Seguridad en redes Inalámbricas

Panda Software

www.pandasoftware.es

Índice general

Introducción

Es un hecho ya consumado la creciente demanda e implantación de todo tipo de redes wireless en entornos corporativos, PYMES y en el ámbito familiar; este tipo de redes ofrecen un gran abanico de ventajas frente a las tradicionales redes cableadas. Facilidad de instalación, amplia cobertura, movilidad, sencilla ampliación, etc... son algunas de ellas; es precisamente gracias a estas características que las redes inalámbricas deben el gran apogeo que viven en este momento.

Sin embargo estas ventajas conllevan una contrapartida en forma de problemas de seguridad que, si bien es cierto que se están dando a conocer, no son siempre tenidos en cuenta por los administradores de dichas redes. A estas alturas está claro y demostrado que las redes wireless son inseguras de forma intrínseca y que es necesaria una mayor dedicación a su securización que con las redes cableadas.

El objetivo de este artículo es dar a conocer las características técnicas a nivel de seguridad de los estándares más empleados en la actualidad, los ataques a los que se tienen que enfrentar y las medidas de que disponen los administradores para securizar este tipo de redes.

Este artículo no pretende ser exhaustivo ni abarcar todos los ataques y sus variantes, para profundizar más en algunas de las técnicas aquí descritas consultar la sección de bibliografía, allí se podrán encontrar enlaces a documentos que tratan cada uno de los ataques de forma más profunda.

Glosario

A continuación se aclaran algunos de los términos empleados a lo largo del documento.

- **Listas de Control de Accesos (Access Control Lists - ACL):** Es la prevención del uso no autorizado de recursos mediante la restricción de su uso en función del usuario.
- **Punto de Acceso (PA):** Cualquier entidad que tiene funcionalidad de estación y provee acceso a servicios de distribución vía inalámbrica para estaciones asociadas.
- **Red Ad Hoc:** red wireless compuesta únicamente por estaciones con iguales derechos.
- **Portal:** punto lógico desde el cual se conecta una red wireless con una no wireless.
- **Estación:** cualquier dispositivo que cumple con un nivel MAC conforme a 802.11 y un nivel físico que posee una interfaz wireless.
- **Estación portátil:** estación que puede ser movida de ubicación, pero que solo puede transmitir o recibir en estado fijo.
- **Estación Móvil:** Estación que permite transmitir o recibir en movimiento.
- **Sniffer:** Programa de captura de paquetes de red; puede ser empleado con fines didácticos, maliciosos o constructivos. El funcionamiento de un sniffer depende del estado en que se coloca la tarjeta de red: modo promiscuo o normal. En modo promiscuo el sniffer captura todo el tráfico de red, a diferencia del modo normal de funcionamiento que solamente intercepta el tráfico saliente o entrante que corresponda a la tarjeta de red.
- **Modo master:** Modo en el que se pone una tarjeta de red cuando se pretende convertir el propio terminal en un Punto de Acceso.
- **CRC (Cyclic Redundancy Check):** Un tipo de función hash empleada para producir un checksum de un archivo, paquete de red, etc... y poder comprobar la integridad de los datos, por ejemplo tras transmisión. El checksum es una serie de bits resultado de una operación hash que mantiene su valor mientras el archivo o paquete no sea alterado.
- **XOR – Puerta lógica O-exclusiva:** Operador lógico que devuelve un estado verdadero si, y sólo si, uno de los operadores (no ambos) es verdadero; para dos operadores A y B, las posibles combinaciones son:

A	B	A xor B
0	0	0
0	1	1
1	0	1
1	1	0

- **DHCPDISCOVER:** Mensaje DHCP (Dynamic Host Configuration Protocol) que envían los clientes de una red cuando necesitan que se les asigne una dirección IP. Cuando un servidor DHCP recibe un mensaje de este tipo ha de asignar una dirección al cliente, o informar de que no queda ninguna libre.
- **Token (ficha):** Objeto virtual que se intercambian los terminales conectados entre ellos para validar la comunicación; sólo aquellos terminales que posean un token válido pueden comunicarse con el resto.

- **RADIUS (*Remote Access Dial-In User Server*):** Es un protocolo de autenticación, autorización y *accounting* para aplicaciones de acceso a la red o movilidad IP.
  Cuando se realiza la conexión con un ISP mediante módem, DSL, cablemódem, ethernet o WiFi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un Servidor de Acceso a la Red sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autentificación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema y le asigna los recursos de red como una dirección IP, etc.
  Una de las características mas importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

A quien va dirigido este artículo

Este artículo se ha escrito con la intención de hacerlo accesible a todo tipo de lectores, desde los más avanzados hasta aquellos que simplemente cuentan con una pequeña red doméstica.

Evidentemente al abarcar tan amplio grupo de lectores se hace necesario presentar unas directrices de lectura en función del grado de conocimientos previos del lector y de lo que éste pretenda profundizar en la materia de la seguridad en redes inalámbricas.

Para aquellos lectores más noveles en el tema se recomienda la lectura de los capítulos de *Conceptos básicos y Estandares Wifi* con el fin de conseguir una sólida base de conocimiento para abarcar el resto del artículo. A partir de aquí será el propio criterio del lector su mejor guía pero se aconseja la lectura de la introducción de todos los capítulos para que el lector adquiera una base de conocimiento más sólida. Este tipo de lectores ha de conseguir a grandes rasgos, mediante esta lectura, entender la situación actual de las redes inalámbricas así como sus riesgos potenciales.

Aquellos lectores que posean unos conocimientos más avanzados pueden saltarse todos aquellos capítulos introductorios pero se recomienda su lectura si se dispone del tiempo necesario pues el lector conseguirá asentar y refrescar estos conocimientos antes de adentrarse en los aspectos técnicos más avanzados de los siguientes capítulos.

Conceptos básicos

Vamos a comenzar con un vistazo a las distintas topologías que puede adoptar una red inalámbrica.

Modo Ad-Hoc

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

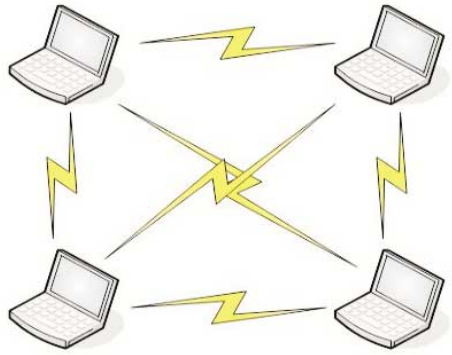

Figura 1 Topología Ad-hoc

Modo Infraestructura

En el modo Infraestructura como mínimo se dispone de un Punto de Acceso (AP) y las estaciones wireless no se pueden comunicar directamente, todos los datos deben pasar a través del AP. Todas las estaciones deben ser capaces de establecer conexión con el AP.

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

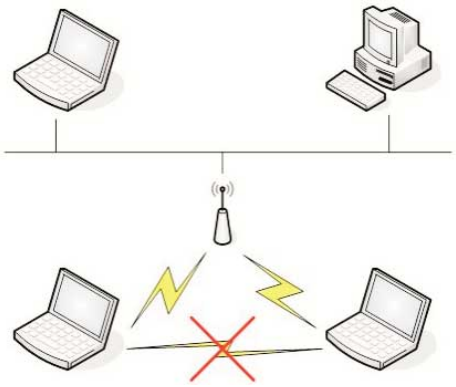

Figura 2 Red en modo infraestructura

ESSID

Cada red wireless tiene un ESSID (Extended Service Set Identifier), que la identifica. El ESSID consta de cómo máximo 32 caracteres y es case-sensitive. Es necesario conocer el ESSID del AP para poder formar parte de la red wireless, es decir, el ESSID configurado en el dispositivo móvil tiene que concordar con el ESSID del AP.

BSSID

Dirección MAC del Punto de Acceso, la emplean las tarjetas wireless para identificar y asociarse a redes inalámbricas.

Beacon Frames

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

WEP

Las redes Wireless (WLANs) son de por sí más inseguras que las redes con cables, ya que el medio físico utilizado para la transmisión de datos son las ondas electromagnéticas. Para proteger los datos que se envían a través de las WLANs, el estándar 802.11b define el uso del protocolo WEP (Wired Equivalent Privacy). WEP intenta proveer de la seguridad de una red con cables a una red Wireless, cifrando los datos que viajan sobre las ondas radioeléctricas en las dos capas más bajas del modelo OSI (capa física y capa de enlace). El protocolo WEP está basado en el algoritmo de cifrado RC4, y utiliza claves de 64bits o de 128bits. En realidad son de 40 y 104 bits, ya que los otros 24 bits van en el paquete como Vector de Inicialización (IV). Se utiliza un checksum para prevenir que se inyecten paquetes spoofeados. Más adelante veremos más a fondo como funciona la cifrado WEP.

Estandares WiFi

WiFi (Wireless Fidelity) es el nombre con el que se bautizó el estándar que describe los productos WLAN basados en los estándares 802.11. Dicho modelo fue desarrollado por un grupo de comercio, que adoptó el nombre de "WiFi Alliance", compuesto entre otros por compañías como 3com, Aironet, Luncent o Nokia y que responde al nombre oficial WECA (Wireless Ethernet Compatibility Alliance http://www.wi-fi.org).

El estándar 802.11 vio la luz en Junio de 1997 y se caracteriza por ofrecer velocidades de 1 y 2 Mbps, un sistema de cifrado sencillo llamado WEP (Wired Equivalent Privacy) y operar en la banda de frecuencia de 2.4 Ghz; en dos años, septiembre de 1999, aparecen las variantes 802.11a y 802.11b que ofrecen velocidades de 54 y 11 Mbsp respectivamente. Pronto se pondrían de manifiesto las carencias a nivel de seguridad de estos estándares.

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

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

A lo largo del estudio nos centraremos únicamente en los estándares 802.11b, 802.11g y 802.11i.

Seguridad en redes Wireless

Redes Abiertas

En este primer apartado vamos a ver las peculiaridades de las llamadas redes abiertas. Estas redes se caracterizan por no tener implementado ningún sistema de autenticación o cifrado. Las comunicaciones entre los terminales y los AP viajan en texto plano (sin cifrar) y no se solicita ningún dato para acceder a la red.

Los únicos elementos con los que se puede jugar para proporcionar algo de seguridad a este tipo de redes son:

- Direcciones MAC
- Direcciones IP
- El ESSID de la red

Filtrar el acceso a la red sólo a aquellos terminales que tengan una dirección MAC o IP determinada o bloqueando el envío de los BEACON FRAMES, de forma que sea necesario conocer de antemano el valor del ESSID para conectarse a la red, son los medios de los que se dispone para asegurar un poco este tipo de sistemas.

Nótese que estas medidas propuestas tienen en común que todas ellas intentan limitar el acceso no autorizado al sistema, pero no impiden que alguien espíe las comunicaciones. A continuación vamos a ver como saltarse las medidas propuestas anteriormente y otro tipo de ataques a los que se pueden ver sometidas las redes abiertas.

Romper ACL's (Access Control Lists) basados en MAC

La primera medida de seguridad implementada en las redes wireless fue, y sigue siendo, el filtrado de conexiones por dirección MAC. Para ello se crea una lista de direcciones MAC en el punto de acceso indicando si estas direcciones disponen de acceso permitido o denegado. La seguridad que proporciona esta medida es nula debido a la sencillez de cambiar la dirección MAC de nuestra tarjeta por otra válida previamente obtenida mediante un simple sniffer.

Si bien es cierto que el hecho de tener dos direcciones MAC en la misma red puede ocasionar problemas, esto se puede solucionar realizando un ataque de tipo DoS a la máquina a la cual le hemos tomado prestada la dirección MAC.

Ataque de Denegación de Servicio (DoS)

El objetivo de éste ataque implementado en una red inalámbrica consiste en impedir la comunicación entre un terminal y un punto de acceso. Para lograr esto sólo hemos de hacernos pasar por el AP poniéndonos su dirección MAC (obtenida mediante un sencillo sniffer) y negarle la comunicación al terminal o terminales elegidos mediante el envío continuado de notificaciones de desasociación.

Descubrir ESSID ocultos

Siendo fieles a la filosofía de *security through obscurity*, se ha aconsejado desde un principio la ocultación del ESSID de una red como método para aumentar la invisibilidad de nuestra red; una vez más sin embargo se ha demostrado que esta política de seguridad no resulta efectiva.

En casi todos los puntos de acceso podemos encontrar la opción de deshabilitar el envío del ESSID en los paquetes o desactivar los BEACON FRAMES. Ante esta medida de seguridad, un presunto atacante tendría dos opciones:

- Esnifar la red durante un tiempo indeterminado a la espera de una nueva conexión a la red con el objetivo de conseguir el ESSID presente en las tramas PROVE REQUEST del cliente (en ausencia de BEACON FRAMES) o en las tramas PROVE RESPONSE.
- Provocar la desconexión de un cliente mediante el mismo método que empleamos en el ataque DoS pero sin mantener al cliente desconectado.

Ataque Man in the middle

Este ataque apareció en escena a raíz de la aparición de los switches, que dificultaban el empleo de sniffers para obtener los datos que viajan por una red. Mediante el ataque *Man in the middlese* se hace creer al cliente víctima que el atacante es el AP y, al mismo tiempo, convencer al AP de que el atacante es el cliente.

Para llevar a cabo un ataque de este tipo es necesario obtener los siguientes datos mediante el uso de un sniffer:

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

Una vez obtenidos estos datos emplearíamos la misma metodología que en el ataque de tipo DoS para romper la conexión entre el cliente y el AP. Tras esta ruptura la tarjeta del cliente comenzará a buscar un nuevo AP en los diferentes canales, momento que aprovechará el atacante para suplantar al AP empleando su MAC y ESSID en un canal distinto. Para ello el atacante habrá de poner su propia tarjeta en modo **master**.

De forma paralela el atacante ha de suplantar la identidad el cliente con el AP real empleando para ello la dirección MAC del cliente, de esta forma el atacante logra colocarse entre ambos dispositivos de forma transparente.

Ataque ARP Poisoning

Al igual que en el caso del ataque man in the middle, el objetivo de este ataque consiste en acceder al contenido de la comunicación entre dos terminales conectados mediante dispositivos inteligentes como un switch. En esta variante de man in the middle se recurre a la alteración de la tabla ARP que mantienen de forma stateless todos los dispositivos de red.

