Seguridad
en redes inalámbricas

Por Ing. Mefístoles Zamora Márquez, Especialista B en Gestión de Recursos Humanos, Dirección Territorial Camagüey, e Ing. Pablo Julio Plá Feria, Subgerente Filial Móvil, Dirección Territorial, Las Tunas, ETECSA
mefi@cmg.etecsa.cu, pablo.pla@ltu.etecsa.cu

Introducción

La libertad que proporcionan los dispositivos inalámbricos es su principal ventaja e, irónicamente, también su principal problema. Al contrario del caso de las redes cableadas tradicionales, un intruso no necesita acceso físico a nuestro edificio u oficina para intentar asaltar la red interna. Las señales de radio que utilizan los dispositivos de red inalámbricos navegan con libertad absoluta a través del aire y, por lo tanto, están al alcance de cualquiera que tenga capacidad para interceptarlas. Un asaltante puede intentar entrar en nuestra red desde la oficina de al lado, desde la calle que vemos a través de nuestra ventana o sentado cómodamente en su coche. Además, la intercepción de paquetes de datos para su análisis pasará inadvertida debido a que no hay modo de saber si alguien lo está haciendo si no los manipula y se mantiene una vigilancia [1].

Esta nueva situación obliga a la búsqueda de soluciones para garantizar la seguridad de los usuarios. Lamentablemente, por parte de los que las implementan, ni siquiera en las empresas, se ha llevado aparejada una elevada consideración hacia la seguridad. En *Wikipedia* se plantea el problema de esta manera: "Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. Un muy elevado porcentaje de redes son instaladas sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o muy vulnerables a los *crackers*), sin proteger la información que por ellas circulan"[2]. Este artículo abordará dicho tema, tan controvertido y escabroso, desde diferentes aristas.

Algunos ejemplos

Podría citarse el caso de que integrantes del equipo de HP realizaron una prueba para comprobar la seguridad de las redes inalámbricas en Madrid. Para ello, se montaron en un automóvil con una computadora portátil dotado de una tarjeta Wi-Fi, y se lanzaron a la caza de redes inseguras. Según Félix Martín, "el resultado de ese estudio fue que el 68 % de las organizaciones no tenían configurada la seguridad básica de sus puntos de acceso. No los había configurado con parámetros distintos a los que vienen de serie en la fábrica" [2].

Un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la empresa. La mala configuración de un acceso inalámbrico es, desgraciadamente, muy común. Un estudio publicado en el año 2003 por RSA Security Inc.4, encontró que de 328 puntos de acceso inalámbricos detectados en el centro de Londres, casi las dos terceras partes no tenían habilitado el cifrado mediante WEP —*Wired Equivalent Protocol*—. Además, ciento de estos puntos de acceso estaban divulgando información que permitía identificar a la empresa a la que pertenecían, y 208 tenían la configuración con la que vienen de fábrica [3].

Redes inalámbricas IEEE 802.11b (Wi-Fi)

El sistema de comunicación inalámbrico para redes más utilizado en la actualidad es el 802.11 en

cualquiera de sus variantes, definido como estándar industrial por el IEEE. Windows XP y Windows 2003 soportan nativamente este estándar en su variante 802.11b —más conocido como Wi-Fi—, que utiliza la banda de los 2,4 GHz y permite alcanzar, en principio, velocidades de hasta 11 Mbps con radios de acción de hasta 400 metros —sin paredes por el medio—. Esta es la variante más utilizada del protocolo.

Los elementos fundamentales dentro de una red inalámbrica Wi-Fi son los Puntos de Acceso —del inglés, *Access Point* (AP)—, que centralizan el servicio de acceso a la red inalámbrica —como un *hub* o *switch* en una red de cable tradicional—, y los nodos inalámbricos o estaciones —en inglés, *Station* (STA)—, que son los diferentes aparatos —normalmente computadoras personales— que se conectan a la red inalámbrica con el uso de algún tipo de adaptador de red sin cables.

