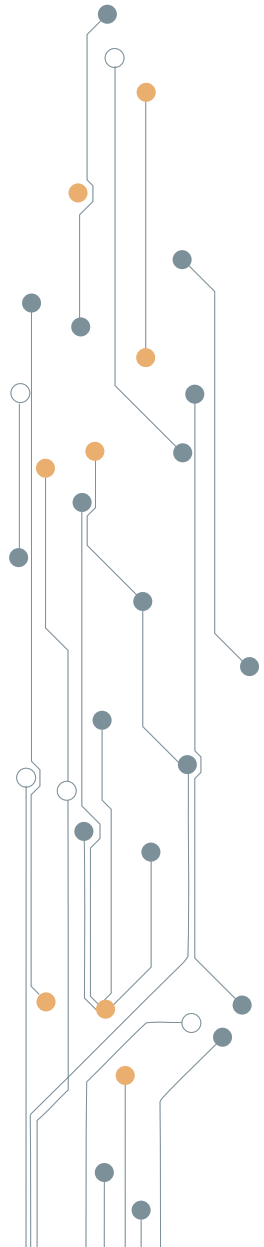
Conceptos básicos y cifrado Wireless

Telefónica EDUCACIÓN DIGITAL

Índice



1 | Introducción y conceptos básicos	3
2 | Cifrado Wireless	6
2.1 | Abierto	6
2.2 | WEP	12
2.3 | WPA/WPA2	22

1. Introducción y conceptos básicos

Se denomina red inalámbrica a la red que utiliza el medio electromagnético para transmitir información. Dicha red está compuesta por un punto de acceso (PA) al que los demás dispositivos se conectan. Podemos diferenciar tres categorías en redes inalámbricas dependiendo de su cobertura:

- WAN/MAN: Wide Area Network /Metropolitan Area Network.
- LAN: Local Area Network.
- PAN/WPAN: Personal Area Network/Wireless Personal Area Network, red inalámbrica sin cables que se extiende en un espacio de uso personal.

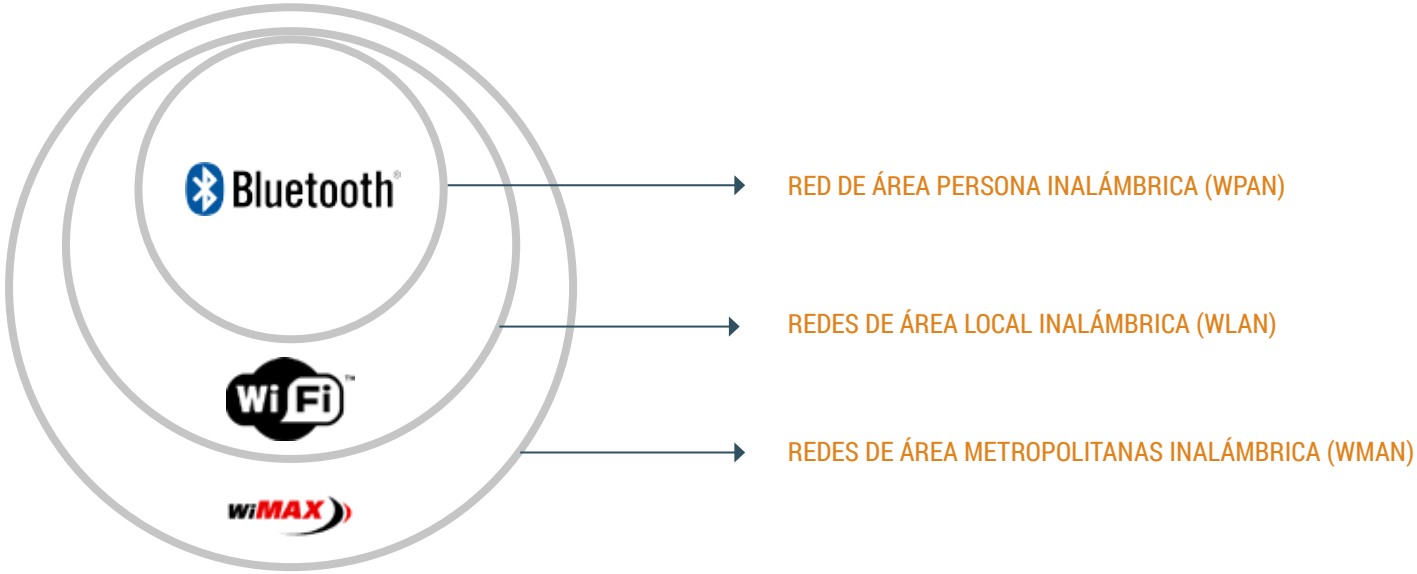


FIGURA 1.1 REDES INALÁMBRICAS

Este tipo de redes tiene ventajas evidentes como la eliminación de cableado o la movilidad, pero tiene también una desventaja considerable: la seguridad. Las redes inalámbricas son inseguras de forma intrínseca y muy vulnerables frente a ataques de seguridad.

Los estándares que rigen las redes inalámbricas son los que fueron creados por la IEEE (Instituto de ingenieros eléctricos y electrónicos), siendo el más utilizado el 802.11n. Este estándar soporta velocidad de transmisión de hasta 600 Mbps y opera en la banda 2,4 GHz y 5GHz.

WiFi (Wireless Fidelity) es el nombre con el que se bautizó al estándar que describe los productos WLAN que se rigen por los estándares 802.11. Para poder estudiar en profundidad la seguridad en redes inalámbricas debemos conocer primero varios conceptos importantes:

Punto de acceso (AP/PA)

Se trata de un elemento de red que interconecta diferentes dispositivos en un entorno inalámbrico para poder formar una red. Básicamente ejerce funciones de puente entre una red Ethernet cableada y una red inalámbrica. Su configuración permite enlazar varios AP para ampliar la huella de cobertura de la red pudiendo proporcionar la configuración TCP/IP mediante un servicio DHCP.

Lista de control de acceso (ACL)

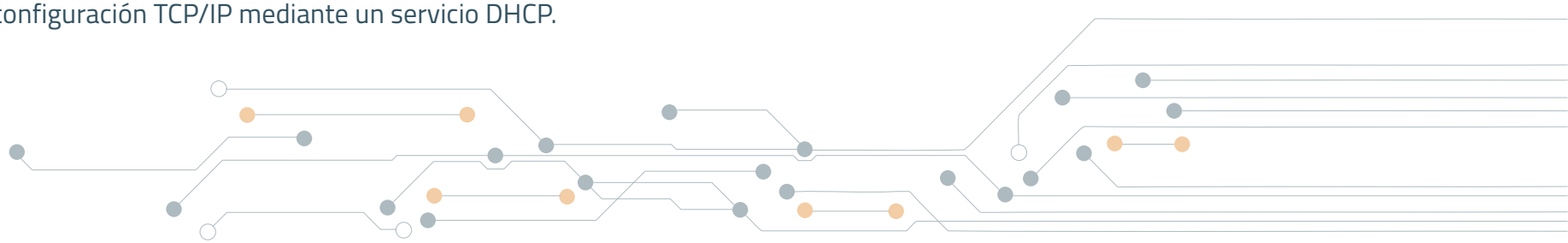
Significa Access Control List y ese encarga de controlar la unión a la red sólo a los dispositivos cuya MAC esté añadida en la lista de direcciones MAC permitidas.

CNAC

Es el acrónimo de Closed Network Access Control. Se trata de otro método de control de acceso que evita que un determinado dispositivo acceda a la red si no tiene conocimiento previo del SSID identificativo.

