Dyna
ISSN: 0012-7353
dyna@unalmed.edu.co
Universidad Nacional de Colombia
Colombia

Monsalve-Pulido, Julián Alberto; Aponte-Novoa, Fredy Andrés; Chaparro- Becerra, Fabián
Análisis de seguridad de una muestra de redes WLAN en la ciudad de Tunja, Boyacá, Colombia
Dyna, vol. 82, núm. 189, febrero, 2015, pp. 226-232
Universidad Nacional de Colombia
Medellín, Colombia

UNIVERSIDAD NACIONAL DE COLOMBIA
SEDE MEDELLÍN
FACULTAD DE MINAS

DYNA
http://dyna.medellin.unal.edu.co/

Security analysis of a WLAN network sample in Tunja, Boyacá, Colombia

Julián Alberto Monsalve-Pulido [a], Fredy Andrés Aponte-Novoa [b] & Fabián Chaparro- Becerra [c]

[a] *Centro de Investigaciones de Ingenierías Alberto Magno, Universidad Santo Tomás Tunja, Colombia. julian.monsalve@usantoto.edu.co*
[b] *Facultad de Ingeniería de Sistemas, Universidad Santo Tomás Tunja, Colombia. fredy.aponte@usantoto.edu.co*
[c] *Facultad de Ingeniería Electrónica, Universidad Santo Tomás Tunja, Colombia. william.chaparro@usantoto.edu.co*

Received: May 2th, de 2014. Received in revised form: October 31th, 2014. Accepted: November 19th, 2014

Abstract
This paper presents results of a safety analysis of WLAN networks in the city of Tunja, Boyacá Colombia, it is based on a random sample distributed in all over the City. The study is a research result of the project "diagnosis of technology security, applied to a sample of organizations in the city of Tunja". It was funded by the University of Santo Tomas Sectional Tunja. The information collected and analyzed was obtained through the techniques warchalking and Wardriving, in a meaningful representation of wireless networks from public, private, educational institutions and households located geographically in different parts of the city. As a result of the research it was demonstrated different risk levels regarding certain technology configurations of devices of the public, private and residential sectors, finally some conclusions and recommendations were made to enhance the level of security through good practice to configurational level and use of these networks.

Keywords: Networks, Security, Warchalking, Wardriving, Wep, Wlan, Wpa.

Análisis de seguridad de una muestra de redes WLAN en la ciudad de Tunja, Boyacá, Colombia

Resumen
Éste documento presenta resultados de un análisis de seguridad de redes WLAN en la ciudad de Tunja Boyacá Colombia basado en una muestra aleatoria distribuida en toda la Ciudad. El estudio es resultado de investigación del proyecto "Diagnóstico de seguridad informática aplicado a una muestra de organizaciones de la ciudad de Tunja" financiado por la Universidad Santo Tomás Seccional Tunja. La información recolectada y analizada se obtuvo mediante las técnicas Warchalking y Wardriving en una representación significativa de redes inalámbricas de empresas públicas, privadas, entidades educativas y hogares ubicados geográficamente en diferentes sectores de la ciudad. Como resultado de la investigación se demostró diferentes niveles de riesgo con respecto a configuraciones de tecnología de algunos dispositivos de entidades públicas, privadas y sectores residenciales, por último se realizaron algunas recomendaciones y conclusiones que mejorarán el nivel de seguridad por medio de buenas prácticas a nivel de configuración y uso de estas redes.

Palabras clave: Redes, Seguridad, Warchalking, Wardriving, Wep, Wlan, Wpa

1. Introducción

Las redes inalámbricas y particularmente las de acceso local buscan ofrecer parámetros de uso que conlleven a la flexibilidad en la forma de conexión y de uso, la movilidad, el impacto frente a la estética de instalaciones y el ahorro de infraestructura. Por otro lado las redes cableadas no ofrecen flexibilidad en conexión, pero son más seguras para cualquier organización. En Colombia para el año 2005 comenzó en firme la proliferación de redes inalámbricas para la interconexión de información.[1] Incentivos del gobierno como el Plan Vive Digital [2] y del sector privado a través de las grandes operadoras de servicios de telecomunicaciones, los cuales integran y respaldan la curva incremental de oferta/demanda de servicios telemáticos, donde las redes inalámbricas son el actor principal en la masificación del transporte de datos. Los nuevos estilos de vida acelerados y con dependencia tecnológica han llevado

a cambiar las formas de comunicación con un uso excesivo de dispositivos móviles y un aumento en la necesidad de conexión a redes inalámbricas [3]. Lo anterior lleva a la proliferación y masificación en la forma de conexión sea más rápida y transparente para el usuario final, sin detenerse a analizar la seguridad de las conexiones y la forma de interactuar con ellas. Además del uso en oficinas y en el hogar, las redes inalámbricas se hacen presentes en procesos de control en la industria, un ejemplo de esto es lo desarrollado en el proyecto "Sistema inalámbrico de monitorización para cultivos en invernadero" compuesto por una red de sensores inalámbricos, también llamada Wsn por sus siglas en inglés (Wireless Sensor Networks), red conformada por nodos sensores capaces de medir cambios en el ambiente, alMacenar la información y transmitirla al nodo vecino a través de redes multi-salto, para luego mostrar esta información al usuario en una interfaz gráfica. [4]

