ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 37 DICIEMBRE DE 2010

"CONFIAR EN LA SEGURIDAD DE REDES WLAN"

AUTORÍA
JOSE YOEL MAESO MARTINEZ

TEMÁTICA
TIC´S

ETAPA
BACHILLERATO, FORMACIÓN PROFESIONAL

Resumen

Los coordinadores TICS y los alumnos de ciclos formativos de informática, telecomunicaciones y los alumnos de 2º Bach con la asignatura (Tecnologías de la información y comunicación) deben tener claro las posibilidades de las redes inalámbricas que están por todas partes en nuestra vida. La seguridad es más que la red funcione, tan poco debe ser una obsesión.

Palabras clave

Inalámbricas (WLAN), punto de acceso (AP), autentificación, privacidad, WEP, WAP, WPA2

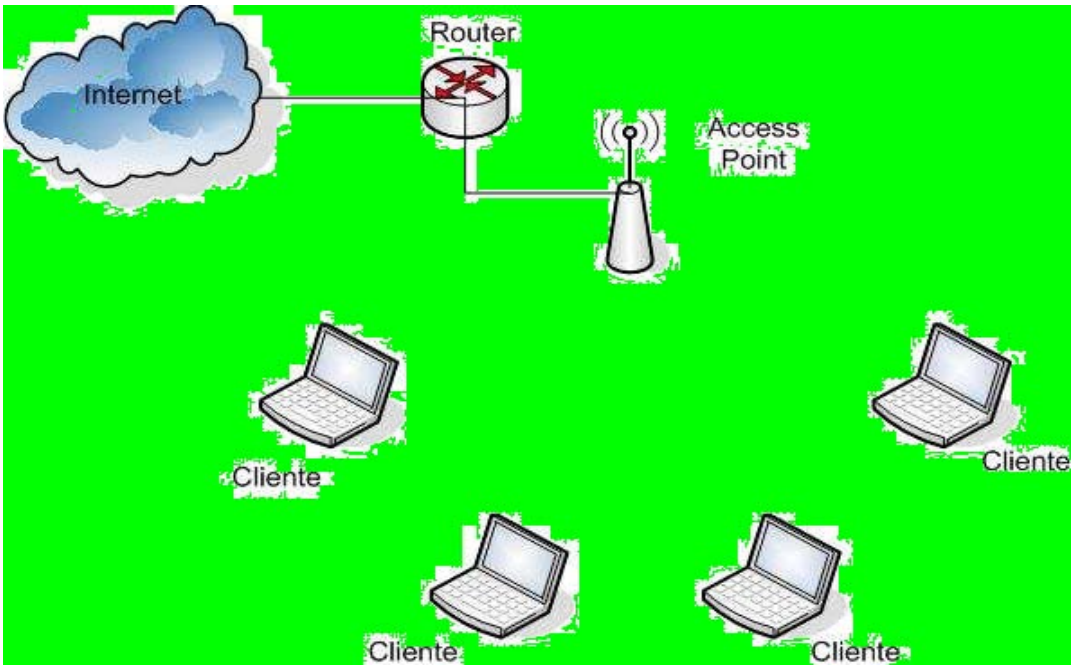
Evolución en la seguridad de redes inalámbricas

Uno de los mayores problemas con los dispositivos de redes inalámbricas es la seguridad. Veamos una evolución de la seguridad en redes inalámbricas.
Formatos de redes:

- De igual a igual (peer-to-peer): Dos equipos se comunican directamente sin necesidad de un equipo intermedio que haga de repetidor.

