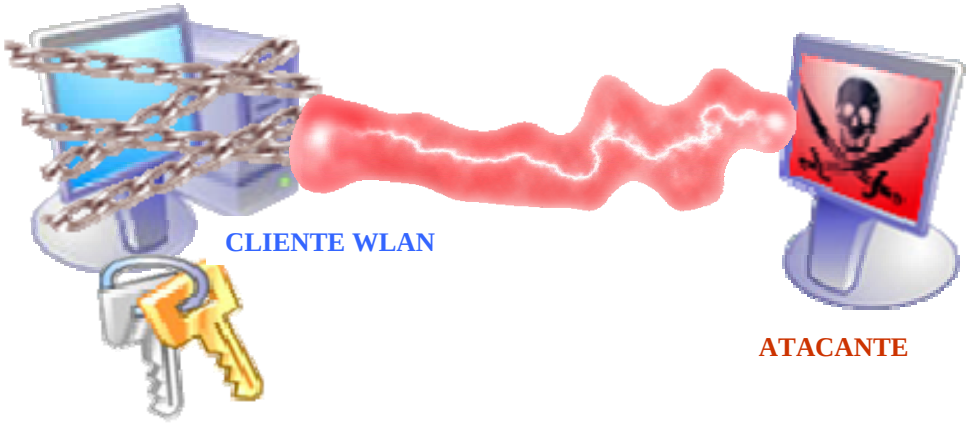
CAPITULO II



DEFENSAS Y ATAQUES A LA SEGURIDAD EN REDES WLAN

2.1.- Defensa a las redes WLAN
2.2.- Ataques de redes WLAN
2.3.- Guía para la seguridad en redes WLAN

Los sistemas informáticos están dispersos en toda la organización. Se dispone de numerosas máquinas de distinto tipo. Se interconectan en red con las sucursales y con otras empresas. Tenemos redes de área amplia, Internet, diversidad de plataformas, múltiples sistemas operativos, usuarios internos, externos, invitados, entre otros, computadoras personales, redes heterogéneas, computación móvil, etc, que pueden ser atacados ya sea sus redes convencionales, redes WLAN o sus sistemas informático por usuarios internos o extensos en cualesquier momento.

Una red WLAN opera de la misma forma que una LAN cableada, salvo que los datos se transportan a través de un medio inalámbrico, normalmente ondas de radio, en lugar de cables. Por lo tanto, una red WLAN presenta muchas de las mismas vulnerabilidades y amenazas que una LAN cableada. En este capitulo explicaremos algunas de las defensas y ataques mas comunes a las que se enfrentan las redes WLAN. [LIB001]

2.1.- Defensa a las redes WLAN

La seguridad WLAN abarca dos elementos: el acceso a la red y la protección de los datos (autenticación y encriptación, respectivamente). Las violaciones a la seguridad de la red inalámbrica, generalmente, vienen de los puntos de acceso no autorizados, aquéllos instalados sin el conocimiento de los administradores de la red, o que operan con las funcionalidades de protección deshabilitadas (que es la configuración por omisión en los dispositivos inalámbricos).

Estos “hoyos” en la seguridad, pueden ser aprovechados por personal no autorizado (hackers o espías), que en caso de que logren asociarse con el punto de acceso, ponen en riesgo no únicamente la infraestructura inalámbrica, sino también la red alámbrica a la cual se conecta.

Para estos problemas las posibles soluciones en seguridades, con respecto a las redes inalámbricas LAN son:

2.1.1.- Mecanismo básico WEP

El mecanismo WEP es el sistema básico de autenticación y cifrado de datos, la autenticación puede realizarse mediante un sistema abierto o mediante clave compartida. Una estación de red que reciba una solicitud puede conceder la autorización a cualquier estación, o sólo a aquellas que estén incluidas en una lista predefinida. En un sistema de clave compartida, sólo aquellas estaciones que posean una llave cifrada serán autenticadas.

2.1.1.1.- Cifrado:

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida, para el cifrado de los datos WEP utiliza el algoritmo RC4.

Para proteger el texto cifrado frente a modificaciones no autorizadas mientras está en tránsito, WEP aplica un algoritmo de comprobación de integridad (CRC-32) al texto en claro, lo que genera un *valor de comprobación de integridad* ICV[1]. Dicho valor de comprobación de integridad se concatena con el texto en claro.

El valor de comprobación de integridad es, de hecho, una especie de huella digital del texto en claro. El valor ICV se añade al texto cifrado y se envía al receptor junto con el vector de inicialización. El receptor combina el texto cifrado con el flujo de clave para recuperar el texto en claro. Al aplicar el algoritmo de integridad al texto en claro y comparar la salida con el vector ICV recibido, se puede verificar que el proceso de descifrado ha sido correcto ó que los datos han sido corrompidos. Si los dos valores de ICV son idénticos, el mensaje será autenticado; en otras palabras, las huellas digitales coinciden. [LIB01]

[1] **ICV** Integrity Check Value, A la trama en claro se le computa con un código de integridad ICVmediante el algoritmo CRC-32

2.1.1.2.- Autenticación:

WEP proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN, y una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red. De los dos niveles, la autenticación mediante clave compartida es el modo seguro.

