas. Si el atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener los textos en claro de

ambas tramas mediante un ataque estadístico. Con el texto en claro de una trama y su respectivo texto cifrado se puede obtener la cifra de flujo; conociendo el funcionamiento del algoritmo RC4 es posible entonces obtener la clave secreta y descifrar toda la conversación.

- WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, sino al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP. El primer programa que hizo esto posible fue WEPCrack[39], que consiste en una serie de scripts escritos en lenguaje Perl diseñados para analizar un archivo de captura de paquetes de un sniffer. La herramienta AirSnort[40] hace lo mismo, pero integra las funciones de sniffer y rompedor de claves, y por lo tanto es más fácil de usar. Airsnort captura paquetes pasivamente, y rompe la clave WEP cuando ha capturado suficientes datos.

4.3.3 Método 3: Las VPN

Una red privada virtual (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP. Se aprecia mejor la estructura de la VPN en la Imagen 4.3.

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

[39] WEPCrack: Software que sirve para crackear redes.
[40] AirSnort: AirSnort es una herramienta para redes Lan Inalámbricas (WLAN) que recupera las claves de cifrado (WEP). AirSnort opera realizando escaneos pasivos progresivos.

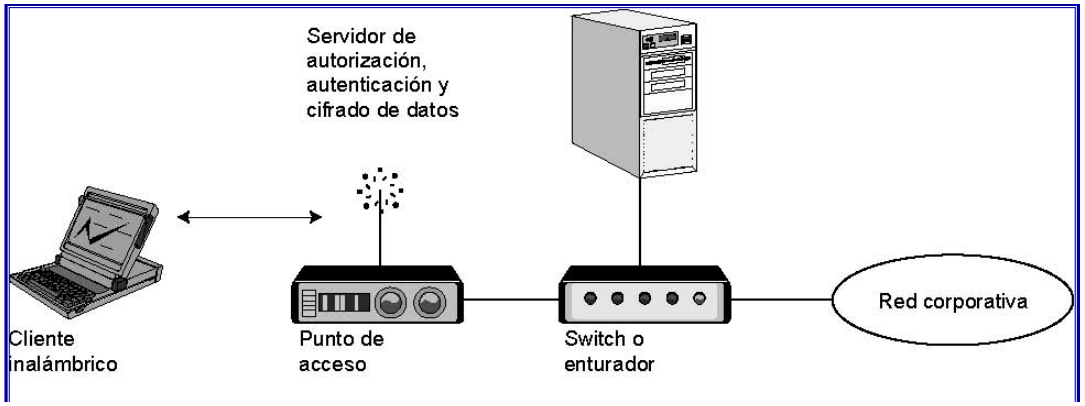


Imagen 4.3 Estructura de una VPN para un acceso inalámbrico seguro

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.

4.3.4 Método 4: 802.1x

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor que restringe la conexión de equipos no autorizados a una red[41]. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x.

El protocolo 802.1x involucra tres participantes como se ve en la Imagen 4.4:

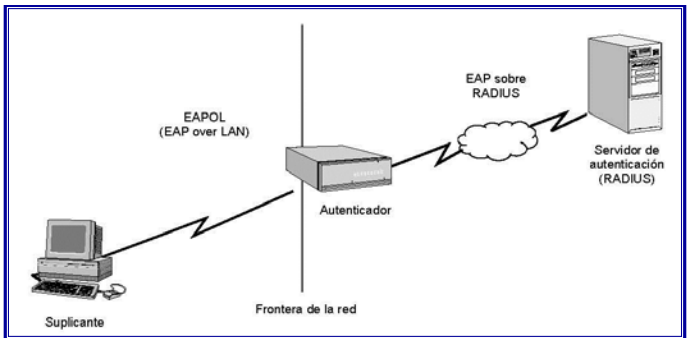


Imagen 4.4 Arquitectura de un sistema de autentificación 802.1x[42]

[41] Suhdir Nath. *802.1x Overview*.Noviembre de 2003
http://www.cisco.com/warp/public/732/Tech/ security/docs/8021xoverview.ppt
*Fecha de consulta: 15 de Abril de 2012

