

Ataques en 802.11

**Giovanni Zuccardi
Juan David Gutiérrez**

Noviembre 5 de 2006

Contenido

- 1.** Definición
- 2.** Ataques al WEP
 - 2.1.** Ataque de fuerza bruta
 - 2.2.** Ataque Inductivo Arbaugh
 - 2.3.** Ataque al metodo Shared Key
- 3.** Ataque contra el ACL(Access Control List) basados en MAC
- 4.** Ataque de denegación de servicio
- 5.** Descubrir ESSID ocultos
- 6.** Ataque Man in the Middle
- 7.** Ataque ARP Poisoning
- 8.** Espionaje (surveillance)
- 9.** Referencias
- 10.** Bibliografía

Ataques en 802.11

1. Definición

Las redes 802.11 tienen vulnerabilidades únicas que las hacen ideales para realizar un ataque. Estas no pueden ser aseguradas físicamente como las redes alámbricas.

Un ataque contra redes inalámbricas puede llevarse a cabo en cualquier lugar: desde la oficina de al lado, desde el parqueadero de tu edificio, cruzando la calle en un parque o alejado varios kilómetros.

Los ataques realizados en contra de IEEE 802.11 se pueden clasificar en pasivos y activos, según la clasificación propuesta por Gonzalo Álvarez en su documento [GAPPP], la cual se resume a continuación.

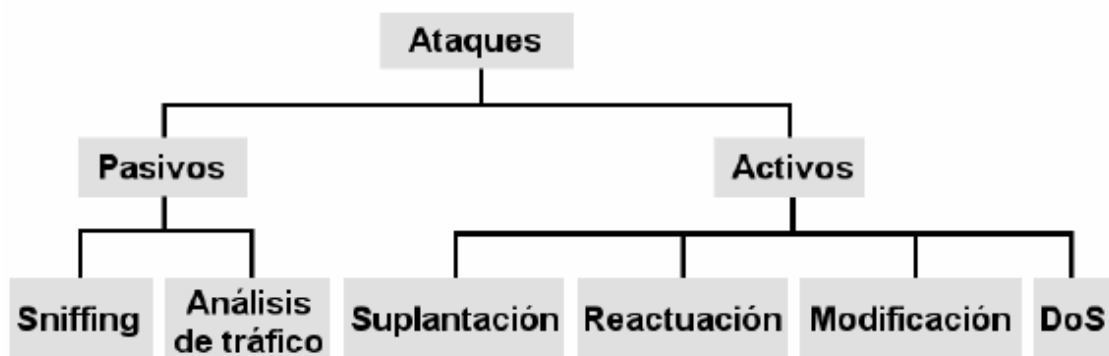


Figura 1: Tipos de Ataques. [GAPPP].

Según lo anterior los ataques pasivos se dividen en Sniffing y Análisis de tráfico.

El **Sniffing** es posible en las redes inalámbricas gracias a que puede espiarse con mucha facilidad comparado a una LAN. Para realizar esto solo es necesario un portátil con una tarjeta inalámbrica y podrá ser capturado el tráfico que no haya sido cifrado y el cifrado con WEP también.

El **Análisis de tráfico** es aquel en el que el atacante obtiene información por el simple hecho de analizar el tráfico y sus patrones, por ejemplo a qué hora se encienden ciertos equipos, cuánto tráfico envían, durante cuánto tiempo, etc.

Los ataques activos se pueden dividir en suplantación, reactuación, modificación y denegación del servicio (Denial-of-Service).

La **suplantación** consiste en hacerse pasar por otro equipo mediante la captura de tráfico, es decir mediante un sniffer obtener varias direcciones MAC válidas, conociendo a que horas debe conectarse suplantando un usuario u otro. Otra forma de suplantación consiste en la instalación de access point fantasmas o ilegítimos (rogue) engañando a los usuarios legítimos quienes se conectan a este en lugar de a un access point autorizado.

La **modificación** consiste en capturar ciertos paquetes para luego ser borrados, manipulados, modificados o reordenados por el atacante.

La **reactuación** consiste en inyectar en la red paquetes interceptados utilizando un sniffer para repetir operaciones que habían sido realizadas por el usuario legítimo.

La **denegación de servicio** consiste en generar interferencia hasta que se produzcan tantos errores en la transmisión que la velocidad caiga a extremos inaceptables o la red deje de operar en absoluto. También es posible mediante la inundación de solicitudes de autenticación, solicitudes de desautenticación de usuarios legítimos, tramas RTS/CTS para silenciar la red, etc.