ESSID/SSID

Las redes inalámbricas tienen un código identificativo denominado ESSID (Extended Service Set Identifier), que está compuesto por un máximo de 32 caracteres alfanuméricos y es sensible a mayúsculas. Necesitamos conocer el ESSID del punto de acceso para ser un componente de la red, ya que tanto el dispositivo móvil, como el punto de acceso tendrán el mismo ESSID. De forma general, nos podemos referir a este identificador en términos de WLAN como SSID (Service Set Identifier). Generalmente, el SSID es conocido como nombre de la red.



BSSID

Se trata de otro código identificativo (Basic Service Set Identifier), con el que se puede identificar a los clientes o dispositivos que están conectados a un AP. Corresponde a la dirección MAC del AP.

Beacon Frames

Es información enviada constantemente por el punto de acceso con el objetivo de que los dispositivos puedan conocer la presencia de la red y posteriormente conectarse a ella. En cada trama se incluye el ESSID, ya que, como se acaba de indicar, el dispositivo móvil y el punto de acceso deben tener el mismo ESSID.

CANAL

Un canal es una determinada banda de frecuencia, destinada exclusivamente a los usuarios de una red bajo la cobertura de un determinado Access Point.

OSA (Open System Authentication)

OSA es el método de identificación por el cual las tramas se envían en texto plano y cualquier dispositivo puede conectarse al Access Point, ya que la autenticación es nula.

SKA (Shared Key Authentication)

Este método incorpora autenticación, utilizando una clave de encriptación compartida de la que tanto el Access Point como el cliente disponen. El sistema consiste en la solicitud de autenticación (Authentication Request) por parte del cliente. Comienza entonces un diálogo en el que el Access Point devuelve un AC (Authentication Challenge), mediante el envío de una trama. Si el cliente devuelve la trama correctamente codificada mediante un Authentication Response, el Access Point le permitirá finalmente establecer comunicación mediante un Authentication Result.

2. Cifrado Wireless

2.1 | Abierto

Como su propio nombre indica las redes abiertas no tienen implementado un sistema de cifrado. La información que viaja entre el cliente y el Access Point lo hace en texto plano y ningún dato es solicitado para realizar una conexión. Es posible aportar un mínimo grado de seguridad mediante diferentes configuraciones en cuanto a direcciones MAC, direcciones IP y el ESSID. Por ejemplo, podemos filtrar el acceso a usuarios con una determinada dirección MAC o IP, podemos bloquear el envío automático de BEACON FRAMES de forma que el usuario deba conocer previamente el valor de ese ESSID para poder acceder a la red, etc.

Ataques en redes abiertas

Como acabamos de comentar la seguridad en este tipo de redes es muy escasa, por tanto, y aunque implementemos algunas medidas como las mencionadas, debemos tener en cuenta que con ellas sólo limitamos el acceso a usuarios sin autorizar. Estas medidas no impiden que un atacante pueda espiar nuestras comunicaciones. A continuación, vamos a estudiar cómo podemos saltarnos las medidas anteriores y otros tipos de ataques a los que son vulnerables las redes abiertas.

Mac Spoofing

Se basa en la suplantación de la MAC del dispositivo que está realizando el ataque, además de instalar una MAC autorizada en la ACL (Access Control List).

Uno de los métodos rudimentarios de control de acceso de las redes abiertas, es realizar este tipo de ataque que genera un listado de direcciones MAC en el AP, especificando también el acceso permitido o denegado de cada entrada de la lista. Queda evidenciada la validez de este método de seguridad ante la facilidad de cambiar las direcciones MAC, sustituyendo una determinada por otra que hayamos averiguado previamente a través de un sencillo sniffer.

Para este sencillo sniffer basta con estar en su misma red, observar la MAC de cualquier cliente y la restricción ya habrá sido saltada. Esto es muy fácil de implementar, por ejemplo en Linux podemos hacer uso del comando ifconfig dependiendo de la tarjeta que tengamos. Además contamos con otros para modificar la MAC, como es el caso de setmac.

Debemos destacar que, aunque el hecho de que haya varias direcciones MAC en una red puede generar contrariedades, es muy sencillo tumbar la otra dirección MAC mediante un ataque de denegación de servicio a la máquina a la que hemos robado dicha dirección MAC.

Ataque de denegación de servicio

Consiste en la inhabilitación de conexión entre el cliente y el Access Point. Lo único que necesitamos hacer es conseguir la dirección MAC del Access Point (a través de un sniffer, por ejemplo) y una vez que la hayamos conseguido, nos pondremos su dirección simulando ser el Access Point y negando la conexión al cliente específico enviando constantemente notificaciones (Management frames) de desasociación. Si buscamos denegar el servicio al total de los usuarios de la WLAN en lugar de a uno en concreto, será necesario enviar esta notificaciones en forma de tramas, a la dirección MAC de broadcast.

Las herramientas más comunes para poder llevar a cabo este ataque son las siguientes:

- Wlan-jack: forma parte del conjunto de utilidades air-jack. Se puede localizar en: **http://802.11ninja.net**
- Dassoc: herramienta que manda tramas de desasociación. Podemos encontrarla en **http://www.atstake.com**

Fuerza bruta a SSID ocultos

Como se ha indicado antes, un cliente y un Access Point deben tener configurado el ESSID para que puedan establecer una conexión. En otras palabras, deben mantenerse en la misma red inalámbrica.

Una medida de seguridad muy extendida es no mostrar el ESSID, ocultando la red y realizando la configuración oportuna para que el Access Point no envíe automáticamente BEACOM FRAMES, y si los manda, que no incluya el ESSID en ellos.

Con esta configuración, si queremos averiguar el ESSID tenemos que esnifar la red, y esperando a que un usuario se conecte, podríamos ver el ESSID en el mensaje PROVE REQUEST del usuario (si no se envían BEACON FRAMES), o en el mensaje PROVE RESPONSE del Access Point.

Otra alternativa es forzar la interrupción de conexión de un usuario, usando un sistema similar que en la denegación de servicio (DoS), pero enviando solamente un mensaje de desasociación o desautenticación en vez de hacerlo varias veces periódicamente. En esencia, establecemos la dirección física del Access Point y enviamos un mensaje DESAUTH o DISASSOC a la MAC del usuario (o a la MAC de broadcast). Esto provocará que el usuario intente volver a autenticarse, pudiendo averiguar el ESSID que aparece en los Management frames.

Para este tipo de ataque la herramienta más común es essid-jack, que de la misma forma, forma parte del paquete air-jack para Linux. Podemos encontrarla en **http://802.11ninja.net**

Man in the Middle para AP

En el ataque Man in the Middle en redes inalámbricas el atacante tiene por objetivo hacer creer a la víctima que el host que se ha situado en medio de la comunicación es el Access Point, cuando en realidad es el dispositivo utilizado por el atacante. También tiene como objetivo hacer pensar al Access Point que el dispositivo del atacante es el usuario.

Para llevar a cabo este tipo de ataque el primer paso es esnifar para conseguir los siguientes datos:

- ESSID de la red.
- Dirección MAC del Access Point.
- Dirección MAC de la víctima.

Cuando consigamos esta información usaremos el mismo sistema que en el ataque de denegación de servicio, con el fin de desautenticar a la víctima del Access Point verdadero. Dicho de otra manera, el intruso spoofea su dirección MAC simulando ser el Access Point y envía tramas DEAUTH a la víctima. La tarjeta WiFi de la víctima comenzará a realizar escaneos de canales buscando un Access Point para poder autenticarse. Es entonces cuando el atacante simulará ser el Access Point, usando su MAC y su ESSID (el ESSID al que la víctima estaba conectada antes) pero en un canal diferente (para todo eso es necesario que la tarjeta WiFi del atacante esté en modo master).

El segundo paso es que el atacante se asocie con el Access Point verdadero usando la dirección MAC de la víctima.

Una vez completado el segundo paso habremos logrado introducir al atacante entre la conexión de la víctima y el Access Point, consiguiendo que todos los paquetes enviados desde la víctima al Access Point y viceversa circulen también por el atacante.

