

La realidad sobre la seguridad en redes LAN inalámbricas



Néstor Carralero, Director de Marketing 3Com Iberia
Ingeniero Técnico de Telecomunicación

Utilizar redes LAN inalámbricas sin las medidas adecuadas de seguridad, puede ocasionar que un hacker, sin que posea un equipamiento caro o sofisticado, se introduzca en una red empresarial. Y una brecha de seguridad en una red es un grave problema para cualquier compañía. Una vez dentro, el hacker puede tener acceso a contraseñas, introducirse en servidores y robar información, cambiar la página web de la empresa o hacer que la red entera deje de funcionar.

¿Qué es lo que hace que las redes inalámbricas sean más vulnerables que las redes de cable? La respuesta es sencilla: desconocimiento de las herramientas de seguridad disponibles para redes inalámbricas. El término "seguridad inalámbrica" no tiene porque ser una expresión contradictoria. De hecho son muchas las personas que piensan que es más difícil "pinchar" un cable que el aire. Hoy en día existen las herramientas de seguridad, funciones y protocolos adecuados para proporcionar una adecuada protección en las LANs inalámbricas.

Wired Equivalent Privacy o WEP

El nivel más básico de seguridad para redes inalámbricas es WEP, o Wired Equivalent Privacy, una característica estándar de todas las redes LAN inalámbricas certificadas con la norma Wi-Fi. WEP, creado por el Instituto de

Ingenieros en Electricidad y Electrónica (IEEE), ha sido diseñado para proporcionar un nivel básico de seguridad, prevenir posibles escuchas de la información y proteger la red mediante la encriptación de todos los datos que se envíen de forma inalámbrica.

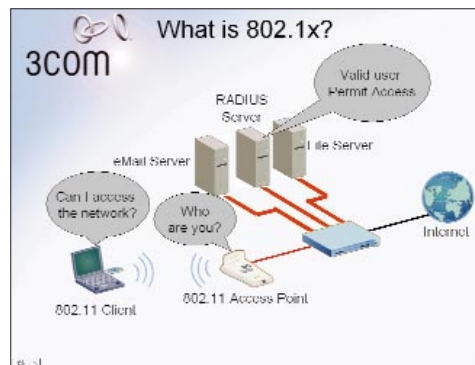
Además de diseñar una solución de seguridad robusta, el evitar simples errores es algo bastante prudente. Evitar errores (como un fallo en la configuración, la instalación no correcta del punto de acceso, no cambiar la clave WEP que viene preestablecida, etc.), mejora de forma significativa el nivel de seguridad de una red LAN inalámbrica. En teoría, las claves WEP, son contraseñas secretas que permiten a los usuarios descodificar los datos encriptados de una comunicación. En la práctica, un hacker puede conseguir acceso a las claves situándose fuera del edificio donde esté situada la red y capturando un flujo de datos encriptados con un ordenador portátil y

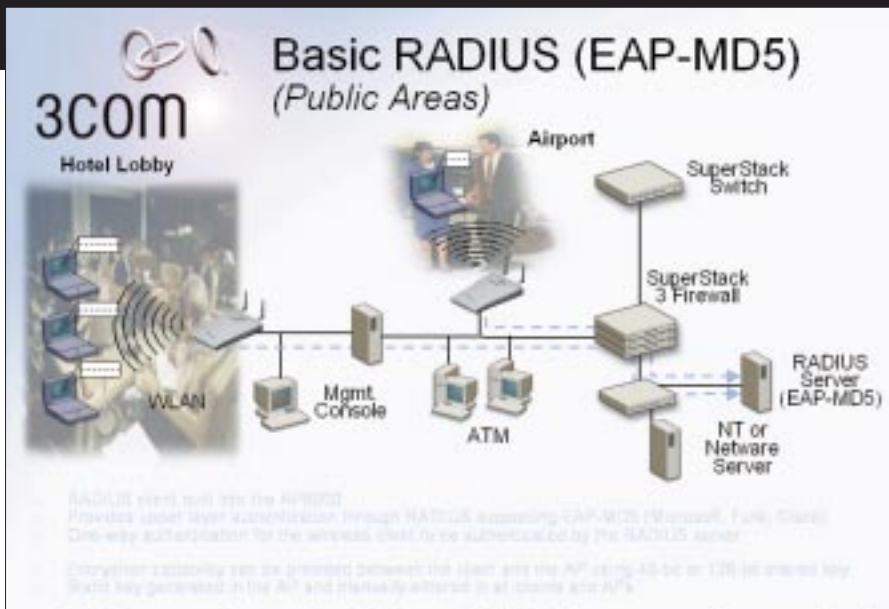
decodificar esta información utilizando un software especial que puede ser encontrado fácilmente en Internet. Este proceso revela la clave al hacker y le permite el acceso a la red de la compañía.