En él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN. Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el *desafío (challenge)*. La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando la misma clave compartida y compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red. Si la estación no dispone de una clave, o si envía una respuesta incorrecta, el punto de acceso la rechaza, evitando que la estación acceda a la red.

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

Esto crea una ventana para que un intruso penetre en el sistema, después de lo cual podrá enviar, recibir, alterar o falsificar mensajes. Es bueno asegurarse de que WEP está habilitado siempre que se requiera un mecanismo de autenticación seguro. Incluso, aunque esté habilitada la autenticación mediante clave compartida, todas las estaciones inalámbricas de un sistema WLAN pueden tener la misma clave compartida, dependiendo de cómo se haya instalado el sistema. [LIB01]

2.1.2.- VPN para redes LAN inalámbricas

Una posible solución a los problemas de seguridad inherentes a una red inalámbrica es habilitar una VPN. En este caso estaríamos hablando de túneles IPSec que se originan en los equipos portátiles de los usuarios y que terminan en algún dispositivo específico de la red cableada. Esta solución resuelve los problemas de cifrado e integridad de los datos (a través del protocolo IPSec[2]) pero no resuelve los problemas de validación de usuario. Además esta solución implica mayor coste (debido a la necesidad del equipo terminador de túneles) y mayor complejidad en la gestión.

El túnel VPN acaba siempre en el servidor VPN, es decir, una puerta de enlace VPN. El sistema VPN puede estar formado de distintas maneras:

- Un AP (Puntos de Acceso), que ya tienen integrado un servidor VPN. Esta variante se utiliza a menudo en pequeñas y medianas empresas, en las que la autentificación se realiza, bien, consultando en una base de datos locales del Access Point o con un servidor RADIUS externo. Un túnel VPN seguro acaba en un Access Point.
- Otra posibilidad es el uso de un servidor VPN central. El servidor VPN puede ser un dispositivo de Hardware o un ordenador en el que haya instalada una aplicación de software VPN. En la red LAN el túnel VPN va desde los clientes pasando por el Access Point hasta el servidor VPN. Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WPA en este esquema.

En la Figura 2.1 vemos la estructura de la VPN para acceso inalámbrico seguro.

[2] **IPSec** Seguridad de Protocolo de Internet, es un conjunto de servicios de protección y protocolos de seguridad basados en criptografía para redes VPN.

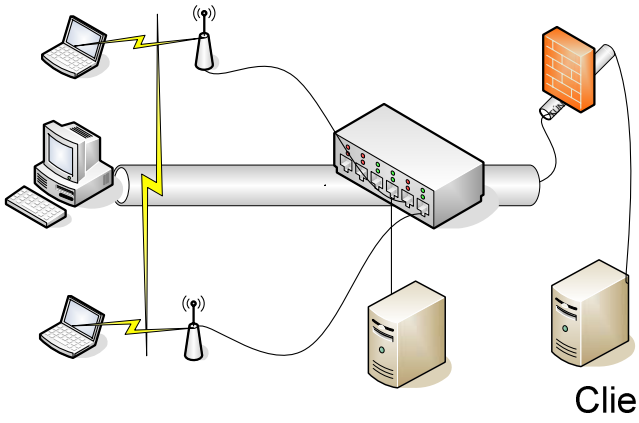


Figura 2.1: Estructura de la VPN con la red WLAN

2.1.3.- WPA (*Wi-Fi Protected Access*, acceso protegido Wi-Fi)

WPA soluciona la debilidad del vector de inicialización de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, el algoritmo utilizado por WPA es RC4, que trabaja con 64 y 128 bits de encriptación. La secuencia del vector de inicialización, conocida por ambos extremos de la comunicación, puede utilizar para evitar ataques de repetición de tramas (*replay*).

Para la integridad de los mensajes Valor del Chequeo de integración (ICV), se ha eliminado el algoritmo de integridad (CRC-32) que se demostró vulnerable en WEP y se ha incluido un nuevo código denominado MIC[3]. Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP [www08].

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1x / EAP / RADIUS. Su inconveniente es que

[3] **MIC** *Message Integrity Code* o Michael. Código que verifica la integridad de los datos en las tramas.

requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

2.1.3.1.- Modos de funcionamiento de WPA

Las estaciones tratarán de conectarse a un puerto del punto de acceso. El punto de acceso mantiene el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP[4] y un servidor AAA[5] (*Authentication, Authorization Accounting*) como puede ser RADIUS (Servicio de usuario de acceso telefónico de autenticación remota). Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

WPA puede funcionar en dos modos: [www10].

2.1.3.1.1.- WPA: 802.1x y EAP

Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad. Para esto utiliza el estándar 802.11x que proporcionar un control de acceso en redes basadas en puertos, en la que daremos una breve descripción.

WPA adopta 802.11x para direcciones de aplicación de autenticación de usuario en WEP 802.1x. Inicialmente se diseño para las redes alámbricas pero es aplicable a redes inalámbricas. El estándar proporciona control de acceso basado en puerto y la autenticación mutua entre los clientes y los puntos de acceso vía servidor de autenticación.

