SEGURIDAD WiFi

Asignatura: Redes y Sistemas de Radio
Curso: 2004/2005

Antonio Bernier Moreno
Víctor M. Vega García
Diego Martínez Lomas

ÍNDICE

RESUMEN

Actualmente las redes inalámbricas de área local (WLAN) basadas en los estándares 802.11 con el sello WiFi están en pleno apogeo. Surgiendo inicialmente como una solución ante nuevas necesidades de movilidad, sus cada vez mejores prestaciones junto con su gran facilidad de instalación han conseguido situar esta alternativa entre las más empleadas por los usuarios.

A lo largo de este texto se tratará de describir brevemente la infraestructura WiFi, para profundizar en sus aspectos de seguridad (autenticación, control de accesos y confidencialidad).
En el apartado de seguridad se describirá la evolución seguida en este campo: desde WEP hasta WPA2. Se explicará en detalle la solución inicial adoptada: WEP y porqué actualmente no se trata de una buena alternativa. Se describirán sus vulnerabilidades y cómo aprovecharlas con el uso de las herramientas adecuadas. Afortunadamente las condiciones actuales de seguridad no son las mismas con la aparición (2004) de la revisión 802.11i del estándar, la cual se debe considerar como algo importante en la seguridad WiFi y que en definitiva presenta una oferta SEGURA, si se configura adecuadamente.

1. PANORAMA GENERAL Y CONCEPTOS BÁSICOS

1.1. Introducción

Una red de área local inalámbrica puede definirse como a una red de alcance local que tiene como medio de transmisión el aire. Al igual que las redes tradicionales cableadas vamos a clasificar las redes inalámbricas en tres categorías:

• **WAN/MAN** (Wide Area Network/Metropolitan Area Network).

• **LAN** (Local Area Network).

• **PAN:** El concepto de red inalámbrica de área personal o WPAN (Wireless Personal Area Network) se refiere a una red sin cables que se extiende a un espacio de funcionamiento personal o POS (Personal Operating Space) con un radio de 10 metros. (Personal Area Network).

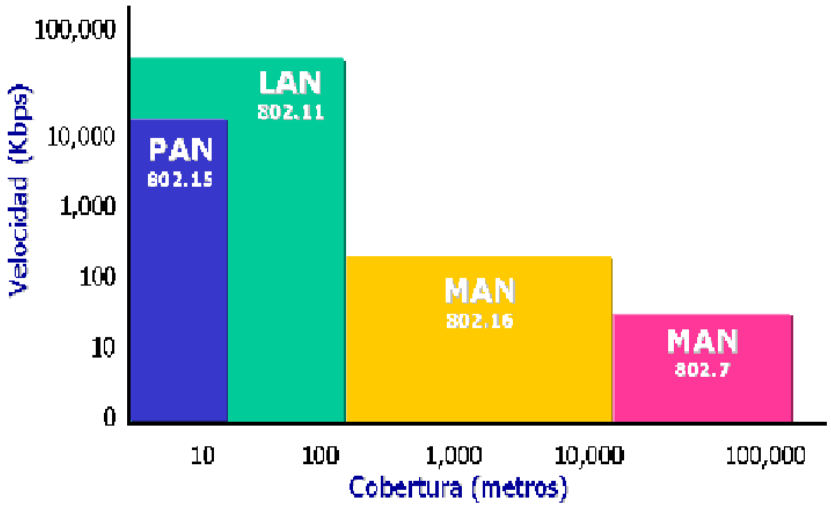


Figura 1: Comparativa Distancia/Velocidad de tipos de redes

1.2. Evolución

WiFi (Wireless Fidelity) es un nombre comercial desarrollado por un grupo de comercio industrial llamado WiFi Alliance (Inicalmente: 3Com – Aironet [hoy parte de CISCO] – Harris – Lucent – Nokia y Symbol technologies, hoy más de 150 miembros), el nombre "oficial" de esta alianza es **WECA** (Wireless Ethernet Compatibility Alliance) y son los primeros responsables de 802.11b.

WiFI describe los productos de WLAN basados en los estándares 802.11 y está pensado en forma más "Amigable" que la presentación eminentemente técnica que ofrece IEEE. Se podría llegar a discutir si cubre o no todo lo que ofrece 802.11 o no, pues alguno de ellos podría ser puesto en duda, pero a los efectos de este texto, se hará más referencia a lo que establece 802.11, sin detenerse en estas diferencias.

La web de esta alianza es: www.wi-fi.org , www.wifi-alliance.net

En estos links se puede también consultar el estado “On Line” de los productos que se encuentran certificados, el path completo de esta consulta es:

http://www.wi-fi.org/OpenSection/Certified_Products.asp?TID=2

El estándar **802.11** de IEEE se publica en junio 1997, luego de seis años de proceso de creación. Propone velocidades de 1 y 2Mbps y un rudimentario sistema de cifrado (el **WEP**: Wired Equivalent Privacy), opera en 2,4 GHz con RF e IR. Aunque WEP aún se sigue empleando, ha sido totalmente desacreditado como protocolos seguro.

En septiembre de 1999 salen a la luz el estándar **802.11b** que ofrece 11Mbps y el **802.11a** que ofrece 54 Mbps, si bien los productos de la primera aparecieron en el mercado mucho antes. Algunos fabricantes ofrece velocidades de 72 e incluso 108 Mbps. Estos procesos, lo logran mediante la “Vinculación de canales”, es decir, dos canales son multiplexados juntos empleando el total de velocidad de la suma de ambos. Esto si bien es favorable aparentemente, tiene las desventajas de no respetar el estándar y de sacrificar la mitad de los canales de 802.11a.

La familia 802.11, hoy se encuentra compuesta por los siguientes estándares:

- **802.11a:** (5,1-5,2 Ghz, 5,2-5,3 Ghz, 5,7-5,8 GHz), 54 Mbps. OFDM: Multiplexación por división de frecuencias ortogonal
- **802.11b:** (2,4-2,485 GHz), 11 Mbps.
- 802.11c: Define características de AP como Bridges.
- 802.11d: Múltiples dominios reguladores (restricciones de países al uso de determinadas frecuencias).
- 802.11e: Calidad de servicio (QoS).
- 802.11f: Protocolo de conexión entre puntos de acceso (AP), protocolo IAPP: Inter Access Point Protocol.
- **802.11g**: (2,4-2,485 GHz), 36 o 54 Mbps. OFDM: Multiplexación por división de frecuencias ortogonal. Aprobado en 2003 para dar mayor velocidad con cierto grado de compatibilidad a equipamiento 802.11b.
- 802.11h: DFS: Dynamic Frequency Selection, habilita una cierta coexistencia con HiperLAN y regula también la potencia de difusión.
- **802.11i:** Seguridad (aprobada en Julio de 2004).
- 802.11j: Permitiría armonización entre IEEE (802.11), ETSI (HiperLAN2) y ARIB (HISWANa).
- 802.11m: Mantenimiento redes wireless.

Quizás el tema más importante a destacar es la posibilidad de expansión de 802.11. El incremento constante de mayores velocidades, hace que los 11 Mbps de 802.11b, estén quedando pequeños. La migración natural es hacia 802.11g, pues sigue manteniendo la frecuencia de

2,4GHz, por lo tanto durante cualquier trancisión en la que deban convivir, ambos estándares lo permiten. En cambio si se comienzan a instalar dispositivos 802.11a, los mismos no permiten ningún tipo de compatibilidad con 802.11b, pues operan en la banda de 5 GHz.

Para acotar únicamente el tema de seguridad, se tratarán sólo 802.11a, b g y 802.11i.

Hoy en día se puede decir que existen tres estándares de WLAN:

-**HomeRF:** Es una iniciativa lanzada por Promix, principalmente en EEUU y orientada exclusivamente al mercado residencial. Tiene sus bases en los estándares de teléfono digital inalámbrico mejorado (DECT)

-**BlueTooth:** Lo inició IBM, orientado al mercado comercial/ventas, y a la interconectividad de elementos de hardware. En realidad no compite con 802.11, pues tiene la intención de ser una estándar con alcance nominal de 1 a 3 metros y a su vez no supera los 1,5 Mbps

-**802.11:** Cubre todo el espectro empresarial.

Una iniciativa que se debe mencionar también es **HiperLAN** en sus versiones 1 y 2. Se trata de una verdadera analogía inalámbrica para ATM. Fue un competidor de 802.11 que opera en la frecuencia de 5 GHz y gozó del apoyo de compañías como Ericsson, Motorola, Nokia; Panasonic y Sony, se llegaron a crear regulaciones por parte de ETSI al respecto, pero no se logró imponer y hoy en día está prácticamente en desuso. En lo particular recuerda mucho a la batalla entre ATM y Ethernet (Fast ethernet, giga ethernet....).

Estándar	Velocidad Máxima	Interface de Aire	Ancho de Banda de Canal	Frecuencia
802.11b	11 Mbps	DSSS	25 MHz	2,4 GHz
802.11a	54 Mbps	OFDM	25 MHz	5,0 GHz
802.11g	54 Mbps	OFDM/DSSS	25 MHz	2,4 GHz
HomeRF2	10 Mbps	FHSS	5 MHz	2,4 GHz
HiperLAN2	54 Mbps	OFDM	25 MHz	5,0 GHz
5-UP	108 Mbps	OFDM	50 MHz	5,0 GHz

Tabla comparativa de estándares WLAN

DSSS: Direct Sequence Spread Spectrum
OFDM: Orthogonal Frequency Division Multiplexing
FHSS: Frequency Hopping Spread Spectrum
5-UP: 5-GHz Unified Protocol (5-UP), Protocolo Unificado de 5 GHz propuesto por Atheros Communications

Tabla resumen:

Estándares Wireless			
Estándar	**802.11b**	**802.11a**	**802.11g**
Aprobado IEEE	Julio 1999	Julio 1999	Junio del 2003
Popularidad	Adoptado masivamente	Nueva tecnología, crecimiento bajo	Nueva tecnología, con un rápido crecimiento
Velocidad	Hasta 11 Mbps	Hasta 54 Mbps	
Coste	Barato	Relativamente caro	Barato
Modulación	CCK	OFDM	OFDM y CCK
Frecuencia	2.4 - 2.497 Ghz	5.15 - 5.35 Ghz 5.425 - 5.675 Ghz 5.725 - 5.875 Ghz	2.4 - 2.497 Ghz
Cobertura	Buena cobertura, unos 300 - 400 metros con buena conectividad con determinados obstáculos	Cobertura baja, unos 150 metros, con mala conectividad con obstáculos	Buena cobertura, unos 300 - 400 metros con buena conectividad con determinados obstáculos
Acceso Público	El número de Hotspots crece exponencialmente	Ninguno en este momento.	Compatible con los HotSpots actuales de 802.11b. El paso a 802.11g no es traumático para los usuarios
Compatibilidad	Compatible con 802.11g, no es compatible con 802.11a	Incompatible con 802.11b y con 802.11g	Compatible con 802.11b, no es compatible con 802.11a
Modos de datos	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps 6, 9, 12, 18, 24, 36, 48, 54 Mbps

A continuación se puede ver una gráfica con la relación entre la distancia (medida en pies, 1 pie = 0.3048 metros) y el ancho de banda que podemos usar en cada caso. Por supuesto las distancias pueden variar dependiendo de la potencia y los dBm radiados por la tarjeta de cada fabricante.

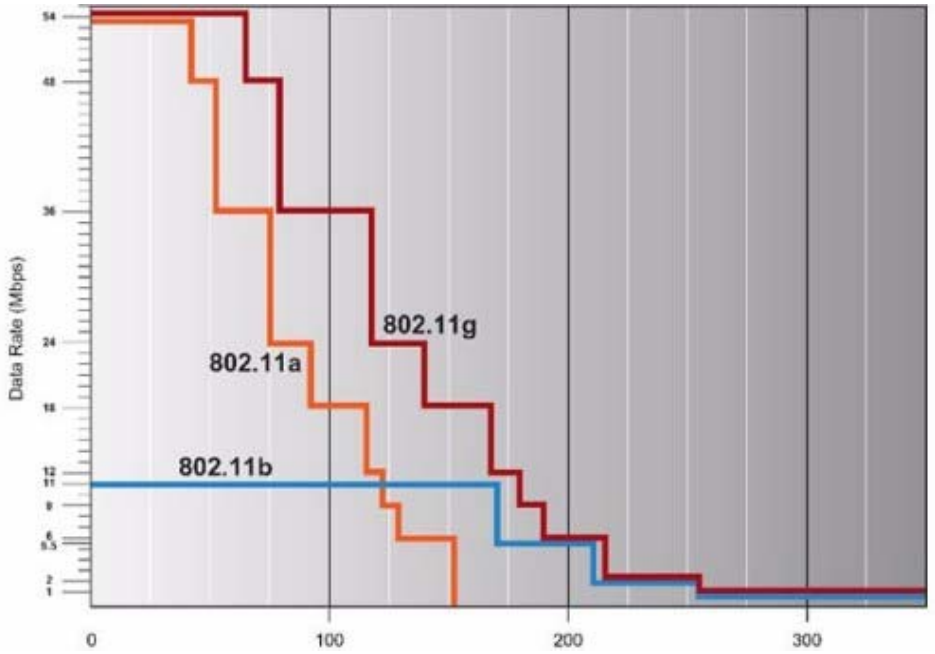


Figura 2. Comparativa entre 803.11b, 803.11a y 803.11g (Mbps/pies)

1.3. Ámbito de aplicación.

Las aplicaciones más típicas de las redes de área local que podemos encontrar actualmente son las siguientes:

• Implementación de redes de área local en **edificios históricos**, de difícil acceso y en general en entornos donde la solución cableada es inviable.

• Posibilidad de **reconfiguración de la topología** de la red sin añadir costes adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.

• Redes locales para **situaciones de emergencia o congestión de la red cableada**.

• Estas redes permiten el acceso a la información mientras el usuario se encuentra en **movimiento**. Habitualmente esta solución es requerida en hospitales, fábricas, almacenes...

• Generación de **grupos de trabajo eventuales** y **reuniones ad-hoc**. En estos casos no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo.

• En **ambientes industriales** con severas condiciones ambientales este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.

• Interconexión de redes de área local que se encuentran en **lugares físicos distintos**. Por ejemplo, se puede utilizar una red de área local inalámbrica para interconectar dos o más redes de área local cableadas situadas en dos edificios distintos.

1.4. Conceptos asociados a redes inalámbricas

1.4.1. Definiciones

• **Punto de acceso (AP/PA)**: Se trata de un dispositivo que ejerce básicamente funciones de puente entre una red Ethernet cableada con una red Wireless sin cables. Su configuración permite interconectar en muchos casos varios Puntos de Acceso para cubrir una zona amplia, pudiendo por si sólo proporcionar la configuración TCP / IP mediante un servicio DHCP. Se suele configurar en un único canal y admite la encriptación WEP, pudiendo enlazar un gran número de equipos entre ellos.