El algoritmo de la clave de encriptación no es defectuoso inherentemente, aunque una mala gestión de la clave puede hacerlo bastante vulnerable a ataques de hackers. A veces los administradores del sistema asignan una única clave para toda la compañía, lo que significa que una vez que un hacker consigue la clave, éste tiene acceso a toda la red de la empresa y un alto potencial para obtener información y acceder a los recursos de la misma.

Otras veces el administrador puede dar a cada usuario una clave diferente, pero no cambiarlas nunca. Así, si un hacker, consigue acceder a la red, podrá hacerlo siempre. La gestión manual de las claves puede ser fácil en una red pequeña, sin embargo, puede convertirse en un trabajo monumental si la red dispone de un gran número de usuarios.

3Com, por ejemplo, evita estos problemas a través de una prestación que llamamos Dynamic Security Link. Si se utiliza un punto de acceso con otros dispositivos cliente, Dynamic Security Link (DLS) genera de forma automática una nueva clave de encriptación WEP de 128-bit para cada usuario y cada sesión o lo que técnicamente se conoce como





asignación dinámica de claves. Esto proporciona un nivel de seguridad mucho mayor que las claves compartidas estáticas, impidiendo que un hacker pueda usurpar la identidad de un usuario, aunque pudiera descifrar la clave dinámica que éste tenga en una sesión determinada. Además DSL libera a los usuarios de la carga de tener que estar cambiando de forma manual su clave.

Para obtener mayor seguridad, Dynamic Security Link también proporciona autenticación de usuario, lo que obliga a cada usuario a introducir un nombre y contraseña en cada sesión. Esta capacidad da un nivel de seguridad y gestión mucho mejor si se compara con el sistema de autenticación basado en direcciones MAC, que simplemente permite el acceso a la red inalámbrica a aquellas direcciones MAC residentes en una tabla o lista.

Cuanto mayor es la dimensión de la red, mayor debe ser su seguridad

Otra ventaja de Dynamic Security Link es que la gestión automática y dinámica de las claves se lleva a cabo en el propio punto de acceso, eliminando la necesidad de servidores e infraestructuras adicionales. El nivel de desarrollo de seguridad inalámbrica hace que este sistema sea perfecto para una empresa de pequeño o mediano tamaño que no pueda afrontar una inversión

elevada en seguridad LAN inalámbrica. También es una solución ideal para las empresas que mantengan la seguridad de su red de una forma descentralizada.

La complejidad de las soluciones, topologías y el elevado número de usuarios que presentan las redes inalámbricas de las grandes empresas, hacen que las capacidades de seguridad analizadas hasta el momento sean "obligatorias", aunque no suficientes. En general, las grandes corporaciones requieren una tecnología de claves de encriptación más robusta, mecanismos de autenticación escalable y gestión de usuario centralizada a lo largo de la infraestructura de red, algo que no puede ser almacenado en la memoria limitada de un punto de acceso inalámbrico.

Mientras que las soluciones de seguridad WEP y Dinamic Security Link residen y se gestionan dentro de los puntos de acceso, un sistema que acomode a miles de usuarios requerirá una solución de seguridad más sofisticada basada en una infraestructura RADIUS (Remote Authenticated Dial-In User Service) cuya gestión se realiza de forma centralizada. RADIUS proporciona la gestión y administración de un amplio número de usuarios autorizados a acceder a los recursos de la red.

