# Seguridad en redes inalámbricas 802.11

Juan Manuel Madrid Molina
*Universidad Icesi*
*jmadrid@icesi.edu.co*

Fecha de recepción: 20-11-2003 Fecha de aceptación: 20-4-2004

**ABSTRACT**
Lack of security in wireless LANs is a problem which has not been correctly assessed by network managers and people in charge of information, in spite of its seriousness. This article presents the existing technologies for heightening the security level in 802.11 wireless LANs, among with their advantages, disadvantages and application scenarios.

**KEYWORDS**
Information Security, Network Security, Wireless Networks.

**RESUMEN**
La falta de seguridad en las redes inalámbricas es un problema que, a pesar de su gravedad, no ha recibido la atención debida por parte de los administradores de redes y los responsables de la información. Este artículo presenta las tecnologías existentes para mejorar el nivel de seguridad en las redes inalámbricas 802.11, con sus ventajas, desventajas y escenarios de aplicación.

**PALABRAS CLAVES**
Seguridad informática, seguridad en redes, redes inalámbricas.

**Clasificación: B**

## INTRODUCCIÓN

Las redes inalámbricas de área local (WLAN) tienen un papel cada vez más importante en las comunicaciones del mundo de hoy. Debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red alambrada. La popularidad de estas redes ha crecido a tal punto que los fabricantes de computadores y motherboards están integrando dispositivos para acceso a WLAN en sus equipos; tal es el caso de Intel,[1] que fabrica el chipset Centrino para computadores portátiles.

Una WLAN se puede conformar de dos maneras:

- **En estrella**. Esta configuración se logra instalando una estación central denominada punto de acceso (*Access Point*), a la cual acceden los equipos móviles. El punto de acceso actúa como regulador de tráfico entre los diferentes equipos móviles. Un punto de acceso tiene, por lo regular, un cubrimiento de 100 metros a la redonda, dependiendo del tipo de antena que se emplee, y del número y tipo de obstáculos que haya en la zona.
- **Red ad hoc**. En esta configuración, los equipos móviles se conectan unos con otros, sin necesidad de que exista un punto de acceso.

El tipo de conformación más común es en estrella; se emplea por lo general cuando se desea ofrecer acceso inalámbrico a una red alambrada ya existente.

En el momento existen tres estándares diferentes para las WLAN, desarrollados por la IEEE:[2,16]

- **802.11b**: Introducido en 1999, como extensión al estándar 802.11 publicado en 1997. Los equipos inalámbricos que operaban con la norma 802.11 nunca llegaron a tener una buena acogida, porque la máxima velocidad de conexión que ofrecían era de 2 Mbps. La norma 802.11b subsanó este problema al permitir lograr una velocidad más alta de transferencia de datos. Dicha velocidad tiene un límite de 11 Mbps (similar al de una red Ethernet convencional). En la práctica, se logran velocidades entre 2 y 5 Mbps, lo que depende del número de usuarios, de la distancia entre emisor y receptor, de los obstáculos y de la interferencia causada por otros dispositivos. El factor interferencia es uno de los que más influye, porque los equipos 802.11b operan en la banda de 2.4 GHz, en la que se presenta interferencia de equipos como teléfonos inalámbricos y hornos microondas. A pesar de sus problemas, el estándar 802.11b se ha convertido en el más popular.
- **802.11a**: Se introdujo al mismo tiempo que 802.11b, con la intención de constituirla en la norma para redes inalámbricas para uso empresarial (802.11b se enfocó hacia las redes caseras y para pequeños negocios). Ofrece velocidades de hasta 54 Mbps (típicamente 22 Mbps) y opera en la banda de 5 GHz. Su alto precio, el hecho de que la banda de 5 GHz esté regulada en algunos países, y su

menor cubrimiento ha hecho que los equipos 802.11a sean menos populares que los 802.11b.

- **802.11g**: Surgió en 2003, como la evolución del estándar 802.11b. Esta norma ofrece velocidades hasta de 54 Mbps (22 Mbps típicamente) en la banda de 2.4 GHz, y es compatible hacia atrás con los equipos 802.11b, por lo cual ha tenido una gran acogida, y se prevé que reemplace por completo al estándar 802.11b en un futuro no muy lejano.

