VNIVERSIDAD NACIONAL AVFNOMA DE MEXICO

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

PROGRAMA DE MAESTRIA Y DOCTORADO EN INGENIERIA

Facultad de Ingeniería

Métodos de protección y seguridad WEP en redes inalámbricas WiFi.

T E S I S

QUE PARA OPTAR POR EL GRADO DE:

MAESTRO EN INGENIERIA

Ingenieria Eléctrica - Telecomunicaciones

P R E S E N T A :

Ing. Medardo Emilio Vélez Simiano

TUTOR:
Dr. Javier Gómez Castellanos

AÑO
2006

JURADO ASIGNADO:

Presidente:	**Dr. Víctor Rangel Licea**
Secretario:	**Dr. Salvador Landeros Ayala**
Vocal:	**Dr. Javier Gómez Castellano**
1er. Suplente:	**Dr. Carlos Rivera Rivera**
2do. Suplente:	**Dr. Miguel Moctezuma Flores**

Lugar o lugares donde se realizó la tesis:

División de Estudios de Posgrado, Facultad de Ingeniería, UNAM

TUTOR DE TESIS:

Dr. Javier Gómez Castellano

_____

FIRMA

Índice

Capítulo 3: Ataques a redes WEP

Capítulo 4: Corrigiendo WEP

Listado de Figuras

Definición del problema

En el mundo de las computadoras e Internet, es ya muy común escuchar sobre el robo de información y de datos electrónicos. Esto se debe en gran medida a lo fácil que puede resultar la captura e interpretación de la información aun y cuando esta se encuentre protegida por codificación. Los protocolos de encriptación que se ha desarrollando para prevenir este tipo de hurto resulta por un tiempo útil pero con el paso del tiempo se descubren las fallas que limitan su alcance y uso.

Por otra parte, es también ya muy común la implementación de redes inalámbricas tanto por la comodidad de la instalación de redes con poca infraestructura y el uso mínimo de cableado, como por el impulso que han propiciado las empresas proveedoras de servicios de Internet. Pero la ventaja que presenta la ausencia de cableado, a su vez representa el inconveniente de que la información viaja a través del espacio sin el limitante inherente que resultaba ser el medio de las redes cableadas. Este hecho permite que prácticamente cualquier persona pueda tomar y analizar la información que uno transmite.

Los protocolos de encriptado y protección de información dan un margen de seguridad, que en la mayoría de los casos resulta ser suficiente como para que uno pueda incluso realizar compras vía electrónica sin preocuparse que por unos instantes, nuestros datos de cuentas bancarias se transmitan por el espacio. Pero así como se tiene una continua evolución en los protocolos de protección, también evolucionaron los métodos de crackeo de claves que vulneran el uso de los mismos.

Actualmente el protocolo de encriptación más difundido y utilizado en redes inalámbricas tipo WiFi es el protocolo WEP (Wired Equivalent Privacy), que es en la mayoría de los casos un protocolo lo suficientemente fuerte como para hacer que el hacker “ocasional” no tenga éxito, pero el hacker “profesional” cuenta con herramientas que proveen métodos y procedimientos que le permiten capturar, procesar e interpretar la información que hurtó.

Así este documento trata sobre las características, vulnerabilidades y medidas de protección que podemos encontrar en el protocolo WEP, así como un estudio de las redes inalámbricas y medidas de seguridad que se siguen en la ciudad de México.

Objetivos

En México la protección de la información es un hábito no muy difundido. La mayoría de la gente cree que con solo encender un equipo, éste de manera automática ya se encuentra protegido y fuera del alcance de usuarios no permitidos, o ignoran que hay medidas de protección alterna a las que brindan los equipos aumentando la seguridad de la red.

Con este trabajo se busca instruir al lector, en cuanto a los principios del protocolo WEP, así como en la detección de puntos vulnerables en las redes inalámbricas tipo WiFi y a su vez motivar un mayor interés por el campo de la seguridad.

Crear conciencia con respecto a lo que implica la seguridad de la información, ya que lo que a simple vista resulta en la captura de información aleatoria e irrelevante, bien podrían costarle a la persona o compañía mucho dinero, además de poner en riesgo la integridad y seriedad de la empresa afectada, así como de otras implicaciones más serias y que por supuesto no deben de ser tomadas a la ligera.

Entonces los puntos fundamentales son:

- Explicar los fundamentos del protocolo WEP, su implementación, así como hablar de sus vulnerabilidades y las medidas de protección que se pueden tomar.
- Mostrar un procedimiento completo y probado, para el rompimiento de claves WEP, las herramientas que se utilizaron y su uso.
- Demostrar el grave problema que se tiene actualmente en México, con respecto a la cultura de la protección de la información, ya que se realizó un estudio donde se demostró que la mayoría de las redes inalámbricas no cuentan con ninguna medida de protección.

Capítulo 1

Redes inalámbricas

Capítulo 1: Redes inalámbricas

1.0 Introducción

Una de las tecnologías más prometedoras que ha tenido un gran desarrollo en esta década es la de la conexión de computadoras mediante Ondas de Radio. Este tipo de tecnología se ha venido desarrollando desde finales de la década de los 70's, pero no fue si no hasta mediados de los 80's que se logró un avance en las comunicaciones inalámbricas y ya en la década de los 90's comenzó su implementación a niveles comerciales, en inmuebles y sitios de poca infraestructura. Las Redes Inalámbricas facilitan la operación donde la computadora no puede permanecer en un solo lugar. La disponibilidad de conexiones inalámbricas y redes LAN inalámbricas puede ampliar la libertad de los usuarios de la red a la hora de resolver problemas asociados a las redes con cableado fijo y en algunos casos, incluso reducir los gastos de implementación de las redes.

Actualmente, existen varias soluciones de redes LAN (Local area network, "Redes de área local") inalámbricas, con distintos niveles de estandarización e interoperabilidad, pero dos soluciones que hoy por hoy lideran el sector son *HomeRF* y WiFi [1] (IEEE 802.11x)[1]. De estas dos, las tecnologías 802.11 disponen de una mayor aceptación en el mercado.

La alianza Wireless Ethernet Compatibility Alliance se encarga de proporcionar certificados de compatibilidad con los estándares 802.11, lo que ayuda a garantizar la interoperabilidad entre los fabricantes. El amplio interés del sector para que exista interoperabilidad y compatibilidad entre los sistemas operativos ha permitido resolver algunas de las cuestiones relacionadas con la implementación de las redes LAN inalámbricas. Con todo, las redes LAN inalámbricas exponen nuevos retos en lo que respecta a la seguridad, la movilidad y la configuración.

Las conexiones inalámbricas pueden ampliar o sustituir una infraestructura con cables cuando es costoso o es difícil el tendido de cables. Las instalaciones temporales son un ejemplo de una situación en la que la red inalámbrica tiene sentido o incluso es necesaria.

El acceso portátil a las redes inalámbricas se realiza a través de equipos portátiles y NIC inalámbricas. Esto permite al usuario viajar a distintos lugares sin perder el acceso a los datos de la red. Sin el acceso inalámbrico, el usuario tendría que llevar consigo cables y disponer de conexiones de red.

En todos estos escenarios, vale la pena destacar que las redes LAN inalámbricas actuales basadas en estándares funcionan a alta velocidad, la misma velocidad que se consideraba vanguardista para las redes con cable hace tan solo unos años.

1.1 Topologías de redes LAN inalámbricas

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas. Para estas topologías se utilizan distintos términos, como "administradas / no administradas", "alojadas / par a par" y como "infraestructura / ad hoc". Una topología de infraestructura como la que se muestra en la figura 1.1, es aquella que extiende una red LAN cableada, al incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN cableada y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio.

[1] WiFi: acrónimo sin significado determinado (véase http://www.boingboing.net/2005/11/08/wifi_isnt_short_for_.html) aunque en algunos textos se define como Wireless Fidelity ("Fidelidad inalámbrica")

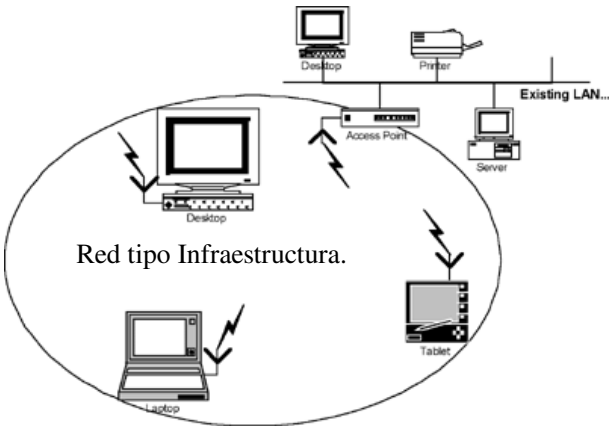


Figura 1.1 Red tipo Infraestructura.

En una topología ad hoc como la mostrada en la figura 1.2, los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

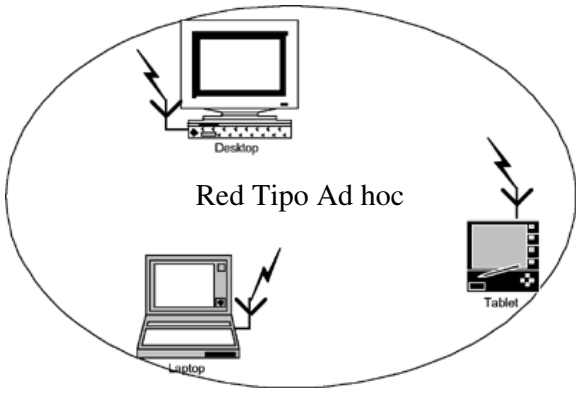


Figura 1.2 Red tipo Ad hoc.

Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo para que un operador se pueda desplazar con facilidad dentro de un almacén u oficina. Existen dos amplias categorías de Redes Inalámbricas:

- De Larga Distancia.- Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos.
- De Corta Distancia.- Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre si.

Existen dos tipos de redes de larga distancia: Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares. Estas últimas en México experimentan aun tarifas con precios elevados por el uso de la infraestructura celular, además de que los módems celulares son más caros y delicados que los convencionales, ya que requieren circuiteria especial, que permite mantener la pérdida de señal cuando el circuito se alterna entre una célula y otra. Esta pérdida de señal no es problema para la comunicación de voz debido a que el retraso en la conmutación dura cientos de milisegundos, lo cual no se nota, pero en la transmisión de información puede hacer estragos. Otras desventajas de la transmisión celular es que puede ser fácilmente interceptada y además las velocidades de transmisión son bajas.

Todas estas desventajas hacen que utilizar una conexión entre redes, vía celular se utilice poco, pero se espera que con los avances en la compresión de datos, seguridad y algoritmos de verificación de errores se permita que las redes celulares sean una opción redituable en algunas situaciones.

La otra opción que existe en redes de larga distancia son las denominadas: Redes Públicas De Conmutación De Paquetes Por Radio. Estas redes no tienen 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 frecuencias restringidas por la propia organización.

Las redes inalámbricas se diferencian de las convencionales principalmente en la "Capa Física" y la "Capa de Enlace de Datos", según el modelo de referencia OSI (Open System Interconection, “Interconexión de Sistemas Abiertos”). La capa física indica como son enviados los bits de una estación a otra. La capa de Enlace de Datos denominada MAC (Media Access Control, “control de acceso al medio”), se encarga de describir como se empacan y verifican los bits de modo que no tengan errores. Las demás capas forman los protocolos o utilizan puentes, ruteadores o compuertas para conectarse.

1.2 Funcionamiento de la topología de infraestructura

El portátil o “estación", primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica, con tramas de sondeo. La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN cableada o inalámbrica.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

1.3 Redes de radio frecuencia

Para las Redes Inalámbricas de Radio Frecuencia, la FCC (Federal Communications Commission "Comisión federal de Comunicaciones") permitió la operación sin licencia de dispositivos que utilizan 1 Watt de energía o menos, en tres bandas de frecuencia: 902 a 928 MHz, 2,400 a 2,483.5 MHz y 5,725 a 5,850 Mhz. Estas bandas de frecuencia, llamadas bandas ISM, estaban anteriormente limitadas a instrumentos científicos, médicos e industriales. Para minimizar la interferencia, las regulaciones de la FCC estipulan que una técnica de señal de transmisión llamada spread-spectrum modulation, la cual tiene potencia de transmisión máxima de 1 Watt deberá ser utilizada en la banda ISM[2]. La idea es tomar una señal de banda convencional y distribuir su energía en un dominio más amplio de frecuencia. Así, la densidad promedio de energía es menor en el espectro equivalente de la señal original. En aplicaciones militares el objetivo es reducir la densidad de energía abajo del nivel de ruido ambiental de tal manera que la señal no sea detectable. La idea en las redes es que la señal sea transmitida y recibida con un mínimo de interferencia. Existen dos técnicas para distribuir la señal convencional en un espectro de propagación equivalente:

- La secuencia directa: En este método el flujo de bits de entrada se multiplica por una señal de frecuencia mayor, basada en una función de propagación determinada. El flujo de datos original puede ser entonces recobrado en el extremo receptor correlacionándolo con la función de propagación conocida. Este método requiere un procesador de señal digital para correlacionar la señal de entrada.
- El salto de frecuencia: En este método los dispositivos receptores y emisores se mueven sincrónicamente en un patrón determinado de una frecuencia a otra, brincando ambos al mismo tiempo y en la misma frecuencia predeterminada. Como en el método de secuencia directa, los datos deben ser reconstruidos en base del patrón de salto de frecuencia.

El método de acceso, tal como la modulación de radio y el ancho de banda disponible, es importante para determinar la eficiencia y la capacidad de un sistema de radio.

1.4 El método de acceso

El tiempo es importante para poder maximizar el servicio, al momento de diseñar la frecuencia en el espacio. El uso del tiempo está determinado por los protocolos y por los métodos de acceso que regularmente usen los canales de transmisión de la estación.

Las características del método de acceso para que se considere que tiene un tiempo eficiente, pueden estar limitadas por los métodos que sean utilizados, algunas de estas características son:

1.- Después de completar una transmisión/ recepción, la comunicación debe de estar disponible para su siguiente uso.

2.- La densidad de distribución geográfica y tiempo irregular de la demanda del tráfico deben ser conocidas.

3.- Para tráfico abundante, se debe de tener una "lista de espera" en la que se manejen por prioridades: "El primero en llegar, es el primero en salir", además de poder modificar las prioridades.

[2] ISM (Industrial Scientific and Medical, "Industrial, científica y medica") son bandas reservadas internacionalmente para uso no comercial de Radio Frecuencia electromagnética en áreas industrial, científica y médica.

4.- Establecer funciones para usar todo el ancho de banda del canal de comunicación, para que el tiempo que exista entre el comienzo de la transmisión y la disponibilidad de la comunicación, sea lo más corto posible.

5.- El uso de un "saludo inicial" minimiza tiempos perdidos, en el caso de que los paquetes transferidos no lleguen correctamente; cuando los paquetes traen consigo una descripción del servicio que requieren, hacen posible que se mejore su organización.

6.- La conexión para mensajes debe ser más eficiente que la selección, particularmente al primer intento, sin embargo la selección puede ser eficiente en un segundo intento cuando la lista de las estaciones a seleccionar sea corta.

Para transacciones de tipo asíncrona, es deseable completar la transacción inicial antes de comenzar la siguiente. El tiempo requerido para una transacción de gran tamaño, es un parámetro importante para el sistema que afecta la capacidad del administrador de control para encontrar tiempos reservados con retardos, como hay un tiempo fijo permitido para la propagación, el siguiente paso debe comenzar cuando termina el actual. El control del tráfico de datos en ambas direcciones, se realiza en el administrador de control.

Cuando el paquete es más pequeño, la proporción del tiempo usado al accesar el canal es mayor, aunque la carga pueda ser pequeña para algunas funciones, la transferencia y descarga de archivos son mejor administrados cuando la longitud del paquete es de buen tamaño, para minimizar el tiempo de transferencia.

En paquetes grandes, se incrementa la posibilidad de que el paquete tenga errores en el envío, en sistemas de radio el tamaño aproximado ideal es de 512 octetos o menos, además un paquete con una longitud de 100-600 octetos puede permitir la salida oportuna de respuestas y de datos prioritarios junto con los datos normales.

Como se ve en la figura 1.3, las computadoras pueden necesitar diferentes anchos de banda dependiendo del servicio a utilizar, ya sean transmisiones de datos, de vídeo y/o de voz, etc. El dispositivo entonces administrara el Ancho de banda de la siguiente manera:

1.- Multiplexandolo de tal manera que un paquete sea un conjunto de servicios.

2.- Administrando el tiempo y la prioridad reservada para los paquetes relacionados con él, así la parte alta de la capa MAC es multiplexada.

La capacidad de compartir el tiempo de estos dos tipos de servicios ha incrementado la ventaja de optimizar la frecuencia en el espacio y los requerimientos para armar un sistema.

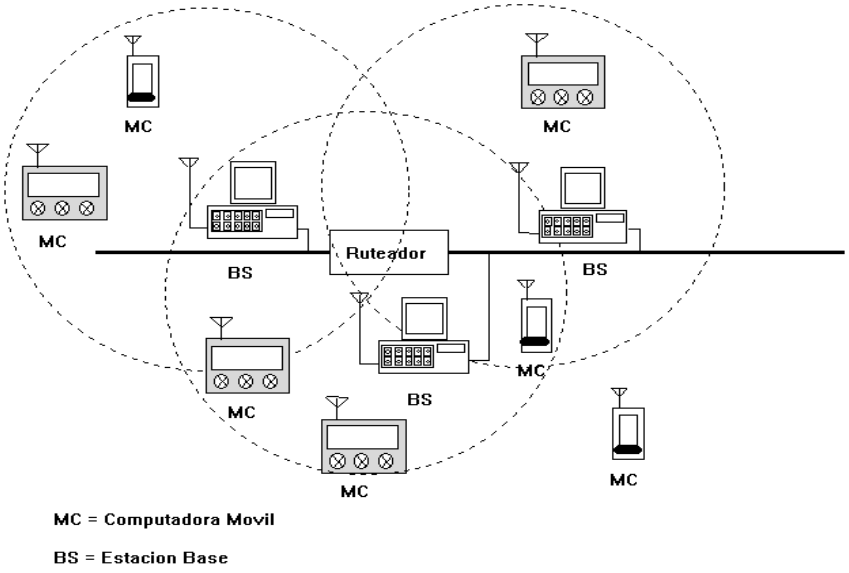


Figura 1.3 Administración de Ancho de Banda.

1.5 Un ejemplo de operación

Para iniciar la sesión, la MC (Computadora Móvil) envía un paquete "Respuesta" a su Cliente correspondiente, de manera normal. Si la MC no está dentro del área de la BS (Estación Base), entonces la transmisión no sirve. Si la MC está dentro del área, será "Adoptada" por la BS que sirve en esa área. En este caso el paquete que se envío, se mandará a la ruta apropiada por el Cliente correspondiente, tal y como ocurre en Internet. Si la MC de momento no está en servicio de alguna BS, se realizarán instrucciones independientes para obtener este servicio por algún protocolo, cuyo diseño no afectará la capa de transmisión IP del paquete saliente. En el caso de que la BS mapee su dirección IP constantemente, la MC al momento de entrar a la nueva área responderá con una petición de servicio a la BS. Las acciones tomadas por la BS y la MC, para establecer la conexión, no afectan al ruteo de paquetes salientes. En la figura 1.4 se muestra como los paquetes serán entregados a una MC cuando ésta se encuentre todavía dentro del área original, y en la figura 1.5 se indica que se tiene que hacer para entregar el paquete en caso de que la MC se haya cambiado a otra cobertura.

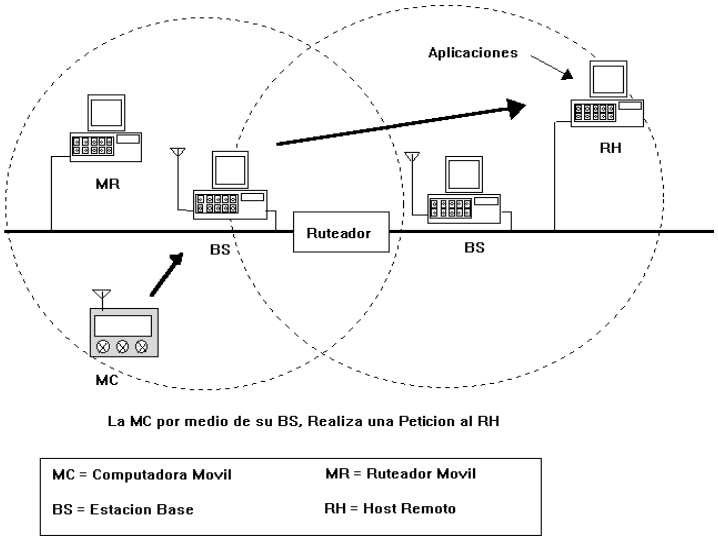


Figura 1.4 Petición de acceso.

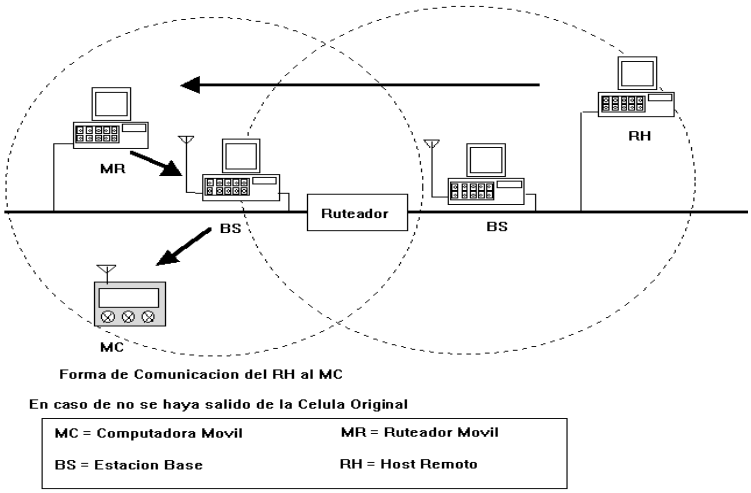


Figura 1.5 Comunicación entre un *Host* remoto y la computadora móvil.

Cuando un Cliente recibe un paquete de un Cliente móvil, y desea responder, éste enviará los paquetes a la ruta de Internet apropiada. Es muy probable que el paquete navegue entre varias redes, antes de que se pueda encontrar entre el Cliente correspondiente y el MR (Ruteador Móvil); el MR que da servicio a la célula indicará la dirección de la computadora móvil

Cuando una computadora móvil se mueve a otra célula, los datos asociados en el MR serán actualizados para reflejarlos a la nueva Estación Base que está sirviendo a la MC. Por consecuencia, cuando el MR es requerido para rutear un paquete a una computadora móvil, presumiblemente tendrá información actualizada con respecto a cual estación base debe de recibir el siguiente paquete.

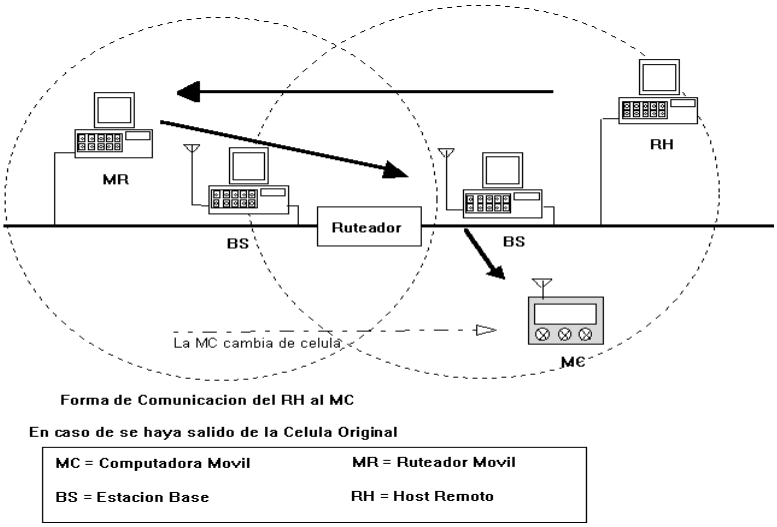


Figura 1.6 Movimiento de computadoras móviles entre células.

Para entregar el paquete a la Estación Base, el MR lo encapsula dentro de un nuevo paquete; conteniendo la dirección de la Estación Base, como la dirección IP de destino. Esta encapsulación puede realizarse con un protocolo determinado; el IPIP (IP dentro de IP). Entonces el paquete encapsulado es entregado por técnicas de ruteo IP convencionales a la estación base apropiada, la cual desenvolverá el paquete original y lo entregará a la computadora móvil.

Se debe de asumir que el MR ha sido propiamente notificado de cualquier cambio en la posición del MC. También cualquier contacto futuro del Cliente correspondiente con la MC, dependerá de la localización futura de la MC la cual de alguna manera se encargará de hacerle saber al MR su posición actual. Así, se considera que la comunicación bidireccional de datos, puede ser mantenida entre MC y cualquier Cliente cercano (móvil o no), debido a que el MR conoce todas las partes de la "Red Lógica" y la dirección de la MC.

Existen varias diferencias entre el modelo presentado y soluciones existentes para el mantenimiento de conexiones de redes IP para computadoras móviles:

1.- Los Clientes móviles pueden ser usados en cualquier parte de la red, sus direcciones han sido configuradas dentro de la tabla de rutas en el resto de la red local.

2.- Se ha utilizado un modelo existente de red con un Ruteo simple en el diseño, esto permite que las funciones del Ruteador sean distribuidas entre varios sistemas.

3.- Desde que la información ruteada es almacenada en el Ruteador, el sistema es protegido contra fallas en la operación de la Estación Base.

4.- Los Clientes remotos pueden fácilmente iniciar una conexión de red a cualquier MC en particular, sin buscar en cada Estación Base o rutas locales.

5.- No se requiere cambiar al protocolo TCP (Transfer Control Protocol, “Protocolo de control de transferencia”).

1.6 Retos de seguridad

Una red con cable está dotada de una seguridad inherente en cuanto a que un posible ladrón de datos debe obtener acceso a la red a través de una conexión por cable, lo que normalmente significa el acceso físico a la red de cables, sobre este acceso físico se pueden superponer otros mecanismos de seguridad.

Cuando la red ya no se sustenta con cables, la libertad que obtienen los usuarios también se hace extensiva al posible ladrón de datos. Ahora, la red puede estar disponible en cualquier lado próximo al ruteador inalámbrico.

Desde sus comienzos, 802.11 ha proporcionado algunos mecanismos de seguridad básicos para impedir que esta libertad mejorada sea una posible amenaza. Por ejemplo, los puntos de acceso 802.11 se pueden configurar con un identificador del conjunto de servicios (SSID). La tarjeta NIC también debe conocer este SSID para asociarlo al Punto de Acceso y así proceder a la transmisión y recepción de datos en la red. Esta seguridad, resulta ser muy débil debido a:

- Todas las tarjetas NIC y todos los AP conocen perfectamente el SSID.
- La tarjeta NIC o el controlador pueden manejarse localmente, si se permite la asociación en caso de que el SSID no se conozca
- No se proporciona ningún tipo de cifrado a través de este esquema

Aunque este esquema puede plantear otros problemas, esto puede o no ser suficiente para detener al intruso más inexperto.

Las especificaciones del protocolo 802.11 proporcionan seguridad adicional mediante el algoritmo de WEP (Wired Equivalent Privacy, “Privacidad equivalente al cableado”) [1] debido a la autenticación y cifrado de la información. El algoritmo WEP define el uso de una clave secreta de 40 bits y 104 bits para la autenticación y el cifrado, pero una limitación importante de este mecanismo de seguridad es que el estándar no define un protocolo de administración de claves para la distribución de las mismas. Esto supone que las claves secretas compartidas se entregan a la estación inalámbrica a través de un canal seguro independiente al 802.11. El reto aumenta cuando están implicadas un gran número de estaciones.

Los siguientes pasos describen un posible planteamiento genérico que se utilizaría para autenticar el equipo de un usuario de modo que obtenga acceso inalámbrico a la red:

- Sin una clave de autenticación válida, el punto de acceso prohíbe el paso de todo el flujo de tráfico. Cuando una estación inalámbrica entra en el alcance del punto de acceso, éste envía una petición a la estación.
- Cuando la estación recibe la petición, responde con su identidad.
- Posteriormente, el punto de acceso solicita las credenciales de la estación, especificando el tipo de credenciales necesarias para confirmar su identidad.
- El punto de acceso valida las credenciales de la estación y transmite una clave de autenticación al punto de acceso. La clave de autenticación se cifra de modo que sólo el punto de acceso pueda interpretarla.
- El punto de acceso utiliza la clave de autenticación para transmitir de manera segura las claves correctas a la estación, incluida una clave de sesión de difusión única para esa sesión y una clave de sesión global para las difusiones múltiples.
- Para mantener un nivel de seguridad, se puede pedir a la estación que vuelva a autenticarse periódicamente.

1.7 Descripción de la criptografía

La criptografía se compone de dos acciones: cifrado y descifrado. El cifrado es el proceso de dar vuelta a un plaintext[3] en un texto cifrado, mientras que el desciframiento es el proceso de volver los datos cifrados o texto cifrado de nuevo a su forma clara original.

La seguridad en la criptografía se basa en la premisa de que solamente el remitente y el receptor conocen la manera en la cual los datos fueron alterados para crear el mensaje. Hay generalmente dos tipos de métodos criptográficos, referidos como cifras, los cuales son: llaves simétricas o privadas, y sistemas dominantes asimétricos públicos.

1.8 Cifras Simétricas

En cifras simétricas, la misma llave se utiliza para cifrar y para descifrar un mensaje.

Aquí se ve un ejemplo: Se cambia de puesto el punto de partida del alfabeto en tres posiciones la llave del cifrado ahora es K=3.

Alfabeto Estándar: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Alfabeto Criptográfico: DEFGHIJKLMNOPQRSTUVWXYZABC

Por ejemplo:

Plaintext: SEGURIDAD INALAMBRICA

Texto cifrado: VHJYULGDG LQDODPEULFD

Algunos idiomas utilizan algunas letras más a menudo que otras, y consecuentemente los criptoanalistas tienen un punto de partida de el cual ellos pueden descifrar un mensaje.

1.9 Cifras Asimétricas

Hasta el advenimiento de la criptografía dominante asimétrica o pública en los años 70, el uso principal de la criptografía era un secreto. Hoy día, la criptografía se utiliza para muchas cosas, incluyendo:

- Prevención del acceso desautorizado de la información.
- Prevención del acceso desautorizado a los datos, a las redes, y su uso.
- Detección al tratar de forzar la inyección de datos falsos o la cancelación de estos.
- Prevenir la renegación

La criptografía asimétrica se base en que el remitente y el receptor no comparten una sola llave, si no que cada uno tiene su propia llave que a su vez se relacionan matemáticamente, de esta manera el conocimiento de una llave no implica ninguna información sobre lo otra.

[3] Un plaintext o texto plano es un texto ordinario antes de que sea encriptado en un texto cifrado o después de ser desencriptado.

Esto hace posible la distribución libre de una de las llaves (designada llave pública) mientras que la otra puede permanecer en secreto (designada llave privada), de tal modo que se elimina la necesidad de un proceso de distribución.

1.10 Protocolos de seguridad

Un protocolo es un conjunto de reglas (algoritmos, formatos de mensajes, interfaces, etc.) perfectamente conocidas por los dispositivos que intercambian información a través de una red de comunicaciones. Cada protocolo responde a un propósito concreto, razón por la que lo habitual es que en una red de comunicaciones intervengan varios de distinta índole. Estos conjuntos de reglas suelen agruparse en niveles o capas de distinta funcionalidad, de forma que cada uno de ellos se apoya en los servicios que le ofrece el anterior, y al mismo tiempo brinda al nivel superior nuevas opciones.