• **BEACON FRAMES:** Los Puntos de Acceso mandan constantemente anuncios de la red, para que los clientes móviles puedan detectar su presencia y conectarse a la red wireless. Estos "anuncios" son conocidos como BEACON FRAMES. Si *esnifamos* las tramas de una red wireless podremos ver que normalmente el AP manda el ESSID(explicado más abajo) de la red en los BEACON FRAMES, aunque esto se puede deshabilitar por software en la mayoría de los AP que se comercializan actualmente.

• **Tarjetas de red, o TR:** serán las que tengamos integradas en nuestro ordenador, o bien conectadas mediante un conector PCMCIA ó USB si estamos en un portátil o en un slot PCI si estamos en un ordenador de sobremesa.

• **ACL**. Significa Access Control List, y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

• **CNAC**. Significa Closed Network Access Control. Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.

• **SSID (Service Set Identification) y ESSID (Extended Service Set Identification)**: Este identificador suele emplearse en las redes wireless creadas con Infraestructura (metodología explicada más adelante). Se trata de un conjunto de Servicios que agrupan todas las conexiones de los clientes en un sólo canal. Suele denominar de manera familiar el nombre de la red wireless que da servicio o un Punto de Acceso. Cada red wireless tiene un ESSID (Extended Service Set Identifier), que la identifica.

El ESSID consta de cómo máximo 32 caracteres y es *case-sensitive*. Es necesario conocer el ESSID del AP para poder formar parte de la red wireless, es decir, el ESSID configurado en el dispositivo móvil tiene que concordar con el ESSID del AP.

• **BSSID (Basic Service Set Identification)**: Suele identificar una red creada Punto a Punto.

• **OSA vs SKA**. OSA (Open System Authentication), cualquier interlocutor es válido para establecer una comunicación con el AP. SKA (Shared Key Authentication) es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación, entonces, el dispositivo TR pide al AP autenticarse. El AP le envía una trama al TR, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.

• **Infraestructura**: Opción de las redes Wireless que sólo puede ser activada por Puntos de Acceso, y utilizada por tarjetas Wireless. Permite el enlace con más puntos de acceso y la agrupación de clientes. Admite el Roaming entre Puntos de Acceso.

• **Canal**: Un canal es una frecuencia de uso único y exclusivo dentro de la cobertura de un AP para sus clientes.

- **WEP (Wired Equivalet Privacy):** Es un protocolo de encriptación a nivel 2 para redes. Puede ser WEP64 (40 bits reales) WEP128 (104 bits reales) y hasta 256 (208 bits reales)

- **OSA (Open System Authentication):** Cualquiera puede formar parte de la red.

1.4.2. Topologías

a) Modo Ad-Hoc

Esta topología se caracteriza por que no hay Punto de Acceso (AP), las estaciones se comunican directamente entre si (peer-to-peer), de esta manera el área de cobertura está limitada por el alcance de cada estación individual.

Figura 3. Conexión *peer to peer*

b) Modo Infraestructura

Como mínimo se dispone de un Punto de Acceso (AP), las estaciones wireless no se pueden comunicar directamente, todos los datos deben pasar a través del AP. Todas las estaciones deben ser capaces de “ver” al AP.

Figura 4. Utilización de un *Punto de acceso*

Figura 5. Utilización de varios Puntos de acceso.

La mayoría de las redes wireless que podemos encontrar en las empresas utilizan modo infraestructura con uno o más Puntos de Acceso. El AP actúa como un HUB en una LAN, redistribuye los datos hacia todas las estaciones.

- **Descripción general de componentes de las mismas (topologías):**

-BSS (Basic Service Set): Es el bloque básico de construcción de una LAN 802.11. En el caso de tratarse de únicamente 2 estaciones ser denomina IBSS (Independent BSS), es lo que a menudo se denomina "Ad Hoc Netwok".

-DS (Distribution System): Es la arquitectura que se propone para interconectar distintos BSS. El **AP** es el encargado de proveer acceso al DS, todos los datos que se mueven entre BSS y DS se hacen a través de estos AP, como los mismos son también STA, son por lo tanto entidades direccionables.

-ESS (Extended Service Set): Tanto BSS como DS permiten crear wireless network de tamaño arbitrario, este tipo de redes se denominan redes ESS.

-La integración entre una red 802.11 y una No 802.11 se realiza mediante un **Portal**. Es posible que un mismo dispositivo cumpla las funciones de AP y Portal.

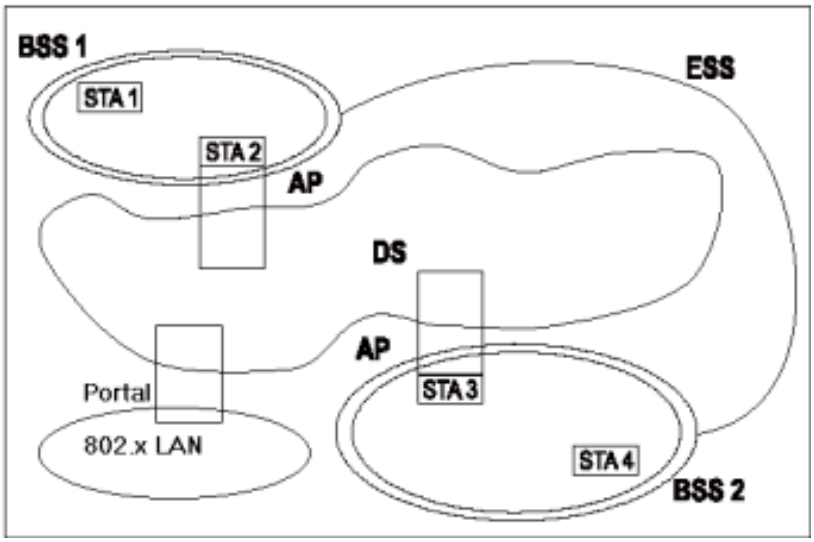


Figura 1 (Componentes de la arquitectura)

1.4.3. Modos de funcionamiento.

Todos los dispositivos, independientemente de que sean TRs o PAs tienen dos modos de funcionamiento. Tomaremos el modo Infraestructura como ejemplo:

a) Modo Managed, es el modo en el que el TR se conecta al AP para que éste último le sirva de concentrador. El TR sólo se comunica con el AP.

b) Modo Master. Este modo es el modo en el que trabaja el PA, pero en el que también pueden entrar los TRs si se dispone del firmware apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida.

Estos modos de funcionamiento nos sugieren que básicamente los dispositivos WiFi son todos iguales, siendo los que funcionan como APs realmente TRs a los que se les ha añadido cierta funcionalidad extra vía firmware o vía SW. Para realizar este papel se pueden emplear máquinas antiguas 80486 sin disco duro y bajo una distribución especial de Linux llamada LINUXAP/OPENAP.

Esta afirmación se ve confirmada al descubrir que muchos APs en realidad lo que tienen en su interior es una placa de circuitos integrados con un Firmware añadido a un adaptador PCMCIA en el cual se le coloca una tarjeta PCMCIA idéntica a las que funcionan como TR.

2. Seguridad en WiFi.

Los tres aspectos fundamentales que se deben tener en cuenta al diferenciar una red WiFi de una cableada, son:

- Autenticación

- Control de acceso

- Confidencialidad

2.1. Autenticación y control de acceso:

Los métodos que se emplean son los siguientes:

1. SSID (Service Set Identifier): Contraseña (**WEP**).El estándar 802.1x (que se menciona a continuación), permite un empleo de WEP para autenticación que se denominó "Dynamic WEP", que permite emplear este algoritmo como parte de 802.1x, de forma un poco más segura que el "WEP estático", pero la alianza WiFI recomienda no emplear ninguno de ellos en entornos seguros.
2. Seguridad por restricción de direccionamiento MAC: Permite restringir a un listado de direcciones, las que se pueden conectar y las que no.
3. Contraseñas no estáticas:
   - Periódicas:
   - OTP (One Time Password): Contraseñas de un solo uso, también conocidas como token flexibles.

4. 802.1x: Este estándar no fue presentado para WiFi, sino para el acceso seguro PPP (en tecnologías de cable). Una de las grandes características de WiFi es la de "no reinventar la rueda" y emplear todas las herramientas que ya existen y pueden prestar utilidad al mismo. 802.1x es uno de los mejores ejemplos de esto.
   La arquitectura 802.1x está compuesta por tres partes:

   - **Solicitante:** Generalmente se trata del cliente WiFi
   - **Autenticador:** Suele ser el AP, que actúa como mero traspaso de datos y como bloqueo
   hasta que se autoriza su acceso (importante esto último).
   - **Servidor de autenticación:** Suele ser un Servidor RADIUS (Remote Authentication Dial In User Service) o Kerberos, que intercambiará el nombre y credencial de cada usuario. El almacenamiento de las mismas puede ser local o remoto en otro servidor de LDAP, de base de datos o directorio activo.
   Otra de las grandes ventajas de emplear 802.1x es que el servidor de autenticación, permite también generar claves de cifrado OTP muy robustas, tema en particular que ya lo posiciona como imprescindible en una red WiFi que se precie de segura.
5. **802.11i:** El Task Group de IEEE 802.11i, se conformó en el año 2001, con la intención de analizar una arquitectura de seguridad más robusta y escalable, debido a la inminente demanda del mercado en este tema y en julio de 2004 aprobó este estándar. Por su parte la WiFi Alliance lo lanzó al mercado en septiembre de ese año.
   En forma resumida, este nuevo estándar, propone a 802.1x como protocolo de autenticación,

pudiendo trabajar con su referencia **EAP** (Extensible Authentication Protocol: **RFC 2284**), este último proporciona una gran flexibilidad (sobre todo a los fabricantes) en la metodología de autenticación.

Previo al estándar, Cisco Systems ofreció el primer tipo de autenticación que se denominó **LEAP** (Lightweight EAP), protocolo que inicialmente fue propietario de Cisco, pero en la actualidad lo emplean varios fabricantes. Cisco se está volcando hacia **PEAP** (se describe a continuación).

Por su parte Microsoft, inicialmente junto con Windows XP (hoy con todos sus SSOO), lanzó al mercado su protocolo denominado **EAP/TLS** (Extensible Authentication Protocol with Transport Layer Security - RFC: 2716), y fue aceptado por IEEE, se basa en certificados en lugar de contraseñas como credenciales de autenticación. Otros fabricantes han presentado **EAP/TTLS** (EAP with Tunneling Transport Layer Security), el cual realiza un túnel de nivel 2 entre el cliente y el AP, una vez establecido el túnel, EAP/TTLS opera sobre él, lo cual facilita el empleo de varios tipos de credenciales de autenticación que incluyen contraseñas y certificados, en realidad no deja de ser una variante de EAP/TLS.

La última variante es **PEAP** (Protected Extensible Authentication Protocol), inicialmente fue la versión "0" y ya está vigente la versión "1", el cual aplica una metodología muy similar a EAP/TTLS en cuanto al empleo de túnel y sobre el una amplia variedad de credenciales de autenticación, este último ya está soportado por los más importantes fabricantes. En general, se considera que PEAP es el método más seguro del momento. Este protocolo fue desarrollado por Microsoft, Cisco y RSA.

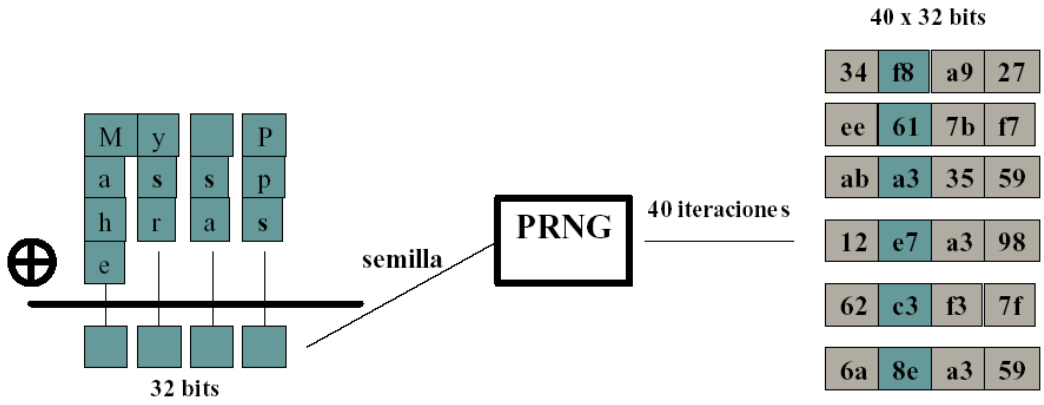
2.2. Cifrado

2.2.1. WEP

Emplea el algoritmo de cifrado de flujo **RC4** (Rivest Cipher 4), este algoritmo es una de las bases de RSA y cabe aclarar que es también empleado en el estándar SSL (Secure Socket Layer), se trata de un algoritmo robusto y veloz. Los problemas de WEP, no son por este algoritmo, sino por la debilidad de sus claves, tanto en 64, 128 (y hoy también 156) bits, de los cuales se deben excluir los 24 del VI (Vector de inicialización), hoy en día cualquier usuario con "Airsnort" lo descifra, sin tener ningún conocimiento especializado, incluso la metodología de "Airsnort" es pasiva, es decir, únicamente escucha tráfico, hoy existen herramientas mucho más potentes que operan de forma activa, que emplean varias técnicas para generar tráfico y basado en las respuestas de la red permiten acelerar exponencialmente el proceso. Estas últimas metodologías se denominan INDUCTIVAS y existen dos grandes familias: ataques de repetición y ataques de modificación de bits.

Existen también ataques de fuerza bruta, basados principalmente en técnicas de diccionario, las cuales en el caso de WEP, son de especial interés, pues el nombre de usuario viaja en texto plano, lo cual ofrece una gran ventaja para generar posibles claves.

2.2.1.1. Creación de las llaves



WEP utiliza el algoritmo RC4 para la encriptación con llaves de 64 bits, aunque existe también la posibilidad de utilizar llaves de 128 bits. Veremos que en realidad son 40 y 104 bits, ya que los otros 24 van en el paquete como Vector de Inicialización (IV).

La llave de 40 ó 104 bits, se genera a partir de una clave (passphrase) estática de forma automática, aunque existe software que permite introducir esta llave manualmente. La clave o passphrase debe ser conocida por todos los clientes que quieran conectarse a la red wireless que utiliza WEP, esto implica que muchas veces se utilice una clave fácil de recordar y que no se cambie de forma frecuente. A partir de la clave o passphrase se generan 4 llaves de 40 bits, sólo una de ellas se utilizará para la encriptación WEP.