Soportar RADIUS con 802.1x, protocolo definido tanto para una red Ethernet cableada como una inalámbrica, mejora aún más la capacidad de autenticación del "usuario

inalámbrico". Dada la naturaleza mixta de las redes actuales y que la mayoría de sistemas operativos desarrollados dentro de las empresas están basados en Windows, 802.1x proporciona capacidades de seguridad superiores y escalables. Entre las funcionalidades técnicas que ofrece podemos encontrar las siguientes:

- Soporte 802.1x para sistemas operativos basados en Windows,
- Certificado de Cliente Universal para permitir la autenticación mutua,
- Gestión de clave protegida con soporte para protocolo RADIUS-EAP-TLS,
- Integración en entornos RADIUS existentes que soporten el protocolo MD-5 para sistemas de autenticación múltiples con protocolo EAP.

Sea cual sea el nivel de seguridad que requiera la infraestructura de red, una solución por capas puede ser adaptada de forma que se ajuste a las necesidades específicas de seguridad de la red inalámbrica. Las soluciones de seguridad pueden ser ampliadas y extendidas más allá de la infraestructura de cable para cubrir también la infraestructura inalámbrica.

Recomendaciones para implementar una Red Inalámbrica Segura

¿Cómo minimizar o eliminar entonces el riesgo de que un hacker pueda entrar en su red inalámbrica? Primero debe controlar quién accede a ella a través de procesos de autenticación y después proteger la información que viaja a través de las ondas de radio mediante técnicas de encriptado.

1. Haga más sencilla la seguridad: integre las políticas inalámbricas y las de cable

La seguridad inalámbrica no es una infraestructura de red aparte cuyos procedimientos o protocolos son completamente distintos. Desarrolle una política de seguridad que combine tanto

seguridad inalámbrica como seguridad para la red de cable, para impulsar las ventajas de gestión y de ahorro de costes. Por ejemplo, integrando la petición de nombre de usuario y contraseña para todos los usuarios que accedan a la red ya sea mediante infraestructura de cable o inalámbrica.

2. Situar el punto de acceso en el lugar adecuado

Comience con lo más básico: en la configuración de la red de su empresa, asegúrese de que los puntos de acceso están fuera de su firewall perimetral en el caso de que su solución inalámbrica no cuente con los sistemas de encriptación y autenticación requeridos, de esta manera su Firewall Perimetral controlará los accesos.

3. Utilizar una dirección MAC para evitar ataques

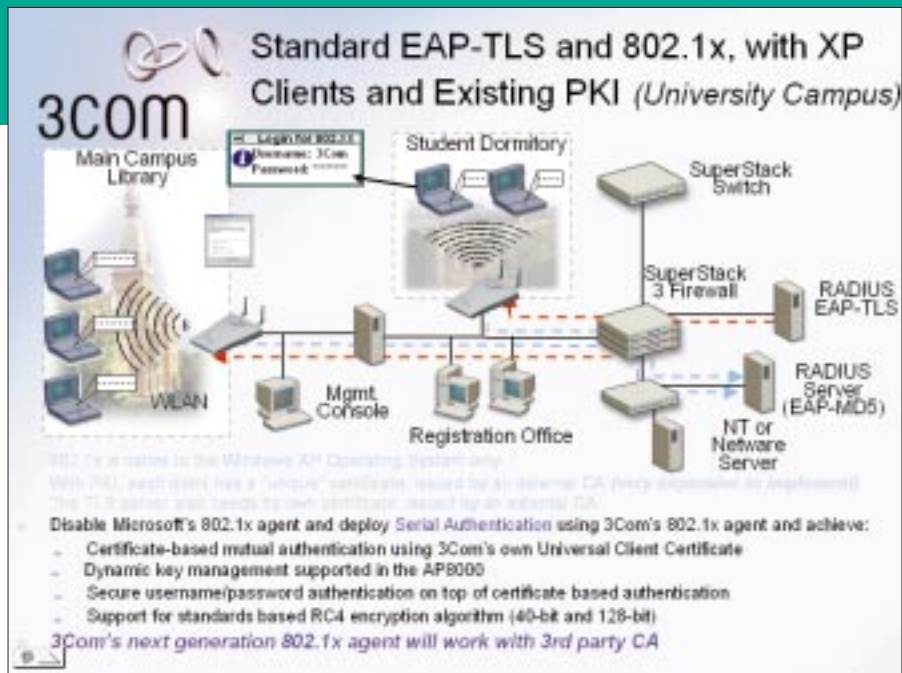
Utilizar una dirección MAC basada en ACLs (Access Control Lists) hará que sólo los dispositivos registrados puedan acceder a la red. El filtro mediante direcciones MAC es como añadir otro cerrojo a la puerta principal, y cuantos más obstáculos encuentre un hacker, más rápidamente desistirá en sus intenciones de intrusión a nuestra red.

