Seguridad en Redes Inalámbricas de Acceso local bajo parámetros de uso de herramientas libres

Security in Wireless Local Access Networks under Free Tool Parameters

Juan Ballesteros[1] Fabián Chaparro[2]

[1] Facultad de Ingeniería Electrónica, Universidad Santo Tomas Colombia, Calle 19 # 11 – 64, Tunja – Colombia
[2] Facultad de Ingeniería Electrónica, Universidad Autónoma de Bucaramanga, {juan.ballesteros, william.chaparro}@usantoto.edu.co

Resúmen. En este paper 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 mimas; 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. Los autores desean referenciar las debilidades de las redes inalámbricas WLAN, sus vulnerabilidades, formas más comunes de ataque y finalmente correlacionar recomendaciones para mitigar los ataques presentados en el desarrollo del documento.

Palabras clave: WIFI, Wlan, Wireless, WPA, WPA, Seguridad en redes inalámbricas

Abstract. In this paper the authors present an audit IEEE 802.11x networks to check how secure are these networks for use in the home and office, It was use for this purpose free software Linux with aircrack suite, tests were done for the 2 encryptions WEP and WPA; they are popular encryptions for security in wireless networks, also show different forms to develop attacks; for example, denial of service, sniffers, fake authentication.

For make intrusion, 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. The authors wish to show the most important weaknesses when use wireless networks, attacks form and give someone recommendations for alleviate the attacks development in this paper.

Keywords: WIFI, Wlan, Wireless, WPA, WPA, security on wireless network

1 Introducción

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

El establecimiento de conexión inalámbrica entre usuarios y puntos de acceso en forma inalámbrica, 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, conlleva el potencial 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.

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 las redes de datos.

2 Hitos Tecnológicos

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 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. Lo anterior con el objetivo de determinar las vulnerabilidades de seguridad de estas llaves de encriptación [1][2].

En primera instancia se referencia WEP (Wired Equivalent Protocol), como un sistema de encriptación propuesto por el comité de la IEEE 802.11; 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, punto de acceso ó estación cliente es la encargada de desencriptar la trama [3] [4] [5].

WEP especifica una llave secreta compartida de 40 - 64 bits para encriptar y desencriptar, utiliza 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 [6].

WPA (Wifi Protected Access), sistema desarrollado para proteger las redes inalámbricas, corrige las deficiencias del sistema previo WEP. WPA implementa el estándar IEEE 802.11i, creado por WIFI Alliance.

WPA basa 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, 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, 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][4] [7].

3 Principales Debilidades en Redes Inalámbricas

En primera instancia se relacionan los ataques de escucha de monitorización pasiva. 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. [4] [7].

Los **ataques de intercepción – inserción**. Los entornos que operan sobre el protocolo 802.11b facilitan la captura y redirección de sesiones; lo anterior fundamentado en que una estación que transmite no es capaz de detectar la presencia de estaciones adyacentes con la misma dirección MAC ó IP, permitiendo que se lleve a cabo un ataque de secuestro de sesión [4] [7].

Los **ataques de denegación de servicio** buscan afectar la disponibilidad en los entornos inalámbricos, 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 [7] [8] [9].

4 Análisis y Resultados

El procedimiento desarrollado inicia la tarjeta en modo monitor y verifica la interface; podemos verificar la tecnología con la cual es compatible, bajo protocolo 802.11 a/b/g/n. El modo de configuración está 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 802.11. Al encontrarse en reposo, la potencia de transmisión es de 0dBm. Estos parámetros mencionados y otros que respaldan el dispositivo se pueden observar en la Fig.1.

```
wchaparro@FabianChaparroBDell:~$ sudo airmon-ng

Interface       Chipset         Driver

wlan0           Unknown         iwlwifi - [phy0]

wchaparro@FabianChaparroBDell:~$ iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11abgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

eth0      no wireless extensions.

wchaparro@FabianChaparroBDell:~$
```

Fig. 1. Interface asignada por wifiway para tarjeta de red externa, mostrando la parametrización del dispositivo.