## EL PROBLEMA DE LA SEGURIDAD

El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere. Cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podría tener acceso a la red inalámbrica. Por ejemplo, si varias empresas tienen sede en un mismo edificio, y todas ellas poseen red inalámbrica, el equipo de un empleado podría encontrarse en cierto momento en el área de influencia de dos o más redes diferentes, y dicho empleado podría conectarse (intencionalmente o no) a la red de una compañía que no es la suya. Aún peor, como las ondas de radio pueden salir del edificio, cualquier persona que posea un equipo móvil y entre en el área de influencia de la red, podría conectarse a la red de la empresa.

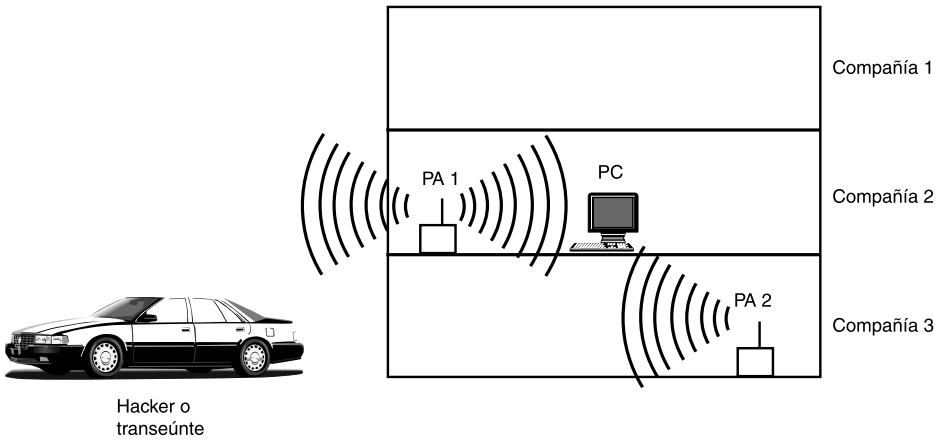


**Figura 1.** Acceso no autorizado a una red inalámbrica.

Lo grave de esta situación es que muchos administradores de redes parecen no haberse dado cuenta de las implicaciones negativas de poseer puntos de acceso inalámbrico en la red de una empresa. Es muy común encontrar redes en las que el acceso a internet se protege adecuadamente con un firewall bien configurado, pero al interior de la red existen puntos de acceso inalámbrico totalmente desprotegidos e irradiando señal hacia el exterior del edificio. Cualquier persona que desde el exterior capte

la señal del punto de acceso, tendrá acceso a la red de la compañía, con la posibilidad de navegar gratis en la internet, emplear la red de la compañía como punto de ataque hacia otras redes y luego desconectarse para no ser detectado, robar software y/o información, introducir virus o software maligno, entre muchas otras cosas. Un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la compañía.

La mala configuración de un acceso inalámbrico es, desgraciadamente, una cosa muy común. Un estudio publicado en 2003 por RSA Security Inc.[4] encontró que de 328 puntos de acceso inalámbricos que se detectaron en el centro de Londres, casi las dos terceras partes no tenían habilitado el cifrado mediante WEP (Wired Equivalent Protocol). Además, cien de estos puntos de acceso estaban divulgando información que permitía identificar la empresa a la que pertenecían, y 208 tenían la configuración con la que vienen de fábrica.

Existen dos prácticas bien conocidas para localizar redes inalámbricas:

- El **warchalking,**[3] que consiste en caminar por la calle con un computador portátil dotado de una tarjeta WLAN, buscando la señal de puntos de acceso. Cuando se encuentra uno, se pinta con tiza un símbolo especial en la acera o en un muro, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no. De este modo, otras personas pueden conocer la localización de la red.