- Modo infraestructura: El equivalente a las LAN tradicionales, consta de un Punto de Acceso (AP) que conecta una LAN ya existente con los equipos que hacen uso de la WLAN.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 37 DICIEMBRE DE 2010



Autentificación

Para poder hacer uso de la red una vez conectado a ella es necesario que la estación se autentifique con el punto de acceso, tanto para el uso de la red inalámbrica como para el acceso a la red convencional a la que esté conectada la primera, en caso que esto suceda. El estándar 802.11 especifica dos tipos de autentificación:

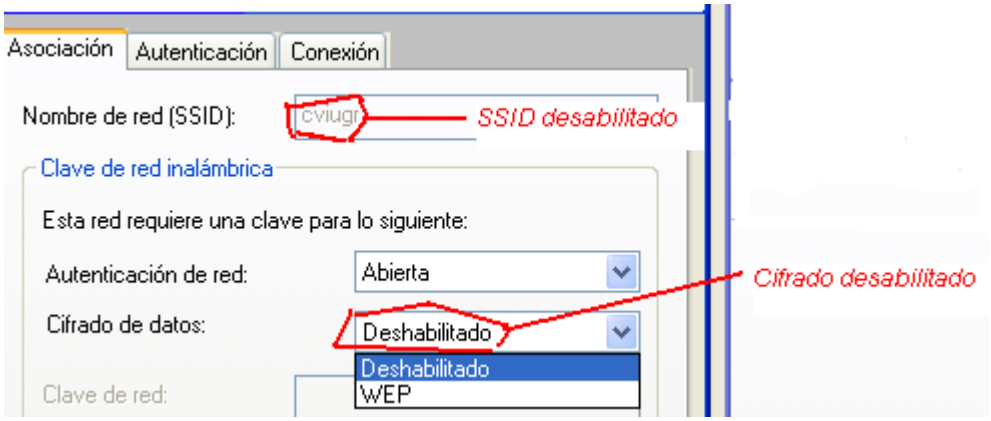
- Autentificación abierta: Simplemente se acepta a cualquier estación.
- Autentificación por clave compartida: La clave compartida usada es la misma que la clave que se usa para la encriptación WEP. Para autentificar una estación, el AP envía un desafío en texto claro a la estación, que esta devuelve encriptado usando la clave compartida. A su vez el AP también realiza la misma operación, y compara ambos resultados. En caso de que ambos coincidan se permite el acceso a la estación.

SSID (Service Set Identifier, identificador que permite acceder al AP)

La identificación de servicio (SSID), llamada nombre de red, nos proporciona la medida más básica de seguridad, es una cadena de identificación de 32 bits que se inserta en el encabezado de cada paquete de datos procesado por un punto de acceso inalámbrico. Los clientes inalámbricos cuya SSID coincida con la del punto de acceso inalámbrico pueden obtener acceso a la red, los que no coinciden son descartados.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 37 DICIEMBRE DE 2010

Los puntos de acceso por omisión vienen configurados con un SSID genérico de fábrica, así 3COM usa “101” Linksys usa “linksys”, pero es más viene configurados para emitir el SSID, el usuario debe cambiar toda esta configuración.
Así lo primero es configurar un SSID exclusivo y cambiar los nombres de inicio de sesión y contraseñas predeterminas y desactivar la emisión de nombre SSID.



Filtrado de direcciones MAC

Una tabla de direcciones MAC almacenada en el punto de acceso inalámbrico contiene las direcciones que pueden participar en la red, cualquier paquete de datos con una dirección que no coincida con las guardadas es rechazado. De manera análoga de puede crear una tabla con las direcciones a las que nos se le va a permitir el acceso a la red. Además de los problemas de mantenimiento con el cambio de tarjetas de red, hay que volver a reconfigurar el punto de acceso.

Cifrado

Con el cifrado cualquier paquete los paquetes atrapados por espías en el aire no puede ser leído a menos que conozca la clave de cifrado.

1. Cifrado de datos usando WEP

El cifrado estándar WEP (Privacidad equivalente al cable), utiliza el algoritmo de cifrado RC4. Cada paquete se encripta con una clave, que consiste en la concatenación del campo IV (que viaja en texto claro en el paquete) junto con la clave compartida WEP. La longitud del campo IV es de 24 bits (hay por tanto 16,8 millones de combinaciones posibles para encriptar un paquete con una misma clave WEP), mientras que la longitud de la clave WEP es de 40 bits, sumando

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 37 DICIEMBRE DE 2010

un total de 64 bits para encriptar el paquete, para mejorar la seguridad se puede utilizar una clave de 128 bits.