Los protocolos de un nivel ocultan la forma en que han sido implementados los servicios ofrecidos a la capa superior, lo que por una parte materializa una arquitectura modular que facilita la evolución de cualquier componente sin que esto conlleve modificaciones en el resto. Por otra parte, permite a los diseñadores abstenerse de la complejidad inherente a la resolución de toda la infraestructura de comunicaciones. Cada nivel que forma parte de la arquitectura de red utilizada en una máquina, únicamente puede "hablar" con su homologo en el otro dispositivo que interviene en la comunicación, siendo el protocolo el lenguaje común utilizado por ambos. No obstante, esto no significa que se este abordando un proceso de transferencia física de datos entre ambas capas en distintos equipos. Los paquetes de datos solo se transfieren entre niveles adyacentes de cada máquina vinculada al proceso de comunicación, para lo que se usan las interfaces entre niveles. Por ello, los paquetes de datos se envían a través de un medio de transmisión perfectamente conocido por uno de los niveles definidos en la arquitectura de la red: la capa física.

En 1983, la organización de estándares internacionales (ISO) propuso un modelo de referencia para la arquitectura de redes al que llamaron OSI (open systems Interconnection, "Interconexión de sistemas abiertos"). Realmente no se trata de una arquitectura en toda la regla, si no que más bien es un boceto que define de que debe encargarse cada nivel. El modelo OSI defiende la implementación de siete niveles de distinta funcionalidad: físico, enlace, red, transporte, sesión, presentación y aplicación, pero su principal problema es que se trata de un modelo muy complejo con funcionalidades incorrectamente situadas que, además están repartidas en niveles de grosor muy diferente. Estas son las razones por las que ya prácticamente no se utilizan en la actualidad (aunque se ha mantenido la denominación de los niveles que establece), algo muy diferente a lo que ocurrió con la arquitectura TCP/IP que constituye la base sobre la que se asienta Internet.

El avance en Internet llevó al desarrollo de los protocolos para transferencia de información de manera inalámbrica. El primer protocolo 802.11 ratificado por la organización IEEE apareció en 1997, y permitía abordar la transferencia de datos a través del medio aéreo a la velocidad de 1 y 2 Mbps. Dos años más tarde surgió la versión 802.11b, una modificación del primer protocolo que utilizaba nuevos métodos de codificación para alcanzar tasas de transferencia de hasta 11 Mbps. Esta revisión utiliza la frecuencia de 2.4000 GHz a 2.4835 GHz, la misma que posteriormente utilizaría 801.11g, una especificación aprobada en junio del 2003 capaz de alcanzar velocidades de transferencia máximas de 54 Mbps (no debemos olvidar que los protocolos utilizaron entre el 2% y el 20% del ancho de banda total, lo que reduce la tasa de transferencia útil), aunque puede también reducirse su tasa de transmisión a 5.5 Mbps, 2 Mbps o 1 Mbps cuando la interferencia afecta la calidad de transmisión.

En el año 2001 comenzó la comercialización de productos que satisfacían las especificaciones del estándar 802.11a, una versión de 802.11 que utiliza la banda de 5.15 GHz a 5.35 GHz y 5.725 GHz a 5.825 GHz. y que al igual que 802.11g, alcanza tasas de transferencia máximas de 54 Mbps. El problema de este protocolo radica en que esta banda esta reservada para otros servicios por lo que solo ha tenido cierto éxito en países como Estados unidos y Japón, en el resto del mundo el protocolo que ha tenido mayor aceptación es el 802.11g. No obstante la especificación 802.11a utiliza una frecuencia mucho menos saturada y por lo tanto, con menos interferencia y por otra parte, dispone de más canales que 802.11b. Esta última característica hace viable la instalación en una misma zona de un mayor número de puntos de acceso.

Sin embargo no todo son diferencias entre las distintas revisiones del estándar 802.11. Todos emplean lógicamente el mismo protocolo de control de acceso al medio, un derivado del CSMA/CD (Carrier Sense Multiple Access with Collision Detection, "Acceso múltiple censando portadora con detección de colisión") que se usa en redes Ethernet denominado CSMA/CA (collision Avoidance, "evitando colisiones"). Este debe de enmarcarse en el subnivel MAC (Media Access Control) de la capa de enlace y es el responsable en última instancia de administrar el acceso a un medio de transmisión compartido por varias máquinas. El problema en el ámbito de las redes inalámbricas es que no es posible detectar las colisiones utilizando el mismo algoritmo empleado en las redes cableadas, por lo que ha sido necesario cambiar el protocolo CSMA/CD por un mecanismo dotado de una mayor robustez en el medio de transmisión aéreo. CSMA/CA satisface estos requisitos solventando la imposibilidad de detectar las colisiones gracias a un algoritmo que exige la confirmación de los paquetes de datos que se transfieren entre emisor y receptor.

En lo que a las técnicas de codificación se requiere, existen importantes diferencias entre las distintas variantes del protocolo 802.11. La primera definición emplea modulación DBPSK (Differential Binary Phase Shift Keying, "Fase binaria diferencial en cambio de llave") o DQPSK (Differential Quadrature Phase Shift Keyed, "Fase cuadratura diferencial en cambio de llave"). 802.11b utiliza la técnica de modulación y conversión de símbolos CCK (Complementary Code Keying, "Código complementario de llaves") y por último, las especificaciones 802.11g y 802.11a usan modulación OFDM (Orthogonal Frecuency Division Multiplexing, "Multiplexado ortogonal por división de frecuencia"), aunque la primera puede emplear también CCK.

1.11 Características de seguridad en las WLAN

Actualmente se discuten las debilidades en el algoritmo WEP para cifrar los datos en transmisiones inalámbricas, y estas mismas debilidades han llevado al desarrollo de herramientas tales como "AirSnort" y "WEPCrack" que de manera automatizada obtienen claves de encriptación para el descifrado de la información. La IEEE ha organizado al 802.11i[4] para tratar los problemas de seguridad del protocolo 802.11x ya que los desarrolladores de hardware se encuentran compitiendo para establecer sus propias medidas de seguridad. No obstante actualmente el ingresar a una red inalámbrica sin autorización o descifrar la información que se maneja no es más que cuestión de tiempo. Más aun nuestra investigación demuestra que la mayoría de las redes inalámbricas no utilizan cifrado ni ningún método de encriptación. WEP está lejos de ser perfecto, pero proporciona por lo menos un impedimento a los intrusos y puede ayudar a prevenir las siguientes situaciones que resultan ser críticas:

- WLANs vulnerables que pueden permitir a un intruso la capacidad de obtener datos confidenciales de la red y de no dejar ningún rastro de ataque.
- WLANs vulnerables, colocadas detrás de un firewall y que por lo tanto se consideran confiables, pero que pueden proveer a un atacante una "entrada trasera" a la red. Este acceso puede conducir a ataques contra las máquinas en otra parte de la red.
- WLANs vulnerables que pueden servir como plataformas de lanzamiento para ataques contra otras redes sin que estas tengan alguna relación.

1.12 Transacciones seguras

Para poder afirmar que una comunicación entre dos entidades es segura se deben de cumplir cuatro requisitos principales:

[4] http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm

1.12.1 Autenticidad: todas las entidades participantes en la transacción deben de estar identificadas antes de comenzar la misma. Debemos estar seguros de que la persona con la que nos comunicamos es realmente quién dice ser, ya que podríamos estar facilitando datos importantes a una persona o entidad no deseada. La Autenticidad se consigue mediante el uso de los certificados y firmas digitales.

La misión principal de un Certificado Digital es garantizar con toda confianza el vínculo existente entre una persona, entidad o servidor web con una pareja de claves correspondientes a un sistema criptográfico de clave pública.

Un Certificado Digital es un documento electrónico que contiene datos de una persona o entidad (empresa, servidor web, etc.) y la llave pública de la misma, haciéndose responsable de la autenticidad de los datos que figuran en el certificado otra persona o entidad de confianza, denominada Autoridad Certificadora. Las principales Autoridades Certificadoras actuales son Verisign[5] y Thawte[6].

Los datos que figuran generalmente en un certificado son:

1. Versión: versión del estándar X.509, generalmente la 3, que es la más actual.
2. Número de serie: número identificador del certificado, único para cada certificado.
3. Algoritmo de firma: algoritmo criptográfico usado para la firma digital.
4. Autoridad Certificadora: datos sobre la autoridad que expide el certificado.
5. Fechas de inicio y de fin de validez del certificado.
6. Propietario: persona o entidad vinculada al certificado.
7. Llave pública: representación de la llave pública vinculada a la persona o entidad (en hexadecimal), junto con el algoritmo criptográfico para el que es aplicable.
8. Algoritmo usado para la misma para obtener la firma digital de la Autoridad Certificadora.
9. Firma de la Autoridad Certificadora, que asegura la autenticidad del mismo.
10. Información adicional, como tipo de certificado, etc.

El certificado Digital vincula indisolublemente a una persona o entidad con una llave pública, y mediante el sistema de firma digital se asegura que el certificado que recibimos es realmente de la persona que consta en el mismo. El sistema de firma digital liga un documento digital con una clave de cifrado.

El procedimiento de firma digital lo que hace es obtener un resumen de un documento o de un texto aleatorio y cifrarlo con llave privada del propietario del certificado. Cuando nos llega un certificado, y su firma digital asociada, tan sólo debemos obtener nosotros el resumen del mismo, descifrar la firma con la llave pública del remitente y comprobar que ambos resúmenes coinciden, lo que nos hace estar totalmente seguros de la autenticidad del certificado. Se firma un resumen del documento y no el documento mismo para evitar ataques contra el sistema de cifrado RSA y para no hacer el proceso demasiado lento. El procedimiento lo podemos seguir en la figura 1.7.

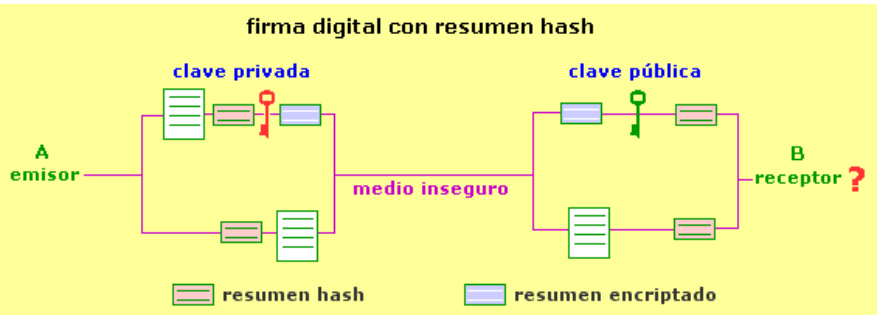


Figura 1.7 Firma digital con resumen *hash.*

[5] http://www.verisign.com/
[6] http://www.thawte.com/

Para obtener el resumen del documento se utilizan las funciones hash o de resumen, algoritmos criptográficos muy rápidos, de uso público e irreversibles (de un sólo sentido). Son funciones de dispersión que no usan ninguna clave, y que transforman el mensaje original en una cadena de dígitos de longitud fija (generalmente de entre 16 y 128 bits).

Los procesos de validación de certificados, obtención de resúmenes, descifrados y comprobación de coincidencia se realizan por el software adecuado del navegador web o programa de seguridad particular de forma transparente al usuario, por lo que éste será informado sólo en el caso de que el certificado no sea válido.

Dependiendo del uso que se vaya a dar al certificado y de qué persona o entidad lo solicita, las Autoridades Certificadoras han dividido los certificados en varios tipos. Del tipo de certificado a emitir van a depender las medidas de comprobación de los datos.

Toda persona o entidad que deseé obtener un certificado debe pagar una cuota a las Autoridades de Certificación, cuota que irá en función de la clase del certificado y del uso que se le vaya a dar al mismo (ambas están relacionadas). A mayor nivel de comprobación de datos (clase mayor), más costará el certificado.

1.12.2 Confidencialidad: debemos estar seguros de que los datos que enviamos no pueden ser leídos por otra persona distinta del destinatario final deseado, o que si esto ocurre, el espía no pueda conocer el mensaje enviado. O en su defecto, que cuando consiga obtener los datos éstos ya no le sirvan para nada. Es decir, debemos estar seguros de que ninguna persona ajena a la transacción puede tener acceso a los datos de la misma. La confidencialidad de consigue en las transacciones electrónicas con el uso de la Criptografía.

1.12.3 Integridad: es necesario estar seguro de que los datos que enviamos llegan íntegros, sin modificaciones, a su destino final. La integridad se consigue combinando Criptografía, funciones hash y firmas digitales.

1.12.4 Sin rechazo: debemos asegurarnos que una vez enviado un mensaje con datos importantes o sensibles, el destinatario de los mismos no pueda negar el haberlos recibido. El no repudio se consigue mediante los certificados y la firma digital.

Capítulo 2

El protocolo WEP

Capítulo 2: El protocolo WEP

2.0 Introducción

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar donde le llegase la señal.

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos).

2.1 WEP: Características y funcionamiento

WEP es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN. Estudiamos a continuación las principales características de WEP.

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

El algoritmo de encriptación utilizado es el RC4[1] [2] con claves (seed) 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 en forma de una clave o llave. 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, cada segmento de la información, para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y al final pueda deducir que clave se utilizó. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Sabemos lo primero, ya que la llave se tiene que capturar 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 posteriormente, observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

A continuación podemos ver el algoritmo que utiliza el protocolo de encriptación WEP, así como el diagrama 2.1.

1. Se calcula un CRC (Código de Redundancia Cíclica) de 32 bits. 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 formando el seed.
3. El PRNG (Pseudos Random Number Generator, "Generador de números pseudos aleatorios") de RC4 genera una secuencia de caracteres pseudoaleatorios (*keystream*), a partir del seed, de la misma longitud que los bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.
5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (frame body) de la trama IEEE 802.11.

[1] **RC4** o *Rivest Cipher 4* es un sistema de cifrado de flujo *Stream cipher*.

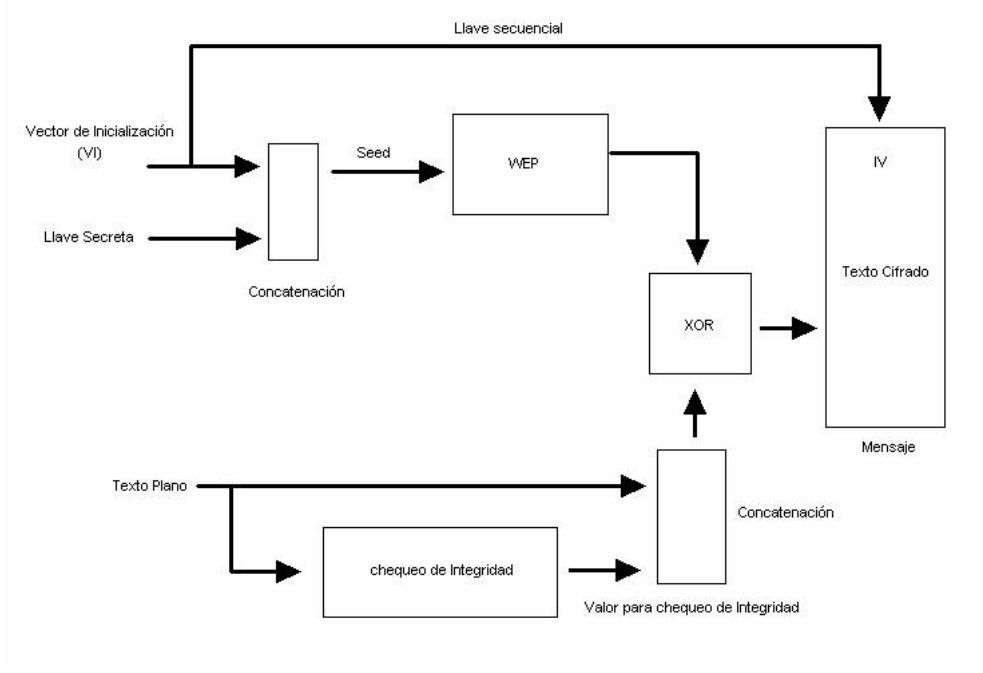


Figura 2.1 Diagrama de bloques del protocolo WEP.

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

2.2 Implementación del Protocolo WEP

El protocolo WEP utiliza una clave secreta "K" que es compartida entre los dispositivos que se comunican, para proteger el flujo de datos transmitidos. El cifrado de la señal procede de la siguiente manera:

- Checksumming: Primero, calculamos la integridad de la suma de comprobación c(M) de un mensaje M, concatenando el mensaje y la suma de comprobación para obtener un Texto Plano P = (M, c(M)), que será utilizado como la información entrante de la segunda etapa. Cabe notar que ni c(M) o P dependen de la clave K.
- Encriptación: En la segunda etapa, ciframos el texto plano P que se obtiene al utilizar RC4. Elegimos un vector de inicialización (VI) que llamaremos "v". El algoritmo RC4 genera entonces un keystream (es decir, una secuencia larga de bytes pseudoaleatorios) en función del vector de inicialización "v" y la clave K. Esta "keystream" es denotado por RC4(v, K). Entonces, Se realiza la operación booleana XOR (simbolizada por $\oplus$) entre el Texto Plano con el keystream para obtener el texto cifrado:

$$C = P \oplus RC4(v_1,k).$$

- Transmisión: Finalmente, transmitimos el IV y el texto cifrado.

Simbólicamente, esto se puede representar de la siguiente manera:

$$A \rightarrow B : v\ (P \oplus RC4(v_1,k))\ \text{donde}\ P = (M, c(M))$$

El formato del cifrado es el siguiente:

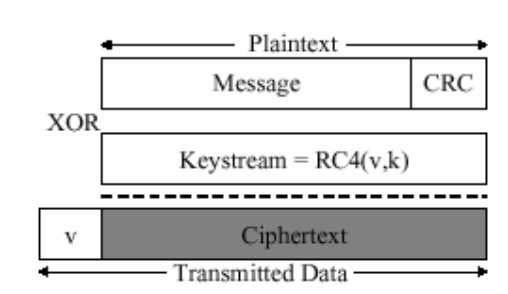


Figura 2.2 Diagrama de cifrado WEP.

Utilizaremos constantemente el término mensaje (M) para referirnos al campo inicial de los datos que se buscan proteger. El Texto Plano (P) lo utilizamos para referirnos a la concatenación del mensaje y de la suma de comprobación como se presenta en el algoritmo de cifrado RC4, y el término "Ciphertext" o texto cifrado (C) para referir a la encriptación del Texto Plano como el que se transmitió sobre nuestra conexión de radio.

Para desencriptar un campo protegido por WEP, el receptor simplemente invierte el proceso de cifrado. Primero, se regenera el keystream RC4(v, K) y se aplica la operación XORs sobre el texto cifrado para recuperar el texto inicial:

$$\begin{aligned} P' &= C \oplus RC4(v,k). \\ &= (P \oplus RC4(v,k)) \oplus RC4(v,k) \\ &= P \end{aligned}$$

2.2.1 Encriptación WEP paso a paso

1. Lo primero que se hace es calcular el checksum del texto que se desea transmitir. Para ello se puede utilizar el CRC-32 del CCITT. A esto se le denomina Valor de Chequeo de Integridad o ICV.
2. A continuación se selecciona una de las claves y se genera el IV, usando el RC4 para obtener un keystream formado por la clave elegida y el IV
3. El siguiente paso es concatenar el texto a cifrar con el ICV y se realiza una XOR bit a bit con el keystream, obteniendo así el texto cifrado.
4. Por último se envía el IV, el número de clave seleccionada y el texto cifrado a través del aire.
5. En la figura 2.3 se muestran todos estos pasos de forma esquemática.

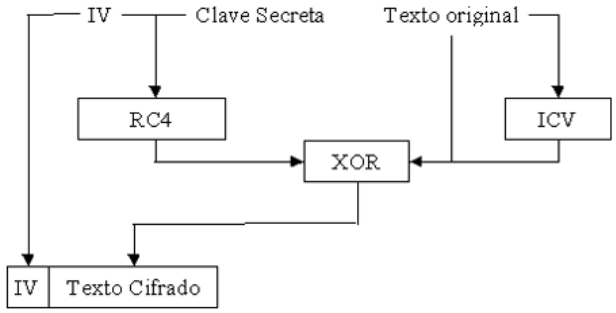


Figura 2.3 Diagrama de encriptado WEP.

2.2.2 Desencriptación WEP paso a paso

Lo primero es utilizar la clave indicada por el número de clave y el IV, ambos valores incluidos en el mensaje recibido, para generar mediante el RC4 el mismo keystream que se generó en el proceso de cifrado.

A continuación se realiza la XOR del keystream con el texto cifrado contenido en el mensaje recibido, obteniéndose así el texto original junto con el ICV.

Por último, se calcula un nuevo ICV de la misma forma que se hizo en el cifrado y se comprueba con el valor recibido en el mensaje. En caso de que los dos valores coincidan, la transmisión se realizó sin errores.

En la figura 2.4 podemos ver estos pasos de forma esquemática.

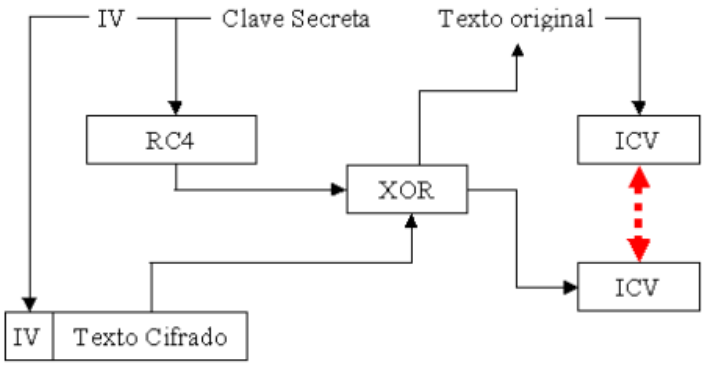


Figura 2.4 Diagrama de encriptado WEP.

2.3 Objetivos en la seguridad WEP

El protocolo de WEP trata de cumplir tres objetivos principales sobre la seguridad:

Secreto: El objetivo fundamental de WEP es prevenir las intromisiones ocasionales.

Control de acceso: El segundo objetivo de este protocolo es proteger el acceso a una red inalámbrica. El estándar 802.11 incluye una característica opcional para desechar todos los paquetes que no se cifren correctamente usando WEP.

Integridad de datos: El tercer objetivo es el evitar que los mensajes transmitidos sean modificados; el campo de la suma de comprobación de la integridad es incluido para este propósito.

En los tres casos, la seguridad se basa en la dificultad para descubrir la clave secreta por medio de un ataque.

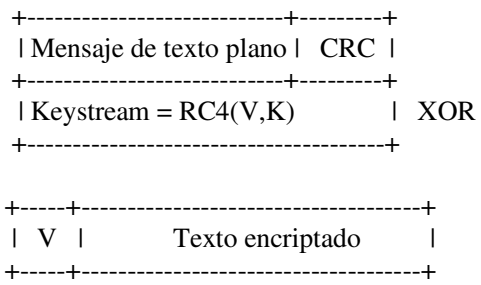
2.4 El Vector de inicialización y RC4

RC4 es un método de encriptación diseñado por Ron Rivest [2] para la RSA Security. Un flujo de cifrado expande una llave de longitud fija en una cadena infinita pseudo-variable con el propósito de encriptar los datos. Al utilizar WEP, los datos son operados por medio de la operación XOR con la cadena infinita pseudo-variable para obtener el texto encriptado. Una “OR” exclusiva (XOR) es un operador booleano que compara dos números y determina si son iguales o diferentes. Si los números son iguales, se obtiene un valor de "0"; si son diferentes, se obtiene un valor de "1". El siguiente ejemplo muestra el equivalente binario de la letra "b" que es operada utilizando el XOR con el equivalente binario de la letra "n":

01100010 Letra b, en binario.
01101110 Letra n, en binario.
00001100 Resultado del XOR.

WEP requiere que cada parte de la red inalámbrica conozca la llave secreta para el cifrado de la información. WEP no define las técnicas de manejo de las llaves tales como el número de claves diferentes que son usadas dentro de una red o de la frecuencia para cambiarlas. En la práctica, las redes utilizan solo una o algunas claves entre puntos de acceso. El flujo de cifrado producido por el algoritmo WEP depende de la llave secreta y de un vector de inicialización (VI). El VI se utiliza para asegurar que los paquetes subsecuentes de datos se cifran con diversos flujos de cifrado, a pesar de usar la misma clave secreta. El VI es un campo de 24 bits que no puede ser desencriptado sin el "header" o encabezado del paquete de datos, según lo que se muestra a continuación:

V = Vector de Inicialización
K = Llave Secreta



Según el informe generado por la universidad de Berkeley[2] [3], el uso de un VI de 24-bit es inadecuado porque es el mismo VI, y por lo tanto el mismo flujo de cifrado, que será reutilizado dentro de un período de tiempo relativamente corto. Un campo de 24 bits puede contener 224 o 16.777.216 valores posibles. Dado que una red puede funcionar por ejemplo a 11 Mbps y que transmiten constantemente paquetes de 1,500 bytes, un VI sería repetido (referido como VI de colisión) cada 5 horas como se detalla en el siguiente cálculo:

11 Mbps ÷ (1,500 bytes por paquete × 8 bits por byte) = 916.67 paquetes transmitidos cada segundo.

16, 777,216 VI ÷ 916.67 paquetes por segundo = 18,302.41745 segundos para usar todos los VI.

18,302.417 segundos × 60 segundos por minuto × 60 minutos por hora = 5.0840 horas para usar todos los VI.

Y este tiempo se podría reducir bajo algunas circunstancias. El panorama ya mencionado asume solamente un dispositivo en el VI de los datos y del incremento de la red que transmite por "1" para cada paquete transmitido. Cada dispositivo adicional que usa la misma llave secreta reduciría este tiempo. Dispositivos que usan VI de manera aleatoria también reducirían el tiempo requerido para que una colisión del VI ocurra. Una vez que una colisión de VI ocurre y un atacante tiene dos mensajes diferentes del texto plano cifrado con la misma llave, es posible obtener el XOR de los dos mensajes al aplicar el operador en ambos mensajes cifrados. El XOR que resulta se puede utilizar para descifrar el tráfico de información. El siguiente cálculo demuestra cómo aplicando la operación XOR en dos textos cifrados se cancela el flujo de cifrado:

[2] http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

C1 = TextoCifrado 1
C2 = TextoCifrado 2
P1 = TextoPlano 1
P2 = TextoPlano 2
V = Vector de inicialización
K = Llave secreta
⊕ = XOR

If C1 = P1 ⊕ RC4(V,K)
And C2 = P2 ⊕ RC4(V,K)
Then C1 ⊕ C2 = (P1⊕ RC4(V,K)) ⊕ (P2 ⊕ RC4(V,K))
= P1 ⊕ P2

Vamos a probar el algoritmo anterior en el siguiente ejemplo:

	Data
Letra “a” texto plano	01100001
Letra “n” llave secreta	01101110
XOR – “a”	00001111

	Data
Letra “b” texto plano	01100010
Letra “n” llave secreta	01101110
XOR – “b”	00001100

	Data
XOR – “a”	00001100
XOR – “b”	00001111
XOR – “a” & “b”	00000011

	Data
Letra “a” texto plano	01100001
Letra “b” texto plano	01100010
XOR – “a” & “b”	00000011

Por lo tanto, al usar la misma llave secreta, el valor de XOR de los mensajes del texto plano ("a" y "b") es equivalente al valor de XOR de los mensajes cifrados. Así, si un atacante tiene conocimiento del contenido de un mensaje del texto cuando ocurre una colisión del VI, el atacante puede entonces descifrar el contenido del otro mensaje del texto plano sin ningún conocimiento del flujo usado para el cifrado.

2.5 Control por redundancia cíclica

Como se había mencionado, WEP utiliza CRC-32 para asegurar la integridad de los datos transmitidos sobre la red inalámbrica. El control por redundancia cíclica (CRC) comprueba la integridad de las transmisiones calculando una suma de autentificación que se incluye con cada paquete de datos. El recipiente calcula la misma suma de comprobación para cada paquete de datos. Si las sumas de comprobación obtienen el mismo resultado, WEP asegura que no han sido modificados los datos durante la transmisión. Los mensajes transmitidos se dividen en longitudes predeterminadas y son divididos por un divisor fijo. El resto es un bit más pequeño que el divisor y sirve como la suma de comprobación.

En el caso de CRC-32, el resto es un número de 32-bits y esta suma de comprobación entonces está añadida sobre el mensaje enviado. En la figura 2.5 vemos una suma de comprobación CRC-32 (10100101001001111111110111111001) para la letra "b" (01100010):

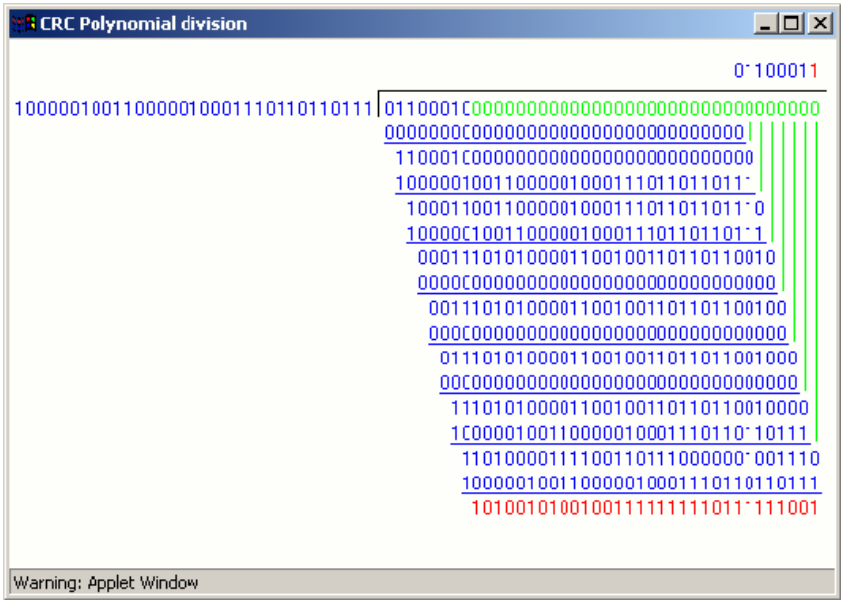


Figura 2.5 Ejemplo CRC.

Según el informe de la universidad de Berkeley [3], CRC-32 no es un método de comprobación apropiado para WEP ya que es una suma de comprobación lineal. Por lo tanto, las modificaciones se podían hacer al texto cifrado, y a la diferencia de bits entre el original y las sumas de comprobación modificadas podrían ser calculadas. Un atacante puede ajustar la suma de comprobación apropiadamente, y un receptor no estaría enterado que se ha alterado la información.

Veamos el siguiente caso: Se está encriptando la letra "b" usando una llave secreta de la letra "n." Para asegurar la integridad de los datos, una suma de comprobación CRC-8 se utiliza y se cifra en el paquete de los datos. El atacante desea alterar el mensaje moviendo bits en el paquete de los datos cifrado. Si el atacante no mueve simplemente los bits apropiados en el texto cifrado, la suma de comprobación descifrada no correspondería más y WEP revelaría que los datos fueron alterados. Por lo tanto, el atacante debe también determinar los bits apropiados para mover en la suma de comprobación cifrada. Antes de cualquier alteración, se calcula el paquete cifrado de los datos como sigue:

	Data	CRC-8
Letra “b” text plano	01100010	00101001
Letra “n” Llave secreta	01101110	01101110
encriptación XOR	00001100	01000111

El atacante podría determinar los bits que necesita mover en la suma de comprobación por la operación de XOR y cambiar los datos y su suma de comprobación correspondiente CRC-8 contra los datos originales y su suma de comprobación, como sigue:

	Data	CRC-8
encriptación XOR	00001100	01000111
Cambio	00000011	00001001
encriptación XOR Alterada	00001111	01001110

Para ver si la suma de comprobación alterada era calculada correctamente, primero se debe descifrar los datos y su suma de comprobación.

	Data	CRC-8
encriptación XOR Alterada	00001111	01001110
Letra “n” Llave secreta	01101110	01101110
Info desencriptada – letra ‘a’	01100001	00100000

Los datos descifrados (01100001) resultan ser la letra "a." Después, calculemos el CRC-8 de la suma de comprobación para la letra "a."

