Avanzando en la seguridad de las redes WIFI

ENFOQUES

Going forward more Secure WIFI Networks

Rodrigo Castro

Resumen

Actualmente la seguridad se ha convertido en uno de los principales problemas de los sistemas de acceso inalámbrico. Varios elementos han contribuido a ello: el hecho de que se utilice un medio de transmisión compartido sin control de las personas o dispositivos con capacidad de acceso a dicho medio, la rápida implantación de esta tecnología en la sociedad, la novedad de la tecnología empleada, y una política en su desarrollo, que ha primado su expansión y ha dejado de lado aspectos relativos a su seguridad. Hoy en día se está realizando un gran esfuerzo en el desarrollo de estándares y tecnologías que eviten estos problemas de seguridad, manteniendo la filosofía de una conexión móvil.

Palabras clave: accesos inalámbricos, seguridad, conexión móvil.

Summary

Over the last years, security has become one of the main problems in the wireless local area network technologies. The WIFI networks have some specific aspects that make security quite more complex. One aspect of WIFI networks is the use of shared communication media with difficult range control, another aspect is the massive implantation policy based on devices with very simple default configurations with few or even none security measure. Nowadays, there is a big effort to standardize access control methods and encryption technologies in order to solve these security problems.

Keywords: wireless access, security, mobile connection, encryption technologies.

Actualmente se está realizando un gran esfuerzo en el desarrollo de estándares y tecnologías que eviten los problemas de seguridad, manteniendo la filosofía de una conexión móvil

1.- Introducción a la tecnología WIFI

Cuando se habla de tecnología WIFI, realmente se está haciendo referencia a la WI-FI Alliance [1]. Se trata de una organización sin ánimo de lucro, que engloba a un amplio grupo de fabricantes, con el objetivo de promocionar el uso de la tecnología inalámbrica en redes de área local, y asegurando la compatibilidad entre fabricantes en base a los estándares IEEE 802.11 [2]. La expansión de este tipo de tecnología ha sido explosiva y se prevé que en los próximos 1 ó 2 años el 90% de los equipos ya dispongan de dispositivos WIFI. Las ventajas que ha supuesto la tecnología inalámbrica son evidentes: abaratamiento y facilidad de implantación de redes LAN, proliferación de aplicaciones y dispositivos móviles, posibilidad de crear espacios con conectividad de manera inmediata, movilidad de usuarios, etc. A toda esta funcionalidad se le suma el bajo coste de los dispositivos necesarios para su puesta en funcionamiento.

Al hablar de tecnología WIFI, realmente se está haciendo referencia a la WI-FI Alliance, organización que engloba a un grupo de fabricantes, con el objetivo de promocionar el uso de la tecnología inalámbrica

Los estándares 802.11 definen diferentes aspectos relativos al acceso inalámbrico a redes LAN. El estándar 802.11a se refiere a un modo de acceso que alcanza hasta 54 Mbps en el rango de frecuencia de los 5 GHz y con la posibilidad de utilizar 8 canales no solapados. Por otro lado, el estándar 802.11b define un acceso de hasta 11 Mbps en el rango de frecuencia de los 2,5 GHz y con la posibilidad de utilizar 3 canales no solapados. A la vista de estos datos aparece el 802.11a como claro ganador, sin embargo a lo largo de los últimos años ha sido el 802.11b el estándar más generalizado con diferencia. Esto se ha debido a varios factores, entre ellos el rango de cobertura, el consumo de potencia, y el coste de la tecnología implicada. Finalmente aparece en los últimos tiempos el 802.11g como estándar más comúnmente implantado. Permite alcanzar anchos de banda de hasta 54Mbps, con capacidad de utilización de hasta 3 canales no solapados en el rango de los 2,5 GHz. Como se puede observar se ha mejorado ostensiblemente el ancho de banda respecto al estándar 802.11b, aunque se siguen manteniendo la utilización de 3 canales en un rango de frecuencias bastante más saturado que el de los 5GHz, lo que limita en parte su rendimiento respecto al 802.11a. Aún así, por ser compatible con 802.11b, su bajo coste de infraestructura y mejora de alcance, se ha consolidado como el estándar sucesor de éste.

2.- Aspectos relativos a la seguridad

Por las características de la tecnología inalámbrica, ésta posee una serie de puntos débiles [3] y ataques característicos a nivel de seguridad que es importante conocer. Por un lado, de cara a facilitar la rápida generalización de este tipo de tecnología entre los usuarios y evitar en lo posible la carga del soporte, se implantan soluciones con configuraciones de arranque en el que prácticamente todas las medidas de seguridad están deshabilitadas: dispositivos cliente que se activan de manera automática, una WLAN (wireless LAN) operativa, software cliente que detecta y conecta de manera automática con una WLAN, etc. Por otro lado, los límites del medio de transmisión resultan difusos y se extienden más allá de lo que puede, en muchos casos, ser controlado.