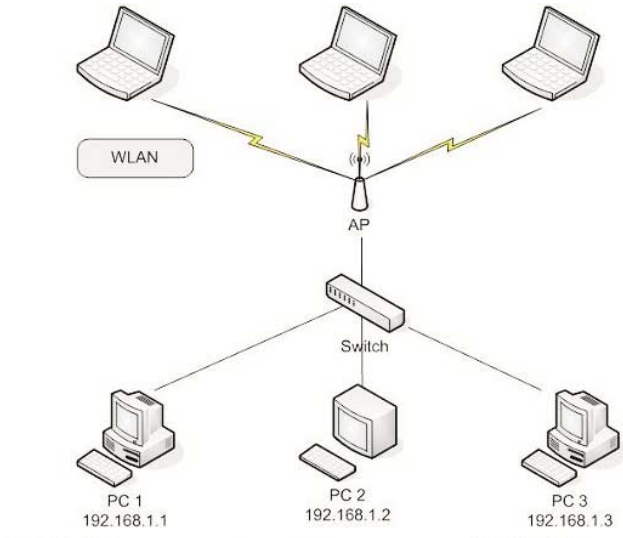

Tabla ARP -PC 1

Dirección IP	Dirección MAC
192.168.1.2	F2:F2:F2:F2:F2:F2
192.168.1.3	F3:F3:F3:F3:F3:F3

Tabla ARP -PC 2

Dirección IP	Dirección MAC
192.168.1.1	F1:F1:F1:F1:F1:F1
192.168.1.3	F3:F3:F3:F3:F3:F3

Tabla ARP -PC 3

Dirección IP	Dirección MAC
192.168.1.2	F2:F2:F2:F2:F2:F2
192.168.1.1	F1:F1:F1:F1:F1:F1

Figura 3 - Red antes del ataque

Para ello el atacante envía paquetes ARP REPLY al PC 3 diciendo que la dirección IP de PC 1 la tiene la MAC del atacante, de esta manera consigue modificar la caché de ARP's del 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 (ver figura 4).

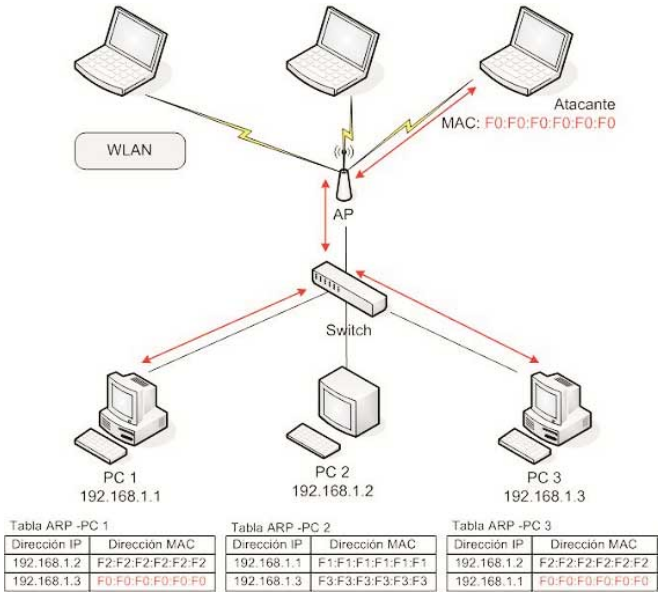

Figura 4 - Red tras el ataque

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.

Para realizar el ataque ARP Poisoning, existen múltiples herramientas, ya que este ataque no es específico de las redes wireless.

WEP

Como ya comentamos en la sección "Redes abiertas", en este tipo de sistemas todas las posibles medidas de seguridad que se pueden implantar se centran en intentar impedir la asociación a la red por parte de usuarios ilegítimos. En cambio ninguna de las medidas anteriores se empleaba para evitar la obtención de la información intercambiada entre terminales y AP (Contraseñas, etc...)

Para remediar esto se puede implementar el cifrado de las comunicaciones de tal forma que si alguien captura las comunicaciones entre los terminales y los AP, sólo obtenga una serie de bytes sin sentido.

El resto de los apartados se dedican a explicar el funcionamiento de WEP y los ataques a los que puede verse sometido este sistema de cifrado.

Principios de funcionamiento

WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cable) es el algoritmo de seguridad empleado para brindar protección a las redes inalámbricas incluido en la primera versión del estándar IEEE 802.11 y mantenido sin cambios en 802.11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. Este sistema emplea al algoritmo RC4 para el cifrado de las llaves que pueden ser de 64 o 128 bits teóricos, puesto que en realidad son 40 o 104 y el resto (24 bits) se emplean para el Vector de Inicialización.

La seguridad ofrecida por WEP tiene como pilar central una clave secreta compartida por todos los comunicadores y que se emplea para cifrar los datos enviados. Pese a no estar así establecido, en la actualidad todas las estaciones y puntos de acceso comparten una misma clave, lo que reduce el nivel de seguridad que puede ofrecer este sistema.

Como mecanismo de verificación de integridad se aplica un algoritmo de de comprobación de integridad (CRC-32) al texto plano, obteniendo un ICV o valor de comprobación de integridad que es añadido al texto cifrado de forma que el receptor del mensaje pueda comprobar que la integridad del mismo no ha sido alterada

Llaves

Las llaves, ya sean de 40 o 104 bits, se generan a partir de un clave que bien puede ser generada de forma automática o introducida manualmente; dicha clave ha de ser conocida por todos los comunicantes y este hecho conlleva a que normalmente se empleen claves muy sencillas y poco cambiantes. Es a partir de esta clave que se generan 4 llaves de 40 bits, de las cuales se empleará una diferente cada vez para realizar el cifrado WEP.

El proceso para obtener las llaves a partir de la clave consiste en la aplicación de una operación XOR con la cadena ASCII de la clave y de la cual se obtiene una semilla de 32 bits. Para realizar esta operación se divide la clave en grupos de 4 bytes de la siguiente manera:

Clave: "Mi clave WEP"

Se divide de esta forma:

M I _ C
L A V E
_ W E P

Y se realiza la operación XOR entre los elementos de cada columna; de esta manera obtenemos la semilla de 32 bits.
Esta semilla es la que emplea un generador de números pseudoaleatorios para generar 40 cadenas de 32 bits cada una. A partir de un bit de cada una de las 40 cadenas se obtienen 4 llaves de 40 bits y (en cada ocasión) una de ellas se usará para realizar el cifrado WEP

Figura 3 - Red antes del ataque

Cifrado

Una vez obtenidas las llaves que emplearemos para cifrar las tramas, vamos a ver el proceso de cifrado de las mismas.

Las tramas a cifrar se componen básicamente de una cabecera (header) y un contenido (payload), el primer paso a realizar es calcular el CRC del payload a cifrar; como ya comentamos, de este proceso obtendremos el valor de chequeo de integridad (ICV: Integrity Check Value) que añadiremos al final de la trama cifrada para que el receptor pueda comprobar que no ha sido modificada.

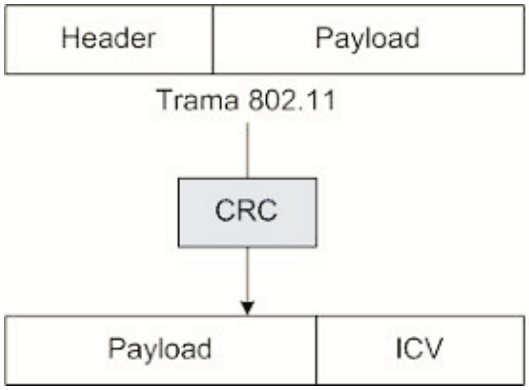

Figura 6 - Creación del ICV

A continuación se selecciona una de las llaves de 40 bits de entre las 4 posibles y se añade el Vector de Inicialización al comienzo de la llave.

El Vector de Inicialización (IV) es simplemente un contador que va cambiando de valor a medida que se generan tramas de forma que, al añadirlo a la llave, se aumenta el número de "llaves" posibles a emplear.

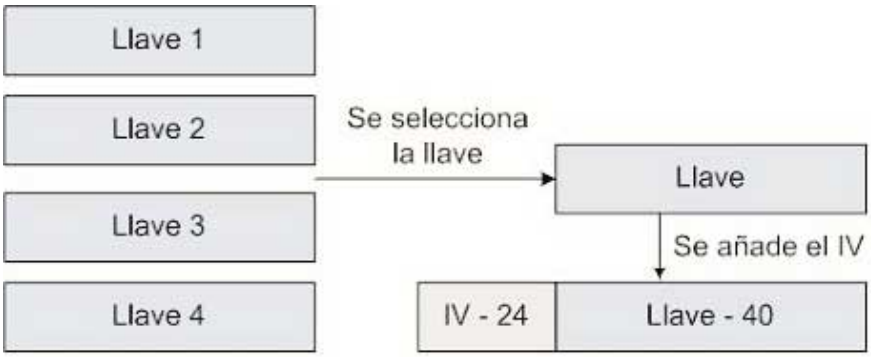

Figura 7 - Se añade el IV a la llave seleccionada

El Vector de Inicialización (IV) es simplemente un contador que va cambiando de valor a medida que se generan tramas de forma que, al añadirlo a la llave, se aumenta el número de "llaves" posibles a emplear.

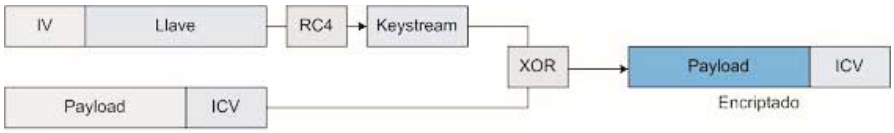

Figura 8 - Obtención del Payload cifrado

Como parte final se realiza un cifrado RC4 al conjunto IV + llave para obtener el keystream o flujo de llave. Dicho keystream se empleará para cifrar el conjunto Payload + ICV mediante una operación XOR.

Tras esto se añade al conjunto [Enc. Payload + Enc. ICV] la cabecera de la trama y el IV, y se obtiene el paquete listo para ser enviado

Figura 9 - Paquete listo para ser enviado

Atacando WEP

Como ya comentamos en la introducción, el protocolo de cifrado WEP demostró su ineficacia bien temprano tras su aparición, veremos a continuación algunos ejemplos de ataques que ponen en entredicho la eficacia de este protocolo.

Ataque de fuerza bruta

Teniendo en cuenta que la semilla (32 bits) que se emplea con el PRNG procede de una passphrase comúnmente compuesta por caracteres ASCII, podemos deducir que el bit más alto de cada carácter será siempre cero; tengamos en cuenta que el rango de caracteres ASCII se comprende entre 00 -> F7.

00 = 0000 0000
...
4F = 0100 0000
...
7F = 0111 1111

Como el resultado de una operación XOR de estos bits también es cero, las semillas sólo se encontrarán en el rango 00:00:00:00 - 7F:7F:7F:7F.

Debido a las peculiaridades del tipo de PRNG empleado la entropía se ve incluso más reducida. Esto se debe a que el PRNG empleado es del tipo LGC (linear congruential generator) o generador lineal congruente de módulo 2^32. Este tipo de PRNG tiene como inconveniente que los bits más bajos sean "menos aleatorios" que los altos. La longitud del ciclo del resultado será 2^24 lo que provoca que sólo las semillas que se encuentren entre 00:00:00:00 y 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.

Mediante esta información podemos reducir el ámbito del ataque de fuerza bruta considerablemente, reduciendo el tiempo necesario para producir todas las llaves de forma secuencial a unos días (210 días con u PIII a 500MHZ).

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.

Ataque Inductivo Arbaugh

Para llevar a cabo este ataque se han de seguir dos pasos; en el primero conseguiremos un keystream de tamaño limitado pero válido, y en un segundo paso repetiremos la fase de ataque todas las veces necesarias para obtener todos los IV posibles.

Como requisito para realizar éste ataque es necesario disponer del texto plano de un paquete; para ello podemos identificar mensajes DHCPDISCOVER de los que conocemos que parte de la cabecera es fija, concretamente las IP de origen y destino. Se lleva a cabo una operación XOR del texto plano con el texto cifrado para obtener n bytes del keystream de un IV concreto como podemos observar en la figura 10.

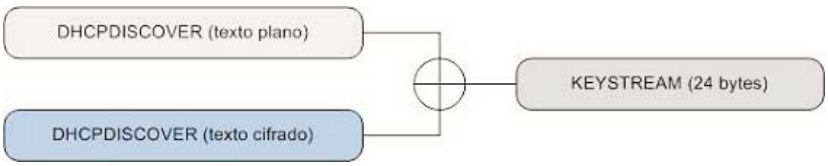

Figura 10 - Obtenemos parte del keystream

Mediante este keytream de n bytes se genera un paquete de tamaño N -3 de longitud; como este ataque es de tipo activo, necesitamos que el paquete generado sea alguno del que podamos obtener una respuesta (ping o arp request). Se calcula el ICV del paquete generado y añadimos sólo los 3 primeros bytes al paquete generado.

Como se aprecia en la figura 11, se lleva a cabo una operación XOR entre el paquete generado y el keystream obteniendo los datos cifrados necesarios para un paquete válido. Se añaden los elementos restantes necesarios para completar el paquete, como la cabecera, el IV y un último byte de valor cambiante que itera entre las 255 diferentes posibilidades.

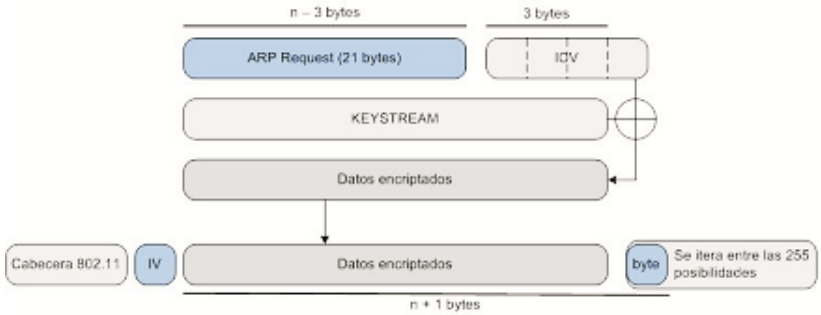

Figura 11 - Proceso de generación de los paquetes

Una vez obtenido el paquete completo hemos de enviarlo iterando entre las 255 posibles opciones hasta obtener respuesta desde el AP, lo que nos indicará que, para ese paquete concreto, el byte n+1 era el último byte del ICV. Se ha de realizar el mismo proceso hasta obtener el keystream completo. El proceso se muestra gráficamente en la figura 12.