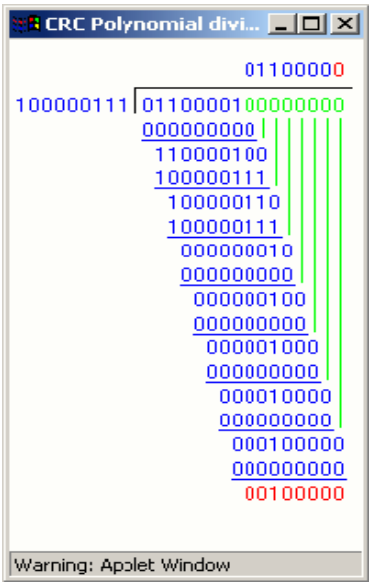


Figura 2.6 Resultado del ejemplo CRC.

La figura 2.6 muestra la suma de comprobación CRC-8 (00100000) fue calculado correctamente; por lo tanto, el paquete alterado no parece haber sido interceptado. Así el atacante no necesita tener completo conocimiento del mensaje original del texto plano. El atacante requiere solamente el conocimiento de los bits a cambiarse.

2.6 Problemas del algoritmo WEP

Los problemas más importantes a los que se enfrenta el algoritmo WEP se enlistan a continuación:

- **Autenticación del mensaje**: El código de redundancia cíclica elegido para la autenticación es débil, debido a que este código fue diseñado para control de errores no para autenticación. Es posible modificar un mensaje tal que el CRC sea válido para el mensaje, pero no será el mensaje enviado. También pueden inyectarse mensajes en otros de la misma manera.
- **Reutilización del keystream**: Debido a que la clave compartida es estática y raramente cambiada, la aleatoriedad del keystream depende del valor del IV. Por tanto, cuando se reutiliza un IV se tienen dos mensajes encriptados con el mismo keystream. A esto se denomina colisión. Si tenemos en cuenta que el tamaño del IV es de 24 bits, se producirán colisiones cada 224 paquetes, es decir, se repetirá el keystream aproximadamente cada 16 millones de paquetes, por lo que puede obtenerse el keystream utilizado.

- **Ataque por reutilización del keystream**: Lo primero es enviar un paquete conocido, por ejemplo un ping (un buen número de ellos) y cuando recibimos la respuesta tenemos el texto cifrado y el IV. Por tanto, tenemos el texto plano y el texto cifrado, por lo que podemos calcular el keystream de la siguiente forma K= P XOR C. Ahora basta con crear una base de dato indexada por el IV conteniendo los diversos keystream obtenidos y, para cada mensaje visto en el futuro, el atacante tendrá el keystream con el que decodificar dicho mensaje.
- **Algoritmo de manejo de clave de RC4**: El principal problema es una debilidad en el modo en el que el algoritmo de encriptación RC4 está implementado en el WEP. El problema es que tener un texto conocido impregnado en la clave (por ejemplo el IV) conduce a claves débiles que generarán texto cifrado conocido mediante el motor del algoritmo RC4, lo que permite al atacante crear un "motor inverso" que genere la clave a través de un texto cifrado conocido. Además, claves de mayor tamaño no solucionan el problema debido a que el ataque recupera cada byte de la clave por separado ya que intenta desencriptar la clave como un entero. Por tanto, el ataque crece linealmente y no exponencialmente como crecería la clave al aumentarla el tamaño.

2.7 Claves de 64 bits y 128 bits

Puede que parezca obvio para una persona no técnica que el esquema de cifrado de 128 bits sea más seguro que un cifrado de 64 bits. Esto sin embargo, no sucede con WEP, ya que existe la misma vulnerabilidad con ambos niveles de cifrado. Con WEP de 64 bits, el administrador de la red especifica una llave de 40 bits, típicamente diez dígitos hexadecimales (0-9, el a-f, o el vector de la inicialización de A-f), un vector de inicialización (IV) de 24 bits es añadido a esta llave de 40 bits, y el esquema del RC4 se constituye de estos 64 bits de información. Este mismo proceso se sigue con el esquema de 128 bits, especificando una llave de 104 bits, donde ahora los dígitos hexadecimales son 26 (0-9, a-f, o A-F). El vector de inicialización de 24 bits se agrega al principio de la llave y se utiliza nuevamente el esquema RC4.

2.8 Problemas en el vector de inicialización

La implementación del vector de inicialización en el algoritmo WEP tiene varios problemas de seguridad. Recordemos que el IV es la parte que varía 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. Según se indica que debería cambiarse en cada trama para mejorar la privacidad, pero no obliga a ello. 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. Y esto ocasiona que las primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente. Más aún si tenemos en cuenta que cada estación utiliza la misma clave secreta, por lo que las tramas con igual clave se multiplican en el medio.

Por otro lado, el número de vectores diferentes no es demasiado elevado (2^{24}=16 millones aprox.), por lo que terminarán repitiéndose en cuestión de horas. El tiempo será menor cuanto mayor sea la carga de la red. Lo ideal sería que el IV no se repitiese nunca, pero como vemos, 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. Observemos 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.

La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse. Bien es cierto que existen implementaciones con claves de 128 bits (lo que se conoce como WEP2), sin embargo, en realidad lo único que se aumenta es la clave secreta (104 bits) pero el IV se conserva con 24 bits. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

2.9 Riesgos de la reutilización del Keystream

Como se ha mencionado, el mayor problema sobre la encriptación de mensajes, es la reutilización del IV y la misma clave en varios mensajes, ya que entonces se puede revelar la información de ellos:

$$\begin{aligned} \text{If} \quad & C_1 = P_1 \oplus RC4(v,k). \\ \text{And} \quad & C_2 = P_2 \oplus RC4(v,k). \\ \text{Then} \quad & C_1 \oplus C_2 = (P_1 \oplus RC4(v,k)) \oplus (P_2 \oplus RC4(v,k)) \\ & = P_1 \oplus P_2 \end{aligned}$$

Es decir al aplicar el XOR sobre los dos textos cifrados (C1 y C2) provoca que el keystream cancele el flujo de salida, y el resultado es simplemente el XOR de ambos textos (P1 ⊕ P2).

Así, la reutilización del keystream puede conducir a un posible ataque ya que si el texto de uno de los mensajes se conoce, el texto del otro mensaje se puede obtener de manera inmediata. En general, los textos tienen a menudo bastante redundancia, por lo que se puede recuperar tanto P1 como P2 realizando la operación "P1 ⊕ P2". Existen técnicas también conocidas que realizan la operación de XOR que buscan textos definidos al realizarse el XOR y que tengan un valor dado de la operación de P1 ⊕ P2. Por otra parte, si tenemos "n" textos cifrados y todos reutilizan el mismo keystream, tenemos un problema llamado "profundidad n". Así la lectura del tráfico con cierta profundidad llega a ser más fácil mientras "n" aumenta, puesto que en parejas el XOR de cada par de textos puede ser calculado, y hay muchas técnicas clásicas que se conocen para solucionar tales dificultades (como por ejemplo, análisis de frecuencia).

Hay que observar que hay dos condiciones requeridas para que esta clase de ataque pueda tener éxito:

1.- La disponibilidad de los textos cifrados donde una cierta porción del keystream se utiliza más de una vez.
2.- Conocimiento parcial de algunos de los textos.

Para prevenir estos ataques, WEP utiliza IV's preconcebidos para variar el proceso de generación del keystream para cada campo de datos que va a ser transmitidos. WEP genera el keystream RC4(v, K) en función de la clave secreta K (que es igual para todos los paquetes) y un vector público v (que puede variar para cada paquete), de esta manera, cada paquete recibe un keystream diferente. El IV se incluye en la porción no encriptada de la transmisión de modo que el receptor pueda saber que IV va a utilizar al derivar el keystream para la desencriptación. El IV está por lo tanto disponible para los atacantes también, pero la clave secreta sigue siendo desconocida y mantiene la seguridad del keystream. El uso de un IV predefinido fue pensado para prevenir ataques derivados de la reutilización del keystream. No obstante, WEP no alcanza por completo este objetivo.

2.9.1 Colisiones del keystream

Una causa de la reutilización del keystream viene del uso incorrecto del IV. Cabe notar que debido a que la clave secreta que es compartida no cambia con regularidad provocando la reutilización de IV y a su vez la reutilización de algunos de los keystream RC4. Puesto que los IV son públicos, los IV duplicados pueden ser detectados muy fácilmente por un atacante. Por lo tanto, cualquier reutilización de los viejos valores del IV expone al sistema a los ataques por "reutilización del keystream". Tal reutilización de un valor del IV se conoce como "colisión".

El estándar de WEP recomienda (pero no requiere) que el IV sea cambiado después de cada paquete, sin embargo, no dice nada sobre cómo seleccionar los IVs. Algunas tarjetas PCMCIA restauran el IV a 0 cada vez que son reinicializadas y después incrementan el IV por cada paquete transmitido. Estas tarjetas se reinicializan cada vez que se insertan en la computadora portátil, Aunque esto puede o no suceder con frecuencia.

Peor aun, el estándar WEP tiene defectos estructurales que expone a todas las implementaciones del WEP a los riesgos de la reutilización del keystream. El campo del IV usado por WEP es de solamente 24 bits, garantizando casi que el mismo IV será reutilizado por los múltiples mensajes. Un cálculo muestra que un acceso ocupado envía 1500 bytes y que ocupa un ancho de banda promedio de 5Mbps (la transmisión completa es de 11Mbps para el 802.11b), así un atacante puede encontrar fácilmente los campos con la clave de validación, porque la longitud del IV es fija (24 bits), esta vulnerabilidad es fundamental: ninguna implementación puede evitarla.

Los detalles de la implementación pueden hacer que el keystream se reutilice con más frecuencia. Se esperará que una implementación que utiliza un IV de 24 bits para cada paquete incurra en colisiones después de transmitir apenas 5000 paquetes, que son solamente algunos minutos de transmisión. Y como el estándar 802.11 no requiere que el IV esté cambiado con cada paquete, una implementación podría reutilizar el mismo IV para todos los paquetes.

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

Otra variante es el WEP dinámico. En este caso se busca incorporar mecanismos de distribución automática de claves y de autentificación de usuarios mediante 802.1x/EAP/RADIUS [3]. Requiere un servidor de autentificación 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.

En el capítulo 4 se ahonda más en este tema, explicando el uso de VPNs, así como de protocolos que buscan sustituir al WEP como el WPA.

[3] RADIUS (Remote Access Dial-In User Server). Es un protocolo de autentificación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Capítulo 3

Ataques a redes WEP

Capítulo 3: Ataques a redes WEP

3.0 Introducción

Para que podamos prevenir un ataque contra nuestra red inalámbrica, es necesario entender cómo un intruso encontraría y atacaría al objetivo. El conocer estos aspectos, nos brinda la posibilidad de implementar las medidas necesarias que aseguren estos puntos débiles. De esta manera, si bien no tenemos una red segura en su totalidad, si brindará el mayor número de obstáculos posibles a un atacante, que buscaran al final hacer de una intrusión una tarea tan ardua y difícil que el atacante posiblemente se abstendrá de realizarla.

3.1 Herramientas y equipo requerido para un ataque

Lo primero que se debe de tener son las herramientas adecuadas para realizar los ataques a las redes inalámbricas. El primer equipo será una computadora (portátil de preferencia).

El segundo artículo será una tarjeta o un equipo que permita una conexión 802.11, esto será utilizado para identificar y localizar las señales de radio.

Finalmente, software. Existen varios programas para localización de redes inalámbricas que se pueden utilizar, dependiendo del sistema operativo. Para Windows se puede descargar el NetStumbler para redes abiertas y Ethernet para redes cerradas, además de WildPacket o AiroPeek como un sniffer[1] o husmeador. Posteriormente en cada uno de los incisos se mencionaran paquetes de software que se pueden utilizar para cada una de las tareas requeridas.

3.2 Encontrar un objetivo

Con pocas excepciones (tales como los Starbucks o los Sanborns), la mayoría de las compañías con una red inalámbrica no anunciará su existencia al mundo exterior. Para evitar riesgos, la mayoría de las compañías publicaran solamente la información de la WLAN a los empleados que la utilizarán.

En la preparación para la intrusión, un hacker tendrá que descubrir si una red inalámbrica existe, así como determina los límites de la red.

Utilizando las herramientas creadas para la identificación de redes inalámbricas como el Wififofun o el NetStumbler se puede "escuchar" la información de una red, tal como el SSID. Cuando se encuentra una red, el software notifica a la persona que realiza la exploración y la agrega a la lista de redes encontradas.

3.2.1 Localizando WLANs

Por diseño, las WLANs 802.11x hacen el proceso de identificación en las redes inalámbricas de una manera relativamente directa. Para encontrarse unos a otros, los puntos de acceso inalámbricos (APs) y los clientes envían "avisos" (que llamaremos beacons) en intervalos predefinidos. Estos "avisos" son esencialmente direcciones que "invitan" y conducen al cliente para encontrar el AP y que se realicen las configuraciones y los ajustes necesarios para que se pueda entablar una comunicación.

Un beacon anuncia el SSID y el canal que la red está utilizando. El SSID es simplemente una secuencia de texto de la cual distingue una red 802.11x otros dispositivos que funcionan en el mismo canal. El canal es un número entre 1 y 11 (E.U.) o 1 y 13 (Europa) que identifica la frecuencia en la cual la red está funcionando.

[1] Un sniffer es un programa que captura tramas de red.

Al configurar una WLAN, el canal y el "service set identifier" (SSID) deben de ser configurados junto a los ajustes tradicionales de la red tales como el "IP ADDRESS" y el "*SubnetMask*[2]". Los canales asignables manejan las siguientes frecuencias:

Channel	Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

El SSID es una secuencia alfanumérica que distingue las redes que funcionan en el mismo canal. Es esencialmente un nombre configurable eso identifica una red individual. Estos ajustes son factores importantes al identificar WLANs y en la detección de tráfico.

Mientras que este sistema permite la simple configuración de redes y reduce al mínimo las molestias al moverse entre redes, es una debilidad muy significativa en la seguridad. Afortunadamente, algunos APs permiten que los paquetes "beacon" sean deshabilitados. Esta acción, sin embargo, no detendría a los scanners (por ejemplo el software de NetStumbler[3]) de poder identificar WLANs, ya que algunos scanners funcionan enviando una corriente constante de paquetes de difusión en todos los canales, entonces los APs responden a los paquetes de difusión para verificar su existencia, aun si la opción los beacons ha sido deshabilitada.

En su última versión, Netstumbler funciona en cualquier sistema wireless. En las versiones anteriores era algo problemático a la hora de utilizar algunos chipsets, mientras que ahora trabaja con la mayoría, incluido el Intel Centrino. La desventaja que tiene es que realmente se trata de una herramienta de detección básica. Si queremos desmontar una red (con buena o mala intención) será necesario contar con una herramienta típica de los hackers. Primero necesitaremos un software capaz de trabajar y compilar código fuente. A continuación, es preciso contar con los drives apropiados de nuestra tarjeta de red y con el software apropiado (En el capítulo 8 ahondaremos más sobre esto). Cuando se pone en marcha el software, buscará un canal simple y nosotros debemos disponer nuestra tarjeta en el modo de "Channel hopping" (Salto de canal), al margen de tener también en cuenta el modo monitor. Cuando este todo listo, empezara el suministro de datos y hay que estar muy atentos y es que no solo se muestra que puntos de acceso y clientes hay a nuestro alrededor, si no quienes están hablando en cada uno de los dispositivos.

Una vez que se ha encontrado al objetivo que nos interesa, habrá que apagar la funcionalidad de "Channel hopping", de manera que veamos los paquetes capturados y podamos analizarlos.

Una prueba que realizaron los laboratorios de iDEFENSE [4] consistió en equipar una unidad móvil con NetStumbler. El equipo constataba de una computadora portátil profesional que corría Microsoft Windows 2000, el NetStumbler v0.3.23 y una tarjeta de red de Lucent Orinoco PC 802.11b. Con esta unidad comenzaron a explorar un área para la localización de WLANs.

Después de aproximadamente 45 minutos el experimento de los Laboratorios iDEFENSE había identificado cerca de 140 WLANs. Esta primera etapa de investigación se llevo a cabo en Virginia del norte, una área que no se encuentra ocupada en gran medida por compañías que pudieran adoptar fácilmente las tecnologías inalámbricas, por lo que el experimento se mudo al área de Manhattan debido a la gran concentración de compañías que podrían estar utilizando WLANs dentro de una isla tan pequeña. Los resultados eran impresionantes ya que no habían pasado más de 15 minutos de recorrido y NetStumbler ya había registrado 236 WLANs, de las cuales 198 no utilizaban ningún tipo de encriptación.

[2] El subnet mask es una dirección de 32 bits, que indica cuantos de esos bits están siendo utilizados para el Network ID
[3] http://netstumbler.com/

El descubrimiento más asombroso era que el 75% de las redes de Manhattan no poseían ningún tipo de cifrado; cerca del 72% de las redes de Virginia tampoco. WEP tiene sus defectos, pero por lo menos proporciona un cierto grado de seguridad. Un intruso, podría tener acceso a centenares de WLANs, de hecho el atacante probablemente ni se incomodaría en tratar de descifrar la encriptación de un WEP ya que las WLANs al no tener la opción habilitada, no ofrecerían ningún tipo de problema para poder entrar a la red.

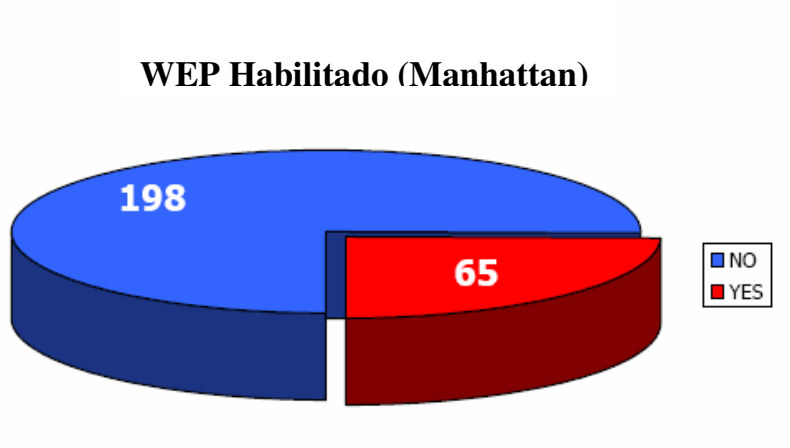


Figura 3.1 Porcentaje de redes inalámbricas con WEP habilitado.

APs	Número	Porcentaje
WEP no habilitado	**198**	**75%**
WEP habilitado	**65**	**25%**
Total	**263**	**100%**

En el mejor de los casos, solo serían necesarias varias horas para obtener una llave de WEP, pero un atacante solo necesita algunos minutos para identificar una red abierta sin ningún tipo de restricción. Una vez que se implementa una WLAN sin que tenga habilitado el WEP, el atacante puede comenzar a detectar tráfico en texto plano de manera inmediata. Si el acceso libre al Internet es el objetivo, el atacante solamente necesita obtener un IP ADDRESS válido, un desafío meramente trivial al tenerse habilitado el DHCP en las WLANs. Igualmente sin DHCP, solamente un número limitado de IP ADDRESS privadas son disponibles por lo que un atacante solo tendría que obtener una de ellas para que estuviera en la posibilidad de poder robar recursos.

3.3 Explotando las debilidades de la WLAN

Un punto de acceso inalámbricas bien configurado no parará a un atacante resuelto, si se cambia el nombre de la red, los SSID y la llave secreta se configura de nuevo manualmente en todos los sitios de trabajo sobre una base algo regular, existen procedimientos que el atacante tomará para comprometer la red.

Si hay un fácil acceso cerca a la red inalámbrica tal como un estacionamiento o garaje al lado del edificio, entonces la única cosa que un atacante necesita es la paciencia y el software indicado. Cuando se han capturado bastantes paquetes "débiles" (colisiones del vector de inicialización, por ejemplo) puede determinarse la llave secreta actualmente en uso en la red. Las pruebas rápidas han demostrado que una red casera media se puede intervenir en una sesión de un par de horas, esto nos dice que necesitaríamos cambiar la llave de WEP por lo menos dos veces por día.

3.4 Husmear, Interceptar y descifrar

Concebido originalmente como herramienta legítima del análisis de la red y de tráfico, los sniffers son ahora una de las herramientas más eficaces para atacar redes inalámbricas.

El hacker tiene muchas herramientas disponibles para atacar o espiar una red inalámbrica, como Ethereal y AiroPeek[4] en Windows y ngrep[5] en UNIX o Linux. Todos los paquetes de software funcionan poniendo su tarjeta de red en modo "Promiscuo", en este modo, cada paquete que va más allá del interfaz se captura y se exhibe dentro de una ventana (Figura 3.2). Si el atacante puede adquirir su contraseña de WEP, después pueden utilizar características dentro de AiroPeek y Ethereal para descifrar los datos.

Una vez que el hacker haya encontrado posibles redes para atacar, una de las primeras tareas es identificar quiénes es el blanco. Muchas organizaciones incluyen su nombre o dirección en el nombre de la red, esto puede permitir que a su vez en Internet se busquen características de la empresa que permitan determinarse su Domain Name, el DNS y otra información que puedan determinar si vale la pena atacar o no.

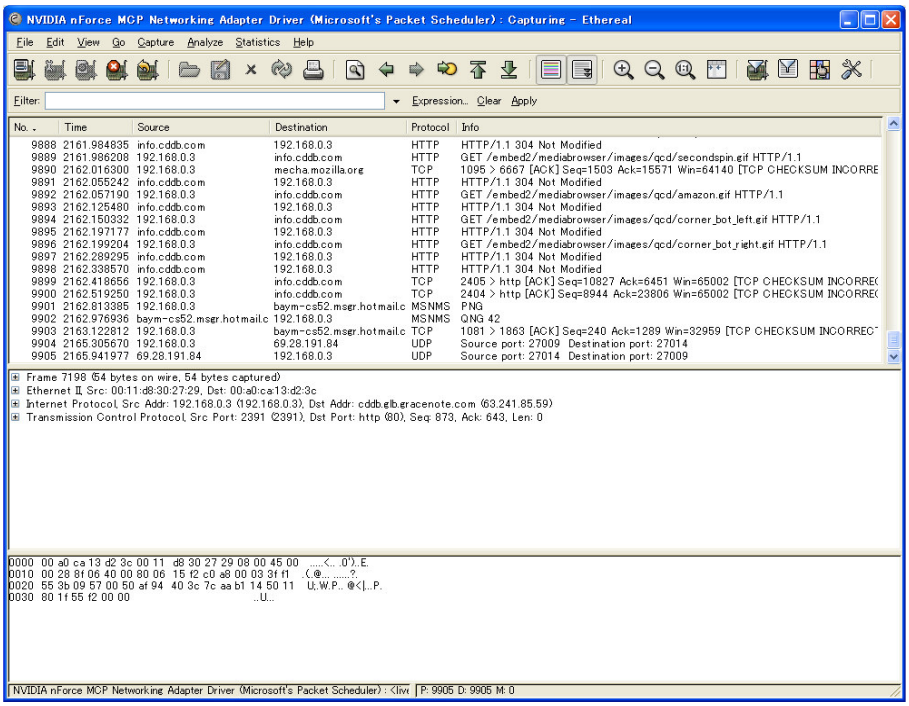


Figura 3.2 Pantalla de Ethereal.

3.4.1 Buscando claves WEP

La automatización de las herramientas de ataque que han desarrollado los hackers, era inevitable. Posterior al lanzamiento de algunos documentos de investigación como "Using the Fluhrer, Mantin and Shamir attack to Break WEP" [5] e "intercepting mobile Communications: The insecurity of 802.11" [6] (Ambos documentos discuten ataques contra algoritmos del WEP), una amplia gama de herramientas estuvieron disponibles para la captura de información vía remota, pero WEPCrack[6] y AirSnort[7] son dos de los más populares. WEPCrack es una serie de "scripts" en Perl diseñados para romper claves de WEP usando los datos capturados por un sniffer. AirSnort, por otra parte, obtiene el tráfico necesario para romper el cifrado sin la necesidad de un sniffer.

[4] www.wildpackets.com/products/airopeek
[5] http://ngrepel sourceforg.net
[6] http://wepcrack.sourceforge.net/
[7] http://airsnort.shmoo.com/

3.4.2 Husmeando el Tráfico

Una vez que se haya obtenido la clave WEP, el proceso para "husmear" en el tráfico descifrado no es muy diferente al que se realiza en una LAN cableada; sin embargo, no todos los *sniffers* trabajan con 802.11b o 802.11g, algunos necesitaran parches para que trabajen correctamente.

Si una WLAN no emplea la encriptación de datos, la única configuración que necesitaremos para comenzar a "husmear" por la red es el canal donde opera la red, que se puede determinar usando las herramientas de scanner de WLAN como por ejemplo NetStumbler. Una vez que esté configurada la tarjeta de la red, se tiene que colocar en "Channel hopping". Este modo se fija generalmente con las herramientas anexadas a los drives de la tarjeta de red. En Linux la herramienta wlanctl-wlanctl-ng puede cambiar la mayoría de los ajustes de la configuración en una tarjeta de red 802.11x, incluyendo el de poder fijar el canal que las aplicaciones de la tarjeta utiliza y la colocación de la tarjeta en modo "promiscuo".

Una vez que la tarjeta de la red se haya configurado correctamente, hay que correr el sniffer, y no queda otra más que sentarse y esperar. Si se esta interesado en leer mensajes privados de E-mail, un sniffer capaz de reensamblar los paquetes haría la tarea mucho más fáciles. Por ejemplo podemos habilitar toda una infraestructura de intromisión en una red utilizando una tarjeta de Lucent ORiNOCO y el softeware de eEye Digital Securitys Iris y Ethereal basados en Windows además de los controladores de Lucent ORiNOCO proporcionados con Wildpackets[8] AiroPeek o AiroPeek NX. Para esto primero se instala el programa de AiroPeek o AiroPeek NX. Posteriormente se actualizan los controladores de la tarjeta de Lucent ORiNOCO contenidos en el directorio \Diver\Lucent para permitir que Iris o Ethereal utilice la tarjeta de Lucent.

3.5 Spoofing y acceso desautorizado

La combinación de debilidades en WEP, y la naturaleza de la transmisión inalámbrica, ha desarrollado el arte del *spoofing* como amenaza verdadera a la seguridad de redes inalámbricas.

Spoofing lo podemos definir como la acción donde un atacante trata de "engañar" a una red para que ésta vea al intruso como una de las máquinas válidas y permitidas de la red. Existen varias maneras de lograr esto, el más fácil es redefinir simplemente el MAC ADDRESS de la tarjeta a una MAC válida, esto se puede lograr adentro de Windows con un registro simple o en UNIX con un simple comando. Varios sistemas inalámbricos también tienen una opción para definir MAC ADDRESS para cada conexión inalámbrica.

El proceso de la autentificación, según lo definido por IEEE 802.11, es un proceso muy simple. En una configuración de llave compartida, el AP envió 128 bytes al azar en un mensaje de cleartext al sitio de trabajo que desea sea autenticado. El sitio de trabajo después cifra el mensaje con la llave compartida, regresa el mensaje cifrado al AP. Si el mensaje empareja lo que está esperando el AP, entonces el sitio de trabajo se autentica sobre la red y se permite el acceso.

Según lo descrito, si un atacante conoce los mensajes del plaintext y del texto cifrado, entonces puede crear mensajes cifrados. Husmeando la red inalámbrica, un atacante puede acumular muchas peticiones de autentificación, cada uno de las cuales incluye el mensaje original del plaintext y la respuesta de texto cifrada. Con esto ya es fácil para el atacante identificar el keystream usado para cifrar la respuesta del mensaje. Así se podrían estar generando mensajes de autentificación que el AP aceptará como autentificación apropiada.

3.5.1 Herramientas de Spoofing

Un hacker no necesita muchas herramientas complejas para tener éxito en realizar un spoofing a MAC ADDRESS, lo complejo es la capacidad de forjar la autentificación sobre una red inalámbrica.

Una vez que el hacker haya identificado el objetivo que van a atacar, el paso siguiente es ser parte de la red inalámbricas. Si la red permite solamente las direcciones MAC válidas, entonces el primer paso que el atacante necesitará tomar será determinar una MAC válida.

[8] http://www.wildpackets.com/

Si la red no permite el cifrado, entonces la necesidad del atacante será solamente determinarse el MAC. Hay poco que se puede hacer para prevenir este tipo de ataques por la misma naturaleza de las transmisiones inalámbricas, lo que se puede hacer es utilizar un medio externo de autentificación, tal como RADIUS o SecurID, que prevendrán que usuario desautorizado tengan acceso a la red y a los recursos inalámbricos. Si se utilizan SSH y el SSL, entonces es posible requerir certificados válidos del cliente al tener acceso a esos recursos.

3.5.2 MAC Spoofing

Si se descubre que un MAC ADDRESS no se puede asociar con el punto de acceso (ver figura 3.3), hay otras maneras de obtener una MAC valida ya que una computadora portátil puede ver la comunicación del resto de las estaciones con cualquier AP dentro de la red. Puesto que las direcciones del MAC de las otras estaciones se transmiten en texto claro, debe ser fácil comenzar a compilar una lista de las direcciones del MAC permitidas en la red.

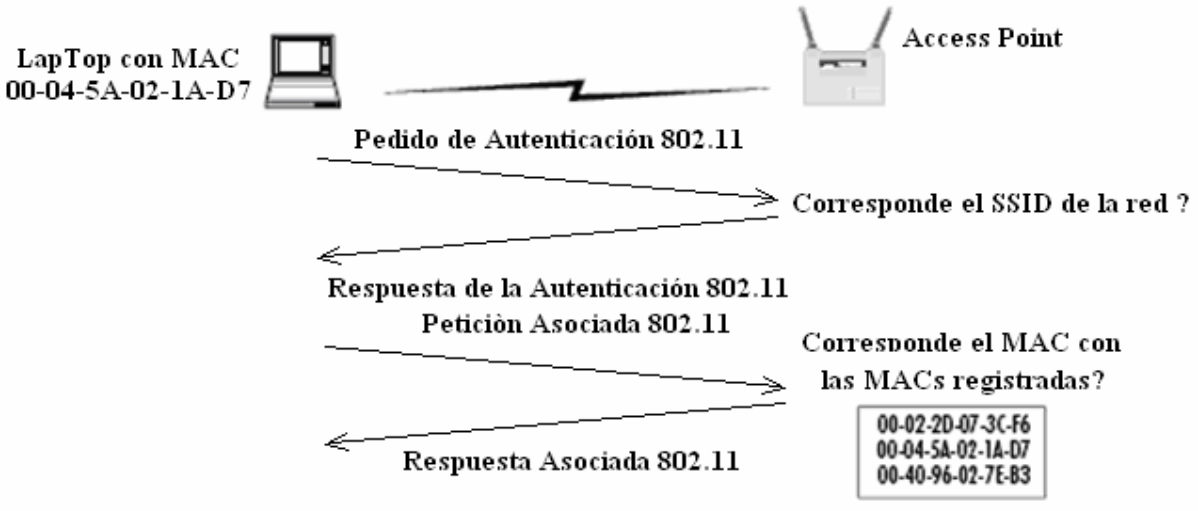


Figura 3.3 Para una asociación exitosa, el dispositivo móvil debe de tener Un Mac Valido.

Una vez que se haya modificado el MAC ADDRESS, se debe poder asociar con el AP. Hay que tener presente sin embargo, si el dispositivo que lleva el MAC ADDRESS que se ha obtenido, todavía está funcionando en la red, no podremos acceder a la red ya que no se permite la operación de dos direcciones duplicadas del MAC al mismo tiempo.

3.5.3 Características del MAC

Si vemos la dirección de 00-00-86-4C-75-48, los primeros tres octetos se llama identificador del proveedor (OUI). La IEEE controla estos OUIs y los asigna a las compañías según lo vayan requiriendo. Si se busca 00-00-86 OUI en el Web site del IEEE[9], indicará que el fabricante de este NIC es 3Com Corporation.

