Seguridad en redes Wi-Fi inalámbricas

por **José Julio Ruiz** | 26-Agst-2004

Autor
José Julio Ruiz

Segunda entrega de la serie Comunicaciones Inalámbricas en donde expongo la necesidad de asegurar nuestra red inalámbrica y las estrategias a seguir para conseguirlo.

1. Introducción

En la primera entrega sobre redes WiFi veíamos de forma general cómo instalar una red WLAN / 801.11 en casa o la oficina.

Mientras que en las redes cableadas es más complicado conectarse de forma ilegítima -habría que conectarse físicamente mediante un cable-, en las redes inalámbricas -donde la comunicación se realiza mediante ondas de radio-, esta tarea es más sencilla. Debido a esto hay que poner especial cuidado en *blindar* nuestra red Wi-Fi.

2. Consideraciones previas

Los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio. Las ondas de radio -en principio- pueden viajar más allá de las paredes y filtrarse en habitaciones/casas/oficinas contiguas o llegar hasta la calle.

Si nuestra instalación está *abierta*, una persona con el equipo adecuado y conocimientos básicos podría no sólo utilizar nuestra conexión a Internet, sino también acceder a nuestra red interna o a nuestro equipo -donde podríamos tener carpetas compartidas- o analizar toda la información que viaja por nuestra red -mediante *sniffers*- y obtener así contraseñas de nuestras cuentas de correo, el contenido de nuestras conversaciones por MSN, etc.

Si la infiltración no autorizada en redes inalámbricas de por sí ya es grave en una instalación residencial (en casa), mucho más peligroso es en una instalación corporativa. Y desgraciadamente, cuando analizamos el entorno corporativo nos damos cuenta de que las redes *cerradas* son más bien escasas.

Sin pretender invitaros a hacer nada *ilegal*, podéis comprobar la cantidad de redes abiertas que podéis encontrar sin más que utilizar el programa Network Stumbler o la función *Site Survey* o escaneo de redes de vuestro PDA con Wi-Fi o de vuestro portátil mientras dáis un paseo por vuestro barrio o por vuestra zona de trabajo.

La terminología utilizada en este documento se explica en la sección Conceptos Básicos sobre Wi-Fi de la entrega anterior.

3. Objetivo: conseguir una red Wi-Fi más segura

El protocolo 802.11 implementa **encriptación WEP**, pero no podemos mantener WEP como única estrategia de seguridad ya que no es del todo seguro. Existen aplicaciones para Linux y Windows (como AiroPeek, AirSnort, AirMagnet o WEPCrack) que, escaneando el suficiente número de paquetes de información de una red Wi-Fi, son capaces de obtener las claves WEP utilizadas y permitir el acceso de *intrusos* a nuestra red. [Más información sobre vulnerabilidad WEP]

Más que hablar de **la gran regla de la seguridad** podemos hablar de una serie de estrategias que, aunque no definitivas de forma individual, en su conjunto pueden mantener nuestra red oculta o protegida de ojos ajenos.

Item	Complejidad
1. Cambia la contraseña por defecto.	Baja
2. Usa encriptación WEP/WPA.	Alta
3. Cambia el SSID por defecto.	Baja
4. Desactiva el broadcasting SSID.	Media
5. Activa el filtrado de direcciones MAC.	Alta
6. Establece el nº máximo de dispositivos que pueden conectarse.	Media
7. Desactiva DHCP.	Alta
8. Desconecta el AP cuando no lo uses.	Baja
9. Cambia las claves WEP regularmente.	Media

Tabla Resumen

A continuación entramos en detalle sobre cada uno de los items de la tabla anterior.

> Nota 1: Antes de realizar los cambios recomendados a continuación, **consulta el manual** del Punto de Acceso y del accesorio o dispositivo Wi-Fi para información detallada sobre cómo hacerlo.
>
> Nota 2: En los siguientes consejos aparece la figura de *el observador*, como la persona de la que queremos proteger nuestra red.

Asegurar el Punto de Acceso:

1. Cambia la contraseña por defecto.

- Todos los fabricantes establecen un password por defecto de acceso a la administración del Punto de Acceso.

  Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible que *el observador* la conozca.

  [!] Evita contraseñas como tu fecha de nacimiento, el nombre de tu pareja, etc. Intenta además intercalar letras con números.

Aumentar la seguridad de los datos transmitidos:

2. Usa encriptación WEP/ WPA.

- Activa en el Punto de Acceso la encriptación WEP. Mejor de 128 bits que de 64 bits... cuanto mayor sea el número de bits mejor.

  Los Puntos de Acceso más recientes permiten escribir una *frase* a partir de la cual se generan automáticamente las claves. Es importante que en esta frase intercales mayúsculas con minúsculas y números, evites utilizar palabras incluidas en el diccionario y secuencias contiguas en el teclado (como "qwerty", "fghjk" o "12345").