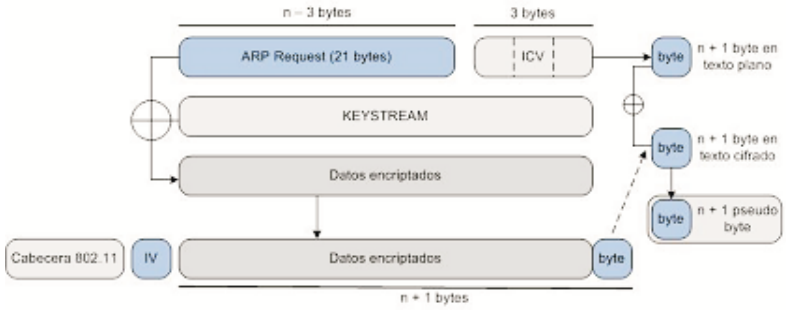

Figura 12 - Obtenemos bytes del keystream

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

Para conseguir el resto de keystreams se ha de volver ha generar un paquete del que se pueda obtener respuesta. Teniendo en cuenta que se conocerá el texto plano de la respuesta y que ésta vendrá siempre con un IV diferente es posible construir una tabla de keystreams por IV.

El atacante necesita almacenar 1500 bytes de keystream por cada IV, por lo que la tabla ocuparía 224x1500 = 24GB y tardaría una media de 30 horas en construir la tabla. Si el ataque se realiza en paralelo 4 hosts atacantes tardarían 7,5 horas y 8 hosts atacantes 3.75 horas.

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

Ataque FMS (Fluhrer-Mantin-Shamir)

El cifrado empleado por las redes inalámbricas (WEP) esta basada en el algoritmo de cifrado RC4 del cual se conocen algunas vulnerabilidades. El ataque estadístico FMS, que obtiene su nombre de las siglas de sus autores (Fluhrer, Mantin y Shamir), se basa en vulnerabilidades derivadas de la implementación específica del algoritmo RC4 en WEP. Dicha vulnerabilidad se describe en el documento titulado "Weaknesses in the Key Scheduling Algorithm of RC4" (http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf).

En febrero del 2002 David Hulton presentó el documento "Practical Exploitation of RC4 Weaknesses in WEP Environments" (http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt) en el que expone una serie de mejoras que optimizan el rendimiento del ataque. Es en este momento cuando aparecen las primeras implementaciones del ataque FMS que consiguen un rendimiento realista para llevarlo a cabo.

> Nota: Aunque vamos a dar un breve repaso a su funcionamiento, no vamos a profundizar en la teoría matemática en la que se sustenta; quien quiera profundizar más en este ataque encontrará toda la información necesaria en los documentos citados anteriormente.

El pilar en el que se basa el ataque FMS son los llamados IVs débiles; identificar este tipo de Ivs consiste en comprobar aquellos que cumplen la siguiente condición: (A + 3, N - 1, X). Estos Ivs tienen la característica especial de que provocan que no se incluya información de la clave en el keystream. Para cada uno de los paquetes que cumplen esta condición se ha de adivinar el byte que no tiene información de la llave. La probabilidad de adivinar el byte de la llave correctamente es de un 5% para cada paquete con un IV débil.

WPA

En el estándar 802.11 se definen unos mecanismos de seguridad que se han demostrado insuficientes e ineficientes:

- La confidencialidad se basa en el sistema denominado WEP (Wired Equivalent Privacy) que consiste en un sistema de cifrado simétrico RC4, utilizando una clave estática que comparten estaciones clientes y el punto de acceso. WEP usa vectores de inicialización (IV) para generar claves diferentes para cada trama. No obstante, WEP es un sistema muy débil ya que se puede conseguir la clave de cifrado monitorizando las tramas y procesándolas.

- La integridad se consigue utilizado técnicas de detección de errores (CRC) que no son eficientes para garantizar la integridad.

- La autenticación es inexistente ya que incluso permite hallar la clave usada por WEP de forma muy sencilla. Algunos fabricantes proporcionan autenticación del equipo a partir de la dirección MAC de la estación, pero es un método muy poco flexible.

Wi-Fi Alliance, como organización responsable de garantizar la interoperabilidad entre productos para redes inalámbricas de fabricantes diversos, ha definido una especificación de mercado basado en las directrices marcadas por el grupo de trabajo 802.11i denominada Wi-Fi Protected Access (WPA), junto con la correspondiente certificación de productos.

Privacidad e Integridad con TKIP

Temporal Key Integrity Protocol (TKIP) es el protocolo elegido con el objetivo de sustituir a WEP y solucionar los problemas de seguridad que éste plantea. Como características mejoradas destacar la ampliación de la clave a 128 bits y el cambio del carácter de la misma de estática a dinámica; cambiando por usuario, sesión y paquete y añadiendo temporalidad. El vector de inicialización pasa de 24 a 48 bits, minimizando la reutilización de claves. Y como colofón se han añadido claves para tráfico de difusión y multidifusión.

TKIP utiliza el algoritmo "Michael" para garantizar la integridad, generando un bloque de 4 bytes (denominado MIC) a partir de la dirección MAC de origen, de destino y de los datos y añadiendo el MIC calculado a la unidad de datos a enviar. Posteriormente los datos (que incluyen el MIC) se fragmentan y se les asigna un número de secuencia. La mezcla del número de secuencia con la clave temporal genera la clave que se utilizará para el cifrado de cada fragmento.

Autenticación Mediante 802.1X/EAP

El cometido principal del estándar 802.11x es encapsular los protocolos de autenticación sobre los protocolos de la capa de enlace de datos y permite emplear el protocolo de autenticación extensible (EAP) para autentificar al usuario de varias maneras.

IEEE 802.1x define 3 entidades:

- el solicitante (supplicant), reside en la estación inalámbrica
- el autenticador (authenticator), reside en el AP
- el servidor de autenticación, reside en un servidor AAA (Authentication, Authorization, & Accounting) como RADIUS

EAP comprende cuatro tipos de mensajes:

- Petición (Request Identity): empleado para enviar mensajes desde el AP al cliente.
- Respuesta (Identity Response): empleado para enviar mensajes desde el cliente al AP.
- Éxito (Success): emitido por el AP, significa que el acceso está permitido.
- Fallo (Failure): enviado por el AP cuando para indicarle al Suplicante que se deniega la conexión.

Proceso de autenticación, tras la asociación:

- Se envía el EAP-Request/Identity desde el Autenticador al Suplicante.
- El Suplicante responde con EAP-Response/Identity al Autenticador, el cual lo pasa al Servidor de Autenticación.
- Se tuneliza el Challenge/Response y si resulta acertado el Autenticador permite al Suplicante acceso a la red condicionado por las directrices del Servidor de Autenticación.

El funcionamiento base del estándar 802.11x se centra en la denegación de cualquier tráfico que no sea hacia el servidor de autenticación hasta que el cliente no se haya autenticado correctamente. Para ello el autenticador crea una puerto por cliente que define dos caminos, uno autorizado y otro no; manteniendo el primero cerrado hasta que el servidor de autenticación le comunique que el cliente tiene acceso al camino autorizado.

El solicitante, cuando pasa a estar activo en el medio, selecciona y se asocia a un AP. El autenticador (situado en el AP) detecta la asociación del cliente y habilita un puerto para ese solicitante, permitiendo únicamente el tráfico 802.1x, el resto de tráfico se bloquea. El cliente envía un mensaje "EAP Start". El autenticador responde con un mensaje "EAP Request Identity" para obtener la identidad del cliente, la respuesta del solicitante "EAP Response" contiene su identificador y es retransmitido por el autenticador hacia el servidor de autenticación. A partir de ese momento el solicitante y el servidor de autenticación se comunicarán directamente, utilizando un cierto algoritmo de autenticación que pueden negociar. Si el servidor de autenticación acepta la autenticación, el autenticador pasa el puerto del cliente a un estado autorizado y el tráfico será permitido.

Los métodos de autenticación contemplados en WPA son: EAP-TLS, EAP-TTLS y PEAP. Todos ellos se basan en el método de Infraestructura Pública (PKI) para autenticar al usuario y al servidor de autenticación mediante certificados digitales. Para ello es necesaria la existencia de una Autoridad de Certificación (CA), bien sea empresarial o pública.

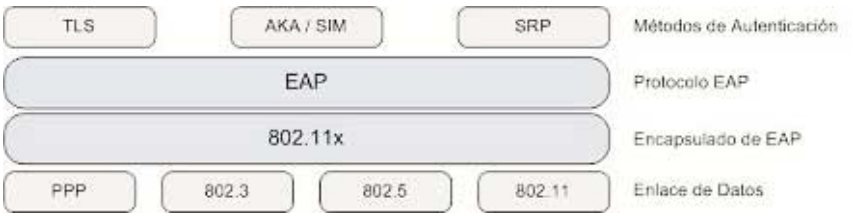

Figura 13 - Estructura EAP / 802.11x

EAP-TLS

Requiere de la posesión de certificados digitales por parte del cliente y el servidor de autenticación; el proceso de autenticación comienza con el envío de su identificación (nombre de usuario) por parte del solicitante hacia el servidor de autenticación, tras esto el servidor envía su certificado al solicitante que, tras validarlo, responde con el suyo propio. Si el certificado del solicitante es válido, el servidor responde con el nombre de usuario antes enviado y se comienza la generación de la clave de cifrado, la cual es enviada al AP por el servidor de autenticación para que pueda comenzar la comunicación segura.

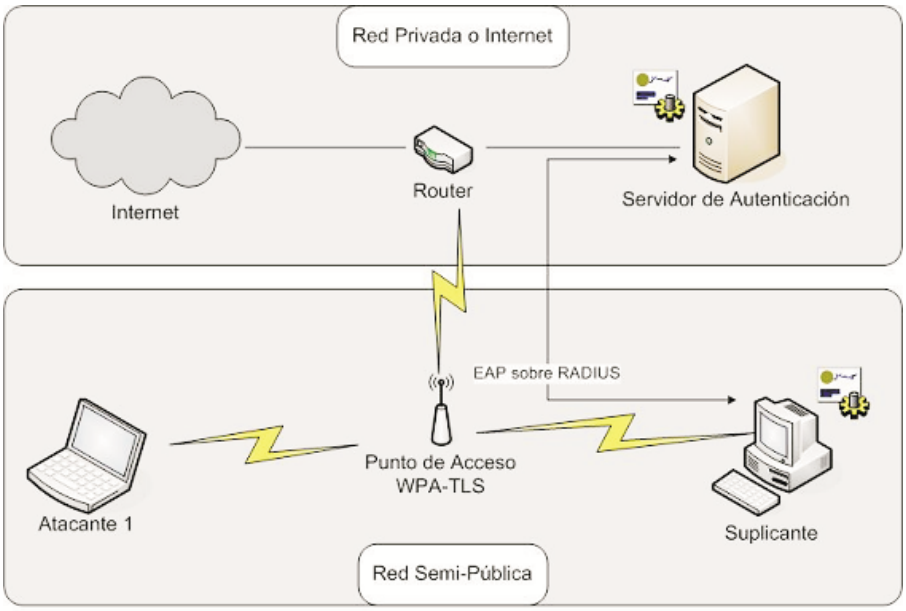

Figura 14 - Estructura necesaria para una red EAP-TLS

Vulnerabilidades en EAP-TLS

En la fase de identificación el cliente manda el mensaje EAP-Identity sin cifrar, permitiendo a un atacante ver la identidad del cliente que está tratando de conectarse.

Ejemplo:

```
No.     Time        Source                Destination           Protocol Info
1       0.000000    192.168.182.190       192.168.182.26        RADIUS   Access Request(1)
(id=15, l=166)

Frame 1 (208 bytes on wire, 208 bytes captured)
    Arrival Time: Jul 12, 2005 08:52:44.825959000
    Time delta from previous packet: 0.000000000 seconds
    Time since reference or first frame: 0.000000000 seconds
    Frame Number: 1
    Packet Length: 208 bytes
    Capture Length: 208 bytes
    Protocols in frame: eth:ip:udp:radius:eap
Ethernet II, Src: 00:01:38:33:8c:5c, Dst: 00:0c:29:b2:9d:b0
    Destination: 00:0c:29:b2:9d:b0 (Vmware_b2:9d:b0)
    Source: 00:01:38:33:8c:5c (XaviTech_33:8c:5c)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.182.190 (192.168.182.190), Dst Addr: 192.168.182.26
(192.168.182.26)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 194
    Identification: 0x03b2 (946)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
    Header checksum: 0x484f (correct)
    Source: 192.168.182.190 (192.168.182.190)
    Destination: 192.168.182.26 (192.168.182.26)
User Datagram Protocol, Src Port: 50000 (50000), Dst Port: radius (1812)
    Source port: 50000 (50000)
    Destination port: radius (1812)
    Length: 174
    Checksum: 0x2966 (correct)
```

```
Radius Protocol
   Code: Access Request (1)
   Packet identifier: 0xf (15)
   Length: 166
   Authenticator: 0xAB338D7E5E8F3EE66874A63AB1C39311
   Attribute value pairs
      t:EAP Message(79) l:25
         Extensible Authentication Protocol
            Code: Response (2)
            Id: 1
            Length: 23
            Type: Identity [RFC3748] (1)
            Identity (18 bytes): Client certificate
      t:Calling Station Id(31) l:19, Value:"00-80-5A-27-5D-B9"
         Calling-Station-Id: 00-80-5A-27-5D-B9
      t:Called Station Id(30) l:30, Value:"00-01-36-0A-E3-29:Wifi_insec"
         Called-Station-Id: 00-01-36-0A-E3-29:Wifi_insec
      t:User Name(1) l:20, Value:"Client certificate"
         User-Name: Client certificate
      t:NAS IP Address(4) l:6, Value:0.0.0.0
         Nas IP Address: 0.0.0.0 (0.0.0.0)
      t:NAS Port(5) l:6, Value:3
      t:NAS Port Type(61) l:6, Value:Wireless IEEE 802.11(19)
      t:NAS Port ID(87) l:10, Value:"wireless"
      t:Framed MTU(12) l:6, Value:1300
      t:Message Authenticator(80) l:18, Value:E8B1EABB064AE8F0F9A02AF3021328C3

0000   00 0c 29 b2 9d b0 00 01 38 33 8c 5c 08 00 45 00   ..).....83.\..E.
0010   00 c2 03 b2 00 00 80 11 48 4f c0 a8 b6 be c0 a8   ........HO......
0020   b6 1a c3 50 07 14 00 ae 29 66 01 0f 00 a6 ab 33   ...P....)f.....3
0030   8d 7e 5e 8f 3e e6 68 74 a6 3a b1 c3 93 11 4f 19   .~^.>.ht.:....O.
0040   02 01 00 17 01 43 6c 69 65 6e 74 20 63 65 72 74   .....Client cert
0050   69 66 69 63 61 74 65 1f 13 30 30 2d 38 30 2d 35   ificate..00-80-5
0060   41 2d 32 37 2d 35 44 2d 42 39 1e 1e 30 30 2d 30   A-27-5D-B9..00-0
0070   31 2d 33 36 2d 30 41 2d 45 33 2d 32 39 3a 57 69   1-36-0A-E3-29:Wi
0080   66 69 5f 69 6e 73 65 63 01 14 43 6c 69 65 6e 74   fi_insec..Client
0090   20 63 65 72 74 69 66 69 63 61 74 65 04 06 00 00    certificate....
00a0   00 00 05 06 00 00 00 03 3d 06 00 00 00 13 57 0a   ........=.....W.
00b0   77 69 72 65 6c 65 73 73 0c 06 00 00 05 14 50 12   wireless......P.
00c0   e8 b1 ea bb 06 4a e8 f0 f9 a0 2a f3 02 13 28 c3   .....J....*...(.
```

De la misma forma el envío de la aceptación/denegación de la conexión se realiza sin cifrar, con lo que un eventual atacante puede reenviar este tipo de tráfico para generar ataques de tipo DoS.

