LANACION·COM | NOTICIAS | Tecnología

Ariel Torres | Ver perfil

La compu

Cómo asegurar tu red inalámbrica hogareña

Lunes 25 de febrero de 2008 | Publicado en la Edición impresa

Como adelanté en el videoanálisis del lunes pasado, las estadísticas mundiales sobre los hotspots inalámbricos se cumplen a rajatabla en la Argentina. Buena parte de los routers quedan completamente abiertos, mientras que una porción menor, aunque igualmente preocupante, utiliza como método de encriptación el obsoleto y frágil Wired Equivalent Privacy (WEP). El nombre no puede ser más oportuno; como un cable, este algoritmo es muy fácil de pinchar. Pero, al revés que un cable, para empeorar las cosas, no hace falta encontrarlo. Literalmente, un enrutador inalámbrico pone nuestros datos en el aire y sólo se necesita una notebook con conectividad Wi-Fi y un sniffer inalámbrico para capturar toda la información que estamos recibiendo y enviando. Es una pésima idea no encriptar este flujo de datos, y es una idea casi igual de mala el utilizar WEP para cifrarlo. Con una notebook promedio se tarda alrededor de 40 segundos en quebrar este algoritmo.

Sólo un 25% de las redes que encontré caminando un rato por varios barrios con mi celular usaban WPA (Wi-Fi Protected Access), una mejor opción que WEP. De hecho, nació como una respuesta a WEP. Con todo, tampoco es inquebrantable. Dicho brevemente, hay que usar contraseñas realmente robustas para que WPA no sea también relativamente fácil de hackear. En este contexto, una clave fuerte significa de más de 20 caracteres. Un experto posiblemente aconseje 40. O una contraseña de al menos 8, pero completamente al azar y que combine mayúsculas, minúsculas, números y símbolos. O sea, imposible de recordar. Ya he tratado el tema de las contraseñas en otras columnas, pero al final de este texto hay algunos consejos prácticos.

WPA2 es mejor que WAP y es el método que deberíamos escoger, si tanto el router como la placa en nuestra PC o notebook le dan soporte.

Dos cerrojos

Una de las cuestiones que más confunden al usuario es que hay dos niveles de seguridad en una red inalámbrica, no sólo uno, como en la PC.

En una PC aislada con Windows o Linux sólo hay que autenticarse por medio de una contraseña. Eso, teóricamente, protege nuestros recursos y documentos. Sería mejor, además, encriptar los datos, por si nos hurtan la computadora, pero en general no es menester para alcanzar cierto grado de seguridad aceptable.

En una red, y sobre todo en una red inalámbrica, las cosas son diferentes. Por un lado, hay que autenticarse. Pero además hay que encriptar los datos, porque, como dije, andan por ahí, flotando en el aire en la forma de ondas electromagnéticas.

Autenticar significa que sólo las personas autorizadas podrán utilizar el router Wi-Fi y, por ende, nuestra conexión con Internet. Si no activamos alguno de los métodos de autenticación y vivimos en una zona más o menos densamente poblada de computadoras, podemos estar seguros de que algún vecino se colgará de nuestra banda ancha. Es decir, estaremos pagándole la conexión con Internet a un colado.

Existen dos formas de asegurarnos que solamente las computadoras autorizadas entrarán al hotspot inalámbrico. Una es por medio de una contraseña. La otra registrando las direcciones MAC de las placas de red de nuestras computadoras. MAC en este caso no tiene nada que ver con Apple Macintosh. Las siglas vienen de Media Access Control y es un identificador alfanumérico de cada placa de red. Si restringimos el acceso solamente a las placas de

red de nuestras computadoras (filtrado por MAC, se llama esto) no hay que poner contraseña y sólo nuestras máquinas se podrán conectar. Esto no significa que no haya que ingresar además una contraseña, porque todavía queda encriptar los datos.

Normalmente, implementar el filtrado por MAC es un más complicado que usar una contraseña, pero vale la pena porque es más resistente a ataques. No significa que sea impenetrable. Nada lo es, en última instancia. Pero si se da maña con este mecanismo de autenticación, prefiéralo. (A propósito, y para que esto no parezca un ejercicio de pura paranoia, la forma de quebrar este método de autenticación es averiguar la MAC de alguna de las placas autorizadas y copiarlo a la tarjeta de red del equipo atacante. Otra treta es simplemente robarse una placa de red autorizada y colocarla en la máquina atacante. Hecha la ley…)

En el aire

Por supuesto, la autenticación no significa que los paquetes de datos que andan por el aire no puedan ser captados y leídos por un sniffer inalámbrico. Por eso, además, hay que encriptar la información. Este es el segundo nivel de seguridad.

Cuando hacemos compras on line, ponemos la contraseña en Hotmail o realizamos una operación de banca en línea, los datos van y vienen encriptados. Pero los expertos saben que tendemos a compartir contraseñas, por ejemplo, y pueden capturar mucha información útil para quebrar nuestra seguridad, y más tarde robarnos dinero o información. Así que la encriptación es obligatoria.

La otra cuestión que solemos olvidar es que al usar una conexión inalámbrica tenemos que sintonizar dos dispositivos. Así, si el router ofrece WPA2 pero la placa en nuestra PC no, entonces no vamos a poder conectarnos. Lamentablemente, todas estas cosas las aprendemos después de comprar los componentes, por lo que no es raro que en muchos casos la seguridad de la red se vea degradada. El mejor consejo es informarnos antes, averiguar las características que necesitamos en el router y las placas Wi-Fi (o los dispositivos inalámbricos, como notebooks, handheld y celulares), y sólo entonces salir de compras.