El uso de redes inalámbricas para la transmisión de datos tiene como principal característica la flexibilidad de uso derivado de la no conectividad física y la disminución de costos referente al despliegue de soluciones cableadas; sin embargo, estas redes están propensas a interferencias y errores de transmisión debido al tipo de bandas de frecuencias libres utilizadas. [5]

Es común encontrar redes Wlan [6] sin seguridad de acceso (abiertas) o con seguridad Wep (Wireless Encryption Protocol), lo cual representa una gran deficiencia en su estructura de seguridad y una vulnerabilidad fuertemente expuesta a ser atacada, las redes abiertas están expuestas a ser suplantadas fácilmente y las protegidas bajo Wep [6] son fuertemente vulnerables en su autenticación debido a que emplea una encriptación de 40 a 128 bits, que en la práctica representa un ataque en promedio de cuatro (4) minutos para lograr acceder a ellas [7]. Wpa (WiFi Protect Access) otro esquema de encriptación, aunque es más robusto en su esquema de seguridad, simplemente retarda el mecanismo de vulnerabilidad a un par de horas adicionales de procesamiento para encontrar la llave de acceso a la red; como solución y medida adoptada para la solución a estas deficiencias, la IEEE desarrollo una arquitectura de seguridad, especificada bajo el estándar IEEE 802.1x, particularmente el estándar IEEE 802.11i especifica cómo se implementa la seguridad en redes inalámbricas [8,9].

En los últimos años se desarrollaron diversos estándares de seguridad para las redes inalámbricas, en la práctica se encontraron razones de no utilización por parte de los usuarios, por limitantes en el hardware, configuración no adecuada, software desactualizado o por desconocimiento de los usuarios frente a las problemáticas y potenciales soluciones derivadas de las mismas. Lo anterior tiene consecuencias perjudiciales en la administración de estas redes, facilitando el ingreso de intrusos a la infraestructura de red y las vulnerabilidades que ello representa para la información que sobre ellas circula. Es importante reseñar que ningún sistema de seguridad es totalmente seguro y que cuando se usa el medio inalámbrico el riesgo aumenta con parámetros altamente significativos. El no disponer de un medio de conexión físico y de políticas de administración de seguridad eficientes en el plano de conectividad inalámbrico, conlleva a una potencial puerta de vulnerabilidad de acceso que se puede abrir con conocimientos mínimos de herramientas informáticas especializadas y por consiguiente el acceso a la información que circula por la red de datos o a la que se encuentra en los dispositivos que conformen la misma.

Se realizó un proceso de vigilancia tecnología en los temas de Warchalking y Wardriving en bases de datos Scopus e IEEE XPLORE donde se encuentra 26 trabajos en el área, se destaca un 69.2% de trabajos presentados en eventos científicos seguido con un 19.2% de artículos publicados en revistas investigativas, con un 11.4% repartido en revisiones, libros y conferencias. Por otro lado el mayor número de publicaciones se central en el año 2010 con 6 registros reduciéndose para el 2012 con 2 publicaciones, el 2013 con 4 y en el 2014 solo registrá 2 trabajos. Los países que más han registrado resultados en esta técnica se centran en los Estados Unidos con 14 trabajos, seguido con el Reino Unido con 5 trabajos, China con 3 trabajos y finalmente Francia con 2 trabajos.

El uso del método Wardriving tiene como objetivo en la investigación la obtención de datos de redes inalámbricas por medio de un vehículo en movimiento [10], utilizando dispositivos tradicionales como un Smartphone, Laptops o un Gps. Investigaciones como [11] analizar los datos Wardriving en Wcdma reales, Gsm y redes WiFi describe cómo el arrastre de la señal degrada su rendimiento para su posterior filtro y análisis. Por otro lado Warchalking es la definición de un lenguaje para marcar los puntos donde las personas pueden conectarse a una red inalámbrica abierta para hacer el uso del internet. Investigaciones como [12] relacionan una metodología de aplicación de Warchalking para las redes abiertas y los retos técnicos de seguridad que se deben tener en cuenta en las redes abiertas con propósito social no delictivo.

1.1. Referentes

Para realizar una auditoria en redes WiFi en la banda de frecuencia de 2.4 GHz y verificar el grado de vulnerabilidad y amenaza, se contempla la caracterización de ataques provenientes de terceros independientes a la infraestructura de red bajo la integración y uso de plataformas libres [13]. Para ello es necesario verificar el grado de seguridad de los tipos de encriptación mayormente utilizados como Wep y Wpa [14], permitiendo determinar las vulnerabilidades más esenciales de seguridad de estas llaves de encriptación.