Para facilitar la generalización de la tecnología inalámbrica entre los usuarios se implantan soluciones con configuraciones de arranque donde prácticamente todas las medidas de seguridad están deshabilitadas

2.1.- WIFI sin proteger

Existen una serie de ideas generalizadas respecto a la seguridad de los sistemas en general, y perfectamente aplicable a las redes WIFI, que suelen resultar fatales a corto o medio plazo, tales como: "nadie conoce el sistema", o "nadie tiene interés en el sistema", así pues ¿para qué gastar recursos y tiempo en protegerlo?. Por desgracia, la experiencia demuestra que ninguno de ambos razonamientos resulta cierto, y que efectivamente hay más personas de las que en un principio parece que conocen de la existencia de ese sistema, y además, tienen intereses en él. Las consecuencias más comunes de ataques a redes WIFI [4] son:

- Consumo de ancho de banda: Ahora mismo resulta sorprendentemente sencillo conseguir una conexión a una de las muchas redes inalámbricas desprotegidas, y sólo un poco más difícil a alguna de las protegidas con algún tipo de medida mínima. Como consecuencia de este tipo de acceso no autorizado, el ancho de banda de las correspondientes redes WIFI se ve claramente mermado, más aún si éstas son utilizadas como medio de acceso a conexiones de tipo ADSL, cable módem, etc.

- Acceso no autorizado a equipos: En general, las protecciones frente a equipos externos a la red local suelen ser más fuertes que aquellas que se aplican frente a equipos que pertenecen a la misma red local. De ahí, que en el momento que un equipo no autorizado se conecta a la red inalámbrica, los equipos que se encuentran conectados a dicha red y los que se encuentran en la misma LAN, suelen ser muy vulnerables. Las consecuencias de un acceso no autorizado a un equipo, puede provocar: el robo o destrucción de datos almacenados en dicho equipo, el robo de claves y contraseñas de acceso a cuentas bancarias, certificados personales, etc.

El medio de transmisión WIFI es un medio compartido donde cualquier dispositivo al alcance de la señal puede escuchar o interferir en el mensaje de la comunicación

- Responsabilidades legales: Como se ha comentado anteriormente, la instrucción en la red inalámbrica suele hacer mucho más vulnerables a los equipos de esa misma LAN, lo que facilita el acceso no autorizado. A partir de aquí, un equipo atacado puede servir como equipo atacante de sistemas remotos, esto podría dar lugar a responsabilidades legales si se considera que el propietario de la red WIFI o la persona que la ha instalado lo ha hecho de manera descontrolada y sin tener en cuenta ningún tipo de medida de seguridad preventiva.

2.2.- Límites difusos

El medio de transmisión WIFI es un medio compartido en el cual cualquier dispositivo que se encuentre en el alcance de la señal puede escuchar o interferir en el mensaje de la comunicación. Además, en el caso de la tecnología WIFI el coste de los elementos hardware necesarios para poder captar o interferir en las comunicaciones es realmente bajo, y cualquiera puede tener acceso a ellos. Todo esto ha hecho que el ámbito de la red local se haya deslocalizado respecto al recinto donde da

servicio y que las medidas de seguridad encaminadas al control de acceso a recintos, salas, edificios, hogares resulten ineficientes de cara a proteger la red local. El problema de gestión del espacio de cobertura de la red WIFI se ve agravado en ocasiones con la instalación de puntos de acceso no autorizados, es decir, sin el control de la organización. Estos puntos no controlados son potenciales entradas a la LAN de la organización, y habitualmente no están configurados con las medidas de seguridad mínimas, ya que normalmente se instalan como una solución rápida, fácil y barata a un problema de conectividad sin tener en cuenta las medidas de seguridad mínimas a adoptar.

Una de las medidas que permite definir en cierto modo el ámbito de cobertura, y por tanto paliar el problema de la indefinición de límites de una red wireless, consiste en realizar su diseño teniendo en cuenta aspectos relacionados con las antenas utilizadas [5], tales como: sus diagramas de radiación (ya sean antenas direccionales u omnidireccionales), su potencia de emisión, y por supuesto su ubicación. Otra medida adicional, consiste en el uso de pinturas especiales que producen un efecto "jaula de Faraday" y evitan la fuga y entrada de señal al recinto. Finalmente, se pueden encontrar en el mercado soluciones basadas en sensores [6], que situados en puntos estratégicos del espacio WIFI a proteger y conectados a un servidor de control, son capaces de establecer un perímetro virtual e identificar y controlar el acceso, tanto a dispositivos conectándose desde fuera del perímetro, como a dispositivos no controlados en el interior del mismo. Esta última solución se basa en la localización de la fuente de radio mediante triangulación de las señales recibidas en los sensores, y su comparación con los perímetros definidos en el servidor de control. Hay versiones mucho más sencillas que consisten en un dispositivo de mano capaz de escanear y guiar hasta emisores no autorizados.