- Modo *ad hoc* o IBSS —*Independent Basic Service Set*—: es equivalente al modo entre iguales de las redes locales comunes. En esta modalidad no existe un dispositivo encargado de centralizar y coordinar las comunicaciones, sino que cada nodo existente en la red se comunica de forma directa con los demás y no hay nodo que prevalezca sobre los demás.
- Modo infraestructura o BSS —*Basic Service Set*—: es el tipo más común y en él existe al menos un AP que centraliza las comunicaciones. Todo el tráfico de los diferentes nodos inalámbricos pasa en primera instancia por el punto central de acceso (AP), que es el encargado de dirigirla a su destino. Si existe más de un punto de acceso en la red, cada uno de ellos puede actuar como repetidor o puente entre redes inalámbricas, y al conjunto se le denomina ESS —*Extended Service Set*— [4].

Seguridad en las redes

La seguridad comienza con la **autenticidad, disponibilidad, confidencialidad e integridad** de los datos y la información que circula por la red [5].

- **Autenticidad**: que el usuario es quien dice ser —suplantación de identidad—.
- **Disponibilidad**: que los datos estarán disponibles en el momento y lugar requerido —protección contra Denegación de Servicios, del inglés *Denial of Service* (DoS) y pobre fiabilidad— [6].

Una vez localizada una red inalámbrica, una persona puede hacer un ataque pasivo de sólo escuchar el tráfico que se genera o de forma activa podría llevar a cabo mayormente dos tipos de ataques [7]:

Ingresar a la red y hacer uso ilegítimo de sus recursos.

Configurar un punto de acceso propio, orientando la antena de tal modo que las computadoras que son clientes legítimos de la red atacada se conecten a la red del atacante.

- **Confidencialidad**: seguridad de que el mensaje es recibido por el receptor y nadie más tiene acceso a él. La información no es legible por terceros —protección contra intercepción o la escucha pasiva—.
- **Integridad**: seguridad de que el mensaje no ha sido cambiado en la transmisión —evitar errores en la transmisión o modificaciones del mensaje malintencionadas—.

Una vez hecho esto, el atacante podría robar la información de dichas computadoras, instalarles un software maligno o dañar la información y realizar ataques tradicionales.

Se analizan, a continuación, algunos de los métodos más usados para garantizar la seguridad en redes inalámbricas.

Filtrado de direcciones MAC

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC —*Media Access Control*— de las tarjetas de red inalámbricas que pueden conectarse al Punto de Acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un *sniffer* y, luego, asignarle una de estas direcciones capturadas a la tarjeta de su computadora, empleando programas como AirJack 6 o WellenReiter 7, entre otros. De este modo, el atacante puede hacerse pasar por un cliente válido. Además los dispositivos inalámbricos ya vienen con la opción para que el usuario o cliente pueda asignarle una dirección MAC.

Figura 1 Filtrado de direcciones MAC

Debe notarse, además, que este método no garantiza la confidencialidad de la información transmitida, porque no prevé ningún mecanismo de cifrado. Se requiere conocer las direcciones MAC. Si se trata de una red pequeña, no es difícil; pero, si es una red grande, se torna complejo.

Encriptación de las comunicaciones y sus problemas

Una de las características que se han mencionado es la de confidencialidad e integridad de los datos para lo cual se usa la encriptación. Todos los protocolos de comunicaciones suelen tener algún mecanismo para proteger los datos que intercambian, y Wi-Fi no es una excepción. El protocolo 802.11b ofrece el sistema de encriptación WEP —*Wireless Equivalent Privacy*—. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN. Tras este pretencioso nombre se esconde, en realidad, el muy conocido algoritmo de cifrado mediante clave simétrica RC4. Este algoritmo se basa en la existencia de una clave compartida entre los nodos y el punto de acceso, a partir de la cual se cifra todo el tráfico [8].

WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas [9].