Las corporaciones pueden poseer vario OUIs, y adquieren a menudo OUIs adicional cuando compran a otras compañías. Por ejemplo, cuando Cisco compró Airones en 1999, agregaron 00-40-96 OUI a otros que ya tenían.

[9] http://standards.ieee.org/regauth/oui/index.shtml

Otros OUIs que se podría ver en una WLAN pueden ser:

_ 00-02-2D -- Agere Communicatios (conocida previamente como ORiNOCO)

_ 00-10-E7 – Breezecom

_ 00-E0-03 -- Nokia

_ 00-04-Ä – Linksys

Los tres octetos restantes en un MAC ADDRESS se queman generalmente en NIC durante la fabricación, así asegurando que no existirán direcciones duplicadas en una red.

3.6 Ataques por infiltración de mensajes

Otra manera de determinar el contenido de uno de los dos mensajes de texto plano es cuando un atacante logra infiltrar un mensaje de texto plano conocido en la red. Consideremos la siguiente posibilidad: Un atacante puede enviar un mensaje de e-mail a un servidor que está utilizando una red inalámbrica. Cuando el usuario recupera el mensaje de e-mail, este fue transmitido desde el servidor de e-mail al punto de acceso inalámbrico, donde sería cifrado con el algoritmo de WEP.

El mensaje cifrado entonces sería transmitido al usuario. Simultáneamente, el atacante podría detectar el tráfico de la red y capturar los paquetes que contienen el e-mail encriptado. Una vez que ocurra una colisión del VI y el atacante captura un mensaje subsecuente cifrado con el mismo flujo de cifrado dominante, la desencriptación del nuevo mensaje de texto plano sería posible. Con los dos mensajes de texto plano y sus valores cifrados de XOR, el flujo de cifrado podía entonces ser calculado. Con el suficiente tiempo y dedicación, un atacante puede desarrollar un diccionario de las claves de flujo de cifrado y en última instancia descifrar todo el tráfico en la red.

802.11 encapsula y encripta los encabezados de los protocolos de alto nivel tales como ARP e IP. Por lo tanto, el primer bit del texto plano del mensaje cifrado llega a ser más fácil de predecir como la estructura de encabezados seguidos de la documentación estándar. Si el atacante puede determinar el tipo de paquete que es enviado, entonces puede delimitar drásticamente las posibilidades del contenido de texto plano del primer bit en el mensaje cifrado. El depender de factores tales como tamaño de paquete o cuanto dure la transmisión de paquetes, hace que la predicción de los tipos de paquetes se convierta en toda una posibilidad.

3.7 Ataque al RC4

En Julio de 2001, los criptógrafos Scott Fluhrer, Itsik Mantin y Adi Shamir publicaron un artículo [7] donde describían una vulnerabilidad en el algoritmo de cifrado RC4. En el documento se explica como puede recuperarse la clave empleada en la encriptación de la información, si la inicialización del algoritmo cumple determinadas premisas que resultan ser muy comunes, y si se intercepta el suficiente número de mensajes.

En el artículo se detallan dos ataques diferentes sobre RC4. El primero de ellos se basa en patrones invariantes. Es decir, existen patrones que de existir en la clave, se propagan también al estado interno del algoritmo, debilitándolo considerablemente. El segundo tipo de ataque describe la recuperación de la clave secreta, cuando la clave del algoritmo se deriva de la concatenación de dicha clave secreta y un vector inicial público y conocido.

- Con la primera vulnerabilidad, el resultado es que los primeros bytes generados por RC4 pueden resultar muy predecibles.
- La segunda vulnerabilidad permite recuperar la parte secreta de la clave RC4 recopilando un gran número de mensajes y vectores iniciales.

Existen, no obstante, algunas sugerencias hechas por la comunidad criptográfica internacional que permiten seguir utilizando RC4 de forma segura (al menos hasta que se descubran nuevos tipos de ataques). Dado que el problema del primer ataque reside en la predicción de los primeros bytes, una posibilidad es descartarlos. Es decir, no empezamos a utilizar la salida RC4 desde el primer byte, sino desde el byte "n". El número de bytes iniciales que desaprovechamos supone un compromiso entre la eficiencia de arranque del sistema, y la seguridad.

El segundo problema se puede solucionar simplemente evitando que el atacante obtenga segmentos largos de la clave RC4, que es lo que consigue con los vectores iniciales y la concatenación típica entre la clave secreta y dichos vectores iniciales. Una opción sería reemplazar el concatenado por una función hash, lamentablemente el uso de una función hash puede suponer una carga considerable en la inicialización RC4, ya que suelen ser funciones lentas, sobre todo si lo comparamos con la inicialización RC4 estándar.

En general, debido a la rapidez y eficiencia de RC4, resulta preferible descartar los primeros 256 bytes generados, que descartar 64 bytes para eliminar el primer problema y calcular un hash para eliminar el segundo. Si descartamos el suficiente número de bytes iniciales, estaremos protegidos contra los dos ataques. El problema es ¿cuántos bytes descartar?

El propio autor del algoritmo RC4, Ron Rivest, menciona lo siguiente:

"En protocolos como el WEP, es necesario generar diferentes claves RC4 para diferentes paquetes derivados de una clave común. Un método que se sugiere para obtener las claves es incluir o concatenar un contador a la clave base. El algoritmo de programación de claves del RC4 es reconocido por lo débil que resulta para este propósito, particularmente cuando los bytes iniciales del texto plano son fácilmente predecibles."

Por esto se recomienda que en lugar de que los usuarios consideren la opción de utilizar solamente un algoritmo de programación de claves, se opte por el preprocesamiento de la clave base y de cualquier contador o vector de inicialización (VI) a través de procesos como el MD5[10].

De manera alternativa, las debilidades que presenta el algoritmo de planeación de claves, pueden prevenirse al descartar los primeros 256 bytes de salida del generador pseudo aleatorio antes de que comience la encriptación. Uno o ambos métodos pueden ser suficientes para poder prevenir ataques en WEP y WEP2."

Así el autor nos confirma que basta con aplicar descarte de valores iniciales o una función hash para tratar de contrarrestar la debilidad mostrada por WEP y que por otra parte no es necesario que empleemos las dos posibilidades de manera simultanea. Como nota curiosa, RC4 se utiliza en el protocolo SSL, pero de forma segura, ya que se emplea hashing.

Veamos las implicaciones, a nivel de tiempo de ejecución, entre las diferentes opciones mencionadas: Las pruebas de rendimiento se hacen sobre un procesador UltraSparc a 143 Mhz, muy anticuado para los estándares actuales, pero que sirve de ejemplo:

	Tiempo de inicialización del algoritmo
Inicialización RC4 estándar	10 milisegundos
Hash MD5	70 microsegundos
Hash SHA-1	80 microsegundos
Descarte de 256 bytes	21 milisegundos

[10] MD5 (*Message-Digest Algorithm 5*, "Algoritmo de Resumen del Mensaje 5") es un algoritmo de reducción criptográfico de 128 bits.

3.8 Claves y autentificación del mensaje

El estándar 802.11 no especifica la manera en que la distribución de claves debe de realizarse. En su lugar confía en un mecanismo externo para distribuir de manera global un arreglo de 4 claves. Cada mensaje contiene un campo clave para el identificador que especifica el índice en el arreglo de la clave que se va a utilizar. El estándar también permite un arreglo que asocie una clave única a cada estación móvil; sin embargo, esta opción no se utiliza extensamente. En la práctica, la mayoría de las instalaciones utilizan una solo clave para una red entera.

Esta práctica afecta seriamente la seguridad del sistema, puesto que es un secreto que se comparte entre muchos usuarios, por lo que no puede permanecer completamente oculta. Algunos administradores de red intentan mejorar este problema, al no revelar la clave secreta a los usuarios, si no que ellos mismos se encargan de configurar cada una de las máquinas. Esto, sin embargo, es solo una mejora temporal ya que las claves se continúan almacenando en las máquinas del usuario.

3.8.1 Modificación de un Mensaje

Como ya se ha mencionado, los mensajes pueden ser modificados durante la transmisión sin que esto sea detectado, violando de esta manera la seguridad. La siguiente característica de la suma de comprobación de WEP nos muestra esta debilidad:

"La suma de comprobación de WEP es una función lineal del mensaje, esto significa que la suma de comprobación se distribuye sobre toda la operación de XOR (es decir, $c(x \oplus y) = (c(x) \oplus c(y))$ para todas las opciones de "x" y de "y", esta es una característica general de todas las sumas de comprobación del CRC."

Una consecuencia de la característica antes dicha es que llega a ser posible hacer modificaciones controladas a un texto cifrado sin la interrupción de la suma de comprobación. Fijemos nuestra atención en un texto cifrado C que ha sido interceptado antes de que alcanzara su destino:

$$A \rightarrow (B') : (v, C').$$

Asumimos que C corresponde a un cierto mensaje desconocido M, de modo que:

$$C = RC4(v,k) \oplus (M, c(M))$$

Mostramos ahora que es posible encontrar un nuevo texto cifrado C' que desencripta a M', donde $M' = M \oplus \Delta$ y Δ puede ser elegida de manera arbitraria por el atacante. Entonces, podremos sustituir la transmisión original por nuestro nuevo texto cifrado:

$$(A) \rightarrow B' : (v, C').$$

Y sobre el desciframiento, el B' obtendrá el mensaje modificado M' con la suma de comprobación correcta. Todo lo que resta es describir cómo obtener C de modo que C' desencripte a M' en lugar de M. Observemos que RC4, también es linear, así que podemos reordenar muchos términos, por lo que se sugiere el siguiente truco: Se aplica la operación XOR a $(\Delta, c(\Delta))$ por ambos lados de la primera ecuación que se mostró anteriormente para conseguir un nuevo texto cifrado C':

$$
\begin{aligned}
C' &= C \oplus (\Delta, c(\Delta)) \\
&= RC4(v,k) \oplus (M, c(M)) \oplus (\Delta, c(\Delta)) \\
&= RC4(v,k) \oplus (M \oplus \Delta, c(M) \oplus c(\Delta)) \\
&= RC4(v,k) \oplus (M', c(M \oplus \Delta)) \\
&= RC4(v,k) \oplus (M', c(M'))
\end{aligned}
$$

En esta derivación, utilizamos el hecho de que la suma de comprobación de WEP es linear, de modo que $c(M) \oplus c(\Delta) = C(M \oplus \Delta)$. Consecuentemente, mostramos cómo modificar C para obtener un nuevo texto cifrado C' que desencriptará a $P \oplus \Delta$. Esto implica que podemos hacer modificaciones arbitrarias a un mensaje cifrado sin que nos preocupe una posible detección. Así, la suma de comprobación de WEP no puede proteger la integridad de datos, una de las tres metas principales del protocolo de WEP.

Notemos que este ataque se puede aplicar sin el conocimiento completo de M: el atacante solamente necesita saber cual es el texto cifrado C' y la diferencia deseada del Texto Plano Δ, para calcular $C' = C \oplus (\Delta, c(\Delta))$ por ejemplo, mover el primer dígito binario de un mensaje, el atacante puede fijar a $\Delta = 1000\ldots 0$. Esto permite que un atacante modifique un paquete con el solo conocimiento parcial de su contenido.

3.8.2 Inyección y desciframiento de un mensaje

A continuación, mostramos que WEP no proporciona un control de acceso seguro. Para esto veremos ahora la siguiente característica de la suma de comprobación de WEP:

"La suma de comprobación de WEP es una función sin clave del mensaje, por consiguiente, el campo de la suma de comprobación puede también ser calcular por el atacante que conoce el mensaje."

Esta característica de la suma de comprobación de la integridad de WEP permite burlar las medidas de control de acceso. Si un atacante puede conseguir el encabezado de un Texto Plano entero que corresponde a un campo transmitido, podrá ser capaz de inyectar tráfico arbitrario en la red. El conocimiento del Texto Plano y del texto cifrado puede revelarnos la clave de cifrado, esta clave se puede reutilizar posteriormente para crear un nuevo paquete usando el mismo IV, es decir, si el atacante sabe cual es el Texto Plano "P" de cualquier paquete dado "C" del texto cifrado, puede recuperar el keystream usado para cifrar el paquete:

$$P \oplus C = P \oplus (P \oplus RC4(v,k))$$

Y puede ahora construir un mensaje cifrado M ':

$$(A) \rightarrow B' : (v, C').$$

Donde

$$C' = (M', c(M')) \oplus RC4(v,k))$$

Hay que observar que el mensaje “rebelde” utiliza el mismo valor del IV que el mensaje original. Por lo tanto, el ataque funciona debido al comportamiento del punto de acceso que utiliza WEP.

Un tipo de defensa natural contra este tipo de ataque, sería el evitar la reutilización de los IV’s en paquetes múltiples, y el hacer que todos los receptores cumplan con esta prohibición. Sin embargo, el estándar 802.11 no hace esto, solo lo recomienda, no requiere cambiarlo con cada paquete. Por lo tanto, cada receptor debe validar los IVs relanzados o arriesgarse con la no interoperabilidad, con el resto de los dispositivos.

Lo que puede sorprendernos es que la capacidad de modificar paquetes cifrados sin que sean detectados, es que también pueden ser desencriptados.

Consideremos WEP desde el punto de vista de un atacante. Puesto que WEP utiliza un flujo de cifrado que se presume seguro (RC4), atacar la criptografía directamente no nos dará ningún resultado. Pero si no podemos desencriptar el tráfico por nosotros mismos, todavía hay alguien que puede: El punto de acceso. En cualquier protocolo criptográfico, el desencriptador legítimo debe poseer siempre la clave secreta para desencriptar. La idea entonces, es engañar al punto de acceso para que desencripte un poco de texto cifrado para nosotros, esto es lo que se explicó anteriormente como ataque por filtración de mensajes y al RC4.

3.9 Red secuestrada

Hay numerosas técnicas disponibles para que un atacante "secuestre" una red inalámbrica, contando con varias herramientas disponible para ello. Muchas de las herramientas disponibles están bajo el ambiente UNIX y se puede encontrar en http://packetstormsecurity.com. Con estas herramientas, el hacker puede trampear fácilmente todas las máquinas en la red inalámbricas.

3.9.1 Panorama de un Caso de Secuestro

Ahora que hemos identificado la red que se atacará, y se ha obtenido una dirección MAC para ser un miembro válido de la red, es posible obtener más información que no se obtiene solo por husmear el tráfico de la red. Si la red que es atacada está utilizando el SSH[11] para proporcionar acceso a sus anfitriones, puede ser más fácil robar ahora una contraseña. Con SSH el anfitrión se podrá conectar como una máquina “rebelde”, así al conectarse de manera automática recibirá su contraseña.

Hay varias herramientas que se pueden utilizar para proteger una red contra el IP spoofing con las herramientas inválidas del ARP requests, tales como ArpWatch que notificará al administrador cuando se consideran las peticiones del ARP, permitiendo que el administrador tome acción apropiada para determinar si hay de hecho alguien que procura entrar de manera inapropiada a la red.

Otra opción es definir las MAC/IP de manera estática, esto evitará que el atacante pueda redefinir esta información. Sin embargo, debido a los gastos indirectos es difícil definir todos los adaptadores de la red

3.10 Cambio de dirección IP

Una vez que se cuenta con suficiente información de la red que se busca intervenir, se pueden realizar varios procedimientos ya sea para afectar a la red de manera directa o indirecta y que a su vez sea detectable o no, por su entorno. Un ejemplo de esto seria el cambio de dirección IP para utilizar una máquina de la red como puente de salida hacia otro tipo de red o a Internet. La primer modificación se conoce como "Cambio de dirección IP" y puede ser utilizada cuando el punto de acceso de WEP actúa como ruteador de IP con Internet; Hay que observar que esto es un acto bastante común porque WEP se utiliza típicamente para proporcionar acceso a la red a dispositivos móviles.

[11] SSH (Secure SHell) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo el ordenador mediante un intérprete de comandos.

La manera más fácil de modificar la dirección IP del destino es prediciendo cual es la dirección IP original del destinatario, y después aplicar la técnica de "modificación de mensaje" para cambiarla a la dirección deseada. El predecir la IP ADDRESS original del destino no es por lo general difícil; todo el tráfico entrante, por ejemplo, será destinado a una dirección IP en la subnet inalámbrica, que debe ser fácil de determinar. Una vez que se desencripte el tráfico entrante, los direccionamientos del IP de los otros extremos de las conexiones serán revelados, y el tráfico saliente se puede entonces desencriptar de manera semejante.

Para que este tipo de ataque funcione, necesitamos modificar no solamente el IP ADDRESS destino, si no que también debemos asegurarnos de que la suma de comprobación del IP en el paquete modificado sea todavía correcto ya que de otra manera el paquete desencriptado será descartado por el otro punto de acceso. Puesto que el paquete modificado se diferencia del paquete original solamente por su IP ADDRESS del destino y puesto que los viejos y nuevos valores para el IP ADDRESS del destino se saben, podemos calcular el cambio que es requerido para la suma de comprobación del IP causada por este cambio en el IP ADDRESS.

Por ejemplo si suponemos que las palabras de 16 bits de altas y bajas del IP ADDRESS original del destino son Dh y Dl y deseamos cambiarlas a D'h y D'l, si la vieja suma de comprobación del IP era X (que no necesariamente sabemos cual es, ya que se encuentra cifrado), el nuevo debe ser:

$$X' = X + D'_H + D'_L - D_H - D_L$$

El truco es que nosotros sabemos solamente como modificar un paquete aplicando un XOR y no necesariamente sabemos lo que debemos aplicar de la operación de XOR a X para conseguir X' aunque sabemos lo que necesitamos agregar (es decir, D'h + D'l - Dh - Dl).

Ahora discutiremos tres maneras para intentar corregir la suma de comprobación del IP del paquete modificado:

La suma de comprobación del IP para el paquete original se conoce:

Si resulta ser el caso en el que conocemos X, entonces simplemente calculamos X' como se mostró anteriormente, posterior a esto modificamos el paquete al aplicar la operación de XOR en $X \oplus X'$, que cambiará la suma de comprobación del IP al valor correcto de X'.

La suma de comprobación original del IP no se conoce:

Si no se conoce X, la tarea resulta ser un poco más difícil. Dado $\varepsilon = X' - X$, necesitamos calcular $\Delta = X' \oplus X$. De hecho, no existe la suficiente información para que calculemos Δ dado solamente ε. Por ejemplo, si ε = 0xCAFE, esta podría ser:

X' = 0xCAFE, X = 0X0000, Asi Δ = 0xCAFE
X' = 0xD00D, X = 0X050F, Asi Δ = 0xD502
X' = 0x1EE7, X = 0X53E8, Asi Δ = 0x4D0F
•••

Sin embargo, no todos los 2^{16} valores para Δ son posibles, y algunos son mucho más probables que otros. En el ejemplo mencionado, hay cuatro valores para Δ (0x3501, 0x4B01, 0x4D01, 0x5501) que ocurren más del 3% del tiempo cada uno. Además, estamos libres de hacer tentativas del múltiplo ya que cualquier conjetura incorrecta no será tomada en cuenta por el punto de acceso. Dependiendo del valor de ε, un número pequeño de tentativas puede tener éxito con un alto índice de probabilidad. Finalmente, un desciframiento acertado de un paquete se puede utilizar para unir el desciframiento de los otros paquetes.

Otra posibilidad es compensar el cambio en el campo de destino por otro cambio en otro campo, de tal manera que la suma de comprobación del paquete siga siendo igual. Cualquier campo de la cabecera que nosotros conozcamos y que no afecta el envío de paquetes es perfecto para esto, por ejemplo, el IP ADDRESS de la fuente. Si se asume que el IP ADDRESS de la fuente del paquete que se desencriptará también se conoce (podemos obtenerlo, por ejemplo, realizando un ataque en un paquete para desencriptarlo y usando este ataque contra los paquetes subsecuentes para que obtengamos la dirección de la primer fuente), restamos ε de la palabra de 16 bits de la dirección IP fuente y del paquete que resulta tendrá la misma suma de comprobación del IP que la original. Sin embargo, es posible que la modificación del direccionamiento de la fuente de esta manera, cause que un paquete sea descartado en base a reglas de filtración.

Un atacantes "inventivo" que vigila el acceso a una red de clase B pueden incluso realizar los ajustes necesarios en el campo de direccionamiento destino solamente, eligiendo D'l = Dh + Dl - D'h. Por ejemplo, si la dirección destino original de un paquete es 10.20.30.40 y el atacante mantiene un control sobre la subnet 192.168.0.0/16, seleccionar la dirección 192.168.103.147 da como resultado un valor idéntico de la suma de comprobación de la cabecera del IP, y el paquete será entregado a la dirección que el atacante controla.

3.11 Ataques de reacción

Hay otra manera de manipular el punto de acceso y de romper el cifrado WEP, que es aplicable siempre que WEP se utilice para proteger tráfico de TCP/IP. Este ataque no requiere conectividad al Internet, así que puede aplicarse incluso cuando los ataques por cambio de dirección de IP no son posibles. Sin embargo, es eficaz solamente contra tráfico del TCP; otros protocolos de IP no pueden ser desencriptados utilizando este tipo de ataque. En este tipo de ataque monitoreamos las respuestas del receptor de paquetes TCP y lo analizamos para deducir la información sobre el Texto Plano desconocido. Este ataque se basa en el hecho de que un paquete del TCP está validado solamente si la suma de comprobación del TCP es correcta, y cuando se valida, un paquete de ACK (acuse de recibo) se envía en respuesta. Los paquetes ACK pueden ser fácilmente identificados por su tipo, sin requerir de un desciframiento. Así, la reacción del receptor será divulgar si la suma de comprobación del TCP era válida cuando el paquete fue desencriptado. El ataque, entonces, procede como sigue:

Interceptamos un texto cifrado (v1, C) con el desciframiento desconocido P:

$$A \rightarrow (B) : (v, C')$$

Analizamos algunos bits en C y ajustamos el CRC cifrado para obtener un nuevo texto cifrado C' con la suma de comprobación válida de WEP. Transmitimos C' en un paquete al punto de acceso:

$$(A) \rightarrow B' : (v, C').$$

Finalmente, observamos si el receptor eventual envía de regreso un paquete TCP ACK; esto permitirá que veamos si el texto modificado pasa la suma de comprobación del TCP y es validado por el receptor.

Hay que observar que nosotros podemos elegir cuales bits de C vamos a modificar utilizando las técnicas analizadas anteriormente. La técnica de monitoreo que se utiliza principalmente es la siguiente: Al tomar una decisión correcta de los bits que se van a modificar, podemos asegurar que la suma de comprobación del TCP sigue siendo la correcta cuando se tiene la condición de los bits:

$$P_i \oplus P_{i+16} = 1$$

Así, la presencia o la ausencia de un paquete del ACK revelará bits de información en el Texto Plano desconocido de P. Repitiendo el ataque para las opciones de "i", podemos conocer casi todo el Texto Plano de P y entonces podremos deducir los bits restantes que aun son desconocidos. De esta manera hemos utilizado al receptor de la transmisión como medio desencriptador del texto cifrado que hemos interceptado. Esto se conoce como "Ataque de reacción", pues trabaja al vigilar la reacción del receptor a nuestras falsificaciones.

Se ha mantenido hasta este momento, los detalles técnicos sobre cómo elegir el nuevo paquete C' para engañar al receptor y así sea revelada la información del texto Plano P que es desconocido. Hay que recordar que la suma de comprobación del TCP es su complemento de 16 bits del mensaje de M, por lo que en general, la suma de comprobación del TCP en un Texto Plano P es válida solamente cuando $P = 0 \text{ Mod } 2^{16}-1$.

Dejamos ahora que $C' = C \oplus \Delta$, de modo que Δ especifica qué posiciones de los bits vamos a modificar. Elegiremos Δ de la siguiente manera: seleccionamos "i" de manera arbitraria, fijamos las posiciones de los bits "i" y "i"+16 de Δ a uno, y dejamos que Δ sea cero en cualquier otra posición. Es una característica conveniente del modulo $2^{16}-1$ que $P \oplus \Delta = P \text{ Mod } 2^{16}-1$ que se mantiene exactamente cuando $Pi \oplus Pi+16 = 1$. Puesto que asumimos que la suma de comprobación del TCP es válido para el paquete original (es decir, $P = 0 \text{ Mod } 2^{16}-1$), esto significa que la suma de comprobación del TCP será válido para el nuevo paquete (es decir, $P \oplus \Delta = 0 \text{ Mod } 2^{16}-1$) cuando $Pi \oplus Pi+16 = 1$. Esto nos da nuestro bit de información en el Texto Plano, como fue requerido.

3.12 Introducción de *Malware*

Muchas configuraciones inalámbricas almacenan la llave secreta de WEP en el sistema de ficheros o en entradas de la configuración, que no tomaría mucho tiempo para que un buen hacker pudiera obtenerlas.

Como ejemplo las tarjetas de Lucent ORiNOCO almacenan esta información dentro del Registro de Windows, y hay herramientas como la creada por Cquire.net[12] que pueden buscar y tomar dicha llave secreta.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-1ÇE-BFC1-8002BE10318}\0009 \.

Esta misma información se puede encontrar en el registro Win98 en HKEY_LOCAL_MACHINE\ System\CurrentControlSet\Services\Class\Net\0004\Config04, o cualquier dispositivo que tenga \ConfigXX\ Encryption\Net\XX \

A continuación se muestra un ejemplo sobre como funciona la herramienta de recuperación de Lucent para una llave que encontró en un registro de Windows.

```
D:\>lrc – d
Registro Encryption/Decryption De Lucent Orinoco
Versión 0.2b
Anders Ingeborn, iXsecurity 2001
La llave descifrada de WEP es: BADPW
```

Las máquinas de Windows no son las únicas susceptibles a este tipo de ataque. Muchas máquinas de Linux almacenan su llave secreta en cleartext dentro de un archivo generalmente legible. En muchas máquinas de Linux esta información puede estar en path/etc/pcmcia/wireless.opts.

[12] www.cqure.net/tools03.html

3.13 Ataques maliciosos

Una vez conectado a una WLAN y conociendo la información disponible sobre los parámetros de la red, un atacante puede negar el acceso a los usuarios legítimos o puede redirigir el tráfico cambiando la configuración en el AP. Los APs son configurados generalmente al conectarse a una computadora utilizando un cable USB, una conexión de Ethernet, o teniendo acceso web al servidor administrativo que funciona a su vez como AP para sí mismo (Este último método resulta ser el que conlleva un mayor riesgo para la red). La configuración del AP conectándose a una página Web resulta ser conveniente, pero sin las precauciones apropiadas, un hacker puede también acceder a la configuración.

Las consolas de configuración están instaladas generalmente con credenciales por default de autentificación y direcciones IP. Tal información se obtiene fácilmente descargando la documentación del distribuidor, este proceso se hace más fácil ya que el AP transmite su MAC ADDRESS dentro de los paquetes de "beacon". Un atacante puede identificar el hardware del vendedor al revisar las direcciones del MAC obtenido usando los scanners de WLAN y al verificar el identificador único de la organización (OUI) asignado por la IEEE.

Las herramientas tales como NetStumbler hacen una referencia a esta información automáticamente. Al tener acceso una vez a la consola de configuración, un atacante tiene libertad total para administrar el AP. Un atacante puede entonces negar un servicio cambiando el canal o el SSID usado por el WLAN. Dependiendo de las capacidades del hardware, el atacante puede volver a redirigir el tráfico. Un hacker podría instalar un *rogue* AP, permitiendo que los clientes inalámbricos se conecten con él, y después volver a redirigir el tráfico a otro destino. Un ataque del tipo "hombre-filtrado" por ejemplo, puede dirigir a los usuarios a un servidor falso instalado por el mismo atacante y ahí puede con toda tranquilidad obtener sus credenciales de autentificación, para utilizarse o distribuirse posteriormente.

3.14 Ataques para negar servicios

La WLAN es susceptible a los mismos ataques basados en los protocolos de las LANs cableadas, pero para perpetrar tales ataques contra una WLAN, un individuo primero necesitaría conectarse con la red. La WLAN también es susceptible a una forma única de ataque llamado "negación-de-servicio" (DOS). La WLAN envía información vía ondas de radio en frecuencias públicas, así que son susceptibles a interferencia inadvertida o deliberada utilizando la misma banda de radio. Para demostrar esta vulnerabilidad, solo hay que colocar una computadora portátil con un NIC 802.11b o g cerca de un microondas con la puerta abierta, como ambos dispositivos utilizan generalmente la frecuencia de 2.4 GHz, la degradación de la señal en la red 802.11b o g ocurrirá mientras el microondas se encuentre en operación. Así un atacante puede utilizar el mismo principio para inhabilitar o degradar una red 802.11b difundiendo tráfico en la misma frecuencia que la red.

Capítulo 4

Corrigiendo WEP

Capítulo 4: Corrigiendo WEP

4.0 Introducción

Existen opciones de configuración disponibles para un administrador de red que pueden reducir la posibilidad de un ataque como los descritos en el capítulo anterior. La mejor alternativa es colocar la red inalámbrica fuera del firewall. En lugar de que intentemos asegurar la infraestructura de la red inalámbrica, así es más simple que la consideremos solo como una amenaza externa ya que los clientes típicos de una red inalámbrica son las computadoras portátiles que son móviles por naturaleza, y que emplearán con frecuencia una red virtual privada (VPN) para tener acceso a las computadoras dentro del firewall. Requerir que el mismo VPN se esté utilizado para tener acceso a la red interna cuando se conecta sobre el protocolo 802.11 evitando así la necesidad de la conexión sobre la capa de seguridad, y reutilizamos un mecanismo bien conocido. Para proporcionar un control de acceso, la red puede ser configurada de tal manera que ninguna de las rutas a Internet sean de la red inalámbrica. Esto evita que la gente que se encuentre dentro del rango de radio de la infraestructura inalámbrica utilice el ancho de banda para una conexión a Internet y se requiera el uso de VPN para cualquier acceso exterior.

4.1 Analizando la amenaza

El análisis de la amenaza se basa en la ciencia de asignar un valor arbitrario o potencial del daño, tomando el coste de las actividades de restauración del proceso y que compara ese coste con la inversión de seguridad y las contramedidas para prevenir el daño. Este es un proceso difícil y arduo, pero inestimable y absolutamente necesario si se va a mantener un negocio que dure la edad de la información que se busca proteger.

Primero se necesita cuantificar la amenaza en lo referente a riesgo. Para realizar esto, se hacen dos preguntas:

- ¿Cuáles son mis vulnerabilidades?
- ¿Cuál podría ser el costo potencial de la recuperación de una situación donde se ha perpetrado un ataque con consecuencias?

Estas dos preguntas determinarán en última instancia la conducta final para asegurar una WLAN.

4.2 ¿La amenaza iguala el riesgo más la vulnerabilidad?

Definamos algunos términos para permitir que se consiga una comprensión de la amenaza, riesgo, y vulnerabilidad.

- La amenaza implica una fuerza con una dirección.
- El riesgo se define en un cierto plazo.
- La vulnerabilidad depende de las medidas que se han tomado o se han omitido para prevenir un ataque futuro.
- La vulnerabilidad identifica una debilidad en la puesta en práctica o el software o el hardware que permite el acceso a los recursos no autorizados.
- Así pues, se debe aplicar algunas pautas generales para analizar posibles amenazas y entonces planificar necesidades específicas.

Aquí está una lista de algunos puntos que podríamos utilizar como referencia para el análisis de posibles amenazas:

- Identificación del método de acceso a objetos de valor desde una perspectiva autorizada.
- Identificar la probabilidad de que alguien (con excepción de un usuario autorizado) pueda tener acceso a los objetos de valor identificados.
- Identificar los daños potenciales.
- Modificación.
- Hurto y/o destrucción de datos.
- Identificar las contramedidas de la seguridad.
- Identificar el costo en la puesta en práctica de las contramedidas de seguridad.
- Hardware y Software
- Personal y Procedimientos
- Limitaciones en el acceso a través de la estructura corporativa
- Comparar los costes de asegurar el recurso contra el coste de control de daños

En todos los casos, algunas reglas universales se aplican, por ejemplo, determinar quién tiene acceso y quién puede desear conseguir el acceso desautorizado a la información, el paso siguiente es evaluar los tipos de amenazas y del daño potencial causado por una vulnerabilidad explotada.