Una de las amenazas más comunes en redes WIFI consiste en la conexión a puntos de acceso piratas

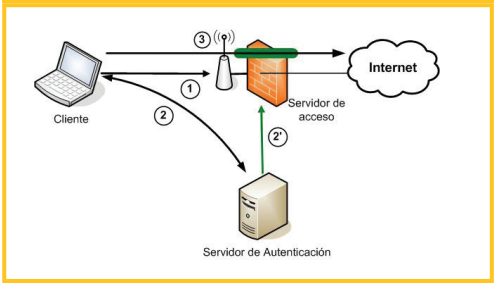
2.3.- Puntos de acceso fantasma

Una de las amenazas más comunes en redes WIFI consiste en la conexión a puntos de acceso piratas [7], es decir, dispositivos que se hacen pasar por puntos "legales". En general se implementan con un simple ordenador con una tarjeta WIFI en modo "master" capaz de actuar como un punto de acceso a todos los niveles. A partir de aquí, todo el tráfico de los equipos que se conecten pasará por él, pudiendo tanto realizar ataques "man in the middle" como accesos no autorizados al equipo conectado.

Existen dos modos comúnmente utilizados para captar clientes que se conecten al punto pirata. El primero se trata, tal y como se muestra en la figura 1, de poner este punto abierto a todo el mundo, sin ningún tipo protección. A partir de aquí, bien un cliente WIFI configurado de tal manera que conecta automáticamente a una WLAN abierta, o bien un usuario que ve la red abierta y la utiliza para su conexión a Internet. El otro modo de conseguir la conexión de un equipo cliente, comienza enviando una trama DEAUTH para que el equipo cliente se desconecte del punto de acceso actual e intente buscar otro. Sólo queda esperar que se conecte al falso y hacer que éste funcione como puente entre el equipo cliente y el punto de acceso auténtico, pero eso sí, controlando todo el tráfico que pasa a través.

Existen dos modos utilizados para captar clientes que se conecten al punto pirata:
- poniendo este punto abierto a todo el mundo
- enviando una trama DEAUTH para que el equipo cliente se desconecte del punto de acceso actual e intente buscar otro

FIGURA 1



3.- Encriptación

3.1.- WEP

Este esquema de encriptación [8] fue incluido en el estándar 802.11 y desde entonces ha sido ampliamente criticado, debido a sus más que demostradas debilidades. Está basado en clave

simétrica, por lo que tanto el cliente como la estación base deben conocer la clave a utilizar. El tamaño de ésta puede ser de 40 ó 104 bits, y se completa con un vector de inicialización de 24 bits. Precisamente, este corto vector ha sido uno de los principales puntos débiles de este esquema. La encriptación se basa en el algoritmo RC4, y utiliza un algoritmo de integridad CRC32 que genera un ICV (Integrity Check Value) independiente de la clave utilizada, lo que también ha ocasionado vulnerabilidades a nivel de seguridad. Se han publicado diversos artículos sobre cómo romper el esquema de encriptación WEP, entre ellos (http://www.uninett.no/wlan/download/wep_attack.pdf)

3.2.- TKIP

Las características de medio compartido y accesibilidad de las redes WIFI hacen del sistema de control de acceso una pieza fundamental de los sistemas WLAN

Este esquema de encriptación surge como alternativa al WEP intentando solucionar sus problemas de seguridad. Uno de los requisitos principales de este nuevo esquema era que pudiera funcionar en el mismo hardware que el antiguo WEP, con una simple actualización del firmware. TKIP también utiliza un algoritmo de encriptación RC4, lo que implica nuevamente clave simétrica compartida entre el cliente y la estación base. En este caso las claves utilizadas (llamadas Temporal Key) son de 128 bits, que son actualizables cada cierto número de paquetes, y el vector de inicialización es de 48 bits, el cual es reiniciado a 0 cada vez que se fija una nueva clave temporal. Para la encriptación se pueden utilizar unas claves derivadas de la TK, llamadas PPK (Per-Packet Key) que son generadas de manera dinámica por cada paquete enviado. Para la integridad de la información, TKIP utiliza MIC (algoritmo de Michael) que introduce un valor de 8 bytes antes del CRC. Este valor es encriptado utilizando una combinación de la información enviada, el vector de inicialización, la dirección origen y destino.