Wep parametriza un sistema de encriptación propuesto por el comité IEEE 802.11 [15], se implementa en la capa Mac (Media Access Control), relacionado en la capa de enlace del modelo OSI. Wep comprime y cifra los datos que se envían a través de las ondas de radio. La tarjeta de red encripta el cuerpo de los paquetes de información y el CRC (Cyclic Redundancy Check) de cada trama 802.11 antes de la transmisión utilizando el algoritmo de encriptación RC4 proporcionando por The Security Division of EMC Corporation (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 ó 64 bits

para encriptar y desencriptar información, la misma utiliza la encriptación simétrica en su proceso [15]. La vulnerabilidad de Wep reside en la insuficiente longitud del vector de inicialización y lo estáticas que permanecen las llaves del cifrado [16,17].

Wep utiliza la misma llave para paquetes diferentes, lo cual lleva a repetir a partir de cierto tiempo la transmisión continua, en este momento es cuando el atacante puede capturar suficientes tramas y determinar la llave compartida.

Wpa es un sistema desarrollado para proteger las redes inalámbricas, este protocolo en principio fue desarrollado para intentar corregir las deficiencias del sistema previo Wep [14,15]. Wpa [18] implementa el estándar IEEE 802.11i [8,14] que mejora las debilidades más representativas presentes en su antecesor.

El funcionamiento de Wpa [19] se basa en la autenticación de usuarios mediante el uso de un servidor, para ello se almacenan credenciales y contraseñas de los usuarios de la red; Wpa permite la autenticación mediante clave pre-compartida al igual que Wep, ella requiere introducir la misma clave en todos los equipos que quieran conectarse a la red. La ventaja de Wpa [20] 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. En Wep [20] por su parte se captura la llave basado en que está viaja con los paquetes intercambiados entre router y usuario, Wpa [20], requiere de la comparación con un diccionario para asociar y encontrar relación directa con la llave intercambiada entre router y usuario, solo en el momento en que se inicia negociación de conexión.

1.2. Principales debilidades en Redes Wlan

Las redes Wlan presentan debilidades en la seguridad por la propagación de señales isotrópicas en el medio no guiado, en esta sección se van a relacionar algunos ataques que pueden tener este tipo de redes [7,14].

Los ataques de escucha de monitorización pasiva se realizan por medio de la autenticación mediante la captura y cracking de cierto número de paquetes, permitiendo acceder y realizar el monitoreo al tráfico presente en el entorno como cualquier cliente autenticado frente al punto de acceso. Análogamente también es posible realizar la inyección y modificación de mensajes sin necesidad de descifrar claves [7].

Los ataques de intercepción – inserción operan sobre el protocolo 802.11, facilitan la captura y redirección de sesiones, la estación que transmite no es capaz de detectar la presencia de estaciones adyacentes con la misma dirección Mac ó IP lo cual permite que se lleve a cabo un ataque de secuestro de sesión mediante el uso de dos estaciones hostiles diferentes; desde el Sistema Operativo Windows de Microsoft, tenemos herramientas de software como Fake Mac para clonar la dirección física asociada a cada tarjeta de red y de esta manera ejecutar ataques. Uno de los ejemplos para este tipo de ataques es realizar una auditoria con la suite de licencia de software libre Aircrack [21], en primer lugar se debe contar con una tarjeta de red asociada al computador que este en capacidad de inyectar paquetes y ponerse en modo de escucha en el espectro electromagnético.

Los ataques de denegación de servicio son relativamente 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, esto limitaría el usuario legítimo en lo concerniente a la capacidad para utilizar servicios primarios. Se referencia 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 limita su capacidad, ocasionando en algunas ocasiones caída completa del servicio. Cuando se está utilizando el protocolo IEEE 802.11n [22-24] 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.

2. Materiales y Métodos

Para esta investigación se analizaron 150 puntos de red WiFi utilizando técnicas como Warchalking y Wardriving [10] tomados en 17 diferentes lugares de la ciudad de Tunja. En la Fig. 1 se observa un mapa de la ciudad con la ubicación de los puntos donde se realizaron las muestras, cada uno de los sitios de muestreo identificados con letras

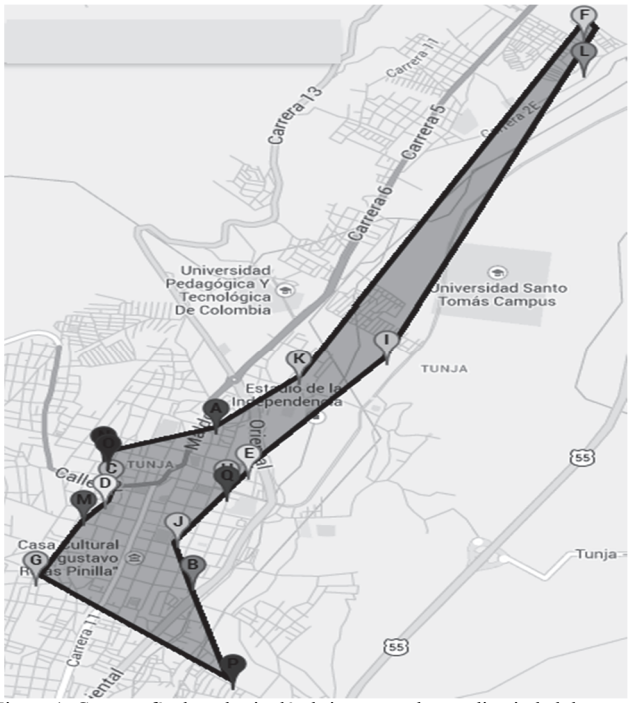

Figura 1. Cartografía de redes inalámbricas caso de estudio ciudad de Tunja.
Fuente: Autores

Tabla 1.
Información general en la toma de datos de redes Wlan en la ciudad de Tunja (Boyacá, Colombia) mediante técnicas de Warchalking y Wardriving.