El estándar 802.1x abarca tres elementos

[4] **EAP** Protocolo de Autenticación Extensible, Sirve para llevar a cabo las tareas de autentificación, autorización y contabilidad, lo utiliza el mecanismo de seguridad WPA
[5] **AAA** Autenticación, Autorización, Contabilidad

- Un solicitante: un usuario o un cliente desea ser autenticado. Puede ser el software del cliente el PC, portátil, PDA u otro dispositivo inalámbrico
- Un servidor de autenticación: un sistema de la autenticación que maneja autenticaciones reales. (Servidor RADIUS)
- Un autenticador: un dispositivo actúa como intermediario entre el servidor de autenticación y el solicitante. Generalmente, el dispositivo es el punto de acceso.

2.1.3.1.2.- WPA-PSK (*WPA Pre-Shared Key*)

Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

El funcionamiento únicamente requiere una password para acceder al punto de acceso. Este modo de trabajo está preparado para ser utilizado con claves de inicio y encriptación de los datos. WPA utiliza TKIP (*Protocolo de integridad de claves*). y MIC (*Codigo de integración de Mensajes*) para distribuir claves dinámicas temporales a los clientes y comprobar la integridad de las tramas recibidas (evita que se modifique tramas capturadas y se reenvíen).

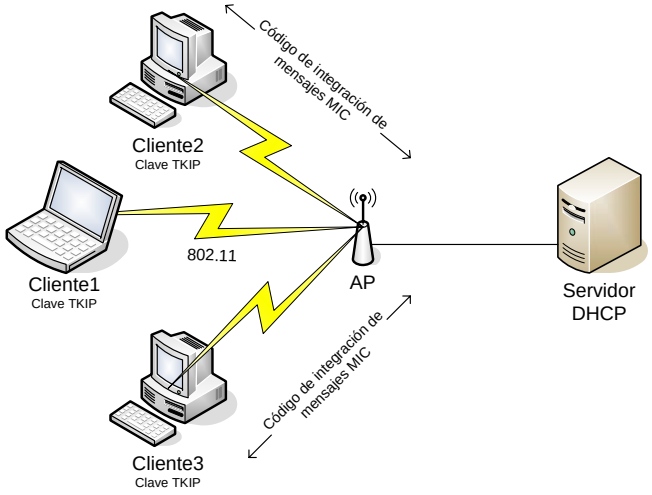


Figura 2.2: Configuración de la red WLAN utilizando WPA-PSK

2.1.4.- Protección de datos con TKIP

Para una mejor codificación de datos el estándar WPA utiliza TKIP (Protocolo de integridad de clave temporal), con el que se reparan todos los puntos débiles de WEP en el área de la codificación de datos. El TKIP, posibilita esta mejora insertando un mecanismo per-packetkey. Es decir, que para calcular la clave se intercala una función HASH, que usa una clave distinta para cada paquete.
Además en el TKIP hay incorporado un controlador de integridad de los datos mejorado, conocido como MIC (Código de integridad del mensaje) o como Michael. Este se utiliza para evitar la manipulación de los datos. El transmisor calcula el MIC a partir del MAC Header (direcciones del remitente y del destinatario), de la prioridad, y de los datos. El MIC se envía y el destinatario lo verifica tras descodificarlo. [www09].

2.1.5.- IEEE 802.11i

Sin embargo los aparatos LAN inalámbricos usados hasta el momento deberían seguir siendo aprovechables (naturalmente con pérdidas en seguridad). Debido a las numerosas funciones nuevas, para los futuros estándares se necesitarán nuevos equipos. Los aspectos centrales en los futuros estándares de seguridad 802.11i son 802.1x, y EAP y AES (Estándar de encriptación avanzado).

El estándar IEEE 802.11i debería cumplir los siguientes puntos:

- Inserción del TKIP compatible con el sistema actual, con las características antes mencionadas (MIC, ampliación del IV, uso de los números de secuencia, etc.)
- Sustitución del algoritmo RC4 por el AES para los nuevos equipos. El algoritmo RC4 usado en WEP se sustituye completamente en el estándar 802.11i por AES. Sin embargo, AES necesita nuevos equipos, ya que utiliza un mecanismo de encriptación diferente. Por razones de

compatibilidad el estándar se basará también en RC4, pero esto sacrificará en cierto modo la seguridad.

- Autenticación a través de un puerto hecha con el estándar 802.1x, basada en EAP. 802.1x tiene un papel decisivo en el estándar 802.11i y posibilita la autenticación específica del usuario. Con el EAP también se podrán usar futuros mecanismos biométricos de autenticación.
- Generación de claves con un administrador de claves dinámico. El administrador de claves se efectuará con la inserción del estándar 802.1x y un servidor de autenticación.
- La autenticación recíproca del cliente y el Access Point para evitar ataques intencionados con puntos de acceso falsos.
- Grupos de claves jerárquicos.
- Administración dinámica de las opciones de autenticación y encriptación.