  También tendrás que establecer en la configuración WEP la clave que se utilizará de las cuatro generadas (*Key 1*, *Key 2*, *Key 3* o *Key 4*).

  Después de configurar el AP tendrás que configurar los accesorios o dispositivos Wi-Fi de tu red. En éstos tendrás que marcar la misma clave WEP (posiblemente puedas utilizar la *frase* anterior) que has establecido para el AP y la misma clave a utilizar (*Key 1*, *Key 2*, *Key 3* o *Key 4*).

  [!] Ya hemos visto que con algunos programas y el suficiente tiempo pueden obtenerse estas claves. En cualquier caso si el observador encuentra una red sin encriptación y otra con encriptación, preferirá "investigar" la primera en vez de la segunda.

- Algunos Puntos de Acceso más recientes soportan también encriptación WPA (Wi-Fi Protected Access), encriptación dinámica y más segura que WEP.

  Si activas WPA en el Punto de Acceso, tanto los accesorios y dispositivos WLAN de tu red como tu sistema operativo deben soportarlo (Palm OS por el momento no y para Windows XP es necesario instalar una actualización).

Ocultar tu red Wi-Fi:

3. Cambia el SSID por defecto.

- Suele ser algo del estilo a "default", "wireless", "101", "linksys" o "SSID".

  En vez de "MiAP", "APManolo" o el nombre de la empresa es preferible escoger algo menos atractivo para *el observador*, como puede ser "Broken", "Down" o "Desconectado".

  Si no llamamos la atención de *el observador* hay menos posibilidades de que éste intente entrar en nuestra red.

4. Desactiva el broadcasting SSID.

- El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual.

  Al desactivarlo tendrás que introducir manualmente el SSID en la configuración de cada nuevo equipo que quieras conectar.

  [!] Si el observador conoce nuestro SSID (por ejemplo si está publicado en alguna web de acceso libre) no conseguiremos nada con este punto.

Evitar que se conecten:

5. Activa el filtrado de direcciones MAC.

- Activa en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente tengas funcionando. Al activar el filtrado MAC dejarás que sólo los dispositivos con las direcciones MAC especificadas se conecten a tu red Wi-Fi.

  [!] Por un lado es posible conocer las direcciones MAC de los equipos que se conectan a la red con tan sólo "escuchar" con el programa adecuado, ya que las direcciones MAC se transmiten "en abierto", sin encriptar, entre el Punto de Acceso y el equipo.

  Además, aunque en teoría las direcciones MAC son únicas a cada dispositivo de red y no pueden modificarse, hay comandos o programas que permiten simular temporalmente por software una nueva

modificarse, hay comandos o programas que permiten simular temporalmente por software una nueva dirección MAC para una tarjeta de red.

6. Establece el número máximo de dispositivos que pueden conectarse.

- Si el AP lo permite, establece el número máximo de dispositivos que pueden conectarse al mismo tiempo al Punto de Acceso.

7. Desactiva DHCP.

- Desactiva DHCP en el router ADSL y en el AP.

  En la configuración de los dispositivos/accesorios Wi-Fi tendrás que introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y el DNS primario y secundario.

  [!] Si el observador conoce "el formato" y el rango de IPs que usamos en nuestra red, no habremos conseguido nada con este punto.

Para los más cautelosos:

8. Desconecta el AP cuando no lo uses.

- Desconecta el Punto de Acceso de la alimentación cuando no lo estés usando o no vayas a hacerlo durante una temporada. El AP almacena la configuración y no necesitarás introducirla de nuevo cada vez que lo conectes.

9. Cambia las claves WEP regularmente.

- Por ejemplo semanalmente o cada 2 ó 3 semanas.

  Antes decíamos que existen aplicaciones capaces de obtener la clave WEP de nuestra red Wi-Fi analizando los datos transmitidos por la misma. Pueden ser necesarios entre 1 y 4 Gb de datos para romper una clave WEP, dependiendo de la complejidad de las claves.

  Cuando lleguemos a este caudal de información transmitida es recomendable cambiar las claves.

  Recuerda que tendrás que poner la misma clave WEP en el Punto de Acceso y en los dispositivos que se vayan a conectar a éste.

4. Conclusión

Es una tendencia general pensar que la informática *per se* es segura, como ya comenté en mi Editorial de agosto de 2001 Seguridad en ordenadores de bolsillo.

En las comunicaciones inalámbricas tendemos a pensar lo mismo...¿será porque no vemos las ondas...? Seguro que no dejamos a cualquiera que pase por la calle subir con su portátil a casa o a la oficina y conectarse a nuestra red "cabledada".

Espero que esta segunda entrega de la serie **Comunicaciones Inalámbricas** nos haga concienciarnos de la necesidad de poner en marcha una serie de estrategias de seguridad para *blindar* nuestra red.

El lector tendrá que valorar si pone en práctica los nueve ítems comentados o sólo algunos de ellos. Con poner en marcha únicamente uno, ya estaremos asegurando nuestra red inalámbrica un punto más que antes.