Punto	Redes Hogar	Redes Comerciales	No ID	Zona
A	1	3	8	B. Maldonado
B	3	5	2	Terminal
C	2	2	1	Trav 16A No 20
D	1	2	1	Ed. Lumol
E	2	1	6	C. R Villa Cecilia
F	5	2	2	B. Suamox
G	3	1	5	B. Centenario
H	5	1	3	Plazoleta Muisca
I	1	27	0	Unicentro
J	2	4	2	Ed. California
K	0	2	1	Glorieta
L	2	0	1	Trav 2E - B. Muiscas
M	6	2	1	Cl 19 No 13
N	1	0	0	Cl 24 No 14
O	9	0	0	Cr 14 No 23
P	6	4	0	B. San Antonio
Q	6	0	6	Cr 7 No 23

Fuente: Los Autores

mayúsculas se encuentran acompañados de un número que representa la cantidad de puntos tomados en ese lugar. Tabla 1. En el proceso de parametrización de redes inalámbricas se utilizó la herramienta de software WiEye que en su fácil uso recolecta información importante para la investigación. A continuación, se muestra la Tabla 1 que correlaciona la información señalada.

Para completar la información en la toma de los datos, fue importante el anexo del geo-posicionamiento de cada uno de los puntos relacionados donde se utilizó la herramienta de software Gps Logger, ya que por su facilidad de uso y por su licencia de software libre, permitió gestionar un proceso de geo-localización dinámico.

Para cada uno de los puntos de red se capturó información como Ssid (Service Set IDentifier) o nombre de la red, Strength (fuerza de la señal), tipo de autenticación, cifrado y canal, además se identificó si la red corresponde a un hogar o a una entidad comercial. En la Fig. 2 se ilustra la agrupación de las redes por este parámetro, se puede observar que el 44% de las redes tienen relación con hogares, un 36% de las mismas con establecimientos comerciales, entre los que se encuentran Pymes, universidades, entidades estatales y privadas, y un 20% de estas redes no pudieron ser identificadas, debido a que presentan en su SSID nombres como "75711804", lo que por lo general está asociado hacia la identificación de abonados residenciales y/o pequeñas empresas.

La encriptación Wep utiliza un vector de inicialización para establecer los valores de la llave de seguridad (encriptación). La característica de estabilidad que permanecen en estas llaves posibilitan que el sistema sea vulnerable, en promedio el proceso de encontrar la llave de seguridad bajo parámetros Wep que no se extiende de cuatro (4) minutos aproximadamente, lo que correlaciona la existencia de problemas serios en este tipo de seguridad; los usuarios que utilicen el tipo de encriptación Wep pueden ser potencialmente vulnerados y la probabilidad del robo de información es alta [15,7]. Lo anterior fundamentado

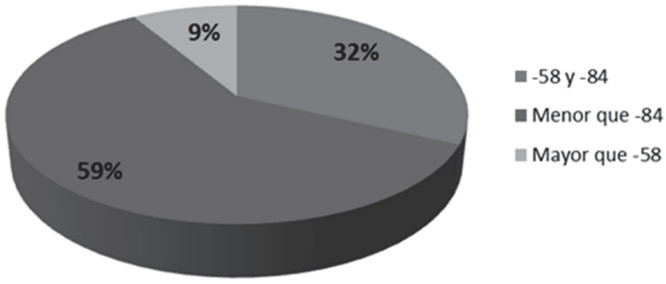

Figura 2. Tipos de redes.
Fuente: Autores

en la posibilidad de adoptar el rol de un usuario valido por parte de un atacante referenciado desde la puerta de la capa dos (2) de modelo OSI "capa de enlace", donde se integran y correlacionan parámetros de identificación física de los dispositivos de red y los parámetros lógicos de la infraestructura. En Wpa y sus respectivas configuraciones se utiliza un esquema similar al empleado en Wep [20]. A diferencia, su vulnerabilidad no es tan latente. Para realizar un ataque dentro de este esquema de seguridad es necesario realizar un ataque de denegación de servicio y de esta manera forzar al usuario para que se valide nuevamente, esto posibilitaría capturar el handshake [7], necesario para descifrar la llave precompartida.