Una buena configuración de seguridad en una red inalámbrica hogareña usaría autenticación con contraseña (no con servidor de autenticación, que sólo tiene sentido en una empresa) y encriptación por medio de WPA. Un esquema más robusto sería filtrar por MAC y encriptar con WPA2.

Como estas tecnologías son relativamente nuevas (el estándar Wi-Fi, también conocido como 802.11x, sigue evolucionando), usted va a encontrar una gran variación en la oferta de soluciones de seguridad en routers y placas. Por ejemplo, es posible que encuentre WPA con AES (Advanced Encryption Standard), que es mejor que el TKIP (Temporal Key Integrity Protocol) que normalmente se asocia a WPA. Suena a trabalenguas, lo sé, ¿pero no hace ya más de un cuarto de siglo que venimos aprendiendo siglas extrañas? Bueno, por fortuna, algunos routers están añadiendo mecanismos que establecen todo el esquema de seguridad apretando solamente un botón. Es una buena idea que probamos y anda bien.

En todo caso, y para no extender demasiado esta columna, el colocar hoy un router inalámbrico como viene de fábrica, con sus funciones de seguridad desactivadas, es cualquier cosa menos una medida inteligente. Es buscarse un gran disgusto.

Contraseñas

Lo prometido, los consejos básicos sobre el eslabón más débil de la seguridad, las claves.

No use la misma contraseña para cosas serias (como el banco) y para foros de entretenimiento donde no se usa autenticación cifrada o segura (la página no muestra el candadito).

No use nombres, fechas o cualquier otra cosa, incluso largas frases, que puedan asociarse con usted. El pirata hace inteligencia antes de atacar, y lo primero que probará son fechas y nombres.

No use palabras de uso común, aunque no puedan asociarse con usted. Los ataques por diccionario permiten quebrar estas claves, además de que ninguna palabra de ningún idioma alcanza a cumplir los básicos de la complejidad que se requiere de una contraseña.

Como mínimo, use contraseñas de ocho caracteres que combinen minúsculas, mayúsculas, números y símbolos.

En el caso de las redes inalámbricas, la contraseña debe ser, por motivos que no viene al caso explicar, mucho más extensa. No menos de 20 caracteres, y si es posible 40 o el máximo de 63, mejor. En ese caso, puede apelar a textos literarios que, de nuevo, no puedan asociarse con sus preferencias personales.

Para más datos y trucos para crear y mantener contraseñas puede consultar mi columna del 21 de mayo último sobre este tema en www.lanacion.com.ar/909837

Por Ariel Torres

Espacio de los lectores: 17 opiniones

17
axelbender1

27.02.08
03:40

Soy un fiel lector de slashdot, pero este blog me gusta mucho tmb, no es tan geek y eso es muy realista de su parte, felicitaciones por el buen trabajo! y al respecto de la nota, hace poco tenia el router wifi logueando la actividad del firewall y me lleve un susto porque encontre miles de paquetes desechados provenientes de distintas IPs, desde EEUU hasta Pakistan, pasando por China por supuesto, y revise toda la seguridad de la red pensando que estaba siendo un intento de conexion automatizado, y finalmente descubri que un robot intentaba conectarse a mi modem (?) para enviar spam... felizmente el firewall se encargo de todo y ya no logueo la actividad de este, solo intentos de ataque y etc, aunque suena a esconderse bajo la frazada jejeje

16
Rich
26.02.08
00:22

El nivel del suplemento es correcto. El lenguaje es inevitable. Seria lo mismo que si se le preguntara al medico sobre un tema de infectología o al técnico de su auto acerca de la puesta a punto del sistema de inyección electrónica. En mi caso vendo enlaces de banda ancha. Lo mas chico que vendo actualmente es de 512 Kbps y lo más grande ha sido 4 Mbps dedicados. Me ha tocado explicar como funciona una red de PC´s con alusiones a las cañerias de agua y las canillas y la gente lo entiende, pero no es ni exacto ni correcto. No hace falta ser ingeniero para manejar un auto, pero a esta altura del partido hay cosas que no se pueden desconocer (tanto para manejar un auto como una PC de escritorio). El tema de seguridad de las redes inalámbricas es un caso tipico. Cuando muchos de mis clientes, muchos de ellos abogados, compraron (hará unos 2 años largos) los primeros routers inalámbricos creyeron haber encontrado el paraiso sin cables, hasta que alguno que sabia un poco más les advirtió "muchachos, con esto es como subir a la terraza y gritarle al vecino de enfrente la información confidencial, cualquiera te puede oir", Cuando la red es la de casa y no hay demasiadas cosas ocultas, una buena contraseña y la configuración como indica Ariel alcanza, pero cualdo es un tema de trabajo en serio, donde hay muchos pesos en danza, lo mejor es contratar un buen profesional para que haga el trabajo y darle bolilla a sus indicaciones, como cuando se va al medico o al mecánico. Saludos a todos.

15
esquierman
25.02.08
16:06

Habría que hacer una diferencia entre una contraseña y una llave de encriptación. Una contraseña es lo que se usa, por ejemplo, para entrar a Windows o Hotmail. Uno la debe tipear cada vez que ingresa al sistema, por lo tanto la debe recordar. Una llave de encriptación es una cadena de código que generalmente se entra una sola vez y el sistema la recuerda, por ejemplo para WPA o para una VPN con llave pre-compartida (PSK). No hace falta recordar de memoria una llave de encriptación cada vez que se usa el sistema, por lo tanto puede se puede usar una cadena aleatoria de código ASCII. Para el caso de la nota, hay una fuente de llaves de encriptación ideales para un WPA bien protegido en www.grc.com/passwords.htm