2.1.6 Comparativa entre WEP, WPA y 802.11i

En las comparaciones de la Tabla 2.1, el punto mas importante es el algoritmo de encriptación, WEP y WPA trabajan con el algoritmo RC4 con 40 y 120 bits de encriptación respectivamente y 802. 11i con el algoritmo Rijndael o AES que es a 128 bits de encriptación. Tanto WPA como 802.11i funcionan con el estándar 802.1x. [www11].

	WEP	**WPA**	**802.11i**
Algoritmo de cifrado	RC4	RC4 (TKIP)	Rijndael (AES-CCMP)
Clave de encriptación	40bit	128bit (TKIP)	128bit (CCMP)
Vector inicialización	24bit	48bit (TKIP)	48bit (CCMP)
Autenticación de clave	Ninguna	64bit (TKIP)	128bit (CCMP)
Chequeo de integridad	CRC-32	Michael (TKIP)	CCM
Distribución de clave	Manual	802.1x (EAP)	802.1x (EAP)
Clave Unica a:	Red	Paquete, sesión, user	Paquete, sesión, user
Clave Jerarquica	No	Derivado de 802.1x	Derivado de 802.1x
Negacion de cifrado	No	Si	Si
Ad-hoc (P2P) seguridad	No	No	Si (IBSS)
Pre-atenticacion (wired LAN)	No	No	Usando 802.1x (EAPOL)

Tabla 2.1: comparación entre WEP, WPA y 802.1i [www23]

2.2.- Ataques a las redes WLAN

En lo que a seguridad se refiere, la primera diferencia entre una red cableada y una red inalámbrica es la definición del "perímetro de la red", como veremos en la Figura 2.3.

Para que un usuario (o posible hacker) pueda enviar datos a una red cableada es necesario que dicho usuario conecte su computador físicamente (cables) que tenga conectividad con la red para poder transmitir datos que están situadas dentro del edificio en el que se asienta la empresa o institución,

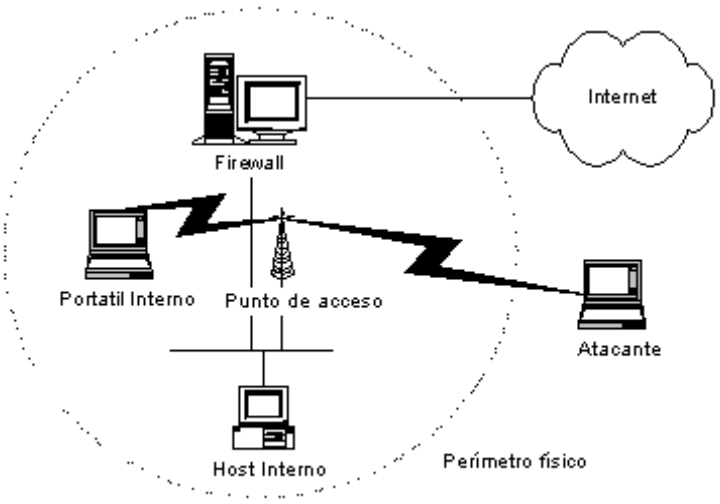


Figura 2.3: Ataque a la red WLAN [www07]

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del administrador de la red WLAN, especificando los servicios y mecanismos de seguridad necesarios.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal a un destino, un ataque no es más que la realización de una amenaza. Las cuatro categorías generales de amenazas o ataques son las siguientes como veremos en la Figura 2.4:

- **Interrupción:** Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

- **Intercepción:** una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos interceptar la comunicación que circula por una red WLAN realizando copias ilícitas de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para revelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

- **Modificación:** una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

- **Fabricación:** una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes adulterados en una red o añadir registros a un archivo.

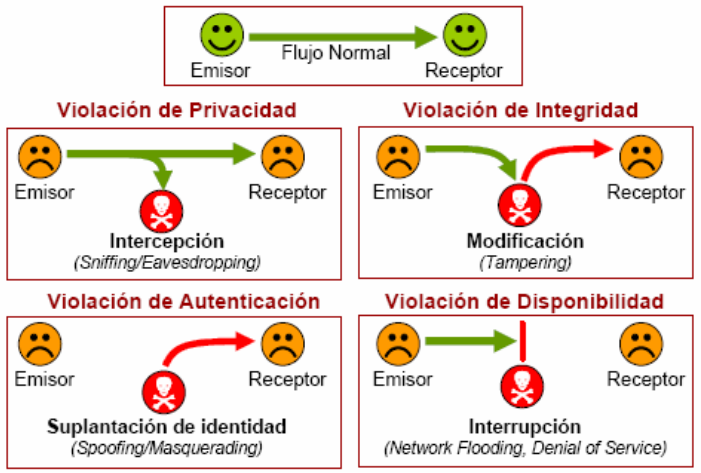


Figura 2.4: Categorías de amenazas o ataques [www24]

Para esto veremos algunos de los ataques tanto activos como pasivos de las redes WLAN como son:

2.2.1.- Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

2.2.1.1.- Escuchas ilegales

La principal amenaza es el potencial de que un tercero no autorizado escuche ilegalmente las señales de radio intercambiadas entre una estación de radio (cliente WLAN) y un Access Point.

