



Estrategias de seguridad para redes inalámbricas

EN EL AIRE

WLAN ofrece acceso a Internet sin cables enredados. Pero si no nos tomamos la seguridad muy en serio, podemos encontrarnos con huéspedes que no han sido invitados.

POR ERIK BÄRWALDT

Las redes inalámbricas se han ganado un lugar permanente en las redes de muchos hogares y oficinas pequeñas. Dispositivos como los routers inalámbricos y los modems DSL o de cable están disponibles en nuestra tienda local de electrónica o en nuestro proveedor de Internet por poco dinero o gratuitamente. La mayoría de los ordenadores actuales vienen con todo lo necesario para una red inalámbrica, e incluso si tenemos que actualizar nuestro sistema de escritorio para el acceso inalámbrico, las tarjetas WLAN PCI para sobremesa no son caras.

Pero la diversión se termina cuando descubrimos que un vecino está utilizando nuestra WLAN para navegar por la red. Aunque un surfista clandestino ocasional no puede hacerle daño a nuestra cuenta banca-

ria en la era del acceso mediante tarifa plana, la navegación sin autorización puede tener consecuencias desagradables. Si ocurre que el buen tipo de la puerta de al lado utiliza nuestra conexión a Internet para hacer algo ilegal, podemos esperar

una visita de la policía. Incluso si no nos encontramos en el centro de un anillo de delitos en Internet, la mera presencia de un usuario externo en su red supone una serie de amenazas a la seguridad. Por ello es muy importante – sobre todo si aún seguimos utilizando un equipo antiguo – activar el máximo de características de seguridad disponibles con nuestros dispositivos inalámbricos. En este artículo ofrecemos algunas sugerencias para mejorar la seguridad en redes inalámbricas.

Los dispositivos 802.11b WLAN que hoy en día se siguen utilizando en muchos hogares pertenecen a una generación de hardware que se remonta a finales de los 90. Estos dispositivos soportan una tasa de

Consejos para Redes WEP

Si continuamos utilizando una red inalámbrica diseñada para el estándar WEP, podemos mejorar la seguridad con las siguientes medidas:

- Seleccionar una clave compartida tan larga como sea posible y asegurarnos de que es una combinación arbitraria de números y letras. Esto reduce el riesgo de los ataques por diccionario.
- Definir cuatro claves y cambiarlas a intervalos regulares para evitar los ataques por fuerza bruta.
- Si es posible, deshabilitar el servidor DHCP que está ejecutando nuestro router. En vez de eso, asignar las direcciones IP estáticamente y definir el espacio de direccionamiento tan pequeño como sea posible.
- Cambiar la contraseña de configuración del router. Las contraseñas pre-

determinadas de los routers más populares son bien conocidas en Internet. La red estará completamente abierta a un atacante que consiga acceder a nuestro router.

- Deshabilitar la visibilidad SSID y las balizas (radiodifusión) de nuestro punto de acceso.
- Colocar nuestro router WLAN de forma que la recepción sea correcta para nuestras necesidades pero que no alcance la propiedad de nuestros vecinos. Debemos recordar que las ondas de radio también se propagan verticalmente.
- Si nuestro hardware permite esta opción, configurar la potencia de transmisión de nuestro router para igualar pero no superar nuestras propias necesidades.

transferencia de datos máxima de 11Mbps, con el ancho de banda compartido entre los clientes. Esto significa que la capacidad global, en perfectas condiciones técnicas, que podemos esperar de la tasa de transferencia es de alrededor de 5Mbps.

Para mejorar la velocidad, muchos fabricantes lanzaron extensiones propietarias que prometían tasas de transferencia más altas. Sin embargo, la mayoría de los componentes propietarios sólo funcionan con productos equivalentes del mismo fabricante. La transmisión WLAN segura suele ser imposible con una colección de dispositivos de diversos proveedores, lo que explica la razón por la que Wi-Fi Alliance creó su propio programa de certificación de forma paralela al estándar WPA. Los dispositivos deben ser 100% compatibles con las normas de Wi-Fi Alliance para que sean aprobados (Véase la Figura 1).

En el momento en que el estándar 802.11b se encontraba bajo desarrollo, realmente nadie estaba preocupado por la seguridad de la red inalámbrica. Además, muchos fabricantes de routers WLAN deshabilitaban los mecanismos de seguridad por omisión – una estrategia mal aconsejada que dejó el tráfico de la red totalmente desprotegido a menos que el usuario modificara intencionalmente la configuración de seguridad.