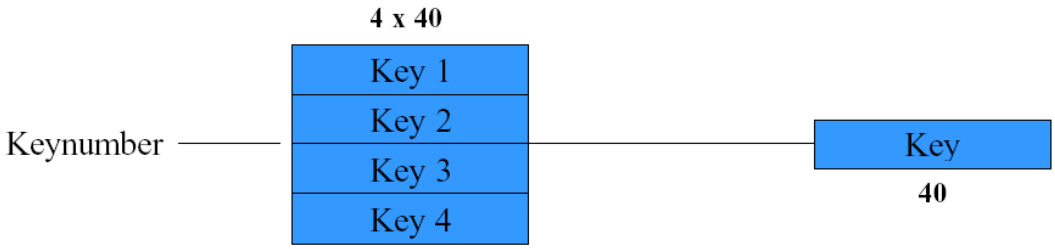
Este es el proceso que se realiza para generar las llaves:

Se hace una operación XOR con la cadena ASCII (*My Passphrase*) que queda transformada en una secuencia de 32 bits que utilizará el generador de números pseudoaleatorios (PRNG) para generar 40 cadenas de 32 bits cada una. Se toma un bit de cada una de las 40 cadenas generadas por el PRNG para construir una llave y se generan 4 llaves de 40 bits. De estas 4 llaves sólo se utilizará una para realizar la encriptación WEP como veremos a continuación.

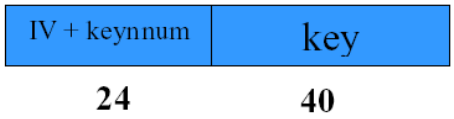
2.2.1.2. Encriptación

Para generar una trama encriptada con WEP se sigue el siguiente proceso:

Partimos de la trama que se quiere enviar. Esta trama sin cifrar está compuesta por una cabecera (Header) y contiene unos datos (Payload). El primer paso es calcular el CRC de 32 bits del payload de la trama que se quiere enviar. El CRC es un algoritmo que genera un identificador único del payload en concreto, que nos servirá para verificar que el payload recibido es el mismo que el enviado, ya que el resultado del CRC será el mismo. Añadimos este CRC a la trama como **valor de chequeo de integridad** (ICV:Integrity Check Value):

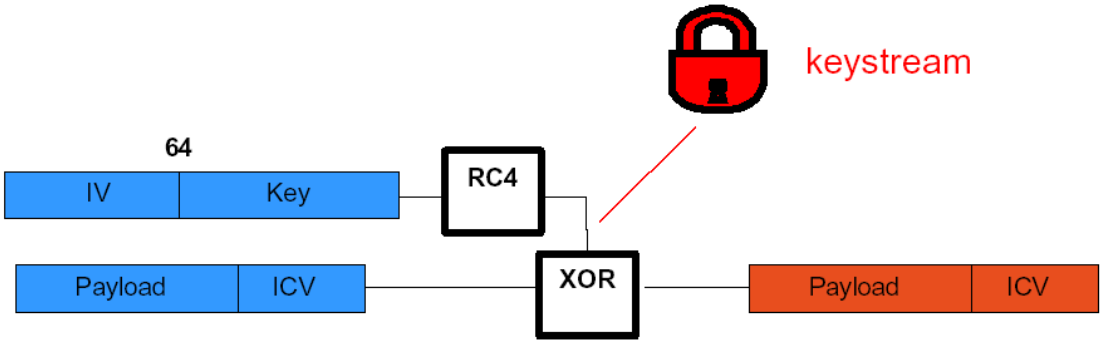


Por otra parte seleccionamos una llave de 40 bits, de las 4 llaves posibles y añadimos el **Vector de Inicialización** (IV) de 24 bits al principio de la llave seleccionada:



El IV es simplemente un contador que suele ir cambiando de valor a medida que vamos generando tramas, aunque según el estándar 802.11b también puede ser siempre cero. Con el IV de 24 bits y la llave de 40 conseguimos los 64 bits de llave total que utilizaremos para encriptar la trama. En el caso de utilizar encriptación de 128 bits tendríamos 24 bits de IV y 104 de llave.

Llegado a este punto, aplicamos el algoritmo RC4 al conjunto IV+Key y conseguiremos el keystream o flujo de llave. Realizando una operación XOR con este keystream y el conjunto Payload+ICV obtendremos el Payload+ICV cifrado, este proceso puede verse en el siguiente grafico. Se utiliza el IV y la llave para encriptar el Payload + ICV:

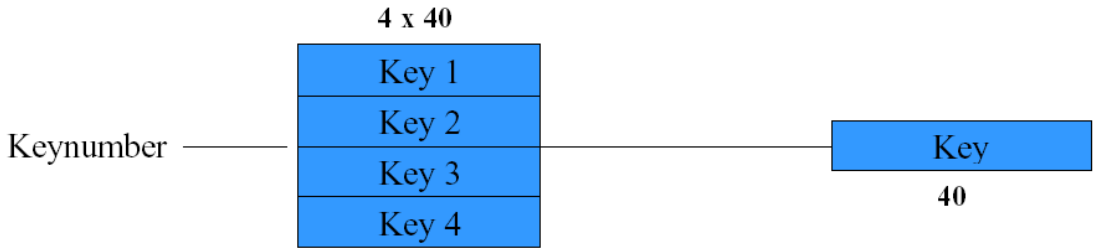


Después añadimos la cabecera y el IV+Keynumber sin cifrar. Así queda la trama definitiva lista para ser enviada:

2.2.1.3. Desencriptación

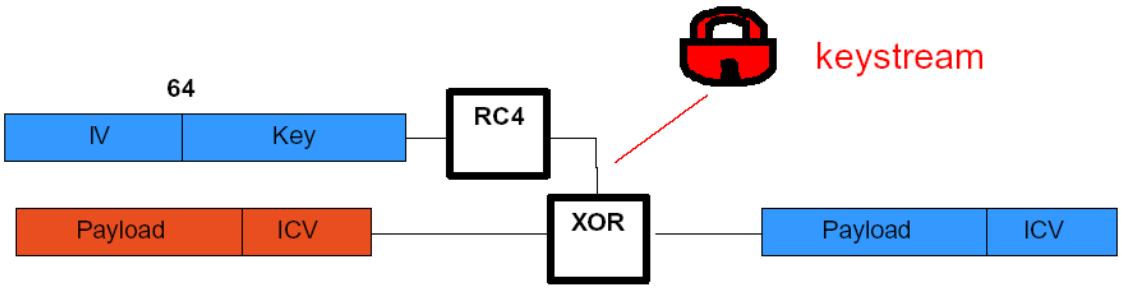
Ahora vamos a ver el proceso que se realiza para desencriptar una trama encriptada con WEP:

Se utiliza el número de llave que aparece en claro en la trama cifrada junto con el IV para seleccionar la llave que se ha utilizado para cifrar la trama:



Se añade el IV al principio de la llave seleccionada, consiguiendo así los 64 bits de llave. Aplicando RC4 a esta llave obtenemos el keystream válido para obtener la

trama en claro (plaintext) realizando una XOR con el Payload+ICV cifrados y la llave completa como se describe a continuación.



Una vez obtenido el plaintext, se vuelve a calcular el ICV del payload obtenido y se compara con el original.

2.2.2. TKIP

Las deficiencias presentadas por RC4 y WEP, se están tratando de solucionar en la actividad de cifrado, a través del protocolo **TKIP** (Temporal Key Integrity Protocol). Esta propuesta aparece a finales de 2002, también se basa en RC4, pero propone tres mejoras importantes:

-**Combinación de clave por paquete:** La clave de cifrado, se combina con la dirección MAC y el número secuencial del paquete. Se basa en el concepto de PSK (Pre-shared Key). Esta metodología, genera dinámicamente una clave entre 280 trillones por cada paquete.

-**VI** (Vector de inicialización) de **48 bits**: Esta duplicación de tamaño implica un crecimiento exponencial del nivel de complejidad, pues si 24 bits son 16 millones de combinaciones, 48 bits son 280 billones. Si se realiza un gran simplificación (pues el caso es más complejo) y se divide 280 billones sobre 16 millones, el resultado es: 17.500.000, por lo tanto si un VI de 24 bits se repite en el orden de 5 horas en una red wireless de una mediana empresa, entonces un VI de 48 bits = 5 x 17.500.00 horas = 87.500.000 horas = 3.645.833 días = 9.988 años, es decir se repetiría después de la Guerra de las Galaxias. Ya se pone complicada la cosa.....

-**MIC** (Message Integrity Check): Se plantea para evitar los ataques inductivos o de hombre del medio. Las direcciones de envío y recepción además de otros datos, se integran a la carga cifrada, si un paquete sufre cualquier cambio, deberá ser rechazado y genera una alerta, que indica una posible falsificación del mismo.

Desafortunadamente TKIP, no está contemplado aún en la totalidad de los productos.

2.2.3. WPA

Microsoft ofrece otra alternativa que inicialmente denominó **SSN** (Simple Security Network), el cual es un subconjunto de 802.11i y al mismo tiempo una implementación de TKIP al estilo Microsoft. SSN lo adoptó 802.11i renombrándolo como **WPA** (WiFi Protected Access), en el año 2004 aparece **WPA2** que es la segunda generación del WPA . Este ya proporciona encriptación con AES (que se menciona a continuación), un alto nivel de seguridad en la autentificación de usuarios y está basado en la norma IEEE 802. 11i y forma parte de ella .

Aunque la WPA impulsa la seguridad WLAN, muchos la consideran una solución temporal pues la solución de 802.11 se orienta más hacia el Modo Conteo con el Protocolo del Código de Autenticación de Mensajes en cadena para el bloqueo de cifrado (Counter-Mode/CBC-Mac Protocol, que se abrevia: **CCMP**), que también forma parte de la norma 802.11i. Se trata de un nuevo modo de operación para cifrado de bloques, que habilita a una sola clave para ser empleada tanto en autenticación como para criptografía (confidencialidad). Se trata de un verdadero "Mix" de funciones, y su nombre completo proviene el "**Counter mode" (CTR**) que habilita la encriptación de datos y **el Cipher Block Chaining Message Authentication Code (CBC-MAC)** para proveer integridad, y de ahí su extraña sigla CCMP.

El protocolo **CCMP** usa la **Norma de Encriptación Avanzada** (**AES**) para proporcionar encriptación más fuerte. Sin embargo, AES no está diseñada para ser compatible con versiones anteriores de software.

A pesar de todos los esfuerzos realizados, muchas entidades siguen considerando a TKIP y WPA como métodos insuficientes de seguridad, el mayor exponente de esta posición es FIPS (Federal Information Process Standard), que excluye a RC4 en las comunicaciones confidenciales. Su publicación **FIPS-197** de finales del 2001, define al estándar **AES** (Advanced Encription Standard) que se mencionó en el punto anterior, con clave mínima de 128 bits, como el aplicable a niveles altos de seguridad. Este estándar, propuesto por Rijndael, surgió como ganador de un concurso mundial que se celebró en el año 2000, para definir la ultima generación de estos algoritmos. La mayoría de los fabricantes están migrando hacia este algoritmo y se aprecia que será el estándar que se impondrá en el muy corto plazo.

El tema de AES tampoco es tan sencillo como parece, pues las implementaciones por software imponen una dura carga de trabajo al sistema, ocasionando demoras de rendimiento que pueden llegar al 50 % de la tasa efectiva de transmisión de información, por lo tanto, se debe optimizar este aspecto para que sea asumido por el mercado.

La WiFi Alliance propone dos tipos de certificación para los productos, cuyas características se presentan a continuación:

- Modelo Empresas:

• WPA:
Autentication: IEEE 802.1x/EAP.
Encryptation: TKIP/MIC.

• WPA2:
Autentication: IEEE 802.1x/EAP.
Encryptation: AES-CCMP.

- Modelo personal (SOHO/personal):

• WPA:
Autentication: PSK.
Encryptation: TKIP/MIC.

• WPA2:
Autentication: PSK.
Encryptation: AES-CCMP.

3. Problemas concretos de Seguridad en WiFi:

a. **Puntos ocultos:** Este es un problema específico de las redes inalámbricas, pues suele ser muy común que los propios empleados de la empresa por cuestiones de comodidad, instalen sus propios puntos de acceso. Este tipo de instalaciones, si no se controlan, dejan huecos de seguridad enormes en la red. El peor de estos casos es la situación en la cual un intruso lo deja oculto y luego ingresa ala red desde cualquier ubicación cercana a la misma. La gran ventaja que queda de este problema es que es muy fácil su identificación siempre y cuando se propongan medidas de auditorías periódicas específicas para las infraestructuras WiFi de la empresa, dentro del plan o política de seguridad.

b. **Falsificación de AP:** Es muy simple colocar una AP que difunda sus SSID, para permitir a cualquiera que se conecte, si sobre el mismo se emplean técnicas de "Phishing", se puede inducir a creer que se está conectando a una red en concreto. Existen varios productos ya diseñados par falsificar AP, en la terminología WiFi se los suelen llamar "Rogue AP" o Fake AP", el más común es un conocido script en Perl denominado justamente "FakeAP", que envía Beacons con diferentes ESSID y diferentes direcciones MAC con o sin empleo de WEP. Se puede descargar de :

Http://www.blackalchemy.to/project/fakeap/

c. **Deficiencias en WEP** (Características lineales de CRC32): Esta característica fue demostrada en teoría por Nikita Borisov, Ian Goldberg y David Wagner. El ICV permite verificar la integridad de un mensaje, por lo tanto, el receptor aceptará el mensaje si su ICV es válido (Recuerdo que es un simple CRC32). Esto presenta dos problemas:
- El CRC es independiente de al clave empleada.
- Los CRC son lineales CRC ($m \oplus k$) = CRC (m) $\oplus$ CRC (k). En virtud de esta linealidad, se puede generar un ICV válido. Un atacante debe interceptar un mensaje (conocido o no) y modificarlo en forma conocida para generar un mensaje m`, operando sobre el mismo obtendrá un paquete que será aceptado por el receptor.

d. **ICV independiente de la llave**: Esta característica fue demostrada en teoría por David Wagner. Nuevamente se trata el ICV, el cual se calcula previamente a comenzar el proceso criptográfico, por lo tanto no depende de la clave ni del IV. Esta debilidad da lugar a que conocido el texto plano de un solo paquete encriptado con WEP, sea posible inyectar paquetes en la red.

e. **Tamaño de IV demasiado corto**: El IV tiene 24 bits de longitud (2^{24} = 16.777.216) y viaja como texto plano. Un punto de acceso que opere con grandes volúmenes de tráfico comenzará a repetir este IV a partir de aproximadamente 5 horas. Esta repetición hace que

matemáticamente se pueda operar para poder obtener el texto plano de mensajes con IV repetido (sin gran nivel de dificultad). El estándar especifica que el cambio de IV es opcional, siendo un valor que empieza con cero y se va incrementando en uno.

f. Deficiencias en el método de autenticación:

Si un atacante captura el segundo y tercer mensaje de administración en una autenticación mutua. El segundo posee el desafío en texto plano y el tercero contiene el mensaje criptografiado con la clave compartida. Con estos datos, posee todos los elementos para autenticarse con éxito sin conocer el secreto compartido (Con esto sólo logra autenticarse, luego queda el acceso a la red).

g. Debilidades en el algoritmo key Scheduling de RC4: scott Fluhrer, Itsik Mantin y Adi Shamir publicaron en Agosto del 2001 la demostración teórica de la vulnerabilidad más devastadora de las existentes hasta ahora en la encriptación WEP. Adam Stubblefield, un trabajador de AT&T Labs, fue la primera persona que implementó este ataque con éxito.
Demostraron que usando sólo la primera palabra de un keystream, podían obtener información de la clave secreta compartida. Se buscan IVs que causen que no haya información de la llave en el keystream. Los autores llamaron a esta condición "*resolved condition*" o condición resuelta.
El número de paquetes que se necesitan recolectar antes de descubrir un byte de la llave varía en función de en que valor se encuentre el contador de IV's de las tarjetas que se estén monitorizando.
Hay 9.000 IV's débiles en los 16 millones de IV's posibles.