Los problemas de la seguridad WEP son:

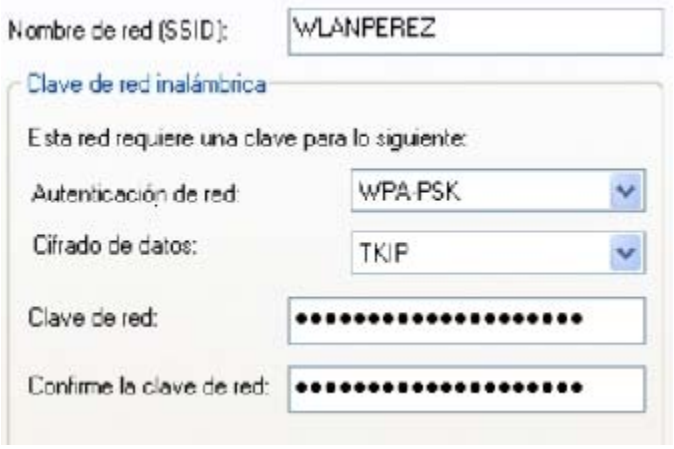
- Funciona sólo en las dos capas de red inferiores: enlace de datos y física, el cifrado se elimina de los datos antes de que atraviesen las siguientes capas de red hasta la de aplicación.
- La clave de cifrado es estática, es la misma en todas las sesiones.
- Compartida, todos los nodos usan la misma.
- No hay un verdadero mecanismo para realizar la autentificación de usuario. Los ordenadores se identifican con las direcciones MAC las cuales son fácilmente duplicadas, abriendo la posibilidad a un ataque.

Amenazas a la autentificación:
La autentificación por clave compartida envía el desafío en texto claro por el canal, el desafío encriptado se devuelve por el mismo canal. Por tanto, usando un ataque de fuerza bruta se puede tratar de descubrir la clave compartida. Así un hacker puede llevar a cabo un ataque pasivo sin ser detectado para descubrir la clave secreta, debido a que a los paquetes se propagan sin control por parte de los participantes de la red.
Una vez descubierta la clave secreta el atacante tiene acceso a la red, podrá encriptar-desencriptar todo el tráfico, debido a que la clave de autentificación es la misma clave de encriptación WEP, convirtiéndose en un usuario más en la red. Una de las soluciones es con la encriptación WEP de 128 bits, con ella, la clave compartida pasa de 40 a 104 bits, haciéndola más resistente al anterior ataque.
Se considera más seguro desactivar la autentificación usando este protocolo, ya que de esta forma se puede proteger más la clave de un ataque.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 37 DICIEMBRE DE 2010

2. Cifrado de datos usando WPA

El cifrado WPA (Acceso Protegido Wi-Fi) ofrece un cifrado extremo a extremo con autentificación. Generación de clave de cifrado dinámica, se envía claves para cada sesión y para cada usuario, una función de comprobación de integridad de clave de cifrado, autentificación de usuario a través del Protocolo de autentificación extensible (EAP).



SSID de la red a lS que nos unimos. Autentificación WPA. Cifrado TKIF. Clave de 64 bits

3. Cifrado de datos usando WPA2

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 37 DICIEMBRE DE 2010

El protocolo de seguridad llamado WPA2 (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

PROTOCOLO EAP PARA WLAN

Es frecuente confundir EAP con un mecanismo de autenticación, cuando de lo que se trata realmente es de un soporte para mecanismos de autenticación. EAP ofrece posibilidades para poder negociar entre partes una autenticación determinada

El 802.1x define el control de acceso por puerto. Para ello, cuando un dispositivo quiere acceder a una red a través de un AP, este solicita unas credenciales al mismo. Esta solicitud se realiza usando EAP (Extensible Authentication Protocol). Una vez recibidas las credenciales por parte de la estación, el AP reenvía las mismas a un servidor de autentificación RADIUS, que realiza la autentificación del usuario y autoriza su acceso.