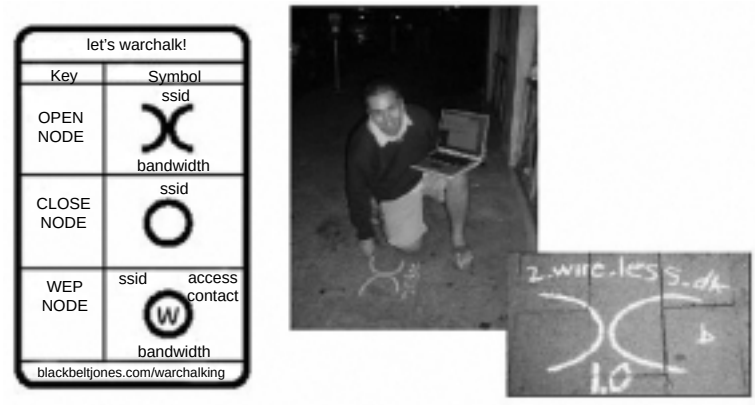


**Figura 2.** Warchalking y su simbología.[3]

- El **wardriving,** propio para localizar puntos de acceso inalámbrico desde un automóvil. Para este fin se necesita de un computador portátil con una tarjeta WLAN, una antena adecuada (que se puede elaborar fácilmente con una lata de conservas o de papas fritas,[5]) un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas, que se consigue libremente en la internet.

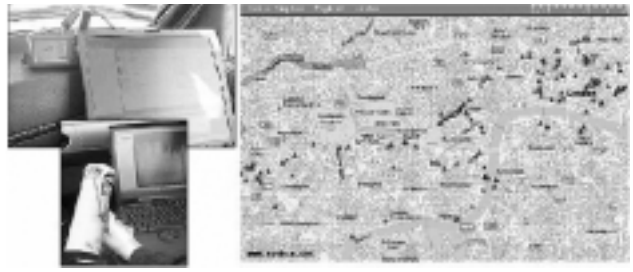

**Figura 3.** Wardriving. A la izquierda puede observarse el equipo necesario (computador, GPS y antena); a la derecha, los triángulos indican sobre el mapa[18] la posición de redes inalámbricas.

Una vez localizada una red inalámbrica, una persona podría llevar a cabo dos tipos de ataques:

- Ingresar a la red y hacer uso ilegítimo de sus recursos.
- Configurar un punto de acceso propio, orientando la antena de tal modo que los computadores que son clientes legítimos de la red atacada se conecten a la red del atacante. Una vez hecho esto, el atacante podría robar la información de dichos computadores, instalarles software maligno o dañar la información.

## GARANTIZANDO LA SEGURIDAD DE UNA RED INALÁMBRICA

Para poder considerar una red inalámbrica como segura, debería cumplir con los siguientes requisitos:

- Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.
- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Existen varios métodos para lograr la configuración segura de una red

inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas. Se hará a continuación una presentación de cada uno de ellos.

**Método 1:**
**Filtrado de direcciones MAC**

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

- No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.
- El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.
- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales como AirJack[6] o WellenReiter,[7] entre otros. De este modo, el atacante puede hacerse pasar por un cliente válido.
- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

**Método 2:**
**Wired Equivalent Privacy (WEP)**

El algoritmo WEP[10] forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

El algoritmo WEP cifra de la siguiente manera (ver Figura 4):

- A la trama en claro se le computa un código de integridad (Integrity Check Value, ICV) mediante el algoritmo CRC-32. Dicho ICV se concatena con la trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.
- Se escoge una clave secreta compartida entre emisor y receptor.

Esta clave puede poseer 40 ó 128 bits.

- Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas en claro iguales producirían tramas cifradas similares. Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.
- La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números seudo-aleatorios. El generador RC4 es capaz de generar una secuencia seudo-aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.
- El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el ICV).
- Se hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada.
- El IV y la trama se transmiten juntos.

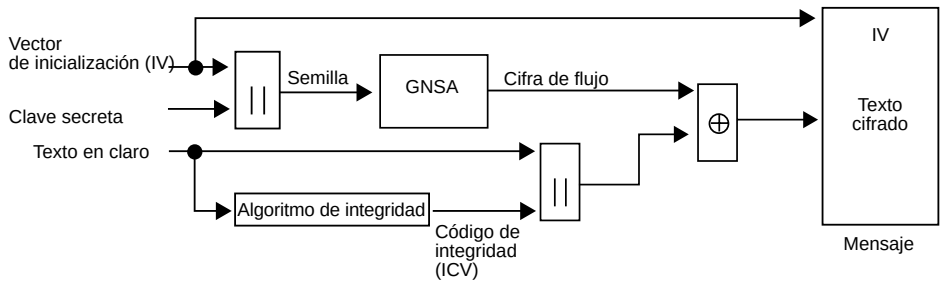


**Figura 4.** Funcionamiento del algoritmo WEP en modalidad de cifrado.[10]

En el receptor se lleva a cabo el proceso de descifrado (Figura 5):

- Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.
- Un generador RC4 produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.
- Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrado, obteniéndose de esta manera la trama en claro y el ICV.
- A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.
- Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

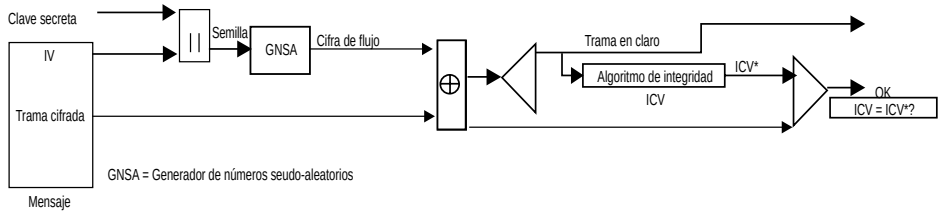


**Figura 5.** Funcionamiento del algoritmo WEP en modalidad de descifrado.[10]

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro en la manera que es empleado en la mayoría de aplicaciones:

- La mayoría de instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.
- El IV que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio de $2^{24}$ IV distintos. Esto no es problemático en una red casera con bajo tráfico, pero en una red que posea alto tráfico se puede agotar el espacio de los IV en más o menos 5 horas. Si el atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener los textos en claro de ambas tramas mediante un ataque estadístico. Con el texto en claro de una trama y su respectivo texto cifrado se puede obtener la cifra de flujo; conociendo el funcionamiento del algoritmo RC4 es posible entonces obtener la clave secreta y descifrar toda la conversación.[17]
- WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP. El primer programa que hizo esto posible fue WEPCrack,[8] que consiste en una serie de scripts escritos en lenguaje Perl diseñados para analizar un archivo de captura de paquetes de un sniffer. La herramienta AirSnort[9] hace lo mismo, pero integra las funciones de sniffer y rompedor de claves, y por lo tanto es más fácil de usar. Airsnort captura paquetes pasivamente, y rompe la clave WEP cuando ha capturado suficientes datos.

**Método 3:**
**Las VPN**

Una red privada virtual (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP.

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

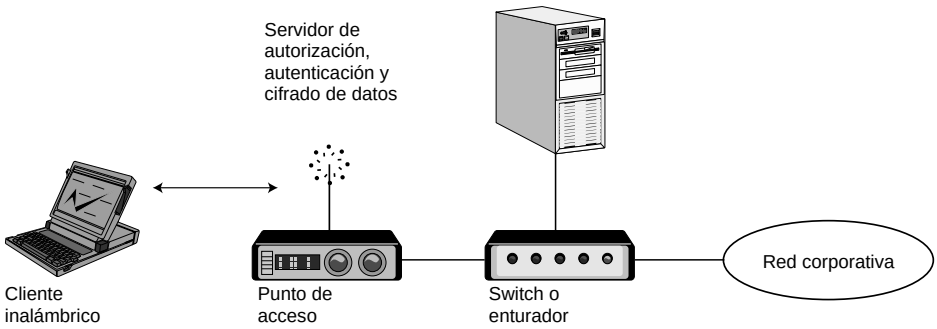


**Figura 6.** Estructura de una VPN para acceso inalámbrico seguro.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.

**Método 4:**
**802.1x**

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red.[11] El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x.

El protocolo 802.1x involucra tres participantes (Figura 7):

- El suplicante, o equipo del cliente, que desea conectarse con la red.
- El servidor de autorización/auten-

tication, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS (Remote Authentication Dial-In User Service), cuya especificación se puede consultar en la RFC 2058. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las LAN.