¿Cuántos paquetes encriptados se necesitan recolectar para crackear la llave WEP?
– La mayoría de las llaves pueden ser adivinadas después de encontrar aproximadamente 2000 paquetes resueltos.
– Algunas llaves requieren que capturemos incluso más de 4000 paquetes resueltos.

Se puede adivinar la llave después de recolectar de 5 a 10 millones de paquetes encriptados.
Poco después de que el trabajo realizado por estos tres autores y la vulnerabilidad práctica de Stubblefield fueran publicados, aparecieron dos herramientas en Internet que implementan totalmente el ataque:
- Wepcrack: http://wepcrack.sourceforge.net/
- Airsnort: http://airsnort.shmoo.com/

Esto fue la sentencia definitiva para WEP.

h. Debilidad en WPA: Un estudio realizado por Robert Moskowitz, director de ICSA Labs, indica que el sistema utilizado por WPA para el intercambio de la información utilizada para la generación de las claves de cifrado es muy débil. Según este estudio, WPA en determinadas circunstancias es incluso más inseguro que WPE. Cuando las claves preestablecidas utilizadas en WPA utilizan palabras presentes en el diccionario y la longitud es inferior a los 20 caracteres, el atacante sólo necesitará interceptar el tráfico inicial de intercambio de claves. Sobre este tráfico, realizando un ataque de diccionario, el atacante puede obtener la clave preestablecida, que es la información necesaria para obtener acceso a la red. Es decir, a diferencia de WEP en que es necesario capturar un volumen significativo de tráfico para poder identificar las claves, en WPA únicamente capturando el tráfico de intercambio de claves para poder realizar este ataque de diccionario. No es un problema nuevo, pues fue apuntado durante la verificación inicial del protocolo. Es solo una muestra que una implementación inadecuada puede afectar negativamente cualquier sistema de cifrado. Como hemos indicado, el problema solo es explotable bajo una serie de circunstancias muy concretas. Este problema puntual no es, en

absoluto, una indicación de la debilidad de WPA. Únicamente es un recordatorio de la necesidad de utilizar claves convenientemente largas y que incluyan caracteres especiales

3.1. Deficiencias en la encriptación WEP

3.1.1. Características lineares de CRC32

Esta vulnerabilidad fue demostrada teóricamente por Nikita Borisov, Ian Goldberg y David Wagner (Universidad de Berkeley).

Como hemos visto anteriormente, el campo ICV (Integrity Check Value) de una trama encriptada con WEP contiene un valor utilizado para verificar la integridad del mensaje. Esto provee de un mecanismo de autenticación de mensajes a WEP, por lo tanto el receptor aceptará el mensaje si el ICV es válido. El ICV se genera simplemente haciendo un CRC (Cyclic Redundancy Check) de 32 bits, del payload de la trama. Este mecanismo tiene dos graves problemas:

-Los CRCs son independientes de la llave utilizada y del IV (veremos este problema más a fondo en el apartado 4.1.2) -Los CRCs son lineares: $CRC(m \oplus k) = CRC(m) \oplus CRC(k)$

Debido a que los CRCs son lineares, se puede generar un ICV valido ya que el CRC se combina con una operación XOR que también es linear y esto permite hacer el '*bit flipping*' como veremos a continuación:

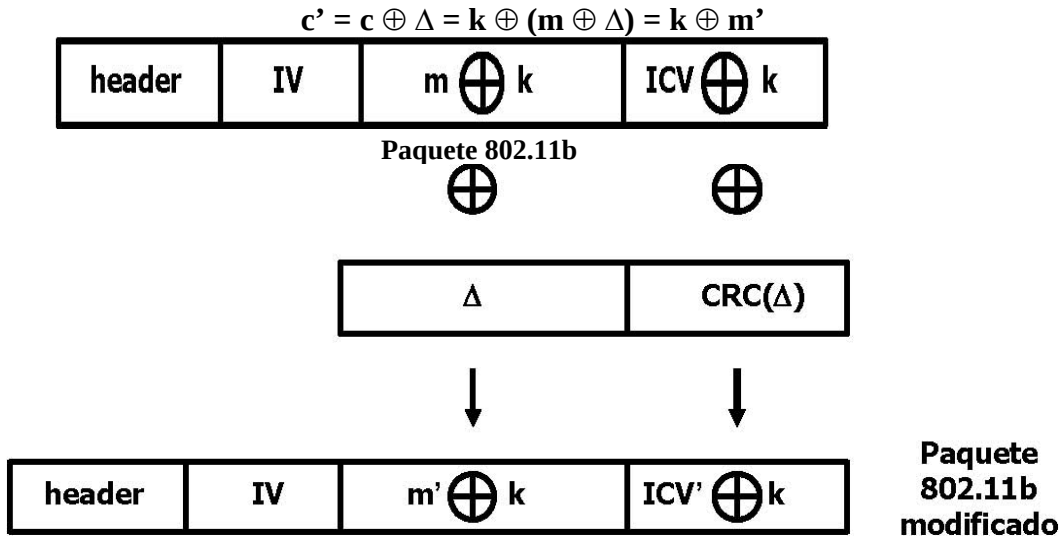
-Un atacante debe interceptar un mensaje m (conocido o no) y modificarlo de forma conocida para producir m':

$$\mathbf{m' = m \oplus \Delta}$$

-Como el CRC-32 es linear, puede generar un nuevo ICV' a partir del ICV de m:

$$\mathbf{IC' = IC \oplus h(\Delta)}$$

-ICV' será valido para el nuevo cyphertext c'



3.1.2. MIC Independiente de la llave

Esta vulnerabilidad fue demostrada teóricamente por David Wagner (Universidad de Berkeley).

Esta vulnerabilidad en WEP es conocida en inglés como "Lack of keyed MIC": Ausencia de mecanismo de chequeo de integridad del mensaje (MIC) dependiente de la llave.

- El MIC que utiliza WEP es un simple CRC-32 calculado a partir del payload, por lo tanto no depende de la llave ni del IV.

Esta debilidad en la encriptación da lugar a que conocido el plaintext de un solo paquete encriptado con WEP sea posible inyectar paquetes a la red.

Esto es posible de la siguiente manera:

-El atacante captura un paquete **c = m** $\oplus$ **k** donde m es conocido
(por ejemplo, el atacante envía un e-mail a la víctima)

-El atacante recupera el flujo pseudo-aleatorio **k = c** $\oplus$ **m** para el IV concreto del paquete

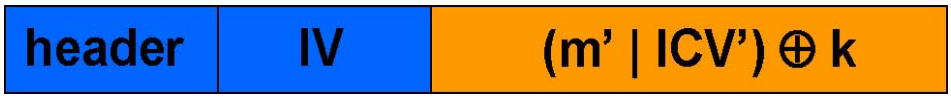
-Supongamos que el atacante quiere inyectar un mensaje m', debe realizar lo siguiente:

$$\mathbf{ICV' = CRC32(m')}$$

- El atacante ya puede ensamblar la parte encriptada del paquete:

$$\mathbf{c = (m'|ICV')} \oplus \mathbf{k}$$

-El atacante obtiene un paquete válido y listo para ser inyectado a la red:



3.1.3. Tamaño de IV demasiado corto

Otra de las deficiencias del protocolo viene dada por la corta longitud del campo IV en las tramas 802.11b. El vector de inicialización (IV) tiene sólo 24 bits de longitud y aparece en claro (sin encriptar). Matemáticamente sólo hay 2^24 (16.777.216) posibles valores de IV. Aunque esto pueda parecer mucho, 16 millones de paquetes pueden generarse en pocas horas en una red wireless con tráfico intenso:

Un punto de acceso que constantemente envíe paquetes de 1500 bytes (MTU) a 11Mbps, acabará con todo el espacio de IV disponible después de 1500*8/(11*10^6)*2^24 = ~1800 segundos, o 5 horas. Este tiempo puede ser incluso más pequeño si la MTU es menor que 1500.

La corta longitud del IV, hace que éste se repita frecuentemente y de lugar a la deficiencia del protocolo que veremos a continuación, basada en la posibilidad de realizar ataques estadísticos para recuperar el plaintext gracias a la reutilización del IV.

3.1.4. Reutilización de IV

Esta vulnerabilidad fue demostrada teóricamente por David Wagner (Universidad de Berkeley). Se basa en que WEP no utiliza el algoritmo RC4 "con cuidado": el Vector de Inicialización se repite frecuentemente. Se pueden hacer ataques estadísticos contra cyphertexts con el mismo IV.

Si un IV se repite, se pone en riesgo la confidencialidad

¡El estándar 802.11 especifica que cambiar el IV en cada paquete es opcional!
El IV normalmente es un contador que empieza con valor cero y se va incrementando de uno en uno, por lo tanto:

-Rebotar causa la reutilización de IV's -Sólo hay 16 millones de IV's posibles, así que después de interceptar suficientes paquetes, seguro que hay IV's repetidos

Un atacante capaz de escuchar el tráfico 802.11 puede descifrar ciphertexts interceptados incluso sin conocer la clave.

3.2. Deficiencias en el método de autenticación Shared Key

El método de autenticación *Shared Key Autentication* descrito anteriormente se puede explotar fácilmente mediante un ataque pasivo:

El atacante captura el segundo y el tercer *management messages* de una autenticación mutua (*Authentication Challenge* y *Authentication Response*). El segundo mensaje contiene el texto de desafío en claro, y el tercer mensaje contiene el desafío encriptado con la clave compartida. Como el atacante conoce el desafío aleatorio (plaintext, P), el desafío encriptado (cyphertext, C), y el IV público, el atacante puede deducir el flujo pseudo-aleatorio (keystream) producido usando WEP utilizando la siguiente ecuación:

$$WEP_{PR}^{K,IV} = C \oplus P$$

El tamaño del keystream será el tamaño de la trama de autenticación, ya que todos los elementos de la trama son conocidos: número de algoritmo, número de secuencia, status code, element id, longitud, y el texto de desafío. Además, todos los elementos excepto el texto de desafío son los mismos para TODAS las *Authentication Responses*.

El atacante tiene por lo tanto todos los elementos para autenticarse con éxito sin conocer la clave secreta compartida K. El atacante envía un *Authentication Request* al AP con el que se quiere asociar. El AP contesta con un texto de desafío en claro. El atacante entonces, coge el texto de desafio aleatorio, R, y el flujo pseudo-aleatorio $WEP^{k,IV}{}_{PR}$ y genera el cuerpo de una trama *Authentiation Response* válido, realizando una operación XOR con los dos valores. El atacante entonces debe crear un nuevo ICV valido aprovechando la vulnerabilidad de *Características lineares de CRC32*. Una vez creado el nuevo ICV, el atacante acaba de completar la trama de

Authentication Response y la envía, de esta manera se asocia con el AP y se une a la red.

Con este proceso el atacante sólo esta autenticado, pero todavía no puede utilizar la red. Como el atacante no conoce la clave compartida, para poder utilizar la red debe implementar algún ataque al protocolo WEP.

4. Medidas de Seguridad en WiFi:

a. Emplear las **mismas herramientas que los intrusos**: realizar la misma actividad, pero para el "lado bueno", es decir realizar controles periódicos con "Netstumbler", Escuchar tráfico e intentar obtener información trivial con "Kismet" o "AirSnort", medir potencias irradiadas con cualquier tarjeta desde los perímetros de la red.

b. **Mejorar la seguridad física**.

c. **Cancelar puertos que no se emplean.**

d. **Limitar el número de direcciones MAC** que pueden acceder. Esta actividad se realiza por medio de ACLs (Access List Control) en los AP, en las cuales se especifica (a mano) las direcciones MAC de las tarjetas a las que se les permitirá el acceso, negando el mismo a cualquiera que no figure en ellas. Cabe aclarar que es tremendamente fácil falsificar una dirección MAC (Ej: en los SSOO Linux es simplemente el comando *"ifconfig").*

e. Ya no se menciona el tema de cancelar las tramas Beacon en los AP, pues cualquier sistema de escucha, por más que no capture la trama Beacon, al capturar la trama PROVE REQUEST del cliente, o la trama PROVE RESPONSE del AP, en ellas también viaja el ESSID.

f. **Satisfacer la demanda:** Si se están empleando AP no autorizados por parte de los empleados, es porque les resulta útil, por lo tanto, se pueden adoptar las medidas para que se implanten, pero de forma segura y controlada, de otra forma, seguirán apareciendo, pero de forma clandestina.

g. **Controle el área de transmisión:** muchos puntos de acceso inalámbrico permiten ajustar el poder de la señal. Coloque sus puntos de acceso tan lejos como sea posible de las paredes y ventanas exteriores. Pruebe el poder de la señal para que usted únicamente pueda conectarse a estos sitios. Luego, asegúrese de cambiar la contraseña predeterminada en todos los puntos de acceso. Utilice una contraseña fuerte para proteger todos los puntos de acceso.

h. **Implemente la autenticación de usuario:** Mejore los puntos de acceso para usar las implementaciones de las normas WPA y 802.11i.

i. **Proteja la WLAN con la tecnología "VPN Ipsec" o tecnología "VPN clientless":** esta es la forma más segura de prestar servicios de autenticación de usuario e integridad y confidencialidad de la información en una WLAN. La tecnología adicional VPN no depende del punto de acceso o de la tarjeta LAN inalámbrica; por consiguiente, no se incurren en costos adicionales de hardware puesto que las normas de seguridad

inalámbrica continúan evolucionando.

j. **Active el mayor nivel de seguridad que soporta su hardware:** incluso si tiene un equipo de un modelo anterior que soporta únicamente WEP, asegúrese de activarlo. En lo posible, utilice por lo menos una WEP con un mínimo de encriptación de 128 bits.

k. **Instale firewalls personales y protección antivirus en todos los dispositivos móviles:** la Alianza WiFi recomienda utilizar la política de seguridad de redes corporativas para imponer su uso continuo.

4.1. Pasos para asegurar una red inalámbrica

Paso 1, debemos activar el protocolo WEP. Parece obvio, pero en la práctica no lo es, muchas redes inalámbricas, bien por desconocimiento de los encargados o por despiste de los mismos no tienen el WEP activado. WEP no es completamente seguro, pero es mejor que nada.

Paso 2, debemos seleccionar una clave de cifrado para el WEP lo suficientemente difícil como para que nadie sea capaz de adivinarla. No debemos usar fechas de cumpleaños ni números de teléfono, o bien hacerlo cambiando (por ejemplo) los ceros por unos.