2. Ataques al WEP

2.1. 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 utilizan 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 más 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 necesitamos 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.

2.2. Ataque Inductivo Arbaugh

Demostrado teóricamente por William A. Arbaugh (Universidad de Maryland). Este ataque se basa en explotar la vulnerabilidad de MIC independiente de la llave [VUL802.11] aprovechando también la redundancia de información producida por el CRC.

La estación receptora en WEP únicamente aceptará un mensaje si el ICV (Integrity Check Value) 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
- Los CRCs son lineales: $CRC(m \oplus k) = CRC(m) \oplus CRC(k)$

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' :

$$m' = m \oplus \Delta$$

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

$$IC' = IC \oplus h(\Delta)$$

- ICV' será valido para el nuevo cyphertext c'

$$c' = c \oplus \Delta = k \oplus (m \oplus \Delta) = k \oplus m'$$

Todo este proceso se puede resumir en la siguiente grafica:

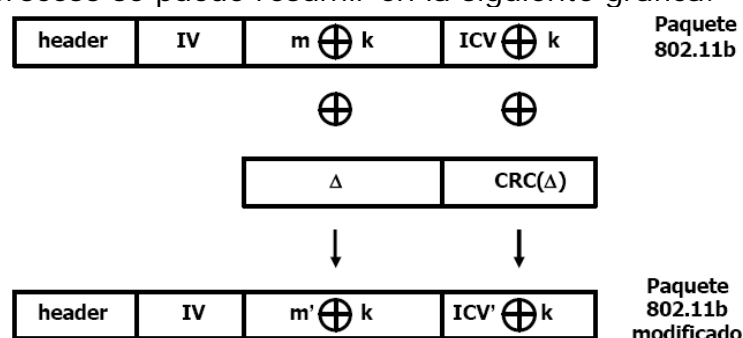


Figura 3: Modificación de un paquete. [INSEG]

2.3. Ataque al metodo Shared Key

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.

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.

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 desafío aleatorio, R, y el flujo pseudo-aleatorio WEP k,IV PR y genera el cuerpo de una trama *Authentication 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.

3. Ataque contra el ACL (Access Control List) basados en MAC

Para llevar a cabo el ataque basta con hacer sniffing 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.

4. Ataque de denegación de servicio

Para realizar este ataque basta con hacer sniffing 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.

5. Descubrir ESSID ocultos

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 inalámbrica. Una medida de seguridad bastante común es "ocultar" el ESSID, 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 hacer sniffing y esperar a que un cliente se conectara, y veríamos el ESSID en la trama Probe Request del cliente (en el caso de que no se manden Beacon Frames), o en la trama Probe 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 de Desautenticación o Disociación 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.

6. 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.

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 hace spoofing (suplantación) de su MAC haciéndose pasar por el AP y manda tramas de desautenticación 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.

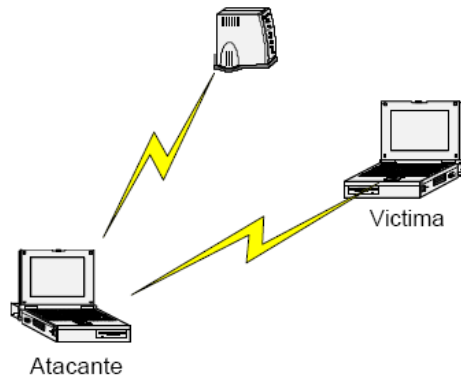


Figura 2: Ataque Man in the Middle. [INSEG]

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.

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 según que tipo de solución podría no ser adecuado para estas redes.

7. 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:

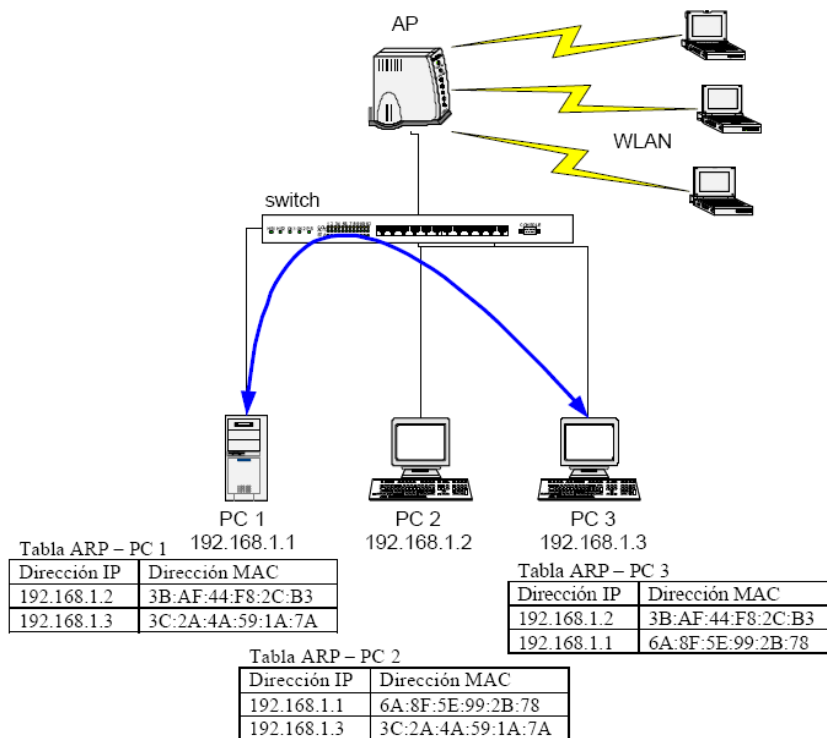


Figura 3: Ataque ARP Poisoning. [INSEG]

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:

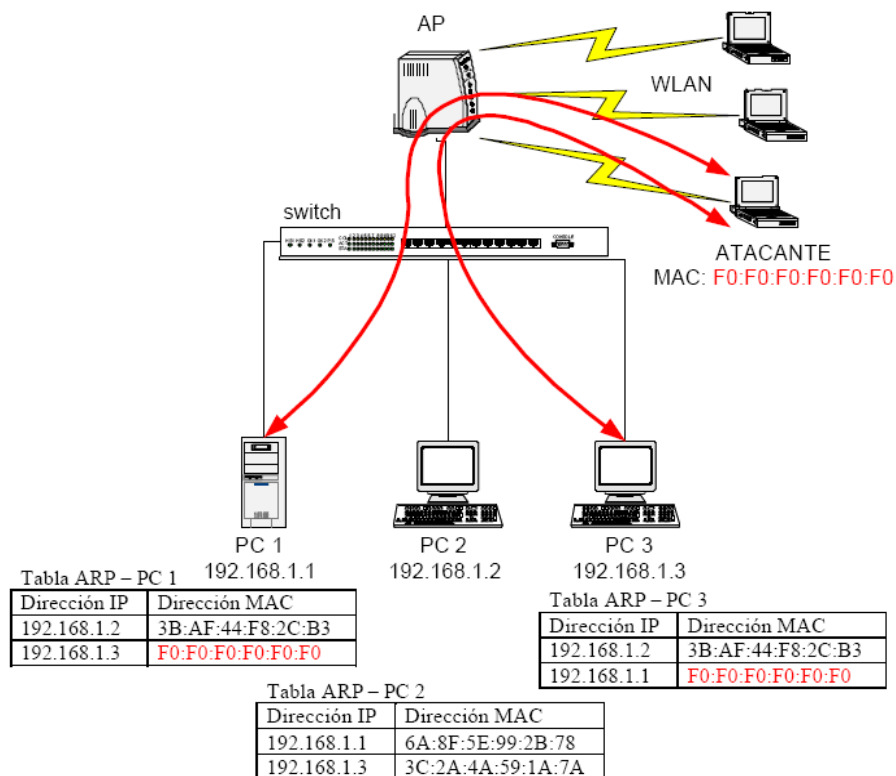


Figura 4: Despues del Ataque ARP Poisoning. [INSEG]

El atacante manda paquetes "ARP REPLY" a PC 3 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 3. Luego realiza la misma operación atacando a PC 1 y haciéndole creer que la dirección IP de PC 3 la tiene también su propia MAC.

Como ARP es un protocolo "stateless", PC 1 y PC 3 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.

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.

8. Espionaje (surveillance)

Este tipo de ataque consiste simplemente en observar el entorno donde se encuentra instalada la red inalámbrica. No se necesita ningún tipo de "hardware" o "software" especial. Sirve para recopilar información y se puede combinar con otros tipos de ataques

Qué observar	Localización
Antenas	muros, techos, tejados, pasillos, ventanas, entradas
Puntos de acceso	muros, techos, falsos techos
Cables de red	atravesan techos, muros, paredes
Dispositivos-scanners/PDAs	personal de la empresa

Tabla 1. Recomendaciones espionaje[SEGW104]

War-Chalking

Se trata de un lenguaje de símbolos utilizado para marcar sobre el terreno la existencia de las redes inalámbricas, de forma que puedan ser utilizadas por aquellos que "pasen por allí".