Ejempo de aceptación:

No.	Time	Source	Destination	Protocol	Info
10	0.305134	192.168.182.26	192.168.182.190	RADIUS	Access Accept(2) (id=19, l=180)

```
Frame 10 (222 bytes on wire, 222 bytes captured)
    Arrival Time: Jul 12, 2005 08:52:45.131093000
    Time delta from previous packet: 0.026146000 seconds
    Time since reference or first frame: 0.305134000 seconds
    Frame Number: 10
    Packet Length: 222 bytes
    Capture Length: 222 bytes
    Protocols in frame: eth:ip:udp:radius:eap
Ethernet II, Src: 00:0c:29:b2:9d:b0, Dst: 00:01:38:33:8c:5c
    Destination: 00:01:38:33:8c:5c (XaviTech_33:8c:5c)
    Source: 00:0c:29:b2:9d:b0 (Vmware_b2:9d:b0)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.182.26 (192.168.182.26), Dst Addr: 192.168.182.190
(192.168.182.190)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 208
    Identification: 0x0000 (0)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0x4bf3 (correct)
    Source: 192.168.182.26 (192.168.182.26)
    Destination: 192.168.182.190 (192.168.182.190)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 50000 (50000)
    Source port: radius (1812)
    Destination port: 50000 (50000)
    Length: 188
    Checksum: 0x76d1 (correct)
Radius Protocol
    Code: Access Accept (2)
    Packet identifier: 0x13 (19)
    Length: 180
    Authenticator: 0xC2A14934417AF1188A78514F8CAE0DF0
    Attribute value pairs
        t:Vendor Specific(26) l:58, Vendor:Microsoft(311)
            t:MS MPPE Recv Key(17) l:52,
Value:A1FFCCC46E6BAD219DC68CDDC363E9E56A4940E4BF9694A89E4319C94F992C864609FEA
EB1675D2A72D1FFE994CFE1CEDB10
        t:Vendor Specific(26) l:58, Vendor:Microsoft(311)
            t:MS MPPE Send Key(16) l:52,
```

```
Value:AD6AEDBC195A3D2CAF96B76F7AEFE1168F042A44B09EB60DB11E610B1F8D127D06F130E
1AA4911629941366EA9B61997B414
      t:EAP Message(79) l:6
         Extensible Authentication Protocol
            Code: Success (3)
            Id: 5
            Length: 4
      t:Message Authenticator(80) l:18, Value:7C24B3EB1C5DDD0CDB717C19F7084F39
      t:User Name(1) l:20, Value:"Client certificate"
         User-Name: Client certificate

0000   00 01 38 33 8c 5c 00 0c 29 b2 9d b0 08 00 45 00   ..83.\..)....E.
0010   00 d0 00 00 40 00 40 11 4b f3 c0 a8 b6 1a c0 a8   ....@.@.K.......
0020   b6 be 07 14 c3 50 00 bc 76 d1 02 13 00 b4 c2 a1   .....P..v.......
0030   49 34 41 7a f1 18 8a 78 51 4f 8c ae 0d f0 1a 3a   I4Az...xQO.....:
0040   00 00 01 37 11 34 a1 ff cc c4 6e 6b ad 21 9d c6   ...7.4....nk.!..
0050   8c dd c3 63 e9 e5 6a 49 40 e4 bf 96 94 a8 9e 43   ...c..jI@......C
0060   19 c9 4f 99 2c 86 46 09 fe ae b1 67 5d 2a 72 d1   ..O.,.F....g]*r.
0070   ff e9 94 cf e1 ce db 10 1a 3a 00 00 01 37 10 34   .........:...7.4
0080   ad 6a ed bc 19 5a 3d 2c af 96 b7 6f 7a ef e1 16   .j...Z=,...oz...
0090   8f 04 2a 44 b0 9e b6 0d b1 1e 61 0b 1f 8d 12 7d   ..*D......a....}
00a0   06 f1 30 e1 aa 49 11 62 99 41 36 6e a9 b6 19 97   ..0..I.b.A6n....
00b0   b4 14 4f 06 03 05 00 04 50 12 7c 24 b3 eb 1c 5d   ..O.....P.|$...]
00c0   dd 0c db 71 7c 19 f7 08 4f 39 01 14 43 6c 69 65   ...q|...O9..Clie
00d0   6e 74 20 63 65 72 74 69 66 69 63 61 74 65        nt certificate
```

PEAP y EAP-TTLS

El mayor inconveniente que tiene el uso de EAP-TLS es que tanto el servidor de autenticación como los clientes han de poseer su propio certificado digital, y la distribución entre un gran número de ellos puede ser difícil y costosa. Para corregir este defecto se crearon PEAP (Protected EAP) y EAP - Tunneled TLS que únicamente requieren certificado en el servidor.

La idea base de estos sistemas es que, empleando el certificado del servidor previamente validado, el cliente pueda enviar sus datos de autenticación cifrados a través de un tunel seguro. A partir de ese momento, y tras validar el servidor al solicitante, ambos pueden generar una clave de sesión.

WPA y Seguridad en Pequeñas Oficinas - WPA-PSK

Los métodos soportados por EAP necesitan de una cierta infraestructura, fundamentalmente de un servidor RADIUS, lo que puede limitar su implementación en redes pequeñas. Wi-Fi ofrece los beneficios de WPA mediante el uso de una clave pre-compartida (PSK, pre-shared key) o contraseña. Esto posibilita el uso de TKIP, pero configurando manualmente una clave en el cliente wireless y en el punto de acceso. El estándar permite claves de hasta 256 bits, lo que proporciona una seguridad muy elevada. Sin embargo el escoger claves sencillas y cortas puede hacer vulnerable el sistema frente a ataques de fuerza bruta o diccionario.

Ataque WPA-PSK

El único ataque conocido contra WPA-PSK es del tipo fuerza bruta o diccionario; pese a la existencia de este ataque la realidad es que el rendimiento del ataque es tan bajo y la longitud de la passphrase puede ser tan larga, que implementarlo de forma efectiva es prácticamente imposible. Los requisitos para llevar a cabo el ataque son:

- PUn archivo con la captura del establecimiento de conexión entre el cliente y el AP.
- PEl nombre de ESSID
- PUn archivo de diccionario.

Se puede auditar la fortaleza de las contraseñas empleadas en un sistema realizando ataques de diccionario o de fuerza bruta, en este último caso empleando herramientas al uso para crear todas las combinaciones de caracteres posibles.

Portales Cautivos

Sistema creado para permitir la validación de usuarios en nodos wireless. Ampliamente empleado para proporcionar conexión regulada a los usuarios de establecimientos públicos, hoteles, aeropuertos, etc.

En un sistema con portal cautivo se definen dos partes diferenciadas: la zona pública y la privada. La zona pública se compone, normalmente, de nodos wireless que posibilitan la conexión de cualquier terminal; en cambio el acceso la zona privada, normalmente Internet, se encuentra regulado por un sistema de autenticación que impide la navegación hasta que el usuario se valida.

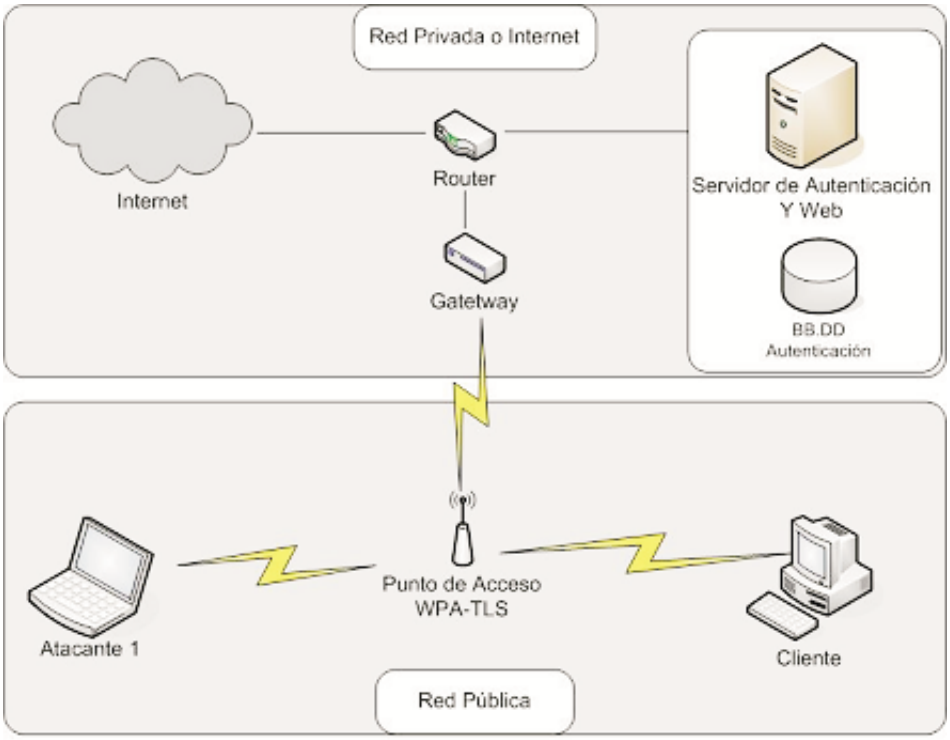

Figura 15 - Infraestructura necesaria para un sistema de Portal Cautivo

El sistema de portales cautivos se compone, en líneas generales, de un serie de APs conectados a un Gateway colocado antes de la zona privada, un servidor web donde colocar el portal y una base de datos donde almacenar los usuario y el servicio de autenticación.

En el momento en que un usuario no autenticado decide conectarse a la zona privada el gateway comprueba si dicho usuario está autenticado; para ello se basa en la posesión de tokens temporales gestionados por https. Si dicho usuario no posee un token válido, el gateway redirecciona la conexión hacia el portal donde al usuario se le solicitarán un usuario y contraseña válidos para asignarle un token. Una vez obtenido un token (y mientras éste sea válido) el gateway permitirá la conexión hacia la zona privada.

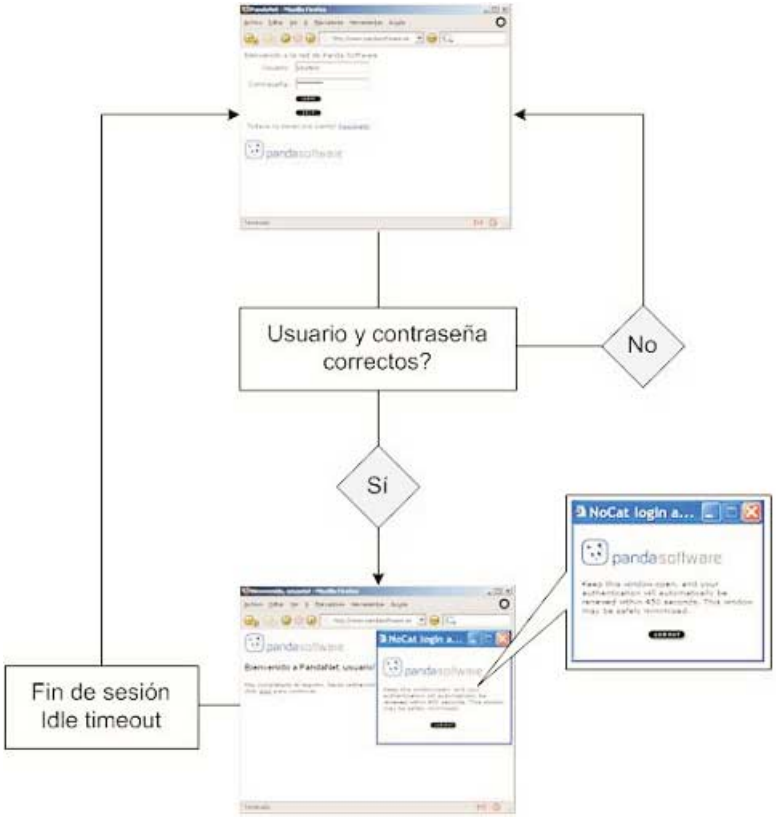

Figura 16 - Proceso de conexión al portal cautivo

Otra aplicación para los portales cautivos se limita a presentar un portal antes de permitir la salida a la zona privada, mostrando las normas de uso, publicidad del establecimiento, etc.

Vulnerabilidades en Portales Cautivos

Debido a las características de la zona abierta de los sistemas que implantan este sistema de portales, se permite la asociación con el AP a cualquier cliente y el tráfico entre los clientes y el AP no va cifrado; por este motivo se puede capturar el tráfico de las conexiones con la zona privada.