Alguien que este realizando escuchando ilegales en una red WLAN puede estar situado a cierta distancia de la red y puede incluso estar fuera de los confines físicos del entorno dentro de la cual la red opera. Esto se debe a que las señales de radio omitidas por un WLAN pueden propagarse más allá del área en la cual han sido originadas, y pueden penetrar las paredes de los edificios y otros obstáculos físicos, dependiendo de la tecnología de transmisión utilizada y de la señal de transmisión.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán mas adelante. [LIB01]

2.2.1.2.- Interferencias aleatorias e intencionadas

Está amenaza a la seguridad de una red WLAN son las interferencias de radio, que pueden degradar seriamente el ancho de banda (la tasa de transferencia de datos). En muchos casos las interferencias son accidentales; dado que las redes WLAN utilizan zonas del espectro que no requieren licencia, otros dispositivos electromagnéticos que estuvieran operando en el espectro de infrarrojos o en la banda de radio frecuencia de 2,4 GHz podría disfrazarse con el tráfico de la red WLAN.

Las fuentes potenciales de interferencia incluyen los transmisores de alta potencia de radioaficionados, militares. Los hornos de microondas también son una posible fuente, otra fuente de preocupación es la operación de dos o más redes WLAN en la misma área de cobertura.

La interferencia también puede ser intencionada, si un atacante dispone de un transmisor potente, puede generar una señal de radio suficientemente fuerte como para cancelar las señales más débiles, interrumpiendo las comunicaciones. Estas interferencias intencionadas constituyen un ataque por denegación de servicio DoS tipos de dispositivos de interferencia que pueden usarse contra el tráfico WLAN. [LIB01]

2.2.1.3.- Romper Lista de Control de Acceso (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 ananlizar los protocolos (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*.

2.2.1.4.- Ataque de Denegación de Servicio (DoS)

Para realizar este ataque basta con monitorear durante un momento la red y ver cual es la dirección MAC del Punto de Acceso. Una vez que conocemos su MAC, actuamos como si fuéramos nosotros mismos al Access Point. 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[6].
- dassoc: envía tramas de desasociación, herramienta desarrollada por @stake[7] (antes L0pht).

[6] **Air-jack** Está herramienta de esniffer se encuentra en: http//www.802.11ninja.net
[7] **@stake** Está segunda herramienta para esniffear se encuentra en: http://www.atstake.com

2.2.1.5.- Port Scanning: (escaneo de puertos)

Como todos los protocolos TCP (Protocolo de control de transmisión) y UDP (Protocolo de datagramas de usuario) que ofrece el computador, es muy útil para espiar el número de puerto usado. Así se puede a través de un número de puerto evitar la función del Firewall para atacar más tarde de forma activa.

El Port Scanning (Escaneado de puertos) funciona de tal manera que el atacante envía datos con distintos números de puerto al ordenador "escaneado". Como con cada TCP se responde a cada petición de acceso, si es necesario se responderá con un mensaje de error y el atacante puede espiar los puertos.

2.2.1.6.- Sniffing:

Aquí el atacante necesita una entrada a la red. Por medio de un analizador de protocolos (ej. Ethherreal, Sniffer…) se graban y analizan todos los datos. Estos ataques son muy difíciles de llevar a cabo en redes convencionales, ya que se necesita o bien un acceso directo o una red interna (Ataque de colaborador), o grabar y analizar todos los datos de un segmento a través de conexión a Internet.

En las redes LAN inalámbricas este acceso es más sencillo, ya que las ondas electromagnéticas también pueden recibirse desde el exterior del edificio. Si los datos no están codificados el "fisgón" puede escuchar y grabarlos fácilmente los datos.

2.2.2.- Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en algunas categorías:

2.2.2.1.- Acceso no autorizado

Un intruso se introduce a una red WLAN disfrazado como un usuario autorizado, el intruso puede violar la confidencialidad e integridad del tráfico de red, enviando, recibiendo o falsificando mensajes. Esto constituye un ejemplo de ataque activo, y puede llevase a cabo utilizando un adaptador inalámbrico que sea compatible con la red objetivo, o utilizando un dispositivo comprometido (por ejemplo, robado) que este conectado a la red.

Instalando un Access Point falso con una señal potente, el atacante puede ser capaz de hacer que una estación se conecte a su propia red, para capturar claves secretas y contraseñas de inicio de sesión, alternativamente, el atacante puede rechazar los intentos de inicio de sesión, pero grabar los mensajes transmitidos durante el proceso inicio de sesión, para los mismos propósitos. [LIB01]

2.2.2.2.- Reactuación

Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

2.2.2.3.- Degradación fraudulenta del servicio

Impide o inhabilita el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes falsificados. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

2.2.2.4.- Spoofing (engaño)

IP Spoofing (engaño de IP): Muchos privilegios en la red se gestionan por medio de direcciones IP inequívocas. El atacante puede acceder a los datos si ha encontrado las direcciones. DNS Spoofing (engaño de DNS): El *Domain Name System,* las direcciones IP correspondientes (198.15.13.12). Cuando el usuario introduce una dirección de este tipo en el navegador origina en un segundo plano una petición en el servidor DNS.