El tiempo de captura en descifrar Wpa puede tardar aproximadamente 6 horas si no se dispone de un diccionario que permita comparar la llave de entrada con esta base de datos, Wpa nos ofrece un método más seguro para proteger los datos en una red WiFi este método es más trascendente ya que presenta forzamiento de la desconexión del usuario legitimo por medio de un ataque de denegación de servicio con el ánimo de capturar la llave precompartida, en este punto se correlaciona con un alto nivel de seguridad comparado con su predecesor Wep, además es necesario forzar la búsqueda de la llave en la comparación con el diccionario a partir de una búsqueda en la Rainbow Table (Tabla de Opciones) [18] .

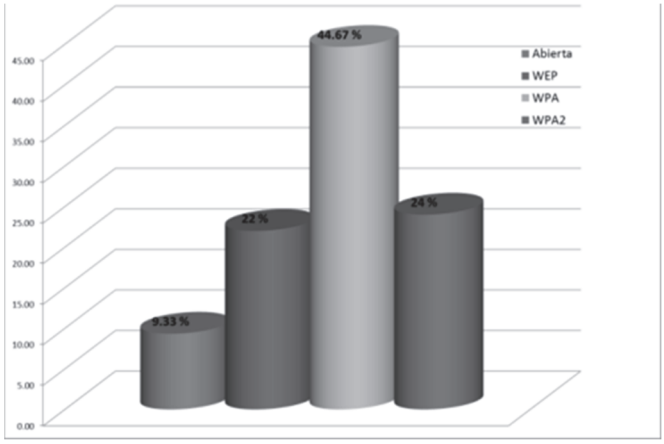

Figura 3. Distribución de la seguridad en Wlan.
Fuente: Autores

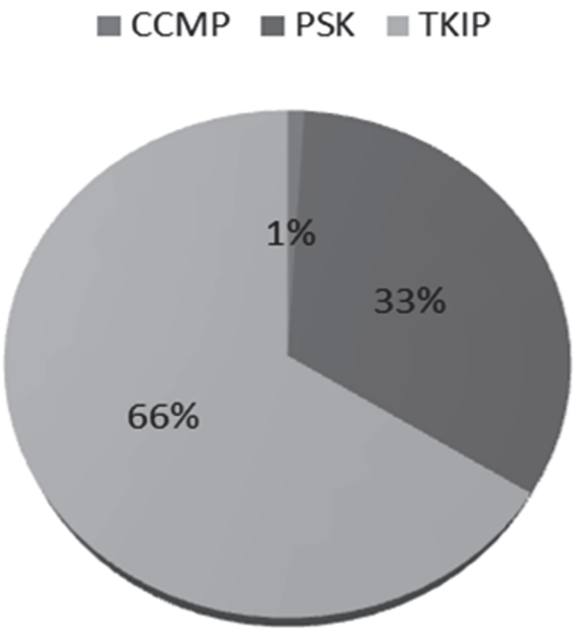

Figura 4. Distribución de la seguridad Cifrado Wpa.
Fuente: Autores

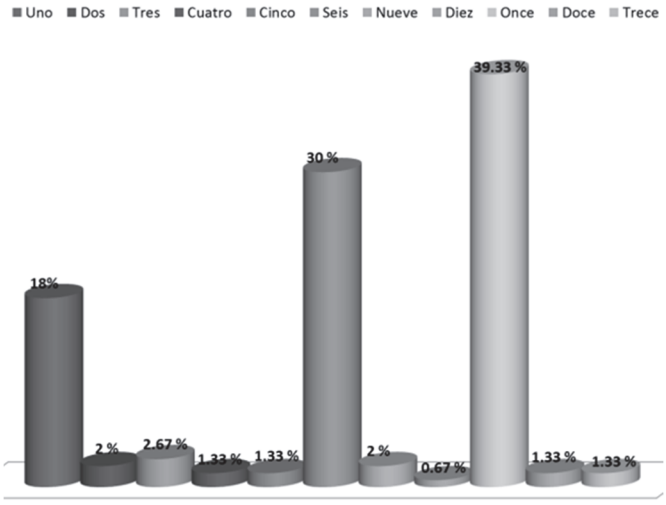

Figura 5. Canales utilizados.
Fuente: Autores

No importa el tipo de configuración que se use hoy en día, existen herramientas que permiten el acceso a redes privadas por medio de parámetros y agujeros que no hacen del todo robusta las llaves desarrolladas de encriptación, no ofrecen confiabilidad frente a lo que actualmente se encuentra desplegado en el ámbito comercial usado por la gran mayoría de usuarios convencionales (empresas, instituciones públicas y privadas y por supuesto a nivel residencial.)

De las redes analizadas se puede decir que un 68.67% se encuentran protegidas con autenticación Wpa, distribuidas en un 44,67% y Wpa2 en un 24%, por otro lado el 31.1% de las redes objeto de estudio presenta un nivel bajo de seguridad [5], representados en un 22% con autenticación Wep, mientras que el 9.33% restante no tienen algún tipo de autenticación, siendo vulnerables a ser atacadas, los anteriores datos se correlacionan en la Fig. 3.

De las redes que presentan autenticación Wpa y Wpa2 (68.67%) se presentan diferentes tipos de cifrado, en la Fig. 4 se observa que un 66% cuentan con cifrado TKIP, un 33% PSK y un 1% con cifrado CCMP [18].