Paso 3, uso del OSA. Esto es debido a que en la autenticación mediante el SKA, se puede comprometer la clave WEP, que nos expondría a mayores amenazas. Además el uso del SKA nos obliga a acceder físicamente a los dispositivos para poder introducir en su configuración la clave. Es bastante molesto en instalaciones grandes, pero es mucho mejor que difundir a los cuatro vientos la clave. Algunos dispositivos OSA permiten el cambiar la clave cada cierto tiempo de forma automática, lo cual añade un extra de seguridad pues no da tiempo a los posibles intrusos a recoger la suficiente información de la clave como para exponer la seguridad del sistema.

Paso 4, desactivar el DHCP y activar el ACL. Debemos asignar las direcciones IP manualmente y sólo a las direcciones MAC conocidas. De esta forma no permitiremos que se incluyan nuevos dispositivos a nuestra red. En cualquier caso existen técnicas de sniffing de las direcciones MAC que podrían permitir a alguien el descubrir direcciones MAC válidas si estuviese el suficiente tiempo escuchando las transmisiones.

Paso 5, Cambiar el SSID y modificar su intervalo de difusión. Cada casa comercial preconfigura el suyo en sus dispositivos, por ello es muy fácil descubrirlo. Debemos cambiarlo por uno lo suficientemente grande y difícil como para que nadie lo adivine. Así mismo debemos modificar a la baja la frecuencia de broadcast del SSID, deteniendo su difusión a ser posible.

Paso 6, hacer uso de VPNs. Las Redes Privadas Virtuales nos dan un extra de seguridad que nos va a permitir la comunicación entre nuestros dispositivos con una gran seguridad. Si es posible añadir el protocolo IPSec.

Paso 7, aislar el segmento de red formado por los dispositivos inalámbricos de nuestra red convencional. Es aconsejable montar un firewall que filtre el tráfico entre los dos segmentos de red.

Actualmente el IEEE está trabajando en la definición del estándar 802.11i que permita disponer de sistemas de comunicación entre dispositivos wireless realmente seguros.

También, en este sentido hay ciertas compañías que están trabajando para hacer las comunicaciones más seguras. Un ejemplo de éstas es CISCO, la cual ha abierto a otros fabricantes la posibilidad de realizar sistemas con sus mismos métodos de seguridad. Posiblemente algún día estos métodos se conviertan en estándar.

5. Ataques

5.1. Ataques al WEP

5.1.1. Ataque de fuerza bruta

La semilla de 32 bits que utiliza el PRNG es obtenida a partir de la passphrase. La passphrase normalmente contiene caracteres ASCII, por lo cual el bit más alto de cada carácter siempre es cero. El resultado de la operación XOR de estos bits también es cero y esto provoca una reducción de la entropía de la fuente, es decir, las semillas sólo podrán ir desde 00:00:00:00 hasta 7F:7F:7F:7F en lugar de hasta FF:FF:FF:FF.

El uso del PRNG con esta semilla también reduce la entropía. De la semilla de 32 bits sólo utiliza n los bits del 16 al 23. El generador es un generador lineal congruente (LGC: linear congruential generator) de módulo 2^32, esto provoca que los bits mas bajos sean "menos aleatorios" que los altos, es decir, el bit 0 tiene una longitud de ciclo de 2^1, el bit 1 de 2^2, el bit 2 de 2^3, etc. La longitud de ciclo del resultado será por tanto 2^24. Con esta longitud de ciclo sólo las semillas que vayan de 00:00:00:00 a 00:FF:FF:FF producirán llaves únicas.

Como las semillas sólo llegan hasta 7F:7F:7F:7F y la última semilla que tiene en cuenta el PRNG es 00:FF:FF:FF, sólo necesitamo s considerar las semillas desde 00:00:00:00 hasta 00:7F:7F:7F por lo que la entropía total queda reducida a 21 bits.

El conocimiento de estos datos nos permite hacer ataques de fuerza bruta contra la encriptación WEP generando llaves de forma secuencial utilizando las semillas desde
00:00:00:00 hasta 00:7F:7F:7F. Utilizando este proceso, un procesador PIII a 500MHZ tardaría aproximadamente 210 días en encontrar la llave, aunque se puede usar computación en paralelo para obtener la llave en un tiempo más razonable.

También existe la posibilidad de utilizar un diccionario para generar sólo las semillas de las palabras (o frases) que aparezcan en el diccionario, con lo que si la passphrase utilizada está en el diccionario conseguiríamos reducir sustancialmente el tiempo necesario para encontrarla.

5.1.2. Ataque Inductivo Arbaugh

Este ataque fue demostrado teóricamente por William A. Arbaugh (Universidad de Maryland).

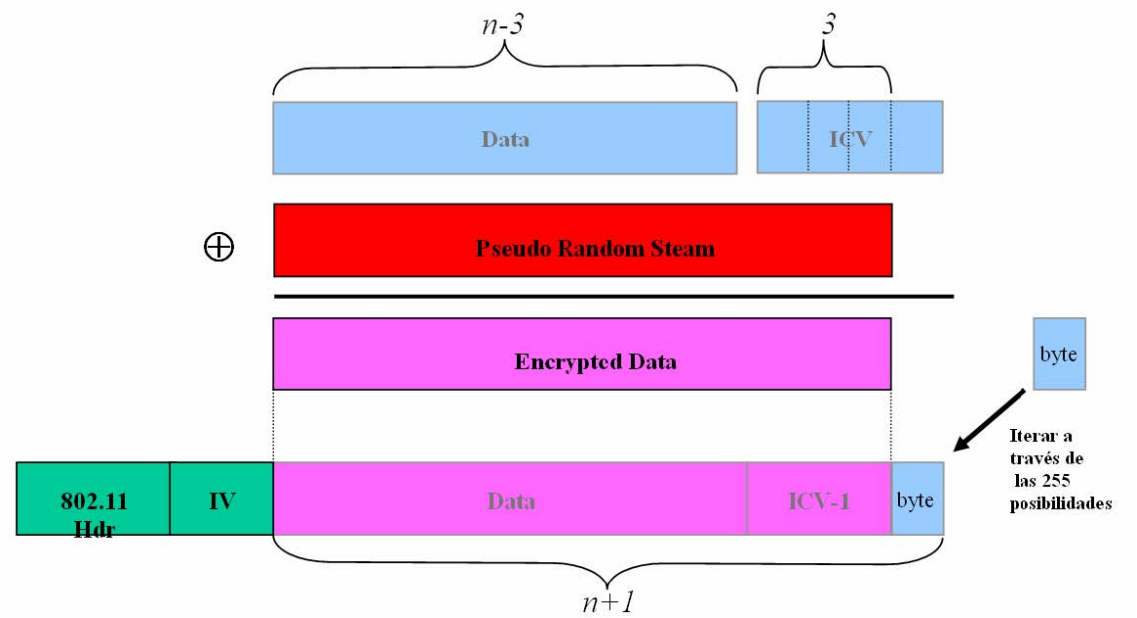
Se basa en explotar la vulnerabilidad de MIC independiente de la llave aprovechando también la redundancia de información producida por el CRC.

Para realizar el ataque hay que conocer parte del plaintext que viaja encriptado en una trama, que podemos obtener por ejemplo identificando mensajes "*DHCPDISCOVER*" de los que conocemos que la cabecera IP tendrá como origen 0.0.0.0 y como destino 255.255.255.255 y tienen longitud fija. Una vez identificada la trama con el mensaje "*DHCPDISCOVER*" realizamos una XOR del plaintext conocido con el cyphertext que hemos recibido, obteniendo así n (en este caso 24) bytes del keystream para el IV concreto del paquete.

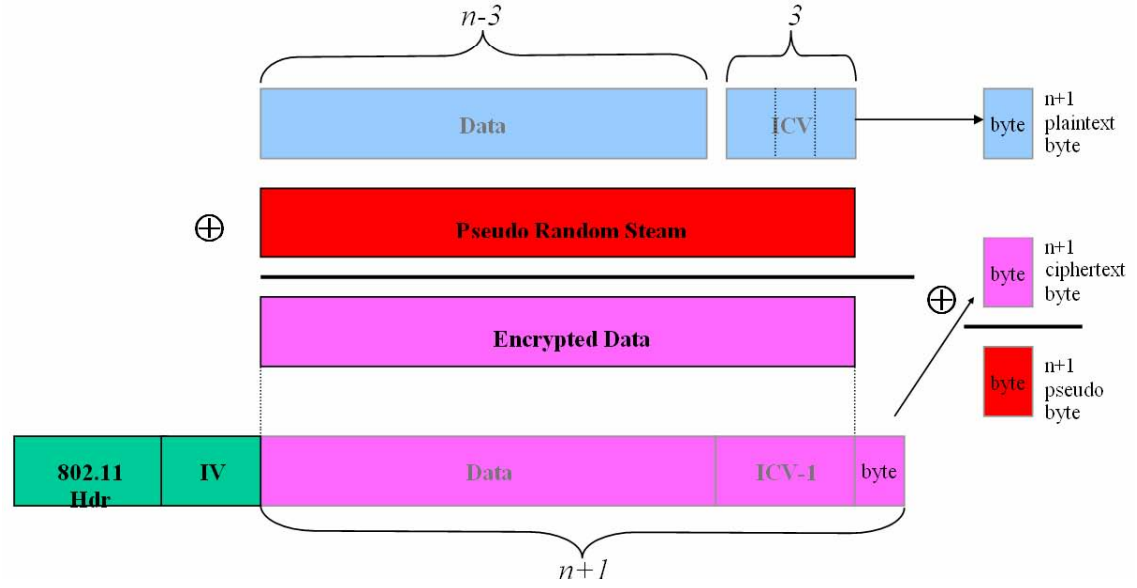
Una vez tengamos estos 24 bytes conocidos del keystream hay que generar un paquete de tamaño n-3, es decir 24-3 = 21 bytes de longitud. Este paquete debe ser algo de lo que podamos esperar una

respuesta, por ejemplo un ping o un ARP Request.

Calculamos el ICV del paquete generado y añadimos sólo los primeros 3 bytes del ICV que hemos calculado. Realiza mos una XOR con el resto del keystream añadiendo el último byte del ICV en el byte n+1 (al final del paquete) tratando de adivinar el siguiente byte del keystream tal y como se muestra en la figura:



Una vez generado el paquete completo lo enviamos y esperamos una respuesta (echo reply, ARP reply…), si no hay respuesta tendremos que ir probando las 255 posibilidades restantes modificando el último byte (n+1). Si hay respuesta podemos afirmar que el byte n+1 era el último byte del ICV, así que tenemos un plaintext que concuerda con el cyphertext y que a su vez nos da el byte n+1 del keystream que es lo que nos interesa. Realizando este proceso repetidas veces obtendremos el keystream completo.



Asumiendo que un atacante puede realizar aproximadamente 100 pruebas por segundo, tardaría una media de 36 minutos en encontrar un keystream completo de 1500 bytes valido para un IV

determinado.

Una vez tenemos un keystream entero, los $2^{24} - 1$ restantes son fáciles de obtener:

El atacante tiene que volver a generar un paquete del cual se le devuelva una respuesta, (lo mejor es enviar broadcast pings, así recibimos múltiples respuestas por cada paquete que enviamos). El atacante conoce el plaintext de la respuesta y el que responde cada vez enviará el paquete con un IV diferente, así es posible construir una tabla de keystreams completos para cada IV que el atacante puede utilizar para descifrar el tráfico encriptado con WEP en tiempo real.

El atacante necesita almacenar 1500 bytes de keystream por cada IV, por lo que la tabla ocuparía 2^{24} x1500 = 24GB y tardaría una media de 30 horas en construir la tabla. Si el ataque se realiza en paralelo 4 hosts atacantes tardarían 7,5 horas y 8 hosts atacantes
3.75 horas.

Cuando el atacante recibe un paquete mira en la tabla a que keystream corresponde el IV recibido y hace una XOR del keystream con el cyphertext del paquete para obtener el plaintext.

5.1.3. Debilidades en el algoritmo key Scheduling de RC4

Scott Fluhrer, Itsik Mantin y Adi Shamir publicaron en Agosto del 2001 la demostración teórica de la vulnerabilidad más devastadora de las existentes hasta ahora en la encriptación WEP.

Su trabajo, de cierta complejidad matemática, se puede encontrar en:
http://www.eyetap.org/~rguerra/toronto2001/rc4_ksaproc.pdf

Demostraron que usando sólo la primera palabra de un keystream, podían obtener información de la clave secreta compartida. Se buscan IVs que causen que no haya información de la llave en el keystream. Los autores llamaron a esta condición "*resolved condition*" o condición resuelta. Cada uno de estos paquetes resueltos sólo tiene ausencia de información de un byte de la llave, y este byte debe ser adivinado correctamente para que el siguiente paquete pueda ofrecer información del siguiente byte de la llave. Para realizar el ataque más rápidamente sólo se buscan los IVs débiles que cumplen esta condición. Hay una posibilidad del 5% de adivinar el byte de la llave correctamente cuando encontramos un paquete resuelto (con un IV débil). Pero como hay gran cantidad de paquetes resueltos viajando por la red, las posibilidades son aún mayores.

Adam Stubblefield, un trabajador de AT&T Labs, fue la primera persona que implementó este ataque con éxito. Añadió que en el tráfico IP se añade una cabecera 802.2 extra, y esto hace que el ataque sea más sencillo de implementar, ya que cada paquete IP tiene el mismo primer byte de plaintext. Para realizar el ataque con éxito, durante la primera fase del ataque, los primeros pocos bytes deben ser adivinados correctamente. Stubblefield utilizo dos métodos para conseguirlo.

El primer método es apuntar los paquetes resueltos para disminuir las posibles combinaciones de bytes de la llave. Se puede comprobar si las llaves son correctas mediante el ICV de los paquetes desencriptados.

El segundo método se centra en la manera en que se distribuyen las llaves WEP. Se supone que el usuario introducirá una clave fácil de recordar en el software de configuración. Una llave fácil de recordar debe contener caracteres ASCII. Comprobando si los bytes de la llave concuerdan con caracteres ASCII cómo letras o símbolos etc. Las posibilidades de adivinar la llave correcta

aumentan.

Cuando se han recolectado suficientes IVs débiles para un valor concreto de un byte de la llave, el análisis estadístico muestra una tendencia hacia un valor en particular para ese byte de la llave. Se le da una puntuación a cada una de las 256 posibilidades según la probabilidad de ser el valor correcto.

La llave se intenta adivinar a partir de los valores con mayor puntuación en el análisis estadístico (Hay un 95% de posibilidades de que un IV no revele información sobre un byte de la llave!).

Los IV's debiles no estan distribuidos de forma lineal a través del espacio de IV's.
El número de paquetes que necesitamos recolectar antes de descubrir un byte de la llave varía en función de en que valor se encuentre el contador de IV's de las tarjetas que estemos monitorizando. Hay 9.000 IV's débiles en los 16 millones de IV's posibles.

¿Cuántos paquetes encriptados necesitamos recolectar para crackear la llave WEP?

