CONTENIDOS
- Noticias
- Artículos
- Tutoriales
- Análisis
- **Modelos de PDAs**
- **Comparador de PDAs**
- Canales para PDA
- Enlaces

- **Enviar Noticias**
- Recomendados
- Más votados

COMUNIDAD
- **Regístrate**
- Tu cuenta
- Miembros
- **Foros**
- Chat
- Eventos
- Galería de Fotos
- Encuestas

GRUPO DE USUARIOS
- Principal
- Crónicas de kedadas
- **Fotos de las kedadas**
- Foro específico

SERVICIOS
- Buscar
- Versión PDA-wireless
- **Promociones**
- **Revista PalmtopUser**
- **Para empresas**

PDAEXPERTOS
- **Colaboradores**
- Nosotros
- Enlázanos

Seguridad en redes Wi-Fi inalámbricas

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

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 conectar ilegítima -habría que conectarse físicamente mediante un cable-, inalámbricas -donde la comunicación se realiza mediante ondas de radi es más sencilla. Debido a esto hay que poner especial cuidado en *b* red Wi-Fi.

2. Consideraciones previas

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

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

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

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

La terminología utilizada en este documento se explica

*en la sección **Conceptos Básicos sobre Wi-Fi** de la entrega ante*

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 d estrategias que, aunque no definitivas de forma individual, en su co mantener nuestra red oculta o protegida de ojos ajenos.

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

Tabla Resumen

A continuación entramos en detalle sobre cada uno de los items de la t

> Nota 1: Antes de realizar los cambios recomendados a continuación, **cor manual** del Punto de Acceso y del accesorio o dispositivo Wi-Fi para infc detallada sobre cómo hacerlo.
>
> Nota 2: En los siguientes consejos aparece la figura de *el observador*, cc 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 c acceso a la administración del Punto de Acceso.

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

  [!] Evita contraseñas como tu fecha de nacimiento, el nomb 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 bits que de 64 bits… cuanto mayor sea el número de bits m

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

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

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

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

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

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

Ocultar tu red Wi-Fi:

3. Cambia el SSID por defecto.

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

  En vez de "MiAP", "APManolo" o el nombre de la empresa e preferible escoger algo menos atractivo para *el observador* 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 c conectarse a la red Wi-Fi identifiquen automáticamente los de la red inalámbrica, evitando así la tarea de configuración manual.

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

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

Evitar que se conecten:

5. Activa el filtrado de direcciones MAC.

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

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

Además, aunque en teoría las direcciones MAC son única dispositivo de red y no pueden modificarse, hay com programas que permiten simular temporalmente por softw nueva dirección MAC para una tarjeta de red.

6. Establece el número máximo de dispositivos que conectarse.

- Si el AP lo permite, establece el número máximo de disposi que pueden conectarse al mismo tiempo al Punto de Acces

7. Desactiva DHCP.

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

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

[!] Si el observador conoce "el formato" y el rango de IPs que 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 n estés usando o no vayas a hacerlo durante una temporada. almacena la configuración y no necesitarás introducirla de n 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 obtene clave WEP de nuestra red Wi-Fi analizando los datos transn por la misma. Pueden ser necesarios entre 1 y 4 Gb de dat romper una clave WEP, dependiendo de la complejidad de l

claves.

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

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

4. Conclusión

Es una tendencia general pensar que la informática *per se* es seg comenté en mi Editorial de agosto de 2001 Seguridad en ordenadores

En las comunicaciones inalámbricas tendemos a pensar lo mismo...¿s vemos las ondas...? Seguro que no dejamos a cualquiera que pase po con su portátil a casa o a la oficina y conectarse a nuestra red "cableda

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

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

Y ahora vota este contenido u opina sobre él:

Votos: 1

- puntúalo -

Vuestros comentarios (4):

Enviado por **Josema8** el **31-Agst-2004**

Router ADSL, WEP, AP, DHCP, submáscara de red, DNS, broadcasting SSID...

¿De verdad es necesario que estas cosas sean tan complejísimas?. :-(
Llevo un mareo con el Wi-fi (y verás cuando entremos en harina de cómo hacerlo realidad en Palm---caso de que siquiera sea posible en la mayoria de ellas---) que no me aclaro. Y no es JJ, ni por los tutoriales, tan claros como un tutorial de esta naturaleza puede ser, si no por es cosas que dan por llamar nuevas tecnologías inalámbricas, realizadas al parecer para ingenie Telecos haciendo tesinas y no para el público de a pie.
Toy frustrado...:-(

Enviado por **Javiero** el **1-Sept-2004**

Jose Julio, muchas gracias por esta valiosa información. Yo soy un paranoico con mi red wifi sabia que se podian escuchar en abierto las direcciones MAC de los equipos que se conectan. me falta ver como hago un detector de escuchadores. :D
Saludos.

Enviado por **JJ** el **2-Sept-2004**

Holas,

poner a andar una red Wi-Fi, sin muchas complicaciones, es más o menos inmediato ya que l configuraciones estándar incluyen (en el router ADSL y en Punto de Acceso) DHCP activado.

Con esto y algún detalle más que ya viene activado por defecto en el Punto de Acceso, esto c una red Wi-Fi en casa es casi "enchufar y listo".

Pero no siempre "lo sencillo" es "lo mejor". Si queremos una red segura...ya nos metemos co de otro costal y hay que tratar con algunos temas un poco más técnicos.

Seguramente muchos de vosotros penséis que no necesitáis tanta seguridad en vuestra red . qué poner una alarma superavanzada en casa, 30 cámaras y 20 sensores de movimiento si s pueden robar la cubertería de plástico del Carrefour?

Al igual que Javiero, me gusta que "las puertas estén cerradas" o, al menos, lo más cerradas

conocimientos me permiten.

Javiero, no hace mucho ví en Espasa Calpe (La Casa del Libro) un libro sobre seguridad WiFi explicaba paso a paso cómo saltarse algunas barreras y, dentro de estas explicaciones, cómo obtener las direcciones MAC (en Linux). Te lo busco y te pongo por aquí la información del lib si quieres mirarlo.

Seguramente en Internet tamb. encontrarás info al respecto. Y sobre el "escuchador" que qu seguro que encuentras algún soft para Linux.
Saludotes a todos/as

Enviado por **[tu nombre]LUPE** el **15-Sept-2004**

COMO CONECTARSE A REDES WI FI

Añade tu mensaje:

Nombre: [tu nombre]

Texto:

* Puedes utilizar html en el mensaje
* Los saltos de línea se convierten automáticamente

Enviar