3.3.- CCMP

CCMP (*Counter Mode with CBC-MAC Protocol)* es un esquema de encriptación que utiliza AES (Advanced Encryption Standard), uno de los algoritmos de clave simétrica más seguros en la actualidad. En el caso de redes WIFI este esquema se integra en el estándar WPA2, y utiliza claves de 128 bits, vector de inicialización de 48 bits y chequeo de integridad. Este esquema de encriptación hace necesario el cambio de hardware para su uso, por lo que no mantiene la compatibilidad con esquemas de anteriores, como ocurría con el TKIP.

El método de control de acceso mediante filtrado por MAC está muy extendido por su facilidad de configuración. Se basa en realizar dicho control mediante la comprobación de la dirección MAC de nivel 2 o nivel de trama

4.- Métodos de control de acceso

Las características de medio compartido y accesibilidad de las redes WIFI hacen del sistema de control de acceso una pieza fundamental de los sistemas WLAN, aunque muchas veces por facilidad de instalación, por evitar problemas de gestión o bien por evitar tener que dar un soporte extra a los usuarios, se instalan puntos de acceso WIFI sin ningún método de autenticación. Los objetivos principales de estos métodos son: máxima efectividad en el control de acceso a la WIFI, seguridad de cara a la transmisión de credenciales de los usuarios, y por último sencillez y facilidad de uso.

4.1.- Filtrado por MAC

Este método de control de acceso está muy extendido por su facilidad de configuración. Se basa en realizar dicho control mediante la comprobación de la dirección MAC de nivel 2 o nivel de trama. Su implantación es muy sencilla, ya que sólo se necesita declarar, bien en el punto de acceso, bien en un servidor aparte, las direcciones MAC que están autorizadas para conectarse a la WLAN. Esta dirección MAC debe ser única para cada uno de los dispositivos conectados a la LAN y viene predefinida de fábrica para todos ellos.

Este sistema de autenticación tiene varios problemas. EL primero es que si los usuarios no son fijos o hay usuarios itinerantes, hay que estar dando de alta y de baja direcciones con la siguiente carga de gestión y el consiguiente peligro de dejar alguna entrada a la lista "olvidada". Otro de los problemas es lo fácil que resulta cambiar la dirección MAC de un dispositivo, lo que hace que resulte muy sencillo sustituirla por una válida, y por tanto, que este método de autenticación resulte muy vulnerable. El método de ataque consiste en escuchar el tráfico que pasa por la WLAN y guardar direcciones MAC válidas, para que en el momento que alguna de ellas quede libre, sustituir ésta por la dirección MAC del dispositivo cliente. De todo esto se deduce inmediatamente que este método de autenticación resulta claramente ineficiente.

4.2.- Clave WEP compartida

Es otro de los métodos más comúnmente utilizado hoy en día y consiste en utilizar una clave WEP en la red WIFI que sólo conocen los clientes autorizados. Efectivamente, es un método que reduce la carga de gestión respecto al método anterior, no hay que tocar la configuración cada vez que hay un cliente nuevo, sino que basta con darle la clave a utilizar. Esta facilidad introduce una clara debilidad y es que muchos clientes llegan a conocer la clave WEP, incluso clientes itinerantes que alguna vez necesitaron conexión y se les proporcionó la clave WEP y nunca más se cambió, ya que cada vez que ésta se actualiza hay que avisar a todos los clientes de que hay una clave nueva y que tienen que cambiarla. Además de todo lo dicho hasta ahora, existe otra vulnerabilidad para este método de autenticación relacionada con el esquema de encriptación utilizado, que es totalmente inseguro.

El sistema de control de acceso a través de un portal web necesita un servidor que realice el control de la conexión al exterior

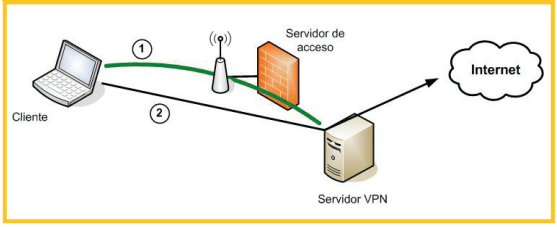
4.3.- Portal WEB

En primer lugar hay que aclarar que este sistema de control de acceso necesita un servidor que realice el control de la conexión al exterior (ver figura 2). Con este método de autenticación, el cliente consigue conectarse a la WIFI sin problemas, e incluso se le asigna una IP, pero sin capacidad de comunicarse fuera del entorno que se haya previamente definido. Cuando el cliente intenta establecer comunicación con una página web externa, automáticamente es redirigido a un portal web en el cual puede autenticarse. Una vez hecho, ya sea con un simple usuario/clave o previo pago de una tarjeta de conexión o incluso con una tarjeta de crédito, el usuario consigue conectividad a Internet durante el tiempo establecido. Para poder mantener la sesión viva, el cliente tiene que mantener una ventana del navegador "popup" abierta que se encarga de comunicar automáticamente y cada cierto tiempo con el portal de acceso, garantizando que la conexión siga abierta.