También hay que tener presente que los costos no son siempre uniformes o monetarios, podría también estar la pérdida de empleados valiosos que se sienten enajenados o molestos por la política que han fijado en su lugar de trabajo.

A continuación se muestra una lista de los puntos de seguridad de una WLAN las cuáles pueden resultar benéficas si se mantienen activas o en continua revisión.

4.2.1 Autentificación Débil

No se deben de utilizar claves de red y password que puedan ser fácilmente deducidas y que además no mezclen el alfabeto con números al igual que el manejo de letras mayúsculas y minúsculas. Entre más complejo sea un password, más tardara un atacante en obtenerlo o descifrarlo.

4.2.2 Diseño e implementación de una red segura

La opción del producto y distribuidor, combinados con el diseño y despliegue de una red, contribuirán perceptiblemente en la determinación del grado de vulnerabilidad que tenga la red.

- ¿Qué debo buscar en un punto de acceso?
- ¿Quién ofrece estos puntos de acceso?

Primero: el AP que se está buscando debe caber en el análisis de la amenaza estructural que acabamos de crear. Debe también resolver algunos requisitos mínimos tales como inhabilitar la difusión del SSID, cifrado de 128-bit WEP, compatibilidad WiFi, y la capacidad de pasar tráfico de VPN.

El paso siguiente es identificar la arquitectura del WLAN. Nuevamente nos preguntamos:

- ¿Quién necesita el acceso?
- En cada localización, ¿cuántos usuarios requieren el acceso?
- Hay otros dispositivos WiFi en la vecindad que podría causar interferencia con la WLAN?

Estas preguntas se relacionan con la disposición física de la red. Las WLANs dependen su seguridad en gran medida por la disposición física. Por ejemplo, no se colocaría una antena direccional en la ventana del edificio ya que esto permitiría que cualquier persona dentro de una distancia dada, la capacidad de recibir la señal del WLAN. Asimismo, parte de la política de seguridad requiere poner datos a disposición de los que la necesiten. No proporcionar la suficiente cobertura puede convertirse en un dolor de cabeza

4.2.3 Alcance de la red inalámbrica

La opción del vendedor para su instalación inalámbrica puede alterar dramáticamente la huella visible de la red inalámbrica. Después de que un punto de acceso esté instalado, comenzará a emitir señales anunciando, su identificador determinado del servicio (SSID). Esta es una función muy útil para que los clientes puedan conectarse con la red. La facilidad del contacto, sin embargo, tiene ciertas implicaciones de seguridad ya que anuncia a amigos o enemigos las características y alcances básicos de la red.

4.2.4 Fuerza de la señal

Desde un punto de vista de la supervisión, la fuerza de la señal es uno de los factores más críticos para considerar. Primero, es importante supervisar su señal regularmente para saber cual es el grado en el cual está disponible. Múltiples APs requerirá investigaciones múltiples para generar un cuadro completo de un sitio.

4.2.5 Detección de una negación del servicio

La supervisión de la red inalámbrica para la negación potencial de ataques debe ser parte del régimen de seguridad. Examinando la red, generando disminución o atenuación de señal, revisando el registro de APs y de las direcciones MAC desconocidas, son maneras proactivas sobre la negación del servicio.

4.2.6 Poner WEP en ejecución

A pesar de sus críticos, WEP todavía ofrece un nivel razonable de la seguridad y como se había mencionado anteriormente, es mejor tener una barrera que pueda o bien detener a los atacantes casuales o mal preparados o el hacer una tarea mas lenta y cansada a los atacantes mas preparados que en su momento los desmotivara para que no realicen un ataque a la red. Es por eso que es importante definir WEP como el estándar de cifrado de la comunicación entre los componentes de la WLAN.

4.3 El proceso de la autentificación de WEP

La autentificación dominante compartida es un proceso de cuatro pasos:

1. El solicitante (el cliente) envía un pedido de asociación.

2. El autenticador (el AP) recibe la petición, y responde produciendo un texto al azar y transmitiéndolo de nuevo al solicitante.

3. El solicitante recibe la transmisión, cifra el paquete con el flujo dominante compartido.

4. El autenticador descifra el texto y compara los valores contra el original. Si emparejan, autentican al solicitante.

4.4 Filtración de MACs

La filtración del MAC es una de las maneras más simples de reducir al mínimo la amenaza de un número de ataques, y aunque es más práctico en redes más pequeñas, sigue siendo una opción viable para redes inalámbricas más grandes. En ambos casos, es extremadamente simple poner en ejecución y el mecanismo mejora la seguridad de la red

4.4.1 Definir el filtrado de MACs

¿Qué significa filtrar los MACs? ¿Que es un MAC? Sin entrar en los detalles del OSI REFERENCE MODEL, un MAC ADDRESS es el número de identificación único de un hardware que tiene una longitud hexadecimal de 48 bits. Este número único identifica a un cliente del resto de la red local y porque es único, se puede tomar su dirección del hardware para identificar su acceso a la red. Para esto se pueden instalar los filtros que previenen los intrusos de la red.

Las ventajas de las direcciones de filtración del MAC bajo el control de acceso son las siguientes:

- Aceptan a los usuarios predefinidos.
- Los MACs filtrados no consiguen el acceso.
- Proporciona un buen primer nivel de defensa.

La desventaja principal de usar los filtros del MAC es el overhead o labor administrativo que depende del número real de nodos inalámbricos que buscan tener acceso a la red.

4.5 Protocolos de filtración

Como la filtración del MAC, los protocolos de filtración son otra manera de reducir los riesgos. Se ponen en ejecución en la forma de reglas de un firewall que sigue un patrón que pueden negar o dar permisos de tráfico basados en la identificación del puerto o como el Simple Mail Transfer Protocol (smtp)[1].

La filtración de protocolos es un método relativamente eficaz de restringir a usuarios de WLAN de procurar el SNMP para tener acceso a los dispositivos inalámbricos y que puedan alterar configuraciones.

Otra buena política con respecto al protocolo que se filtra en el WLAN está previniendo del Internet Control Message Protocol (ICMP). La filtración del MAC ocurre en la capa 2 del modelo de referencia OSI, el resto de los protocolo de filtración se encuentran en las capas 3 y 4, dependiendo de que protocolos se va a utilizar. Algunas de las desventajas de la filtración del protocolo incluyen la restricción involuntaria de usuarios válidos.

4.6 VPNs

El uso de redes privadas virtuales ha aumentado en los últimos años ya que con una correcta configuración, las VPNs aumentan la seguridad en redes inalámbricas, proporcionando las ventajas de la autentificación y quizás eliminando el riesgo que presentó WEP con el uso de llaves compartidas. VPN esencialmente cifra transmisiones de tal manera que solo se ve un remitente, un receptor, y ninguna inteligencia intermedia que pueda descifrar el contenido de la transmisión.

[1] El SMTP o protocolo simple de transferencia de correo electrónico se basa en el intercambio de mensajes de correo electrónico entre computadoras y/o otros dispositivos como PDA's, Celulares, etc.

En el protocolo de túnel Punto-a-Punto, el VPN se realiza de la siguiente manera:

El tráfico se envía bajo el protocolo de "*stack*" (apilado) en un IP de manera normal. La dirección destino se pone como de costumbre en la cabecera del IP. Una vez que se pasa a la capa de trasmisión de datos, entonces el paquete con la cabecera se le agrega otra cabecera de IP, que se forma con la dirección destino del servidor de VPN. Entonces se pasa al apilado otra vez y se envía de manera normal. El VPN recibe el paquete, retira las cabeceras dejando solo el paquete original, así el paquete es inservible para otro destinatario que no sea el VPN servidor.

Hay muchas situaciones donde éste procedimiento puede ser implementado, como por ejemplo en un servidor de VPN para una red corporativa, ya que proporciona el requisito de la autentificación que permite el acceso seguro a la red corporativa. En otro caso, el servidor de VPN puede proporcionar los servicios necesarios para hacer un túnel de datos y distribuirlos a los destinos apropiados, mientras que un servidor RADIUS proporciona el acceso remoto de autentificación.

En un tercer panorama, el servidor de VPN se proporciona localmente vía el AP. Algunos APs pueden ser configurados como servidores de VPN y el tráfico del cliente al AP es así protegido bajo un mismo modelo de cifrado, pero con una ventaja importante: Es el AP el que proporciona la autentificación, y por lo tanto la comunicación entera se cifra vía mecanismos de autentificación de VPN.

4.6.1 Ventajas de una VPN

Las ventajas de los servicios de VPN son limitadas, pero el valor asociado detrás de esas ventajas no se pueden expresar sin una comprensión del riesgo que se asocia a la pérdida de datos críticos.

- El uso de VPNs proporciona un cifrado de llaves múltiples que cambia cada hora o a intervalos definidos. Esto previene que cualquier persona fuera de la VPN pueda tomar y usar una llave de manera indefinida.
- No se limita a usuarios individuales ya que permite que se conecten áreas de corporativos y sucursales sobre Internet. Si la oficina tiene una cuenta del *DSL*, es mucho más barata y se cuenta con más ancho de banda que una conexión del *ISDN*.

4.6.2 Desventajas de VPN

Generalmente las VPNs pueden ser complejas, difíciles de instalar y difíciles de administrar. Las ventajas de las redes del cliente y del servidor de VPN pueden evaporarse rápidamente si los gastos indirectos no se calculan y los planes de contingencia no se hacen adecuadamente. Además, como con cualquier política de la seguridad, agregan responsabilidades al administrador.

4.6.3 Estableciendo la protección usando un VPN

La Figura 4.1 representa un VPN de una perspectiva cableada e inalámbrica.

El dispositivo inalámbrico de un cliente de VPN puede utilizar su conexión inalámbrica a VPN con el AP al conjunto de VPN en el conjunto de DMZ. Este VPN determina el túnel de VPN mientras que el servidor de RAS proporciona la autentificación. Finalmente, el tráfico autenticado pasara a través del firewall para tener una capa final de seguridad antes de transmitirse al sitio remoto protegido de la LAN.

Al mirar este diagrama, se ve inmediatamente el número de capas de seguridad que se deben de tener para poder presumir de un lugar seguro.

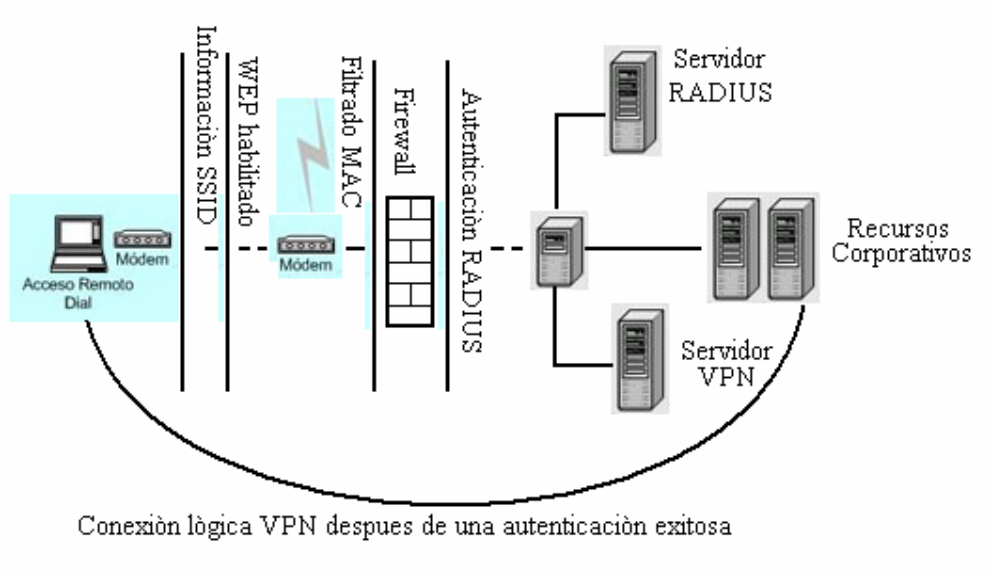


Figura 4.1 Conexión de una VPN.

Ahora por otra parte, aquí se notará la necesidad del cliente de tener la información apropiada del SSID. Si no, el AP no aceptará una conexión. Después, se verá si la llave WEP no empareja, de ser así, el AP no concederá una conexión. Incluso si esa información está correcta, pero el MAC no se reconoce, el AP no concederá el acceso. Si toda esa información está correcta en el cliente, pero el IP ADDRESS no se obtiene en la categoría correcta, o si el protocolo en uso no se permite, el firewall bloqueará el tráfico. Además, cuando inicialmente la información que se provee, si el username de la autentificación y la contraseña no emparejan con una cuenta legítima en el servidor del RADIUS, el acceso no se concederá.

4.7 Filtración de puertos

La filtración de puertos es como el acceso de filtración basado en direcciones del IP a diferencia que en lugar de conceder acceso a todos los servicios que se ofrecen, el filtro especificará una gama de puertos permitidos en una dirección IP específica. Esto puede ser muy útil en la limitación de los tipos de tráfico que se pueden transportar en el WLAN. Por ejemplo, Se puede determinar que solamente el puerto 22 de las transmisiones del TCP sea autorizado y que se bloqueen todas las comunicaciones del puerto 23 (telnet).

Una consideración de diseño, sería agregar un proxy server[2] en la red, que administraría un puerto en especial y todo el tráfico relacionado al HTTP tendría que pasar por el permitiendo un filtrado mas especifico.

4.8 Asegurando a los usuarios

No hay programa de seguridad completo sin la participación de los usuarios. Este punto es especialmente importante en una red inalámbrica, debido a las limitaciones en el modelo de seguridad. Algunas medidas apropiadas para asegurar al usuario son:

- Educar a los usuarios sobre las amenazas y riesgo de uso.
- Crear las cuentas y las políticas adecuadas de seguridad.
- Evaluar la política contra actividad requerida del usuario para prevenir relaciones adversas.

[2] El Proxy Server, es un servidor que intercepta las conexiones de red que un cliente hace a un servidor de destino.

Otros puntos para tomar en cuenta son:

- Ningún punto de acceso externo, donde nadie deben traer su propia terminal.
- Tener un Inventario de todas las tarjetas inalámbricas y sus direcciones MAC correspondientes.
- Ningunas antenas sin consentimiento administrativo.
- Contraseñas fuertes en los dispositivos inalámbricas de la red.
- Límites inalámbricos de la red, así como su supervisión para saber si se están excediendo.
- Monitoreo de la fuerza de la señal para contener a la red.
- Software de detección de intrusos cerciorándonos de que este sea configurable y actualizable.
- Utilizar las herramientas como NetStumbler para medir la fuerza de la señal 802.11.x.
- Utilizar los resultados para saber dónde mejorar las defensas.
- Aumentar la supervisión de los puntos potenciales de riesgo

4.9 Supervisión para el buen funcionamiento de la red

Vigilar el funcionamiento de su red es siempre una buena idea. Sabiendo su uso, los tipos de tráfico que viajan en la red, tan bien como los patrones de tráfico impares que pudieron ocurrir, ayudarán no solamente para mantener la capacidad del sistema, si no para detectar posibles intrusiones.

Supervisar la red nos dará una buena idea de su capacidad actual, ya que por ejemplo, la red puede tener su máximo uso por la mañana con una carga del 45 %, y si durante la supervisión de su funcionamiento el registro nos avisa de picos de uso con un ancho de banda mayor de lo normal, es una señal de una posible anomalía que debe ser investigada. Además, si al checar la red, se encuentra un consumo de ancho de banda inusual y se tiene solamente cuatro o cinco usuarios con un uso mínimo, esto se debe de tomar como una bandera roja ya que el motivo común de un ataque es que los intrusos busquen acceder al ancho de banda.

4.9.1 Herramientas para la supervisión

Hay muchas herramientas de supervisión, con precios y niveles de supervisión muy variados. Paquetes de software como el OpenView[3] de HP tienen gran demanda en el mercado. OpenView se puede configurar para supervisar cualquier aspecto de la red, servidores, ancho de banda, e incluso del tráfico. Sin embargo es un paquete poco amigable ya que requiere el uso del User Datagram Protocol (UDP), que es algo que no siempre trabaja con los firewalls debido al hecho de que sea un protocolo sin conexión y esto no permiten que los firewalls verifiquen que todas las transmisiones sean solicitadas, es decir no hay un "Handshake" en la conexión como con el protocolo de control de transporte (TCP).

Ejecutar OpenView puede ser un verdadero desafío y puede requerir algunos sacrificios en la seguridad. Por otra parte si se está buscando algo con precio bajo y que además sea más fácil de instalar, EtherApe[4] para LINUX es una buena opción. Este software es gratuito y proporciona una interfaz gráfica muy buena mostrando el ancho de banda consumido y donde se realiza un mayor consumo. Si se notan grandes retardos en la red y se quiere ver rápidamente qué o quien consume los recursos, EtherApe permite monitorear la red e identificar el tráfico, protocolos, y carga de la red. Además, verifica el tráfico de la fuente y el destino, proporcionando un cuadro visual de la red.

[3] http://h20229.www2.hp.com/
[4] http://etherape.sourceforge.net/

4.10 WPA

WPA (WiFi Protected Access o acceso protegido WiFi) es la respuesta de la asociación de empresas WiFi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

Cuando apareció WPA, el planteamiento inicial era permitir que el mayor número de tarjetas antiguas pudieran beneficiarse de sus virtudes. Su paso hacia WPA se lograría mediante la actualización en el firmaware y los controladores de las tarjetas. Esto fue crucial a la hora de escoger el nuevo mecanismo de cifrado, puesto que, aunque la opción más acertada era emplear AES, se opto por el TKIP[5], otro mecanismo más seguro que WEP, pero que utiliza las mismas operaciones elementales. De esta manera, el hardware capaz de cifrar con WEP podría trabajar con TKIP.

Por otra parte WPA se encarga de autenticar a los clientes de una forma segura. Su funcionamiento es ligeramente complejo, puesto que intervienen varios elementos, entre ellos un servidor RADIUS. Este se encarga de autentificar la entrada de un nuevo cliente a la red. La idea es que este servidor contenga la información de todos ellos y que, si hay algún cambio, solo sea preciso modificar los datos aquí, olvidándonos del punto de acceso para las tareas administrativas. La renovación de las claves se hace de manera automática, por lo que prácticamente solo nos tendremos que ocupar de dar de alta a los nuevos usuarios y eliminar a los antiguos.

Sin embargo, como no todo el mundo necesitara un servidor adicional RADIUS para navegar por Internet, existe la posibilidad de utilizar WPA SPK (Pre Shared Keys, claves pre-compartidas). Aunque WPA pierde gran parte de sus ventajas de gestión sin RADIUS.

4.10.1 Características de WPA

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

WPA incluye las siguientes tecnologías:

- **IEEE 802.1X**. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un *switch*, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP 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. 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 [8], 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). Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN).
- **TKIP**. Es el protocolo encargado de la generación de la clave para cada trama.
- **MIC** (Message Integrity Code). Código que verifica la integridad de los datos de las tramas.

[5] TKIP (*Temporal Key Integrity Protocol*), Protocolo de Integridad de Clave Temporal que cambia claves dinámicamente a medida que el sistema es utilizado.

4.10.2 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^{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, se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC[6].

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.

4.10.3 Modos de funcionamiento de WPA

WPA puede funcionar en dos modos:

- Con servidor AAA, RADIUS normalmente. Este es el modo indicado para las empresas. 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.

4.10.4 WPA SPK

Los que no quieran complicarse la existencia con FreeRADIUS[7] y tenga un número pequeño de usuarios pueden recurrir a un método de autenticación mas simple. El problema es que WPA SPK no esta disponible como opción de autenticación por defecto, por lo que tendremos nosotros que instalar previamente la actualización de Microsoft para su sistema operativo. Si contamos con una tarjeta de red reciente, probablemente ya soporte WPA SPK, sin embargo conviene instalar el firmware mas reciente disponible en el portal del fabricante. Una vez que se descargo e instala el "parche" y el firmware, solo queda dirigirnos a la pantalla de configuración de redes inalámbricas de XP de Microsoft (el fabricante puede tener su propia pantalla de configuración pero se recomienda el de XP para el WPA SPK). A continuación seleccionaremos el SSID adecuado en redes disponibles y elegiremos "configurar". En autenticación de red escogemos WPA SPK, y en cifrado, aquel que soporte nuestro punto de acceso (como por ejemplo AES). En "Clave de red" y "Confirme clave de red" introduciremos la contraseña que emplearemos. Tras aplicar esto, abriremos en un equipo conectado al punto de acceso mediante cable un navegador a la ventana de configuración del dispositivo. Finalmente, solo resta seleccionar el tipo de autenticación y el mecanismo de cifrado, que han de coincidir en ambas partes. De vuelta en el cliente, este debería conectarse a la red sin problemas y beneficiándose de AES.

[6] MIC (Message Integrity Code, "Código de integridad de los mensajes")
[7] http://www.freeradius.org/

4.11 WPA2 (IEEE 802.11i)

802.11i es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Se espera que esté concluido todo el proceso de estandarización para finales del 2006. WiFi está haciendo una implementación completa del estándar en la especificación WPA2.

Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.

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 proceso 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.

Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

4.12 Resumen de la prevención y reacción a incidentes

Si se tiene ya una política de reacción a incidente, hay que mantenerla actualizada para reflejar nuevos incidentes potenciales. La amenaza de un ataque por más remota que se perciba, es verdadera, por lo que hay que estar preparados. A continuación se muestra un breve resumen de lo visto en el capítulo haciendo énfasis en los puntos a tener en cuenta para que se cuente con una red lo más segura posible:

NO CONFIAR EN WEP PARA EL ENCRIPTADO: Es un hecho que WEP es inseguro, esto no es una revelación sino una realidad. No fue diseñada para proporcionarle a la terminal una solución, solo un nivel de seguridad y privacidad equivalente al de las LANs por lo que no hay que ver a WEP como solución de seguridad. Por lo que se recomienda utilizar WEP en combinación con otros estándares de encriptación.

SEGREGAR LAS REDES INALAMBRICAS: Las WLANs presentan diferentes riesgos de seguridad como las LANs cableadas, por lo que es mejor no tener una tráfico directo entre ambas plataformas, al no existir un ambiente completamente seguro, lo que se recomienda es la instalación de "firewalls" entre las LANs y las WLANs y que se habilite la autenticación entre el tráfico de las dos topologías.

NO UTILIZAR UN NOMBRE DESCRIPTIVO PARA SSID O ACCESS POINT: La creación de nombres descriptivos, tales como el nombre de la compañía, hace el trabajo de un hacker mucho más fácil porque identificar la fuente de la señal se convierte en un ejercicio trivial. Así si investigamos una compañía por medio de su Web site podemos obtener su dirección y podemos entonces verificar si su AP maneja el mismo nombre, de ser así solo se tendría que verificar si utiliza o no WEP y el resto del trabajo ya estará prácticamente hecho.

DIRECCIONES MAC "HARD CODE" QUE PUEDA UTILIZAR EL AP: Muchos fabricantes de APs proporcionan la capacidad de identificar las direcciones del MAC de las tarjetas de red para el AP. Un inventario de tarjetas autorizadas se debe mantener, este esfuerzo proporciona una ventaja razonable con respecto a la seguridad. Mientras que un hacker podría todavía identificar el APs y "husmear" el tráfico, ellos no podrían conectarse si los anfitriones se encuentran enlazados a la red ya que no contarían con un MAC ADDRESS legítimo.

CAMBIAR CONSTANTEMENTE LAS CLAVES DE ENCRIPTADO: Cambiar las claves de encriptado periódicamente no asegura por completo el nivel de seguridad de WEP, ya que un atacante puede romper una clave en un par de horas por lo que prácticamente tendríamos que cambiar de clave cada hora, aun así cambiar las claves de encriptado periódicamente nos previene de un ataque indefinido ya que si bien un atacante ya podría haber obtenido la clave WEP en una ocasión, el cambiar esa clave significa que el atacante tendrá que realizar nuevamente el proceso de Crackeo de clave para poder infiltrarse a la red nuevamente y si ese cambio se realiza de manera periódica esto hará más difícil la intromisión a nuestra red. Ahora desafortunadamente, esto puede tomarnos mucho o poco tiempo dependiendo del número de máquinas que conformen nuestra red, ya que el cambio de claves requiere de una actualización de manera manual. Poner esta recomendación en ejecución depende de encontrar un equilibrio entre la seguridad y la conveniencia.

INHABILITAR LOS PAQUETES DE BEACON: Algunos APs proporcionan la opción para evitar que el AP anuncie su presencia con paquetes periódicos de beacon. Estos APs requieren que las tarjetas de red inalámbricas utilicen el mismo SSID antes de que él responda al tráfico, esta característica evita que los hackers utilicen alguna de las herramientas de scanneo de WLAN.

COLOCAR EL APS DE MANERA CENTRALIZADA: Es un factor importante determinar la gama de difusión de un AP, pero hay que asegurarse que la señale alcance todas las áreas necesarias dentro del edificio, y no se difunda en otras innecesarias.

CAMBIAR LAS DIRECCIONES DE PASSWORDS/IP QUE SE TIENEN POR DEFAULT: La mayoría de los APs tienen un web server que se utiliza como consola de administración. Mientras que esto resulta muy conveniente, también puede permitir a un atacante tener acceso a la consola de administración del AP si logra abrir un navegador de web y colocándose un IP ADDRESS asignado al AP. Cambiar el IP ADDRESS y las "credenciales" de autentificación para el AP es tan simple como descargar la documentación de ayuda del Web site del desarrollador. Herramientas de escaneo de WLAN, como el NetStumbler, puede identificar al desarrollador del hardware comparando las MAC ADDRESS de transmisión en los listados publicados por el IEEE. Si un atacante puede tener acceso a la consola de administración del AP y la contraseña que utiliza es la que se da por default, el atacante podría entonces inhabilitar cualquier ajuste de seguridad o que se niegue cualquier servicio de ajuste tales como el canal o SSID. Esto evitaría que los clientes inalámbricos utilizaran el punto de acceso.

EVITAR CLAVES WEP DEBILES: Los desarrolladores están comenzando a proporcionar actualizaciones de firmware para los productos 802.11x que evitan el uso de VIs que den lugar a supuestos paquetes interesantes (por ejemplo claves débiles) para las herramientas como AirSnort. Este desarrollo será eficaz solamente si todos los productos inalámbricos son actualizados.

NO UTILIZAR DHCP EN WLANS: Un hacker necesita obtener un IP ADDRESS válido, el subnet mask del WLAN, identificar direcciones válidas del IP en una red y esto no requiere un esfuerzo significativo, pero ¿porqué hacer el trabajo de un hacker sea más fácil de lo necesario? Sin DHCP, identificar una dirección IP requiere de un monitoreo pasivo del tráfico y la revisión de los paquetes capturados. Un hacker podría también utilizar fuerza bruta, como el número de direcciones privadas ya que la gama resulta ser limitada. En concreto, un hacker podría identificar direcciones y máscaras válidas del subnet si DHCP está habilitado o no, pero las direcciones de IP estáticas son una más disuasiva y esto puede hacer que un hacker vaya a la siguiente red que sea menos segura.

IDENTIFICAR LOS ROGUE ACCESS POINT: En grandes compañías, los usuarios pueden causar gran preocupación ya que pueden instalar su propio hardware o software. Así como un empleado puede instalar un módem para tener acceso desde su casa, también puede agregar una red inalámbrica para entrar a la red según su conveniencia. El bajo costo del hardware y la relativa facilidad de instalación hace de esto una preocupación para los administradores de la red. La única manera de identificar los puntos de acceso "rebeldes" es buscándolos, de esta manera ahora nosotros realizaremos las labores de un hacker utilizando nuestra computadora portátil, una NIC inalámbrica y un scanner de WLAN para comenzar la "cacería".

Capítulo 5
Caso de estudio

Capítulo 5: Caso de estudio

5.0 Introducción

Con lo que se ha expuesto en los capítulos anteriores, hemos visto que obtener claves WEP resulta un trabajo trivial que lo más que nos puede exigir es tiempo de captura de vectores débiles, pero ahora se vuelve a mencionar que el objetivo de este trabajo no es dar herramientas de "crackeo" al intruso ocasional, si no crear una metodología que permita al encargado de una red, detectar los problemas de seguridad existentes y de igual manera brindarle procedimientos para proteger o hacer menos vulnerable a su red.

La metodología que nosotros exponemos consta de tres puntos básicamente.

- Detección de la red inalámbrica.
- Captura de información.
- Análisis de la información para obtener datos significativos de la red, así como la clave WEP en caso de que la red se encuentre protegida por el protocolo de encriptación.

A continuación comenzaremos a explicar cada uno de los puntos, así como el software que nos auxilio en este proceso, este por lo general se procuro que fuera software de libre acceso (gratuito) para que no se tuviera que adquirir o pagar regalías a los creadores, además de los que se realizaron por nuestra parte.

5.1 Detección de redes inalámbricas

Esta parte del trabajo puede que sea la más sencilla o una de las más engorrosas ya que se podría suponer en un inicio que conocemos o la ubicación de la red o el área que se requiere inspeccionar, pero si no es así, se tendrá que investigar la localización de los lugares donde se requiere hacer la búsqueda y si esta resulta ser un área grande, pues nos tomará tiempo el poder delimitar exactamente el lugar donde comenzaremos a trabajar.

Para nuestro trabajo se comenzó a utilizar el paquete de NetStumbler[1], el inconveniente que se encontró en este paquete es que se debe de instalar en equipos tipo LapTop que si bien son portátiles, pueden resultar sospechosas o estorbosas. Si uno quiere inspeccionar su red esto no será un problema ya que no tendrá la presión de que sea descubierto mientras inspecciona el área para detectar señales de redes inalámbricas, pero si además se busca verificar el grado de seguridad que se encuentre alrededor de nuestra área de trabajo, convienen equipos de menor tamaño que llamen menos la atención. Nosotros utilizamos el software WiFiFoFum[2], el cual es un explorador de radio frecuencias 802.11 para dispositivos con PocketPC 2003. Sus características permiten explorar y visualizar en pantalla, emulando un radar convencional (ver figura 5.1), todos los puntos de acceso WiFi disponibles en la zona de cobertura del dispositivo inalámbrico.

Si el dispositivo portátil como la PocketPc dispone de un módulo GPS, se puede visualizar la posición de los satélites en cobertura para conocer la posición casi exacta de la red inalámbrica al proporcionarse las coordenadas en latitud y longitud de la misma.

[1] http:// www.netstumbler.com/downloads/netstumblerinstaller_0_4_0.exe
[2] http://wififofum.softonic.com/ie/33768

Figura 5.1 Pantalla del WiFiFoFum.

En la pantalla del software se puede apreciar el nombre o la identificación de la red inalámbrica que se encuentra dentro de la cobertura del dispositivo inalámbrico, en una posición relativa si es que no se cuenta con el sistema GPS, dependiendo del número de paquetes capturados y de la intensidad con la cual se reciben, esta posición relativa se ira ajustando dependiendo de la distancia a la cual nos encontremos de la red, así entre más cerca nos encontremos, más al centro del radar aparecerá.

Ya que se ha identificado la red inalámbrica, se tiene otra ventana donde se puede ver la siguiente información:

WEP	MAC	SSID	Type	RSSI	Channel	FirstSeen	LastSeen	Lat	Lon
On	00:0D:72:A6:C4:F1	2WIRE455	AP	-27	6	03:00:35	04:12:00	0	0
Off	00:0D:72:8D:92:B9	2WIRE152	AP	-90	6	03:00:40	04:12:00	0	0
Off	00:10:E7:F5:D4:60	Control	AP	0	6	03:55:47	04:12:00	0	0

El primer campo nos permite conocer de primera mano si la red tiene o no habilitado el protocolo de encriptación WEP, lo que a su vez nos ahorro tiempo y esfuerzo en la intervención de la red, ya que al no tener habilitado el protocolo de encriptación WEP, ni ningún otro método alterno, se podrá acceder a la red casi de manera automática y si el usuario o administrador tiene habilitada la posibilidad de conexión automática a Internet, entonces conectarnos a la WWW será tan simple, como aceptar la conexión a la red Inalámbrica y activar el navegador de Internet.