Este servidor DNS, a su vez, memoriza las direcciones por servidores superiores, es decir, por peticiones anteriores. Ya que el servidor DNS no comprobó la veracidad de los datos, también graba la información falsa que le proporciona un atacante. El usuario es enviado a un servidor falso, y no se da cuenta del ataque, ya que casi nunca conoce la dirección IP correspondiente. MAC Spoofing (de engaño de MAC): Al igual que con IP Spoofing, aquí se utiliza una dirección MAC conocida de un usuario para poder fingir una identidad falsa.

2.2.2.5.- Ataque Man in the middle (ataque de intercepción)

El ataque de *Man in the middle*, también conocido como *Monkey in the middle* consiste en convencer al cliente (la victima) de que el host que hay en el medio (el atacante) es el Access Point, y hacer lo contrario con el Access Point , es decir, hacerle creer al Access Point que el atacante es el cliente. Ejemplo. [www07]

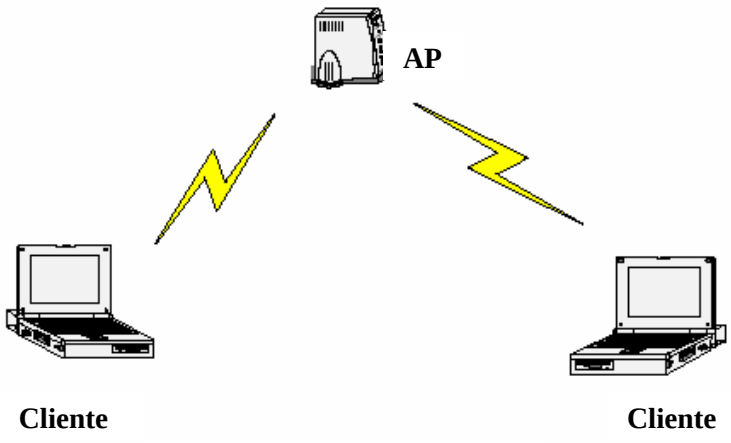


Figura 2.5: Antes del ataque

Para realizar este ataque, primero debemos esnifar para obtener:

- El SSID (Nombre de la red WLAN)
- La dirección MAC del Access Point
- La dirección MAC de la victima

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

El atacante hace creer a la victima que él es el Access Point real, utilizando la misma MAC y el mismo SSID que el Access Point al que la victima 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 Access Point real, utilizando la dirección MAC de la victima. De esta manera hemos conseguido insertar al atacante entre la victima y el Access Point, veamos como quedaría la WLAN después de realizar el ataque.

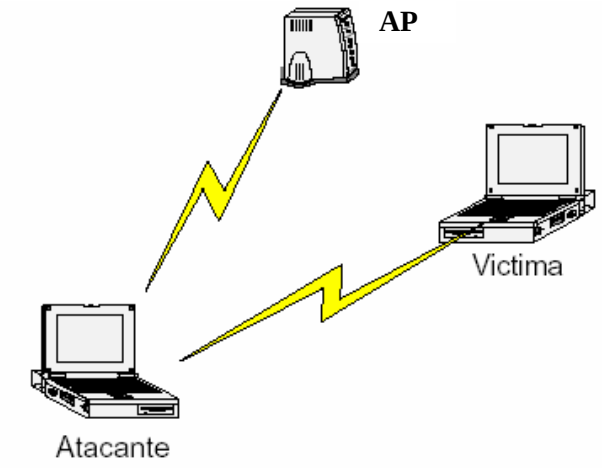


Figura 2.6: WLAN después del ataque

De esta manera todos los datos que viajan entre la victima y el Access Point 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 asumen que la capa física y la de enlace del modelo OSI son seguras, esto como hemos visto es falso para las redes Wireless y por tanto el uso de la seguridad depende del tipo de red en que se baya a implementar.

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.

2.2.2.6.- Ataque ARP Poisoning (Envenenamiento)

El *ARP cache poisoning (envenenamiento a la cache ARP)* es un ataque que sólo se puede llevar a cabo cuando el atacante está conectado a la misma LAN lógica que las victimas, transmite 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 (puente) transparentes de capa 2 del modelo OSI, lo que permite que los paquetes ARP pasen de la red Wireless hacia la LAN donde está conectado el Access Point 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. [www08].

Vamos a ver en la Figura 2.7 para entender mejor el ejemplo.