Existen numerosos ejemplos de este tipo de sistema a través de portal web que ahora mismo está operando en todo el mundo. Su utilización más habitual corresponde con accesos WIFI en espacios públicos "hotspots".

Existen numerosos ejemplos de este tipo de sistema que ahora mismo está operando en todo el mundo. Su utilización más habitual corresponde con accesos WIFI en espacios públicos "hotspots". Esto se debe a que el navegador es una herramienta muy extendida, la mayoría de dispositivos con acceso WIFI tienen un navegador, y su utilización resulta muy natural para los usuarios, permitiendo así mismo el pago del servicio (conexión a Internet) de una manera fácil.

FIGURA 2



A nivel técnico, existen diversos ejemplos de implementación. Quizá el más extendido sea "NoCat" (http://nocat.net/). Se trata de una implementación en software abierto que permite la implantación de un sistema de acceso vía web en un sistema Linux con Iptables. La arquitectura del sistema está formada por los punto de acceso, un

sistema de acceso que controla las conexiones al exterior, y un portal web para poder autenticar a los usuarios. Este portal puede estar situado en la misma máquina que controla las conexiones o puede instalarse en un servidor web aparte. En todos los sistemas en los que hay una fase de comprobación de credenciales (acceso vía web, EAP-TTLS,...) hay un servidor de autenticación que bien chequea dichas credenciales contra alguna base centralizada de usuarios o bien delega la autenticación a un segundo mecanismo con chequeo de credenciales (por ejemplo un servidor POP de correo).

Como desventajas de este sistema de autenticación, destacar que la comunicación va en claro (sin ningún tipo de encriptación) por lo que es susceptible de ser escuchada por cualquier estación en el alcance de la WIFI, de ahí que se recomiende el complementar este sistema de acceso con algún sistema que asegure el contenido de la comunicación: VPNs, SSH, HTTPS, etc.

Otro modo de control de acceso se basa en la existencia de un servidor VPN que sirve de único punto de conexión al exterior desde la red WIFI

4.4.- Acceso VPN

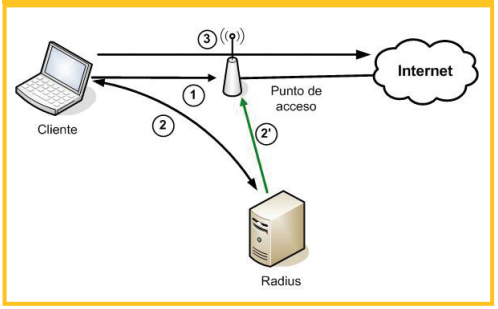
Como se muestra en la figura 3, este modo de control de acceso se basa en la existencia de un servidor VPN que sirve de único punto de conexión al exterior desde la red WIFI. Cuando un usuario se conecta a la WLAN, sólo se le permite el acceso al servidor VPN, lo que le obligará a autenticarse para poder conectarse a Internet. Con este sistema de acceso, se asegura la confidencialidad de las comunicaciones en base al protocolo seguro utilizado por la VPN (IPsec, SSL,...) y se habilita los métodos de autenticación que el servidor VPN soporta.

4.5.- 802.1X

Es un estándar de control de acceso a nivel de acceso al medio (nivel 2), con lo que a diferencia de otros sistemas, como por ejemplo el del portal web anteriormente comentado, en este caso el cliente no tiene una conexión efectiva con acceso al medio hasta que no se haya autenticado satisfactoriamente. EAP (Extensible Authentication Protocol) es un componente fundamental del estándar 802.1X, y surgió como mejora del método de autenticación empleado en PPP (Point to Point Protocol), y que sirve de base sobre la que implementar diferentes modos de paso de credenciales (normalmente usuario/password), tales como: PAP, MS-CHAP, MD5, etc., lo que le ha dado gran flexibilidad y se ha convertido en uno de los aspectos a los que debe gran parte de su éxito. Dentro del 802.1X se define la encapsulación de EAP en tramas Ethernet sobre una LAN, llamado EAPOL (EAP over LAN).