Se hace un barrido para observar que redes están al alcance y bajo qué características de potencia; este valor es muy importante derivado en 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. Los parámetros mencionados se pueden observar en la Fig. 2. Definida la red de auditoría definida por la MAC del dispositivo y/o por el BSSID, se filtra la información de la red de análisis, este procedimiento puede observarse en la Fig. 3. Se representa la encriptación utilizada, se correlaciona WEP y el nivel de potencia en un valor de 70 dBm.

```
CH  9 ][ Elapsed: 48 s ][ 2015-11-30 13:40

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

28:BE:9B:5A:98:5C  -40      146      328    0   6  54e  WPA2 CCMP   PSK  54220280
D8:97:BA:E3:AF:F0  -67       75        0    0   1  54e  WEP  WEP         30415962
00:18:9B:9C:1E:0E  -70       94        0    0   9  54   WPA  CCMP   PSK  FAMILIA
28:BE:9B:5A:AF:BD  -72       94        1    0  11  54e  WPA2 TKIP   PSK  FAMILIA
28:BE:9B:5A:BD:E7  -73      102        0    0   6  54e  WPA2 CCMP   PSK  03032828
FC:94:E3:25:F7:38  -72       53        0    0   7  54e  WEP  WEP         74282609
1C:3E:84:03:F4:16  -73       83        0    0   6  54e  WEP  WEP         52293941
80:C6:AB:EC:FF:66  -73       83        0    0  11  54e  WEP  WEP         91869677
8C:09:F4:8E:6D:E0  -75       38        0    0   6  54e  WPA2 CCMP   PSK  ARRIS-6D
E0:41:36:6A:90:B0  -75       35        0    0   6  54e. WPA2 CCMP   PSK  Movistar
98:6B:3D:7B:1B:B0  -77       40       19    0   1  54e  WPA2 CCMP   PSK  ARRIS-1B
98:6B:3D:04:DB:A0  -76       39       23    0   1  54e  WPA2 CCMP   PSK  ARRIS-DB
20:18:69:79:53:6D  -76       40        2    0   6  54e  WPA2 CCMP   PSK  Movistar
8C:04:FF:B8:49:83  -76       42        0    0   6  54e  WEP  WEP         74107079
98:6B:3D:03:FF:40  -77       26        1    0   1  54e  WPA2 CCMP   PSK  Dr. ELIA
E8:40:F2:59:76:22  -77       34        0    0   1  54e. WEP  WEP         30417745
28:BE:9B:68:B3:BB  -77       25        0    0   1  54e  WEP  WEP         30470173
28:BE:9B:56:01:82  -78       31        0    0   1  54e  WEP  WEP         44245462
70:18:8B:61:DE:F5  -78       29        0    0  11  54e  WPA2 CCMP   PSK  82767831
58:D3:89:E0:48:3B  -78       34        2    0  11  54e  WPA2 CCMP   PSK  Mi Luna
00:AC:E0:4C:95:E0  -78       23        0    0   1  54e  WPA2 CCMP   PSK  FLIA DUR
80:C6:AB:65:21:5B  -79        8        0    0  11  54e  WEP  WEP         50740745
80:C6:AB:C7:FD:26  -80       11        0    0  11  54e  WEP  WEP         62245592
BC:85:56:9D:AF:6E  -80       11        0    0  11  54e  WEP  WEP         80202856
E0:41:36:37:17:78  -80       13        3    0   1  54e. WPA2 CCMP   PSK  Movistar
94:87:7C:FA:51:60  -81        2        0    0  11  54e  WPA2 CCMP   PSK  ARRIS-51
7C:B7:33:89:4A:66  -81        3        1    0   1  54   WPA  TKIP   PSK  Movistar
```

Fig. 2. Proceso de búsqueda de las posibles redes a realizar auditoría, mostrando el tipo de encriptación utilizada.

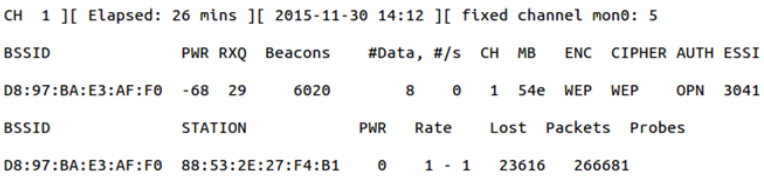

Fig. 3 Filtrado de canal a auditar mostrando la encriptación utilizada, el nivel de potencia.