[42] Paul Congdon. *IEEE 802.1x Overview Port Based Network Access Control*. Marzo de 2000.
http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF
*Fecha de consulta 20 de Abril de 2012

- El suplicante o equipo del cliente que desea conectarse con la red.
- El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS (Remote Authentication Dial-In User Service), cuya especificación se puede consultar en la RFC 2058. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las LAN.
- El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto...) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

La autenticación del cliente se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocol) y el servicio RADIUS, de la siguiente manera:

- El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red (en el caso alambrado) o logra enlazarse o asociarse con un punto de acceso (en el caso inalámbrico). En ese momento la interfaz de red tiene el acceso bloqueado para tráfico normal, y lo único que admite es el tráfico EAPOL (EAP over LAN), que es el requerido para efectuar la autenticación.

- La estación de trabajo envía un mensaje EAPOL-Start al autenticador, indicando que desea iniciar el proceso de autenticación.
- El autenticador solicita a la estación que se identifique, mediante un mensaje EAP-Request/Identity.
- La estación se identifica mediante un mensaje EAP-Response/Identity.
- Una vez recibida la información de identidad, el autenticador envía un mensaje RADIUS-Access- Request al servidor de autenticación, y le pasa los datos básicos de identificación del cliente.
- El servidor de autenticación responde con un mensaje RADIUSAccess-Challenge, en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso. Dicho desafío

puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada.

- El autenticador envía el desafío al cliente en un mensaje EAP-Request.
- El cliente da respuesta al desafío mediante un mensaje EAP-Response (Credentials) dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje
- RADIUS-Access-Response.
- Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje RADIUS-Access-Accept, que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red.
- El autenticador envía un mensaje EAP-Success al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS.

En el caso del acceso inalámbrico, el servidor RADIUS despacha en el mensaje RADIUS-Access-Accept un juego de claves WEP dinámicas, que se usarán para cifrar la conexión entre el cliente y el punto de acceso. El servidor RADIUS se encarga de cambiar esta clave dinámica periódicamente (por ejemplo, cada cinco minutos), para evitar el ataque de rompimiento de la clave descrito en la sección referente a WEP.

Existen varias variantes del protocolo EAP, según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas.
Las variantes de EAP que emplean certificados de seguridad son las siguientes:

- EAP-TLS: Requiere de instalación de certificados en los clientes y en el servidor. Proporciona autenticación mutua fuerte (es decir, el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEP. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Transparent Layer Substrate).

- EAP-TTLS: Desarrollada por Funk Software y Certicom. Proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor. Esto garantiza la autenticación fuerte del servidor por parte del cliente; la autenticación del cliente por parte del servidor se efectúa una vez que se establece la

sesión TLS, utilizando otro método tal como PAP, CHAP, MS-CHAP o MS-CHAP v2.

- PEAP: Desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAPTTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

El empleo de certificados permite una autenticación fuerte entre cliente y servidor, sin embargo posee también varias desventajas:

- La administración de los certificados de seguridad puede ser costosa y complicada, especialmente en los esquemas donde se necesitan certificados en los clientes y en el servidor. Es necesario comprar los certificados a una autoridad de certificación (CA) conocida, o montar una CA propia.

- El diálogo de autenticación es largo. Esto ocasiona que el proceso sea algo demorado, siendo especialmente molesto para usuarios que tienen que reautenticarse con mucha frecuencia (por ejemplo, usuarios en movimiento que cambien de un punto de acceso a otro).

- La manipulación del certificado puede ser engorrosa para el usuario. En muchos casos se elige instalar el certificado en la terminal del usuario, con lo cual, si la terminal es robada y el certificado es el único nivel de seguridad que se posee, la seguridad de la red estaría en riesgo. Otra solución sería llevar el certificado en una tarjeta inteligente (smart card), lo que obligaría a instalar hardware adicional en las terminales para leer dichas tarjetas.