El estándar 802.11 define una serie de mecanismos básicos que tienen como objetivo proporcionar una seguridad equivalente a la de una red tradicional cableada. Para ello buscamos dos objetivos básicos:

Autentificación: el objetivo es evitar el uso de la red (tanto en la WLAN como la LAN a la que conecta el AP) por cualquier persona no autorizada. Para ello, el Punto de Acceso solo debe aceptar paquetes de estaciones previamente autentificadas.

Privacidad: consiste en encriptar las transmisiones a través del canal radio para evitar la captura de la información. Tiene como objetivo proporcionar el mismo nivel de privacidad que en un medio cableado.

Los requerimientos para métodos EAP usados en LAN inalámbricas son descritos en la RFC4017. Este documento define los requisitos para métodos EAP usados en las implementaciones de IEEE 802.11 LAN inalámbrica. Los estándares WPA y WPA2 han adoptado tipos de EAP como sus mecanismos de autenticación.

Es una estructura de soporte, no un mecanismo específico de autenticación que provee algunas funciones comunes y negociaciones para los mecanismos de autenticación escogidos. Estos mecanismos son llamados métodos EAP, además de algunos específicos de proveedores comerciales, los definidos por los RFC incluyen EAP-MD5, EAP-TLS, EAP-IKEv2, EAP-SIM, y EAP-AKA .

Ejemplo:

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 37 DICIEMBRE DE 2010

Autentificación EAP-MD5

- En el caso de EAP-MD5 se utiliza un hash MD5 del nombre de usuario y su clave para llevar a cabo la autentificación. Debido a ello, no existe peligro en este sentido de usar la autentificación para poder romper la clave WEP.
- Adicionalmente, debido a que la autentificación es por usuario, existen más posibilidades de restringir el uso de la red para usuarios concretos, sin la necesidad de tener que cambiar la clave WEP en todos los AP y todas las estaciones.
- EAP-MD5 no ofrece ninguna prestación adicional.

Los métodos modernos capaces de operar en ambientes inalámbricos incluyen EAP-TLS, EAP-SIM, EAP-AKA, PEAP, LEAP y EAP-TTLS. Cuando EAP es invocada por un dispositivo NAS (Network Access Server) capacitado para 802.1X, como por ejemplo un punto de acceso 802.11 a/b/g, los métodos modernos de EAP proveen un mecanismo seguro de autenticación y negocian un PMK (Pair-wise Master Key) entre el dispositivo cliente y el NAS. En esas circunstancias, la PMK puede ser usada para abrir una sesión inalámbrica cifrada que usa cifrado TKIP o AES.

Ejemplos:

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 37 DICIEMBRE DE 2010

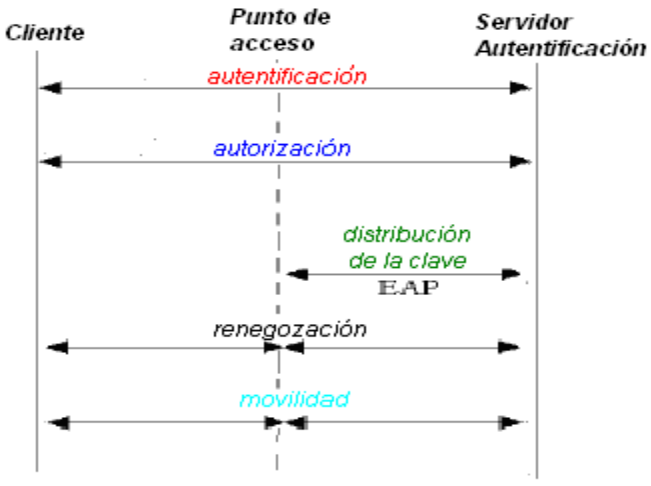
Autentificación EAP TLS

EAP –TLS usa certificados X.509 para llevar a cabo la autentificación, en lugar de nombres de usuario y palabras clave. Por ello, es necesario un servidor de certificados para poder hacer uso de esta autentificación. Además, es necesario poder expedir los certificados necesarios, o poder comprar los mismos a una autoridad certificadora.