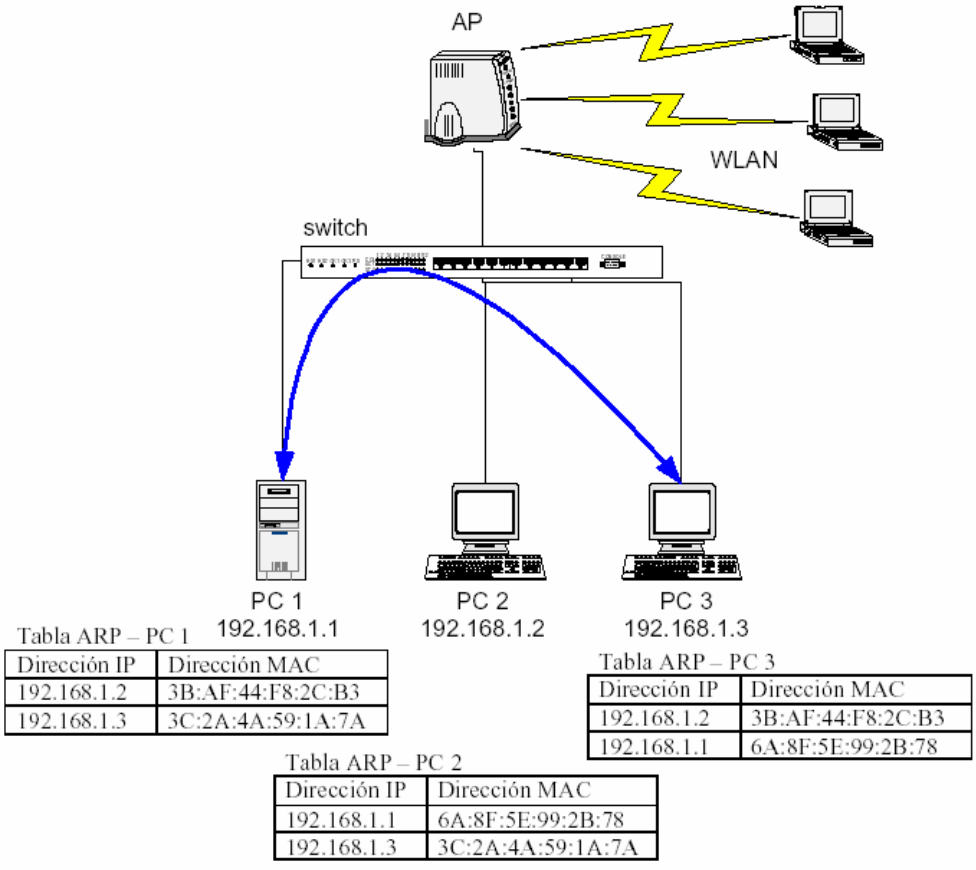


Figura 2.7: Comunicación de la Red WLAN y Cableada antes del Ataque. [www08].

El atacante envía paquetes *ARP* (Address Resolution Protoco, Protocolo de resolución de Direcciones) REPLY (Replica) a PC 3 diciendo que la dirección IP de PC1 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.

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

El servidor PC 1 se comunica con PC 3 a través del switch, si un atacante desde la WLAN adultera la tabla de ARP's de PC 1 y de PC 3 podrá realizar un ataque del tipo *Man in the Middle (interceptar el tráfico entre el Access Point y el cliente)* situándose entre los dos hosts de la red cableada.

Así es como se efectuaría la comunicación después del ataque como se ve en la Figura 2.8:

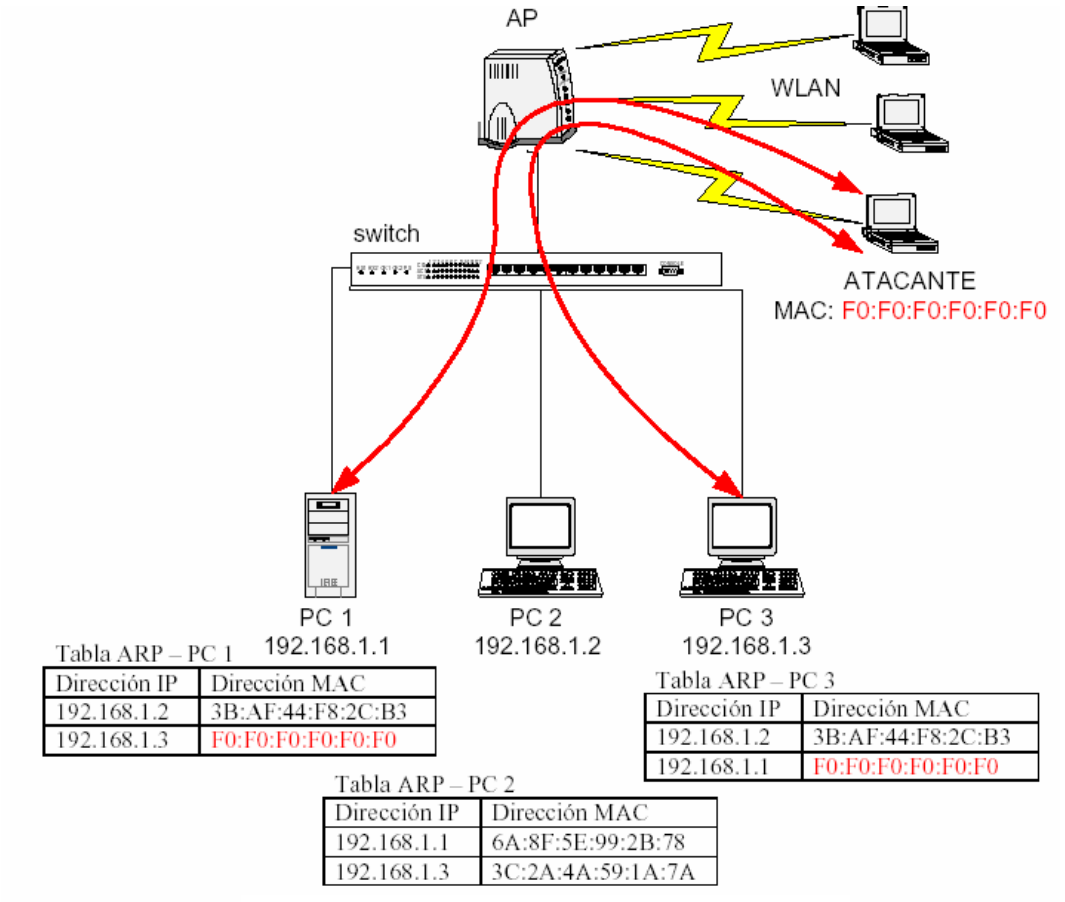


Figura 2.8: Ataque ARP Poisoning [www08].

2.2.3.- Vulnerabilidades del WEP

En la norma IEEE 802,11 para redes LAN inalámbricas está definido el uso del protocolo WEP. El protocolo WEP está basado en un algoritmo de encriptación simétrico que tiene un código secreto. Este código secreto lo tienen grabado tanto el cliente como el Punto de Acceso. Si el atacante conoce el texto sin cifrar (ya sea

por haber causado un fallo o por promedios estadísticos), podrá piratear la clave. Por tanto, el cifrado WEP no es seguro al ciento por ciento.

Las posibilidades actuales de proteger las redes LAN inalámbricas con encriptación WEP utilizando el algoritmo RC4, no son suficientes debido a los puntos débiles que contiene y que se describe en la Tabla 2.2.

Vulneravilidades	Descripción
El protocolo RC4 es un estádar débil para el cifrado de datos.	Debilidades propias del algoritmo de cifrado RC4, permiten ejecutar ataques de criptoanálisis eficientes.
La autenticación de dispositivos es simple	El modo "Challenge-Respons responde al acceso, " usado en la autenticación es vulnerable a ataques que permiten acceso no autorizado.
El Vector de inicialización VI es estático o no tiene un tamaño adecuado.	El tamaño del VI de 24-bits hace posible la visualización de frames Wireless cifrados
El mecanismo de protección de integridad no es adecuado.	Es posible modificar frames y generar de nuevo el CRC.
La llave de cifrado que se usa no tiene el mayor tamaño posible	El protocolo perimte llaves de 40-bits y 104-bits, el tamaño normalemente usado es 40-bit
La llave no puede ser modificada automaticamente.	Las mejores prácticas de seguridad siempre recomiendan el cambio periódico de las contraseñas
No se realiza autenticación de usuarios	Únicamente se autentifican los dispositivos de la red y no los usuarios.
No se permiten generar pistas de auditoría	No se puede hacer un seguimeinto de las actividades de los usuarios
Las características de seguridad bienen deshabilitadas por defecto.	Quien instala únicamente se preocupa porque quede funcionando.
Interferencia generada por gran cantidad de señales (jamming).	Se genera gran cantidad de interferencia de manera que los usuarios pierden acceso a la WLAN.

Tabla 2.2: Vulnerabilidades y descripción de WEP [www23]

2.2.4.- Amenazas físicas

Una WLAN utiliza una serie de componentes físicos, incluyendo los puntos de acceso, cables, antenas, adaptadores inalámbricos y software. Los daños sufridos por cualquiera de estos componentes podrían reducir la intensidad de las señales, limitar el área de cobertura o reducir el ancho de banda, poniendo en cuestión la capacidad de los usuarios para acceder a los datos y a los servicios de información Un atacante podría robar un dispositovo (Access Point, Tajeta inalámbrica, etc.)

o comprometer a una estación, adaptador inalámbrico, y utilizarlo para tratar de interceptar tráfico WLAN para obtener acceso no autorizado a la red. [www.07].

2.3.- Guía para la seguridad de redes WLAN

Los factores diferenciadores más importantes entre estos enfoques y una solución basada en 802.1x se resumen en la siguiente Tabla (aunque la opción "Sin WLAN" no se incluye puesto que no se puede comparar directamente con las demás). Las más importantes características de la seguridad de redes WLAN se resumen en la Tabla 2.3.

Característica	**WLAN 802.1X**	**WEP estática**	**VPN**	**IPSec**
Autenticación segura	Sí	No	Sí, Las VPN que utilicen autenticación de clave compartida.	Sí, Si se emplea autenticación de certificados o Kerberos.
Cifrado de datos de alta seguridad	Sí	No	Sí	Sí
Conexión transparente y reconexión a la WLAN	Sí	Sí	No	Sí
Autenticación de usuario	Sí	No	Sí	Sí
Autenticación de equipo	Sí	Sí	No	Sí
Difusión y tráfico de multidifusión protegidos	Sí	Sí	Sí	No
Se requieren dispositivos de red adicionales	Servidores RADIUS	No	Servidores VPN, servidores RADIUS	No
Acceso seguro a la propia WLAN	Sí	Sí	No	No