FIGURA 2.1.1. MAN IN THE MIDDLE 1

Debido a que el ataque es en la capa 2, las tramas son susceptibles de ser vistas, capturadas e incluso modificadas en las capas superiores de OSI.

Es muy sencillo desarrollar este modelo de ataques usando el driver air-jack mediante la herramienta monkey-jack.

Un último aspecto a tener en cuenta es que muchas de las soluciones son diseñadas dando por hecho que las capas 1 y 2 son seguras. Debemos prestar especial atención en desarrollos como VPN, en la que algunas comprobaciones de autenticación no son realizadas.

Bypass DHCP

En muchas circunstancias, los usuarios se conectan a redes inalámbricas que se encuentran abiertas, es decir, no hay cifrado entre el punto de acceso y los clientes que se conectan a estas redes. Esto quiere decir, que cualquier persona que disponga de un adaptador wireless, que pueda configurarse en modo monitor podría "leer" el tráfico que circula entre el punto de acceso y los clientes conectados. En otras ocasiones, se puede conseguir el tráfico en una red inalámbrica con cifrado WEP o WPA/2, la gran diferencia es que éste se encuentra cifrado y, a priori, no se puede visualizar.

La herramienta airdecap-ng es una herramienta de la suite aircrack-ng. La herramienta permite descifrar el tráfico cifrado que se tenga en un archivo PCAP. El archivo PCAP se puede conseguir a través del uso de herramientas como airodump-ng. Hay que recordar que esta herramienta permite "dumpear o volcar" todo el tráfico que circula en el medio de comunicación que es el aire.

Es importante ver si el tráfico entre punto de acceso y clientes está cifrado, ya que, en función de esto, se tendrá acceso al tráfico en plano, como es el caso de las redes abiertas, o tráfico cifrado con WEP o WPA/2 en redes más seguras, al menos las WPA2.

Las tramas en plano significan que la red no tiene ningún tipo de cifrado, por lo que si se configura la herramienta airodumpg-ng para capturar lo que circula por el aire se podrá visualizar el tráfico HTTP, FTP, SMTP y otros protocolos que no dispongan de cifrado propio. De este modo, se pueden capturar credenciales sin necesidad de realizar, por ejemplo, ARP Spoofing, o capturar cookies para realizar hijacking de una sesión HTTP.

Escenario: saltar protección DHCP en un punto de acceso no abierto

En este escenario se utilizará la herramienta airdecap-ng para descifrar el tráfico de una red, de la cual se conoce la clave o se ha obtenido la clave en un ataque wireless. El objetivo del escenario es el siguiente:

- Bypass DHCP del punto de acceso o router.
- Realizar técnica Man in the Middle, sin estar conectado o asociado al punto de acceso.

El punto de partida es conocer la clave de la red WiFi o haberla obtenida en un ataque wireless. Cuando el usuario se conecta a la red, el DHCP no le asigna direcciones IP, ni servidor DNS, ni puerta de enlace. ¿Qué ocurre? El dueño o propietario de la red ha configurado una medida de protección básica en redes inalámbricas, como es la

configuración de red manual. El que entra a la red debe conocer el rango de la red, es decir, la máscara de red, el direccionamiento y todos los datos relativos a la configuración de red, ya que no habrá DHCP que proporcione estos datos. No es una gran medida de seguridad, es considerada básica, pero suma en poner las cosas difíciles.

Mediante el uso de airodump-ng -w <fichero PCAP> mon0 (o la interfaz WiFi en modo monitor que se disponga), se obtiene el tráfico que hay en el aire dentro de nuestro radio wireless. Una vez generado el fichero PCAP hay que tratarlo con airdecap-ng. Esta herramienta dispone de una sintaxis muy sencilla y diferenciada para redes de tipo WEP y WPA.

- Para una red de tipo de cifrado WEP, se debería ejecutar la siguiente instrucción para descifrar el tráfico: airdecap-ng -w CLAVE HEXADECIMAL SIN PUNTOS <archivo PCAP>. Para sacar la clave en hexadecimal, se puede ejecutar echo -n <clave ASCII> | xxd -p.
- Para una red de tipo WPA, se debe ejecutar airdecap-ng -e <nombre de la red> -p <clave WPA> <archivo PCAP>. Se necesita que el handshake de la conexión de algún usuario legítimo de dicha red se encuentre en el archivo PCAP, pero esto puede lograrse de forma sencilla con los ataques de desautenticación de la red.

```
                                airdecap-ng -e wireless -p 1234567891234  captura-01.cap
Total number of packets read          9455
Total number of WEP data packets         0
Total number of WPA data packets       113
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         8
```

Una vez se obtiene el fichero PCAP descifrado, se puede investigar los rangos de red que los usuarios legítimos de la red están trabajando. Por ejemplo, si se visualiza en el fichero PCAP descifrado, que hay un usuario con la dirección IP 192.168.56.12, se puede entender que el router o punto de acceso trabaja en una red parecida a 192.168.56.0, dónde la máscara de red sería /24, generalmente.

¿Y el MiTM? En este fichero descifrado se puede ir viendo todos los paquetes de las víctimas, por lo que todo lo que haya ido por protocolos no seguros, como HTTP, FTP, SMTP, etcétera, está al alcance de cualquiera. Por esta razón, es fácil realizar un Man in the Middle en entornos de redes WiFi abiertos, que sería otro escenario distinto a este, pero muy potente. Cuando se utilizan redes inalámbricas abiertas, como son centros comerciales, restaurantes, hoteles, etcétera, hay que tener esto en cuenta, y no realizar operaciones sensibles o vitales, como consultar cuentas bancarias o correo electrónico importante, etc.

2.2 | WEP

WEP, o como deberíamos decir Wired Equivalent Privacy es un protocolo de cifrado incluido en IEEE 802.11 destinado a las redes Wireless. Utiliza el algoritmo RC4 para cifrar las llaves de 64 o 128 bits. Realmente son 40 o 104, ya que 24 bits son utilizados en el Vector de Inicialización. La seguridad que proporciona está muy limitada, ya que sus sistemas son obsoletos y son muy conocidos los métodos para el descifrado de la información de las tramas que se cifran con este método. Dicha seguridad tiene como base una clave secreta compartida que se utiliza para el cifrado de todos los datos que se envían.

Para comprender el funcionamiento de este protocolo debemos distinguir entre tres aspectos diferentes: la autenticación, la confidencialidad y por último, la integridad.

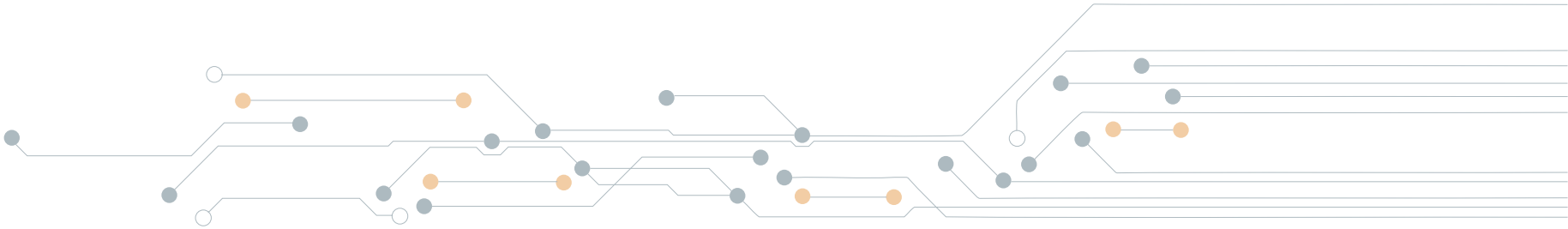
Existen dos métodos de autenticación: Open System y Shared Key.

