CONEXIONES INALÁMBRICAS: ¿Una puerta abierta para los hackers?

Ing. Morris William Díaz Saravia [1]

Resumen. El desarrollo y alcance logrado por la Internet ha hecho ineludible la expansión de las redes inalámbricas. De hecho, el Gobierno de Finlandia ha declarado –en enero del 2010- que el acceso a Internet por banda ancha es un derecho universal y que todos los finlandeses deben tener una conexión de 100 Mbps en el transcurso de 5 años.

Una forma económica de ampliar las redes y llegar a mayor cantidad de usuarios son los puntos de acceso de red inalámbrica, los cuales tienen la ventaja de no necesitar cableado y permiten la movilidad de los equipos conectados a él.

Dicha circunstancia ha propiciado la proliferación de los puntos de acceso en las empresas y los hogares. Este artículo describe los problemas de seguridad que se introducen en la red al agregar puntos de acceso inalámbrico, así como las alternativas de solución para proteger dichas redes del ataque de hackers.

En este artículo se describen las comunicaciones inalámbricas para redes de datos, comúnmente denominada WI-FI: sus principios, equipos y protocolos que se utilizan, con énfasis en la seguridad, mostrando sus debilidades así como detallando las contramedidas necesarias para mejorarla.

Palabras clave. *Sistemas de transmisión de datos, antenas (electrónica), redes inalámbricas, seguridad inalámbrica, conexiones inalámbricas.*

Desarrollo

Una red inalámbrica basada en la pila de protocolos 802.11 es una forma económica de ampliar una red preexistente, así como de implementar una nueva red. Una red inalámbrica, a diferencia de las redes cableadas, no necesita del proceso de cableado; basta con instalar las tarjetas de red WIFI en los equipos de cómputo agregando (aunque no es necesario) un Access Point, AP (con su configuración de fábrica, lo cual no es muy recomendable), y casi de forma automática se tiene configurada y operando la red.

La principal ventaja de las redes inalámbricas es su bajo costo de instalación; otra ventaja es la movilidad que otorga a los equipos portátiles.

Comunicaciones Inalámbricas

Las comunicaciones inalámbricas en las redes de computadoras se basan en los protocolos de comunicación 802.11 de la IEEE (Institute of Electrical and Electronics Engineers).

1. Ingeniero Electricista, Docente- Coordinador de la carrera de Ingeniería de las Telecomunicaciones. Escuela *Ingeniería Eléctrica y Electrónica. Escuela Especializada en Ingeniería ITCA-FEPADE, Sede Santa Tecla. E-mail:* wsaravia@itca.edu.sv

A) Protocolos de Comunicación inalámbrica
Se refieren a la capa física y capa de enlace del modelo OSI (siglas en inglés de Open Systems Interconnection). Los estándares de redes inalámbricas a la fecha son:
802.11a: es una norma que permite la comunicación hasta 54 Mbps; opera en la banda ISM (banda gratuita para aplicaciones industriales, científicas y médicas) de 5 Ghz, lo cual la vuelve incompatible en Japón y parte de Europa, donde dicho espectro está dedicado a la Hyperlan2. Utiliza OFDM (Orthogonal Frecuency Division Multiplexing) como esquema de modulación.

802.11b: es uno de los protocolos más utilizados desde su normalización de 1999. Tiene una de transmisión de 11 Mbps, utiliza la banda ISM desde 2.4 Ghz hasta 2.484 Ghz. No es compatible con 802.11a. Utiliza un esquema de modulación DSSS (Direct Sequence Spread Spectrum – espectro expandido por secuencia directa).

802.11g: es el estándar por defecto actualmente; es compatible con 802.11b y tiene una tasa de transmisión máxima de 54 Mbps, aunque utiliza la misma banda (2.4 Ghz) que la 802.11b; su esquema modulación es diferente: OFDM.

802.11n: es el estándar más reciente. Fue ratificado por la IEEE en Septiembre de 2009; trabaja en las bandas de 2.4 Ghz y 5 Ghz y su velocidad máxima se ha dispuesto en 600 Mbps. Algunos fabricantes ya disponen de dispositivos 802.11n (AP y tarjeta WIFI) que trabajan hasta 300 Mbps (estable de 1 a 108 Mps). Esta tecnología es compatible con 802.11a, 802.11b y 802.11g, transmite en múltiples canales utilizando hasta 3 antenas diferentes.

B) Modos de trabajo de una red inalámbrica 802.11
El bloque constructivo de una red es el conjunto básico de servicios (Basic Services Set o BSS). Un BSS es un conjunto de estaciones que se comunican unas con otras y la comunicación tiene lugar en un área de límites difusos denominada área básica de servicios. A cada BSS se le asocia un SSID (Service Set Identifier), que es un nombre incluido en cada paquete de la red WIFI. Dicho identificador puede tener hasta 32 caracteres alfanuméricos y se constituye en el nombre de la red. Cuando deseamos unirnos a una red inalámbrica, aparece el SSID como identificador de dicha red.

Se pueden tener dos modos de trabajo de los BSS:

Ad Hoc: las estaciones del BSS no utilizan un Access Point; se comunican únicamente con su tarjeta WIFI, una de las tarjetas asume la función del AP.
El SSID en este caso recibe el nombre de BSSID (Basic Service Set Identifier).

Infraestructura: son redes en las cuales, además de las estaciones inalámbricas, existe un Access Point (AP) y la comunicación se da en dos saltos: de la estación 1 al AP, y del AP a la estación 2.
En este caso, el SSID toma el nombre de ESSID (Extended Service Set Identifier)

C) Alcance de un Access Point
El alcance de la señal WIFI es la distancia máxima entre el AP y el cliente WIFI que permita una comunicación satisfactoria. Un AP tiene un alcance entre 20 metros y 200 metros (este último lo obtiene el fabricante en un ambiente ideal de laboratorio). Aunque el alcance puede ser inferior en base a factores como los obstáculos y el protocolo usado, en general se puede aumentar utilizando antenas de mayor ganancia y mediante amplificadores.

El alcance de la señal afecta la máxima velocidad de transmisión: a mayor distancia entre AP y cliente inalámbrico, la señal recibida es más débil. En este escenario el AP asegura la comunicación

disminuyendo la velocidad de transferencia

Los factores que afectan el alcance son:

Paredes y obstáculos: en un ambiente libre de obstáculos como paredes, muebles metálicos, etc., la señal inalámbrica tendrá un mayor alcance que en uno que tenga dichos obstáculos. Se corrige colocando el AP en un lugar alto (1.5 mts. a 2 mts. sobre el piso).

Interferencias electromagnéticas: las producen hornos microondas, teléfonos celulares y otros AP.

Potencia de transmisión: en el AP, ésta se puede considerar constante, aunque en algunos es un valor parametrizable, puede variar entre 30 mW a 200 mW o más. El componente donde se puede regular, y generalmente está disminuida la intensidad de la señal es en los equipos portátiles, donde el ahorro de la batería es crítico, y por defecto el sistema minimiza la señal de la tarjeta WIFI para un mayor tiempo-batería. En este escenario el sistema operativo proporciona la herramienta para cambiar la potencia de la antena.

Ganancia de la antena: la forma y direccionalidad de la antena afecta su alcance. Por defecto un AP tiene una antena omnidireccional, la cual emite en todas las direcciones. El mismo principio es aplicado a la antena del adaptador inalámbrico en el computador. Para mejorar el alcance se puede instalar amplificadores o antenas bidireccionales o unidireccionales con mayor ganancia, las cuales logran mayor alcance en una dirección sacrificando la ganancia en otras direcciones.

Interferencia de otros AP: ésta puede ser intercanal o cocanal. Las distintas frecuencias en la que se transmite la señal se denominan canales. El estándar define 14 canales, pero por limitaciones en diferentes regiones del mundo, sólo se utilizan 11 canales, que son los que traen definidos la mayoría de AP. La figura 1 muestra la distribución de dichos canales:

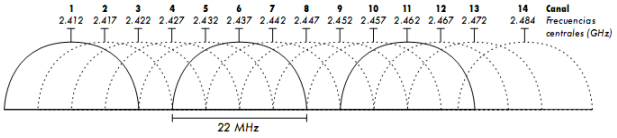

Figura 1. Canales de transmisión del estándar 802.11

Los canales tienen 22 MHz de ancho; están separados por 5Mhz, pero como se observa en la figura, hay una superposición de canales contiguos. Sólo existen tres canales que no se superponen: 1, 6 y 11. Se denomina interferencia intercanal cuando 2 AP usan el mismo canal, e interferencia cocanal cuando son canales adyacentes.

Un AP 802.11g u 802.11b sólo transmite por un canal. Si se van a tener múltiples BSS se recomienda una configuración de canal como la mostrada en la figura 2 para evitar interferencias.

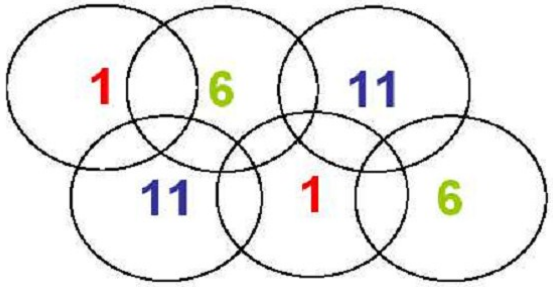

Figura 2. Configuración recomendada de canales cuando existen múltiples Access Point.

Aunque se pueda pensar que los teléfonos inalámbricos y los hornos microondas son las principales causas de interferencias en las redes WLAN (Wireless Local Area Network), las propias redes WLAN de los vecinos están empezando a ser la creciente causa de ruido e interferencias.

D) Seguridad inalámbrica

En una red cableada la seguridad se simplifica: si una persona tiene acceso a un computador conectado a un SWITCH de la red, entonces puede usar los recursos de la misma. La red es considerada confiable si todos los equipos de ésta son accedidos por personas de confianza.

En una red inalámbrica el modo de acceso es muy diferente al planteado para redes cableadas:

1. Aunque el alcance del AP idealmente puede oscilar arriba de los 100 metros, en la práctica cualquiera que tenga una antena de alta ganancia puede acceder al AP desde kilómetros de distancia. Las ondas de radio del AP no se cortan bruscamente en el límite de la propiedad, estas siguen, es "difuso" su límite. El record Guiness de alcance de una red WIFI es de 382 Km.
2. No hay un cable visible que se pueda rastrear hasta el intruso, puede estar en cualquier ubicación dentro del alcance del AP. El intruso puede estar en el cuarto de al lado o a algunos kilómetros de distancia.
3. Dicho intruso puede rastrear los paquetes sin necesidad de transmitir ninguno, almacenar los paquetes rastreados en un disco duro y luego aplicar algoritmos de desencriptado para obtener contraseñas de correo y de las cuentas de banco.

Al descifrar dichos paquetes puede elaborar un sofisticado plan de ataque a la red.
Es necesario pensar en mecanismos de seguridad confiables que limiten a un mínimo cualquier intrusión, pero al tomar decisiones de seguridad debe considerarse por encima de todo, que la red existe para facilitar la comunicación de todos sus usuarios.

Por otra parte, el factor humano introduce una falla de seguridad extra: usuarios involuntarios que se conectan a cualquier red disponible, cazadores de redes inalámbricas e intrusos que tienen las herramientas y la mala intención de acceder a los datos de la red.

E) Técnicas de seguridad inalámbrica

Aunque una red inalámbrica presenta algunas ventajas, a nivel de seguridad abre una puerta trasera a la red, presentando múltiples problemas a los cuales tiene que enfrentarse el diseñador de la red. A continuación se verán las herramientas y técnicas para aumentar la seguridad de las redes inalámbricas, así como sus fortalezas y debilidades.

1. Filtrado MAC: cada tarjeta de red tiene una dirección única de 6 bytes denominada MAC; en el filtrado MAC se autentican las estaciones clientes en el AP el cual tiene una tabla de direcciones aprobadas.

Fortaleza.

- Los usuarios involuntarios no pueden conectarse a la red.

Debilidad.

- Un usuario malintencionado corre una aplicación, lee los paquetes y detecta una o más MAC validadas en la tabla y mediante software cambia la MAC de su tarjeta pudiendo acceder al AP.

2. Configuración de Red Cerrada: los AP difunden al medio su ESSID varias veces por segundo, permitiendo a sus clientes que la detecten. En una red cerrada, el AP no difunde su ESSID y obliga a los clientes a que conozcan el ESSID para conectarse.

Fortaleza.

- No está visible el ESSID, por tanto no es desplegado por los clientes de forma explícita.

Debilidad.

- Los clientes mandan sus paquetes y si estos son capturados por usuarios malintencionados pueden extraer el ESSID.
  Por otro lado genera múltiples inconvenientes este método:
  - Los usuarios de la red requerirán mayor soporte técnico para conectarse y pueden generar múltiples quejas al fallar el soporte.
  - Si se instala una red adyacente por un tercero, aunque se haga un estudio de las redes existentes del lugar, al no ver la red (ESSID) podría existir interferencia intercanal o cocanal.
  - El nivel de seguridad es pobre frente al software que corren usuarios malintencionados para leer los paquetes. Por ejemplo el software Kismet.

F) Métodos de encriptación

Los siguientes son métodos de encriptación. Si se utiliza una fuerte encriptación se puede autenticar a los usuarios de forma segura y confiable; además evita que los usuarios malintencionados fisgoneen fácilmente el tráfico de red.

1. Encriptación WEP: del inglés Wired Equivalent Privacy, WEP, utiliza una clave compartida de 40 bits para autenticar al cliente con el AP.

Fortaleza:

- Cuando alguien desea conectarse al AP éste solicita la clave WEP desalentando su intención. Provee cierto nivel de privacidad, aunque actualmente hay ataques muy difundidos en la red que obtienen la clave WEP mediante técnicas de hacking.
- Otra ventaja es que la clave WEP está muy difundida en los AP y casi todos soportan los protocolos 802.11b, g y n.

Debilidad:

- Es una clave compartida y en nuestro medio significa que un buen porcentaje de usuarios no necesariamente de confianza la conocerán con mínima Ingeniería social.
- Actualmente, la encriptación WEP se considera deficiente por vulnerabilidades descubiertas que posibilitan generar un ataque, con el cual en menos de 15 minutos se obtiene la clave WEP.

2. Encriptación WPA: del inglés WIFI Protected Access, es un sistema de encriptación que supera las debilidades de WEP. Puede ser de una clave de 20 caracteres (160 bits) o de 63 caracteres (504 bits). Entre más larga será más difícil de descifrar, así como de recordar.

Fortaleza:

- No está limitado a una clave compartida; también puede usar una clave asignada a cada usuario e incluso puede usar un certificado SSL para autenticar el cliente con el AP.
- Tiene la posibilidad de usar rotación de claves en la misma sesión mediante el protocolo TKIP (siglas en inglés de Temporal Key Integrity Protocol), lo cual dificulta su desciframiento.
- En general, provee un nivel de autenticación y privacidad significativamente mejor que WEP.

Debilidad:

- Necesita una configuración laboriosa.
- Se necesita equipo de última generación y con su firmware actualizado para mejorar la interoperabilidad.
- Una baja fortaleza en las claves asignadas puede facilitar su desciframiento mediante ataques de diccionarios de claves.

3. Portal Cautivo: es una forma de autenticar por medio de un servidor web. Cuando el usuario entra a navegar, es redireccionado hacia el portal que le solicita sus credenciales (usuario y contraseña). Cuando es autenticado por el servidor, el usuario hace uso de los recursos de la red.

Fortaleza:

- Proporciona una mínima seguridad y desalienta a los usuarios poco experimentados a acceder a la red.
- Es ideal para sistemas de prepago, por ejemplo mediante el uso de tarjetas.

Debilidad:

- No utiliza encriptación, por lo que no es recomendable para redes que necesiten una seguridad fuerte. Es ideal para cibercafés, hoteles y otros lugares de acceso público.

G) Descripción de la debilidad de clave WEP

WEP, acrónimo de Wired Equivalency Protocol, es un sistema de cifrado incluido en 802.11 para cifrar las transmisiones y así proporcionar confidencialidad equivalente al cable. Este se basa en el algoritmo de cifrado de flujo RC4 con claves de 64 bits y 128 bits, el cual se caracteriza por ser sencillo de implementar y proporciona un cifrado veloz.

El algoritmo utiliza una clave de 40 bits o 104 bits, a los cuales se les agrega un Vector de Inicialización (VI) de 24 bits, completando de esa forma una clave de 64 bits o 128 bits. Luego esta clave se utiliza para cifrar los datos. La falla de seguridad radica en dos puntos:

1. La poca longitud de los vectores de inicialización.
2. La pésima aleatoriedad para generar los vectores.

Para simplificar la programación los fabricantes generan estos vectores de una forma no tan aleatoria, lo que facilita su desciframiento.

Debido a esto, muchos paquetes se cifran con el mismo vector de inicialización y el principio del ataque de desciframiento radica en encontrar dos textos planos cifrados con el mismo VI, a partir de los cuales, mediante ataques estadísticos y otras vulnerabilidades encontradas en el protocolo, se puede descifrar la clave en algunos minutos.

Estas vulnerabilidades fueron descubiertas por analistas criptográficos en el 2001 y la IEEE generó la corrección de dichas vulnerabilidades en la norma 802.11i, la cual dio base a los actuales sistemas de ciframiento WPA y WPA2.

A pesar de que la IEEE revocó el uso de WEP como sistema de cifrado en el 2004, desautorizando su uso, una gran mayoría de fabricantes de AP aún lo ofrecen en sus equipos como primera opción de seguridad, más que todo para mantener la compatibilidad con equipo fabricado antes de la fecha de revocación.

H) Descripción del ataque WEP

El protocolo WEP, a pesar de que la IEEE no recomienda su uso, en El Salvador, hay más de un operador de Internet cuyos equipos lo utilizan para cifrado. Se recomienda el uso de otros métodos de ciframiento como WPA o WPA2, ya que WEP sólo es un mecanismo de disuasión que no ofrece una protección real.
Para un ataque de este tipo de redes basadas en cifrado WEP hay suites de programas como "Aircrack" que contienen todas las herramientas para descifrar claves WEP. Incluso, hay imágenes ISO en Internet que contienen una versión LIVE de Linux (por ejemplo Backtrack) que cargan todas las herramientas al arrancar un CD o DVD quemado con dicha imagen.
Una de las suites más comunes es Aircrack (que viene en la imagen ISO de Backtrack), basa su ataque en tres pasos:

1. Captura de una gran cantidad de paquetes generados por la red inalámbrica.

2. Inyección de paquetes a la red para incrementar el tráfico (Ataque de envenenamiento de ARP).

3. Desciframiento de la clave WEP a partir de los paquetes capturados.

La descripción de cada una de las herramientas se muestra a continuación.

Una vez cargado Backtrack en la máquina virtual, se ejecutan estos comandos desde una línea de consola:

1. Airmon-ng: habilita y deshabilita la tarjeta de red.

2. Macchanger: cambia la MAC de la tarjeta WIFI.

3. Airodump-ng: para hacer un escaneo de las redes WIFI cercanas y capturar los paquetes de dichas redes guardándolo en un archivo.

4. Aireplay: inyecta paquetes en la red del AP escogido para aumentar el tráfico.

5. Aircrack: desencripta la contraseña WEP basado en el archivo capturado, como resultado muestra la clave de la red.

CONCLUSIONES Y RECOMENDACIONES

Medidas de seguridad
Como se puede concluir, todo tipo de mecanismo de seguridad tiene sus debilidades, pero siempre será mejor tener algún tipo de seguridad a no tenerla. La idea básica es persuadir a los posibles intrusos y dificultar el acceso a la red intrusivamente, facilitando el acceso a los usuarios de confianza. La seguridad, más que una regla específica es un conjunto de estrategias que de forma individual tienen un mayor o menor grado de

vulnerabilidad, pero que en conjunto pueden mantener la red mejor protegida.

Las medidas que se recomiendan son:

1. Asegurar el punto de acceso: todos los AP tienen un usuario y contraseña por defecto, la cual está documentada en Internet. Ésta es necesario cambiarla por una contraseña con gran fortaleza que mezcle letras mayúsculas, minúsculas, números y símbolos y con al menos 15 caracteres de longitud.

2. Usar encriptación WPA: entre más bits tenga la clave, mejor será. Requerirá configuración en los clientes. Si se utiliza una contraseña por equipo y rotación de contraseña con TKIP, la seguridad será mayor. Si no se usa la rotación entonces cambiar periódicamente las contraseñas.

3. Desactivar difusión SSID: requerirá mayor trabajo de soporte al usuario final y se necesitará un chequeo constante del espectro inalámbrico para evitar interferencia de APs vecinos, agregados posteriormente.

4. Activa el filtrado MAC: se requerirá introducir la tabla MAC en cada AP.

5. Desactivar DHCP: de esta forma, aunque se autentique un intruso, no obtendrá una dirección IP. Se debe limitar los clientes que se pueden conectar.

6. El administrador debe estar informado y actualizado con las últimas técnicas de hacking para implementar sus propias medidas de protección.

BREVE DESCRIPCIÓN DE LOS ESTÁNDARES INALÁMBRICOS

IEEE 802.11 – Estándar para redes inalámbricas con línea visual.

IEEE 802.11a – Estándar superior al 802.11b, pues permite velocidades teóricas máximas de hasta 54 Mbps, apoyándose en la banda de los 5GHz. A su vez, elimina el problema de las interferencias múltiples que existen en la banda de los 2,4 GHz (hornos microondas, teléfonos digitales DECT, BlueTooth). Es aplicada a una LAN inalámbrica. La especificación está aplicada a los sistemas de ATM (silgas en inglés de Asynchronous Transfer Mode) inalámbricos.

IEEE 802.11b – Extensión de 802.11 para proporcionar 11 Mbps usando DSSS. También conocido comúnmente como WIFI (Wireless Fidelity), término registrado y promulgado por la WECA (siglas en inglés de Wireless Ethernet Compatibility Alliance) para certificar productos IEEE 802.11b capaces de ínteroperar con los de otros fabricantes. Es el estándar más utilizado en las comunidades inalámbricas.

IEEE 802.11e – Estándar encargado de diferenciar entre video-voz-datos. Su único inconveniente es el encarecimiento de los equipos.

IEEE 802.11g – Utiliza la banda de 2,4 GHz, pero permite transmitir sobre ella a velocidades teóricas de 54 Mbps. Se consigue cambiando el modo de modulación de la señal, pasando de 'Complementary Code Keying' a 'Orthogonal Frequency Division Multiplexing'. Así, en vez de tener que adquirir tarjetas inalámbricas nuevas, bastaría con cambiar su firmware interno.

Bibliografía consultada

1. AGUIRRE, José Eduardo. Redes inalámbricas [en línea]. [Fecha de consulta: 18 julio 2012] Disponible en: http://www.ilustrados.com/tema/246/Redes-Inalambricas.html
2. GONZÁLEZ Fernández, Víctor R. La computadora como sistema de control manejo de puertos. Saber electrónica, 18 (5): 5-20, 2007. ISSN: 01884395.
3. HUIDOBRO Moya, José Manuel, MILLÁN Tejedor, Ramón Jesús y ROLDÁN Martínez, David. Tecnologías de las telecomunicaciones. Madrid: Creaciones Copyright, 2005. 552 p. ISBN: 8496300080.
4. JIMENO García, María Teresa, MIGUEZ Pérez, Carlos y MATAS García, Abel Mariano. Hacker: edición 2010. Madrid: Anaya Multimedia, 2010. 368 p. ISBN: 9788441527157
5. NICHOLS, Randall K, LEKKAS, Panos C. Seguridad para comunicaciones inalámbricas: redes, protocolos, criptografía y soluciones computadoras. México, D. F: McGraw-Hill, 2003. 563 p. ISBN: 9701047818
6. REDES inalámbricas en los países en desarrollo. 2ª. ed., por ROB Flickenger [et al.]. Canadá: Limenhouse Book Sprint Team. 2007. 334 p. ISNB: 9780977809356
7. YOUNG, G. O. Synthetic structure of industrial plastic (Book style with paper title and editor). En: PETERS, J. (ed) Plastics. vol. 3. 2nd. ed. New York, McGraw-Hill, 1964. pp. 15-64