Por otra parte es posible implementar ataques de tipo spoofing o hijacking mientras el token que emplea el usuario legítimo sea válido.

DNS tunneling

En la mayoría de los casos, el gateway que filtra las conexiones y las redirige en función de la presencia del token permite el paso de las peticiones DNS hacia la zona privada; con esto en mente es posible encapsular el tráfico TCP/IP dentro de peticiones DNS y saltarse las restricciones del portal cautivo.

Sin embargo esta técnica plantea varios problemas:

- El tráfico DNS emplea el protocolo UDP, el cual no está orientado a conexión y, como veremos, no se garantiza el reensamblado correcto de los paquetes.
- Las peticiones DNS están limitadas a un tamaño máximo de 512 bytes por paquete, insuficiente para un encapsulado de TCP/IP.
- Los servidores DNS sólo pueden enviar paquetes como respuesta a un solicitud, nunca de forma independiente.

Para solucionar estos inconvenientes es necesaria la creación de un servidor específico que pueda saltarse estas restricciones y que, junto con una aplicación creada a tal efecto, permita encapsular las comunicaciones a través de peticiones UDP a través del puerto 53.

Otro requisito sería la creación de un protocolo propio que amplíe el tamaño máximo de los paquetes y los dote de algún mecanismo para mantener el orden de reensamblado. Por supuesto este protocolo tendría que ser empleado por nuestro servidor y la aplicación.

Este trabajo a sido llevado a cabo con éxito mediante un protocolo bautizado como "NSTX Protocol - Nameserver Transfer Protocol" y una aplicación llamada "nstx".

Más información se puede encontrar en: http://nstx.dereference.de/

Rogue AP

Rogue AP: *Punto de acceso no autorizado.*

Introducción

Este tipo de ataques consiste, a nivel básico, en colocar un punto de acceso bajo nuestro control cerca de las instalaciones de la víctima de forma que los clientes asociados o por asociar a esa red se conecten a nuestro AP en lugar de uno legítimo de la víctima debido a la mayor señal que

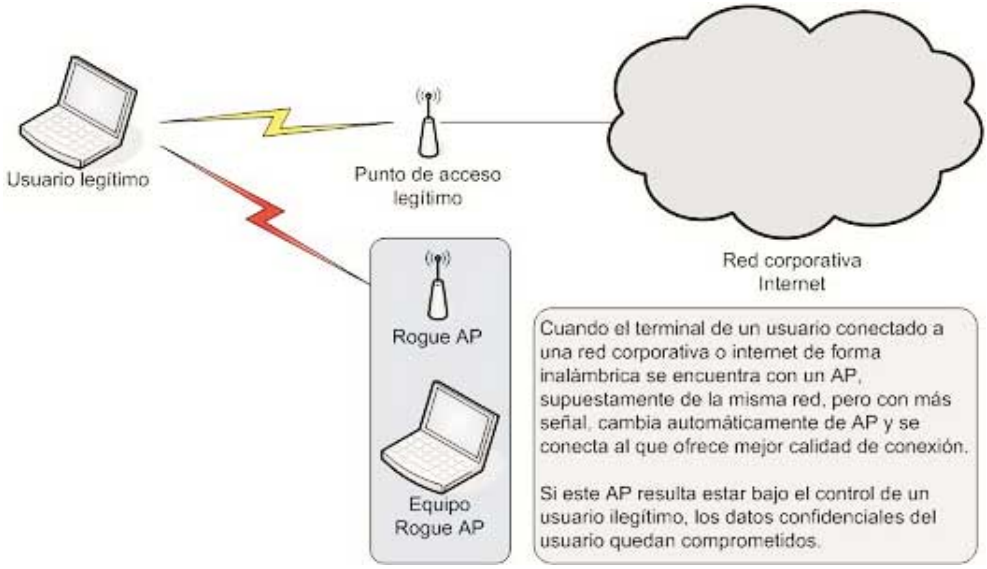

Figura 15 - Infraestructura necesaria para un sistema de Portal Cautivo

recibe del nuestro.

Una vez conseguida la asociación al Rogue AP, el atacante puede provocar ataques de tipo DoS, robar datos de los clientes como usuarios y contraseñas de diversos sitios web o monitorizar las acciones del cliente.

Este tipo de ataques se ha empleado tradicionalmente para:

- Crear puertas traseras corporativas.
- Espionaje industrial.

La filosofía de este ataque se podría resumir en la frase:
"Porque forzar la cerradura si puedes pedir, y que te den, la llave?"

Rogue AP básico

Una vez visto un breve esbozo del funcionamiento básico de los ataques mediante Rogue AP vamos a profundizar un poco más en los detalles.

El Rogue AP puede consistir en un AP modificado o un portátil con el software adecuado instalado y configurado. Este software ha de consistir en: Servidor http, Servidor DNS, Servidor DHCP y un Portal Cautivo con sus correspondientes reglas para redirigir el tráfico al portal. Todo este proceso de instalación y configuración se puede simplificar bastante mediante Airsnarf, herramienta que automatiza el proceso de configuración y arranque de un Rogue AP.

Sin embargo hace falta algo más para poder montar un Rogue AP, se requiere que la tarjeta wireless sea compatible con HostAP, un driver específico que permite colocar la tarjeta en modo master, necesario para que nuestro terminal pueda comportarse como si fuese un AP. Si queremos montar un Rogue AP sobre un Windows deberemos encontrar una tarjeta compatible con SoftAP para poder cambiar el modo a master, y emplear Airsnarf para configurar los distintos servicios.

El proceso de configuración que lleva a cabo Airsnarf consiste en colocar el portal cautivo y arrancar el servidor http, configurar el servidor DHCP para que proporciones IP, gateway y DNS al cliente; evidentemente el gateway y el servidor DNS será el terminal del atacante convertido en Rogue AP. Por último se configura el servidor DNS para que resuelva todas las peticiones con a la IP del atacante, de forma que se puedan redireccionar todas hacia el portal cautivo del Rogue AP.

> Nota: Para redireccionar todas, o algunas, de las peticiones http al portal cautivo se emplea iptables en Linux o RRaS (Routing and Remote Access Service) en Windows.

Una vez el usuario introduce su usuario y contraseña en el portal cautivo, el atacante ya las tiene en su poder. Lo normal es cambiar la apariencia del portal cautivo para que sea igual a la del portal del sistema al que se está suplantando.

Otra opción es dejar navegar al usuario normalmente pero redirigir determinadas páginas a otras copias locales con el fin de obtener usuarios y contraseñas. Para ello se puede modificar el servidor DNS para resolver aquellas páginas que nos convengan a nuestra dirección local donde tendremos preparada una copia falsa de la página.

Rogue RADIUS

Por este nombre se conocen aquellos montajes que, a parte del Rogue AP clásico, incorporan un servidor RADIUS en el terminal del atacante. Para este fin se emplea comúnmente un servidor FreeRADIUS adecuadamente configurado para responder a las peticiones de los usuarios legítimos.

Este tipo de montaje se emplea contra sistemas que cuentan con servidores de autenticación y redes securizadas mediante EAP de forma que el atacante pueda suplantar todos los dispositivos y servidores presentes en el sistema legítimo de forma convincente, autenticador y servidor de autenticación.

Rogue RADIUS vs. EAP

Antes de ver las vias de ataque a emplear contra sistemas protegidos por EAP, vamos a profundizar en los mecanismos de autenticaión que se usan en las variantes de EAP más extendidas, concretamente vamos a repasar el intercambio de mensajes que se produce en una autenticación pues, como veremos, es en este intercambio donde reside su vulnerabilidad.

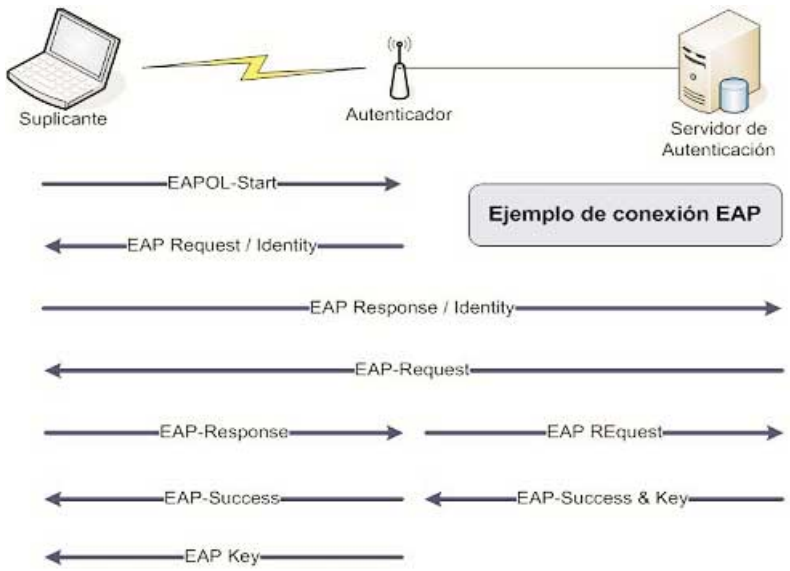

Figura 18 - Ejemplo de conexión EAP

Como se puede apreciar en el gráfico, una autenticación EAP consiste en dos fases diferenciadas; en una primera el suplicante proporciona al servidor de autenticación su identidad a través del autenticador, en la segunda el servidor de autenticación propone un reto al suplicante que, al superarlo, se gana el derecho a acceder a la red. Este acceso se mantiene limitado por el autenticador en función de las directrices marcadas por el servidor de autenticación. Directrices que a su vez varían en función de la identidad del suplicante.

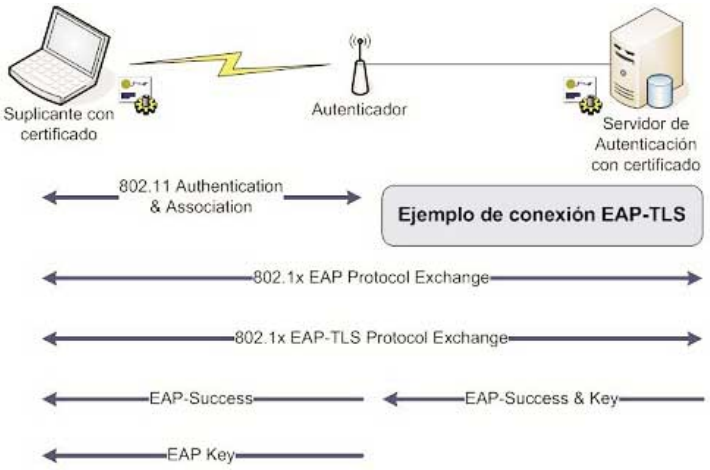

Figura 19 - Ejemplo de conexión EAP-TLS

EAP-TLS pretende mejorar la seguridad de EAP mediante la implantación de certificados digitales instalados en todos los clientes y servidores. De esta manera se añade la necesidad de poseer un certificado válido para completar la autenticación. Tras el intercambio de certificados entre el suplicante y el servidor de autenticación, estos negocian un secreto común que se emplea para cifrar el resto de las comunicaciones a partir de ese momento.

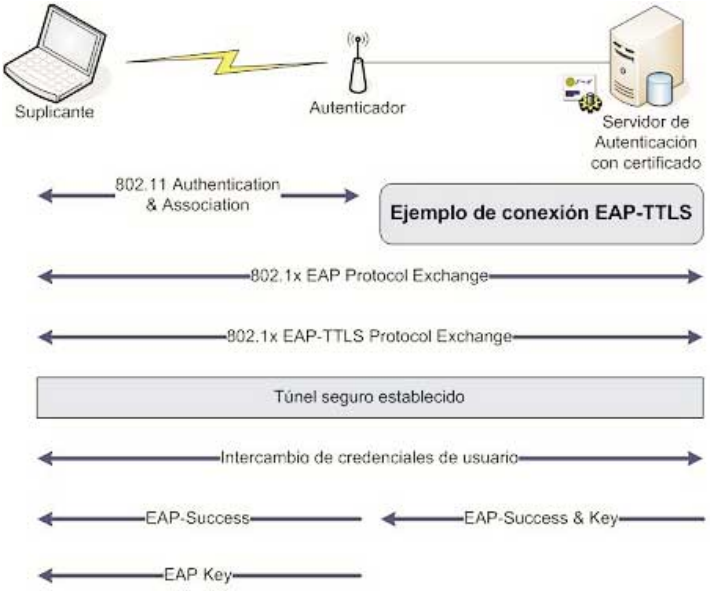

Figura 20 - Ejemplo de conexión EAP-TTLS

EAP-TTLS (EAP-Tunneled-TLS) añade a las características de seguridad de EAP-TLS el establecimiento de un canal de comunicación seguro para el intercambio de las credenciales de usuario. De esta forma se incrementa la seguridad frente a ataques de sniffing que pretendan hacerse con estos datos.

Por otra parte elimina la necesidad de contar con certificados en todos los clientes, que conlleva un proceso de distribución y mantenimiento engorroso y caro.

De esta forma, el proceso de autenticación pasa por una primera fase de asociación del suplicante con el autenticador y una segunda en la que el servidor de autenticación envía su certificado al suplicante que, una vez validado, emplea para crear un túnel de comunicación seguro por donde enviar las credenciales y finalizar la autenticación.

Una vez repasados los diferentes métodos de autenticación que proporcionan las variantes más comunes de EAP vamos a investigar de que manera la incorporación de un servidor RADIUS a nuestro Rogue AP puede ayudarnos a lograr una autenticación completa como usuario legítimo, provocar una denegación de servicio, etc...

Tras montar un Rogue AP con un Rogue RADIUS el atacante puede desasociar a un cliente y cuando este cliente se intente conectar, se asociará al Rogue AP por ofrecer este mayor intensidad de señal. Una vez asociado se repetirá el proceso de autenticación mediante EAP-TLS/TTLS/PEAP pero contra el Rogue RADIUS bajo nuestro control. De esta forma podremos:

- Desasociar usuarios
- Recolectar usuarios y contraseñas
- Recolectar las credenciales de los usuario.
- Suplantar a otros usuarios en la red legítima.

Nota: Aunque hasta el momento hemos comentado las formas de montar un Rogue AP bajo plataformas Linux, es posible montar el mismo sistema en entornos Windows mediante:

- SoftAP
- TreeWalk
- Apache
- ActivePerl
- Airsnarf

Para ello seguir las instrucciones que encontrareis en la página de airsnarf para windows.