802.1X es un estándar de control de acceso a nivel 2, que a diferencia de otros sistemas, en este caso el cliente no tiene una conexión efectiva con acceso al medio hasta que no se haya autenticado satisfactoriamente

FIGURA 3

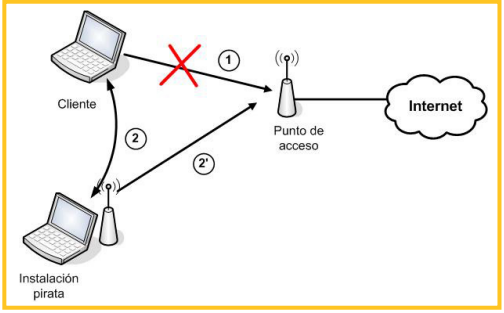


En el protocolo EAP, como se muestra en la figura 4, intervienen tres tipos de elementos: el cliente que solicita acceso, el autenticador que sirve de enlace entre el cliente y el servidor de autenticación –que en el caso de redes WIFI es el punto de acceso– y el servidor de autenticación que es el que realiza la comprobación de credenciales que en nuestro caso se trata de un servidor Radius.

El protocolo funciona de la siguiente forma: el cliente solicita conexión al punto de acceso que filtra todo el tráfico menos el correspondiente al protocolo EAPOL. El punto de acceso se percata de que hay un nuevo cliente pidiendo acceso y le envía una solicitud de identificación. Éste le responde con el identificador, que es directamente reenviado al servidor Radius junto con una solicitud de acceso. El servidor lo utiliza para comenzar la fase de autenticación con el cliente (el punto de acceso hace de

mero intermediario), enviándole una solicitud de credenciales. El cliente le responde con las correspondientes credenciales (dependiendo del tipo de autenticación elegido) y finalmente, el servidor Radius las chequea devolviendo un "accept" o "error" dependiendo de si todo es correcto autorizando el acceso o no, y el punto de acceso en consecuencia abrirá o no la conexión al cliente.

FIGURA 4



En EAP los mensajes son trasmitidos en claro, además de no requerirse ningún tipo de autenticación por parte del servidor ni del cliente, lo que supone una clara vulnerabilidad a nivel de seguridad (más aún en entornos wireless). Como mejoras al protocolo, se han incluido variantes que crean canales seguros entre el cliente y el servidor de autenticación: EAP-TLS, EAP-PEAP, y EAP-TTLS. EAP-TLS se trata de una variante de EAP en la cual se realiza una negociación SSL con autenticación basada en certificado, tanto por parte del cliente como del servidor. Tanto en el caso de EAP-PEAP como de EAP-TTLS, la conexión segura se realiza a partir exclusivamente del certificado del servidor (sería el equivalente a HTTPS en web). En el caso de TLS, las credenciales corresponden al certificado de cliente, mientras que en el de PEAP y TTLS éstas son comunicadas utilizando uno de los métodos ya comentados: MS-CHAP, PAP, etc. A nivel de usuario, en el primer caso (TLS) basta con tener el certificado de cliente instalado, mientras que en los otros (PEAP y TTLS) tendría que proporcionar las credenciales, por lo general un usuario/password.

En EAP los mensajes son trasmitidos en claro, además de no requerirse ningún tipo de autenticación por parte del servidor ni del cliente, lo que supone una clara vulnerabilidad a nivel de seguridad

Otra de las ventajas que incluye 802.1X es la posibilidad de generar, de manera dinámica y en la fase de autenticación, las claves que permitirán una conexión segura entre cliente y punto de acceso. Es decir, el servidor de autenticación genera una clave que es distribuida de manera segura al cliente y al punto de acceso, para que utilizando el esquema de encriptación convenido, cifren toda la comunicación hasta el cierre de la sesión. Esto hace que no haya una única clave que tenga que ser conocida por todos los clientes que acceden a la WIFI, sino que se genera y distribuye de manera automática en el momento de la autenticación.

5.- Estándares

Los grupos más importantes en el desarrollo de estándares para la seguridad en redes wireless son el IEEE, el IETF (Internet Engineering Task Force) y la WI-FI Alliance (Wireless Fidelity Alliance). Los dos primeros son grupos consagrados en el desarrollo de estándares y el último es la unión de un grupo de empresas interesadas en el desarrollo de la tecnología inalámbrica y la interoperatividad de los productos de diferentes empresas.

Los grupos más importantes en el desarrollo de estándares para la seguridad en redes wireless son el IEEE, el IETF

5.1.- IEEE 802.11

Uno de los primeros estándares, en el cual no hay mucho que destacar a nivel de seguridad. Se introdujo el esquema de encriptación WEP, que con el tiempo se ha demostrado ineficiente.

5.2.- WPA

El estándar WPA (Wi-Fi Protected Access) [9] surge como anticipo del, entonces en desarrollo, estándar IEEE 802.11i, para paliar los graves problemas de seguridad surgidos del esquema de

encriptación WEP. El principal hándicap en su desarrollo era que todas las medidas contempladas deberían ser compatibles con la mayoría de las tarjetas y puntos de acceso ya vendidos.