En la Fig. 4 podemos ver la autenticación falsa y las peticiones ARP (Address Resolution Protocol). 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].

La Fig. 5 muestra como a medida que existe tráfico entre el cliente legítimo y el Access point las peticiones ARP incrementan. Finalmente cuando los datos superen los 50.000 paquetes ejecutamos el comando aircrack-ng para descifrar la clave.

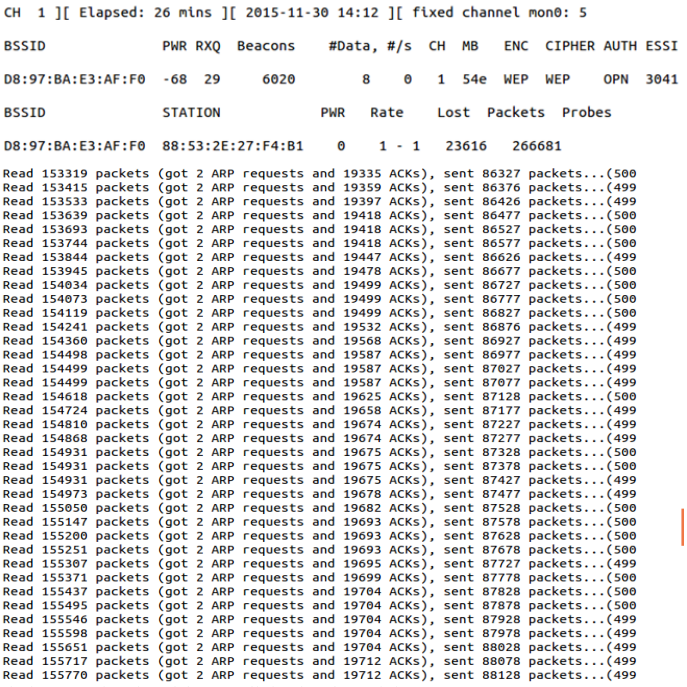

Fig. 4 Muestra de la autenticación falsa y solicitudes de peticiones ARP.

En la Fig. 6 se muestra la contraseña; el procedimiento tardo 4 minutos, indicador de 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) [7].

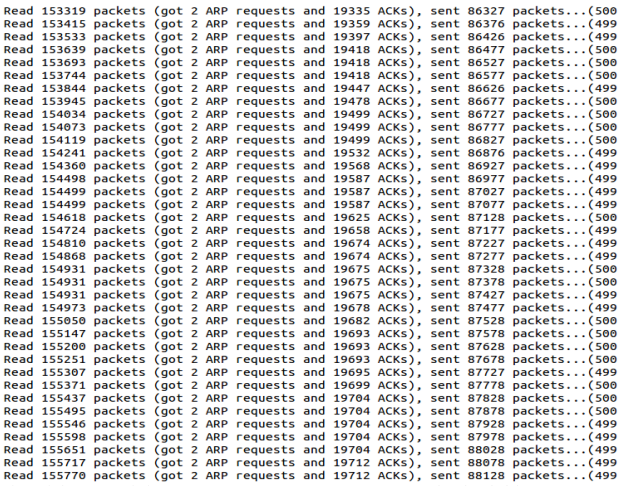

Fig. 5 Autenticación falsa y peticiones ARP en aumento como resultado del incremento del tráfico.

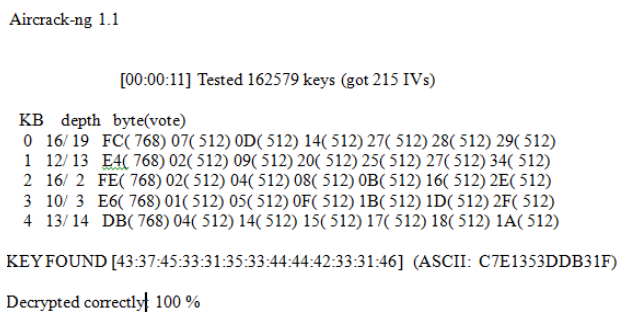

Fig. 6 Contraseñas desencriptadas.