Open System permite que todos los usuarios se autentiquen en el Access Point. Por el contrario, con Shared Key es necesario que el usuario mande una solicitud de conexión. Entonces el Access Point responde con un desafío, que debe ser cifrado por el cliente y enviado al Access Point. Si el Access Point puede descifrar el mensaje se dará por válida la autenticación.

En segundo lugar tenemos el paso de confidencialidad, que cuenta con una serie de elementos clave:

- RC4: se trata del algoritmo usado para la generación del keystream.
- IV: vector de inicialización. Se trata del fragmento dinámico del keystream. Cada una de las tramas lleva un vector de inicialización distinto, siendo generados de forma aleatoria. Este fragmento dinámico no está cifrado en la trama WEP.

RC4 es simétrico, ya que se puede descifrar con la misma clave que se cifra.



En el siguiente esquema se procede a explicar el procedimiento que se debe completar cuando se forma la trama WEP que posteriormente se mandará, independientemente de si se trata la del usuario o la del Access Point (el proceso es el mismo).

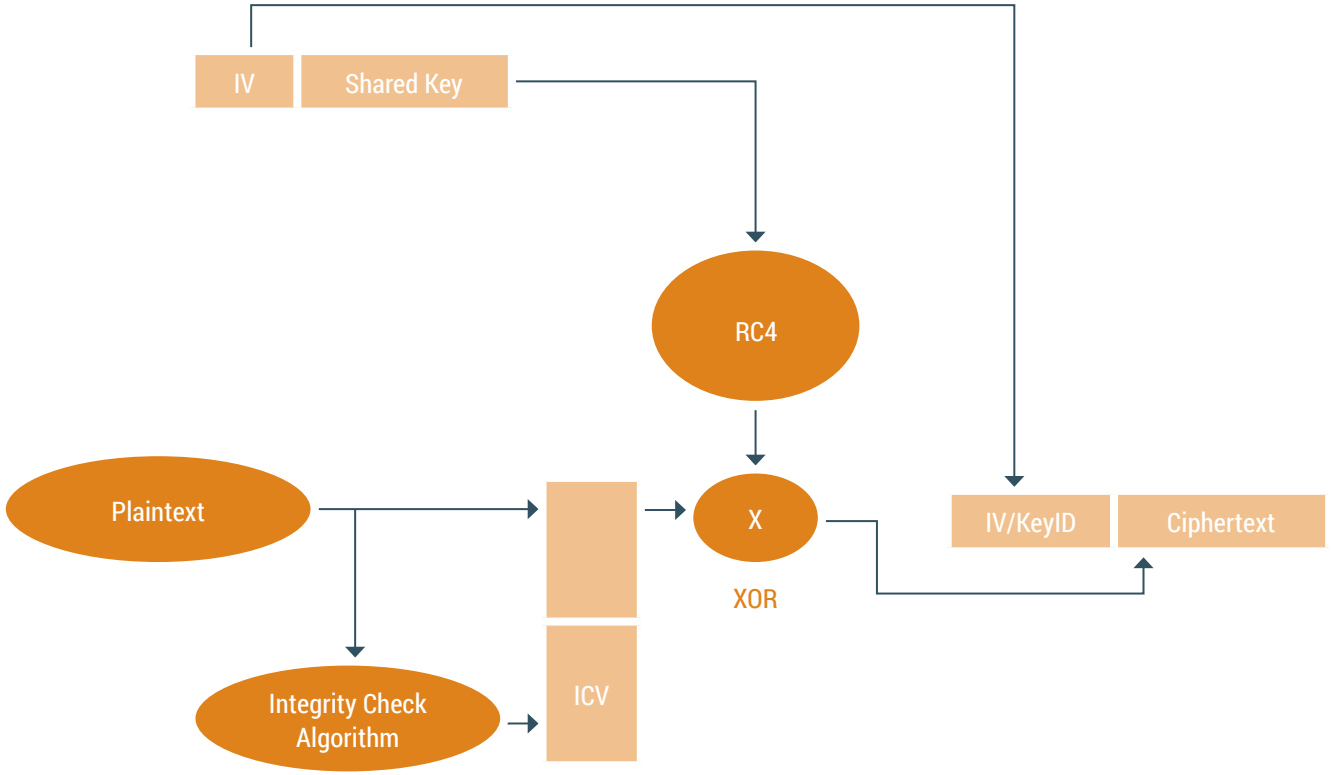


FIGURA 2.2.1 ENCRIPTACIÓN WEP 1

- La shared key es estática. Se trata de una clave que ha sido configurada por el propietario de la red en el Access Point.
- Los IV cambian de forma aleatoria en cada trama que se envía. El vector de inicialización se concatena con la clave estática convirtiéndose en la entrada de datos para el algoritmo RC4. La salida de este algoritmo es el KEYSTREAM.
- El KEYSTREAM creará el cifrado utilizando la operación matemática XOR.
- El fragmento cifrado de la trama WEP es el resultado de la operación XOR entre el KEYSTREAM y el tráfico plano sin cifrar.
- La integridad se obtiene sobre el texto plano, a través del ICV.
- Para poder comprender plenamente el funcionamiento debemos recordar que XOR es una operación de disyunción que solamente es verdadera si ambas entradas corresponden a valores diferentes.

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

FIGURA 2.2.2 TABLA XOR 1

XOR puede generar el resultado inicial con su inversa, ya que sólo cuando A y B son iguales el resultado final es 0, por el contrario, el resultado es 1. Es decir:

A XOR B XOR B = A

Por tanto, si el usuario crea el segmento cifrado de la trama se usa un "KEYSTREAM" XOR" texto plano" y se obtiene una palabra cifrada.

Una vez que el Access Point recibe esta trama le aplicará un KEYSTREAM XOR CIFRADO igual, y obtendrá el texto. Dicho de otra forma:

texto XOR KEY STREAM XOR KEY STREAM = texto

El Keystream se genera a través de RC4, que tiene como entradas el Vector de Inicialización y la clave estática. A continuación se detalla la formación final de la trama WEP.

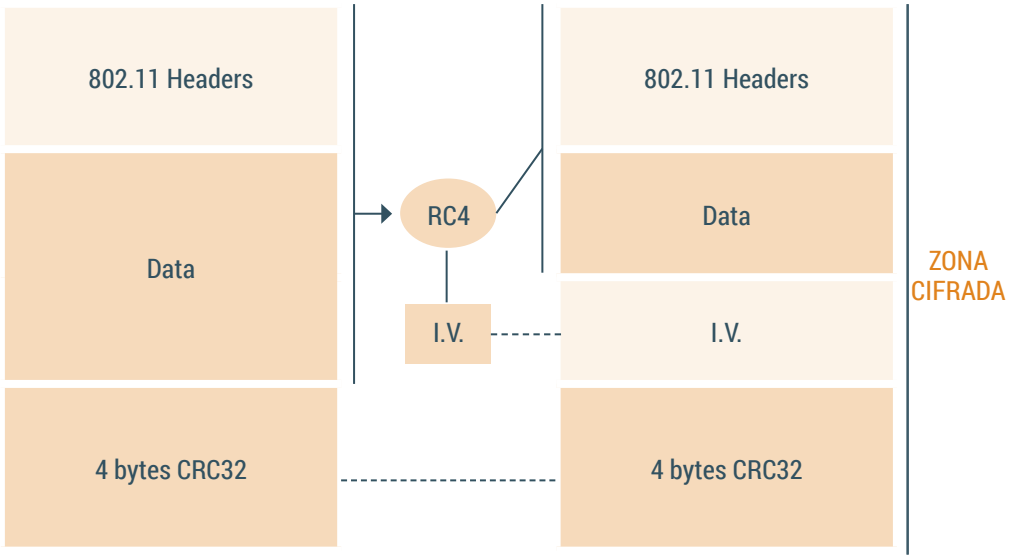


FIGURA 2.2.3 CIFRADO TRAMA WEP

Ataques en WEP

Es muy sencillo, mediante observación, obtener el patrón de la clave consiguiendo la clave estática. Debemos tener en cuenta que el Vector de Inicialización siempre manda en plano, dejando esa información vulnerable de ser interceptada por cualquier usuario. Además, el vector tiene una longitud muy pequeña (24 bits) por lo que mediante la observación y la estadística podremos obtener fácilmente la clave.