A continuación vamos a ver los métodos existentes para atacar diferentes sistemas de autenticación basados en EAP.

Vamos a comenzar por vulnerar un sistema de autenticación basado en EAP-TTLS mediante un Rogue AP con Rogue RADIUS. Veamos el siguiente esquema:

Figura 21 - Ejemplo de ataque contra EAP-TTLS

Como se puede apreciar del estudio del esquema, tras desasociar al cliente el AP legítimo el cliente procede a reasociarse con el AP bajo control del atacante. Se ha de tener en cuenta que para que éste ataque pueda ser llevado a cabo con exito el cliente no ha de estar configurado para validar el certificado del servidor, una situación más habitual de lo que pueda parecer.

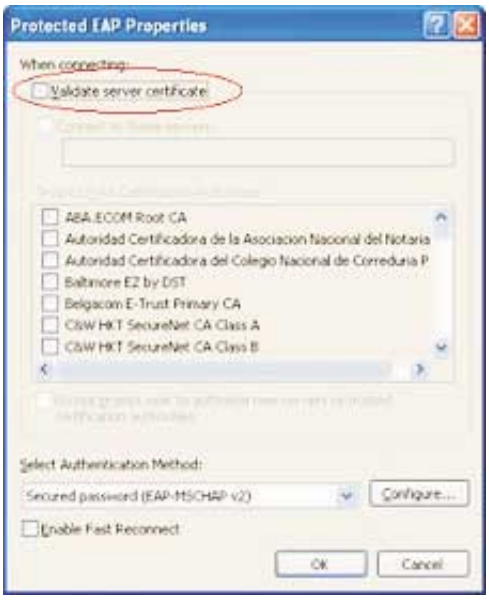

Figura 22 - Ventana de configuración de certificados

De esta manera, una vez creado el túnel, al atacante le llegan las credenciales del cliente. Como hemos visto, mediante esta técnica se pueden reproducir una gran variedad de ataques, incluyendo DoS por desasociación, suplantación de identidad o captura de información sensible.

A continuación vamos a estudiar el método de ataque empleado contra sistemas EAP-TTLS con PAP. Para ello primero explicar que PAP (Password Authentication Protocol) es el sistema de autenticación más simple para redes PPP en el que un usuario y contraseña son validados contra una tabla, generalmente cifrada, almacenada en el servidor de autenticación.
Las credenciales empleadas por este protocolo viajan en texto plano (sin cifrar) lo que permite capturar de forma sencilla el usuario y contraseña del cliente una vez éste ha sido desasociado del autenticador legítimo y se conecta al Rogue AP del atacante, como vemos en el gráfico siguiente:

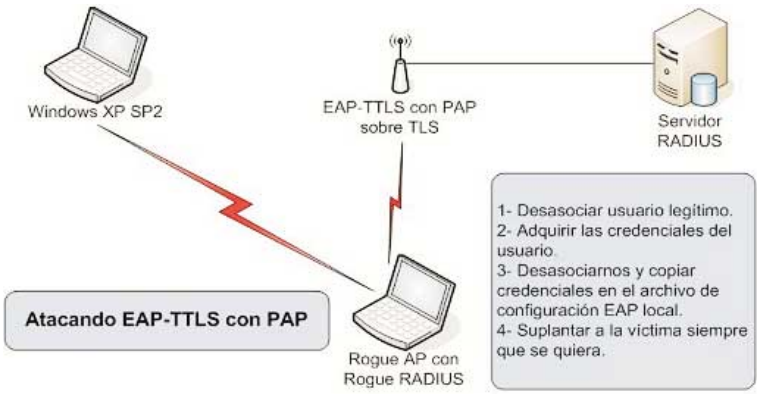

Figura 23 - Ejemplo de ataque contra EAP-TTLS/PAP

El mismo proceso, de forma similar, se puede repetir contra sistemas PEAP pudiendo obtener los dominios del sistema así como usuarios y contraseñas validos.

Para conseguir información ampliada a cerca de este y otros ataque contra EAP consultar las presentaciones de Beetle del grupo Shmoo.

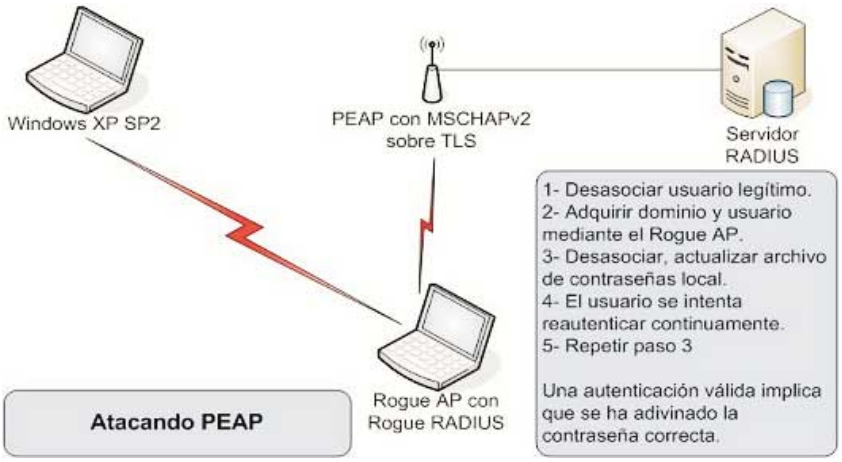

Figura 24 - Ejemplo de Ataque contra PEAP

Defensa frente a Rogue APs

En la tarea de defender nuestros sistemas frente a este tipo de ataques nos encontramos con dos frentes a defender: el cliente y la infraestructura.

Comencemos por el cliente. El peligro al que se enfrenta el usuario de un terminal móvil es la asociación a un Rogue AP de forma voluntaria o no. Es de sobra conocida la habilidad de Windows XP para manejar las conexiones inalambricas por si mismo, y es precisamente esta característica la más apreciada por los atacantes pues el sistema operativo se basa sólo en la intensidad de la señal y el SSID para asociarse a un AP u otro. Es por ello que los terminales así configurados son presa fácil de los Rogue AP.

El grupo shmoo, creador entre otros de airsnarf, ha desarrollado una herramienta que monitoriza la conexión wireless del terminal donde esta instalado para detectar ataques mediante Rogue APs. Para ello vigila:

- Autenticaciones/Desautenticaciones y asociaciones masivas
- Firmas de Rogue APs conocidas
- Aumento repentino de la intensidad de la señal junto a un cambio de AP

Estas técnicas no son definitivas pero aumentan sensiblemente la seguridad frente a este tipo de ataques.

Ahora vamos a ver como podemos intentar defender nuestra infraestructura de los ataques mediante Rogue APs.

Como hemos visto a lo largo del capítulo, casi todos los sistemas de autenticación pueden ser vulnerados de una u otra manera, de forma que la mejor protección frente a este tipo de ataques pasa por la vigilancia constante del sistema tanto por parte del personal encargado de la seguridad como por parte de sistemas de detección adecuadamente instalados.

Comparativa

A continuación se presenta una tabla resumen de las características más destacadas de los protocolos de cifrado empleados en redes inalámbricas.

	WEP	WPA	WPA2
Cifrado	RC4	RC4	AES
Longitud de clave	40 bits	128 bits enc. 64 bits auth.	128 bits
Duración de clave	24-bit IV	48-bit IV	48-bit IV
Integridad de datos	CRC-32	Michael	CCM
Integridad de cabecera	Ninguna	Michael	CCM
Control de claves	Ninguno	EAP	EAP

Se puede apreciar el progresivo endurecimiento de los protocolos de cifrado hasta llegar a WPA2 que por fin cambia RC4 como protocolo para implementar AES; tambien resulta evidente el esfuerzo que se ha hecho en reforzar la integridad de los datagramas tanto a nivel de datos como, posteriormente de cabecera.

Anexo A

Infraestructura de pruebas

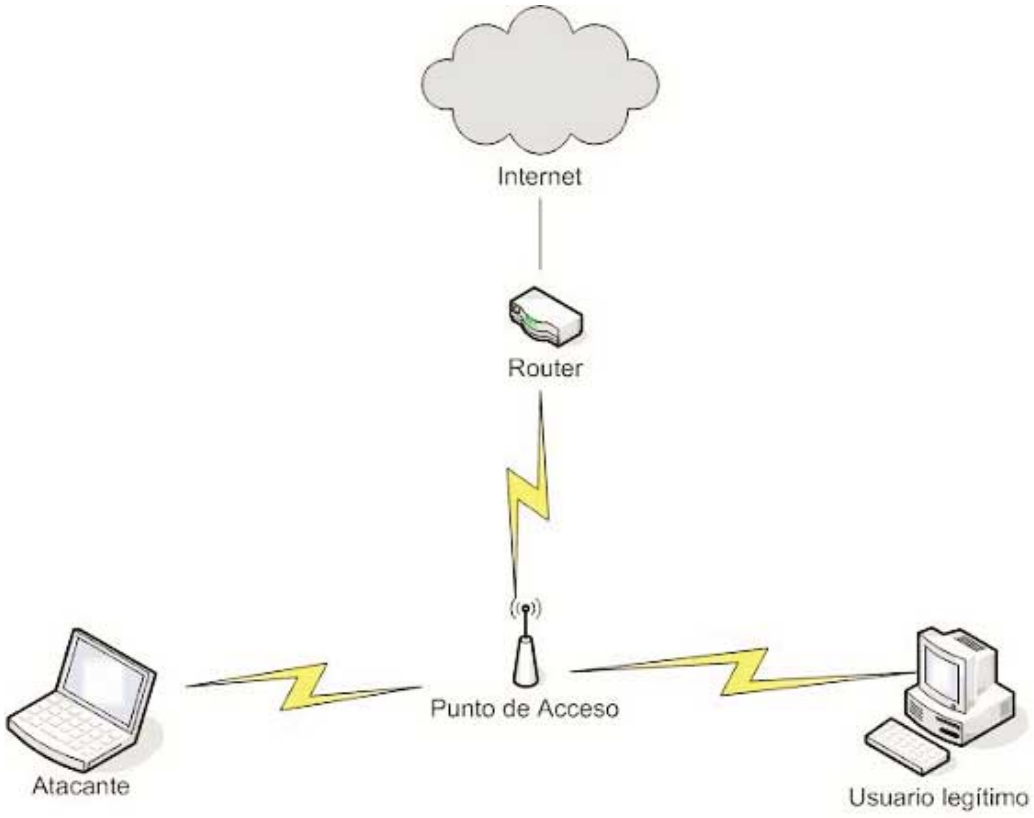

Figura 25 - Red de tipo abierta empleada para las pruebas

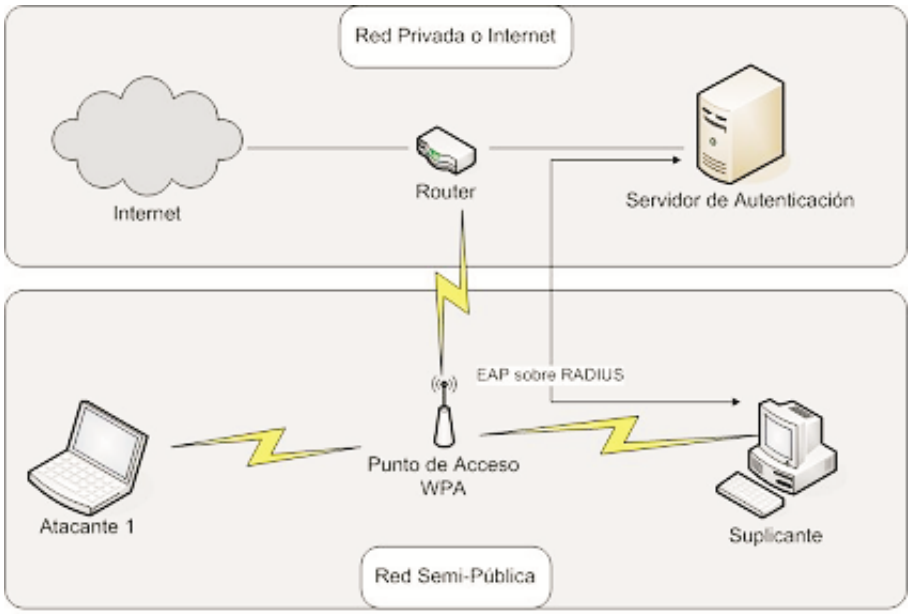

Figura 26 - Red Protegida por WPA empleada en las pruebas

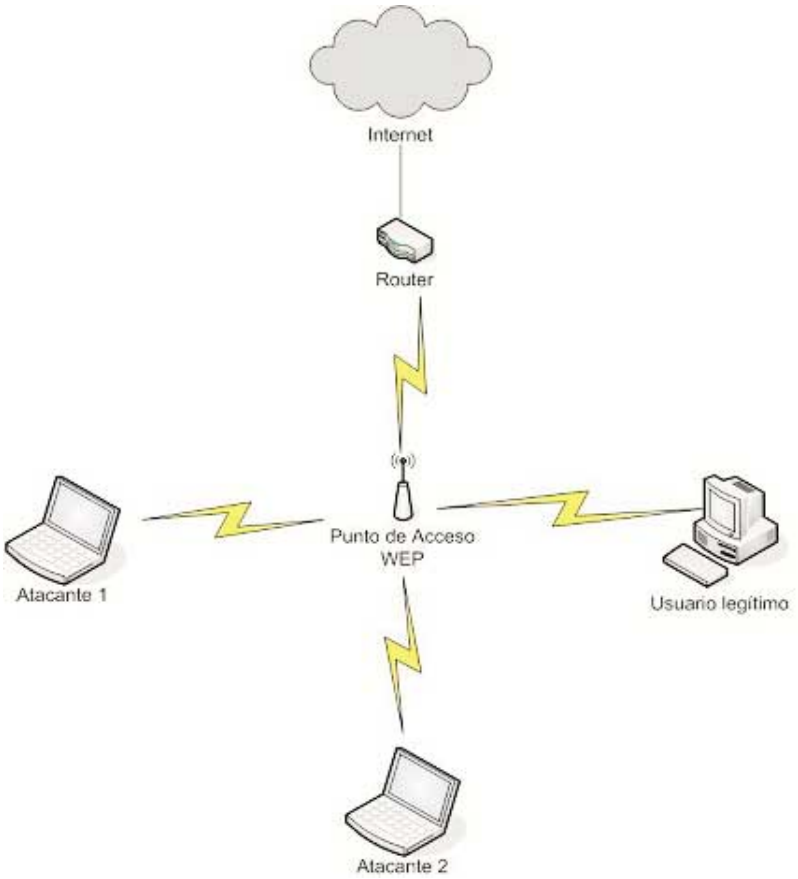

Figura 27 - Red protegida por WEP empleada en las pruebas

Wardriving

Como colofón a las pruebas realizadas, se ha querido comprobar el nivel de concienciación de las empresas y particulares en lo referente a la seguridad de sus redes inalámbricas.