El segundo campo de información que resulta muy útil es el del identificador MAC ya que como se había mencionado anteriormente los primeros tres octetos de la dirección nos permiten identificar el tipo de tarjeta que se esta utilizando en los dispositivos inalámbricos y a su fabricante. En el ejemplo anterior se pueden ver dos tipos diferentes de tarjetas, los octetos que inician con 00:0D:72 pertenecen a las tarjetas y dispositivos inalámbricos de la marca 2WIRE, y los octetos 00:10:E7 pertenecen a la marca BreezeNet. De esta manera al conocer al fabricante, podemos también darnos una idea de a que sistema nos estamos enfrentando. En el Anexo 2 se puede ver una lista con los octetos pertenecientes a las compañías y fabricantes más comunes de la industria del WiFi.

El tercer campo es el SSID (Service Set Identifiers) que se utiliza para identificar al dispositivo inalámbrico.

Los sistemas ya cuentan con identificadores por Default como en el ejemplo anterior donde las tarjetas 2WIRE tienen un identificador 2WIRE455. Esto puede resultar peligroso ya que de manera automática y sin necesidad de buscar el identificador MAC, se puede conocer el tipo de tarjeta por el fabricante, en otro caso se ha cambiado el identificador de la tarjeta BreezeNet por el de Control, lo que obliga una identificación por octetos de MAC.

El cuarto campo muestra el tipo de dispositivo de la red inalámbrica, en este caso AP es el Punto de acceso (Access Point).

Finalmente el resto de los campos nos muestran la siguiente información: "RSSI" (el nivel o la potencia de la señal), "Channel" (cual de los canales se esta utilizando en la red inalámbrica), "FirstSeen" (la hora en la cual se detecto la red) y "LastSeen" (la hora en la cual se dejo de detectar). En el caso de tener habilitado el GPS, aparecería en los dos últimos campos las coordenadas del dispositivo dados en Latitud y longitud.

Ya que tenemos localizada la red y contamos con una serie de datos de la misma, el segundo paso es el comenzar a capturar la información que se transmite a través de la red.

Si por alguna razón estamos monitoreando nuestra red, pero obtenemos muy poca información o nada de ella, esto se puede deber a que los beacons frames no estén activados, o que los beacons estén activos pero el ESSID este oculto. En estos casos lo único que podemos hacer es poner nuestra tarjeta a monitorear sin ningún tipo de filtro, ni para los canales ni para las MAC de los APs (BSSID), de este modo captaremos todos lo paquetes que andan sueltos por ahí.

5.1.1 Los Puntos de acceso (access point)

En este momento haremos una pequeña pausa en el procedimiento y en su lugar analizaremos el AP, esto debido a que desde un inicio podríamos localizar redes inalámbricas sin ninguna medida de protección lo que a su vez nos podría llevar a la modificación o manipulación de los parámetros que guarda. El punto de acceso suele ser un router o un módem-router, ya que lo proveedores de Internet (ISP) últimamente dentro de la oferta WiFi ofrecen un router inalámbrico que al mismo tiempo funcionan como modem para acceso a Internet. Por lo tanto, no todas las redes inalámbricas tienen porque tener conexión a Internet, aunque la mayoría la tendrán por lo que se comentó anteriormente.

Hablando sobre la configuración de los routers, estos por lo general tienen un "Wizard" que nos permite acceder a su configuración, donde podremos activar o desactivar todos los elementos de seguridad (WEP, WAP, ACL, etc.) de que se dispongan, también podremos configurar el direccionamiento de los puertos (NAT), etc.

Para acceder al router por medio del "Wizard", disponemos de una pagina Web, aunque también pueden ser por Telnet, o incluso por FTP (para subir archivos de configuración ROM). Para poder visualizarlos usualmente se pone en la barra de direcciones del navegador la IP del router (usualmente 192.168.0.1 o 192.168.1.1) o si preferimos por Telnet, se debe de hacer el Telnet a la IP.

Es en este paso donde encontramos uno de los primeros puntos débiles de la red WiFi, ya que para entrar a la configuración del router se nos pedirá un UserName y un Password, o simplemente un Password (dependiendo del modelo del router). Por lo que debemos de conocer estos dos parámetros que implementa el fabricante por default. Se recomienda que una vez que se ha accesado y modificado los parámetros del router, se cambie el Password del router ya que existen paginas en Internet donde se muestran modelos de router con el UserName y Password de fabrica, así, si un intruso busca introducirse a una red y logra entablar comunicación con el router, podrá obtener una MAC con la que puede averiguar quien es el fabricante del mismo y probar los diferentes UserName y Passwords del fabricante, hasta que, finalmente y en el caso de que no se hayan modificado, pueda el intruso modificar los parámetros de acceso a la red WiFi.

En la siguiente página se puede ver esta información:

http://www.phenoelit.de/dpl/dpl.html

5.2 Configuración de las tarjetas de red

La tarjeta de red es el siguiente elemento que analizaremos. Además comenzaremos con algunos conceptos a tomar en cuenta para la configuración de los sistemas para la captura de IV. En este caso se recomienda adquirir o utilizar una buena tarjeta con soporte en drives y documentación que respalden su uso ya que bien aun cuando en el mercado existe una gran cantidad de tarjetas de red inalámbricas, no todas se pueden colocar en modo promiscuo o los drives de su chipset no son compatibles con el software que se utiliza. La gran mayoría son PCI para máquinas de escritorio y PCMCIA o CARDBUS para las portátiles y últimamente tarjetas USB.

Otros parámetros a considerar en las tarjetas inalámbricas son la sensibilidad de recepción, la potencia de salida, la posibilidad de añadir una antena (conectores), el estándar o protocolo que utiliza (IEEE 802.11a/b/g), la posibilidad de calibrar la potencia de emisión, etc.

Ahora, entrando al campo que nos interesa, es importante también conocer el CHIPSET de nuestra tarjeta. Existen diferentes marcas de chipsets, a continuación se presentan los más comunes en el mercado:

- TI (Texas Intruments)
- Atheros
- Cisco Aironet
- Intersil Prism
- Hermes u Orinoco
- Realtek
- Symbol
- Atmel
- Marvell

Pues bien, la cuestión esta en averiguar que chipset incorpora nuestra tarjeta y a esto podemos añadir que cada fabricante, cada modelo e incluso cada revisión no tienen porque tener el mismo chipset, es decir diferentes fabricante pueden coincidir en dos modelos con el mismo chipset. A continuación se presenta una página web donde se muestra una gran variedad de tarjetas inalámbricas y cual chipset es el que manejan:

http://www.linux-wlan.org/docs/wlan_adapters.html.gz

Si una tarjeta no sale en la lista, se puede realizar una búsqueda por Internet.

Por otra parte si aun no contamos con una tarjeta de red inalámbrica, se recomienda adquirir una con un chipset Atheros o Realtek, que según la pagina Web del programa AirCrack, tiene una compatibilidad del 100% con este programa (lo cual se explicara posteriormente).

Una vez que contamos con el modelo del chipset, podemos buscar y obtener los drives necesarios para poder colocar una tarjeta de red inalámbrica en modo “promiscuo”, ya que la tarjeta de red con los drives del fabricante permite únicamente entablar una comunicación entre el Punto de acceso y la red configurada, descartando toda la información que no este referida a esta conexión, así si en el entorno existen mas redes inalámbricas la información que se esta transmitiendo entre estas será desechada.

Pero para nuestro trabajo buscamos justamente lo contrario. Si lo que queremos es verificar la seguridad de una red a la cual se supone que no estamos autorizados a conectarnos, no contaremos con ninguno de los parámetros de configuración que permitan la conexión inalámbrica, así si nuestra tarjeta solo cuenta con los drives del fabricante, no podremos "capturar" los paquetes que se estén transmitiendo los diferentes elementos de la red, pero al poder colocar una tarjeta de red en modo "promiscuo", seremos capaces de capturar toda la información que se encuentre en nuestro entorno y con esta información posteriormente podremos analizarla y obtener datos y parámetros importante de la red como puede ser su llave de acceso a la misma en el caso de que se tenga habilitado el protocolo de encriptación WEP, UsarName y Passwords, direcciones IP, etc.

Entonces, una vez que conocemos el modelo del chipset de nuestra tarjeta podemos acceder a diferentes lugares en Internet donde podemos descargar los drives requeridos. A continuación se muestra una página de Internet que puede sernos de utilidad:

http://www.wildpackets.com/support/downloads/drivers

Al visitar esta pagina Web, vemos un listado de tarjetas compatibles por lo que hay que buscar el driver indicado y si nuestra tarjeta no está por ningún lado, pero sabemos, gracias a la lista de adaptadores que nuestra tarjeta tiene un chipset Atheros, pues simplemente hay que ir al enlace y descargar el driver para Atheros.

5.2.1 Instalación de drivers

Una vez que contamos con el Driver indicado hay que instalarlo en la máquina que estamos utilizando junto con la tarjeta inalámbrica, para esto simplemente hay que actualizar el controlador. A continuación mostramos un procedimiento:

- Descomprimimos el archivo que contiene el drive.
- Ejecutamos: compmgmt.msc
- Seleccionamos "Administrado de Dispositivos"
- Buscamos los adaptadores de red
- Identificamos nuestra tarjeta inalámbrica instalada
- Sobre la tarjeta le damos al botón derecho del Mouse y se selecciona "Actualizar"
- En la opción "Desea que Windows se conecte" se le da que NO, en su lugar se selecciona "Instalar desde una ubicación"
- Incluimos la ubicación del drive en la búsqueda y quitamos la marca de buscar en CDs.
- Examinamos el archivo *.inf.
- Si nuestra tarjeta sale en el menú, se selecciona.
- Si no sale, se selecciona el modelo genérico (Atheros por ejemplo)
- Después de que se instale, reiniciamos la Pc.

En este punto ya contamos con los drivers instalados, por lo que podemos poner a la tarjeta en modo "promiscuo" o de monitor, y así poder "husmear" paquetes con programas como el AiroPeek, Ethreal, Airodump, etc.

5.3 Captura de Información

La captura de la información se puede hacer de manera abierta frente al lugar donde se encuentra la red si el ambiente y la situación lo permite o en caso contrario de manera oculta, pero ahora si utilizando una LapTop ya que no existe aun software de este tipo para equipos tan compactos como una Pocket, principalmente por la capacidad de almacenamiento.

Las ligas que a continuación mostramos son de los programas que se habían mencionado anteriormente para la captura de paquetes:

http://www.wildpackets.com/products/airopeek/overview

Software muy potente pero que no es gratuito.

http://www.ethereal.com/

Software potente y gratuito (es el que recomiendo).

http://www.netstumbler.org/forumdisplay.php?f=25

Software potente y gratuito.

En nuestro caso hemos seleccionado dos paquetes de software, el airodump y el Ethereal por dos motivos, el primero que son gratuito y el segundo que son también muy fáciles de utilizar. El Ethereal resulta ser más amigable al trabajar bajo ventanas y además nos permite desplegar toda la información obtenida, el airodump se encuentra mas proyectado a trabajar bajo un ambiente de comandos y no puede desplegar la información.

5.3.1 Ethereal

Ethereal es un potente analizador libre de protocolos de redes, que nos permite capturar los datos directamente de una red u obtener la información a partir de una captura en disco (puede leer más de 20 tipos de formato distintos). Destaca también por su impresionante soporte de más de 300 protocolos, gracias sin duda a la licencia GPL y sus más de 200 colaboradores de todo el mundo.

Una de las cosas que más cuesta entender cuando uno comienza con ethereal es la utilización de los filtros a la hora de capturar datos, puesto que utiliza un sistema para visualizar los datos y otro totalmente diferentes e incompatible para realizar las capturas (tcpdump).

Ethereal se puede ejecutar sobre Windows NT4, 2000 o XP en cualquiera de sus variantes, Una vez que se han descomprimido los archivos del setup del programa, hay que instalar el archivo "WinPcap_3_0.exe" ya que de no ser así el Ethereal no capturara la información de la manera correcta marcando un error. Una vez que hemos instalado el programa de Ethereal en nuestra máquina y al correrlo veremos la una ventana como la mostrada en la figura 5.2 (Si deseamos adentrarnos en este paquete, existen también algunos tutoriales en la red, aquí explicaremos simplemente como comenzara a capturar paquetes para su posterior uso).

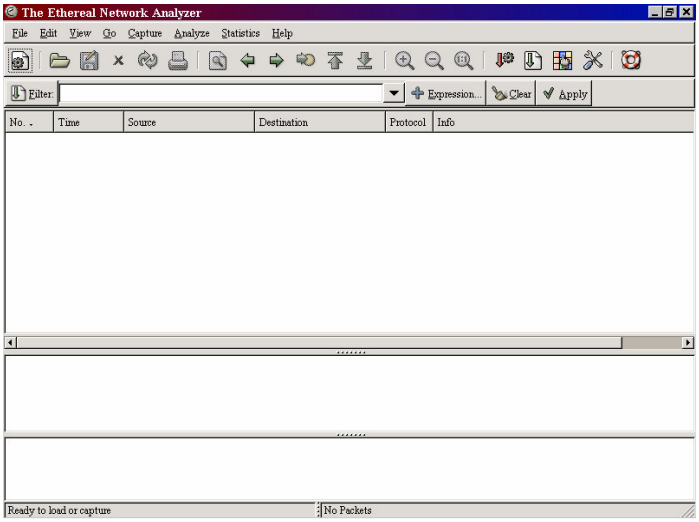


Figura 5.2 Pantalla del Ethereal.

En la parte superior izquierda de la pantalla oprimimos el icono Start (figura 5.3):

Figura 5.3 Icono de Start.

Con el cual aparecerá la ventana de configuración para la captura de paquetes (Figura 5.4):

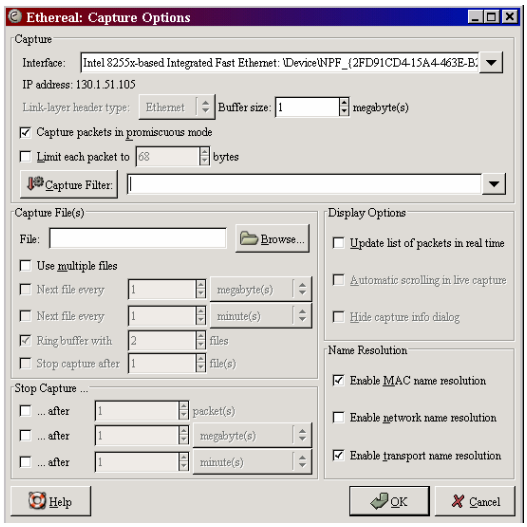


Figura 5.4 Ventana de configuración.

Los parámetros que contiene esta ventana, no es necesario que se modifiquen, pero si debemos asegurarnos que la opción de captura en modo promiscuo deba de encontrarse habilitada, además deberemos de darle una ruta y nombre al archivo donde guardaremos la información capturada, una vez hecho esto solamente bastara en oprimir el botón de "OK" para que comience el programa a funcionar.

Cabe recordar que la cantidad de información que debemos de capturar, deberá de contener miles de vectores de inicialización (IV's) para que aumente el grado de éxito en nuestra tarea de obtener una clave WEP, entre mayor es el número de vectores, serán mayores las posibilidades de lograr esto, y aunque se tenga un gran tráfico de información en el momento de la captura, esta cantidad de vectores se logra en tiempos de alrededor de 4, 5 o mas horas.

Si no activemos las opciones "Update list of packets in real time" y "Automatic scrolling in live capture" en la pantalla de opciones anteriores, no podremos consultar la información de cada paquete hasta que no se termine la captura.

Cuando hemos capturado el suficiente número de vectores se puede detener la aplicación y en la pantalla del Ethereal aparecerá la información como se muestra en la figura 5.6:

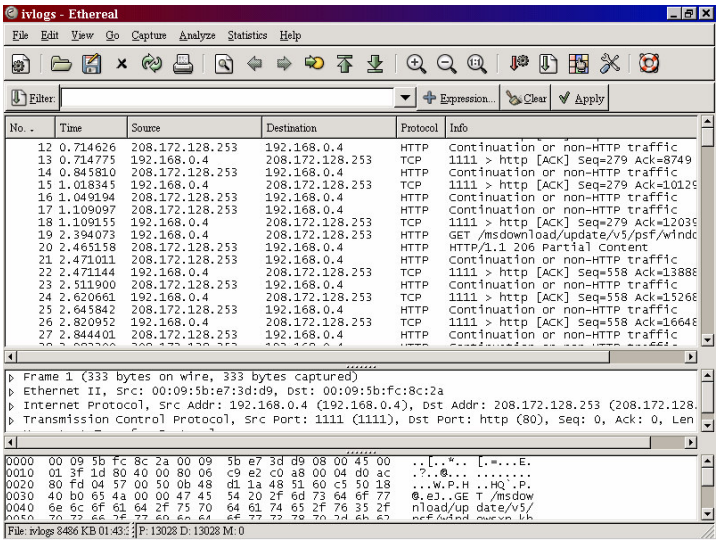


Figura 5.5 Ventana con la información capturada.

Por si sola la información que nos muestra esta pantalla ya es de un gran valor, ya que si se monitoreo una red la cual no contaba con algún tipo de encriptación, podríamos por ejemplo descubrir el Password del correo electrónico de alguien que desafortunadamente en ese lapso de tiempo lo hubiera utilizado, ya que contiene el programa filtros y opciones de búsqueda en valor hexadecimal, string, etc. Que nos permite buscar información muy especifica, como por ejemplo, la palabra "Password" en toda esta avalancha de letras y números. La acción de utilizar el Ethereal por un administrador de red WiFi puede mostrarle el grado de protección con la que cuenta su red, si se encuentra protegida o es visible para cualquier persona.

Una vez finalizada la captura, veremos tres ventanas de información. La primera muestra un listado de todos los paquetes capturados, con información relevante a ellos, así como los puertos utilizados. Seleccionando uno veremos información más detallada sobre su procedencia o destino, las direcciones IP y MAC (como en la identificación de la red obtuvimos la dirección MAC, aquí podremos comparalas y ver que en realidad los paquetes capturados pertenecen a la red deseada), los protocolos y puertos utilizados, así como su tamaño. Igualmente, se nos mostrará el contenido del paquete en formato hexadecimal y ASCII. En general, la información resultará poco comprensible, aunque nos ayudará a saber qué máquinas se conectan a otras y a través de qué puertos, gracias a lo que podremos ver situaciones anómalas.

Sin embargo, una prueba de lo que podemos llegar a conocer con una de estas herramientas pasa por espiar un servidor de correo o una máquina concreta. Si lo hacemos, veremos cómo en los paquetes enviados/recibidos a los puertos 110 y 25 del protocolo POP3 y SMTP se incluyen las claves y nombres de usuario del buzón de correo. Podremos visualizar dicha información siempre que se envíen en formato de texto plano, lo más habitual con la mayoría de los proveedores

5.3.2 Airodump

El segundo paquete que se menciona es el airodump el cual se encuentra completamente ligado al software que utilizaremos para la obtención de claves WEP, por lo que si bien, la información que nos proporciona el Ethereal tiene gran valor en el análisis de la red, los archivos que se obtienen también resultan ser de gran tamaño y posteriormente hay que transformarlo a un formato que manejan los programas que obtienen las claves WEP como el Aircrack y el ClaveWep (Este ultimo de nuestra propia autoría y que se puede ver en el Anexo 1 de este trabajo), por lo que el Ethereal se puede utilizar en una primera instancia como un analizador de datos, pero para una red que cuenta con una clave WEP, es más recomendable la captura de información con el paquete de airodump.

Este paquete junto con el Aircrack (ambos se encuentran en el mismo archivo Zip) los podemos descargar desde la siguiente dirección:

http://www.cr0.net:8040/code/network/aircrack-2.1.zip

Ahora, este programa no contiene tres archivos que resultan ser esenciales:

- Peek.dll
- Peek5.sys
- MSVCR70.dll

Estos archivos se pueden buscar en Internet y deben de colocarse una vez que se obtuvieron, en la misma carpeta donde se encuentran los archivos “aircrack.exe” y “Airodump.exe”.

Al igual que el Ethereal, tenemos que ejecutar el Airodump.exe en el área donde se encuentra el tráfico que buscamos obtener, una vez que se corra el programa, este detectara todas las tarjeta habilitadas en el sistema de manera automática, por lo que debemos de introducir el número de nuestra tarjeta inalámbrica.

El siguiente paso es seleccionar el tipo de interfaz de la red, (Atheros, Aironet / Orinoco Realtek), que depende del driver y de la tarjeta que tengamos.

Ahora seleccionamos el canal que se busca vigilar. Si ponemos cero, dará por entendido el programa que no queremos filtrar ningún canal lo cual resulta ser lo más común ya que difícilmente sabremos que canal es el que utiliza la red inalámbrica.

El siguiente paso es nombre del archivo donde se guardara la información, no hace falta poner ninguna extensión, ya que automáticamente la crea el paquete.

La siguiente opción que se ve en la pantalla, sirve para filtrado de MACs, es decir el programas solo aceptara los paquetes de la MAC que se seleccione, el formato debe ser 00:00:00:00:00. Para no filtrar ninguna y procesar todos los paquetes de todas las MACs, solo hay que escribir una “p”.

Finalmente al dar enter se comenzaran a capturar los paquetes. Como ya se había mencionado, con un millón de IVs es suficiente para una llave de 128 bits (104 bits reales) y para una de 64 necesitaremos la mitad.

Como consejo, se recomiendo que una vez que se ha comenzado una captura, esta no se detenga por si acaso no se tiene la suficiente información para obtener una llave, pues a veces el programa nos muestra un mensaje, que dice "No luck, sorry" y como se había parado la aplicación, ésta se tiene que comenzar nuevamente desde cero. Por otra parte si no funciona la primera vez seguiremos capturando más información para tratar nuevamente mas tarde.

Si vemos que capturamos muy poca información o si simplemente no capturamos ningún IVs, esto podría ser porque:

- No monitoreamos una red WEP si no una WPA
- Estamos muy lejos de la red y solo nos llegan los Beacon Frames
- Si nuestra tarjeta no es compatible con el 802.11g y el AP solo emite en 802.11g y no en 802.11b, no funcionará.
- Si existen más redes en el entorno, puede ser necesario especificar la MAC del AP.

También existe la posibilidad de que nuestro driver este mal instalado, por lo que hay que reinstalarlo.

5.4 Crackeando la red

Los dos programas que utilizamos para la obtención de claves resultan muy fáciles de utilizar, nuestro ClaveWep[3] utiliza el mismo formato de archivos que el Airocrack (*.cap), aunque éste muestra una ventana de configuración que resulta ser más atractivo que el primero.

ClaveWep se creo más que nada, para mostrar como funcionan estos programas y que algoritmos se aplican para la deducción de la clave WEP, esta escrito en el lenguaje Perl y para correrlo es necesario contar con el programa compilador, teniendo la siguiente sintaxis:

C:\perl clavewep.pl –t

El archivo se toma del mismo directorio donde esta el script, el cual debe de llamarse “Ivfile.log” en todos los casos.

Este programa en las pruebas preliminares presentó un alto grado de aciertos en la decodificación de claves WEP, pero debido a la limitante de que no todos tienen el perl instalado en sus máquinas y que no se puede crear un archivo auto ejecutable, se explicará más a fondo como trabaja el programa de airocrack y se deja al final del capítulo el análisis del programa ClaveWep y en el anexo 1, el código y para quien este interesado en revisar los algoritmos que se aplican en los paquetes obtenidos para deducir la posible llave WEP que tenga implementada la red inalámbrica.

[3] Ver Anexo 1

5.4.1 Airocrack

Airocrack trabaja tanto desde la línea de comandos como desde una ventana en Windows (Figura 5.6), a continuación se enumeran las opciones que componen al programa:

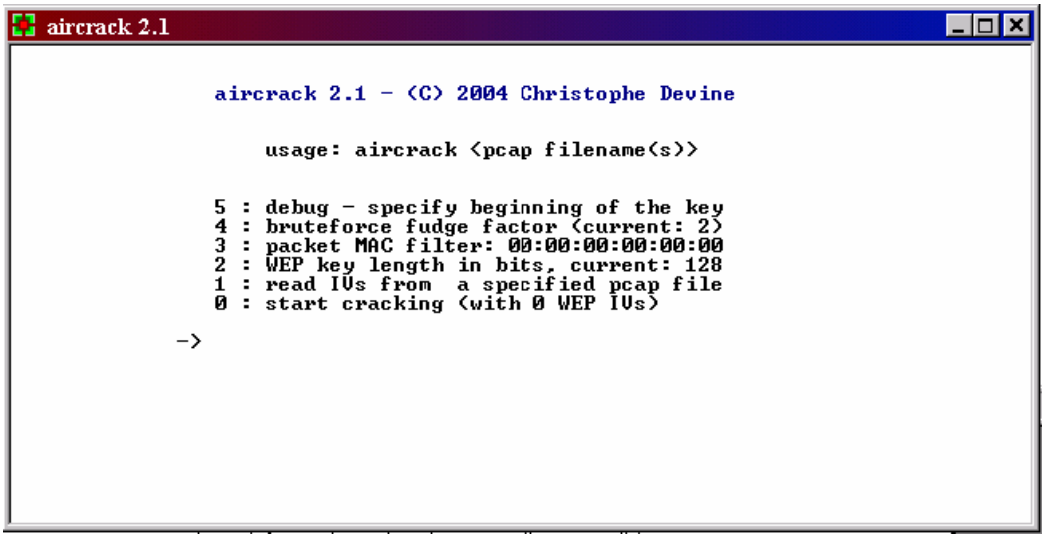


Figura 5.6 Ventana del Aircrack.

Opción 5: Esta opción la utilizamos cuando conocemos el inicio de una clave y tal vez no conocemos el resto de ella, por lo que esta pista nos puede ayudar ahorrándonos tiempo de análisis de información.

Opción 4: Esta opción es difícil de manejar por lo que se recomienda no utilizarla al menos que el mensaje de "No luck, sorry" aparezca muy seguido. Sirve para aumentar la cantidad de llaves a probar. Es decir si con 5000 llaves no encuentra la clave acertada, pues aumenta el número (por defecto 2) y así probara más llaves posibles.

Opción 3: Filtro de paquetes que solo acepta los de la MAC introducida.

Opción 2: Se utiliza para especificar la longitud de la llave. Por defecto es 128 (lo mas común). Se recomienda dejar esta opción tal cual ya que en la opción de 128 sacara esta y la de 64 en caso de que este sea su tamaño, pero si se configura a 64 bits descartara la de 128 bits.

Opción 1: En esta opción se leen los vectores validos (IVs) del archivo.cap y se enumeran. Solo hay que introducir el nombre del archivo (este debe de estar en la misma carpeta y hay que incluir la extensión, normalmente *.cap)

Opción 0: Con esta opción comienza el análisis de la información.

Cuando acabe el análisis, se tendrán dos opciones. La que buscamos es el mensaje de KEY FOUND, como se muestra a continuación:

```
                                aircrack 2.1

* Got  286716! unique IVs | fudge factor = 2
* Elapsed time [00:00:03] | tried 1 keys at 20 k/m

KB    depth   votes
 0    0/  1   DA(  60) 70(  23) 55(  15) A2(   5) CD(   5) 3E(   4)
 1    0/  2   BD(  57) 2A(  32) 29(  22) 1D(  13) F9(  13) 9F(  12)
 2    0/  1   8C(  51) 67(  23) 48(  15) DD(  15) D6(  13) FA(  12)
 3    0/  3   1D(  30) A5(  17) 07(  15) 7B(  12) 4B(  10) 63(  10)
 4    0/  1   43(  66) B1(  15) D2(   6) 1A(   5) 20(   5) 21(   5)
 5    0/  5   92(  27) 23(  25) 02(  18) 2F(  17) C1(  16) 36(  12)
 6    0/  1   C6(  51) 54(  17) 50(  15) 66(  15) 01(  13) 4A(  13)
 7    0/  2   84(  29) C0(  17) EE(  13) 80(  12) 49(  11) F6(  11)
 8    0/  1   81(1808) 09( 119) 99( 116) 32(  75) 49(  75) 9D(  65)
 9    0/  1   C4(1947) E1( 125) FC( 123) BD( 105) 8C(  98) 2F(  85)
10    0/  1   8A( 580) 41( 120) 18(  93) ED(  85) B0(  65) 97(  60)
11    0/  1   08(  97) FF(  29) 5D(  20) 1E(  17) 18(  15) 5E(  15)
12    0/  1   1B( 145) DD(  21) 46(  20) 1C(  15) 76(  15) 07(  13)

                KEY FOUND! [ DABD8C1D4392C68481C48A081B ]
```

La otra opción es: "**No luck, sorry**". Si aparece este mensaje tendremos que realizar toda la labor de captura y análisis de información nuevamente, y aunque resulta muy fácil la captura de paquetes a veces esto se torna insoportable.

Después de aprender como se puede crackear un cifrado WEP, podemos pasar a otros puntos de seguridad en una red inalámbrica.

5.5 Después de detectar la red y averiguada su WEP ¿que?

Una vez que tenemos la llave WEP, determinamos que nuestra red en realidad se encuentra a merced de cualquier hacker con un poco de experiencia, por lo que debemos de implementar otros métodos de seguridad o complementar el existente para cubrir estos “huecos”. En este punto podría finalizar nuestra prueba de seguridad, pero podemos de igual manera continuar y ver hasta donde somos capaces de llegar, de esta manera continuaremos identificando otros puntos débiles o bien, encontrar puntos sin retorno o acceso que en realidad limiten la acción de un intruso dentro de la red. Para esto, es importante volver a instalar los drivers anteriores de la tarjeta e intentamos conectarnos o asociarnos a la red, configurando nuestra tarjeta, activando el DHCP para que el router nos proporcione una IP de manera automática.

Pero como cada programa es diferente, explicaremos brevemente algunas de las características de Windows en cuanto a protección.

Cuando sale una imagen de un candado y dice "Esta red tiene seguridad habilitada", esto significa que tiene el cifrado activo, y por lo tanto necesitamos la clave que antes conseguimos.

Un punto importante es que la obtención de claves WEP no es una ciencia exacta, por lo que tal vez la clave que obtuvimos no necesariamente es la correcta, existe una gran posibilidad de que si sea, pero de igual manera pudo haber una fluctuación en los paquetes capturados que “confundieran” al algoritmo y provoque es este entregue una llave errónea.

Cuando introducimos la clave o simplemente no se tiene activado el cifrado, pero aun así sale un mensaje de "Conectividad Nula o Limitada", esto se puede deber a que:

La llave WEP que se obtuvo o se capturo, no es la correcta (se recomienda rescribirla).

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

Para averiguar la puerta de enlace (gateway), podemos analizar la información que se obtuvo con el Ethereal o el WiFiFoFum. Una vez que se obtuvieron estos datos, hay que configurar el IP, la puerta de enlace y la mascara de subred (que casi siempre es 255.255.255.0).

Una vez configurada la puerta de enlace y todo lo demás y si la red no tiene ningún tipo de seguridad en capas más altas (Ipsec, SSH), podemos ya tener una conexión a Internet.

Si la red tiene un filtro para MACs (ACL), es decir solo acepta la lista de MACs configurada en el router, la cosa se puede solucionar fácilmente, ya que Ethereal al monitorear el tráfico en la red, captura las MAC's de las máquinas que se conectaron y solo bastara reutilizar una de estas direcciones en nuestra máquina para que podamos entrar a la red sin problemas con el ACL. Para cambiar la MAC, existe un programa muy básico y sencillo llamado etherchange[4].

Si conseguimos entrar al router (como ya se vio por medio de su Password y UserName), podríamos añadir a la tabla de MACs una MAC que posteriormente utilizaríamos, así no reutilizaríamos otras que si se llegara a dar se repetirían en la tabla de acceso de la MAC, lo que podría disparar una alarma.