4. Administrar su nombre de red

Todas las redes inalámbricas tienen asignado por defecto un nombre de red o SSID (Service Set Identifier). Cámbielo, inmediatamente, por un código alfanumérico. Si su organización puede encargarse de la administración de la red, cambie del SSID de forma regular. E inutilice la función de reconocimiento automático de la contraseña en su ordenador, para evitar que el SSID sea identificado fácilmente.

5. Impulsar los servidores RADIUS existentes

Los usuarios remotos de las compañías más grandes son a veces autenticados para utilizar la red a través de un servidor RADIUS (Remote Authentication Dial-In User Service). Los directores de TI pueden integrar las redes LAN inalámbricas en la



infraestructura RADIUS ya establecida para hacer más sencilla su gestión. Esto no sólo hace posible la autenticación inalámbrica, sino que además asegura que los usuarios de la red inalámbrica siguen el mismo proceso de y aprobaciones que los usuarios remotos.

6. Instalar el Protocolo de seguridad WEP

WEP (Wired Equivalent Privacy) es el protocolo de seguridad inalámbrico del estándar 802.11b. Se ha diseñado para proporcionar protección mediante encriptación de datos al tiempo en que se transmite la información, exactamente igual que se hace en las redes de cable. Sólo tiene que instalarlo, habilitarlo y cambiar de forma inmediata la clave WEP, ya que aparecerá una por defecto. Lo ideal es que genere sus claves WEP de forma dinámica cuando un usuario se identifique, haciendo que la clave de acceso a la red inalámbrica sea diferente para cada usuario y en cada ocasión, de esta manera se consigue una mejor protección.

7. La clave WEP no lo es todo

Pero no se limite al protocolo WEP. Éste es sólo un nivel más de seguridad de entre muchos otros que se deben tener en cuenta. Esta es una lección que muchos administradores de red han aprendido de la manera más dura.

8. VPN es uno de los mejores mecanismos de seguridad

Si cada opción de seguridad es un impedimento que un hacker debe salvar – cambiar el SSID, habilitar filtros

mediante direcciones MAC y generar claves WEP de forma dinámica - una red privada virtual o VPN es una cámara acorazada. Las VPN ofrecen un nivel más de seguridad basado en la creación de un túnel seguro entre el usuario y la red.

9. No todas las Redes Inalámbricas son iguales

Mientras que 802.11b es un protocolo estándar y todos los equipos que lleven la acreditación Wi-Fi operan con la misma funcionalidad base, no todos los dispositivos inalámbricos han sido creados de la misma manera. Wi-Fi asegura interoperabilidad, mientras que los productos de muchos fabricantes no incluyen prestaciones avanzadas de seguridad.

10. No permita que cualquier "usuario avanzado" configure su red inalámbrica

La configuración de una WLAN es lo suficientemente sencilla como para que no haga falta que el personal técnico instale los puntos de acceso en su propio departamento, sin pararse a pensar demasiado en el aspecto de la seguridad. Antes debe analizarse la red regularmente, con herramientas de detección de intrusos para evitar que la red pueda convertirse en un punto potencial susceptible de ser atacado por un hacker. Por tanto, se debe establecer una política que restrinja que las WLANs puedan ser implementadas sin el desarrollo y aprobación del administrador de la red.