Para ello, se han realizado dos estudios. El primero de ellos, por algunas de las principales calles de una importante ciudad española. El otro, de alcance internacional, por 12 ciudades pertenecientes a un total de 9 países europeos y americanos.

Este tipo de pruebas, que se llevan a cabo mediante un ordenador portátil, una tarjeta inalámbrica y los programas necesarios, se conocen como wardriving, y consisten en buscar y anotar la situación, tanto física como lógica, de las redes inalámbricas presentes en una ciudad.

Estudio 1: calles principales de una ciudad española

En un paseo de aproximadamente media hora, se descubrió y anotó la situación de 79 redes inalámbricas, de las cuales 52 carecían de cualquier tipo de cifrado o autenticación. En cuanto a las redes protegidas (27), solamente 7 tenían implementado algún sistema diferente de WEP como WPA o WPA-PSK.

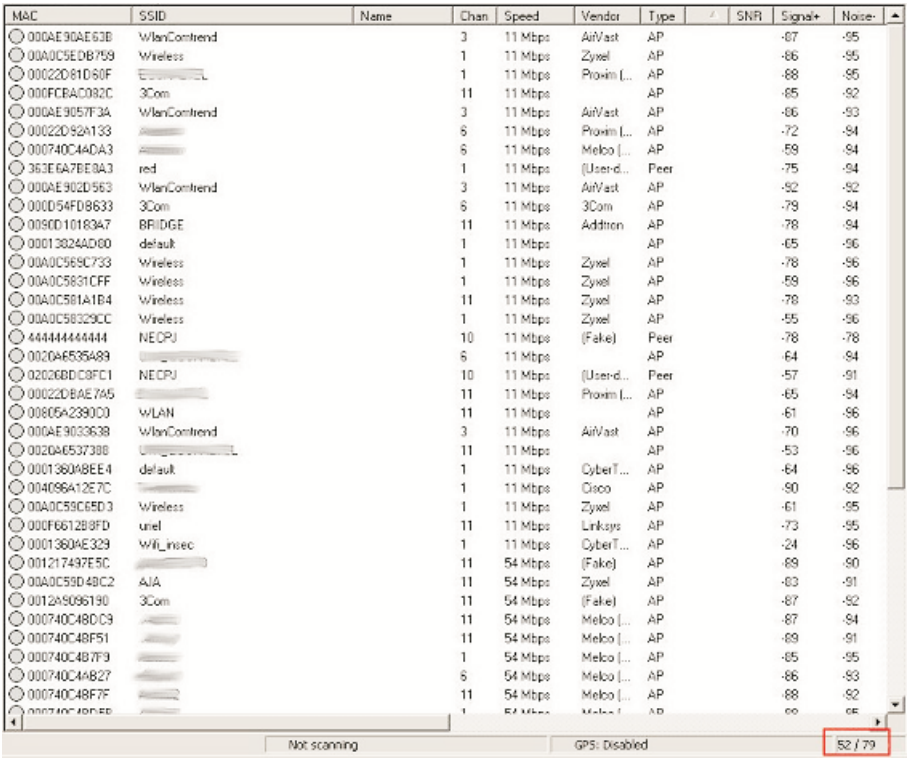

Figura 28 - Redes desprotegidas detectadas

Otra de las sorpresas que deparaba la prueba era el número de APs encontrados con la configuración (aparentemente) de fábrica, cuanto menos en lo referente al ESSID asociado al modelo del AP. Concretamente, 7 de las 79 redes detectadas presentaban esta característica, como se puede observar en la siguiente figura.

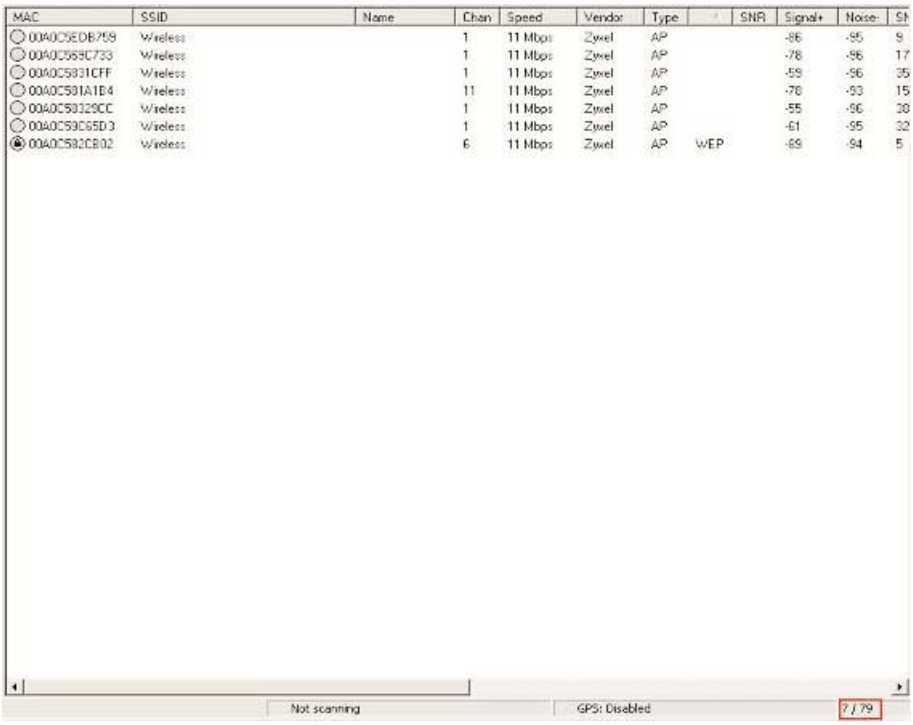

Figura 29 - Captura de las redes con configuración de fábrica

En cuanto a los datos, la mayoría estaban (como cabía esperar) sin cifrar, permitiendo identificar el protocolo y el contenido, así como los datos sensibles que portaban. Si bien es cierto que se capturó gran parte de tráfico DHCP o ARP, hay que destacar la importante presencia de tráfico NetBIOS, POP3 o SMTP y HTTP. Un presunto atacante podría pasar una captura como ésta por algún programa que reconstruyese las sesiones de los diferentes protocolos llegando a recuperar páginas visitadas, imágenes, correos, archivos, y casi cualquier cosa.

Estudio 1: estudio internacional

Las ciudades donde se llevaron a cabo los recorridos fueron:

- Estocolmo, Suecia
- La Paz, Bolivia
- Ciudad de México, México
- Montevideo, Uruguay
- Buenos Aires, Argentina
- Celje, Liubliana y Maribor, Eslovenia
- Ottawa, Canadá
- Lisboa, Portugal
- Madrid y Bilbao, España

Los recorridos se efectuaron a través de zonas de negocios importantes de cada ciudad y durante horas de actividad de negocio. Además, se efectuaron otros recorridos por zonas residenciales con nivel económico medio-alto, para poder recoger los datos de instalaciones WiFi residenciales, no solo de negocios.

Resultados

Los resultados sobre la seguridad de las redes aportaron muchos datos sobre la situación de las redes. En general, la seguridad es pobre, ya que la mitad de las redes no cuentan con sistemas de cifrado adecuados para evitar la intrusión de los usuarios en el sistema inalámbrico. De un total de 905 redes, 374 (41,33%) disponían de algún sistema de cifrado, mientras que un sorprendente 58,37%(531 redes) carecían de cifrado.

El caso se agrava en cuando pensamos en que dentro de las redes sin cifrado alguno también conservan el identificador y el fabricante de la red por defecto el 3,75% de las redes, lo que puede ser indicativo de una configuración también por defecto y una altísima probabilidad de que un ataque contra esas redes tenga éxito.

Por países, la distribución de redes con cifrado activado es la siguiente:
España (19,55%), Bolivia (32,50%), Canadá (36,96%), Uruguay (41,46%), Portugal (44,12%), Argentina (48,75%), Eslovenia (53,85%), Suecia (84,62%), México (100%). Total (41,33%).

NOTA: Los datos de México no deben ser tenidos en cuenta, ya que la muestra recibida era muy reducida, sin significación estadística.

Son destacables el caso de Eslovenia, cuyo nivel de seguridad se encuentra por encima del 50%, y el sorprendente de Suecia, con más del 84% de redes cifradas. En el otro extremo, España aparece como el país con menos conciencia de seguridad, en donde ni siquiera el 20% de las redes inalámbricas se encuentran protegidas por sistemas de cifrado.

Exceptuando los datos de México, muchos países se encuentran por debajo de la media de protección, que ya de por sí es muy baja.

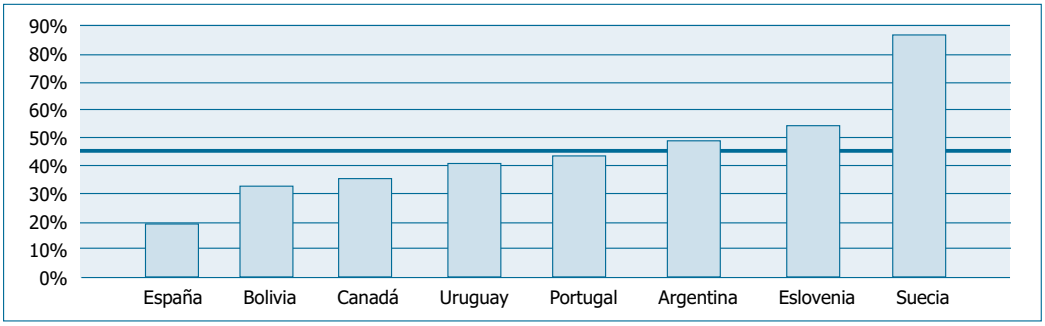

Gráfico 1. - Porcentaje de redes inalámbricas con sistemas de cifrado en función del país.

Cifrado en función del sistema de red inalámbrico

Las redes inalámbricas pueden ser de dos tipos: puntos de acceso o punto a punto. Las primeras permiten el acceso a todos los dispositivos que se encuentren en su radio de alcance, mientras que las segundas únicamente sirven para que dos únicos dispositivos de conecten.

En cualquiera de los dos casos es posible evitar intrusiones con sistemas de cifrado, y la distribución de los cifrados es bien distinta:

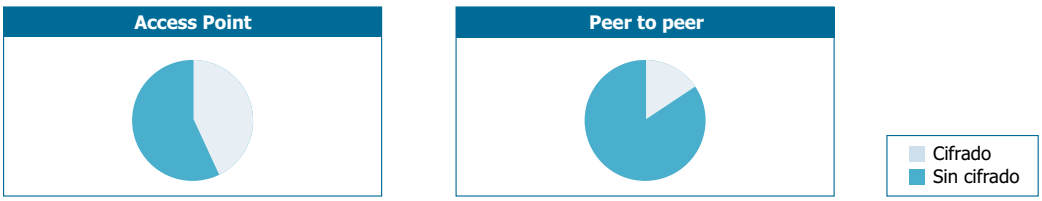

Gráfico 2. - Distribución de sistemas de cifrado en función del tipo de conexión.

	Punto de acceso	Conexión punto a punto
Con cifrado	43,42%	12,90%
Sin Cifrado	56,58%	87,10%

La seguridad en los sistemas Peer to peer es mucho más reducida. Una posible explicación es que mientras que en los puntos de acceso están en muchos casos instalados por los ISP que quizá advierten de los peligros, en el caso de accesos peer to peer (con un porcentaje de sistemas sin cifrado se eleva hasta el 87,10%) son los propios usuarios los que instalan y configuran los sistemas.

El caso extremo

Como anécdota, cabe mencionar que la peor situación posible en un punto de acceso inalámbrico se ha llegado a dar, pero afortunadamente en únicamente tres casos.

En los tres casos, la red inalámbrica estaba sin cifrar, ofreciendo el fabricante del punto de acceso, con el SSID por defecto e incluso mostrando la IP que utilizaba. Y de los tres, uno de ellos llegaba a mostrar el rango de IP que empleaba su DHCP.

Lo peor de los tres casos: estaban todos situados en la misma ciudad, aunque en puntos distintos de la misma.

El futuro

A lo largo de este artículo se han pretendido dejar claras dos situaciones, el gran momento por el que están pasando las redes inalámbricas y las grandes carencias de seguridad que presentan. Juntando estos dos hechos con otro aparentemente no relacionado, como es el de la expansión del malware y, concretamente, los gusanos, se puede llegar a la conclusión de que es sólo cuestión de tiempo que los creadores de malware quieran dotar a sus creaciones de mayores capacidades de propagación propias de este medio.

En la edición del 2004 de la conferencia anual ToorCon sobre seguridad informática el grupo Shmoo, representado por Beetle, presentó un estudio realizado sobre las capacidades de control de conexiones inalámbricas que presenta WMI (Windows Management Instrumentation) y de como, mediante sencillos scripts, se pueden adaptar estas capacidades a malware de todo tipo.

WMI (Windows Management Instrumentation)

Windows Management Instrumentation (WMI) es la respuesta de Microsoft a la propuesta de la WBEM (Web-Based Enterprise Management) para desarrollar una tecnología estándar para acceder a los recursos informáticos en un entorno corporativo. WMI emplea el estándar CIM (Common Information Model) para proporcionar acceso a remoto a los diferentes componentes de la máquina (sistemas, aplicaciones, configuraciones de red, dispositivos, etc...). Mediante la tecnología WMI prácticamente cada pieza de software o hardware puede ser manejada de forma remota.

La idea principal reside en emplear las características que ofrece WMI a la hora de manejar sistemas Windows mediante sencillos scripts para dotar a los gusanos de un mayor control sobre los terminales infectados permitiéndoles, entre otras cosas, escanear en busca de redes inalámbricas, cambiar entre ellas, modificar la configuración de la tarjeta inalámbrica, etc...