No obstante, procedemos a explicar los principales ataques en WEP.

Inyección de paquetes

La inyección de ARP (ataque 3 de aireplay-ng) consiste en la re-inyección de ARP para conseguir vectores de inicio y ARP rápidamente. Se utiliza un paquete ARP ya que se genera como respuesta a nuevos iv's y no es un paquete grande, así que podremos alcanzar la tasa de inyección más alta. El ARP se utiliza para traducir una dirección IP a una dirección física.

Para realizar este tipo de ataque usaremos la herramienta aireplay, que inyecta tráfico para elevar la captura de los iv's e incorpora el ataque de re-inyección de paquete ARP.

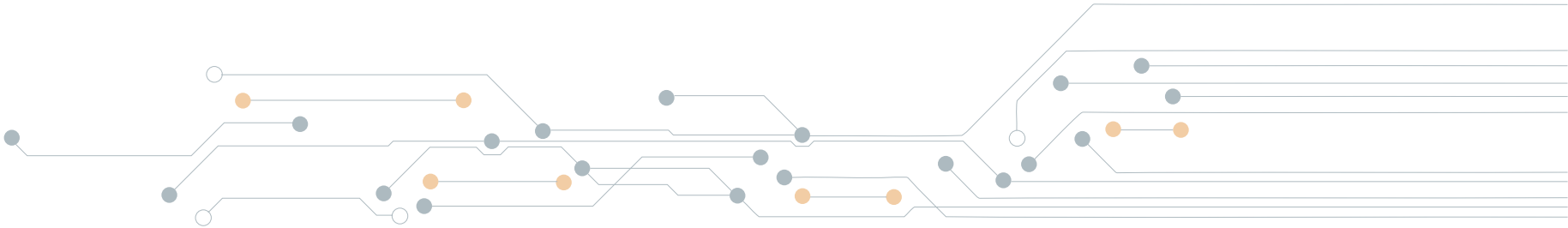
El código es: **aireplay-ng -3 -b [BSSID_Router] -h [MAC_Cliente] interfaz.**

Si no añadimos la MAC del cliente se usará la de nuestro dispositivo.

Podemos utilizar esto dentro de un contexto de ataque simple de crackeo WEP, en el que sirviéndonos de kali Linux utilizaremos dos técnicas fundamentales para generar tráfico wifi para conseguir la clave. Las dos técnicas son las siguientes:

- Falsa asociación, utilizando aireplay-ng "A1".
- Re-inyección de paquetes ARP aireplay –ng -3 "A3", que nos permite crear datos e inyectarlos.

Esto puede hacerse haciendo un sniffing de la red, capturando paquetes cifrados y ejecutando el programa. WEP es bastante fácil de romper, ya que sólo utiliza una clave para cifrar todo el tráfico. El principio básico es que la comunicación entre dos nodos en la red se basa en la dirección MAC. Cada host recibe paquetes sólo destinados a la dirección MAC de su propia interfaz. Sin embargo, si un nodo establece su propia tarjeta de red en modo "promiscuo" también recibirá paquetes que no se dirigen a su propia dirección MAC.



Para ello vamos a seguir los siguientes pasos, asumiendo que la tarjeta de red inalámbrica está instalada y que admite el modo monitor.

1. Instalación AIR Crack.

```
# apt-get install aircrack-ng
```

2. Identificación de la interfaz de red inalámbrica. El primer paso es identificar el nombre de la interfaz de la red inalámbrica. Si está instalada correctamente el comando iwconfig debería mostrar algo similar a lo siguiente:

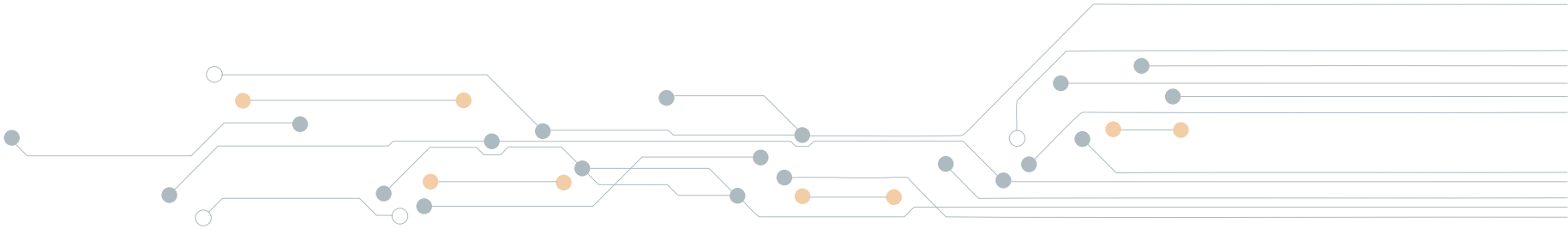
```
$ /sbin/iwconfig
wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.437 GHz  Tx-Power=20 dBm
```

3. Puesta en modo monitor.

```
# airmon-ng start wlan0
Interface       Chipset         Driver
wlan0                     rt18180 - [phy0]
      (monitor mode enabled on mon0)
```

4. Identificación del BSSID de la red. En este paso identificamos el BSSID de la red.

```
# airodump-ng wlan0
```



5. Sniffing de la red inalámbrica. En esta etapa podemos empezar a capturar paquetes entre la base y la estación. El siguiente comando comenzará a capturar paquetes. Se recomienda capturar al menos 5000 paquetes. El número de paquetes requeridos depende de la longitud de la clave WEP en uso. El número 6 equivale a nuestro canal.

```
# airodump-ng -c 6 -w data-capture wlan0
```

6. Inyección de paquete. Aireplay-ng creará tráfico para poder capturar más paquetes por un tiempo específico. Ya que estamos hackeando nuestra propia red.

```
# aireplay-ng -3 -b 00:11:95:9F:FD:F4 -h 00:13:02:30:FF:EC wlan0
```

7. Crackeo de la clave WEP. Como último paso, rompemos la clave WEP usando paquetes capturados y el comando aircrack-ng. Todos los paquetes capturados ahora se almacenarán en el archivo data-capture-01.cap.

```
# aircrack-ng -z data-capture-01.cap
```

```
Read 450 packets.

   #  BSSID              ESSID                     Encryption

   1  00:11:95:9F:FD:F4  linuxconfig.org           WEP (210 IVs)
   2  00:17:3F:65:2E:5A  belkin54g                 None (0.0.0.0)

Index number of target network ?

1

                              Aircrack-ng 1.0 rc1


                [00:00:13] Tested 485 keys (got 16690 IVs)

   KB    depth   byte(vote)
    0    9/ 13   00(20992) 06(20736) 27(20736) 3F(20736) A2(20736)
    1    0/  1   F3(28416) A8(23296) 34(21248) 57(21248) A3(21248)
    2    0/  2   8E(25856) BC(23808) 3F(23040) D2(22784) 69(21504)
    3    0/  5   6E(24320) 35(22528) 5A(22016) 95(22016) B8(22016)
    4    3/  4   98(21504) 7C(20992) 84(20992) E0(20992) F0(20992)

                          KEY FOUND! [ 3F:F9:8E:6E:98 ]
        Decrypted correctly: 100%
```

ChopChop

Este ataque es uno de los que se hicieron famosos por ser válidos contra configuraciones de redes Wi-Fi con cifrado WEP. El principal objetivo de la técnica de Korek, o más conocido ataque ChopChop, es la de descifrar el tráfico generado entre un punto de acceso y un cliente Wi-Fi que utilizan el protocolo de cifrado WEP, sin conocer la contraseña real de la red inalámbrica.

