

Las WLAN buscan su coraza

Eva Carrasco

Un estudio realizado por la Oficina de Educación en Wi-Fi, estima que sólo en el Reino Unido hay decenas de miles de empresas que están abiertas y en riesgo de sufrir un ataque externo. Este momento de auge de los equipos Wi-Fi ha llevado a la consultora IIR a celebrar un Fasttrack Day dirigido a directores de sistemas y de informática, administradores de red y responsables de nuevas tecnologías para profundizar en los problemas y riesgos de la utilización de LAN inalámbricas y aprender cómo disminuir la vulnerabilidad. No en vano el 60% del tráfico que va por las redes de comunicación inalámbrica es tráfico de control.

Uno de los ponentes, Antonio Caamaño, director del Departamento de Teoría de la Señal y Comunicaciones de la ETSIT de la Universidad Rey Juan Carlos de Madrid, acotó los fallos de WEP (*Wired Equivalent Privacy*), sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. El WEP está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del vector de inicialización IV) o de 128 bits. Los fallos que señaló Caamaño los agrupó en dos grupos: los relacionados con la gestión de claves y los derivados de RC4.

Puntos débiles

Caamaño puso de manifiesto que “la gestión manual de claves es problemática y la clave de 40 bits muy pequeña”. Además, si éstas no se cambian, las claves pueden compilarse en “diccionarios”, lo que supone un riesgo para el usuario. Por otra parte, WEP utiliza CRC (Código de Redundancia Cíclica que se utiliza para controlar errores de Interfaz) para chequeos de integridad, que no es “fuerte” criptográficamente, y el Punto de Acceso es un punto de descifrado privilegiado. Respecto a la RC4, desde que en agosto de 2001 se publicara un artículo sobre un ataque al algoritmo RC4 se admite que las redes WEP son completamente vulnerables.




En cuanto al Wireless Lan, alertó de que las señales no se limitan a los edificios en los que están confinados, lo que hace que "exista un potencial para acceso no autorizado por parte de personal fuera del área de cobertura a través del medio radio".

Ante este escenario de inseguridad aportó algunas soluciones como la múltiple autenticación o la generación y gestión de certificados en WEP. Recomendó la encriptación a niveles superiores con IPSEC y con Open SSH, pero Caamaño alertó que "debemos ser conscientes que perdemos ancho de banda, por ejemplo de 1 mega pasaríamos a 800k". Otra solución es un filtrado HMAC, que en realidad supone una gestión de recursos para ver quiénes están conectados y dónde, ya que es muy débil y en la actualidad existen ó drivers que pueden hacer suplantación de identidad MAC. "Todas estas soluciones combinadas son una mejora enorme respecto a WEP pero no son balas de plata y no se va a solucionar la gestión de las llaves".

Implantar WLAN

En cualquier proyecto telemático, considerar la seguridad durante la fase de análisis trae consigo numerosas ventajas que se plasman en importantes ahorros de costes. En WLAN estos beneficios pueden ser aún mayores. Empezar por lo más general, construyendo la casa desde los "cimientos al tejado"; en definitiva, se

debe pensar globalmente y actuar localmente. Los lugares y situaciones más adecuados para desplegar la red WL son nuevas ubicaciones ya que no precisa cableado, para dar servicio a usuarios móviles dentro del edificio con cableado tradicional, en ampliaciones del edificio, en espacios especiales de movilidad como salas de reuniones o salas de espera y lugares temporales de actividad como hoteles o ferias.

Carlos Marcos Sánchez, ingeniero superior de Telecomunicaciones por la Unive rsidad Pbliténica de Madrid y miembro de la Internet Society e ISACA, detalló la mejor manera de realizar el despliegue físico de la red. Recomendó limitarlo a lo necesario para alcanzar los objetivos propuestos (ancho de banda, cobertura, número de usuarios...) teniendo en cuenta que las ondas 3D traspasan techos y paredes. No debemos elegir siempre la opción de menor número de puntos de acceso ni la máxima potencia. Marcos reclama "especial atención a la atenuación de materiales, además del metal, a los armarios, al cristal de seguridad, papel, personas, cemento/ ladrillo...". En cambio, como medida de seguridad, en casos extremos, se pueden utilizar cortinas metálicas en vez de plásticas, vidrios aislantes o pintura metálica. 



¡Visite ahora nuestra tienda online!
rutronik.com/webg@te

**100% rendimiento.
24 horas a su servicio.**

- Con Rutronik Webg@te tendrá acceso directo a la información más actual e importante. ¡24 horas al día!
- **Catálogo on-line:** Administración, componentes pasivos y microelectrónica, medios de almacenamiento, así como displays y empaques custom y productos submontados.
- **Pedidos de muestras y pedidos al por mayor:** Atención inmediata y transparencia de precios, servicio 24 horas.
- **PCNs y PTNs:** Facilidades, actualización rápida al sitio y la finalización de la transacción (B2B) online.
- **E-Procurement:** Información sobre el pedido y el estado del pedido (B2B) online.
- **Help Desk:** Asesoramiento e información (B2B).

Committed to excellence.



RUTRONIK EUROPE