WEP

Las configuraciones de este tipo, que, creámoslo o no, siguen existiendo a día de hoy, han dado a cualquiera que esté dentro del alcance de la WLAN la capacidad de asociarse con el punto de acceso y usar la red. Para empeorar las cosas, incluso si el usuario hizo un esfuerzo para habilitar las características de cifrado disponibles con el dispositivo, la seguridad es a menudo ineficaz. El sistema de seguridad Wired Equivalent Privacy (WEP) utilizado con el estándar 802.11b pronto resultó ser inútil. Ya en 2001, los expertos demostraron que el cifrado WEP tiene algunas vulnerabilidades graves.

El método WEP utiliza claves con una longitud de 40 ó 104 bits (232

bits en casos excepcionales). Todos los dispositivos de la red utilizan esta clave. La estándar permite configurar un máximo de cuatro claves, pero no soporta cambios dinámicos. Además, cada paquete de datos incluye un vector de inicialización (IV), con una longitud fija de 24 bits.

Los fabricantes de componentes WLAN anunciaron el cifrado de 64 o de 128 bits para 802.11b; sin embargo, el vector de inicialización se transmite en claro. Para el vector hay disponible un máximo de 17 millones de valores. Si se repite varias veces en un período de sesiones y si la clave no cambia, los atacantes pueden calcularla y utilizarla para descifrar los mensajes. Un atacante sólo tiene que husmear los suficientes paquetes de datos y ejecutar un ataque de fuerza bruta para comprometerla.

Para una red grande con un volumen de tráfico alto, el agresor no necesita mucho tiempo para olfatear los paquetes suficientes para romper la clave. Para una pequeña red privada, el intruso ha de escuchar durante un tiempo más largo, pero existen disponibles herramientas especiales para generar tráfico al punto de acceso para acelerar el proceso de descifrado de la clave.

Otra manera de romper la clave WEP en una WLAN asegurada es lanzar un ataque de diccionario. Un ataque de diccionario implica que el atacante debe probar diferentes claves (normalmente varios millones de variaciones) hasta que es descubierta la correcta. Este método es exitoso a menudo, pero llevará más tiempo y más capacidad de computación.

Para más estrategias para elevar las barreras a los hackers véase el cua-



Figura 1: El logotipo Wi-Fi indica conformidad completa con los estándares.

dro “Consejos para Redes WEP”. La mayoría de los dispositivos 802.11b WEP heredados no son compatibles con las normas más actuales, lo que significa que el paso a una mejora de la seguridad WLAN casi siempre implica equipos nuevos.

El Sucesor Interino: WPA

Las múltiples vulnerabilidades de WEP empujaron a Wi-Fi Alliance a desarrollar una alternativa, Wi-Fi Protected Access (WPA), para cerrar la brecha hasta que el nuevo estándar 802.11i pueda ofrecer mecanismos de seguridad más robustos. WPA es un compromiso entre WEP y el más reciente WPA2: Por una parte, apoya un nuevo método de autenticación que se basa en las claves pre-compartidas, con contraseñas de entre ocho y 63 dígitos. Por otro lado, los desarrolladores de la WPA mantuvieron el algoritmo de cifrado RC4, que se ha demostrado inseguro.

Según la Wi-Fi Alliance, esta dependencia de la continuación RC4 fue necesaria debido a las deficiencias técnicas de los puntos de acceso disponibles en el momento. Estos dispositivos no tienen la suficiente capacidad computacional interna como para cambiar a un algoritmo de cifrado más seguro como AES mediante una actualización de firmware.

En la introducción de WPA, los desarrolladores modificaron los métodos de autenticación y cifrado

para proporcionar más seguridad: los clientes utilizan claves previamente compartidas o (en las grandes redes LAN inalámbricas) un servidor Radius para asociarse con el punto de acceso. Después de la autenticación, el cliente y el punto de acceso negocian una clave individual de 128 bits para evitar que otras estaciones en la WLAN rastreen el tráfico de datos. Además de estas mejoras de seguridad, WPA utiliza un vector de inicialización de 48 bits. La renegociación periódica de la clave entre el cliente y el punto de acceso añade más seguridad a la WPA estándar, eliminando la posibilidad de que un intruso ponga en marcha un ataque de fuerza bruta contra grandes volúmenes de paquetes de datos husmeados.