A grandes rasgos WPA incrementa el tamaño de las claves y el número en uso e introduce un nuevo mensaje de control de integridad más seguro. Concretamente WPA contempla:

- IEEE 802.1X como estándar de control de acceso. Maneja dos opciones para su implantación: el modo "personal" que considera el uso de una clave compartida como método de autenticación para evitar el tener que instalar un servidor Radius, y el modo "enterprise" basado en el uso de un Radius como servidor de autenticación.

- TKIP como esquema de encriptación con claves de 128 bits y vector de inicialización de 48 bits, además de contemplar un sistema para la asignación dinámica de claves y rotación de las mismas. Cara al control de integridad incorpora el algoritmo MIC.

El estándar WPA incrementa el tamaño de las claves y el número en uso e introduce un nuevo mensaje de control de integridad más seguro

5.3.- IEEE 802.11i - WPA2

El estándar WPA2 de la WIFI Alliance consiste en una mejora del WPA, cambiando el esquema de encriptación a AES-CCMP. El algoritmo de encriptación AES resulta muy interesante, ya que ha sido adoptado como estándar de privacidad por el National Institute of Standards and Technology (NIST), para el gobierno de EEUU. En este caso la WIFI Alliance vuelve a adelantarse al IEEE sacando un estándar muy parecido al tan esperado 802.11i, en previsión de que se alargue la aprobación de éste. En aspectos relativos a la seguridad son prácticamente idénticos.

6.- Herramientas básicas

Existe un conjunto de herramientas que permiten desde detectar los puntos de acceso disponibles hasta inyectar tráfico falso en medio de las comunicaciones encriptadas, pasando por la ruptura del cifrado de las comunicaciones

Existe un conjunto de herramientas [10] para diversas plataformas que permiten desde detectar los puntos de acceso que hay disponibles en un lugar determinado, hasta inyectar tráfico falso en medio de las comunicaciones encriptadas, pasando por la ruptura del cifrado de las comunicaciones dentro del rango del dispositivo portador de la herramienta. Todo este conjunto de herramientas sirven para dar una idea al administrador de lo fuerte o débil que resultan sus instalaciones WIFI a nivel de seguridad. Es decir, son la base para auditar a nivel de seguridad dichas instalaciones.

6.1.- Detectores de puntos de acceso

Este tipo de herramientas se encarga de observar el tráfico correspondiente a redes WIFI dentro de su alcance y generar cierto tráfico, al cual, los puntos de acceso dentro de su alcance responden, y por tanto, quedan a la vista. También permiten conocer los SSIDs de las redes WIFI de su entorno, incluso si no están siendo publicados en modo broadcast. Suelen ser muy utilizados para detectar puntos de acceso y posteriormente comprobar si están "abiertos" o se pueden abrir, dentro de una población o un recorrido. A esta práctica se la llama wardriving.

- Airfart: http://airfart.sourceforge.net/
- AP Radar: http://apradar.sourceforge.net/
- APTools: http://winfingerprint.sourceforge.net/aptools.php
- ClassicStumbler: http://www.alksoft.com/classicstumbler.html
- iStumbler: http://www.istumbler.net/

- NetChaser: http://www.bitsnbolts.com/netchaser.html
- NetStumbler - MiniStumbler: http://www.stumbler.net/
- PrismSumbler: http://prismstumbler.sourceforge.net/
- Wardrive CD.iso: http://www.wardrivers.be/files/software/wardrivecd/
- WiFiFoFum : http://www.aspecto-software.com/WiFiFoFum/

6.2.- Sniffers

Estas herramientas leen el tráfico de las redes WIFI que se encuentran en su alcance y permiten almacenarlo en ficheros para su posterior procesamiento. Además, en muchos casos, permiten relacionar los diferentes paquetes leídos y clasificarlos por conversaciones, protocolos, paso de claves, etc. En otros casos, los ficheros generados son compatibles con herramientas que realizan este análisis.

Los sniffers son un tipo de herramientas que lee el tráfico de las redes WIFI que se encuentran en su alcance y permiten almacenarlo en ficheros para su posterior procesamiento

- Kismet: http://www.kismetwireless.net/
- Mognet: http://www.node99.org/projects/mognet/
- SSIDsniff: http://www.bastard.net/%7Ekos/wifi/

6.3.- Crackers

Se utilizan para romper el cifrado utilizado en una red WIFI. Para ello se alimentan, bien de tráfico que escuchan directamente y corresponde a las comunicaciones de esa WLAN o de ficheros proporcionados por sniffers que anteriormente han escuchado dichas comunicaciones. Para la ruptura del cifrado, en algunos casos, estas herramientas utilizan técnicas derivadas de vulnerabilidades en la encriptación bien conocidas, como por ejemplo en el caso del cifrado WEP, mientras que en otros casos, prueban con claves derivadas de combinaciones de palabras de diccionarios o estructuras comúnmente utilizadas a la hora de establecer claves. Finalmente, y como última opción, estas herramientas permiten la búsqueda de la clave por la fuerza bruta, es decir, probando todas las combinaciones posibles.