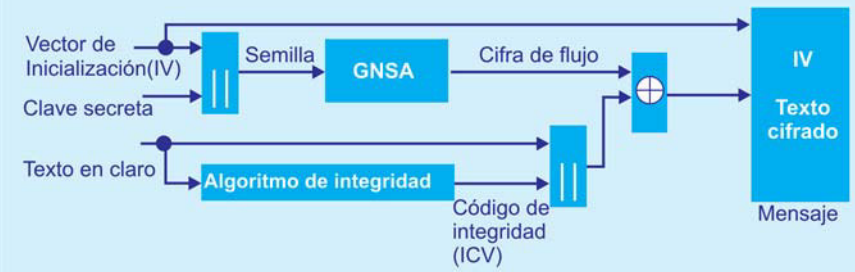

Figura 2 Funcionamiento del algoritmo WEP en modalidad de cifrado

El algoritmo de encriptación de WEP es el siguiente:

1-Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes —del inglés, *Integrity Check Value* (ICV)—.

2-Se concatena la clave secreta a continuación del IV—del inglés, *Inicialization Vector*— formando la semilla.

3-El PRNG —*Pseudo-Random Number Generator*— de RC4 genera una secuencia de caracteres pseudoaleatorios (*keystream*), a partir de la semilla, de la misma longitud que los bits obtenidos en el punto 1.

4-Se calcula el Or exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.

5-Se envía el IV —sin cifrar— y el mensaje cifrado dentro del campo de datos —*frame body*— de la trama IEEE 802.11 [10].

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces la semilla y, con ello, podrá generar el *keystream*. Realizando el XOR entre los datos recibidos y el *keystream*, se obtendrá el mensaje sin cifrar —datos y CRC-32—. A continuación, se comprobará que el CRC-32 es correcto.

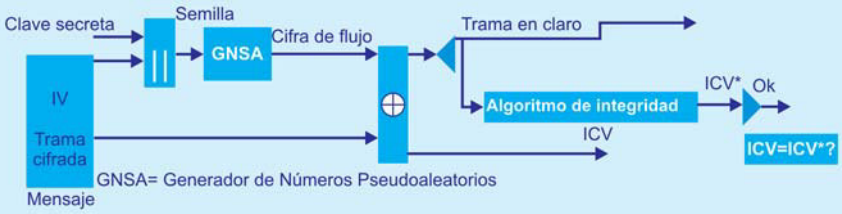

Figura 3 Funcionamiento del algoritmo WEP en modalidad de descifrado

WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el Punto de Acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

WEP utiliza una misma clave simétrica y estática en las estaciones y el Punto de Acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de las ocasiones, que la clave se cambie poco o nunca.

Como demostraron ya hace casi un par de años algunos expertos en seguridad, es posible averiguar la clave de encriptación si se rastrea el tráfico durante el tiempo suficiente, debido a que un fallo en el algoritmo generador de números aleatorios del estándar reduce la longitud efectiva de las claves a sólo 22 bits en lugar de los 64 ó 128 que define WEP [11].

El IV que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio de 224 IV distintos. Esto no es problemático en una red casera con bajo tráfico, pero en una red que posea alto tráfico puede agotarse el espacio de los IV en más o menos 5 horas. Si el atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener los textos

en claro de ambas tramas mediante un ataque estadístico. Con el texto en claro de una trama y su respectivo texto cifrado, puede obtenerse la cifra de flujo; conociendo el funcionamiento del algoritmo RC4 es posible obtener la clave secreta y descifrar toda la conversación [3].

¿Qué puede hacerse una vez que se hayan capturado varias tramas con igual IV? Se necesita conocer el mensaje sin cifrar de una de ellas. Haciendo el XOR entre un mensaje sin cifrar y el mismo cifrado, dará el *keystream* para ese IV. Al conocer el *keystream* asociado a un IV, se descifrarán todas las tramas que usen el mismo IV. El problema está en conocer un mensaje sin cifrar, aunque esto no es tan complicado porque existen tráficos predecibles o bien pueden ser provocados —mensajes ICMP de solicitud y respuesta de eco, confirmaciones de TCP, etc.— [12].

Nótese que el que logre romper la clave habrá roto también los conceptos definidos como seguridad. No obstante, para redes hogareñas, de pequeñas empresas y SOHO es una solución viable, porque WEP provee cierta seguridad y privacidad en la transmisión, contra la escucha y, en caso de un ataque, es necesario que el intruso gane el acceso, lo que le llevará cierto tiempo [7, 13].

Algunos beneficios son:

- Todos los mensaje son encriptados lo que ofrece cierto grado de resistencia.
- La privacidad se mantiene por la encriptación, si no se tiene la llave no puede leerse el mensaje.
- Es extremadamente fácil de implementar: se fija la clave en el AP y se repite en los clientes y ya está listo.
- Permite un nivel básico de seguridad en las WLAN.
- Las llaves definidas por los usuarios son ilimitadas y pueden ser cambiadas por este.

Pero como se ha visto presenta sus vulnerabilidades a causa de que su uso depende del nivel de seguridad que se necesite mantener y de la importancia de la red. De ahí que las principales desventajas son [7, 13]:

- El algoritmo de cifrado RC4 es bien conocido, por lo tanto, el atacante puede descubrir la llave y descifrar la información y tener acceso a nuestra red.
- No provee un adecuado nivel de seguridad.
- WEP debe ser implementado en cada cliente y AP, lo que hace engorroso el trabajo.

Las VPN

Una Red Privada Virtual —del inglés, *Virtual Private Network* (VPN)— emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP [14].

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea *switching*. Dicha lista de acceso y VLAN, solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando este ha sido debidamente autorizado y autenticado.

802.1x

No hay que confundir este estándar de autenticación con el estándar de comunicaciones inalámbricas 802.11x sobre el cual se ha venido hablando. El estándar 802.1x no es exclusivo de redes inalámbricas y se usa para gestionar el proceso de autenticación en protocolos de comunicaciones, así como la gestión y el reparto de claves de cifrado. Además, permite el uso del Protocolo Extendido de Autorización —del inglés, *Extensible Authentication Protocol* (EAP)— para integrarse con sistemas externos de autenticación y autorización. Su único inconveniente es que, dependiendo de cómo se configure la autenticación, esta se lleva a cabo sólo para el cliente y permite la suplantación del servidor de autenticación por parte de un atacante para obtener información de manera ilegal —la conocida metodología de ataque "hombre en el medio"— [12].

El protocolo EAP fue diseñado como método de autenticación para PPP —del inglés, *Point-to-Point-Protocol*—. EAP puede ser configurado para soportar un gran número de métodos de autenticación, por ejemplo, el uso de tarjetas, llaves públicas, certificados, PINs, entre otros.

El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x. Este protocolo involucra tres participantes:

-El suplicante o equipo del cliente que desea conectarse con la red.

-El servidor de autorización/ autenticación, que contiene la información necesaria para saber qué equipos o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS —del inglés, *Remote Authentication Dial-In User Service*—, cuya especificación puede consultarse en la RFC 2058. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remo-

tos por conexión vía telefónica; dada su popularidad, se optó por emplearlos también para autenticación en las LAN.

-El autenticador o equipo de red —*switch*, enrutador, servidor de acceso remoto— que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

Cisco utiliza el algoritmo siguiente para la implementación en sus equipos y tener una autenticación segura:

1-El servidor RADIUS y el cliente determinan que la llave WEP va a ser utilizada mientras dure la conexión.

2-El servidor RADIUS transmite la llave WEP a través de la red local (cableada) al AP.

3-El AP encripta la llave de *broadcast* y de sesión y los envía al cliente encriptados con la llave nueva. El cliente utiliza su llave para desencriptar la información.

4-El cliente y el AP activan el WEP. Luego pueden usar las llaves de sesión y *broadcast* para todas sus comunicaciones mientras dure la sesión.

5-Para mejorar la seguridad las llaves de sesión y de *broadcast* se cambian cada cierto tiempo y se reconfiguran en el servidor RADIUS [7].

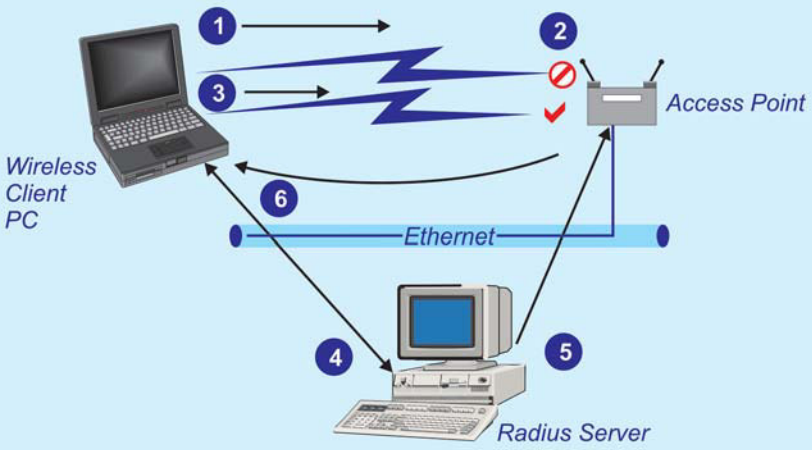

Figura 4 Algoritmo de Cisco para autenticación

WPA —*WI-FI Protected Access*—

Este estándar desarrollado por la Wi-Fi *Alliance* pretende ser el sustituto de WEP. Durante su diseño, se trató que fuera compatible con la mayor cantidad de dispositivos existentes en el mercado. WPA puede ser incorporado en muchos sistemas diseñados para WEP sin más que una actualización de *firmware*.

Con WPA se resuelven tres problemas de seguridad :

-RADIUS provee la autentificación.

-TKIP la privacidad.

-MIC la integridad.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP —del inglés, *Temporary Key Integrity Protocol*—. Este protocolo se encarga de cambiar la clave compartida entre Punto de Acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP.

TKIP, al contrario de WEP, utiliza claves de sesión dinámicas de 128 bits para cada usuario, cada sesión y cada paquete. Los usuarios deben acceder a través de un servidor de autentificación, típicamente un RADIUS. Una vez autentificados mutuamente, el servidor genera una clave *master* que transmite de manera segura al cliente y que será utilizada para enviar el resto de claves auxiliares que serán empleadas durante esa sesión.

MIC —del inglés, *Message Integrity Check*— es un sistema que garantiza que un paquete no ha sido modificado en tránsito.

Según la complejidad de la red, un Punto de Acceso compatible con WPA puede operar en dos modalidades:

- **Modalidad de red empresarial:** para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El Punto de Acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.
- **Modalidad de red casera, o PSK —*Pre-Shared Key*—:** WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces, introducir una contraseña compartida en el Punto de Acceso y en los dispositivos móviles. Solamente podrán acceder al AP los dispositivos móviles cuya contraseña coincida con él. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas —20 o más caracteres—, porque ya se ha comprobado que WPA es vulnerable a ataques de

diccionario si se utiliza una contraseña corta.

La norma WPA data de abril de 2003, y es de obligatorio cumplimiento para todos los miembros de la Wi-Fi *Alliance* a partir de finales de dicho año. Según esta entidad, todo equipo de red inalámbrica que posea el sello Wi-Fi *Certified* podrá ser actualizado por software para que cumpla con la especificación WPA.

Mejoras de WPA respecto a WEP

WPA soluciona la debilidad del Vector de Inicialización de WEP mediante la inclusión de vectores del doble de longitud —48 bits—, y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (*replay*).

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática, por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un Punto de Acceso con esta funcionalidad [15, 16].

Problemas de seguridad más frecuentes, tipos de ataques y soluciones

El advenimiento de las redes inalámbricas no ha creado una nueva legión de intrusos. Muchos de ellos utilizan los mismos ataques, con los mismos objetivos que son usados en las redes cableadas. Si no se protege la infraestructura WLAN con técnicas y métodos apropiados, estableciendo políticas y metodologías para identificar los riesgos y desarrollar nuestra seguridad, sencillamente la integridad de la WLAN se verá amenazada.

Sniffing, intercepción y escucha a escondidas

El *sniffing* originalmente concebido como una herramienta de análisis de tráfico, se ha convertido en una de las técnicas de ataques más efectivas en redes inalámbricas, permite tener un mapa de la red total o en parte, capturar *password* o capturar y desencriptar datos.

El *sniffing* es una forma de escucha pasiva de las comunicaciones a través de la red. El atacante sólo necesita conectarse a un punto para ver el tráfico de la red completa.

La única forma de proteger la red del atacante es con el uso de sesiones encriptadas donde sea posible. Usar SSL en el correo, SSH en Telnet y SCP —*Secure Copy*— en ftp. Evitar el tráfico *broadcast*.

Spoofing y acceso no autorizado

La combinación de las debilidades del WEP y la propia naturaleza de las transmisiones inalámbricas hacen que el *spoofing* sea una amenaza seria para la seguridad de estas redes. Sobre todo que estas debilidades se conozcan, permiten que exista un sinnúmero de herramientas y *exploits* que aprovechen las vulnerabilidades.

El *spoofing* es un mecanismo de ataque donde el atacante al entrar a la red hace creer que tiene una dirección válida. Puede ser a nivel MAC —llamado *spoofing* MAC— donde averigua una dirección MAC válida y la utiliza. En la actualidad, en los equipos inalámbricos es muy fácil cambiar esta dirección, opción que dan los fabricantes en sus aplicaciones para sus dispositivos. También se da el *spoofing* IP que le reporta esto al atacante, al entrar como un dispositivo válido a la red ya puede utilizar los servicios y tener acceso a los recursos.

En realidad, es poco lo que puede hacerse para prevenir este tipo de ataques. La mejor protección es, sin duda, añadir unos cuantos recursos más a la red y usar una fuente externa de autenticación como un servidor RADIUS o Escurrid, para prevenir el acceso no autorizado. Si el atacante logra obtener una MAC válida, no puede realizarse mucho, excepto que adicionalmente se disponga de una autenticación externa. La otra protección adicional es utilizar una conexión segura para todos los *host* de servicios y acceso a la red. Si usamos SSH y SSL, se necesitan certificados válidos para acceder a estos servicios, de esta forma si el *hacker* logra tener acceso a la red, no tiene acceso a los sistemas críticos.

Denegación de servicio

La naturaleza de la transmisión, especialmente la modulación por espectro esparcido hacen las WLAN vulnerables a ataque *foolding* —en grandes cantidades— y a la (DoS)—. El equipamiento necesario para este tipo de ataque es libremente asequible.

Este ataque se caracteriza porque a un mismo *host* se le realizan una avalancha de peticiones lo que impide su accesibilidad. Uno de los más conocidos es el llamado *ping* de la muerte. En las WLAN un sin-

número de causas pueden ocasionar la interrupción de un servicio. Probablemente lo que más fácil puede provocar este conflicto es el uso del espectro radio eléctrico por muchos dispositivos, lo que puede producirse si estos intentan acceder al mismo recurso en la misma frecuencia. Muchos teléfonos inalámbricos utilizan la misma frecuencia que 802.11, por lo que una simple llamada telefónica puede impedir que los usuarios accedan a la red [7].

En el ambiente inalámbrico no es necesario que el atacante esté cerca, puede encontrarse a una gran distancia con una buena antena. Por esto es recomendable utilizar herramientas como el NetStumbler para identificar si otras redes están en conflicto con la nuestra y la solución es cambiar el canal.

Conclusiones

La seguridad en las redes inalámbricas es un aspecto crítico que no debe descuidarse. Las transmisiones viajan por un medio inseguro, por tal razón se requieren mecanismos que protejan la confidencialidad de los datos, así como su integridad y autenticidad.

Se considera una red inalámbrica segura, cuando cumpla los siguientes requisitos:

- Las ondas de radio se confinan tanto como sea posible. Esto es difícil de lograr totalmente, pero puede hacerse un buen trabajo con el empleo de antenas direccionales y con la configuración adecuada de la potencia de transmisión de los Puntos de Acceso.
- Existe un mecanismo de autenticación en doble vía, que permite al cliente verificar que se está conectando a la red correcta; y a la red, constatar que el cliente está autorizado para acceder a ella.
- Los datos viajan cifrados por el aire, para evitar que equipos ajenos a la red los capturen mediante escucha pasiva.

Finalmente, todo mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada. El seguimiento de una política consistente evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, y garantiza la calidad y confidencialidad de la información presente en los sistemas de la empresa.

Referencias bibliográficas

[1] Alarcón, J.M. "Seguridad en las redes inalámbricas". *Revista PC World*, no. 201 (2003): pág.116. Disponible en: http://www.idg.es. (Consulta: 23/02/2007).

[2] "Wi-Fi". Disponible en: http://es.wikipedia.org/wiki/Wi-Fi. (Consulta: 2/02/2007).

[3] Martín, E. "La seguridad en redes inalámbricas". Foro de nuevas tecnologías de Cibernos Televisión. *Revista PC World,* no. 1008 (2004): pág.12. Disponible en: http://www.idg.es. (Consulta: 23/02/2007).

[4] Sánchez, Y. "Garantías de la seguridad en las redes inalámbricas". *Revista DealerWorld*, no. 166 (2004): pág. 300. Disponible en: http://www.idg.es. (Consulta: 23/02/2007).

[5] Gil, J. "Conceptos de seguridad en redes inalámbricas 802.11". (2004), Universidad de Vallalodid. Disponible en: http://www.gui.uva.es/~laertes/nuke/index.php?option= com_content&task=view&id=39&Itemid=41. (Consulta: 23/02/2007).

[6] Stanley, Richard A. "Wireless LAN Risks and Vulnerabilities", Information Systems Audit and Control Foundation. (2002). Disponible en: http://www.isaca.org. (Consulta: 23/02/2007).

[7] Molina, J.M.M. "Seguridad en redes inalámbricas 802.11". *Revista Sistemas y Telemática* (2004): 16-28. Disponible en: http://www.gui.uva.es/~laertes/nuke/index.php?option=com_content&task=view&id=39&Itemid=41. (Consulta:23/02/2007).

[8] Eric Oullet, R.P. *Building a CISCO Wireless LAN*. (2002). Syngress Publishing, Inc. xxvi, 475.

[9] Marco, P. D. "Sin cables, pero seguro. Seguridad en redes inalámbricas". *Revista Comunicaciones World*, no. 170 (2002): 12. Disponible en: http://www.idg.es. (Consulta: 23/02/2007).

[10] "Seguridad para redes inalámbricas".(2003). *Windows TI Magazine*. Disponible en: http://www.windowstimag.com/atrasados/2003/77_jul03/articulos/seguridad.asp. (Consulta: 23/02/2007).

[11] Nordin, B.A. *Certified Wireless Network Administrator. Official Study Guide*. McGraw-Hill/Osborn, 2006.

[12] *Using the Fluhrer, Martin and Shamir Attack to break WEP*. (2004). Disponible en: http://www.cs.rice.edu/~astubble/wep_attack.pdf. (Consulta: 23/02/2007).

[13] Barajas, S., Protocolos de seguridad en redes inalámbricas. (2004). Disponible en: http://www.saulo.net/pub/inv/SegWiFi-art.htm. (Consulta: 23/02/2007).

[14] Aspinwall, J. *Installing, Troubleshooting and Repairin Wireless Networks*. USA. McGraw Hill, 2003.

[15] "Avaya aumenta la seguridad de las redes VPN inalámbricas". *Revista Computer World*, no. 901, (2001): 13. Disponible en: http://www.idg.es. (Consulta: 23/02/2007).

[16] Madariaga, B. "3COM presenta la seguridad de nivel 3 para redes inalámbricas". *Revista Dealer World*, no. 90, (2000): 142. Disponible en: http://www.idg.es. (Consulta: 23/02/2007).

[17] Org, W.-F., *Wi-fi Alliance. Wi-fi Security at Work on the Road*. Disponible en: http://www.wi-fi.org/OpenSection/secure.asp?TID=2. (Consulta: 23/02/2007).

[18] Mobility, N. *Security for Wireless Networks*. Disponible en: http://www.netmotionwireless.com/resource/whitepapers/security.asp. (Consulta: 23/02/2007).