Estado del Arte

WPA2, que fue presentado en 2004, hace la WLAN aún más segura. Los desarrolladores abandonaron las características de seguridad heredadas de la infraestructura inalámbrica mediante, por ejemplo, la sustitución del inseguro algoritmo RC4 con el estándar superior AES. Además de esta mejor base, la nueva norma incorpora los métodos de autenticación y el cifrado WPA. Gracias a estas mejoras, los atacantes ya no se benefician del rastreo de una WLAN durante horas o días y ejecutan ata-

```

- Networks -----
SSID          T W Ch Data LLC Crypt Wk Flags
default       A N 06 6  51  6  0
<Keine aktuelle SSID> P N 00 0  1  0  0

----- Info -----
Ntwrks       2
Pckets      67
Cryptd       6
Weak         0
Noise        0
Elapsd      000051
H-M-S-

----- Status -----
Found new probed network "<Keine aktuelle SSID>" bssid 00:12:F0:A6:FD:FA
Connected to Kismet server version 2005.04.R1 build 20050403003117 on localhost:2501

```

Figura 2: El escáner WiFi Kismet puede comprobar las vulnerabilidades de nuestras redes inalámbricas y mostrar información acerca de los protocolos utilizados en nuestra red.

ques de fuerza bruta contra los resultados.

WPA2 introduce una norma en dos partes: El subgrupo WPA2 Personal especifica un estándar de características reducidas para el consumidor y el mercado SOHO. Aunque esta variante ofrece todas las características básicas de seguridad más populares, no es compatible con el beneficio adicional de autenticación a través de un servidor Radius. La versión Enterprise WPA2 abarca todo el estándar 802.11i, y por tanto permite la autenticación RADIUS.

Asegurado con WPA2

A partir de este escrito, las redes inalámbricas basadas en WPA2 son

consideradas como las más seguras. Los ataques de diccionario a la clave son el vector más probable – suponiendo que el atacante tenga suficiente tiempo y potencia de computación. Teóricamente, la difusión y multidifusión de claves representan otra vulnerabilidad. Todos los nodos de la red necesitan conocerlas, y un atacante que descubra una de las claves puede, al menos, husmear el intercambio de claves entre el punto de acceso y la estación de trabajo.

Gracias al diseño de seguridad del estándar WPA2, las modernas redes inalámbricas disponen ahora de una seguridad bastante eficaz. El mayor factor de incertidumbre es con el usuario. Hoy en día, cuando un intruso curioso obtiene acceso a una moderna infraestructura WLAN y le aplica la suficiente energía criminal para acceder a la red y causar daños, la causa suele ser un punto de acceso configurado de forma negligente. Por tanto, hay que tomar algún tiempo para considerar cuidadosamente cada una de las opciones del router de nuestra WLAN (Figura 2).

Si deseamos reducir aún más el riesgo residual, podemos añadir a la WLAN protección basada en software. Si utilizamos un túnel, como una VPN con IPSec, podemos incluso aumentar la barrera para los hackers experimentados. Como suele ocurrir, el sistema operativo libre Linux, con sus muchos componentes de seguridad incorporado, es una elección perfecta para la eliminación de riesgo residual. ■

Consejos para Redes WPA/WPA2

Mejor prevenir que curar. Como con cualquier sistema de autenticación por contraseña, seleccionamos contraseñas que sean tan largas como sea posible y nos aseguramos que incluyan una combinación arbitraria de números y letras.

- Configuramos nuestro router WLAN para negociar nuevas claves con los clientes a intervalos regulares. Esto hace que los ataques por fuerza bruta sean más difíciles.
- Deshabilitamos la configuración predeterminada del servidor de DHCP y asignamos direccionamiento IP estático.
- Utilizaremos diferentes nombres para SSID y ESSID.
- Deshabilitamos el balizamiento del router.

- Si nuestro hardware lo permite, definiremos Listas de Control de Acceso (ACLs) para que solicite las direcciones MAC de nuestras tarjetas de red.
- Cambiaremos la ubicación de nuestro router y la potencia de transmisión para que la recepción sea adecuada para nosotros, pero evitando alcanzar la propiedad de nuestros vecinos.
- En el caso de tener un dispositivo MIMO con tres antenas, debemos colocar las antenas frente a frente para mejorar la fuerza de la transmisión y de la recepción.
- Para prevenir el rastreo siempre utilizaremos conexiones cableadas para configurar nuestro router WLAN.