- El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto...) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

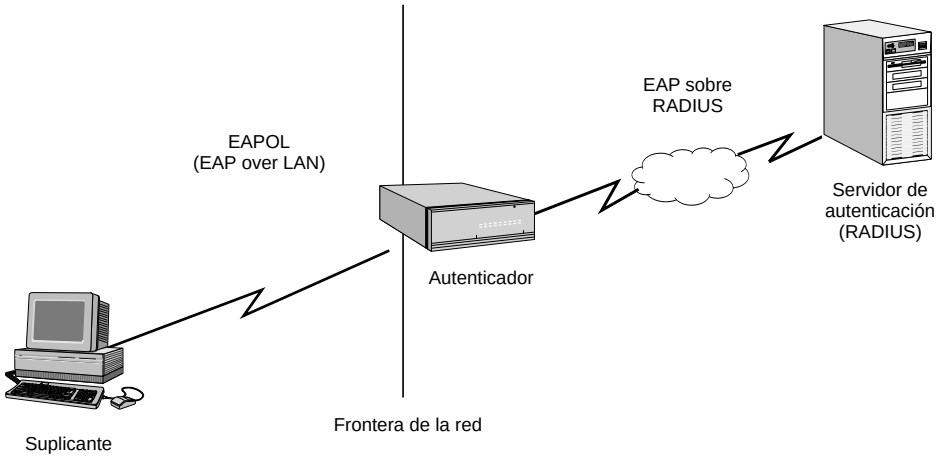


**Figura 7.** Arquitectura de un sistema de autenticación 802.1x. [12]

La autenticación del cliente se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocol) y el servicio RADIUS, de la siguiente manera:

- El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red (en el caso alambrado) o logra enlazarse o asociarse con un punto de acceso (en el caso inalámbrico). En ese momento, la interfaz de red tiene el acceso bloqueado para tráfico normal, y lo único que admite es el tráfico EAPOL (EAP over LAN), que es el requerido para efectuar la autenticación.

- La estación de trabajo envía un mensaje EAPOL-Start al autenticador, indicando que desea iniciar el proceso de autenticación.
- El autenticador solicita a la estación que se identifique, mediante un mensaje EAP-Request/ Identity.
- La estación se identifica mediante un mensaje EAP-Response/ Identity.
- Una vez recibida la información de identidad, el autenticador envía un mensaje RADIUS-Access-Request al servidor de autenticación, y le pasa los datos básicos de identificación del cliente.
- El servidor de autenticación responde con un mensaje RADIUS-Access-Challenge, en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso. Dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje EAP-Request.
- El cliente da respuesta al desafío mediante un mensaje EAP-Response (Credentials) dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje RADIUS-Access-Response.
- Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje RADIUS-Access-Accept, que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red.
- El autenticador envía un mensaje EAP-Success al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS.

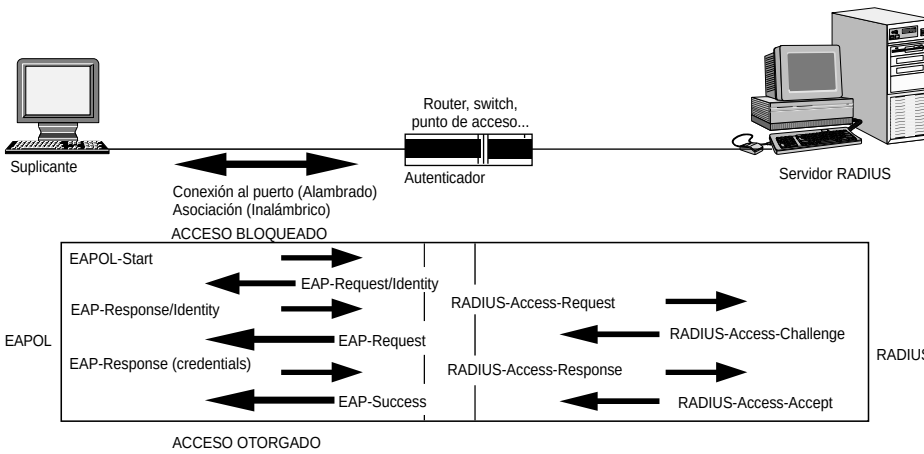


**Figura 8.** Diálogo EAPOL-RADIUS.[12,16]

En el caso del acceso inalámbrico, el servidor RADIUS despacha en el mensaje RADIUS-Access-Accept un juego de claves WEP dinámicas, que se usarán para cifrar la conexión entre el cliente y el punto de acceso. El servidor RADIUS se encarga de cambiar esta clave dinámica periódicamente (por ejemplo, cada cinco minutos), para evitar el ataque de rompimiento de la clave descrito en la sección referente a WEP.