- La mayoría de las llaves pueden ser adivinadas después de encontrar aproximadamente 2000 paquetes resueltos
- Algunas llaves requieren que capturemos incluso más de 4000 paquetes resueltos

Podremos adivinar la llave después de recolectar de 5 a 10 millones de paquetes encriptados.

Poco después de que el trabajo realizado por estos tres autores y la vulnerabilidad práctica de Stubblefield fueran publicados, aparecieron dos herramientas en Internet que implementan totalmente el ataque:

- Wepcrack: http://wepcrack.sourceforge.net/

- Airsnort: http://airsnort.shmoo.com/

5.2. Ataques a redes wireless

Vista la manera romper la encriptación WEP ya no debería ser un problema para nosotros, por eso en la implementación de los ataques que vamos a ver a continuación no vamos a hablar de WEP ya que si la WLAN que estamos "auditando" tiene encriptación WEP ya disponemos de las herramientas necesarias para obtener la clave y por tanto, podremos realizar los distintos ataques tanto si existe encriptación WEP como si no.

5.2.1. Romper ACL's basados en MAC

Una de las medidas más comunes que se utilizan para asegurar una red wireless es restringir las máquinas que podrán comunicarse con el Punto de Acceso haciendo filtrado por dirección MAC en éste. Para esto se suele crear una tabla en el punto de acceso que contiene todas las MACs de los clientes que están autorizados para conectar.

Aunque esto pueda parecer una medida de seguridad efectiva, no lo es, ya que es muy fácil cambiar la dirección MAC que aparece en los paquetes que un cliente envía, y hacernos pasar por uno de los equipos que si que tienen acceso a la red.

Para llevar a cabo el ataque basta con *esnifar* durante un momento el tráfico y fijarnos en la MAC de cualquiera de los clientes, sólo hace falta que nos pongamos su misma MAC y ya habremos saltado la restricción. Esto es sencillo de implementar, por ejemplo en el sistema operativo Linux se

puede realizar con el comando *ifconfig* dependiendo del tipo de tarjeta que tengamos. También existen otras utilidades para cambiar la MAC como por ejemplo *setmac*.

Hay que tener en cuenta que si hay dos máquinas en la red con la misma dirección MAC podemos tener problemas, aunque generalmente en las redes wireless esto no suele ser un problema muy grave ya que el Punto de Acceso no puede distinguir que verdaderamente hay dos máquinas con la misma MAC. De todas formas, si queremos podemos "anular" a la máquina que le hemos "robado" la dirección MAC. Para hacer esto, debemos implementar un ataque de Denegación de Servicio, como el que veremos seguidamente.

5.2.2 Ataque de Denegación de Servicio (DoS)

Para realizar este ataque basta con esnifar durante un momento la red y ver cual es la dirección MAC del Punto de Acceso. Una vez conocemos su MAC, nos la ponemos y actuamos como si fuéramos nosotros mismos el AP. Lo único que tenemos que hacer para denegarle el servicio a un cliente es mandarle continuamente notificaciones (*management frames*) de desasociación o desautenticación. Si en lugar de a un solo cliente queremos denegar el servicio a todos los clientes de la WLAN, mandamos estas tramas a la dirección MAC de broadcast.

Existen varias herramientas para realizar este ataque, las más comunes para el sistema operativo Linux son:

- *wlan-jack*: perteneciente a las utilidades air-jack, presentadas en la concentración Black Hat 2002 en Las Vegas, se puede encontrar en http://802.11ninja.net.
- *dassoc*: envia tramas de desasociacion, herramienta desarrollada por @stake (antes L0pht), se puede encontrar en http://www.atstake.com.

5.2.3. Descubrir ESSID ocultados

Como hemos comentado anteriormente, para que un cliente y un AP se puedan comunicar, ambos deben tener configurado el mismo ESSID, es decir, deben pertenecer a la misma red wireless.

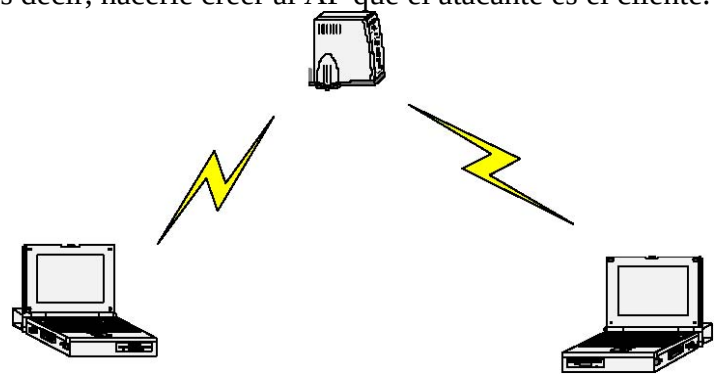
Una medida de seguridad bastante común es "ocultar" el ESID, es decir, hacer que el AP no mande BEACON FRAMES, o en su defecto no incluya el ESSID en éstos.

En este caso, para descubrir el ESSID deberíamos esnifar y esperar a que un cliente se conectara, y veríamos el ESSID en la trama PROVE REQUEST del cliente (en el caso de que no se manden BEACON FRAMES), o en la trama PROVE RESPONSE del AP. Pero también podemos "provocar" la desconexión de un cliente, utilizando el mismo método que en el ataque DoS, pero mandando sólo una trama de desasociación o de desautenticación en lugar de mandarlas repetidamente, es decir, nos ponemos la dirección física del AP y mandamos una trama DEAUTH o DISASSOC a la dirección MAC del cliente (o a la de broadcast), entonces el cliente intentará volver a asociarse o autenticarse, con lo que podremos ver el ESSID en los *management frames*.

Para implementar el ataque podemos usar la herramienta essid-jack, que también pertenece al paquete de utilidades air-jack para Linux (http://802.11ninja.net).

5.2.4. Ataque Man in the middle

El ataque de *Man in the middle*, también conocido como *Monkey in the middle* consiste en convencer al cliente (la víctima) de que el host que hay en el medio (el atacante) es el AP, y hacer lo contrario con el AP, es decir, hacerle creer al AP que el atacante es el cliente.



WLAN antes del ataque

Para realizar este ataque, primero debemos esnifar para obtener:

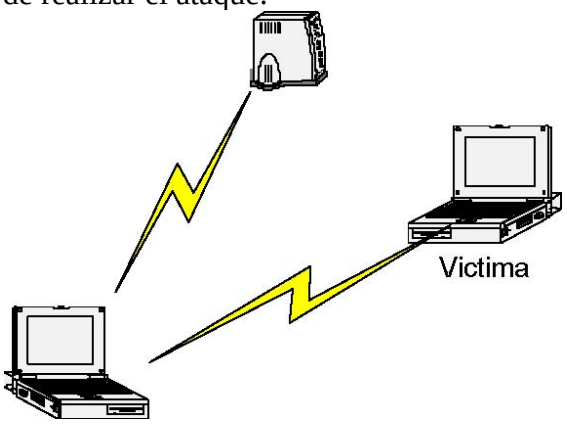
-El ESSID de la red (si esta ocultado, usaremos el método anterior)
-La dirección MAC del AP
-La dirección MAC de la víctima

Una vez conocemos estos datos, utilizamos el mismo método que en el ataque DoS, para desautenticar a la víctima del AP real, es decir, el atacante spoofea su MAC haciéndose pasar por el AP y manda tramas DEAUTH a la víctima. La tarjeta wi-fi de la víctima empezará entonces a escanear canales en busca de un AP para poderse autenticar, y ahí es donde entra en juego el atacante.

El atacante hace creer a la víctima que él es el AP real, utilizando la misma MAC y el mismo ESSID que el AP al que la víctima estaba autenticada anteriormente, pero operando por un canal distinto. Para realizar esto la tarjeta wi-fi del atacante debe estar en modo **master**.

Por otra parte, el atacante debe asociarse con el AP real, utilizando la dirección MAC de la víctima.

De esta manera hemos conseguido insertar al atacante entre la víctima y el AP, veamos como quedaría la WLAN después de realizar el ataque.



WLAN después del ataque

De esta manera todos los datos que viajan entre la víctima y el AP pasan a través del atacante. Como el ataque ha sido realizado a nivel de enlace (nivel 2), el atacante puede ver, capturar e incluso modificar las tramas en los niveles superiores del modelo OSI.

Es muy fácil implementar este tipo de ataques utilizando el driver air-jack con la herramienta monkey-jack.

Hay que tener en cuenta que muchas soluciones de seguridad están pensadas asumiendo que las capas 1 y 2 son seguras, esto como hemos visto es incierto para las redes wireless y por tanto el uso de segú n que tipo de solución podría no ser adecuado para estas redes. Hay que ir con mucho cuidado sobre todo en implementaciones de VPN que no realizan las comprobaciones necesarias de autenticación para protegerse de ataques *Man in the middle* en redes wireless.

5.2.5. Ataque ARP poisoning

El *ARP cache poisoning* es un ataque que sólo se puede llevar a cabo cuando el atacante está conectado a la misma LAN lógica que las víctimas, limitando su efectividad a redes conectadas con switches, hubs y bridges, pero no routers. La mayoría de los Puntos de Acceso 802.11b actúan como bridges transparentes de capa 2, lo que permite que los paquetes ARP pasen de la red wireless hacia la LAN donde está conectado el AP y viceversa. Esto permite que se ejecuten ataques de *ARP cache poisoning* contra sistemas que están situados detrás del Punto de Acceso, como por ejemplo servidores conectados a un switch en una LAN a los que se pueda acceder a través de la WLAN.

Vamos a ver el ejemplo para entender mejor la idea:

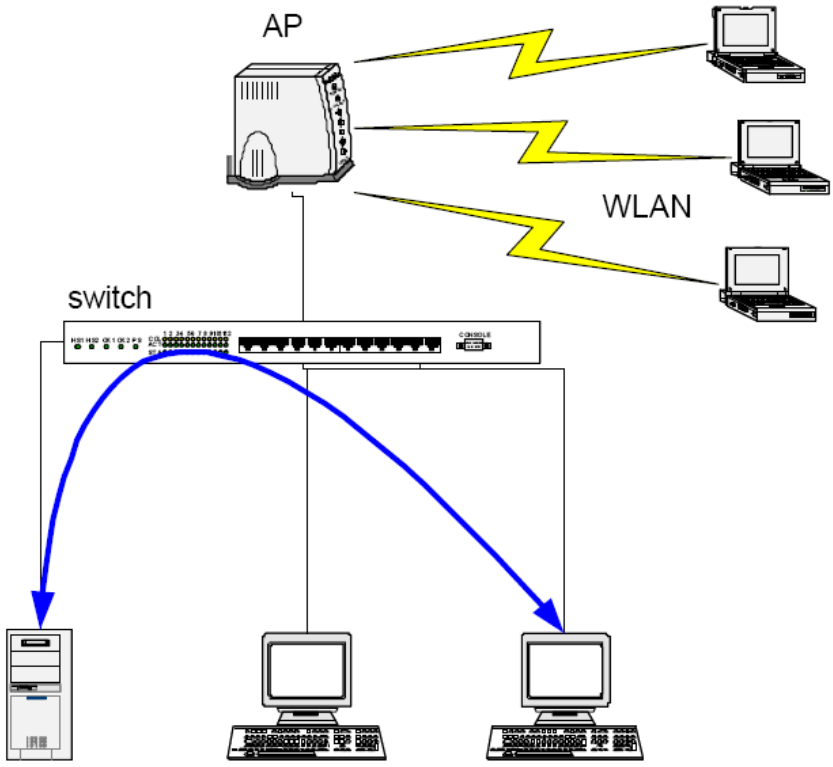


Tabla ARP – PC 1

Dirección IP	Dirección MAC
192.168.1.2	3B:AF:44:F8:2C:B3
192.168.1.3	3C:2A:4A:59:1A:7A

Tabla ARP – PC 3

Dirección IP	Dirección MAC
192.168.1.2	3B:AF:44:F8:2C:B3
192.168.1.1	6A:8F:5E:99:2B:78

Tabla ARP – PC 2

Dirección IP	Dirección MAC
192.168.1.1	6A:8F:5E:99:2B:78
192.168.1.3	3C:2A:4A:59:1A:7A

El servidor PC 1 se comunica con PC 3 a través del switch, si un atacante desde la WLAN envenena la tabla de ARP's de PC 1 y de PC 3 podrá realizar un ataque del tipo *Man in the Middle* situándose entre los dos hosts de la red con cables.

Así es como se efectuaría la comunicación después del ataque:

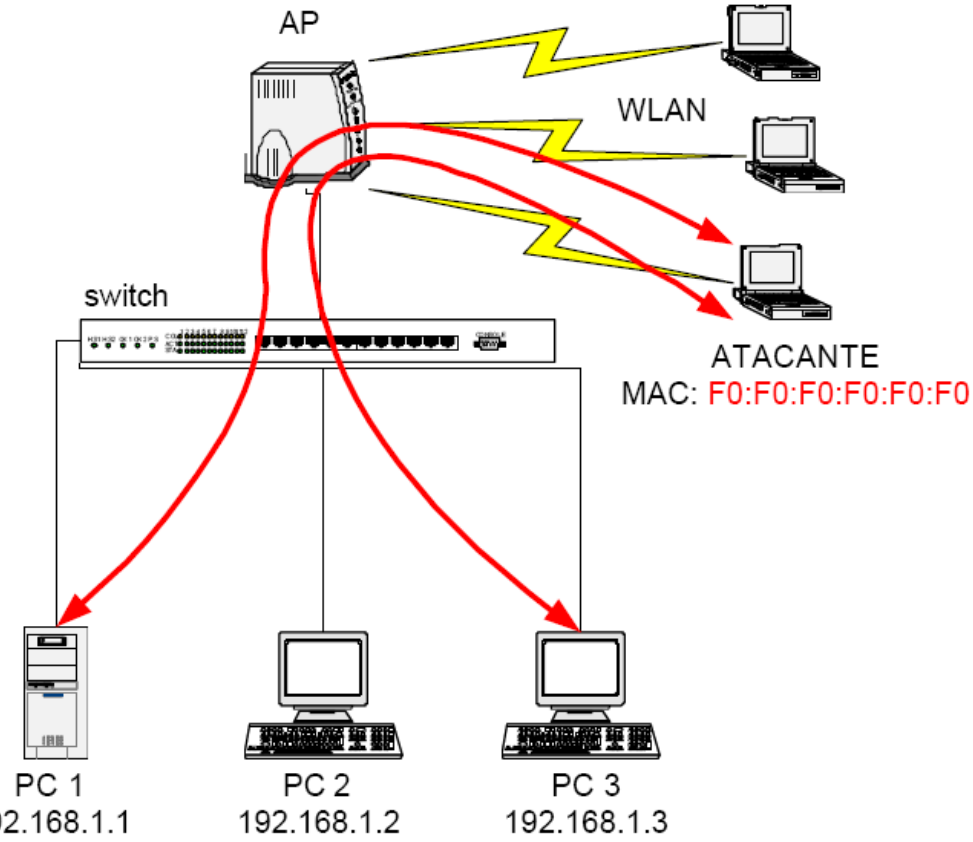


Tabla ARP – PC 1

Dirección IP	Dirección MAC
192.168.1.2	3B:AF:44:F8:2C:B3
192.168.1.3	F0:F0:F0:F0:F0:F0

Tabla ARP – PC 3

Dirección IP	Dirección MAC
192.168.1.2	3B:AF:44:F8:2C:B3
192.168.1.1	F0:F0:F0:F0:F0:F0

Tabla ARP – PC 2

Dirección IP	Dirección MAC
192.168.1.1	6A:8F:5E:99:2B:78
192.168.1.3	3C:2A:4A:59:1A:7A

El atacante manda paquetes *ARP REPLY* a PC 2 diciendo que la dirección IP de PC 1 la tiene la MAC del atacante, de esta manera consigue "envenenar" la caché de ARP's de PC 2. Luego realiza la misma operación atacando a PC 1 y haciéndole creer que la dirección IP de PC 2 la tiene también su propia MAC.