Las variantes de EAP, se aprecian en la Imagen 4.5; que utilizan contraseñas son las siguientes:

- EAP-MD5: Emplea un nombre de usuario y una contraseña para la autenticación. La contraseña se transmite cifrada con el algoritmo MD5. Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede

ensayar a cifrar múltiples contraseñas con MD5 hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente). Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está conectando a la red adecuada), y el esquema no es capaz de generar claves WEP dinámicas. Por estos problemas, EAP-MD5 ha caído en desuso.

- LEAP: Esta variante es propietaria de Cisco. Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP. Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.

- EAP-SPEKE: Esta variante emplea el método SPEKE (Simple Password-authenticated Exponential Key Exchange), que permite verificar que tanto cliente como servidor comparten una información secreta (en este caso, una contraseña) a través de un medio inseguro. Se ha comprobado que el método es muy seguro, aun con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servicio de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

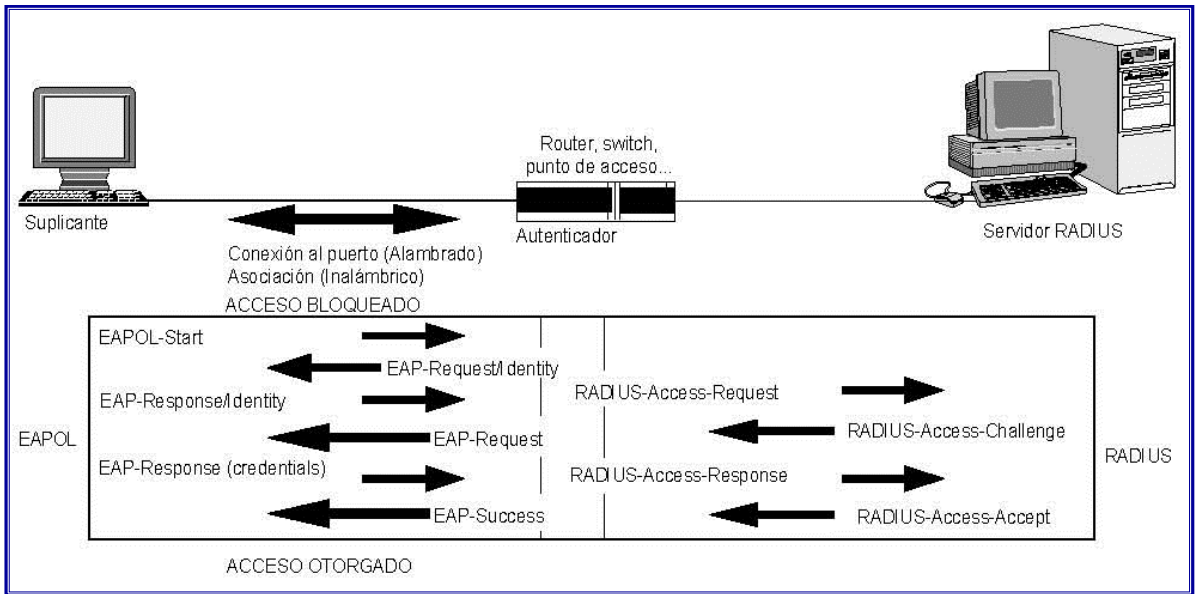


Imagen 4.5 Diálogo EAPOL-RADIUS[43].

[43] Eduardo Tabacman. *Seguridad en Redes Wireless.* En las memorias de la I Jornada de Telemática "Comunicaciones Inalámbricas, Computación Móvil". ACIS, Bogotá (Colombia), Noviembre 13 y 14 de 2003.
*Fecha de consulta: Abril de 2012

4.3.5 Método 5 wpa (wi-fi protected access)

WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP.
El mecanismo de autenticación usado en WPA emplea 802.1x y EAP.

Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

- Modalidad de red empresarial: Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

- Modalidad de red casera, o PSK (Pre-Shared Key): WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta[44].