El procedimiento que marca esta técnica es el siguiente:

- En primer lugar, se captura tráfico entre el punto de acceso y el cliente. Esto puede ser llevado a cabo a través de herramientas como airodump-ng, de la suite aircrack-ng.

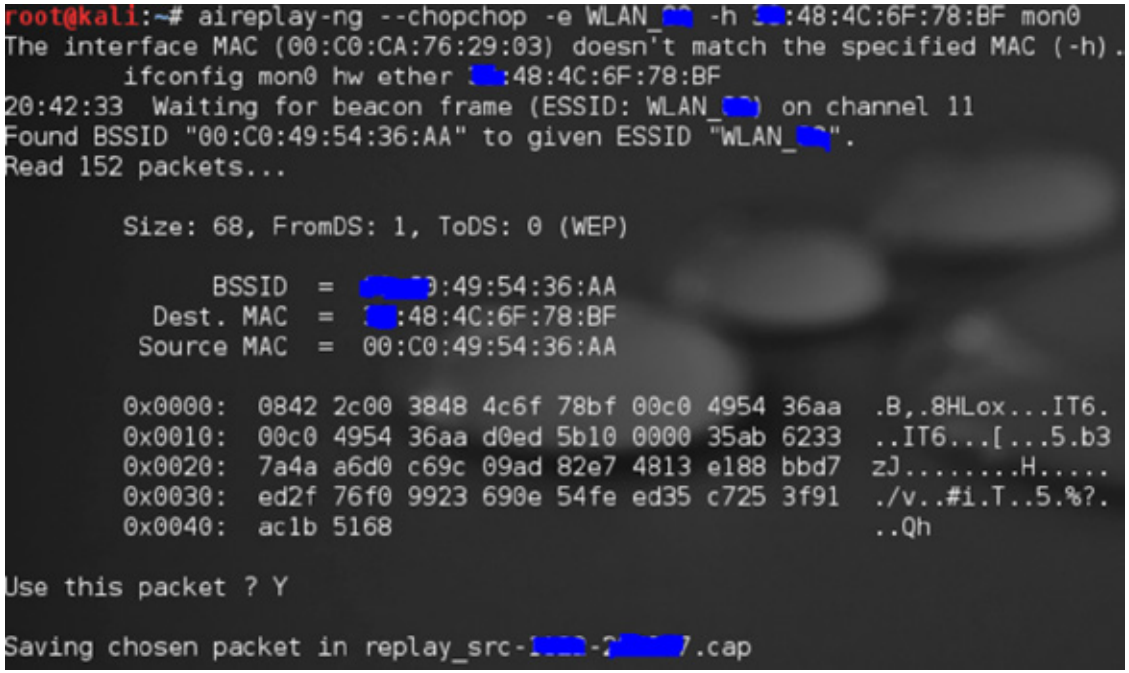
Bytes	Nuevo-ICV	¿Aceptado?
00	ICV - 1	No
01	ICV - 2	No
02	ICV - 3	No
...	...	...
CD	ICV-n	Sí

- Una vez se tiene el tráfico, se coge un paquete de datos cifrado y se elimina el último byte.
- El byte eliminado solo podrá tener valores, en hexadecimal, entre el \x00 y el \xFF. En otras palabras, se tienen 256 posibilidades. El atacante generará 256 paquetes distintos con los distintos posibles valores y se los irá enviando al punto de acceso, por lo que 1 de los 256 será válido. De esta manera ya se ha descifrado el último byte del paquete.
- Hay que tener en cuenta que por cada paquete que se envía se está comprobando el ICV conocido con el nuevo generado con los cambios en el último byte. Lo que realmente se quiere ver es si generando un nuevo paquete de datos cambiando el último byte por un valor conocido, y generando el ICV (vector de inicialización) el paquete es aceptado por el punto de acceso. En este caso, el byte es el que se encuentra cifrado. Es decir, en caso de que el paquete sea aceptado, se habrá descifrado el último byte.
- Después, se realiza el mismo proceso con el penúltimo paquete. Esto se realizará con cada uno de los bytes correspondientes con la parte cifrad.
- Se puede coger la dirección MAC del cliente que esté autenticado en el punto de acceso para poder utilizarlo y engañar al punto de acceso para que piense que el tráfico viene de un cliente legítimo.

A continuación, se muestra un pequeño ejemplo de este ataque que ayuda a entender las debilidades del protocolo de cifrado inalámbrico WEP, y su escasa utilización hoy en día. La herramienta Aireplay-ng implementa el ataque ChopChop, mediante la invocación del parámetro –chopchop.

En primer lugar, se utiliza la herramienta airodump-ng para poder visualizar las redes inalámbricas que se encuentran en el aire y con las que se tiene contacto desde el adaptador wireless. Una vez se captura el tráfico de una red Wi-Fi con protocolo de cifrado WEP, se debe utilizar la herramienta aireplay-ng de la siguiente forma aireplay-ng –chopchop -e [ESSID de la red Wi-Fi] -h [dirección MAC de la víctima o estación] <adaptador de red en modo monitor>.

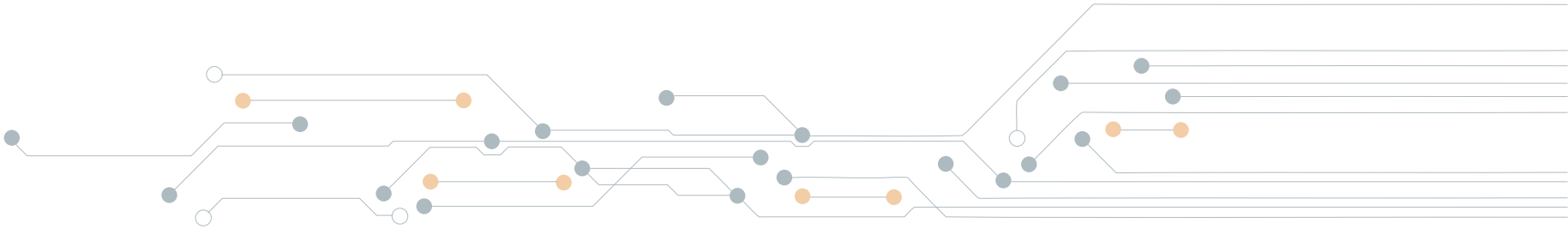
El paquete tendrá que tener como dirección MAC origen la de la víctima, esta es la que justo se está suplantando.



Se solicita al usuario que si se quiere utilizar este paquete, el cual fue capturado por airodump-ng y se puede visualizar con aireplay-ng para realizar el ataque. El paquete está almacenado en un fichero pcap. Si se abre el fichero pcap, se puede observar que está cifrado y que no se puede ver el contenido.

```
Offset   40 (79% done) | xor = 84 | pt = 06 |  325 frames written in  5458ms
Offset   39 (82% done) | xor = AD | pt = 00 |  137 frames written in  2295ms
Offset   38 (85% done) | xor = 01 | pt = 08 |  485 frames written in  8112ms
Offset   37 (88% done) | xor = 9D | pt = 01 |  231 frames written in  3865ms
Offset   36 (91% done) | xor = C6 | pt = 00 |   18 frames written in   304ms
Offset   35 (94% done) | xor = D6 | pt = 06 |  229 frames written in  3834ms
Offset   34 (97% done) | xor = AE | pt = 08 |  147 frames written in  2465ms

Saving plaintext in [redacted].cap
Saving keystream in [redacted].xor

Completed in 124s (0.24 bytes/s)
```

Cuando aireplay-ng termine se indicará que almacena el paquete descifrado en otra captura. Al final se obtiene el tráfico descifrado a través de dicho método. No es un método rápido, pero es un método que permite entender grandes debilidades del protocolo WEP.