Como ARP es un protocolo *stateless*, PC 1 y PC 2 actualizan su caché de acuerdo a la información que el atacante ha inyectado a la red.

Como el switch y el AP forman parte del mismo dominio de broadcast, los paquetes ARP pasan de la red wireless a la red con cables sin ningún problema.

Para realizar el ataque ARP Poisoning, existen múltiples herramientas en Internet, ya que este ataque no es específico de las redes wireless, la más famosa es el sniffer Ettercap (http://ettercap.sourceforge.net).

Podríamos frenar este ataque creando dos VLAN's en el switch, una para la boca a la que está conectado el AP y la otra para el resto de máquinas. Otra forma de frenarlo sería utilizando tablas de ARP estáticas.

6. ANEXOS

6.1. WARCHALKING (Encontrar redes wireless)

Material necesario:

· Ordenador portátil o PDA
· Tarjeta Wi-Fi con firmware adecuado.
· Programa o driver que permita poner la tarjeta en modo monitor
· Sniffer

Otros materiales adicionales:

· Antena direccional o omnidireccional
· GPS
· Equipo electrógeno
· Mochila
· Auriculares
· Medio de transporte (coche, patines, bicicleta…)

Proceso a seguir

Antes de salir en busca de una red wireless, hay que configurar el equipo que nos permitirá detectar la red. Se debe poner la tarjeta wi-fi en modo **monitor**, este modo es parecido al modo "promiscuo" de las tarjetas ethernet convencionales, lo que hace es dejar la tarjeta "a la escucha" por la frecuencia utilizada en 802.11b (2,4 GHz). El método para poner la tarjeta en modo monitor es distinto para cada sistema operativo, y para tipo de tarjeta (según chipset).

Explicaremos el método a seguir para las tarjetas Prism y Orinoco utilizando el sistema operativo GNU Linux, si se dispone de otro chipset u otro sistema operativo, es recomendable buscar esta información por Internet (ojo, esto no es posible con todos los chipsets!).

Instalar wireless-tools:
http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

Instalar pcmcia-cs: http://pcmcia-cs.sourceforge.net/

Si la tarjeta tiene el chipset Orinoco hay que parchear la pcmcia-cs para poder ponerla en modo monitor, el parche se puede encontrar en la siguiente página:
Orinoco Monitor Mode Patch Page http://airsnort.shmoo.com/orinocoinfo.html

Una vez cargados los módulos de la tarjeta (provistos por el pcmcia-cs), hay que utilizar el comando "iwpriv" (provisto por las wireless-tools) para ponerla en modo monitor, con la siguiente sintaxis: *# iwpriv wlan0 monitor 1 #canal*

Una vez tenemos la tarjeta en modo monitor, hay que instalar un sniffer que nos permita capturar las tramas wireless. Los más comunes son los siguientes:

Sistema Operativo Linux:

- Kismet: http://www.kismetwireless.net/
- Airsnort: http://airsnort.shmoo.com/
- Ethereal: http://www.ethereal.com/

Sistema Operativo Windows:

- Airopeek: http://www.wildpackets.com/products/airopeek
- NetStumbler: http://www.netstumbler.com/

En este punto, ya estamos listos para salir a la calle en busca de una red wireless. Es aconsejable desplazarse a poca velocidad, moverse cerca de los edificios y hacerlo preferiblemente en horario laboral.

Según el medio de transporte que utilicemos, esta práctica se denomina de la siguiente manera:

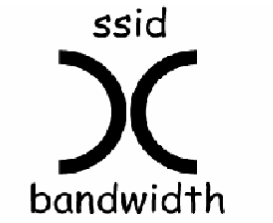
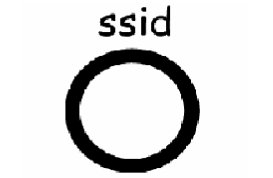
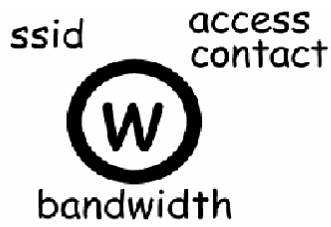
- WarWalking: Andando
- WarSkating: En patines
- WarCycling: En bicicleta o ciclomotor
- WarFlying: Avión
- WarDriving: Coche

El sniffer más cómodo para estas prácticas es el NetStumbler, ya que emite un tono por la salida de audio cuando detecta una red wireless. Se suele poner el portátil en una mochila, con los auriculares conectados, y el monitor en modo Stand-by (para ahorrar batería).

Podemos utilizar el kismet o el Airsnort, que permiten comunicación directa con dispositivos GPS. Cuando el sniffer detecta una WLAN, guarda un registro con toda la información que ha podido obtener de la red mientras hemos tenido cobertura, si disponemos de GPS podemos saber en que posición exacta estaba situada la red y que área de cobertura tenía.

Marcado de una red wireless

Una vez hayamos encontrado una red wireless, es aconsejable marcarla con los datos que conozcamos, para que otra persona pueda localizarla fácilmente si en el momento que ve la marca no dispone del material necesario para conectar a la red wireless. Esta práctica es conocida como WarChalking y consiste en realizar una marca con tiza en una pared de la zona donde haya cobertura. La convención de símbolos utilizada es la siguiente:

SÍMBOLO	SIGNIFICADO
	Nodo Abierto
	Nodo cerrado
	Nodo con WEP

Se puede encontrar más información de WarChalking en Internet, y por ejemplo en http://www.warchalking.org

6.2. ARTICULO: “Como el FBI rompe la seguridad de una red con encriptación de 128 bits en 3 minutos”

Noticia: *The Feds can own your LAN too*
Autor: Humprey Cheung
Link: http://www.tomsnetworking.com/Sections-article111.php

Como ejemplo práctico de todos los aspectos relacionados con la seguridad en redes inalámbricas nos ha parecido interesante mostrar una noticia aparecida en los websites relacionados con el mundo de las redes inalámbrica. Se trata de una demostración de cómo el FBI ha conseguido romper una red inalámbrica con seguridad WEP de 128 bits en sólo 3 minutos con herramientas de software libre al alcance de cualquier usuario. La noticia original está redactada en inglés, pero nos ha parecido que tiene interés traducirlo para hacerlo llegar a un mayor número de personas de forma clara.

“The Feds can own your LAN too”

El FBI ha realizado una demostración de las técnicas actuales para penetrar en una red gíreles, en el cual lograron vencer un cifrado WEP de 128 bits.

1. *Introducción*

   Millones de puntos de acceso (PA) inalámbricos están dispersos a los largo de EEUU y del Mundo. Sobre un 70% de estos PA están sin protección, abiertos ampliamente para quien quiera entrar. El otro 30% están protegidos por cifrado WEP y una pequeña cantidad por el nuevo estándar WPA.

   En el último encuentro ISSA (Information System Security Association) celebrada en los ángeles, un equipo de agentes del FBI demostraron las técnicas actuales de WEP-Cracking y rompieron la seguridad de una clave WEP de 128 bits en aproximadamente 3 minutos. El agente especial Geoff Bickers mostró la presentación en PowerPoint, mientras que los otros agentes (que no quisieron dar su nombre ni ser fotografiados) hicieron el trabajo sucio, monitorizaron y rompieron la red.

   Este artículo será una vista general de los procedimientos que siguieron los agentes del FBI. Un futuro artículo dará paso a paso instrucciones de cómo replicar el ataque.

2. *WEP Cracking. The next Generation*

   WEP es un esquema de encriptación, basado en el cifrado RS4, el cual está disponible en todos los productos 802.11 a, b y g. WEP usa un conjunto de bits llamado clave para codificar la información en las tramas de datos que salen del PA o adaptador del cliente y se decodifican en el destino.

   En Ambos lados (transmisor y receptor) se debe tener la misma clave WEP, la cual es usualmente de 64/128 bits, un nº semialeatorio de 24 bits llamado vector de inicialización (IV), es parte de la clave, de esta manera los 64 bits de las claves son sólo 40 bits de codificación “fuerte” mientras que en el caso de claves de 128 bits tenemos 104 significativos. El IV está dispuesto en el encabezado de las tramas, y es transmitido como texto plano (o claro).

   Tradicionalmente, crackear claves WEP había sido un proceso lento y aburrido. Un ataque debía capturar cientos de miles o millones de paquetes, un proceso que podía llevar horas o

incluso días, dependiendo del volumen de información a través de la red wireless. Después de capturar suficiente información, un programa de crackeo WEP como airCrack podría ser usado para encontrar la clave WEP.

A finales del último verano, la última generación de herramientas WEP fueron mejoradas. Esta generación actual usa la combinación de técnicas estadísticas centradas en IV´s únicas capturadas y en un diccionario de ataque de fuerza bruta para romper claves WEP de 128 bits en minutos en vez de en horas. Como el agente especial Bickers hizo notar, “No importa que uses claves de 128 bits, tu eres vulnerable”.

3. *Comienza el Show*

Antes de introducirnos en los pasos que uso el FBI para romper WEP, debería tenerse en cuenta que hay numerosas maneras de hachear una red wíreless. El equipo del FBI uso herramientas de uso público y enfatizaron que ellos están demostrando un ataque que mucha otra gente puede reproducir. De otro lado, romper la clave WEP puede no necesariamente darnos acceso completo a la red. Podría haber otros mecanismos de protección tales como VPNs o servidores Proxy.

Para la demostración el agente especial Bickers trajo un punto de acceso NETGEAR y le asigno una SSID de NETGEARWEP. Codificó el acceso al PA con una clave de 128 bits- pulsando una combinación aleatoria de letras y números.

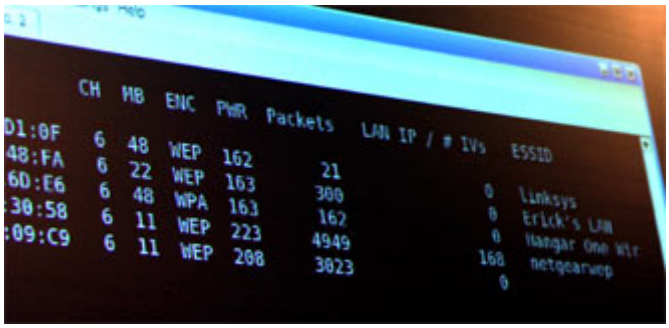
Destacar que normalmente, hay que encontrar redes gíreles antes de poder atacarlas. Las dos herramientas de escaneo seleccionadas fueron NETStumbler para windows y Kismet para Linux. Desde que otras herramientas de ataque WEP están basadas en Linux, la mayoría encuentra más sencillo trabajar en con Kismet, de manera que no tengan que cambiar entre windows y Linux.

Otro agente del FBI arranco Kismet inmediatamente encontró el punto de acceso NETGEARWEP. Sólo por diversión, un tercer agente uso su estación corriendo la aplicación FAKEAP, un programa que confunde a los programas de escaneo poniendo PA falsos.

4. *Ataque*

Después de encontrar la WLAN, el siguiente paso es empezar a capturar paquetes y convertirlos a formato pcap (short for packet capture). Estos archivos pcap serán procesados después por otros programas. Muchas herramientas, comerciales o de fuente abierta, pueden ser usados para capturar paquetes, pero los dos favoritos parecen ser Kismet y Airdump (parte de Aircrack). Idealmente una estación debería ser escaneada, mientras que otro portátil o estación realiza el ataque (de esta forma la hizo el FBI).

Aproximadamente media docena de herramientas software fueron usadas por el equipo del FBI, están listadas- en sus links de descarga- al final del artículo. Agradecer a Auditor´s Security collection, el cual nosotros analizamos el último año, que es un CD live que contiene todas las herramientas instaladas, incluso el FBI usa esta distribución.



Si el hacker es suficientemente afortunado y encuentra una red extremadamente ocupada. El sniffing pasivo debería proveer los suficientes paquetes buenos como para permitir recuperar las claves WEP. En la mayoría de los casos, sin embargo, un ataque activo o una serie de ataques es necesario para saltar el proceso y producir más paquetes. Notar que los ataques activos genera un tráfico que puede ser asimismo detectado y alerta al objetivo del ataque.

El equipo del FBI usó la característica “deauth” de “void11” para disociar repetidamente la estación del punto de acceso. El tráfico adicional deseado fue generado cuando Windows XP intentaba volver a asociarse al PA. Tener en cuenta que este no es un ataque de incógnito particular, el usuario será notificado en su barra de tareas dentro de su escritorio.

Otro método de ataque usado por el FBI es el ataque “replay”. La premisa básica de este ataque es capturar al menos un paquete viajando del portátil a la víctima al PA víctima. Este paquete puede ser repuesto en la red, causando que el PA responda y nos proporcione más tráfico que capturar.

Aireplay (de Aircrack) puede ejecutar un ataque “replay” basado en los paquetes ARP capturados (ardes Resolution Protocol), los cuales son difundidos en intervalos regulares en redes tanto inalámbricas como cableadas y que son fáciles de capturar. Aireplay automáticamente escanea el archivo PCAP capturado, saca las supuestas respuestas ARP, y las replica al PA.

Después de aproximadamente 3 minutos de capturar y atacar, el equipo del FBI encontró la clave correcta, y la mostraron en la pantalla del portátil proyectado. El agente Bickers, todavía hablando en la audiencia, se giró, miro a la pantalla y se sorprendió, “usualmente el proceso toma entre 5-10 minutos”.

5. *Medidas a tomar y conclusiones*

¿Qué se puede hacer para prevenir que los hackers entren en tu red?. El agente especial Bickers y su equipo tienen algunos consejos para los usuarios de gíreles. Él comento que las medidas son para el uso doméstico, y que no deberían ser prácticas recomendadas para los negocios.

