Seguridad en Redes Inalámbricas (Wi-Fi)

Alumnos: Diego González (2503033-8)
Rodrigo Gutiérrez (2630022-3)
Universidad: Federico Santa María
Fecha: 26 de junio de 2009

Resumen

Debido a las características de las redes inalámbricas Wi-Fi, se hace sencillo capturar tráfico (Sniffing) que potencialmente puede ser descifrado y utilizado con fines diversos, por lo que se hace imprescindible la implementación de métodos para asegurar la no infiltración a la red; los ataques activos o pasivos. Para ello, se creó el sistema WEP, que al poco andar mostró sus falencias, lo que lo catalogó como método poco seguro. Para contrarrestar esto, fué creado un método mejorado llamado WPA, el cual cubría las fallas del anterior WEP. Posteriormente WPA2 salió como una actualización con mejoras de la anterior versión, pero la robustez de este método, hace que sea muy confiable, siempre y cuando se utilice correctamente tomando las precauciones para no ser víctima de un ataque. Estos dos métodos utilizan un algoritmo de encriptación de flujo llamado RC4; sus tópicos principales serán vistos posteriormente, al igual que WEP y WPA. También es importante mencionar las falencias de WEP, para poder entender el porque de su “marginación” de parte de los usuarios.

Finalmente, es necesario aconsejar respecto a lo que hay que tener en cuenta a la hora de configurar una red Wi-Fi para contar con la seguridad apropiada y así tener la confianza que sus datos que viajan por un medio inalámbrico, lleguen a destino sin ser vistos por otras personas.

Introducción

En los tiempos actuales, debido al rápido avance de la tecnología y a su vez, a la facilidad para adquirir conocimientos desde Internet, es necesario tomar resguardo de posibles situaciones que pudieren afectar nuestras redes; específicamente redes inalámbricas en que transitan datos (información) privada. Existen personas que están dispuestas a captar una señal con el fin de interceptar esa información y utilizarla con fines que potencialmente son maliciosos. Para evitar ello, fueron diseñados sistemas de seguridad específicos para redes Wi-Fi y algunos de ellos quedaron obsoletos, debido a personas que fueron capaces de vulnerar la seguridad que brindaban; WEP. Actualmente esta en uso WPA y WPA2, que son mejores sistemas, pero su durabilidad en el tiempo solo depende, pues hasta que se vulneren, no va haber urgencia en innovar al respecto. A continuación se mencionarán los conceptos importantes para poder entender mejor el tema de las redes y se explicarán sus funciones principales.

A continuación, se definen algunos términos y conceptos que sirven para crear una visión general del tema seguridad en redes inalámbricas.

Sniffing: Es la acción de captar tráfico de información, ya sea vía cable u inalámbrico. Para lograr esto el sniffer coloca la tarjeta de red o NIC en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos (ver niveles OSI) no son descartadas las tramas no destinadas a la MAC address de la tarjeta; de esta forma se puede capturar (esnifar) todo el tráfico que transita por la red.

Para conseguir este propósito, existen softwares diseñados con este fin. Se llaman packet sniffers. Existen packet sniffers para medios cableados como Ethernet/LAN y unos ejemplos de ello son Wireshark (anteriormente conocido como Ethereal), Ettercap, WinDump, WinSniffer, Hunt, Darkstat, traffic-vis, TCPDump, KSniffer) y también los hay para redes inalámbricas como Kismet o Network Stumbler.

Tipos de ataques

Pasivos: es cuando el intruso monitorea el tráfico en la red para apresar passwords u otra información para su uso ulterior.

Activos: el sniffer intercepta e interfiere el tráfico que fluye a través de la red, interactuando de manera engañosa con el protocolo de comunicación.

Dentro de la categoría de los activos, se encuentran los siguientes métodos.

Suplantación: Mediante un programa sniffer puede hacerse de MAC’s validas y por el trafico sabrá a qué horas debe conectarse para poder suplantar al usuario.
Re actuación: Inyectar en la red paquetes interceptados utilizando un sniffer para repetir operaciones que habían sido realizadas por el usuario legítimo.

Denegación de Servicio: El atacante puede generar interferencias hasta que se produzcan tantos errores en la transmisión que la velocidad caiga a extremos inaceptables o que la rede deje de operar en lo absoluto.

Ataque de diccionario: Es un método de cracking que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario. Los ataques de diccionario tienen pocas probabilidades de éxito con sistemas que emplean contraseñas fuertes con letras en mayúsculas y minúsculas mezcladas con números y con cualquier otro tipo de símbolos.

Ataque de fuerza bruta: se denomina a la manera de recuperar una clave probando todas las combinaciones posibles hasta hallar aquella que permite el acceso.

Conceptos netamente relacionados con Wi-Fi.

Agoritmo RC4

Inicialmente el algoritmo era un secreto registrado, pero en septiembre de 1994 una descripción del algoritmo fue posteada anónimanente en una lista de correo de Cypherpunks. En seguida pasó al grupo de correo sci.crypt y de ahí fue publicado en númerosos sitos de Internet. Este algoritmo genera un flujo pseudoaleatorio de bits (un keystream) que, para cifrar, se combina con el texto plano usando la función XOR como en cualquier Cifrado Vernam. La fase de descifrar el mensaje se realiza del mismo modo. La permutación se inicializa con una clave de longitud variable, habitualmente entre 40 y 256 bits usando un algoritmo de programación de claves (Key scheduling algorithm o KSA).

EAP

El Extensible Authentication Protocol o EAP es un protocolo que permite varios métodos de autenticación como EAP-MD5, EAP-TLS y otros métodos. Las modalidades de autenticación pueden ser por certificados de seguridad o por contraseñas.

SSID*

Service Set ID o SSID es un código alfanumérico que identifica una red inalámbrica. Cada fabricante utiliza un mismo código para sus componentes que fabrica. Usted debe alterar este nombre y deshabilitar la opción de " broadcast SSID" al punto de acceso para aumentar la seguridad de la red. Cuando el "broadcast SSID" está habilitado, el punto de acceso periódicamente envía el SSID de la red permitiendo que otros clientes puedan conectarse a la red. En redes de acceso público es deseable que se realice la propagación del SSID, para que cualquier persona pueda conectarse a la red. Como el SSID puede ser extraído del paquete transmitido a través de la técnica de "sniffing" no ofrece buena seguridad para la red. Aún así, se debe alterar el nombre para evitar que otros usen la misma red, accidentalmente.

RADIUS*

Remote Authentication Dial-In User Service es un patrón de encriptación de 128 bits propietaria. Sin embargo, está disponible sólo en algunos productos más costosos, debido a la adición de una capa extra de criptografía.

(*): Cita textual desde referencia.

MAC*

Medía Access Control o MAC, cada placa de red tiene su propio y único número de dirección MAC. De esta forma, es posible limitar el acceso a una red solamente a las placas cuyos números MAC estén especificados en una lista de acceso. Tiene la desventaja de exigir una mayor administración, pues necesita actualizar la lista de direcciones MAC cuando se cambia una computadora en la red o para proveer acceso a un visitante, o incluso en redes públicas. Otra desventaja se debe al hecho de poder alterar vía software el número MAC de la placa de red y emular un número válido con acceso a la red.

WEP*

Wired Equivalency Privacy o WEP. Como sugiere el nombre, este protocolo tiene la intención de suministrar el mismo nivel de privacidad de una red con cable. Es un protocolo de seguridad basado en el método de criptografía RC4 que utiliza criptografía de 64 bits o 128 bits. Ambas utilizan un vector de inicialización de 24 bits. Sin embargo, la clave secreta tiene una extensión de 40 bits o de 104 bits.

Todos los productos Wi-Fi soportan la criptografía de 64 bits, sin embargo no todos soportan la criptografía de 128 bits. Además de la criptografía, también utiliza un procedimiento de comprobación de redundancia cíclica en el patrón CRC-32, utilizado para verificar la integridad del paquete de datos. El WEP no protege la conexión por completo sino solamente el paquete de datos. El protocolo WEP no es totalmente intocable, pues ya existen programas capaces de quebrar las claves de criptografía en el caso de que la red sea monitorizada durante un tiempo considerable.

WPA*

Wi-Fi Protected Access o WPA fue elaborado para solucionar los problemas de seguridad del WEP. El WPA posee un protocolo denominado TKIP (Temporal Key Integrity Protocol) con un vector de inicialización de 48 bits y una criptografía de 128 bits. Con la utilización del TKIP la llave es alterada en cada paquete y sincronizada entre el cliente y el Access point, también hace uso de autenticación del usuario por un servidor central.

WPA2.*

Es una mejoría de WPA que utiliza el algoritmo de encriptación denominado AES (Advanced Encryption Standard).

(*): Cita textual desde referencia.

Configuración Segura Wi-Fi

♦Eliminar todos los valores predeterminados:

►SSID

►Contraseña de la aplicación de administración.

►Acceso al router desde de Internet.

♦Activar el cifrado de datos (128 bits).

♦Cerrar la red a dispositivos ajenos: ►Desactivar la difusión del SSID.

►Especificar lista de direcciones MAC permitidas.

♦Utilizar WPA/WPA2 (no WEP).

♦Autenticar los usuarios de manera individualizada.

♦Segregar el entorno Wi-fi:

►Proteccion por FW/VPN/IPS.

Conclusiones

Al realizar este proyecto, tratamos de dar una mirada global a los aspectos de seguridad que envuelven las redes inalámbricas. Nos hemos dado cuenta de la fragilidad de las redes inalámbricas y los perjuicios que se podrían ocasionar si es que alguien desease infiltrar una red. Tan sólo se necesita un notebook con antena para poder captar señales desde cientos de metros; no es necesario estar en el alcance de la señal emitida por el router. El snifer, por medio de una antena Wi-Fi unidireccional, puede hacer este cometido, incluso con una antena casera, dado que este tipo de antenas es sencillo de fabricar. Así que pensar en el hecho que la señal emitida por el router tiene pocos metros de alcance omnidireccional da seguridad y tranquilidad es un error, ya que podemos sufrir un ataque desde distancias mayores. Un método para resguardar la señal puede ser aislar las paredes, de tal modo que no salga de cierto perímetro, entre otros.

La gran mayoría de las redes Wi-Fi caseras poseen un mínimo de seguridad, dado que pocas personas se encargan de configurar un router o algún elemento preventivo; estos traen un pequeño manual que a veces no es suficiente y no toda la gente conoce como poder configurar una red inalámbrica.

Existen soluciones para evitar que esto ocurra, pero no es cosa de llegar y hacerlo, ya que se deben tener los conocimientos necesarios para llevar a cabo dicha tarea, porque quizás por tratar de evitar un mal genere otro peor.

En definitiva ningún método produce un 100% de efectividad, pues siempre habrá alguna mente que irá más allá de lo conocido y que podrá botar toda la seguridad que uno posea, pero hasta que ello ocurra, es mejor asegurarse de las posibles amenazas que circulan por la red.

Referencias.

- http://www.elhacker.net/manual_hacking_wireless.htm
- http://www.iec.csic.es/gonzalo/descargas/SeguridadWiFi.pdf
- http://es.tech-faq.com/wireless-security.shtml
- (*) http://www.informatica-hoy.com.ar/redes-inalambricas-wifi/Seguridad-en-redes-WIFI.php
- http://es.wikipedia.org