Existen varias variantes del protocolo EAP,[13] según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas.

Las variantes de EAP que emplean certificados de seguridad son las siguientes:

- EAP-TLS: Requiere de instalación de certificados en los clientes y en el servidor. Proporciona autenticación mutua fuerte (es decir, el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEP. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Transparent Layer Substrate).
- EAP-TTLS: Desarrollada por Funk Software y Certicom. Proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor. Esto garantiza la autenticación fuerte del servidor por parte del cliente; la autenticación del cliente por parte del servidor se efectúa una vez que se establece la sesión TLS, utilizando otro método tal como PAP, CHAP, MS-CHAP ó MS-CHAP v2.
- PEAP: Desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAP-TTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

El empleo de certificados permite una autenticación fuerte entre cliente y servidor, sin embargo posee también varias desventajas:

- La administración de los certificados de seguridad puede ser costosa y complicada, especialmente en los esquemas donde se necesitan certificados en los clientes y en el servidor. Es necesario comprar los certificados a una autoridad de certificación (CA) conocida, o montar una CA propia.
- El diálogo de autenticación es largo. Esto ocasiona que el proceso sea algo demorado, siendo especialmente molesto para usuarios que tienen que reautenticarse con mucha frecuencia (por ejemplo, usuarios en movimiento que cambien de un punto de acceso a otro).
- La manipulación del certificado puede ser engorrosa para el usuario. En muchos casos se elige instalar el certificado en la terminal del usuario, con lo cual, si la terminal es robada y el certificado es el único nivel de seguridad que se posee, la seguridad de la red estaría en riesgo. Otra solución sería llevar el certificado en una tar-

jeta inteligente (smart card), lo que obligaría a instalar hardware adicional en las terminales para leer dichas tarjetas.

Las variantes de EAP que utilizan contraseñas son las siguientes:

- EAP-MD5: Emplea un nombre de usuario y una contraseña para la autenticación. La contraseña se transmite cifrada con el algoritmo MD5. Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede ensayar a cifrar múltiples contraseñas con MD5 hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente). Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está conectando a la red adecuada), y el esquema no es capaz de generar claves WEP dinámicas. Por estos problemas, EAP-MD5 ha caído en desuso.
- LEAP: Esta variante es propietaria de Cisco. Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP. Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.
- EAP-SPEKE: Esta variante emplea el método SPEKE (Simple Password-authenticated Exponential Key Exchange), que permite verificar que tanto cliente como servidor comparten una información secreta (en este caso, una contraseña) a través de un medio inseguro. Se ha comprobado que el método es muy seguro, aun con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servicio de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

**MÉTODO 5**
**WPA (WI-FI Protected Access)**

WPA[14] es un estándar propuesto por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP.

El mecanismo de autenticación usado en WPA emplea 802.1x y EAP, que fueron discutidos en la sección anterior.

Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

- Modalidad de red empresarial: Para operar en esta modalidad se requiere de la existencia de un

servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

- Modalidad de red casera, o PSK (Pre-Shared Key): WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.[15]

La norma WPA data de abril de 2003, y es de obligatorio cumplimiento para todos los miembros de la Wi-Fi Alliance a partir de finales de 2003. Según la Wi-Fi Alliance, todo equipo de red inalámbrica que posea el sello "Wi-Fi Certified" podrá ser actualizado por software para que cumpla con la especificación WPA.

## CONCLUSIONES

La seguridad en las redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite. Sin embargo, la gran cantidad de las redes inalámbricas actualmente instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, con lo cual se está poniendo en peligro la confidencialidad e integridad de dicha información.

Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas. Su implementación depende del uso que se vaya a dar a la red (casera o empresarial), de si es una red ya existente o una nueva, y del presupuesto del que se disponga para implantarla, entre otros factores.