- Seguridad de la Red. Pon tu punto de acceso en una subred separada, con un firewall separando los usuarios gíreles y los internos.
- Cambia los parámetros por defecto en tu PA. Parámetros por defecto (SSID, password admin., canal) son bien conocidos incluso como parte de algunas herramientas de ataque WLAN.
- Usa WPA con clave "fuerte". WPA es una mejora definitiva sobre WEP suministrando seguridad inalámbrica. Pero la versión para uso domésticos y SOHO-WPA-PSK- adolece de la una debilidad compartida por cualquier mecanismo de seguridad basado en clave por frase. La elección de frases simples, comunes o cortas puede permitir que la WLAN sea comprometida vía diccionario de ataque.
- Actualiza tu firmware. Esto es de ayuda si tu PA o cliente no soporta actualmente WPA. Muchos fabricantes tienen firmwares más recientes para productos 802.11g que añaden soporte WPA. Tu también puedes encontrar esto para 802.11b, pero no es tan común.
- Apaga la WLAN cuando no esté en uso. Un timer de 5$ en tu ferretería local esuna simple, pero efectiva manera de mantener tu WLAN o LAN segura cuando estas durmiendo.

Bickers también dijo que si tuenes un PA que cambie las claves lo suficientemente rápido, serás capaz de defenderte de un atacante. "La mayoría se aburre y ataca a alguien distinto". Para la mayoría de propietarios de WLAN, este método no es práctico.

El FBI ha demostrado este ataque para profesionales de seguridad en el encuentro ISSA con objeto de mostrar la protección inadecuada que ofrece WEP. Esta es una razón para leer como la protección WEP se rompe en minutos, pero es traumático ver el ataque delante de tus ojos, es rápido y simple.

Agradecimientos al FBI, son buenos Chicos.
Humprey Cheung.

6.3. MECANISMOS DE ACCESO INALÁMBRICOS

6.3.1. Protocolos con arbitraje

La multiplexación en frecuencia (FDM) divide todo el ancho de banda asignado en distintos canales individuales. Es un mecanismo simple que permite el acceso inmediato al canal, pero muy ineficiente para utilizarse en sistemas informáticos, los cuales presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).

Una alternativa a este sería asignar todo el ancho de banda disponible a cada nodo en la red durante un breve intervalo de tiempo de manera cíclica. Este mecanismo, se llama multiplexación en el tiempo (TDM) y requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias. Este esquema ha sido utilizado con cierto éxito sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

6.3.2. Protocolos de acceso por contienda

Tienen similitudes al de Ethernet cableada de línea normal 802.3. Veremos cinco tipos:

1-CSMA (Code-division multiple access = Acceso múltiple por división de tiempo). Se aplica específicamente a los sistemas de radio de banda esparcida basados en una secuencia PN. En este esquema se asigna una secuencia PN distinta a cada nodo, y todos los nodos pueden conocer el conjunto completo de secuencias PN pertenecientes a los demás nodos. Para comunicarse con otro nodo, el transmisor solo tiene que utilizar la secuencia PN del destinatario. De esta forma se pueden tener múltiples comunicaciones entre diferentes pares de nodos.

2-CSMA/CD (Carrier Sense, Multiple Access, Collision Detection) Como en estos medios de difusión (radio, infrarrojos), no es posible transmitir y recibir al mismo tiempo, la detección de errores no funciona en la forma básica que fue expuesta para las LAN cableadas. Se diseñó una variación denominada detección de colisiones (peine) para redes inalámbricas. En este esquema, cuando un nodo tiene una trama que transmitir, lo primero que hace es generar una secuencia binaria pseudoaleatoria corta, llamada peine la cual se añade al preámbulo de la trama. A continuación, el nodo realiza la detección de la portadora si el canal está libre transmite la secuencia del peine. Por cada “1” del peine el nodo transmite una señal durante un intervalo de tiempo corto. Para cada “0” del peine, el nodo cambia a modo de recepción. Si un nodo detecta una señal durante el modo de recepción deja de competir por el canal y espera hasta que los otros nodos hayan transmitido su trama.

La eficiencia del esquema depende del número de bits de la secuencia del peine ya que si dos nodos generan la misma secuencia, se producirá una colisión.

3-El que más se utiliza es el CSMA/CA (Carrier-Sense, Múltiple Access, Collision Avoidance). Este protocolo evita colisiones en lugar de descubrir una colisión, como el algoritmo usado en la 802.3.

En una red inalámbrica es difícil descubrir colisiones. Es por ello que se utiliza el CSMA/CA y no el CSMA/CD debido a que entre el final y el principio de una transmisión suelen provocarse colisiones en el medio. En CSMA/CA, cuando una estación identifica el fin de una transmisión espera un tiempo aleatorio antes de transmitir su información, disminuyendo así la posibilidad de colisiones.

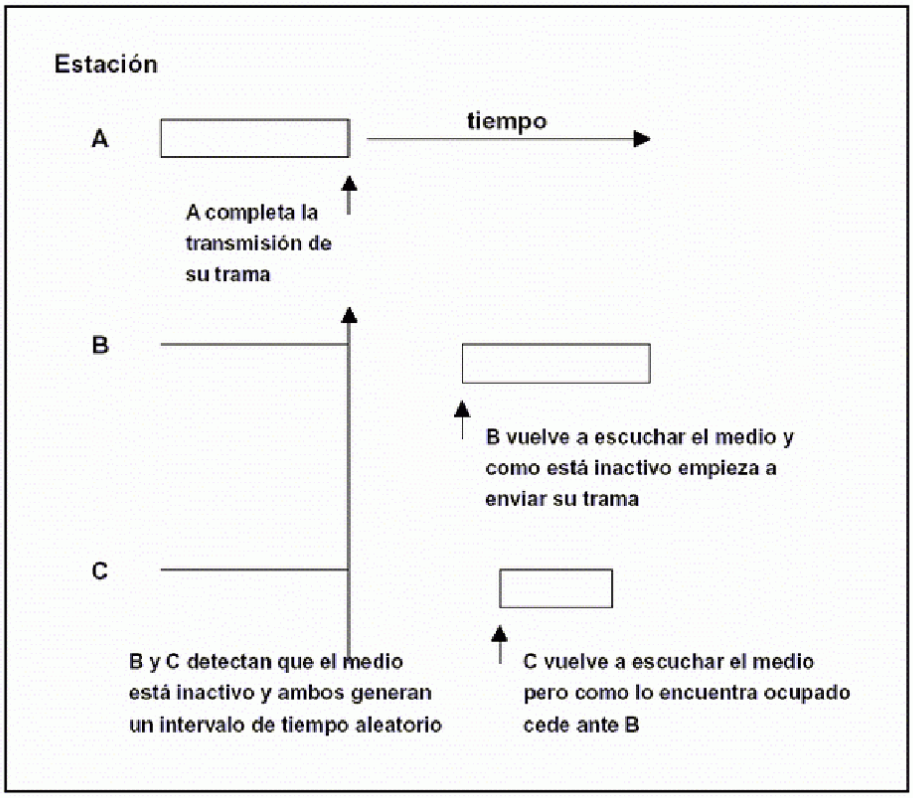


Figura 6. CSMA/CA

La capa MAC opera junto con la capa física probando la energía sobre el medio de transmisión de datos. La capa física utiliza un algoritmo de estimación de desocupación de canales (CCA) para determinar si el canal está vacío. Esto se cumple midiendo la energía electromagnética de la antena y determinando la fuerza de la señal recibida. Esta señal medida es normalmente conocida como RSSI.

Si la potencia de la señal recibida está por debajo de un umbral especificado, el canal se considera vacío, y a la capa MAC se le da el estado del canal vacío para la transmisión de los datos. Si la energía electromagnética está por debajo del umbral, las transmisiones de los datos son retrasadas de acuerdo con las reglas protocolares.

4-El estándar proporciona otra opción, CCA, que puede estar sola o con la medida RSSI. El sentido de la portadora puede usarse para determinar si el canal está disponible. Esta técnica es más selectiva ya que verifica que la señal es del mismo tipo de portadora que los transmisores del 802.11.

En comunicaciones inalámbricas, este modelo presenta todavía una deficiencia debida al problema conocido como de la terminal oculta (o nodo escondido)

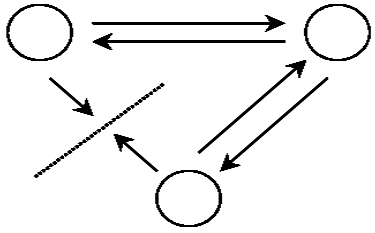


Figura 7. Ejemplo de Nodo Escondido

Un dispositivo inalámbrico puede transmitir con la potencia suficiente para que sea escuchado por un nodo receptor, pero no por otra estación que también desea transmitir y que por tanto no detecta la transmisión.

5-Para resolver este problema, la norma 802.11 ha añadido al protocolo de acceso CSMA/CA un mecanismo de intercambio de mensajes con reconocimiento positivo, al que denomina Reservation-Based Protocol, que se trata en la 2ª subcapa MAC.

Cuando una estación está lista para transmitir, primero envía una solicitud (destino y longitud del mensaje) al punto de acceso (RTS – "request to send") quien difunde el NAV (Network Allocation Vector) -un tiempo de retardo basado en el tamaño de la trama contenido en la trama RTS de solicitud- a todos los demás nodos para que queden informados de que se va a transmitir (y que por lo tanto no transmitan) y cuál va a ser la duración de la transmisión. Estos nodos dejarán de transmitir durante el tiempo indicado por el NAV más un intervalo extra de backoff (tiempo de retroceso) aleatorio. Si no encuentra problemas, responde con una autorización (CTS – "clear to send") que permite al solicitante enviar su trama (datos). Si no se recibe la trama CTS, se supone que ocurrió una colisión y los procesos RTS empiezan de nuevo.

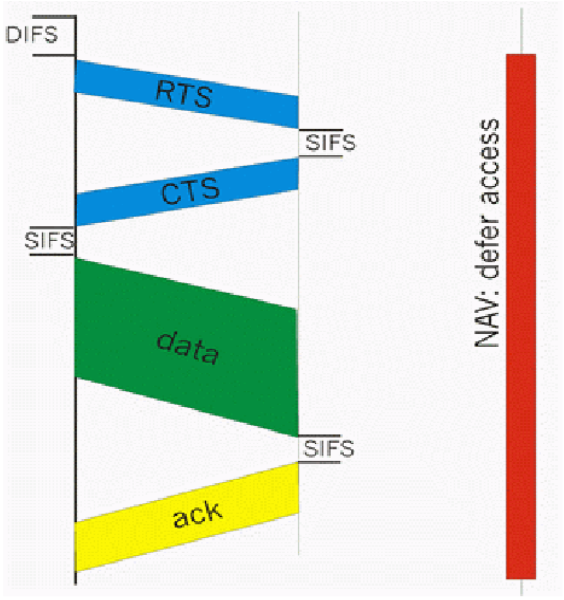


Figura 8. Proceso de transmisión de información

Después de que se recibe la trama de los datos, se devuelve una trama de reconocimiento (ACK - ACKnowledged) notificando al transmisor que se ha recibido correctamenta la información (sin colisiones).

Aún así permanece el problema de que las tramas RTS sean enviadas por varias estaciones a la vez, sin embargo estas colisiones son menos dañinas ya que el tiempo de duración de estas tramas es relativamente corto.

Este mismo protocolo también puede utilizarse si no existen dispositivos auxiliares en las redes ad-hoc, en este caso no aparecería la trama NAV.

6.4. CARACTERÍSTICAS TECNOLÓGICAS

Con todos estos conceptos básicos podríamos definir las redes Wireless como un estándar desarrollado por la **IEEE** (Institute of Electrical and Electronic Engineers) que permite conectar dispositivos mediante una frecuencia de 2,4 Ghz, con drivers que permiten comunicarse a través de los protocolos actuales de comunicación (TCP / IP), disponiendo cada dispositivo de una dirección única a nivel de Hardware (MAC address), y con una potencia de transmisión que va desde los 10-20 mW a los 100 mW (según la FCC(Comisión Federal de Comunicaciones)/ CEPT o la legislación de cada país).

La frecuencia más usada es la de 2.4Ghz. Dicha frecuencia es libre en prácticamente todos los países del mundo, ya que se trata de una frecuencia reservada para la investigación, educación o sanidad. Sin embargo en muchos países determinadas frecuencias dentro de los 2.4 Ghz están reservadas por el ejército o los gobiernos. Es por eso que hay que tener a veces cuidado con las compras fuera de España, ya que podemos comprar determinados productos que tengan cerrados algunos canales.

En la tabla adjunta se observa la relación entre los canales y la frecuencia.

Relación entre canal y frecuencia	
Canal	**Frecuencia**
1	2.412 Ghz
2	2.417 Ghz
3	2.422 Ghz
4	2.427 Ghz
5	2.432 Ghz
6	2.437 Ghz
7	2.442 Ghz
8	2.447 Ghz
9	2.452 Ghz
10	2.457 Ghz
11	**2.462 Ghz**
12	2.467 Ghz
13	2.472 Ghz
14	2.484 Ghz

En la siguiente tabla podemos ver los canales disponibles (no olvidar que están relacionados con la frecuencia) dependiendo de cada país:

Países y Canales	
Países	**Canales**
Europa (ETSI)	1 - 13
USA (FCC)	1 - 11
Francia	10 - 13
Japón	1 - 14

Por último recordar que la legislación española o europea no es muy clara al especto, y que en un principio no podemos emitir más allá de los 100 mW fuera de las paredes de nuestra casa o despacho. Esto es lógico sabiendo que la mayoría de dispositivos están limitados por la FCC/CEPT a esa cantidad, aunque podamos encontrar algunas excepciones, como por ejemplo la tarjeta Senao que alcanza los 200 mW. Es decir, sin ningún tipo de modificación por nuestra parte de cualquier dispositivo Wireless, estamos dentro de la legalidad. Si lo modificamos de una manera u otra para conseguir más potencia, podríamos encontrarnos con un problema legal. Lo que no está legislado tampoco es la existencia de antenas en nuestras instalaciones Wireless. Dichas antenas nos permitirían ampliar el radio de acción en el caso de las antenas Omnidireccionales, o la conectividad con un vecino a más metros de distancia mediante una antena sectorial (un ángulo medio de unos 45º) o una direccional (un ángulo cerrado de unos 20º). Dichas antenas no aumentan la potencia emitida, sino que nos da más ganancia en la calidad de la señal, pudiendo llegar más lejos y con más ancho de banda.

7. BIBLIOGRAFÍA

-Página web del IEEE: "http://grouper.ieee.org/groups/802/11" o "http://www.ieee802.org/11".

-Web del estándar Wi-Fi (WECA) 802.11b: "http://www.wi-fi.com".

-NATHAN, J. Muller. “Wi-Fi for the enterprise”. Ed. McGraw-Hill. 2003 United States of America.

-Portales de Internet sobre grupos wireless :"http://madridwireless.net", "http://www.matarowireless.net".

-Portal sobre seguridad inalámbrica "http://www.airdefense.net".

-Portales sobre wireless: "http://www.newswireless.net", "http://www.communitywireless.org".

-Portal relacionado con dispositivos portátiles: "http://www.mipcdebolsillo.com".

-Documentación "Redes Inalámbricas: IEEE 802.11" de Enrique de Miguel Ponce y cols.

- Documento : “Seguridad en WiFi” de Alejando Corletti Estrada. 2005