2.3 | WPA/WPA2

WPA (Wifi Protected Access) nace como una mejora temporal de la Wi-Fi Alliance para paliar la debilidad de la seguridad de WEP, antes estudiada, hasta que la IEEE finalmente desarrollara una solución definitiva que mejorara los problemas del método de cifrado anterior. Cuando finalmente lo hizo, Wi-Fi Alliance otorgó la calificación WPA2 a los dispositivos compatibles con las características del nuevo estándar creado.

Los dos diseños trabajan bajo el protocolo 802.1x en lo relacionado a la autenticación en infraestructuras grandes y con clave compartida (PSK, Pre-Shared key) para entornos más pequeños y familiares.

Los conceptos de WPA y WPA2 son similares aunque existen diferencias en el método de cifrado que utilizan.

Por una parte, WPA se sirve del algoritmo TKIP (Temporary Key Integrity Protocol) para el cifrado de sus conexiones, que igual que WEP se basa en RC4. Por otra parte, WPA2 usa CCMP (Counter-mode/CBC-MAC Protocol), que se basa en AES (Advanced Encryption System).

Otro punto en el que ambos sistemas difieren es la integridad del mensaje, y es que WPA utiliza un método más primitivo para generar el MIC (Message Integrity Code). WPA2 cuenta con una versión más desarrollada de este proceso.

Arquitectura WPA/WPA2 PSK

Ambas tecnologías son vulnerables y podemos atacar a sus redes para poder, o bien utilizar la red, o bien monitorizar y analizar el tráfico que circula por la misma.

El primer paso y más importante, clave para poder entender la vulnerabilidad de estos sistemas es la asociación de un usuario a la red inalámbrica. El procedimiento es similar, sin dependencia del método elegido (WEP, WPA, WPA2), aunque sí que tiene dependencia de si el Access Point emite BEACON FRAMES, dando a conocer su red publicando su ESSID. Si el ACCESS POINT emite BEACON FRAMES el proceso de conexión a la red se realiza en dos fases: la primera, en la que se realiza la autenticación (abierta o clave compartida) y la segunda, en la que el usuario se asociará a la red.

Suponiendo que el Access Point no emite BEACON FRAMES hay una prueba en el comienzo de la conexión en la que el usuario manda el ESSID de la red inalámbrica a la que desea asociarse y permaneciendo a la espera de que el Access Point responda y poder pasar así a las siguientes fases, que corresponden a la fase de autenticación y fase de asociación.

En la imagen que se muestra a continuación podemos diferenciar las tres fases explicadas:

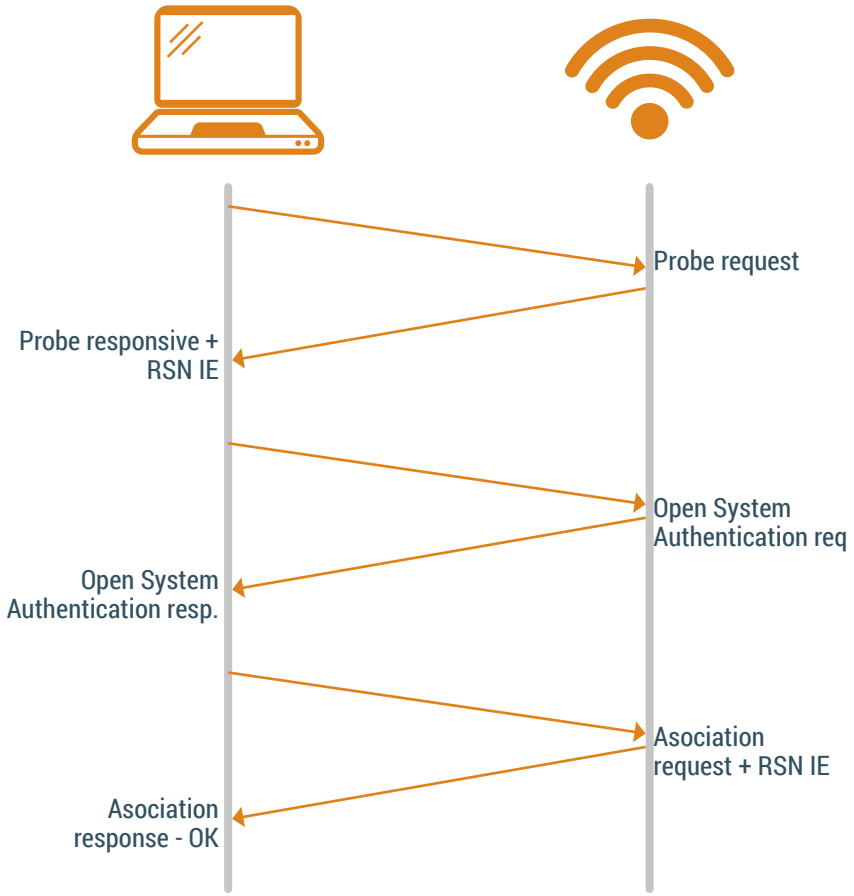


FIGURA 2.3.1 NEGOCIACIÓN SIN ESSID 1

Sólo existe una distinción ante la red abierta o WEP, y es que el Access Point y el usuario pactan previamente la política de seguridad del proceso, que equivale a la primera fase del procedimiento en autenticación de WPA/WPA2.

Como puede observarse en el esquema, el usuario se conecta al principio a la red sin comenzar el procedimiento de autenticación WPA/WPA2 (sea o no mediante PSK) así que el tráfico se está cifrando aún. Un atacante puede aprovechar esta vulnerabilidad, enviando una trama de des-asociación a otro usuario de la red, provocando que se desconecte e y comience otra vez el proceso de autenticación WPA/WPA2. Este tipo de ataque es conocido como ataque 0 o des-asociación.

El nuevo desarrollo de autenticación se haría solamente si la conexión fuera WPA/WPA2 empresarial (configuración en 802.1x y Extended Authetication Protocol) contra un RADIUS (Remote Authentication Dial-In Service) como medio para autenticar la nueva conexión. En WPA/WPA2 con PSK saltamos de forma directa al intercambio de claves.

En esta fase el usuario y el Access Point usan PSK para crear una clave denominada PMK (Pairwise Master Key). Dicha PMK consiste en una derivada si el protocolo es WPA/WPA2 empresarial, en cambio, en contextos WPA/WPA2 PAK, la PMK será exactamente la misma.

Con la PMK se crea una clave destinada a los procesos por separado de autenticación de los diferentes usuarios. Esa clave recibe el nombre de PTK y consiste en dos números que son generados de forma aleatoria: uno por el usuario y otro por el Access Point. Los dos los intercambiar con el fin de conseguir una clave PTK igual. A todo ese procedimiento se le denomina 4-way-Handshake.

Cuando finalmente el usuario ha llevado a cabo la autenticación, el protocolo TKIP usa 6 claves de cifrado en cada sesión: 4 para conexiones unicast y los dos restantes para las broadcast. Por último, debemos destacar que las claves son únicas por cada relación cliente-sesión y se actualizan en el tiempo. Además, se crean partiendo de derivadas de las direcciones MAC, ESSID y TPK.

Ataques en WPA/WPA2

El atacante que desee hackear una red WPA/WPA2 lo hará de forma que intentará interceptar dicho intercambio de cifras generadas de forma aleatoria con el objetivo de conocer estos números y posteriormente, contando también con el SSID y las MAC del usuario y el Access Point, intentará obtener la secuencia que usó. Cuando el atacante consiga la clave compartida podrá finalmente conectarse a la red.