Un factor importante a tener en cuenta en el rendimiento de una red WiFi es el canal utilizado, en la Fig. 5 se encuentra la distribución del uso de los canales en las redes analizadas.

Se identificó que los canales más usados son el uno (18%), el seis (30%) y predomina el canal once (39.33%), aunque esta distribución minimiza el efecto de interferencia derivado de consecuencias de interferencia co-canal, observamos que el mismo puede presentar limitante de área de cubrimiento, latencias, intermitencias y falta de estabilidad en el funcionamiento derivado de la sobrecarga de uso en los espectros de frecuencia que ocupan estos canales citados, especialmente el del canal número 11. Por lo anterior se recomienda a nuevos accesos y equipos instalados de cobertura inalámbrica nivelar el uso de canales a partir de la configuración del canal número 1 del espectro de frecuencias en el área metropolitana de la ciudad de Tunja y de esta forma caracterizar un adecuado sistema de multiplexación ortogonal de frecuencia que se disminuirá la sobrecarga por uso de canales comunes y de manera transversal el potencial efecto de traslapamiento de canales entre usuarios cercanos.

Otro aspecto importante a tener en cuenta al momento de verificar la vulnerabilidad de una red inalámbrica es el Strength (fuerza) o intensidad de la señal, si presenta valores entre -58 y -84 dBm es vulnerable a ser atacada, es más fácil la captura de paquetes handshake para efectuar ataques, caso contrario se presenta en valores inferiores a -84 dBm donde se expone a la presencia de pérdida de paquetes en la captura de datos y en el caso de valores superiores a – 58 dBm se dificulta capturar la información circundante en el espectro radioeléctrico. En la Fig. 6 se observa la distribución de las redes analizadas en el rango de estos valores de Strength, con lo cual podemos identificar que un 32% de los puntos de red capturados son sensibles a ser atacados.

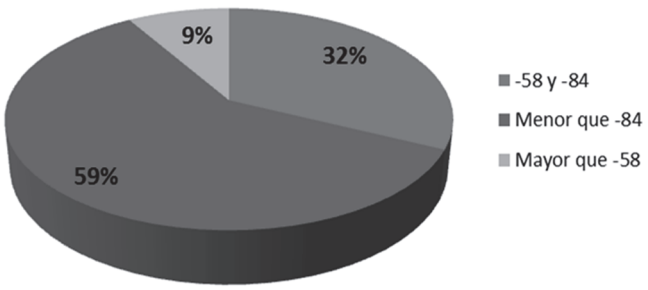

Figura 6. Porcentajes de intensidad de señal.
Fuente: Autores

La seguridad de una red WiFi depende de muchos factores, como son el tipo de autenticación, el cifrado entre otros. Actualmente existen en el mercado un gran número de dispositivos hardware y de software que permiten realizar ataques a este tipo de redes de una forma más efectiva, es por esto que se debe tomar medidas de seguridad robustas en nuestras redes de datos inalámbricas principalmente. Para evitar ser víctimas de ataques, a continuación se presentan algunas recomendaciones muy útiles para aumentar el grado de seguridad en redes Wlan.

3. Resultados

Ocultar el SSID en la configuración del Router es una buena práctica de seguridad para empresas y hogares, el nombre de la red Wifi queda invisible a la vista de atacantes, solo se puede conectar a la red las personas que conozcan el nombre de la red, esto puede ser bastante dispendioso para redes con alto volumen de usuarios pero para redes pequeñas pues ser una buena opción.

Otra práctica de seguridad es configurar el router para que solo acepte conexiones confiables de dispositivos previamente registrados con su respectiva MAC desde la administración del mismo. Los limitantes que existen es la administración permanente ya que se debe registrar cada dispositivo del usuario para la autorización de conexión. Es una buena opción para redes con crecimiento no exponencial. Aunque el filtrado por MAC usado para proteger las redes WiFi es una medida buena de seguridad, no es suficiente ya que existen muchas herramientas que permiten cambiar la dirección MAC del equipo atacante para emular el de un cliente legítimo.

Es recomendable utilizar contraseñas fáciles de recordar pero difíciles de adivinar, se recomienda contraseñas donde se utilice combinación de letras, números junto con caracteres especiales como el # ó @.

En las organizaciones empresariales públicas o privadas la administración de la red inalámbrica siempre va ser de gran importancia para cuidar los activos del negocio, se recomienda una administración basada en estándares como ISO 27000 donde proponen prácticas certificadas para la administración de usuarios en redes inalámbricas, donde el uso de cortafuegos, directorios activos, LDAP, proxys, autenticaciones seguras deben correlacionarse para reducir los riesgos.