- AirCrack: http://www.cr0.net:8040/code/network/aircrack/
- AirSnort: http://airsnort.shmoo.com/
- AirTraf: http://www.elixar.com/corporate/history/airtraf-1.0/
- Anwrap: http://www.securiteam.com/tools/6O00P2060I.html
- Asleap: http://asleap.sourceforge.net/
- WepCrack: http://sourceforge.net/projects/wepcrack/
- WepLab: http://sourceforge.net/projects/weplab
- WPACracker: http://www.tinypeap.com/html/wpa_cracker.html

Las características de las redes WIFI hace que sean muy sensibles a la seguridad. Hay que evaluar aspectos relativos a los límites de la WLAN evitando los puntos de acceso no autorizados

7.- Conclusiones

Las características de las redes WIFI hace que sean un elemento muy sensible a la seguridad. Hay que evaluar aspectos relativos a los límites de la WLAN, tanto desde el punto de vista de la cobertura de la señal, como del control de los dispositivos en dicho entorno, evitando los puntos de acceso no autorizados. Así mismo hay que tener en cuenta los avances en los estándares que mejoran la seguridad de estas instalaciones, y por supuesto, educar a los usuarios en prácticas que les ahorren disgustos como por ejemplo, no habilitar una tarjeta en modo ad-hoc, o no dejar configurado el cliente WIFI para que se conecte a cualquier WLAN abierta. Como medidas generales a tener en cuenta en una instalación WIFI debemos señalar:

- Activar el filtrado por MAC
- Deshabilitar la publicación del SSID
- Habilitar un sistema de control de acceso 802.1X, bien mediante un servidor Radius o mediante clave compartida (para instalaciones pequeñas).
- Habilitar la generación dinámica de la clave compartida
- Habilitar la rotación de claves
- Utilizar un esquema de encriptación seguro (no utilizar WEP).

Por supuesto todo este conjunto de medidas está condicionado a los requisitos particulares del sistema, pero las nuevas instalaciones deben ser, al menos, compatibles WPA.

A pesar de todo la carrera de las tecnologías inalámbricas es imparable ya que ofrecen un sin fin de ventajas por su flexibilidad de instalación y uso

A pesar de todo lo expuesto en este artículo, la carrera de las tecnologías inalámbricas es imparable ya que ofrecen un sin fin de ventajas por su flexibilidad de instalación y uso.

Rodrigo Castro
(rodrigo.castro@rediris.es)
Área de Middleware
RedIRIS

Referencias

[1] WI-FI Alliance. Consultado en: http://www.wi-fi.org/. Jun. 2005

[2] CISCO. "Capacity Coverage & Deployment Considerations for IEEE 802.11g". Consultado en: http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_white_paper09186a00801d61a3.shtml. Jun. 2005

[3] Andrew A. Vladimirov; Konstantin V. Gavrilenko. "Hacking Wireless – Seguridad de Redes Inalámbricas". Anaya Multimedia (2005). ISBN:84-415-1789-4

[4] Livingston, Brian . "Windows Secrets Newsletter" . "Wi-Finally: wireless security that actually works". Issue 54. 26/05/2005.
Consutado en: http://www.windowssecrets.com/ comp/050526/#story1 Jun. 2005

[5] Garaizar, Pablo. "Seguridad en redes inalámbricas".
Consultado en: http://www.e-ghost.deusto.es/docs/SeguridadWiFiInestable2005.pdf. Jun. 2005

[6] Newbury Networks. "The Power of Location-Based WALN Security & Managment".
Consultado en: http://www.newburynetworks.com/products/whitepapers.php. Jun. 2005

[7] UNINETT. "Wireless Security Threats".
Consultado en: http://www.uninett.no/wlan/wlanthreat.html. Jun. 2005

[8] Keller, Dan. "Wireless Network Security".
Consultado en: http://www.keller.com/wifi/CNIT107HW6.html. Jun. 2005

[9] "Wi-Fi Protected Access".
Consultado en: http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access. Jun. 2005

[10] Wardrive.net. "802.11 Security Tools & Software".
Consultado en: http://www.wardrive.net/security/tools. Jun. 2005