La restricción de acceso mediante direcciones MAC es insuficiente para cualquier red, dado el gran número de herramientas disponibles libremente para cambiar la dirección MAC de una tarjeta cualquiera.

El método mediante WEP con clave estática es el mínimo nivel de protección que existe. En una red casera puede ser suficiente; en una corporativa, el uso de WEP está formalmente desaconsejado, por la facilidad con la que se pueden romper las claves WEP en un entorno de alto tráfico.

El uso de las VPN es una alternativa interesante cuando ya se tiene una red inalámbrica, y no se posee hardware inalámbrico que soporte el protocolo 802.1x. Requiere de la instalación de software especializado en los clientes inalámbricos, y de un servidor o una serie de servidores que manejen las tareas de cifrado de datos, autenticación y autorización de acceso.

La alternativa de 802.1x y EAP es la adecuada si los equipos de la red inalámbrica se pueden actualizar, o si se va a montar una red nueva. Puede usarse la solución de WEP con clave dinámica, o la de WPA; ambas ofrecen un excelente grado de protección.

Finalmente, todo mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada. El seguimiento de una política consistente evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, y garantiza la calidad y confidencialidad de la información presente en los sistemas de la empresa.

## BIBLIOGRAFÍA


1. *Intel Centrino Mobile Technology*. http://www.intel.com/products/mobiletechnology/
2. *802.11 standards: 802.11b, 802.11a, 802.11g: Which one is right for you?* http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm
3. *Warchalking*. http://www.warchalking.org
4. Dennis Fisher. *Study Exposes WLAN Security Risks*. Marzo 12 de 2003. http://www.eweek.com/print_article/0,3048,a=38444,00.asp
5. Rob Flickenger. *Antenna on the Cheap (er, Chip)*. Julio 5 de 2001. http://www.oreillynet.com/pub/wlg/448
6. *AirJack*. http://802.11ninja.net/airjack/
7. *Wellenreiter* – WLAN Hacking. http://www.wellenreiter.net/
8. *WEPCrack Project Info*. http://sourceforge.net/projects/wepcrack
9. *AirSnort Homepage*. http://airsnort.shmoo.com/
10. *Authentication and Privacy*. En ANSI / IEEE Standard 802.11, 1999 Edition. http://standards.ieee.org/getieee802/download/802.11-1999.pdf , 59-68 pp.
11. Suhdir Nath. *802.1x Overview*. Noviembre de 2003 http://www.cisco.com/warp/public/732/Tech/security/docs/8021xoverview.ppt
12. Paul Congdon. *IEEE 802.1x Overview Port Based Network Access Control*. Marzo de 2000. http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF
13. IEC. *EAP Methods for 802.11 Wireless LAN Security*. http://www.iec.org/online/tutorials/acrobat/eap_methods.pdf
14. Wi-Fi Alliance. *Overview: Wi-Fi Protected Access*. Octubre 31 de 2002. http://www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf
15. *WPA's Little Secret*. Noviembre 4 de 2003. http://www.stargeek.com/item/20270.html
16. Eduardo Tabacman. *Seguridad en Redes Wireless*. En las memorias de la I Jornada de Telemática "Comunicaciones Inalámbricas, Computación Móvil". ACIS, Bogotá (Colombia), Noviembre 13 y 14 de 2003.

17. Nikita Borisov, Ian Goldberg, David Wagner. *Security of the WEP algorithm*. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

18. *Wireless LAN in London*. Enero 26 de 2002. http://www.hoobie.net/wlan

## CURRÍCULO

**Juan Manuel Madrid Molina** es Ingeniero de Sistemas de la Universidad Icesi (1995), Especialista en Gerencia de Informática con concentración en Redes y Comunicaciones de la misma Universidad (1999) y candidato a Doctor en Ciencias de la Computación de la Universidad de Kansas, con la disertación "Aspectos temporales de perfiles para búsqueda en la Web". Ha estado vinculado laboralmente con la Universidad Icesi desde 1994, y desempeñó hasta 1999 funciones de soporte técnico a sistemas, diseño, puesta en marcha y administración de la red institucional. En la actualidad es profesor de tiempo completo del Departamento de Redes y Comunicaciones y director del programa de Ingeniería Telemática.