Si hemos logrado llegar hasta aquí, es evidente la carencia de seguridad de la red que inspeccionamos, si nos quedamos en uno de los pasos anteriores puede ser que estos no se realizaron de la manera adecuada, o (lo que nos daría gusto) alguno de los métodos de protección ha funcionado. Ahora esto no significa que esta metodología sea la única que se puede aplicar a una red para que esta sea vulnerada, como se había mencionado anteriormente, existen muchos métodos de *Crackeo*, pero el conocer nuestros puntos débiles permite que estos sean corregidos, protegidos o de plano cancelados.

Se recomienda que continuamente se instalen los parches y las actualizaciones que Windows saca al mercado, ya que estos por lo general cubren vulnerabilidades en cuanto a la seguridad de este paquete. Como ya es obvió nos evocamos a Windows y no a Linux o Mac, ya que el 98% del mercado de las computadoras lo conforman máquinas PC y de este el 80% maneja la plataforma de Windows, y aunque cada vez es mayor el uso del Linux el cuál también presenta mejoras y problemas en cuanto a seguridad en redes inalámbricas, el grueso del mercado y por lo tanto el grueso de las redes inalámbricas se tiene bajo la plataforma de Windows.

Finalmente se reiteran nuevamente las medidas de protección básicas para las redes inalámbricas:

- Activar el cifrado WEP.
- Desactivar el broadcasting (emisión de frames de autenticación).
- Ocultar el ESSID y cambiar su nombre (la longitud en este caso no importa).
- Activar ACL (filtrado de MACs)
- Desactivar el DHCP del router y cambiar su password de acceso, así como actualizar su firmware.

[4] http://www.ntsecurity.nu/downloads/etherchange.exe

Capítulo 6

Caso práctico

Capítulo 6: Caso práctico

6.0 Introducción

Si bien, gracias a que actualmente varias compañías telefónicas que proveen el servicio de Internet, promocionan el uso de redes inalámbricas vendiendo o incluso regalando Hubs Wifi y que también es cada vez más común adquirir equipos de escritorio o portátiles que ya traen integrado el "WiFi", esto ha ocasionado un "boom" del uso de la tecnología inalámbrica, que a su vez a abierto cientos o miles de puertas a curiosos, intrusos o crackers que buscan un ancho de banda para conexión a Internet que sea "gratuito", o en el peor de los casos información del usuario que se esta interviniendo.

En México existen problemas en cuanto a la "cultura de protección de información" ya que la gran mayoría de la gente y de las empresas carecen de los conocimientos básicos en cuanto a la protección de la información, y es que muchos de ellos se quedan con la idea de la transmisión cableada donde el intruso tenia que intervenir directamente las instalaciones de la máquina y donde además con protección vía software se podía delimitar el acceso del personal deseado o no deseado (firewalls, RADIUS, listas de acceso, etc), lo que brindaba esa seguridad que el usuario buscaba, pero ahora en el mundo del "WiFi" ya no tenemos que introducirnos a las instalaciones o la máquina que se busca intervenir, solo hay que estar dentro del radio de cobertura de la red inalámbrica y punto, lo que nos provee el anonimato y seguridad necesaria para no ser detectados.

6.1 Estudio de la seguridad en redes inalámbricas en la Ciudad de México

Por esto mismo se realizo un estudio de redes inalámbricas en la Zona sur de la ciudad de México debido a la gran cantidad de empresas, zonas habitacionales, comerciales e instituciones de Educación, que brindaban un amplio espectro de muestreo. En si se realizaron búsquedas de redes inalámbricas en las avenidas de los Insurgentes, Lázaro Cárdenas, División del Norte, en los centros comerciales de Coyoacán, Galerías Coapa, Perisur, así como en diferentes calles de Coyoacán. Estos estudios nos muestran los problemas existentes en cuanto a la seguridad de la información, así como los diferentes sectores que son más propensos a proteger o dejar desprotegida la red inalámbrica.

La tabla 6.1 es solo una de las 7 muestras que se tomaron, y corresponde a un muestreo que se tomo alrededores y dentro de la Facultad de Ingeniería, donde se presentan dos casos interesantes. El primero es la gran cantidad de redes inalámbricas que no cuentan con protección pero que se debe a que muchas de ellas brindan acceso a estudiantes fuera de las instalaciones o áreas de computo. Por ejemplo desde el edificio de postgrado uno se puede conectar de manera remota a Internet accesando a la red del laboratorio de computo que se encuentra enfrente del edificio y se desconoce si se lleva un control de este acceso a esta red, pero mientras tanto uno puede checar su email o bajar información de la red.

La tabla 6.1, presenta si tiene habilitado o deshabilitado el encriptado WEP, el tipo de red, el nombre del dispositivo o del Hub inalámbrico, la MAC que maneja, el SRI que nos muestra con cuanta potencia recibimos la señal, que a su vez lo podemos interpretar como que tan lejos o cerca estamos de la red inalámbrica y finalmente que canal esta utilizando la red, de los once disponibles. La tabla es la siguiente:

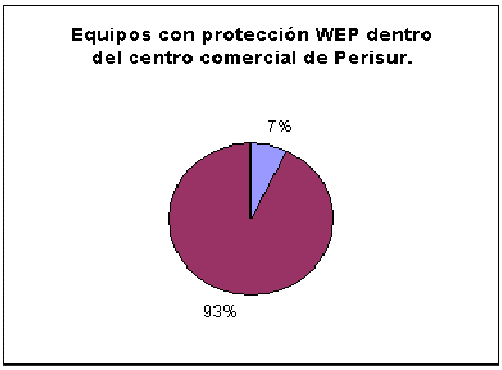
	Proteccion	Type	SSID	MAC	RSSI	Channel
1	None	Infrastructure	RIU	00:0B:86:C9:07:C0	-72	1
2	None	Infrastructure	control	00:06:25:DA:30:9B	-90	6
3	WEP	Infrastructure	RIU	00:0B:86:C9:BF:40	-87	1
4	None	Infrastructure	CUC	00:12:17:7A:93:D5	-90	11
5	None	Infrastructure	mobilelan	00:0D:54:A9:D6:A8	-90	6
6	None	Infrastructure	RIU	00:0B:86:CF:40:A0	-83	11
7	None	Infrastructure	DGEP-DireccionB	00:20:A6:59:DF:BB	-90	10
8	None	Infrastructure	2WIRE823	00:12:88:E0:C1:E9	-90	6
9	WEP	Infrastructure	LIDSOL	00:90:D1:01:35:C5	-73	11
10	None	Infrastructure	T1-2-T3	00:A0:F8:C9:7E:4E	-74	11
11	None	Infrastructure	T1-Feed2	00:A0:F8:4E:19:C6	-90	6
12	None	Infrastructure	CUC	00:12:17:7B:42:3C	-90	11
13	None	Infrastructure	ECS461	00:11:95:4C:EB:65	-90	6
14	None	Infrastructure	ApContraloria1	00:12:17:AA:24:AD	-90	9
15	None	AdHoc	LiteShow	02:0F:9E:2E:97:49	-75	10
16	None	Infrastructure	kaliman	00:10:E7:F5:57:D7	-90	11
17	WEP	Infrastructure	MATERIALES	00:13:46:70:68:B4	-74	2
18	None	Infrastructure	2WIRE164	00:12:88:84:F5:39	-75	6
19	None	Infrastructure	T1-2-T2	00:A0:F8:4E:19:A9	-90	6
20	None	Infrastructure	wireless	00:09:92:00:81:12	-79	11
21	None	Infrastructure	CUIB	00:13:46:45:D0:A8	-69	6
22	None	Infrastructure	CCAT	00:0E:6A:CD:86:2B	-90	6
23	None	Infrastructure	T1-2-T2	00:A0:F8:4E:19:CB	-90	6
24	WEP	Infrastructure	RIU	00:0B:86:C8:3B:E0	-71	11
25	None	Infrastructure	MATERIALES	00:11:95:E9:5E:0B	-90	2
26	WEP	Infrastructure	RIU	00:0B:86:C8:4B:C0	-74	11
27	None	Infrastructure	diedimeiG	00:0D:54:F7:82:C9	-90	1
28	None	Infrastructure	RIU	00:0B:86:CF:2E:20	-75	11
29	None	Infrastructure	RIU	00:0B:86:C8:A2:40	-83	11
30	None	AdHoc	hpsetup	C2:30:D3:E7:31:7D	-90	6
31	WEP	Infrastructure	MATERIALES3	00:12:A9:D0:0D:B6	-90	10
32	None	AdHoc	lamesa	00:0E:6A:7F:07:96	-73	11
33	None	Infrastructure	disenoindustrial	00:30:4F:40:C8:82	-90	8
34	None	Infrastructure	default	00:40:F4:94:B9:2B	-79	6
35	WEP	Infrastructure	RIU	00:0B:86:CF:26:C0	-90	1
36	None	Infrastructure	RIU	00:0B:86:C9:08:00	-90	1
37	None	Infrastructure	FamiliaAmbia	00:12:17:27:D8:2F	-90	6
38	WEP	Infrastructure	olas	00:0F:CB:A0:ED:A2	-70	11
39	None	Infrastructure	lmsrTEMPORAL	00:15:E9:17:00:9A	-90	7
40	None	Infrastructure	INA_CIFE	00:01:F4:ED:2D:09	-90	3
41	None	Infrastructure	2WIREFINAL	00:12:88:98:69:D1	-90	6
42	None	Infrastructure	3Com	00:04:75:65:5E:79	-70	11
43	WEP	Infrastructure	RIU	00:0B:86:C8:94:C0	-73	1
44	WEP	Infrastructure	RIU	00:0B:86:CF:21:80	-90	6
45	None	Infrastructure	2WIRE324	00:12:88:92:67:41	-90	6
46	None	Infrastructure	2WIRE471	00:0D:72:7D:88:91	-90	6
47	None	Infrastructure	IVirtual	00:14:7C:43:5B:C8	-70	11
48	None	Infrastructure	fanTM	00:A0:F8:4E:1A:66	-90	6
49	None	Infrastructure	belkin54g	00:30:BD:9A:6D:D0	-90	11

Tabla 6.1 Muestreo tomado alrededor de la Facultad de Ingeniería. 13/01/2006.

Con WEP Activado
2 7%

Sin WEP
25 93%

Total de redes 27



Con WEP Activado
0 0%

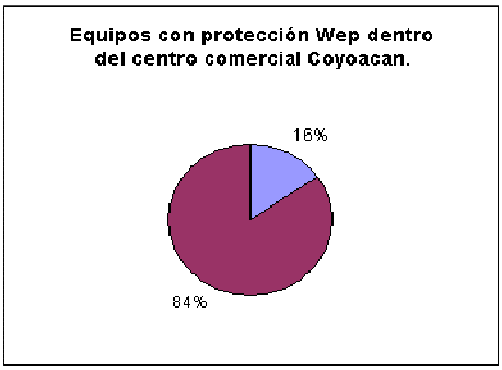
Sin WEP
28 100%

Total de redes 28

Con WEP Activado
7 13%

Sin WEP
38 84%

Total de redes 45



Con WEP Activado
0 0%

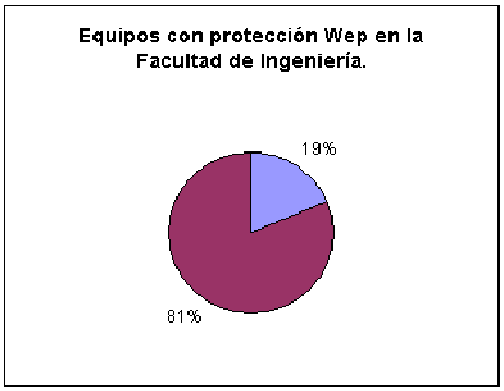
Sin WEP
51 100%

Total de redes 51

Con WEP Activado
10 19%

Sin WEP
43 81%

Total de redes 53



Con WEP Activado
22 14%

Sin WEP
138 86%

Total de redes 160

Con WEP Activado
19 11%

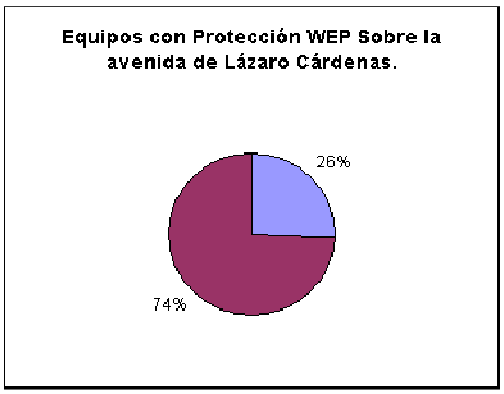
Sin WEP
157 89%

Total de redes 176

Con WEP Activado
52 26%

Sin WEP
150 74%

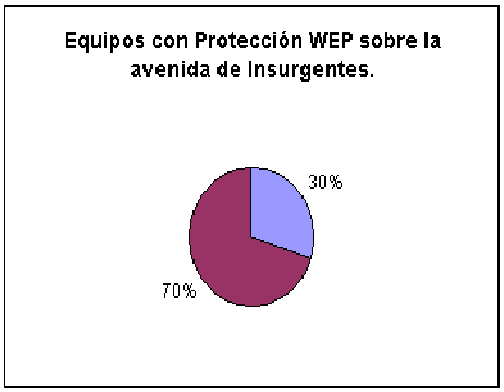
Total de redes 202



Con WEP Activado
195 23%

Sin WEP
448 77%

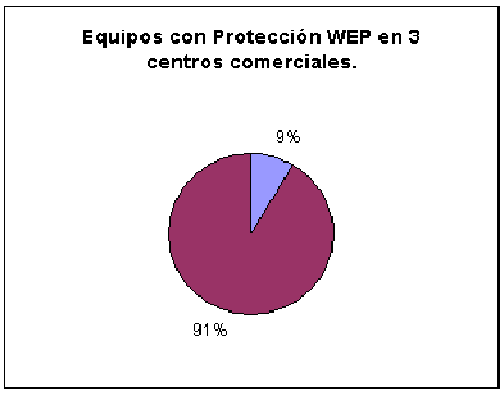
Total de redes 643



Con WEP Activado
9 9%

Sin WEP
92 91%

Total de redes 101



Con WEP Activado
19 8%

Sin WEP
208 92%

Total de redes 227

Con WEP Activado
269 27%

Sin WEP
736 73%

Total de redes 1005

Total de redes con WEP Activado

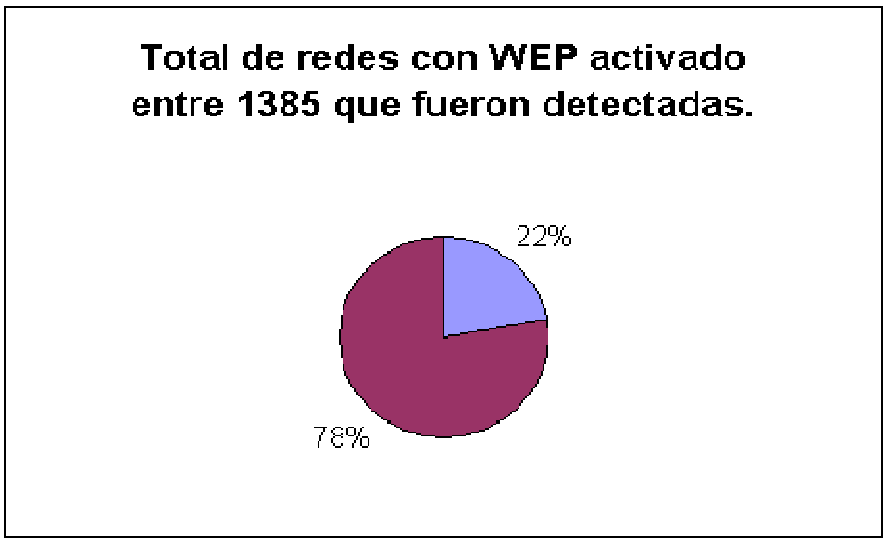
307 22%

Total de redes sin WEP Activado

1078 78%

Total de redes inspeccionadas

1385



Este estudio nos muestra que aproximadamente en promedio uno de cuatro usuarios protege sus transmisiones inalámbricas con el encriptado WEP, ahora es mucho más común ver redes sin protección en zonas habitacionales que en zonas de oficinas y negocios, donde una de cada tres redes cuenta con un encriptado WEP, mientras que en Centros comerciales es prácticamente imposible ver una red con protección, de igual manera que en lo obtenido en la Facultad de Ingeniería, muchas redes cuentan con un sistema abierto, por que brindan este servicio a sus clientes, como son los cafés, bares, etc. Pero hay establecimientos que tal vez manejen su contabilidad, movimientos bancarios, relaciones de empleados, clientes, etc que pueden administrar por medio de la PC y que da paso a que éstos datos puedan ser "adquiridos" por gente no deseada que podría darle un mal uso a esta información, por lo mismo deberá de ser en estos lugares donde se deberían de tener todos los parámetros de seguridad habilitados por su propia seguridad y de las personas que hagan uso de este servicio.

6.2 Caso práctico de Crackeo WEP

A continuación se mostrará el procedimiento de crackeo ya aplicado a una red inalámbrica para descubrir la llave secreta de encriptación WEP. Este ejemplo se realizó en nuestra propia red, con lo que hacemos énfasis nuevamente en que este no es un manual para Crakers. De esta manera mostramos como una red de apariencia segura, puede ser violada si no se cuenta con los medios necesarios de protección.

La figura 6.1 nos muestra la pantalla de una Pocket PC con el software WiFiFoFum, la cuál como se había mencionado, nos permite localizar redes inalámbricas:

Figura 6.1 Ventana del WiFiFoFum.

En este caso, se encuentran dos redes inalámbricas, la nuestra que se llama “Wifi_Base01” y una externa llamada “2Wire747”. Las características de ambas redes las podemos ver en la figura 6.2:

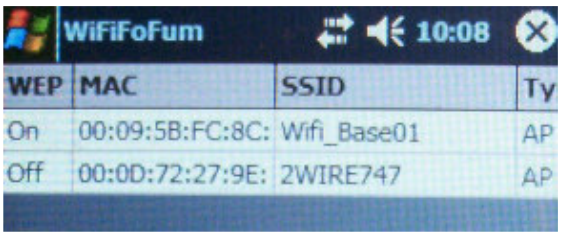


Figura 6.2 Características de las redes inalámbricas.

Este par de redes inalámbricas nos muestran el primer punto de protección que debemos de tomar en cuenta, ya que si bien, en la imagen se puede apreciar en la columna de encriptado “WEP” que nuestra red tiene habilitada la encriptación de información por el cifrado WEP, la segunda no cuenta con un cifrado de protección, además se descubre también otro de los puntos débiles en la seguridad, ya que se recomienda ampliamente que las redes no se auto “promocionen” mandando su identificador al ambiente para que sean detectadas por otros equipos. Otro inconveniente que acarrea esto es que el identificador de la red puede darnos más datos sobre la red que se quiere “inspeccionar” que los esperados. La primera red tiene un identificador muy ambiguo (ya que fue modificado, cambiando el dado por el fabricante), pero en la segunda red por el tipo de identificador, notamos de inmediato que se trata de una red “infinitum” de Telmex. Así el no deshabilitar el “beacon” o la transmisión del identificador de la red, permite que de manera instantánea sea identificada una red inalámbrica y además comencemos a recabar información sobre la red que posteriormente pueda ser de utilidad.

Una vez que ya tenemos plenamente identificada la red que se busca inspeccionar, comenzamos a capturar los paquetes cifrados que se transmiten por el ambiente para que una vez que se cuente con los suficientes VI’s, se proceda al creckeo de la clave WEP. En este primer caso se colocó una máquina HP modelo 5030la con una tarjeta inalámbrica USB a comunicarse con el hub inalámbrica mientras un programa “per to per” bajaba archivos grandes de la red, esto con el motivo de acelerar un poco el proceso provocando un gran tráfico de información en la red, aunque claro esto puede variar de situación en situación lo que a su vez repercute en el tiempo que se emplea en la captura de paquetes. Por otra parte, se utilizó una LapTop Vaio con tarjeta Realteck PCI sin configurar como elemento externo “promiscuo”.

La LapTop desde un inicio detecto a ambas redes inalámbricas, con la primera que se identifica como 2WIRE747 se pudo conectar sin ningún problema (en este momento ya estábamos cayendo en una falta, pero si la red no cuenta con la mas mínima medida de seguridad, y es el mismo ambiente el que no restringe una conexión, entonces, en realidad estamos cometiendo una falta???), lo que resulta aun peor es que si utilizamos un software como el Ethereal (Figura 6.3), que se encarga de capturar los paquetes de manera promiscua que se encuentren en el ambiente y que además permite su manejo e interpretación, podríamos fácilmente obtener Passwords del sistema, así como datos importantes que se transmitan por la red como podrían ser números confidenciales de tarjetas de créditos, nips, nombres, direcciones, etc.

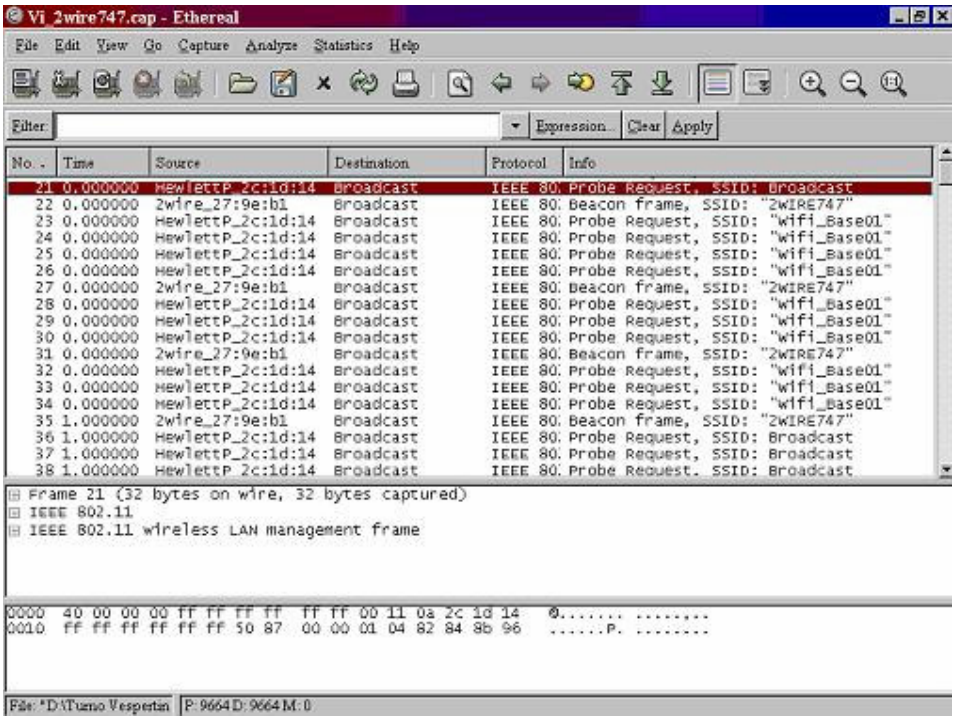


Figura 6.3 ventana de Ethereal con información de las redes inalámbricas.

Pero al buscarse la conexión en la segunda red (nuestra red “WifiBase_01”) se solicito una clave de acceso, la cuál no se proporciono a la máquina para que se continuara con el ejercicio.

En la LapTop “intrusa” se instalo el software de “airodump”, que es un “sniffer” que utilizaremos en la captura de información. Este paquete al correr despliega la siguiente pantalla de configuración (Figura 6.4):

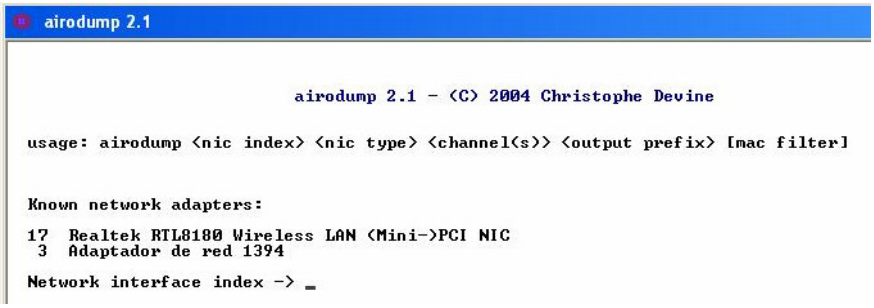


Figura 6.4 ventana de configuración del airodump.

Aquí simplemente se selecciona la tarjeta de red que se utilizará para la captura de la información, en la figura 6.5, se muestra el resto de los parámetros de configuración:

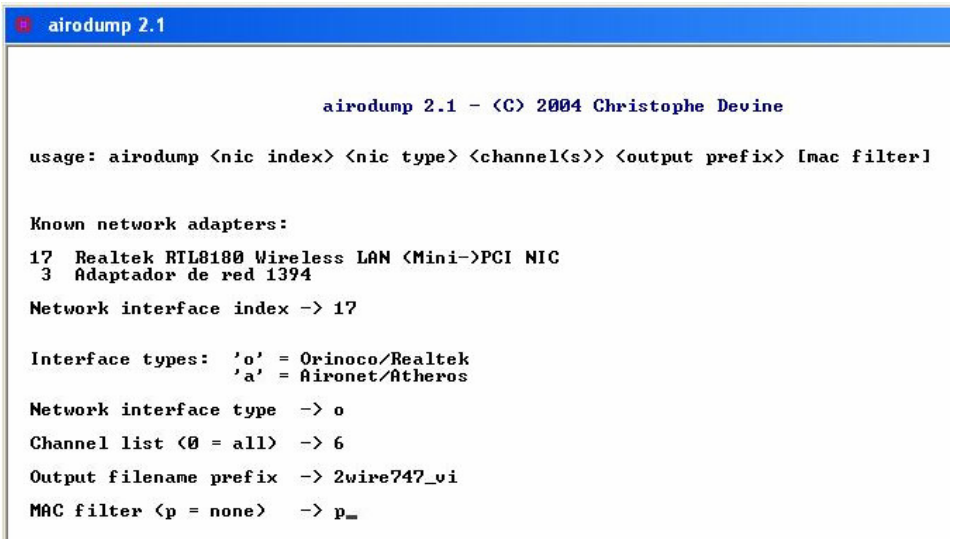


Figura 6.5 Segunda ventana de configuración del airodump.

Así podemos también delimitar los parámetros de configuración, determinando el canal a inspeccionar, un MAC en especifico (esto podría resultar trivial, pero se recuerda que por lo general la captura de información se refleja en archivos muy extensos de varios megas, así si tenemos la opción de delimitar parámetros, esto repercutirá en el tamaño del archivo final.) y que nombre llevará el archivo donde se guardará toda la información. Ya configurados los parámetros, comienza la captura de paquetes como se muestra a en la figura 6.6:

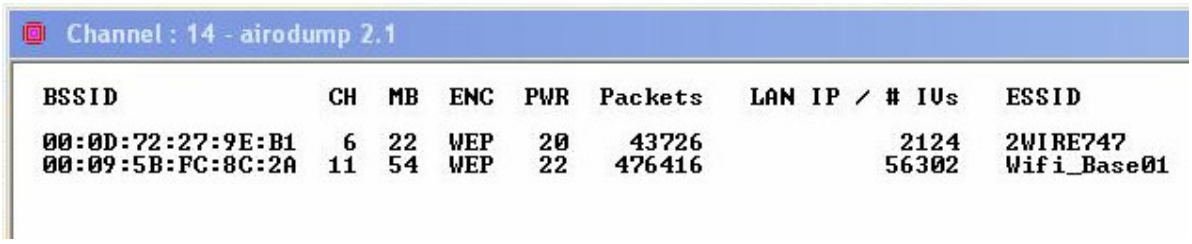


Figura 6.6 Captura de información con el airodump.

En la imagen se muestran ambas redes detectadas, sus respectivas MAC, canal de transmisión utilizado, encriptado, potencia de transmisión, paquetes capturados y IV's o vectores de inicialización obtenidos. Como se había mencionado anteriormente, en nuestra red se provoco un alto tráfico de información, mientras que en la segunda red es mucho menor el número de paquetes y VI's obtenidos.

Una vez que se han obtenido un número suficiente de VI's (se recomienda como mínimo 5000, pero este número en la mayoría de los casos resulta ser insuficiente, por lo que de nuestra parte se recomienda capturar entre 25000 y 50000 IV's y claro entre mayor sea el número de vectores, aumentaran las posibilidades de un crackeo exitoso.), para este ejercicio se obtuvieron mas de 50000 vectores en un lapso de poco mas de seis horas.

El archivo con los IV's, tuvo un tamaño de 88 Megas (aquí es donde se comienzan a valorar los incisos de configuración, que limitan los parámetros de captura de información, ya que si en lugar de dos redes, solo se hubiera inspeccionado una, el tamaño del archivo hubiera disminuido), este archivo que llamamos VI_datos.cap se tenía que procesar para aplicar el algoritmo inverso de encriptación que a su vez resulta en la clave de encriptación que se utilizó para el cifrado de la información, esto se realizo por medio del paquete "aircrack ver 2.1" cuya pantalla se muestra en la figura 6.7:

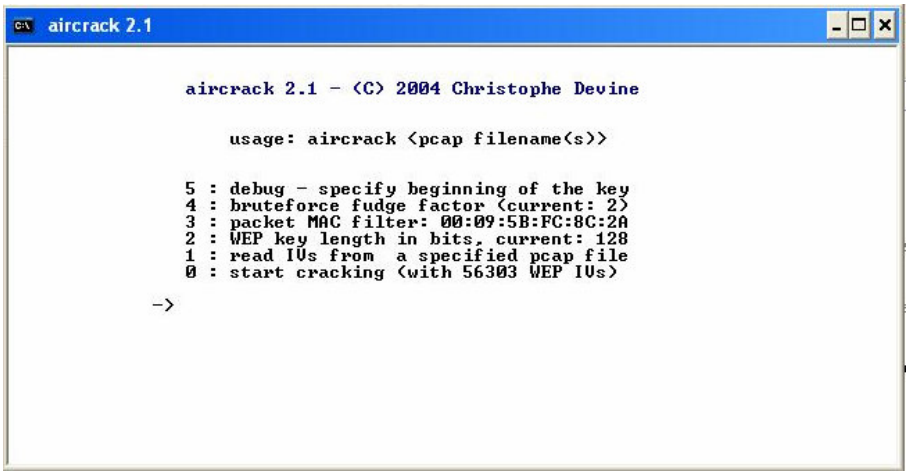


Figura 6.7 Ventana del aircrack.

Una vez que tenemos esta pantalla solamente bastara con arrastrar el archivo donde tenemos almacenados los IV's (extensión CAP) a la ventana del aircrack, para que se comience a procesar la información. Si esta no fue lo suficientemente extensa, aparecerá la leyenda de IV's insuficientes y recomendara realizar de nuevo la captura de IV's, pero si el número de vectores fue el requerido aparecerá la siguiente ventana (figura 6.8) la cuál despliega los datos de vectores utilizados y la clave WEP resultante:

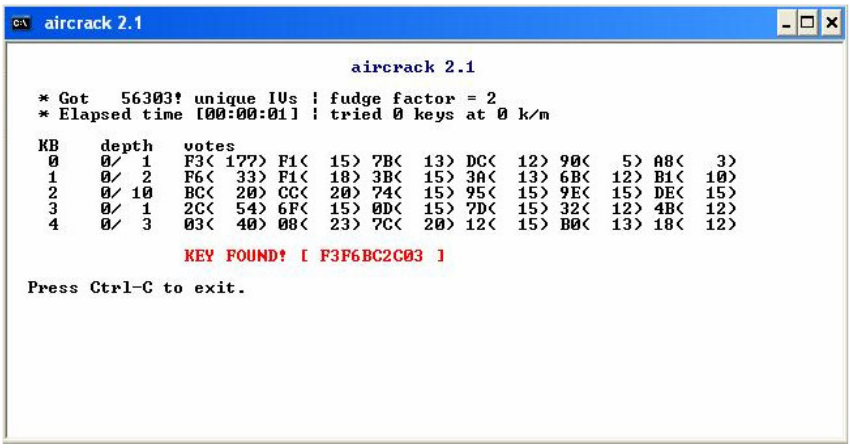


Figura 6.8 Ventana con el resultado del aircrack.