Para el proceso de auditoría de la suite aircrack bajo el uso del esquema de encriptación WPA (Wireless Pprotect Access), se utiliza un proceso similar al empleado en WEP (Wired Encryption Protocol); sin embargo, a diferencia de ella, para poder vulnerar WPA es necesario realizar un ataque de denegación de servicio, un registro de comparación con un diccionario alfa númerico y de esta manera hacer que el cliente legitimo se re-autentique, capturando el handshake (llave de ingreso) imprescindible para descifrar la pre chared key (llave compartida).

Toda la auditoria tardo un aproximado de seis (6) horas teniendo en cuenta herramientas avanzadas para generar el rainbow table (tabla de equivalencias) y dos (2) horas aproximadamente en comparar caracteres y descifrar el passphrase (contraseña) 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 no está exenta de monitorización pasiva (evidente en el momento de verificar el BSSID (Base Service Set Identification) y la MAC (Media Access Control – Identificación física de la tarjeta de red) del router y la 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 [8] [9].

5 Conclusiones

La utilización de encriptación WEP deja al descubierto el tráfico de datos entre el cliente y el router. Su vulneración es muy sencilla y rápida, sin importar el número de caracteres presentes en el passphrase. La arquitectura del diseño del sistema es un factor que no genera mayor seguridad a la red.

El cambio de la dirección física de un dispositivo (MAC) es muy sencilla. De esta manera se emula en el router la legitimidad equivoca de usuario. La creación de una tabla con las direcciones MAC utilizada como medida de seguridad debe ser descartada. 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 legítimo para capturar el handshake. Por la estructura de su funcionamiento se requiere la implementación de un password con caracteristicas poco comunes, entre las principales se referencian la combinación de caracteres alfa-númericos sin relación lógica.

Ninguna de la dos encriptaciones nos representa una solución absoluta de seguridad y tiene que ser complementada con otros factores; podemos mencionar 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 (Dynamic Host Configuration Protocol) para la red inalámbrica, teniendo números de IP fijas, se garantiza que aún si la contraseña es descubierta pero no se conoce el rango de los números de IP en la red no se podrá acceder; actualizar periódicamente el firmware de los dispositivos inalámbricos ayuda a cubrir posibles agujeros, inhabilitar la emisión broadcast del SSID (Service Set Identification), 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. 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 El comsoft password recovery (software de recuperación de contraseñas), se puede descifrar la contraseña; 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 [9].

Referencias

1. Baghaei, N. y Hunt, R.: IEEE 802.11 wireless LAN security performance using multiple clients. Networks, 2004 (ICON 2004). Proceedings. 12th IEEE International Conference on. (2004) 299-303.
   doi: 10.1109/ICON.2004.1409151
2. Khakurel S., Tiwary P. K., Maskey N. y Sachdeva G.: Security Vulnerabilities in IEEE 802 .11 and Adaptive Encryption Technique for Better Performance. (2010) IEEE Symposium on Industrial Electronics and Applications (ISIEA 2010), 207–210.
3. Georgia S., Xiao Yang U. y Chaitanya B.: Vulnerabilities and Security Enhancements. IEEE Globecom 2005 proceedings, (2005) 1655–1659.
4. Gu J.: Research on WLAN Security Technology Based on IEEE 802.11. 3rd International Conference on Advanced Computer Control. (2011) 234–237.
5. García I., Montalvo M., Zavala X y Quezada L.: Gestión de una red Lan Inalámbrica usando herramienta propietaria. LITERATURA GRIS. CAMBIARLA. http://www.dspace.espol.edu.ec/xmlui/handle/123456789/1406
6. Ross J. The Book of Wireless: A Painless Guide to Wi-Fi and Broadband Wireless. 2 Edition. (2005)
7. Kipper G. : Wireless Crime and Forensic Investigation. Auerbach Publication. (2007)
8. Wang Y., Jin Z. y Zhao X.: Practical Defense against WEP and WPA-PSK Attack for WLAN. Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on. (2010) 1-4.
9. Lashkari A., Mansoor M., Danesh A.: Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). 2009 International Conference on Signal Processing Systems. (2009) 445-449.