[44] *WPA's Little Secret.* Noviembre 4 de 2003.
http://www.stargeek.com/item/20270.html
*Fecha de consulta: 25 de Abril de 2012

La norma WPA data de abril de 2003, y es de obligatorio cumplimiento para todos los miembros de la Wi-Fi Alliance a partir de finales de 2003. Según la Wi-Fi Alliance, todo equipo de red inalámbrica que posea el sello "Wi-Fi Certified" podrá ser actualizado por software para que cumpla con la especificación WPA.

4.4 COMO TENER UNA MAYOR SEGURIDAD EN LA RED CASERA

¿Cómo saber qué protección tiene mi Wi-Fi?

Lo más fácil es ver tu router Wi-Fi. Es un aparato con una o varias antenas que habrá traído y configurado quien instaló tu red inalámbrica.

Dale la vuelta al router y ve la etiqueta de abajo. Allí suele aparecer si es WEP o WPA. Al lado de una ristra de cifras y letras, que es la clave asignada a ese router.

¿Cómo proteger tu red Wi-Fi?

- Asegúrate de que tu router, los PC de tu red inalámbrica y los adaptadores de red sean compatibles con WPA2. Pregunta en la tienda donde los compres o consulta sus especificaciones.
- Al configurar tu red Wi-Fi usa WPA2-Personal con cifrado AES.
- Define una contraseña Wi-Fi fuerte. Por fuerte quiero decir en concreto que:
  - ✓ Tenga al menos 15 caracteres.
  - ✓ Combine letras mayúsculas y minúsculas, números y caracteres especiales ($, #, @, etc.).
  - ✓ No incluya NINGUNA información personal, como nombres, fechas de cumpleaños o aniversarios o el nombre de tu mascota.
  - ✓ No contenga palabras completas en ningún idioma, por raras que sean.
  - ✓ No ser obvios. Claves como "qwerty", "1234" o "contraseña" no son originales ni seguras, créeme.
- Y después de hacer todo eso cambia tu contraseña Wi-Fi cada cierto tiempo siguiendo las mismas recomendaciones. Ninguna clave es segura eternamente.

Finalmente…

Todos los métodos anteriores pueden ser vulnerados con los suficientes conocimientos y paciencia. Existen programas capaces de leer los nombres ocultos de las redes o falsificar un número MAC. Además, mientras que en un hogar con pocas computadoras la configuración es sencilla, en una oficina con personas que entran y salen, empieza a ser muy engorrosa. En estos casos la forma más segura y cómoda de proteger la red es utilizar un cifrado WEP y las contraseñas WPA-PSK. Para evitar la entrada a algún usuario ocasional.

CONCLUSIONES

Muchas redes wifi se dejan abiertas porque configurar las contraseñas es complicado, pero hay otras soluciones más inmediatas.

Los puntos de acceso wifi en hogares y oficinas se quedan abiertos porque sus dueños no saben cómo cerrar el acceso a los extraños. A otros simplemente no les importa, hasta el día en que descubren que un par de vecinos están monopolizando el ancho de banda con descargas masivas. Entonces deciden poner fin al 'robo de la señal' y llaman al pariente más próximo con conocimientos de informática para que eche el cerrojo al acceso.

Además del uso del ancho de banda, hay otros motivos para proteger el acceso. Si la red local (la que forman los ordenadores de la casa y el router) no está configurada con las medidas de seguridad adecuadas, los extraños podrían acceder a los archivos del disco duro. No tiene mucha importancia si se trata de las fotos familiares, pero en una empresa puede ser más grave al dejar al descubierto documentos confidenciales.

La forma más habitual de protección es colocar una contraseña WEP o WPA, pero esto exige configurar el router por un lado, y las computadoras que se conectan a él por otro, introduciendo la contraseña.

Hay otras medidas más sencillas que no ofrecen una protección tan elevada, pero que evitan que 'los de casa' tengan que introducir contraseñas. Pueden resultar muy efectivas para desanimar a la gente que intente conectarse, aunque alguien con conocimientos avanzados puede traspasarlas.

REFERENCIAS

CAPÍTULO 1:

Fuentes Bibliográficas

Tanenbaum, Andrew S., *Redes de computadoras*
4ª ed., México, Ed. Pearson Educación de México, 2003.