Para los usuarios comunes que buscan redes en cualquier lugar para usar el servicio de internet, se recomienda desconfiar siempre si no es una red conocida, no todas están abiertas por desconocimiento de seguridad, la gran mayoría son creadas con un fin delictivo, ya que estas redes públicas abiertas están dispuestas a capturar información de usuarios y nos exponemos a posibles ataques permitiendo que la información como contraseñas, historiales de navegación y demás sean vistos y hurtados por los delincuentes. Ninguno de los esquemas de seguridad representa una solución completa, estos se deben fortalecer o combinar con otras prácticas como por ejemplo el intercambio de clave dinámica, eliminando el direccionamiento dinámico DHCP forzando las maquinas a tener IP´s fijas (estáticas), garantizando que aún si la contraseña es descubierta pero no se conoce el rango de direccionamiento, no se podrá acceder a la misma; actualizar el firmware de los dispositivos inalámbricos, inhabilitar la difusión abierta del SSID, así como utilizar programas de gestión de redes que sean capaces de detectar clientes nuevos. Por lo anterior se correlacionan dentro de premisa a favor para la correcta protección de acceso en una red inalámbrica de datos.

4. Conclusiones

Se identificó que el 9,33% de las redes Wlan no cuentan con mecanismos de autenticación, mientras que el 22% de las mismas presentan autenticación Wep, lo que representa que el 31.1% de las redes son vulnerables a ser atacadas, por consiguiente se requiere de que los dueños de estas redes aumenten su seguridad para disminuir el nivel de exposición.

El estudio evidenció malas prácticas de configuraciones en las redes inalámbricas en el área de estudio (Tunja - Boyacá – Colombia), en el análisis en las configuraciones se muestra un desconocimiento por parte de los administradores o los proveedores de servicio de internet aumentando los riesgos de ataques desde el exterior de las organizaciones o hogares y exponiendo datos importantes empresariales o personales.

Las redes inalámbricas con baja seguridad se centran en sectores concurrentes, como por ejemplo centros comerciales y sectores con alta presencia de personas. Se identificó un riesgo alto de exposición debido a que los delincuentes pueden tener una ubicación física sin despertar sospechas en cualquier sitio público, es importante recordar que la calidad en la receptividad de la señal es fundamental para iniciar un ataque y por consiguiente se debe estructurar planes de cobertura descentralizada inteligente y no forzar la radiación en un área demasiado extensa que exceda los límites físicos de la empresa o hogar ya que se convierte en puntos fáciles de acceso por parte atacantes a la infraestructura de comunicación.

Referencias

[1] Rodrigo, C., Avanzando en la seguridad de las redes Wifi. Enfoques [Online]. 73, pp. 23-32, 2005. [date of reference January 25th of 2014]. Available at: http://www.rediris.es/difusion/publicaciones/boletin/73/ENFOQUE1.pdf

[2] Ministerio de las Tecnologias de la Información y las Comunicaciones. [en línea]. MinTic, 2010. [consulta, 10 de febrero de 2014]. Available at: http://www.mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-6106.html

[3] Khetarpal, R. and Dronamraju, S., SMART—A Solution for Managing, the capacity, growth, and performance of wireless networks. IEEE - Bell Labs Technical Journal, pp. 182-193, 1997.

[4] Cama-Pinto, A., Gil-Montoya F., Gómez-López, J., García-Cruz, A. and Manzano-Agugliaro, F., Wireless surveillance sytem for greenhouse crops, DYNA, 81 (184), pp. 164-170, 2014.

[5] Tao, C., Lijun, C. and Tracey, H., Distributed optimization in wieless networks using broadcast advantage. Proceedings of the 46th IEEE Conference on Decision and Control, pp. 5839-5844. 2007.

[6] Sheldon, F.T. and Weber, J.M., Seong-Moo, Y. and Pan, W.D., The insecurity of wireless networks. Security & Privacy, IEEE, 10, pp. 54-61. 2012.