Ventajas de EAP-TLS

- Se dialoga sobre TLS, que es la estandarización de SSL
- Autentificación de ambas partes
- Uso de claves WEP dinámicas y de un solo uso
- Asignación para cada sesión de las claves, un usuario legítimo de la red no podrá interceptar tráfico de otro usuario
- Imposición de autentificación cada pocos minutos, de forma que vuelve totalmente imposible el ataque pasivo. Esto es gestionado de manera transparente al usuario.

Esquema de autentificación en EAP-TLS



- Fase de autenticación

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 37 DICIEMBRE DE 2010

La primera fase funciona siguiendo el estándar IEEE 802.1X, es decir, cuando el cliente entra en el área de cobertura del punto de acceso, este le pide su identidad, y el cliente se la proporciona.

Tras esta fase inicial se realiza el proceso de establecimiento de conexión TLS entre los extremos, donde según el estándar tanto el cliente como el servidor de autenticación se autentican mutuamente mediante certificados X.509 y negocian los parámetros de configuración necesarios para establecer el canal de comunicación seguro.

Una vez terminada la negociación, se establece un canal TLS entre el cliente y el servidor de autenticación basado en la posesión por ambas partes de un secreto compartido que posteriormente se utilizará para derivar la clave WEP.

- Fase de autorización

En esta fase, el cliente indica al servidor de autenticación cual es el tipo de conexión que desea en cuanto al ancho de banda requerido y el tiempo que va a estar conectado, junto con los certificados SPKI que demuestran que dicho usuario está autorizado a realizar el uso de la red que pide. Entonces el servidor evalúa los certificados y comprueba si todo es correcto y si el nivel de privilegios del cliente es el necesario, continuando con el protocolo si todo va bien y desautorizando al cliente a acceder a la red si hay algún problema. De esta forma no es necesario acceder a ninguna base de datos de usuarios para comprobar los permisos de los mismos, sino que sólo se necesita confiar en las entidades emisoras de dichos certificados de autorización.

Los parámetros del cliente se mandan en una estructura firmada, de manera que el servidor de autenticación pueda estar seguro de que nadie ha modificado estos parámetros. Además, toda la información relativa a la autorización del cliente, parámetros y certificados, se manda a través del canal TLS establecido anteriormente, de manera que solo pueden haber sido enviados por parte del cliente con el que se ha iniciado el proceso de conexión. La estructura firmada contiene el certificado del cliente con el que se ha realizado la firma para que el servidor pueda verificar que la firma es correcta. En el mensaje mediante el cual el servidor le pide al cliente sus parámetros de conexión, se incluye un identificador de 4 octetos aleatorio, que posteriormente se utilizará para derivar la clave WEP junto con la dirección MAC del punto de acceso y la clave maestra de la conexión TLS anteriormente establecida.

- Fase de distribución de clave

En esta fase del protocolo, participan únicamente el punto de acceso y el servidor de autenticación, y consiste en que éste el servidor le pase al punto de acceso un descriptor de la clave WEP que debe utilizar con el cliente, así como el tipo de servicio que el cliente espera que se le ofrezca. Esta clave WEP la habrá generado el servidor como resultado de una función de

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 37 DICIEMBRE DE 2010

resumen digital MD5 aplicada sobre la concatenación de la clave maestra generada por EAPTLS, la dirección MAC del punto de acceso.

Por su parte, el punto de acceso debe comprobar que en su situación actual puede soportar las necesidades del nuevo cliente, es decir debe comprobar que la suma total del ancho de banda necesitado por todos los usuarios que actualmente hay conectados, junto con el requerido por el nuevo cliente, no sobrepase su capacidad; y que vaya a estar disponible el tiempo que el cliente requiere; informando al servidor de autenticación sobre la decisión que tome.

Tras estas fases, el proceso de conexión ha terminado, y si todo se ha realizado correctamente, el servidor de autenticación notifica al punto de acceso la autorización por su parte a que el cliente haga uso de la red. El punto de acceso traslada entonces al cliente esta decisión para que inicie la comunicación. El cliente, que habrá generado la misma clave WEP que obtuvo el punto de acceso, puede comenzar a hacer uso de la red, con la garantía de que sus mensajes son sólo descifrables por el punto de acceso, dado que la clave WEP generada es distinta para cada usuario.