Es decir, es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico.

En este tipo de ataque los símbolos eran pintados con tiza ("chalk" en inglés) aunque actualmente se utilizan otros medios, como la pintura normal, spray de color, etc. El significado de cada símbolo existente es el siguiente:

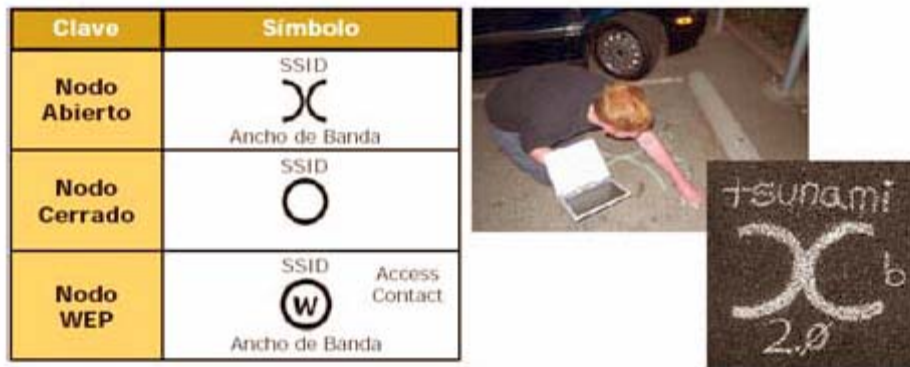


Figura 5. War-Chalking[SEGWI04]

War-driving

Es el método más conocido para detectar las redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como una notebook o un PDA. El método es realmente simple: el atacante pasea con el dispositivo móvil, y en el momento en que detecta la existencia de la red, se realiza un análisis de la misma.

El dispositivo móvil puede estar equipado con un sistema GPS para marcar la posición exacta donde la señal es más fuerte, o incluso una antena direccional para recibir el tráfico de la red desde una distancia considerable.

Si la red tiene DHCP, el dispositivo móvil se configura para preguntar continuamente por una IP dentro de un cierto rango, si la red no tiene DHCP activado se puede ver la IP que figure en algún paquete analizado.

Existen varias herramientas útiles para detectar redes inalámbricas, las más conocidas son el AirSnort o Kismet para Linux y el NetStumbler para sistemas Windows.

Para realizar el Wardriving se necesitan realmente pocos recursos. Los más habituales son una computadora portátil con una tarjeta inalámbrica, un dispositivo GPS para ubicar el PA en un mapa y el software apropiado (AirSnort para Linux, BSD- AriTools para BSD o NetStumbler para Windows).



Figura 6. War-Driving[SEGWI04]

En la figura 6, los puntos rojos indican nodos protegidos (WEP Activado) y los puntos verdes están desprotegidos (WEP Desactivado).

9. Referencias

- [GAPPP] "Seguridad en redes inalámbricas WiFi". Gonzalo Álvarez Marañon - Pedro Pablo Pérez García. Consultado el 2/11/2006 de <http://www.iec.csic.es/gonzalo/descargas/SeguridadWiFi.pdf>.
- [VUL802.11] "Vulnerabilidades 802.11", Giovanni Zuccardi – Juan David Gutiérrez. <http://pegasus.javeriana.edu.co/~edigital/index-1.html>.
- [INSEG] "(In)seguridad en redes 802.11b", Oliva Fora, Pau. Consultado el 23/09/2006 de http://www.eslack.org/pof/In-Seguridad_802.11b.pdf.
- [SEGWIO4] SEGURIDAD EN REDES WIRELESS –Seguridad Informática – 2004. Israel Cors y Patricia Pernich

10. Bibliografía

- [1] Álvarez Marañon, Gonzalo - Pérez García, Pedro Pablo. "Seguridad en redes inalámbricas WiFi". Consultado el 2/11/2006 de <http://www.iec.csic.es/gonzalo/descargas/SeguridadWiFi.pdf>
- [2] Fleck, Bob – Potter, Bruce. "802.11 Security". Editorial O'Reilly 2002. Pág. 208
- [3] Oliva Fora, Pau. "(In)seguridad en redes 802.11b". Consultado el 23/09/2006 de http://www.eslack.org/pof/In-Seguridad_802.11b.pdf.