Como podemos apreciar, el software realiza un conteo de vectores de inicialización, y dependiendo el número de veces que estos aparecen, es como los va clasificando, formando la clave con los que un mayor de veces hayan resultado.

Posteriormente la clave de cifrado resultante se introdujo en la configuración de la red inalámbrica de la LapTop, con lo que de inmediato pudimos ingresar a la red "Wifi_Base01", así con esta acción estuvimos en la posibilidad de utilizar el ancho de banda del sistema, como también correr el software de Ethereal y poder obtener claves y datos relevantes que se transmiten por la red. Otras posibilidades que pueden quedar abiertas son la modificación de los parámetros del hub inalámbrico, que si bien es un poco más difícil, permiten re rutear canales de información a nuestra máquina o insertar una dirección MAC al sistema en caso de que esta tuviera un filtrado MAC para que no se sospechara que una máquina ajena al sistema estaba infiltrándose, sin ninguna medida de seguridad o en un caso extremo, simplemente cambiar la clave de acceso WEP para así deshabilitar las máquinas conectadas a la red inalámbrica, resultando en un uso total del ancho de banda con el que cuenta la red. El usuario afectado en este caso tiene la opción de desconectarse de su ISP mientras restituye los parámetros que por default tiene el Hub, pero esto además de engorroso se deriva en una perdida de tiempo y de recursos que en realidad no tienen razón de ser.

Conclusiones generales

Cada vez es más común la implementación y uso de redes inalámbricas en nuestro país. Este tipo de tecnología continuamente evoluciona, brindándonos equipos con un mejor alcance y conexión, provocando una sustitución de redes cableadas por inalámbricas. Esto se pudo apreciar en el estudio que se realizo en la zona sur del Distrito Federal, donde tuvimos la oportunidad de detectar 1385 redes inalámbricas tipo WiFi, donde solo 307 redes tenían el encriptado WEP habilitado y más de 1000 redes no contaban con un método de protección, situación que justifica el desarrollo de este trabajo.

La tesis propicia la toma de conciencia para la implementación de medidas de seguridad (ya sean WEP, WAP, Firewalls, RADIUS, paquetes de detección de intrusos, etc.) y el preparar a los usuarios de la red para que las utilicen. Y es que si bien dentro de la comodidad que nos puede brindar una red inalámbrica con la libertad de movimiento, también abrimos las puertas a los curiosos e intrusos que siempre están en busca de incautos que les permitan "tomar" su información o acceder al ancho de banda que brinde la conexión, ya sea solo por curiosidad o para hacer mal uso de ella.

Con este trabajo cubrimos varios puntos que son:

- Mostrar los principios de una red inalámbrica, como funciona, de que esta compuesta, etc.
- Explicar los fundamentos del protocolo WEP.
- Las vulnerabilidades de las redes inalámbricas que utilizan el protocolo WEP como medio de encriptación.
- Algunos métodos que se utilizan para obtener claves WEP
- Los métodos más comunes que existen actualmente para proteger una red inalámbrica.
- Un Estudio del uso de medios de protección en redes inalámbricas en la ciudad de México.

En lo que se hace énfasis dentro de la vulnerabilidades que se exponen y que se tratan de explotar, mostrando los métodos de creckeo para las redes inalámbricas, es en el hecho de que éstos se exponen para verificar que tan protegida se encuentra una red detectando puntos débiles, y no como un manual de hacker que buscará lo contrario a lo que hemos expuesto. En el libro del "El Arte de la Guerra" un principio básico habla del conocer al enemigo para estar siempre un paso delante de él. Este documento sigue la misma filosofía, así al poner a nuestra red inalámbrica en prueba buscando vulnerabilidades y corrigiéndolas, si es que son detectadas, eliminamos puntos y situaciones que otros podrían explotar.

Finalmente no existe la red cien por ciento segura, pero si tenemos la curiosidad o la intención de proteger nuestros datos y la integridad de nuestra red, entonces el camino y las medidas que se proponen son una muy buena manera de comenzar a trabajar.

Otros sistemas de seguridad

A.1 Introducción

Toda transacción segura por la red debe contemplar los aspectos de Autenticidad, Integridad, Confidencialidad y no rechazo. Son varios los sistemas y tecnologías que se han desarrollado para implementar estos aspectos en las transacciones electrónicas, siendo sin duda SSL el más conocido y usado en la actualidad. SSL permite la Confidencialidad y la Autentificación en las transacciones por Internet, siendo usado principalmente en aquellas transacciones en la que se intercambian datos sensibles, como números de tarjetas de crédito o contraseñas de acceso a sistemas privados. SSL es una de las formas base para la implementación de soluciones PKI (Infraestructuras de Clave Pública).

A.2 Secure Socket Layer

Secure Socket Layer es un sistema de protocolos de carácter general diseñado en 1994 por la empresa Nestcape Communcations Corporation, y está basado en la aplicación conjunta de Criptografía Simétrica, Criptografía Asimétrica (de llave pública), certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet. De los sistemas criptográficos simétricos, motor principal de la encriptación de datos transferidos en la comunicación, se aprovecha la rapidez de operación, mientras que los sistemas asimétricos se usan para el intercambio seguro de las claves simétricas, consiguiendo con ello resolver el problema de la Confidencialidad en la transmisión de datos.

SSL implementa un protocolo de negociación para establecer una comunicación segura a nivel de socked (nombre de máquina más puerto), de forma transparente al usuario y a las aplicaciones que lo usan.

Desde el punto de vista de su implementación en los modelos de referencia OSI y TCP/IP, SSL se introduce como una especie de nivel o capa adicional, situada entre la capa de Aplicación y la capa de Transporte, sustituyendo los sockets del sistema operativo (Véase figura A.1), lo que hace que sea independiente de la aplicación que lo utilice, y se implementa generalmente en el puerto 443. (Los puertos son las interfaces que hay entre las aplicaciones y la pila de protocolos TCP/IP del sistema operativo).

Figura A.1 Capa SSL.

SSL proporciona servicios de seguridad a la pila de protocolos, encriptándo los datos salientes de la capa de Aplicación antes de que estos sean segmentados en la capa de Transporte y encapsulados y enviados por las capas inferiores. Es más, también puede aplicar algoritmos de compresión a los datos a enviar y fragmentar los bloques de tamaño mayor a 214 bytes, volviéndolos a reensamblar en el receptor.

La versión más actual de SSL es la 3.0. que usa los algoritmos simétricos de encriptación DES, TRIPLE DES, RC2, RC4 e IDEA, el asimétrico RSA, la función hash MD5 y el algoritmo de firma SHA-1.

A.3 Protocolo TLS - Transport Layer Security

Para intentar corregir las deficiencias observadas en SSL v3 se buscó un nuevo protocolo que permitiera transacciones seguras por Internet, sobre todo teniendo en cuenta que SSL es propiedad de la empresa Nestcape. El resultado de esta búsqueda fue el protocolo TLS, que permite una compatibilidad total con SSL siendo un protocolo público, estandarizado por el IETF.

TLS busca integrar en un esquema tipo SSL al sistema operativo, a nivel de la capa TCP/IP, para que el efecto "túnel" que se implementó con SSL sea realmente transparente a las aplicaciones que se están ejecutando.

A.4 Protocolo S-HTTP

El protocolo Secure HTTP fue desarrollado por Enterprise Integration Technologies, EIT, y al igual que SSL permite tanto el cifrado de documentos como la autenticación mediante firma y certificados digitales, pero se diferencia de SSL en que se implementa a nivel de aplicación. Se puede identificar una página web con este protocolo viendo la extensión .shtml en lugar de .html como las páginas normales.

El mecanismo de conexión mediante S-HTTP, lleva una serie de pasos parecidos a los usados en SSL, en los que cliente y servidor se intercambian una serie de datos formateados que incluyen los algoritmos criptográficos, longitudes de clave y algoritmos de compresión a usar durante la comunicación segura.

En cuanto a estos algoritmos, lo usados normalmente son RSA para intercambio de claves simétricas, MD2, MD5 o NIST-SHS como funciones hash de resumen, DES, IDEA, RC4 o CDMF como algoritmos simétricos y PEM o PKCS-7 como algoritmos de encapsulamiento.

A diferencia de SSL, el protocolo S-HTTP está integrado con HTTP, actuando a nivel de aplicación, negociándose los servicios de seguridad a través de cabeceras y atributos de página, por lo que los servicios S-HTTP están sólo disponibles para el protocolo HTTP. Recordemos que SSL puede ser usado por otros protocolos diferentes de HTTP, ya que se integra a nivel de shocked.

A.5 Protocolo SET

En febrero de 1996 un grupo de empresas del sector financiero, informático y de seguridad (Visa International, MasterCard, Microsoft, Nestcape, IBM, RSA, etc.) anunciaron el desarrollo de una nueva tecnología común destinada a proteger las compras a través de redes abiertas como Internet basadas en el uso de tarjetas de crédito. Esta nueva tecnología se conoce con el nombre de Secure Electronic Transatrions (Transacciones Electrónicas Seguras), y ha sido creada exclusivamente para la realización de comercio electrónico usando tarjetas de crédito.

SET se basa en el uso de certificados digitales para asegurar la perfecta identificación de todas aquellas partes que intervienen en una transacción on-line basada en el uso de tarjetas de pago, y en el uso de sistemas criptográficos de clave pública para proteger el envío de los datos sensibles en su viaje entre los diferentes servidores que participan en el proceso. Con ello se persigue mantener el carácter estrictamente confidencial de los datos, garantizar la integridad de los mismos y autenticar la legitimidad de las entidades o personas que participan en la transacción, creando así un protocolo estándar abierto para la industria que sirva de base a la expansión del comercio electrónico por Internet.

Las especificaciones del protocolo SET 1.0 se hicieron públicas el 31 de mayo de 1997, y se pueden encontrar en el sitio web oficial de SETco, organismo encargado de homologar los módulos de programación y los certificados desarrollados por empresas privadas que se usen en implementaciones del protocolo SET.

A.6 OSA (Open Systen Authentication)

Es un mecanismo de autenticación definido por el estándar 802.11 para autenticar todas las tramas que recibe. El problema que tiene es que no realiza ninguna comprobación de la estación cliente. Además, las tramas de gestión son enviadas sin encriptar, por lo que lo hace un mecanismo poco fiable.

A.7 CNAC (Close Network Access Control)

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo a aquellas estaciones cliente que conozcan el nombre de la red (SSID), actuando este como contraseña.

A.8 ACL (Access Control List)

Utiliza, como medio de autenticación, las direcciones MAC de las estaciones cliente, permitiendo el acceso a aquellos clientes cuyas MAC consten en la Lista de Control de Acceso.

A.9 SKA (Shared Key Authentication)

Se basa en que todas las estaciones autorizadas de la red compartan la misma clave. Para demostrar que una estación conoce la clave encripta un “challenge text”.

A.10 SSID (Service Set Identifier)

Se utiliza el identificador de la red (cadena de 32 caracteres como máximo) como clave. Si no se conoce el SSID no se puede conectar a la red.

Anexo A

Programa desarrollado para la obtención de la llave de encriptado cuando se utiliza el protocolo WEP.

ClaveWep.pl

```
#!/usr/bin/perl
# Facultad de Ingeniería.
# Programa que obtiene la llave de encriptado WEP/RC4
# Basado en el trabajo de Scott Fluhrer, Itsik Mantin, and Adi Shamir.
#
# El script crea un archivo con una lista de los Ivs y el primer byte encriptado
# para deducir que clave se ha utilizado.

$i=0;
$j=0;
$ik=0;
$x=0;

# La primera trama debe de ser el primer byte de texto plano en el paquete WEP
@text = (0xaa);

if (!-f "IVFile.log") {
        die("Error :\nNo se encontro el archivo IVFile.log\n");

}
# Se abre el archivo log y se comienza a analizar la informacion de los Ivs que contiene
open (IVFILE, "IVFile.log");
@IVList=<IVFILE>;
close (IVFILE);

$keysize=$IVList[0];
chomp($keysize);
splice(@IVList, 0, 1);

$bitsize=$keysize*8;
print("Keysize = $keysize \[$bitsize bits\]\n");

for ($B=0; $B < $keysize; $B++) {
        # Inicia el arreglo que de manera estadistica tomara cada uno de los valores
        # de la clave WEP
        for ($i=0; $i < 256; $i++) {
                $stat[$i]=0;
        }

        foreach $IVRec (@IVList) {

                @IV=split(" ",$IVRec);
                $key[0]=$IV[0];
                $key[1]=$IV[1];
                $key[2]=$IV[2];
              $encr=$IV[3];

#               if ($key[0] eq $B+3) {
```

```
# Procedimiento que busca los Ivs que se igualan con la llave del primer byte

                        $i=0;
                        $j=0;
                        $ik=0;

                        for ($i=0; $i<256; $i++) {
                                $S[$i]=$i;
                        }

                        # 0 to 3+K[b]
                        for ($i=0; $i< $B + 3; $i++) {
                                $j=($j+$S[$i]+$key[$i]) % 256;
                                $temp = $S[$i];
                                $S[$i] = $S[$j];
                                $S[$j] = $temp;
                                if ($i eq 1) {
                                        $S1[0]=$S[0];
                                        $S1[1]=$S[1];
                                }

                        }
                        $X=$S[1];
                        if ($X < $B + 3) {
                                if ($X+$S[$X] eq $B + 3) {
                                if ($S[0] ne $S1[0] || $S[1] ne $S1[1]) {
                                                #print("Throwaway IV $IV[0], $IV[1], $IV[2]\n");
                                        }

# Procedimiento para aplicar la operacion XOR en los bytes que llegan y salen para obtener S[3]
# Concatenamos S[3] con el valor de J y substraemos  (5+x+S[3]) para obtener el valor de K
                                        $S3Calc = $encr ^ $text[0];
                                        $leaker = $S3Calc-$j-$S[$i] %256;
                                        $stat[$leaker]++;
                                }
                        }
        $max=0;
        $count=0;
        foreach $rank (@stat) {
                if ($rank > $max) {
                        $max=$rank;
                        $winner=$count;
                }
                $count++;
        }
#}
}
print("$clave ");
push (@key, $clave);
}

        print("\n");
```

Anexo B

Octetos que utilizan los fabricantes para identificar ruteadores y tarjetas inalámbricas.

Octetos / Fabricante
00:00:00 Xerox
00:00:01 Xerox
00:00:02 Xerox
00:00:03 Xerox
00:00:04 Xerox
00:00:05 Xerox
00:00:06 Xerox
00:00:07 Xerox
00:00:08 Xerox
00:00:09 Xerox
00:00:0C Cisco
00:00:95 Ericsson/Sony
00:00:AA Xerox
00:00:E2 Acer
00:00:E8 Accton
00:00:F0 Samsung
00:00:FF Camtec
00:01:02 3Com
00:01:03 3Com
00:01:24 Acer
00:01:42 Cisco
00:01:43 Cisco
00:01:4A Ericsson/Sony
00:01:4C Berkeley
00:01:63 Cisco
00:01:64 Cisco
00:01:96 Cisco
00:01:97 Cisco
00:01:C7 Cisco
00:01:C9 Cisco
00:01:EC Ericsson/Sony
00:01:F4 Enterasys
00:01:F9 Global
00:02:07 Global
00:02:16 Cisco
00:02:17 Cisco
00:02:2D Proxim ORiNOCO
00:02:4A Cisco
00:02:4B Cisco
00:02:6F Senao
00:02:7D Cisco
00:02:7E Cisco
00:02:88 Global
00:02:8A Ambit
00:02:9C 3Com
00:02:A5 Compaq
00:02:B3 Intel
00:02:B9 Cisco
00:02:BA Cisco
00:02:DD Bormax
00:02:EE Nokia
00:02:FC Cisco
00:02:FD Cisco
00:03:2F Global
00:03:31 Cisco
00:03:32 Cisco
00:03:47 Intel
00:03:6B Cisco
00:03:6C Cisco
00:03:93 Apple
00:03:9F Cisco
00:03:A0 Cisco
00:03:E3 Cisco
00:03:E4 Cisco
00:03:FD Cisco
00:03:FE Cisco

Octetos / Fabricante
00:03:FF Microsoft
00:04:0B 3Com
00:04:0D Avaya
00:04:1F Ericsson/Sony
00:04:25 Atmel
00:04:27 Cisco
00:04:28 Cisco
00:04:31 Global
00:04:4D Cisco
00:04:4E Cisco
00:04:5A Linksys
00:04:6D Cisco
00:04:6E Cisco
00:04:9A Cisco
00:04:9B Cisco
00:04:C0 Cisco
00:04:C1 Cisco
00:04:C6 Yamaha
00:04:DD Cisco
00:04:DE Cisco
00:04:E2 SMC
00:04:E3 Accton
00:05:00 Cisco
00:05:01 Cisco
00:05:02 Apple
00:05:1A 3Com
00:05:31 Cisco
00:05:32 Cisco
00:05:3C Xircom
00:05:3D Proxim ORiNOCO
00:05:5D D-Link
00:05:5E Cisco
00:05:5F Cisco
00:05:73 Cisco
00:05:74 Cisco
00:05:75 CDS
00:05:86 Lucent (WaveLAN)
00:05:9A Cisco
00:05:9B Cisco
00:05:DC Cisco
00:05:DD Cisco
00:06:25 Linksys
00:06:28 Cisco
00:06:2A Cisco
00:06:52 Cisco
00:06:53 Cisco
00:06:6E Delta(Netgear)
00:06:7C Cisco
00:06:8C 3Com
00:06:C1 Cisco
00:06:D6 Cisco
00:06:D7 Cisco
00:06:EB Global
00:07:0D Cisco
00:07:0E Cisco
00:07:4F Cisco
00:07:50 Cisco
00:07:84 Cisco
00:07:85 Cisco
00:07:B3 Cisco
00:07:B4 Cisco
00:07:E9 Intel
00:07:EB Cisco
00:07:EC Cisco
00:08:02 Compaq
00:08:0F Proxim(WaveLAN)

Octetos / Fabricante
00:08:20 Cisco
00:08:21 Cisco
00:08:7C Cisco
00:08:7D Cisco
00:08:A3 Cisco
00:08:A4 Cisco
00:08:C2 Cisco
00:08:C7 Compaq
00:08:E2 Cisco
00:08:E3 Cisco
00:09:11 Cisco
00:09:12 Cisco
00:09:43 Cisco
00:09:44 Cisco
00:09:5B Netgear
00:09:7B Cisco
00:09:7C Cisco
00:09:B6 Cisco
00:09:B7 Cisco
00:09:E1 Gemtek
00:09:E8 Cisco
00:09:E9 Cisco
00:0A:04 3Com
00:0A:27 Apple
00:0A:41 Cisco
00:0A:42 Cisco
00:0A:5E 3Com
00:0A:8A Cisco
00:0A:8B Cisco
00:0A:95 Apple
00:0A:B7 Cisco
00:0A:B8 Cisco
00:0A:D9 Ericsson/Sony
00:0A:E9 AirVast
00:0A:F3 Cisco
00:0A:F4 Cisco
00:0B:45 Cisco
00:0B:46 Cisco
00:0B:5F Cisco
00:0B:60 Cisco
00:0B:89 Global
00:0B:AC 3Com
00:0B:BE Cisco
00:0B:BF Cisco
00:0B:C5 SMC
00:0B:CD Compaq
00:0B:FC Cisco
00:0B:FD Cisco
00:0B:FF Berkeley
00:0C:1E Global
00:0C:30 Cisco
00:0C:31 Cisco
00:0C:41 Linksys
00:0C:85 Cisco
00:0C:86 Cisco
00:0C:CA Global
00:0C:CC Bluesoft
00:0C:CE Cisco
00:0C:CF Cisco
00:0C:F1 Intel
00:0D:28 Cisco
00:0D:29 Cisco
00:0D:3A Microsoft
00:0D:54 3Com
00:0D:65 Cisco
00:0D:66 Cisco

00:0D:72 2Wire
00:0D:88 D-Link
00:0D:93 Apple
00:0D:B5 Global
00:0D:BC Cisco
00:0D:BD Cisco
00:0D:EC Cisco
00:0D:ED Cisco
00:0E:07 Ericsson/Sony
00:0E:0C Intel
00:0E:35 Intel
00:0E:38 Cisco
00:0E:39 Cisco
00:0E:6A 3Com
00:0E:83 Cisco
00:0E:84 Cisco
00:0E:D6 Cisco
00:0E:D7 Cisco
00:0E:ED Nokia
00:0F:23 Cisco
00:0F:24 Cisco
00:0F:34 Cisco
00:0F:35 Cisco
00:0F:3D D-Link
00:0F:5B Delta(Netgear)
00:0F:66 Cisco
00:0F:8F Cisco
00:0F:90 Cisco
00:0F:B3 Premax
00:0F:B5 Netgear
00:0F:CB 3Com
00:0F:DE Ericsson/Sony
00:0F:E2 3Com
00:0F:F7 Cisco
00:0F:F8 Cisco
00:10:07 Cisco
00:10:0B Cisco
00:10:0D Cisco
00:10:11 Cisco
00:10:14 Cisco
00:10:1F Cisco
00:10:29 Cisco
00:10:2F Cisco
00:10:4B 3Com
00:10:54 Cisco
00:10:5A 3Com
00:10:79 Cisco
00:10:7A Ambicom
00:10:7B Cisco
00:10:A4 Xircom
00:10:A6 Cisco
00:10:B3 Nokia
00:10:B5 Accton
00:10:E3 Compaq
00:10:E7 BreezeNet
00:10:F6 Cisco
00:10:FF Cisco
00:11:11 Intel
00:11:20 Cisco
00:11:21 Cisco
00:11:24 Apple
00:20:14 Global
00:20:7B Intel
00:20:88 Global
00:20:A6 Proxim(WaveLAN)
00:20:AF 3Com
00:20:D8 NetWave-Bay
00:20:E0 Premax
00:26:54 3Com
00:30:19 Cisco
00:30:1E 3Com
00:30:24 Cisco
00:30:40 Cisco
00:30:65 Apple
00:30:6D Lucent (WaveLAN)
00:30:71 Cisco
00:30:78 Cisco
00:30:7B Cisco
00:30:80 Cisco
00:30:85 Cisco
00:30:94 Cisco
00:30:96 Cisco
00:30:98 Global
00:30:A3 Cisco
00:30:AB Delta(Netgear)
00:30:B6 Cisco
00:30:B8 Delta(Netgear)
00:30:BD Belkin
00:30:F1 Accton
00:30:F2 Cisco
00:40:05 Ani
00:40:0B Cisco
00:40:27 SMC
00:40:33 Addtron
00:40:43 Nokia
00:40:96 Aironet
00:40:AE Delta(Netgear)
00:50:04 3Com
00:50:0B Cisco
00:50:0F Cisco
00:50:14 Cisco
00:50:18 Adv
00:50:2A Cisco
00:50:3E Cisco
00:50:50 Cisco
00:50:53 Cisco
00:50:54 Cisco
00:50:73 Cisco
00:50:80 Cisco
00:50:8B Compaq
00:50:98 Global
00:50:99 3Com
00:50:A0 Delta(Netgear)
00:50:A2 Cisco
00:50:A7 Cisco
00:50:BA D-Link
00:50:BD Cisco
00:50:D1 Cisco
00:50:DA 3Com
00:50:E2 Cisco
00:50:E4 Apple
00:50:F0 Cisco
00:50:F2 Microsoft
00:50:F3 Global
00:60:08 3Com
00:60:09 Cisco
00:60:1D Lucent (WaveLAN)
00:60:2F Cisco
00:60:3E Cisco
00:60:47 Cisco
00:60:5C Cisco
00:60:67 Acer
00:60:70 Cisco
00:60:83 Cisco
00:60:8C 3Com
00:60:97 3Com
00:60:B3 Z-Com
00:60:D2 Lucent
00:80:37 Ericsson/Sony
00:80:5F Compaq
00:80:C8 D-Link
00:90:04 3Com
00:90:0C Cisco
00:90:0E Handlink
00:90:21 Cisco
00:90:27 Intel
00:90:2B Cisco
00:90:4B Gemtek
00:90:5F Cisco
00:90:6C Global
00:90:6D Cisco
00:90:6F Cisco
00:90:86 Cisco
00:90:92 Cisco
00:90:A6 Cisco
00:90:AB Cisco
00:90:B1 Cisco
00:90:BF Cisco
00:90:D1 Addtron
00:90:D9 Cisco
00:90:E6 Acer
00:90:F2 Cisco
00:A0:24 3Com
00:A0:40 Apple
00:A0:60 Acer
00:A0:8E Nokia
00:A0:C9 Intel
00:A0:DE Yamaha
00:A0:F8 Symbol
00:AA:00 Intel
00:AA:01 Intel
00:AA:02 Intel
00:B0:4A Cisco
00:B0:64 Cisco
00:B0:8E Cisco
00:B0:C2 Cisco
00:C0:03 Global
00:C0:49 U.S. Robotics
00:C0:AC Ambit
00:D0:06 Cisco
00:D0:58 Cisco
00:D0:59 Ambit
00:D0:63 Cisco
00:D0:77 Lucent
00:D0:79 Cisco
00:D0:90 Cisco
00:D0:96 3Com
00:D0:97 Cisco
00:D0:9E 2Wire
00:D0:AB Netgear
00:D0:B7 Intel
00:D0:BA Cisco
00:D0:BB Cisco
00:D0:BC Cisco
00:D0:C0 Cisco
00:D0:D3 Cisco
00:D0:D8 3Com
00:D0:E4 Cisco
00:D0:FF Cisco
00:E0:03 Nokia
00:E0:14 Cisco
00:E0:1E Cisco
00:E0:34 Cisco
00:E0:38 WaveLAN
00:E0:4F Cisco
00:E0:78 Berkeley
00:E0:85 Global
00:E0:8F Cisco
00:E0:A3 Cisco
00:E0:B0 Cisco
00:E0:E4 U.S. Robotics
00:E0:F7 Cisco
00:E0:F9 Cisco
00:E0:FE Cisco
02:60:8C 3Com
02:C0:8C 3Com
08:00:05 Symbol
08:00:07 Apple
08:00:37 Xerox
08:00:46 Ericsson/Sony
08:00:4E 3Com
08:00:72 Xerox

Glosario

AES: Advanced Encryption Standard, “Estándar de encriptación avanzado”.

AirSnort: Herramienta para redes inalámbricas que determina claves de encriptación.

Ciphertext: Texto cifrado.

ClearText: Texto antes de ser cifrado o después de ser decodificado.

CRC: Código de Redundancia Cíclica.

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance, “Acceso múltiple evitando colisiones”.

CSMA/CD: Carrier Sense Multiple Access with Collision Detection, “Acceso múltiple censando portadora con detección de colisión”.

DBPSK: Differential Binary Phase Shift Keying, “Fase binaria diferencial en cambio de llave”.

DQPSK: Differential Quadrature Phase Shift Keyed, “Fase cuadratura diferencial en cambio de llave”.

DSL: Digital Subscriber Line, “Línea de abonado digital”. Término utilizado para referirse a todas las tecnologías que proveen una conexión digital sobre la línea la red telefónica local.

HomeRF: Referencia cacera.

ICV: Integrity Check Value, “Valor para la verificación de la Integridad”.

IP: Internet protocol, “Protocolo de internet”.

IP SPOOFING: Suplantación de IP. Consiste básicamente en sustituir la IP origen de un paquete. **IV**: El vector de Inicialización.

LAN: Local Area Network “Red de área Local”.

MAC: Media Access Control, “control de acceso al medio”.

Malware: Programa o archivo dañino para una sistema.

MD5: *Message-Digest Algorithm 5*, “Algoritmo de Resumen del Mensaje 5”.

OFDM: Orthogonal Frecuency Division Multiplexing, “Multiplexado ortogonal por división de frecuencia”.

OSI: Open System Interconection, “Interconexión de Sistemas Abiertos”.

PRNG: Pseudos Random Number Generator, “Generador de números pseudos aleatorios”.

RADIUS (Remote Access Dial-In User Server): Es un protocolo de autentificación y autorización para aplicaciones de acceso a la red o movilidad IP.

RC4: *Rivest Cipher 4* (sistema de cifrado de flujo *Stream cipher)*.

RDSI o **ISDN:** Red Digital de Servicios Integrados.

Smtp: Simple Mail Transfer Protocol, “Protocolo de transferencia de correo simplificado”.

Sniffer: Un sniffer es un programa que captura tramas de red.

SSID: service set identifier, “Conjunto de servicios para la identificación”.

TCP/IP: Transfer Control Protocol over Internet Protocol, “Protocolos de control de transferencia sobre los protocolos de internet”.

WEP: Wired Equivalent Privacy, “Privacidad equivalente al cableado”.

WEPCrack: Programa que se utiliza para el calculo de claves de encriptación.

WiFi: Acrónimo sin significado determinado aunque en algunos textos se define como Wireless Fidelity, “Fidelidad inalámbrica”.

WPA: Wireless Protected Access, “Acceso inalambrico protegido”.

Bibliografía

BARNES CHRISTIAN, BAUTTS TONY, LLOYD DONALD and OUELLET ERIC
Hack Proofing your Wireless Network (Protect your wireless network from attack).
Sysgress Publishing Inc. 800 Hingham Street Rockland, MA 02370. 2002.

CASTRO ELIZABETH
Perl y CGI. Segunda edición.
Pearson Educación. S.A. Madrid 2001.

ENGST ADAM and FLEISHMAN GLENN
The Wireless Networking Starter kit. Second edition.
Peachpit Press 1249 Eighth Street Berkeley CA. 2004.

GAST MATTHEW
802.11 Wireless Networks: The Definitive Guide
O'Reilly & Associates, Inc.1005 Gravenstein Highway North Sebastopol, CA 95472

MACAULAY TYSON,
Hardening IEEE 802.11 wireless networks
EWA Canada. 2002.

MALLICK MARTYN
Mobile and Wireless Design Essentials
Wiley publishing, Inc. Indianapolis, Indiana. 2003.

MILLER MICHAEL.
Discovering Bluetooth
SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501. 2001.

PAUL, HELTZEL.
Complete home wireless networking : Windows XP edition.
Prentice Hall PTR. 2003.

SIKORA AXEL
Wireless LAN
Addison-Wesley Verlag, 2001.

WEISMAN CARL J.
The Essential Guide to RF and Wireless. Second edition.
Prentice Hall PTR, Upper Saddle River, NJ 07458. 2002.

WHEAT JEFFREY, HISER RANDY, TUCKER JACKIE and NEELY ALICIA
Designing a Wireless Network. Understand how wireless communication Works
Syngress Publishing, Inc. 800 Hingham Street Rockland, MA 02370. 2001

[1] IEEE 802.11x Wireless LANs
3Com Corporation 5400 Bayfront Plaza P.O. Box 58145 Santa Clara, CA.

[2] Cifrado RC4
http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html

[3] ISAAC Internet Security, Applications, Authentication and Cryptography
http://www.isaac.cs.berkeley.edu/

[4] iDefense
http://labs.idefense.com/labs.php

[5] “Using the Fluhrer, Mantin and Shamir attack to Break WEP"
http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/stubbl.pdf#search=%22Using%20the%20Fluhrer%2C%20Mantin%20and%20Shamir%20attack%20to%20Break%20WEP%22

[6] "intercepting mobile Communications: The insecurity of 802.11"
http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf#search=%22intercepting%20mobile%20Communications%3A%20The%20insecurity%20of%20802.11%22

[7] Weaknesses in the Key Scheduling Algorithm of RC4
http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf#search=%22Scott%20Fluhrer%2C%20Itsik%20Mantin%20Adi%20Shamir%20%22

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

El WiFi más practico.
PC actual No. 168 pp. 39

Protocolos 802.11, sin ninguna atadura.
PC actual No. 168 pp. 40 - 45.

Detección de una red. “Jugar al escondite”
PC actual No. 168 pp. 46 – 49.

Cifrado WPA, Evolución segura.
PC actual No. 168 pp. 60 - 64.

http://sky.prohosting.com/redwifi/

http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml

http://www.microsoft.com/latam/technet/seguridad/articulos/ddmmyy_reforzamiento_cifrado_inalambrico.asp

http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml