Seguridad en Redes Inalámbricas de Acceso Local Bajo Parámetros de Uso de Herramientas Libres

Security Access Local Wireless Network with Use of Free Tools

Juan Ballesteros[1 *], Fabián Chaparro[2]
[1] Universidad Santo Tomas, Colombia
2 Universidad Autónoma de Bucaramanga, Colombia

RESUMEN

En este documento se presenta una auditoria en redes bajo funcionamiento en protocolo IEEE 802.11xx, redes utilizadas para la comunicación entre dispositivos en casa y oficina para verificar la seguridad que garantizan las mismas; para este propósito se utilizó software libre que funciona bajo sistema operativo Linux, específicamente la suite de Aircrack; se presenta la auditoria a las redes que funcionan con encriptación WEP y WPA, populares y utilizadas en redes inalámbricas de este tipo; de manera transversal se muestran los diferentes tipos de ataques disponibles por mencionar sniffers, ataques de denegación de servicio y autenticaciones falsas con clonación de direcciones MAC, particularmente.

Palabras clave.- Wife, Welan, Inalámbrico, Wpa Wep.

ABSTRACT

In this paper we present an audit IEEE 802.11x networks to check how secure these networks are for use in the home and office, will be used for this purpose free software Linux with aircrack suite, tests were done for the 2 encryptions WEP and WPA these popular encryptions for security in wireless networks, also show different forms to develop attacks for example denial of service sniffers, fake authentication, etc. The dictionary attack is the most popular and will be the starting point for the audit, but it is important also to mention other equally effective methods to develop this attack.

Key words.- Wife, Wlan, Wireless, Wpa Wep.

1. INTRODUCCIÓN

El término red inalámbrica (Wireless network en inglés) [1], es un término que se utiliza en redes para designar la conexión de nodos sin necesidad de una conexión física (cables), la misma se presenta por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos a convenir bajo el protocolo de comunicación pertinente.

Una de las principales ventajas es la notable disminución de costos al despliegue de soluciones cableadas, ya que se elimina el uso del referente cable Ethernet y la disminución de conexiones físicas entre nodos; sin embargo no todo son ventajas, por otro lado se tiene una considerable desventaja derivada de la fácil vulnerabilidad en seguridad de la transmisión que requiere la implementación de políticas exigentes y robustas para evitar el ingreso a la infraestructura.

La conexión inalámbrica que se establece entre los usuarios remotos y una red proporcionan a las empresas flexibilidad y beneficios muy importantes como son movilidad y el poner en red equipos donde el acceso es difícil para desplegar soluciones cableadas. Uno de los principales problemas que tiene que afrontar una red Inalámbrica es la seguridad de la información que se transmite. El no contar con un medio guiado como el cable, en donde el acceso tiene que hacerse directamente sobre el medio físico acarrea, el permitir el tendiente fácil acceso a la información que viaja por el aire; por lo cual, usuarios no autorizados pueden tentativamente obtener dicha información y acceder a ella para obtener los beneficios derivados de políticas no robustas frente a procesos débiles de restricción.

* Corresponding
E-mail: juan.ballesteros@usantoto.edu.co

La flexibilidad y la movilidad que nos proporcionan estas redes inalámbricas han hecho que su utilización crezcadíaadía. En Colombiaparaelaño 2005 comenzó en firme la proliferación de este tipo de soluciones para la interconexión de información. Actualmente es común ver esta solución en el sector empresarial y en el hogar, derivado de la flexibilidad de instalación y uso donde no es necesario un medio físico directo proporcionado por cables, sumado a que ello conlleva el no detrimento en cuánto la estética y el ahorro de costos en cableado estructurado y adecuamiento locativo necesario para las instalaciones.

El presente documento muestra una investigación que relaciona la visión general del estado actual de la seguridad en las redes inalámbricas, particularmente las WLAN (Wireless Local Access Network), acompañada de estándares pertinentes y justificando la importancia en cuánto a la vulnerabilidad y riesgos para los usuarios que hacen uso de la misma, el objetivo de los autores no es concientizar a los usuarios sobre la supresión del uso de esta tecnología, por el contrario lo que se intenta es justificar e informar la importante necesidad de blindar las redes inalámbricas de las cuales hacen uso, para evitar la alteración y/o eliminación de la información que circula por estas redes de datos.

Lo que resta del artículo se organiza de la siguiente manera.

En la sección II se define el marco conceptual utilizado. En la sección III se caracterizan las principales debilidades de las redes inalámbricas, que será objeto de estudio para parametrizar los resultados de los escenarios propuestos de evaluación y obtención de resultados. Posteriormente en la sección IV se muestra el proceso de la auditoría bajo la suite Aircrack de Linux. La sección V describe los experimentos realizados y los resultados obtenidos para que finalmente en la sección VI se presenten las conclusiones del trabajo.

2. REFERENTES

Para Realizar una auditoria en redes WIFI en banda libre, generalmente de 2.4 GHz y verificar el grado de vulnerabilidad de las redes WLAN[2] bajo la caracterización de ataques de terceros y el uso de plataformas de uso libre, es necesario verificar el grado de seguridad de los tipos de encriptación como WEP y WPA [3] (los más usados), para determinar las vulnerabilidades de seguridad de estas llaves de encriptación.

En primera instancia se referencia WEP [3 y 1] (Wired Equivalent Protocol), como un sistema de encriptación propuesto por el comité de la IEEE 802.11, implementado en la capa MAC y soportado por la mayoría de vendedores de soluciones inalámbricas. WEP comprime y cifra los datos que se envían a través de las ondas de radio. La tarjeta de red encripta el cuerpo y el CRC (Cyclic redundancy check) de cada trama 802.11 antes de la transmisión utilizando el algoritmo de encriptación RC4 proporcionando por la RSA Security. La estación receptora, sea un punto de acceso o una estación cliente es la encargada de desencriptar la trama.

WEP especifica una llave secreta compartida de 40 - 64 bits para encriptar y desencriptar, utilizando la encriptación simétrica.

La vulnerabilidad de WEP reside en la insuficiente longitud del vector de inicialización y lo estáticas que permanecen las llaves del cifrado pudiendo no cambiar en mucho tiempo, por ejemplo si utilizamos solamente una llave de 24 bits.

WEP utiliza la misma llave para paquetes diferentes, lo cual acarrea el repetir a partir de cierto tiempo la transmisión continua, en este momento es cuando el intruso puede capturar suficientes tramas y determinar la llave compartida. En segundo momento los autores referencian WPA [3] (Wifi Protected Access), como un sistema desarrollado para proteger las redes inalámbricas, este protocolo intenta corregir las deficiencias del sistema previo WEP. WPA implementa el estándar IEEE 802.11i [4], creado por WIFI Alliance.

El funcionamiento de WPA se basa en la autenticación de usuarios mediante el uso de un servidor, donde se almacenan credenciales y contraseñas de los usuarios de la red, WPA permite la autenticación mediante clave precompartida que de un modo similar al WEP requiere introducir la misma clave en todos los equipos que quieran conectarse a la red. La ventaja de WPA frente a WEP es que la clave precompartida solo se envía una vez y no como en WEP, donde el envío de la llave es constante, podemos denominar a este proceso un "handshake" que correlaciona la negociación de apertura entre el cliente y el router para el intercambio de información.

3. PRINCIPALES DEBILIDADES EN REDES INALÁMBRICAS

En primera instancia se relacionan los ataques de escucha de monitorización pasiva [4]. La autenticación

es posible tras la captura y cracking de cierto número de paquetes y es posible accesar y monitorizar el tráfico presente en el entorno como cualquier cliente autenticado frente al access point. Análogamente también es posible realizar la inyección y modificación de mensajes sin necesidad de descifrar claves.
Desde otro referente encontramos los ataques de intercepción – inserción [4]. Los entornos que operan sobre el protocolo 802.11b facilitan la captura y redirección de sesiones, ya que una estación que transmite no es capaz de detectar la presencia de estaciones adyacentes con la misma dirección MAC ó IP, esto permite que se lleve a cabo un ataque de secuestro de sesión mediante el uso de dos estaciones hostiles diferentes, desde el S.O Windows tenemos programas como fake MAC para clonar la dirección física asociada a cada tarjeta de red y de esta manera ejecutar ataques.

Los ataques de denegación de servicio [8] sencillos de realizar, buscan afectar la disponibilidad en los entornos inalámbricos, pueden ser realizados desde varios enfoques como aquellos que utilizan un dispositivo de radiofrecuencia de alta potencia para generar interferencias, limitando al usuario legitimo en lo concerniente a la capacidad para utilizar el servicio.
Por último abordamos la interferencia propia de canales, las mismas se producen por ejemplo cuando otro dispositivo como un router WIFI ó dispositivo que se encuentre operando en la frecuencia de 2.4 o 5.8 GHz (dependiendo de la tecnología) interfiere en el canal que tiene seleccionado el primer Access Point, esto provoca reenvíos continuos de datos con lo que la conexión se pone lenta y en ocasiones se corta.

Cuando se está utilizando el protocolo IEEE 802.11n el problema puede ser aún peor, derivado del funcionamiento en que se basa el envío de múltiples ondas de radio en un punto de acceso para conseguir una mayor velocidad, en el momento en que una de ellas es interferida el resto no funciona de manera correcta [8].

4. AUDITORIA BAJO SUITE AIRCRACK

Para el desarrollo de la auditoria se tiene en cuenta las diferentes debilidades antes mencionadas para intentar vulnerar la seguridad, se generan pruebas para cada uno de los sistemas, en primera instancia en una red con encriptación WEP y luego bajo encriptación WPA.

Claramente la manera de realizar los ataques es muy similar; sin embargo, debido al algoritmo que utiliza la encriptación WPA, se parametriza la aplicación de procesos adicionales descritos en detalle más adelante.

Para hacer una auditoria, primero tiene que existir una tarjeta de red asociada al computador que tenga la capacidad de inyectar paquetes y ponerse en modo de escucha en el espectro electromagnético; para esta práctica se utilizará una tarjeta Air Span con chip realtek rtl8187l.

5. PROCEDIMIENTO

En primera instancia se describirá la auditoria con suite de aircrack utilizando encriptación WEP.

Se inicializa la tarjeta en modo monitor y se verifica la interface; podemos verificar la tecnología con la cual es compatible, en este caso podemos conectarnos a Access point con protocolos 802.11 a/b/g/n. El modo de configuración está configurado como administrador. La tasa de bit es consecuente con el protocolo de trabajo, por lo tanto caracteriza una tasa de transmisión soportado en ese instante de tiempo bajo el protocolo IEEE 802.11xx. Al encontrarse en

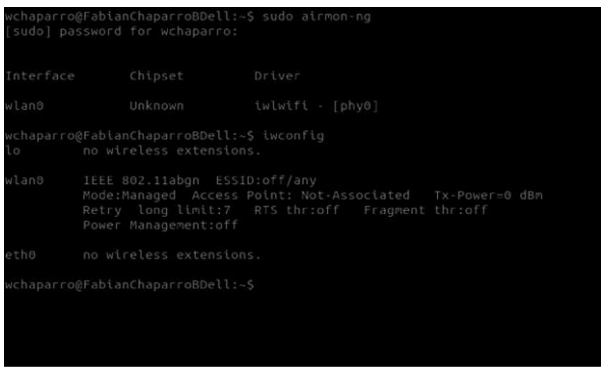

Figura 1. Interface asignada por wifiway para tarjeta de red externa.

reposo La potencia de transmisión es de 0 dBm. Estos parámetros mencionados y otros que respaldan el dispositivo se pueden observar en la Figura 1.

Luego de esto se hace un barrido para observar que redes están al alcance y bajo qué características de potencia; este valor es muy importante derivado que de él depende que la auditoria tenga éxito. Para realizar el procedimiento se recomienda ubicarse a una potencia no menor a 78 dBm que garantice conectividad. Por protección del presente documento se han etiquetado todos los access point escaneados para evitar atentar contra la seguridad de las redes capturadas en el análisis. Los parámetros mencionados se pueden observar en la Figura 2.

A continuación se relacionan las siglas que respaldan

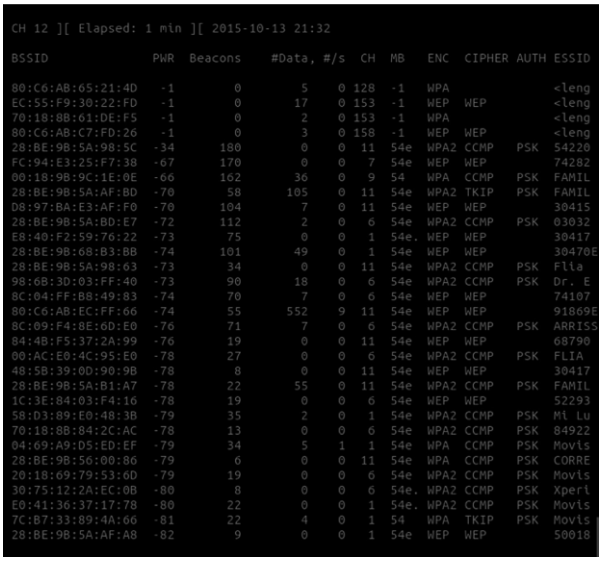

Figura 2. Escaneo redes cercanas.

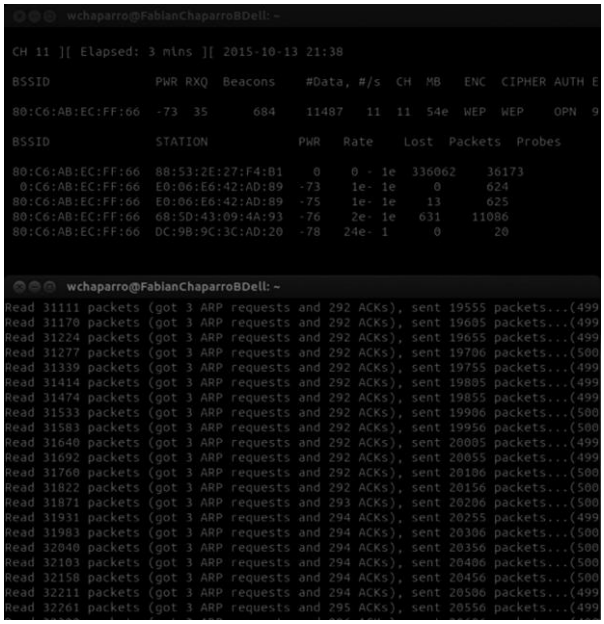

Figura 4. Autenticación falsa y peticiones ARP.

la terminología empleada en la auditoría.

AP: Access point, punto de acceso inalámbrico (router).
PWR: Potencia de Access point.
Beacons: son datos de anuncio emitidos por cada router
#Data: es la cantidad de tráfico generada por el cliente y el router
CH: canal por donde emite cada router datos a los clientes
MB: número de megabytes por segundo que admite el Access point
ENC: encriptación puede ser WEP WPA/WPA2 u open
AUTH: tipo de autenticación requerida por la red
ESSID: nombre de la red.

Una vez definida la red a la cual se le desea realizar la auditoría definida por la MAC del dispositivo y/o por el ESSID, se filtra la información de esa red a abordar, este procedimiento puede observarse en la Figura 3.

La imagen también permite representar la encriptación que utiliza, para ello correlaciona a WEP y el nivel de potencia en un valor de 70 dBm, que para los propósitos prácticos de auditoria son suficientes para modelar el entorno de evaluación.

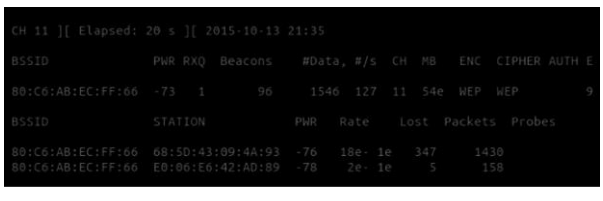

Figura 3. Filtrado de bssid en canal 11.

En la Figura 4 podemos ver la autenticación falsa y las peticiones ARP (Address Resolution Protocol), que para este momento están en 0.

Cuando existe tráfico entre el cliente legítimo y el punto de acceso, la autenticación falsa se ha hecho de manera correcta, esto puede parametrizarse en las peticiones que representan un crecimiento de manera significativa. [6].

En la Figura 5 se muestra como a medida que existe tráfico entre el cliente legítimo y el Access

Figura 5. Autenticación falsa y peticiones ARP.

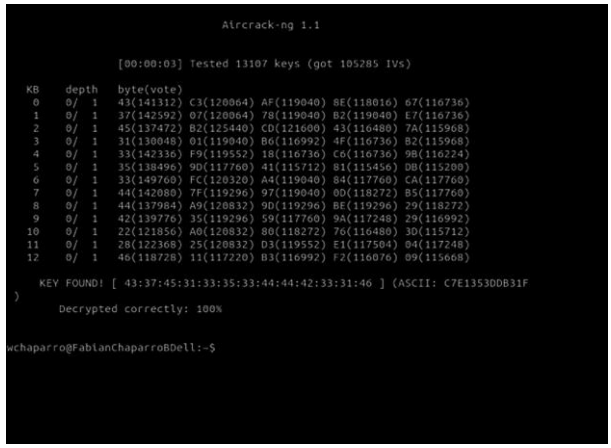

Figura 6. Contraseñas desencriptada.

Figura 7. Filtrado bssid y cliente legítimo conectado.

datos enviados), ejecutamos el comando aircrack-ng para descifrar la clave.

En la Figura 6 podemos ver la contraseña, para encontrar la llave es necesario capturar alrededor de 50.000 paquetes, recordemos que la encriptación WEP utiliza vector de inicialización para establecer los valores de encriptación y lo estáticas que permanecen las llaves del cifrado hacen que este sistema sea muy vulnerable; este procedimiento desde su inicio no tardo más de 4 minutos lo que indica que existen problemas serios en la seguridad utilizando WEP, claramente los datos de los usuarios que utilicen esta encriptación pueden ser potencialmente vulnerados y el robo de datos es algo inminente una vez se puedan efectuar simulaciones de usuario desde la capa 2 del modelo OSI (capa de enlace), donde conjugan parámetros de identificación física de los dispositivos de red y la interface o comunicación con los parámetros lógicos [7] de la infraestructura.

Para el proceso de auditoría de la suite aircrack bajo el uso del esquema de encriptación WPA, se utiliza un proceso similar al empleado en WEP; sin embargo, a diferencia de ella, para poder vulnerar WPA es necesario realizar un ataque de denegación de servicio y de esa manera hacer que el cliente legitimo se reautentique y capturar el handshake

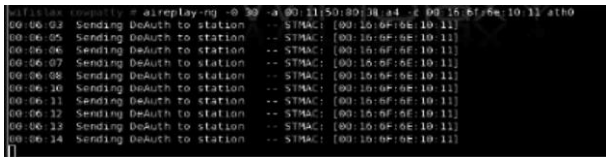

Figura 8. Ataque de denegación de servicio.

imprescindible para descifrar la pre chared key (llave compartida). A continuación se describen los pasos necesarios desarrollados para realizar la auditoria:

En la Figura 7 se muestra la MAC del Access point y MAC del cliente, para poder ver estos datos se está utilizando un ataque de monitorización pasiva (escucha).

Para poder realizar la auditoria en una red con encriptación WPA es indispensable que exista un cliente legitimo conectado de lo contrario no se podrá realizar el ataque.

Podemos notar en la Figura 8 el ataque de denegación de servicio. Para que este sea efectivo hay que tener

Figura 9. Handshake capturado luego de ataque de denegación de servicio.

Figura 10. Contraseña descubierta utilizando comparación con rainbow table.

point las peticiones ARP incrementan, (siempre que la autenticación falsa tenga éxito). Finalmente cuando los datos superen los 50.000 paquetes (En encriptación WEP la contraseña va en los paquetes de en cuenta dos variables, la primera que el nivel de potencia entre el Access Point y la tarjeta de red del cliente legítimo y el usuario intruso sean similares y así poder desconectar el router del cliente genuino,

la segunda es la cantidad de envíos de paquetes de des-autenticación para sacar de servicio al usuario legítimo. Se observa el handshake en la Figura 9, necesario para concluir la auditoria. Luego de esto se pueden utilizar diferentes maneras de comparar los caracteres para encontrar el passphrase (contraseña-llave), este procedimiento queda a decisión del auditor, para la presente auditoria se utilizara ataque por diccionario y el uso de la suite de aircrack, de esta forma aplicando el uso de un diccionario de 33GB y 10.245,698 palabras para encontrar el passphrase.

En la Figura 10, se observa el passphrase "pruebawpa" aplicando método por diccionario que no es más que comparar cada palabra con cada uno de los ficheros secuenciales donde en cada línea hay diferentes caracteres escritos.

Como normalmente las contraseñas WPA admiten como mínimo 8 caracteres y como máximo 64 suponiendo que la clave sea de 8 caracteres aproximadamente tendríamos 324.293.000.000.00 0.000.000.000 posibles combinaciones y se estaría hablando de años ininterrumpidos de procesamiento, para encontrar el passphrase. Si se utilizaran las letras del alfabeto y los números del 1 al 9 serian 36 caracteres y 221.073.919.720.733.357.899.776 palabras o combinaciones posibles suponiendo que el programa que estamos utilizando para comparar palabras y la capacidad de procesamiento del computador es de 200.000 palabras por segundo tardarían 3.505.104.000 años para encontrar dicha contraseña [5].

Toda la auditoria tardo un aproximado de seis (6) horas teniendoencuentaherramientasavanzadasparagenerar el rainbow table y dos (2) horas aproximadamente en comparar caracteres y descifrar el passphrase además de un computador con núcleos cuda con capacidad de procesamiento de 0.99 teraflop el cual agilizo de manera significativa el desarrollo de la auditoria.

Como observamos durante todo el procedimiento la encriptación WPA nos ofrece un método más seguro para proteger los datos en una red WIFI, al enviar la contraseña en el primer paquete, cuando el cliente se autentica nos obliga a tener un usuario legitimo para la desconexión del mismo; por medio de ataques de denegación de servicio y así capturar el handshake, en este punto ya son varias la fortalezas comparado con WEP, luego para descifrar la contraseña es necesario ataques por fuerza bruta, por diccionario, a partir de rainbow table o algunos otros métodos que lo vuelve aún más dispendioso para vulnerar la seguridad de una red que tenga este tipo de encriptación.

Sin embargo con las herramientas necesarias es posible violar los parámetros de seguridad y esto refleja agujeros de seguridad y confiabilidad que puede ofrecer esta encriptación.

De la misma manera y al igual que la encriptación WEP, WPA [9] no está exenta de monitorización pasiva (evidente en el momento de verificar el bssid y la MAC del router y la MAC del cliente legitimo) y ataques de denegación de servicio (desconexión del cliente y router para capturar handshake), el cual es el ataque más peligroso ya que además de permitir capturar el paquete con la contraseña, también puede dejar sin servicio de manera permanente y constante al cliente, si lo vemos desde un punto de vista corporativo este tipo de ataques pueden dejar fuera de servicio a una gran cantidad de abonados con desfavorables consecuencias de uso y de servicios.

6. CONCLUSIONES

Es evidente que la utilización de encriptación WEP deja casi al descubierto el tráfico de datos entre el cliente y el router y su vulneración es muy sencilla y rápida, así mismo sin importar el número de caracteres presentes en el passphrase no es un punto relevante; ya que por la arquitectura del diseño del sistema es un factor que no genera mayor seguridad a la red.

Es un problema muy grave en una red inalámbrica poder cambiar la dirección física de un dispositivo (MAC) y de esta manera hacer creer al router que es un cliente legítimo y entregar acceso a la red, así la creación de una tabla con las direcciones MAC para utilizar como medida de seguridad se descarta, sin embargo encontrar solución a este problema es muy complicado ya que no existe manera de controlarlo; bajo estos parámetros descritos, si alguien con malos propósitos quiere robar datos sensibles a una organización sin ser descubierto, el camino más favorable es clonar la MAC por la de un cliente legítimo y esto agilizará el proceso de una forma más inmediata y efectiva, en definitiva la encriptación WEP es obsoleta y no debe ser utilizada.

Si la intención de un atacante es dejar sin servicio de manera indefinida a los usuarios puede hacerse de manera sencilla aplicando un ataque de denegación de servicio. Si por limitaciones de Hardware o compatibilidad entre dispositivos la utilización de encriptación WEP es absolutamente necesaria una manera eficaz de brindar seguridad a la red es la utilización de una VPN, esta emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de usó público.

WPA nos ofrece un entorno más seguro para el envío de datos al ser absolutamente necesario la existencia de un cliente legitimo para capturar el handshake, imprescindible para encontrar el passphrase, además de la generación de diccionarios aleatorios el cual es el punto más dispendioso y en ocasiones si no se utiliza las herramientas adecuadas el resultado negativo en la intención de encontrar la contraseña; también el tener acceso a un computador con gran capacidad de procesamiento, esta coalición de variables hacen que WPA sea más robusta que su antecesora WEP, dejando claro que no es absolutamente invulnerable.

El uso de diccionarios presenta una forma sencilla y viable respecto a las otras formas de encontrar el passphrase, sin embargo, es fundamental la calidad y no la cantidad de trafico presente en la red, así asegura solamente el handshake es necesario para poder realizar el ataque utilizando este método que compara cada palabra con cada uno de los ficheros secuenciales donde en cada línea hay diferentes caracteres escritos, y solo dependerá del cliente verificar la seguridad de la red, al contrario de WEP donde nunca dependerá de la configuración ya que por definición y pruebas en este paper son por definición inseguras totalmente.

Así ninguna de la dos encriptaciones nos representa una solución absoluta de seguridad y tiene que ser complementadaconotrosfactores;podemosmencionar mecanismos de intercambio de clave dinámica aportado por los diferentes productos comerciales, teniendo en cuenta en no generar sobrecostos por cambio masivo de hardware; otro recurso disponible fácil de implementar y muy efectivo es inhabilitar DHCP para la red inalámbrica, teniendo IPs fijas, se garantiza que aun si la contraseña es descubierta pero no se conoce el rango de IPs en la red no se podrá acceder a la misma, actualizar periódicamente el firmware de los dispositivos inalámbricos ayuda a cubrir posibles agujeros, inhabilitar la emisión broadcast del SSID, además de utilizar programas de gestión de redes que sean capaces de detectar clientes nuevos, son puntos a favor para la correcta protección de los datos en una red inalámbrica.

En la actualidad los autores están buscando soluciones para mitigar los ataques a redes WIFI por terceros; se han realizado nuevas auditorías teniendo en cuenta el uso software libre y las investigaciones han arrojado los siguientes resultados:

La forma más viable y efectiva es la utilización de contraseñas que incluyan letras y números alternado mayúsculas y minúsculas junto con signos poco usuales, sin embargo no es una solución radical ya que con software especializado como Elcomsoft password recovery [10], se puede descifrar la contraseña, además los ataques de denegación de servicio y los ataques de escucha solamente se han podido contrarrestar utilizando Access point muy robustos que permiten trabajar en bandas de guarda donde las tarjetas de red ordinarias no pueden acceder; de la misma forma se ha encontrado una solución reduciendo el ancho de canal de 40Mhz a 10Mhz, sin embargo el uso de este hardware más robusto incrementa desmesuradamente los precios tanto de los equipos emisores como receptores, y en el momento de realizar la implementación no es viable.

REFERENCIAS

[1] Baghaei N, Engineering S and Zealand N 2004 *Performance Using Multiple Clients IEEE 2004* pp 2–6

[2] Khakurel S, Tiwary P K, Maskey N, Sachdeva G 2010 Security Vulnerabilities in IEEE 802.11 and Adaptive Encryption Technique for Better *Performance 2010 IEEE Symposium on Industrial Electronics and Applications* pp 207–210

[3] Xiao Y and Bandela C 2005 Vulnerabilities and Security Enhancements for the *IEEE Globecom 2005 proceedings* pp 1655–1659

[4] Gu J 2011 Research on WLAN Security Technology Based on IEEE 802 .11 *2011 3rd International Conference on Advanced Computer Control (ICACC 2011)* pp 234–237

[5] García M and Montalvo X Gestión de una red Lan Inalámbrica usando herramienta propietaria

[6] Ross J The Book of Wireless: A Painless Guide to Wi-Fi and Broadband Wireless

[7] Kipper G Wireless Crime and Forensic Investigation

[8] Wang Y, Zhigang Y and Zhao X Practical defense against WEP and WPA-PSK attack for WLAN

[9] Habibi A and Mansoori M Wired Equivalent Privacy (WEP) versus WIFI Protected Access (WPA)

[10] Elcom SoftCo.Ltd [Online]http://www.elcomsoft.com/company.html