- Fase de movilidad

Esta fase se apoya en la anterior, ya que cuando un cliente detecta que está en el área de cobertura de un nuevo punto de acceso, en lugar de iniciar el proceso de conexión descrito desde el principio, inicia un proceso de renegociación de conexión TLS. Al basarse la nueva conexión en la anterior, la generación del secreto compartido se puede realizar de forma más ligera, y además se evita que el servidor de autenticación tenga que validar de nuevo al usuario. Una consecuencia directa es también que de forma automática se inicia la fase de renegociación de clave WEP, lo cual implica un cambio de la misma para trabajar con el nuevo punto de acceso

Autentificación EAP-TTLS

Creada por Funk Software, EAP-TTLS es similar a EAP-TLS con algunas modificaciones. Mientras que el AP se sigue autentificando mediante un certificado, la estación usa un nombre de usuario y clave, que transmite usando cualquier mecanismo de autentificación estándar (PAP, CHAP, MS-CHAP, PAP/Token Card o EAP). El AP usa un servidor RADIUS para comprobar la autenticidad del usuario y permitirle el acceso. Es algo menos seguro que EAP-TLS, aunque más sencillo de implementar.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 37 DICIEMBRE DE 2010

Autentificación PEAP

PEAP son las siglas de EAP protegido, un protocolo desarrollado conjuntamente por Microsoft y Cisco como una alternativa a EAPTLS. Este protocolo usa TLS y certificados para realizar el transporte de la información de autentificación, pero esta se realiza usando MS-CHAPv2. Por tanto, únicamente se requiere un único certificado X.509 para TLS, sin necesidad de un certificado por usuario. La autentificación se hace mediante usuario y clave directamente a un servidor RADIUS, sin necesidad de disponer de un servidor de certificados. Así se mantiene un alto nivel de seguridad pero no se requiere una infraestructura de clave pública como en el caso de EAP-TLS, reduciendo costes.

Al igual que EAP-TLS, PEAP dispone de clave WEP dinámica.

EAP fue diseñado para utilizarse en la autenticación para acceso a la red, donde la conectividad de la capa IP puede no encontrase disponible. Dado a que EAP no requiere conectividad IP, solamente provee el suficiente soporte para el transporte confiable de protocolos de autenticación y nada más.

EAP es un protocolo el cual solamente soporta un solo paquete en transmisión. Como resultado, EAP no pude transportar eficientemente datos robustos, a diferencia de protocolos de capas superiores como TCP.

Aunque EAP provee soporte para retransmisión, este asume que el ordenamiento de paquetes es ofrecido por las capas inferiores, por lo cual el control de orden de recepción de tramas no está soportado. Ya que no soporta fragmentación y re-ensamblaje, los métodos de autenticación basados en EAP que generan tramas más grandes que el soportado por defecto por EAP, deben aplicar mecanismos especiales para poder soportar la fragmentación (Por ejemplo EAP-TLS). Como resultado, puede ser necesario para un algoritmo de autenticación agregar mensajes adicionales para poder correr sobre EAP. Cuando se utiliza autentificación basándose en certificados, el certificado es más grande que el MTU de EAP, por lo que el número de round-trips (viaje redondo de paquetes) entre cliente y servidor puede aumentar debido a la necesidad de fragmentar dicho certificado. Se debe considerar que cuando EAP corre sobre una conexión entre cliente y servidor donde se experimenta una significante pérdida de paquetes, los métodos EAP requerirán muchos round-trips y se reflejará en dificultades de conexión.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 37 DICIEMBRE DE 2010

Bibliografía

Huidobro, J. (2006). Redes de datos teoría y práctica. Madrid: Mc Grawn Hill.

Meyers, M. (2005). Redes Gestión y soluciones. Madrid: Anaya

Autoría

- Nombre y Apellidos: José Yoel Maeso Martinez
- Localidad: Granada
- E-mail: josemaesomartinez@hotmail.com