Resulta evidente que todas estas características dotarán a estos especimenes de un control sobre los terminales infectados mucho mayor al que poseen actualmente y les permitirá ampliar considerablemente su capacidad de propagación.

A continuación se muestran algunos ejemplos de scripts en vbs (Visual Basic Script) que permiten controlar o monitorizar conexiones inalámbricas. Dos de los scripts aquí mostrados fueron presentados por Beetle del grupo Shmoo en la conferencia Toocon.

SsidScan.vbs permite determinar los ssids que recibe la tarjeta del terminal mediante pocas líneas de código.

```
' SsidScan.vbs
' Beetle <beetle@shmoo.com>
' Simple SSID scanner using VBScript
on error resume next
set objSWbemServices = GetObject("winmgmts:\\.\root\wmi")
set colInstances = objSwbemServices.ExecQuery("SELECT * FROM MSNDis_80211_BSSIList")
for each obj in colInstances
        if left(obj.InstanceName, 4) <> "WAN " and right(obj.InstanceName, 8) <> "Miniport"
then
                for each rawssid in obj.Ndis80211BSSIList
                        ssid = ""
                        for i=0 to ubound(rawssid.Ndis80211SSid)
                                decval = rawssid.Ndis80211Ssid(i)
                                if (decval > 31 AND decval < 127) then
                                        ssid = ssid & Chr(decval)
                                end if
                        next
                        wscript.echo ssid
                next
        end if
next
```

El resultado de ejecutar este script es el que se muestra a continuación.

```
C:\cscript SsidScan.vbs
Microsoft (R) Windows Script Host versión 5.6
Copyright (C) Microsoft Corporation 1996-2001. Reservados todos los derechos.

PandaWiFi
```

WifiLocalSignal.vbs permite controlar los BSSID, SSID y RSSI de una máquina Local con Windows XP mediante WMI:

```
' edit strComputer, save to a dir, open up cmd shell, and type: cscript WiFiLocalSignal.vbs
filename = "WiFiLocalSignal.vbs"
program = "Wi-Fi Local Signal Monitor"
version = "0.1"
description = "BSSID, SSID, and RSSI monitor of local XP machine's Wi-Fi card via WMI."
authorInfo = "Beetle <beetle@shmoo.com>"

strComputer = "." ' THIS computer
set objSWbemServices = GetObject("winmgmts:\\"& strComputer & "\root\wmi")

wscript.echo program & vbcrlf & version & vbcrlf & description & vbcrlf & authorInfo & vbcrlf

' find adapters by querying for active signal
set colInstances = objSwbemServices.ExecQuery _
  ("SELECT * FROM MSNdis_80211_ReceivedSignalStrength WHERE Active = True")
if wscript.Arguments.Count = 0 Then ' spit out usage and cards if no args
    wscript.echo "Usage: cscript " & filename & " [cardno]"
        card_no=1
        for each objInstance in colInstances ' more than one instance per card may show up,
btw
                wscript.echo card_no & " = " & objInstance.InstanceName
                card_no=card_no +1
        next
    wscript.quit
end If

' numberify the arg and set our adapter, matching command arg with an instancename
card_no=abs(wscript.Arguments(0))
x=1
for each objInstance in colInstances
        if x = card_no then
                wifiAdapter = objInstance.InstanceName
                x = x + 1
        end if
next
wscript.echo "Using " & wifiAdapter & vbcrlf


last_signal = 0 ' we need to initialize this, but I'm not sure if -90 would be a better val to
start with

i=1
do while i=1 ' an infinite loop.  duh.

' get bssid
bssid = ""
```

```
set colInstances = objSwbemServices.ExecQuery ("SELECT * FROM
MSNdis_80211_BaseServiceSetIdentifier WHERE Active = True AND InstanceName ='" &
wifiAdapter & "'")
for each objInstance in colInstances
        macbyte = 0
        ' convert decimals to hex.  pad zeros & slip in colons where needed
        for each decval in objInstance.Ndis80211MacAddress
                if decval<17 then
                        bssid = bssid & "0"
                end if
                bssid = bssid & Hex(decval)
                if macbyte < 5 then
                        bssid = bssid & ":"
                        macbyte = macbyte + 1
                end if
        next
next

' get ssid
ssid = ""
set colInstances = objSwbemServices.ExecQuery _
  ("SELECT * FROM MSNdis_80211_ServiceSetIdentifier WHERE Active = True AND InstanceName
='" & wifiAdapter & "'")
for each objInstance in colInstances
        ' convert decimals to chars and avoid non-alphanumerics
        for each decval in objInstance.Ndis80211SsId
                if (decval > 31 AND decval < 127) then
                        ssid = ssid & Chr(decval)
                end if
        next
next

' this could be tricky, as I've read signal strength is reported in different ways per card.  YMMV.
set colInstances = objSwbemServices.ExecQuery _
  ("SELECT * FROM MSNdis_80211_ReceivedSignalStrength WHERE Active = True AND
InstanceName ='" & wifiAdapter & "'")
for each objInstance in colInstances
                        sigraw = objInstance.Ndis80211ReceivedSignalStrength ' raw number for
later comparison
                        signal = sigraw & "dB" ' make it a string that says dB
next

last_signal = sigraw
Wscript.echo "BSSID: " & bssid & "  SSID: " & ssid & "  RSSI: " & signal

wscript.sleep(1000) ' let's rest half a sec between loops instead of blasting WMI.  increase
to 1000?

loop
```

El resultado de ejecutar este script se muestra en la siguiente figura.

```
C:\cscript WifiLocalSignal.vbs
Microsoft (R) Windows Script Host versi¢n 5.6
Copyright (C) Microsoft Corporation 1996-2001. Reservados todos los derechos.

Wi-Fi Local Signal Monitor
0.1
BSSID, SSID, and RSSI monitor of local XP machine's Wi-Fi card via WMI.
Beetle <beetle@shmoo.com>

Usage: cscript WiFiLocalSignal.vbs [cardno]
1 = Conceptronic 54Mbps USB adapter
2 = Conceptronic 54Mbps USB adapter - Minipuerto del administrador de paquetes

C:\cscript WifiLocalSignal.vbs
Microsoft (R) Windows Script Host versi¢n 5.6
Copyright (C) Microsoft Corporation 1996-2001. Reservados todos los derechos.

Wi-Fi Local Signal Monitor
0.1
BSSID, SSID, and RSSI monitor of local XP machine's Wi-Fi card via WMI.
Beetle <beetle@shmoo.com>

Using Conceptronic 54Mbps USB adapter

BSSID: 00:11:20:70:6A:90 SSID: PandaWifi RSSI: -30dB
BSSID: 00:11:20:70:6A:90 SSID: PandaWifi RSSI: -40dB
BSSID: 00:11:20:70:6A:90 SSID: PandaWifi RSSI: -38dB
```

Para crear los siguientes scripts y recalcar la sencillez con la que éstos pueden ser creados se ha empleado la herramienta de Microsoft Scriptomatic, disponible para descarga en la página de esta empresa.

El siguiente script lista las redes disponibles en la ubicación actual.

```
On Error Resume Next

Const wbemFlagReturnImmediately = &h10
Const wbemFlagForwardOnly = &h20

arrComputers = Array("WINPRUEBAS")
For Each strComputer In arrComputers
   WScript.Echo
   WScript.Echo "==========================================="
   WScript.Echo "Terminal: " & strComputer
   WScript.Echo "==========================================="

   Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\WMI")
```

```
Set colItems = objWMIService.ExecQuery("SELECT * FROM MSNdis_80211_BSSIList", "WQL",
_
                                       wbemFlagReturnImmediately + wbemFlagForwardOnly)

  For Each objItem In colItems
    WScript.Echo "Activo: " & objItem.Active
    WScript.Echo "Nombre de tarjeta: " & objItem.InstanceName
    strNdis80211BSSIList = Join(objItem.Ndis80211BSSIList, ",")
      WScript.Echo "Ndis80211BSSIList: " & strNdis80211BSSIList
    WScript.Echo "Numero de redes: " & objItem.NumberOfItems
    WScript.Echo
  Next
Next
```

Y la tabla que mostramos a continuación es un ejemplo de la salida que produce su ejecución:

```
Microsoft (R) Windows Script Host versi¢n 5.6
Copyright (C) Microsoft Corporation 1996-2001. Reservados todos los derechos.


==========================================
Terminal: WINPRUEBAS
==========================================
Activo: Verdadero
Nombre de tarjeta: Conceptronic 54Mbps USB adapter
Ndis80211BSSIList:
Numero de redes: 3
```

Estos ejemplos pretenden demostrar el potencial que demuestra WMI en el control de conexiones inalámbricas e ilustrar el peligro que entrañaría la absorción de este tipo de comandos por parte de los creadores de malware.

Conclusiones

Llegados a este punto vamos a recapacitar a cerca de lo que hemos visto a lo largo del artículo intentando sacar algunas conclusiones generales.

Lo primero que parece llamar la atención de lo visto en el artículo es lo inseguro que ha demostrado ser WEP como sistema de cifrado, frente a lo fiables que se presentan las alternativas como WPA o WPA-PSK. Llegado este momento vamos a romper una lanza en favor de WEP y recordar que fue durante muchos años la única medida eficaz de protección de redes inalámbricas con la que contaban los administradores. Si bien es cierto que la aparición de las primeras vulnerabilidades parece temprana, también es verdad que el rendimiento de estos ataques en los primeros tiempos era ridículo y que muchas veces lo importante no es evitar que la información se filtre, si no evitar que lo haga en un tiempo prudencial.

Una vez aclarado este punto es cierto que este artículo parece una caza de brujas contra WEP y que, a lo largo del mismo, se han ido desmontando una a una todas las protecciones que ofrece WEP, en ocasiones de varias maneras diferentes. La primera conclusión que se puede extraer de este artículo es pues que WEP sólo ofrece una protección virtual que, en el mejor de los casos, retrasa el éxito de una intrusión pero no lo detiene.

Partiendo de este punto se recomienda encarecidamente que, siempre que se pueda, se implante WPA o WPA-PSK como sistema de cifrado pero haciendo hincapié en el hecho de que siempre es mejor tener configurado WEP que mantener la red abierta.

WPA ha demostrado, por ahora, su efectividad y ofrece dos variantes en función de los recursos de los que se disponga. Pese a existir ataques de fuerza bruta contra WPA-PSK, se ha demostrado que es muy difícil conseguir la clave en un tiempo razonable siempre que la clave elegida no sea fácil de deducir. Nunca nos cansaremos de repetir que, por muy bueno que sea un sistema de seguridad, una sola clave débil lo hecha todo a perder.

Por último hemos de mencionar lo preocupantes que son los resultados obtenidos de nuestra pequeña prueba de Wardriving. El número de redes detectadas en un recorrido tan corto refuerza la afirmación de lo rápido que se están implantando las redes inalámbricas; como contrapartida, la proporción de redes desprotegidas o que emplean WEP frente a las protegidas por WPA resulta muy preocupante. Este hecho deja patente lo despreocupadamente que se están montando este tipo de redes y nos obliga a recordar que de nada sirven los mejores sistemas criptográficos o de autenticación si no se emplean.

Wireless Checklist

A continuación se listan una serie de medidas de seguridad que consideramos básicas para poder mantener lo más seguro posible nuestro terminal bajo cualquier circunstancia:

- Cambiar los valores del ESSID, usuarios y contraseñas que trae el AP por defecto. Sustituir el ESSID y las contraseñas por otras más complejas y difíciles de adivinar.
- Deshabilitar o bloquear los Beacon Frames y cualquier mensaje de tipo broadcast que no sea necesario.
- Cifrar las comunicaciones mediante el nivel de cifrado más alto del que se disponga, dando siempre preferencia a WPA frente a WEP, y éste frente a dejar la red abierta.
- Filtrar las conexiones mediante una lista de direcciones MAC o IP blancas. Puede resultar engorroso de realizar y mantener pero amplía el margen de seguridad.
- Deshabilitar la asignación automática de direcciones IP mediante DHCP.
- Cambiar el rango de direcciones IP que trae por defecto el AP.

Mientras que las medidas propuestas pueden prevenir el uso indeseado de nuestra red por parte de terceros no autorizados, no conviene olvidar la seguridad de nuestros propios terminales, para ello es imprescindible disponer de:

- Instalar software Antivirus en el ordenador y, lo más importante de todo, mantenerlo actualizado en todo momento frente a las últimas amenazas.
- Emplear un cortafuegos personal en nuestro terminal, el empleo de un cortafuegos personal es recomendable independientemente de otros elementos de seguridad perimetral que puedan estar instalados.
- Disponer de software de detección de intrusos en el ordenador.
- Si el terminal va ha ser empleado por menores es muy aconsejable implantar un software de control parental para evitar el acceso a contenidos no recomendables.

Bibliografía

How to crack WEP

Parte 1: http://www.tomsnetworking.com/Sections-article118.php
Parte 2: http://www.tomsnetworking.com/Sections-article120-page1.php

WEP dead again

Parte 1: http://www.securityfocus.com/infocus/1814
Parte 2: http://www.securityfocus.com/infocus/1824

Freeradius + EAP-TLS

http://www.dslreports.com/forum/remark,9286052~mode=flat802.1X Port-Based Authentication HOWTO
http://howtos.linux.com/howtos/8021X-HOWTO/

PEAP/TLS + freeradius
http://www.kevan.net/cisco_freeradius_tls_peap_auth.php

WPA, seguidad en redes inalámbricas
http://www.coitt.es/antena/pdf/154/06c_Reportaje_Seguridad.pdf

(In)seguridad en redes 802.11b
http://pof.eslack.org/writings/In-Seguridad en redes 802.11b.pdf

Seguridad en redes Wi-Fi
http://www.e-ghost.deusto.es/docs/SeguridadWiFiInestable2005.pdf

Nuevos protocolos de seguridad en redes Wifi
http://www.e-ghost.deusto.es/docs/2005/conferencias/NuevosProtWiFi.pdf

Weaknesses in the Key Scheduling Algorithm of RC4

http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

WepLab Homapage
http://weplab.sourceforge.net/

Shmoo Group
http://www.shmoo.com
http://airsnarf.shmoo.com

WMI
http://www.shmoocon.org/2005/wifiwmd4win32.sxi

Java y WMI
http://wbemservices.sourceforge.net/
http://wbemservices.sourceforge.net/
http://j-integra.intrinsyc.com/products/com/