Ataque de fuerza bruta al handshake

El handshake en red inalámbrica con cifrado WPA/WPA2 es el proceso en el que la autenticación en la red se lleva a cabo. La captura de este intercambio de paquetes puede llevar a la consecución de la clave. Este hecho no es sencillo, ya que lo que se puede obtener está cifrado y habrá que utilizar el cracking como técnica para lograr la clave de la red WiFi.

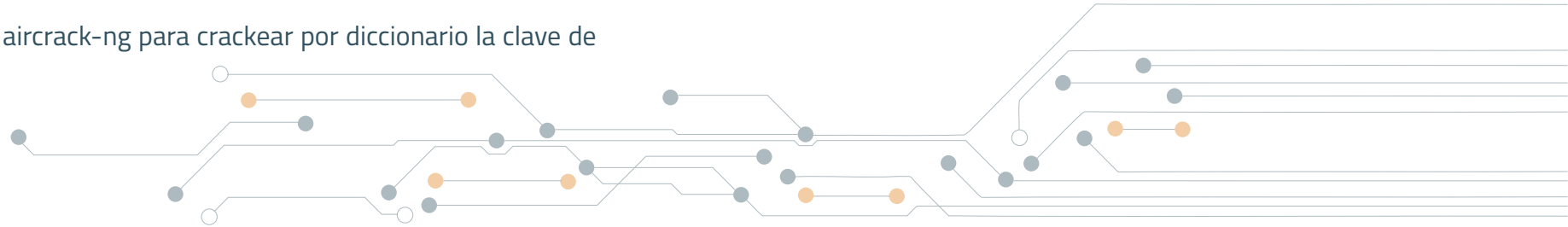
En estas líneas, se presenta un paso a paso del proceso explicado en detalle y viendo de forma práctica cómo funcionan estos casos. A continuación, se enumeran los pasos que se detallarán más adelante:

- Tarjeta WiFi en modo monitor y a la "escucha" del aire.
- Captura de tráfico aéreo con el objetivo de capturar el handshake.
- Deautenticación o ataque 0 para obligar al punto de acceso a desautenticar a un cliente asociado en la red WPA/WPA2.
- Ejecución de aircrack-ng para crackear por diccionario la clave de la red WiFi.

En primer lugar, se debe configurar la tarjeta WiFi en el denominado o conocido como modo monitor. Con este modo configurado el adaptador puede "escuchar" lo que circula en el aire, además, de capturar cualquier paquete, tal y como se ha visto en ejemplos anteriores. Se debe ejecutar la siguiente instrucción airmon-ng start <interfaz de red wireless>.

En segundo lugar, se debe ejecutar la herramienta airodump-ng con el objetivo de capturar lo que circula en el aire. Se puede "afinar" hacia una red o canal concreto, ya dependiendo de los parámetros con los que se ejecute airodump-ng. Para este ejemplo, se supone que se ejecuta la siguiente instrucción airodump-ng -c 6 –bssid ca:fe:ca:fe:ca:fe -w captura1.pcap mon0. A continuación, se detalla que significa cada parámetro:

- El parámetro -c indica el canal por el que la herramienta escuchará.
- El parámetro –bssid indica la dirección MAC del punto de acceso o router. Hace que la aplicación no "escuche" otras redes, y solo se centre en dicho punto de acceso.
- El parámetro -w indica el nombre del fichero dónde se almacenará todo el tráfico capturado, incluyendo, en esta ocasión el handshake.



Un ejemplo de captura real sería:

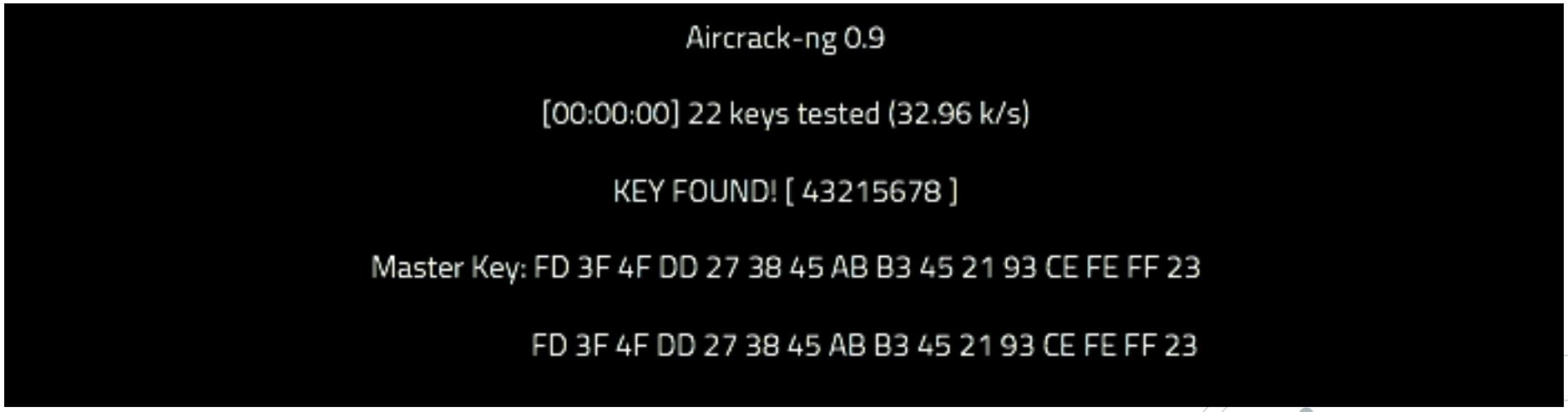
```
CH  9 ][ Elapsed: 4 s ][ 2007-03-24 16:58

 BSSID              PWR RXQ  Beacons   #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

 CA:FE:CA:FE:CA:FE  -34 100    5         223   22   6  54  WPA2 CCMP   PSK  TDE

 BSSID       STATION       PWR  Lost  Packets  Probes

 CA:FE:CA:FE:CA:FE  FA:BA:DA:FA:BA:DA  -35    0    146
```

En tercer lugar, hay que utilizar la herramienta aireplay-ng para ejecutar el ataque 0 o de desautenticación contra el cliente conectado al punto de acceso de la red. En este caso, se lanzará un paquete hacia el punto de acceso con dirección MAC CA:FE:CA:FE:CA:FE, indicándole que el cliente con dirección MAC FA:BA:DA:FA:BA:DA se quiere salir de la red. Para ello, se ejecuta la siguiente instrucción aireplay-ng -0 1 -a CA:FE:CA:FE:CA:FE -c FA:BA:DA:FA:BA:DA mon0. A continuación, se especifica lo que significa cada parámetro:

- El parámetro -0 Esto es la implementación del ataque de desautenticación. Después, se indica el número 1 que son el número de deautenticaciones enviadas al punto de acceso.
- El parámetro -a indica la dirección MAC del punto de acceso.
- El parámetro -c indica la dirección MAC del cliente que se suplantará y se desautenticará.
- El último argumento es la interfaz de red por la que se envía dicho paquete.

Una vez que se lleva a cabo el ataque de tipo 0 o de desautenticación, el cliente legítimo volverá a conectar a la red WiFi, pero en esta ocasión el atacante estará con airodump-ng "escuchando" todo, por lo que se capturará el handshake. Este dato ha quedado almacenado en el fichero PCAP, generado con la herramienta airodump-ng.

Por último, hay que crackear el handshake con la herramienta aircrack-ng. La sintaxis sería: aircrack-ng -w <fichero con claves posibles o diccionario> -b <dirección MAC del punto de acceso> <fichero PCAP>.



Telefónica EDUCACIÓN DIGITAL