Carballar, José A., *Wi-Fi. (Cómo construir una red inalámbrica).*
2ª ed., México, Ed. Alfaomega Grupo editor, 2005.

Burch, John G. y gary Grudnitski., *Diseño de sistemas de información*
5ª ed., México, Ed. Limusa, S. A. de C. V, 1998.

Baran, Nicolas, Revista PC/Tips Byte, Artículo: *Redes Inalámbricas*
Abril 1992, pag 94-98

Boyle, Padriac, Revista PC/Magazine, Artículo: *Sin Conexión*
Marzo 1995, pag 86-97

Fuentes electrónicas

Redes inalámbricas
(10 de Noviembre de 2011), es.kioskea.net/contents/wireless/wlintro.php3

Redes inalámbricas y sus tipos
(15 de Noviembre de 2011), www.manual-wifi.com/tipos-de-redes-inalambricas/

CAPITULO 2

Fuentes Bibliográficas

Armand S-Pierre William Stephanos, *Introducción a la comunicación de datos.*
Editorial Trillas

Maximiliano Eschoyez, Wireless *LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,* ANSI/IEEE Std 802.11, 1999 Edition.

Saulo Barajas. *Protocolos de seguridad en redes inalámbricas.*
Prentice-Hall Hispanoamericana S.A.

Fuentes electrónicas

Protocolos de seguridad en redes inalámbricas.
Consulta (25 de Julio de 2012), www.saulo.net/pub/inv/SegWiFi-art.htm

El cifrado WEP no es muy seguro en realidad
Consulta (29 de Julio de 2012), www.kde.og
De nuevo: las redes wireless no son seguras.
(03 de Agosto de 2012), www.virusprot.com/Nt240821.html

Seguridad en 802.11.
(03 de Agosto de 2012), lcd.efn.unc.edu.ar/frames/archivos/wep.pdf

Wired Equivalent Privacy.
(04 Agosto de 2012), lasecwww.epfl.ch/securityprotocols/wep/WEP.pdf

Using NetMotion Mobility with WEP.
(06 de Agosto de 2012), www.netmotionwireless.com

Cisco. Configuring Wired Equivalent Privacy (WEP).
(08 de Agosto de 2012), www.cisco.com

Herve Schauer, *Seguridad Wi-Fi – WEP, WPA y* WPA2
www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

CAPITULO 3

Fuentes Bibliográficas

Doug Lowe, *WPA 2*
St Editorial, Inc., Capítulo 20, pp. 320.

Douglas E. Comer, *WPA2*
Prentice-Hall Hispanoamericana S.A.

Fuentes electrónicas

Herve Schauer, *Seguridad Wi-Fi – WEP, WPA y* WPA2
(10 de Septiembre de 2012), www.hsc.fr/ressources/articles/hakin9_wifi/
hakin9_wifi_ES.pdf

*WPA2*standard - Wi-Fi Alliance
(10 de Septiembre de 2012), www.wi-fi.org/.../wpa2%25E2%2584%25A

CAPITULO 4

Fuentes electrónicas

Alberto Escudero Pascual , *Seguridad en Redes Inalámbricas*
(10 de Septiembre de 2012), www.wilac.net/tricalcar

Guillaume Lehembre, *Seguridad Wi-Fi – WEP, WPA y WPA2*
(10 de Septiembre de 2012), www.hakin9.org

Roberto Hernando, *Seguridad en Redes Inalámbricas*
(9 de julio de 2012), www.rhernando.net

Authentication and Privacy
(10 de Agosto de 2012), standards.ieee.org/getieee802/download/802.11-1999.pdf

EAP Methods for 802.11 Wireless LAN Security
(10 de Agosto de 2012) www.iec.org/online/tutorials/acrobat/eap_methods.pdf

Wi-Fi Alliance. Overview: Wi-Fi Protected Access.
(11 de Agosto de 2012), www.weca.net/OpenSection/pdf/WiFi_Protected_Access_Overview.pdf