[7] Ballesteros, C.J. y Chaparro, F., Seguridad en redes inalámbricas de acceso local bajo parámetros de uso de herramientas libres. Congreso Internacional de Investigación en Ingeniería de Sistemas,1, pp. 1-6. 2014.
[8] Molina, J.M., Seguridad en redes inalámbricas 802.11. Sistemas & Telemática, 1, pp. 13-28. 2004.
[9] Han, J.A., Lee, J.B., Kwon, T.A., Jo, D.C., Ha, T.D. and Choi, Y.A., How to mitigate signal dragging during wardriving. IEEE Pervasive Computing, 9, pp. 20-27. 2010.
[10] Battiti, R., Cigno, R.L., Sabel, M., Orava, F. and Pehrson, B., Wireless LANs: From warchalking to open access networks. Mobile Networks and Applications, 10, pp. 275-287. 2005.
[11] Jinyoung, H., Jeongkeun, L., Kwon, T,. Daehyung J., Taejoon H. and Yanghee C., How to mitigate signal dragging during wardriving, Pervasive Computing, IEEE, 9 (1), pp. 20-27, 2010. http://doi:10.1109/MPRV.2010.6
[12] Battiti, R., Lo-Cigno, R., Sabel, M., Orava, F. and Pehrson, B., Wireless LANs: From WarChalking to open access networks, Mobile Networks and Applications, 10 (3), pp. 275-287, 2005. http://doi:10.1007/s11036-005-6422-4
[13] Khakurel, S., Tiwary, P.K., Maskey, N. and Sachdeva, G., Security vulnerabilities in IEEE 802.11 and adaptive encryption technique for better performance, Industrial Electronics & Applications (ISIEA), 2010 IEEE Symposium on, pp. 207-210, 2010. http://doi:10.1109/ISIEA.2010.5679467
[14] Bandela-Chaitanya, X.Y., Vulnerabilities and Security Enhancements for the wireless networks. IEEE Globecom 2005 proceedings,1 (1), pp. 1655-1659. 2005.
[15] Lashkari, A., Danesh, M. and Samadi, B., A survey on wireless security protocols (WEP, WPA and WPA2/802.11i), Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on, pp.48-52, 2009. http://doi:10.1109/ICCSIT.2009.5234856
[16] Reddy, S., Sai, R., Rijutha, K., Ali, S.M. and Reddy, C.P., Wireless hacking - a WiFi hack by cracking WEP, Education Technology and Computer (ICETC), 2010 2nd International Conference on, pp. V1-189-V1-193, 2010. http://doi:10.1109/ICETC.2010.5529269
[17] Kavka, O., Garasym, I. and Dudykevych, V., The analyse of wireless communication encryption technologies. Modificated WEP protocol, Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), 2010 International Conference, pp.186-187, 2010.
[18] Xiaona, L., Shaoqing, M. and Kaining, Lu., Security issues and solutions of WPA encrypted public wireless Local Area Network, Multimedia Technology (ICMT), 2011 International Conference on, pp. 3655-3657, 2011. http://doi:10.1109/ICMT.2011.6002258
[19] Lei, Z., Jiang, Y., Zugao, D. and Renfei, Z., The security analysis of WPA encryption in wireless network, Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, pp. 1563-1567, 2012. http://doi:10.1109/CECNet.2012.6202145
[20] Lashkari, A., Mansoor, M. and Danesh, A., Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA), 2009 International Conference on Signal Processing Systems, pp. 445-449, 2009. http://doi:10.1109/ICSPS.2009.87
[21] Aircrack-ng. [en línea]. [consulta, 1 de Agosto de 2013]. Available at: http://www.aircrack-ng.org
[22] Mohamed, E.M., Kinoshita, D., Mitsunaga, K., Higa, Y. and Furukawa, H., IEEE 802.11n based wireless backhaul enabled by Dual Channel IPT (DCH-IPT) relaying protocol, Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on, pp. 525-530, 2010. http://doi:10.1109/ICUMT.2010.5676587
[23] Arslan, M., Pelechrinis, K., Broustis, I., Singh, S., Krishnamurthy, S., Addepalli, S. and Papagiannaki, K., ACORN: An auto-configuration framework for 802.11n WLANs, Networking, IEEE/ACM Transactions on, 21 (3), pp. 896-909, 2013. http://doi:10.1109/TNET.2012.2218125
[24] Mohamed, E., Kinoshita, D., Mitsunaga, K., Higa, Y. and Furukawa, H., MIMO wireless backhaul enabled by IPT forwarding, Telecommunications (ICT), 2010 IEEE 17th International Conference on, pp. 763-770, 2010. http://doi:10.1109/ICTEL.2010.5478810

J.A. Monsalve-Pulido, received the Bs. Eng. in Systems in 2005, a MSc. in Free Software in 2008, from the Universidad Autónoma de Bucaramanga, Colombia and the Universitat Oberta de Catalunya. Spain. Currently he works as a research professor in the Systems Engineering Faculty at the Universidad de Santo Tomás, Tunja, Colombia, he is a leader of the research group GIBRANT and director of engineering research group Alberto Magno. His research areas are information systems and learning networks . His research interests included; software engineering, computer security, free software and data mining

F.A. Aponte-Novoa, received the Bs. Eng. in Systems and Computing in 2006, from the Universidad Pedagogica y Tecnologica de Colombia, a MSc. in Free Software in 2011 from the Universidad Autónoma de Bucaramanga, Colombia and the Universitat Oberta de Catalunya, Spain. From 2007 to 2011, he worked as a teacher for the System Engineering Program at Universidad Pedagógica y Tecnológica de Colombia. From September 2008 to date he has worked as a teacher at System Engineering Program at Universidad Santo Tomas, Tunja, Colombia. His research interests include: Information Systems, Learning networks and communication networks.

F. Chaparro-Becerra, received the Bs. Eng in Electronics Engineering in 2005 and the Sp. degree in Network Communications in 2010, both from the Universidad Santo Tomás, Colombia, and the MSc. in Telematics in 2013, from Universidad Autónoma de Bucaramanga, Colombia. He has experience in the public and private sectors in the Instituto Nacional Penitenciario and Carcelario de Colombia INPEC (2005-2006), Empresa de Teléfonos de Bogotá – ETB (2007-2008), dedicated of university academy since 2008, he is a member of the research group GIDINT, attached to the Universidad Santo Tomás, Colombia. His research interests include: networking, IPTV, Available Bandwith Estimation, and NetFPGA.