Artículo **Revista de Tecnología Informática**
Septiembre 2017 Vol.1 No.2 32-40

Análisis de vulnerabilidades en redes inalámbricas instaladas en diversos municipios del Estado de Hidalgo

GONZÁLEZ-MARRÓN, David†, PÉREZ-HERNÁNDEZ, Iridian, MARQUÉZ-CALLEJAS, Alejandro y BADILLO-PAREDES, Leonardo

Instituto Tecnológico de Pachuca, Felipe Angeles Km. 84.5, Venta Prieta, 42083 Pachuca de Soto, Hgo., México

Recibido Julio 27, 2017; Aceptado Septiembre 21, 2017

Resumen

En este artículo se muestra un análisis de vulnerabilidades con información recolectada en diferentes APs (access points) conectados a una red WiFi localizados en diversos municipios del estado de Hidalgo, México, identificando el nivel de seguridad inalámbrica implementada en los equipos instalados. La recolección de información se realiza utilizando la técnica de Wardriving, la cual nos muestra las características de conexión utilizadas, ubicación física y nombre asignado a cada dispositivo. Se realiza un muestreo en diversas municipios del estado y se seleccionan los atributos relacionados con la seguridad y ubicación mediante el proceso ETL (Extracción, Transformación y Cargado) , se realiza el proceso de minería de datos para obtener estadísticas de seguridad existentes en los diversos municipios analizados, se reportan los hallazgos obtenidos de forma gráfica y tabular, proporcionando el perfil de riesgos de equipos actuales en base a la evolución de las herramientas de análisis de vulnerabilidades actuales, concluyendo con predicciones acerca de la seguridad inalámbrica dentro del Estado de Hidalgo.

Wardriving, seguridad informática, minería de datos, criptografia

Abstract

This article describes a vulnerability analysis with information collected from different access points for Internet interconnection located in different municipalities of the state of Hidalgo, Mexico. The level of wireless security implemented in the installed equipment is identified. The collection of information is done using the Wardriving technique, which shows the connection characteristics used, physical location and name assigned to each device. A sampling is carried out in several municipalities of the state and the attributes related to security and location are selected by means of the ETL process (Extraction, Transformation and Loading), it is realized the data mining process which allows to obtain existing security statistics in the several municipalities analyzed using diverse methods of data analysis, reporting the findings obtained in a graphical and tabular way, providing the risk profile of current equipment based on the evolution of the analysis tools of Current vulnerabilities and concluding with predictions about wireless security within the State of Hidalgo.

Wardriving, information security, data mining, criptography

Citación: GONZÁLEZ-MARRÓN, David, PÉREZ-HERNÁNDEZ, Iridian, MARQUÉZ-CALLEJAS, Alejandro y BADILLO-PAREDES, Leonardo. Análisis de vulnerabilidades en redes inalámbricas instaladas en diversos municipios del Estado de Hidalgo. Revista de Tecnología Informática 2017, 1-2: 32-40

† Investigador contribuyendo como primer autor.

Introducción

Considerando el gran auge que ha tenido internet en los últimos años es notable el incremento y el fácil acceso a éste.

La tecnología Wi-Fi (Wireless Fidelity) es una de las tecnologías líder en la comunicación inalámbrica, incorporandose en cada vez más aparatos portátiles. Pero un aspecto que en ocasiones pasa desapercibido es la seguridad [1].

Tomando en cuentan a la población total en México en el año 2016 se determinó que el 59.5% tiene acceso a internet [2], al ser un número considerable de usuarios conectados, se toma en cuenta cierto tráfico en la red incluyendo información de todo tipo que se transmite al navegar por este medio, en la Gráfica 1 se muestra el aumento que ha tenido internet en los hogares de México desde el año 2013 al 2016.

Gráfico 1 Hogares con conexión a Internet, INEGI. Modulo sobre disponibilidad y uso de tecnologías de la información en los hogares [3]

Debido a este incremento, es cada vez mas importante considerar la seguridad de las comunicaciones, pues los datos al estar transmitiéndose dentro del área de influencia del AP (Access Point) generan diversos tipos de riesgo que el atacante puede explotar, debido a que los datos son transmitidos a través del aire, este es tema abordado por la seguridad informática.

Cabe destacar que existen diferentes métodos de protección de redes que van desde los más simples hasta los más robustos, en la actualidad existen diferentes métodos de protección de redes que van desde las encriptaciones más simples hasta las más robustas, la primer encriptación de WiFi implementada fue la WEP (Wired Equivalent Privacy) la cual fue implementada por el estándar IEEE 802.11 en 1999 [1], sin embargo aunque fue un buen intento para lograr seguridad en las comunicaciones WiFi, su implementación no fue bien realizada, debido a que es vulnerable a ataques.

WPA y WPA2 (Wireless Protected Access), implementación de una versión temprana del estándar 802.11i, basada en el protocolo de encriptación TKIP [1], 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 [4];

La diferencia de WPA [5] 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.

ISSN-2531-2197

Otro mecanismo de seguridad es el anunciar la existencia de un equipo o no, los equipos que anuncian su existencia lo realizan mediante un SSID, el cual es un acrónimo de (Set Service IDentifier) y permiten que sean vistos por dispositivos que utilizan tarjetas que permitan el uso del WiFi, se considera que aquellos equipos que ocultan su SSID tienen un mecanismo de protección básico ya que la mayor parte de los equipos ignoraran su existencia

Mediante este análisis, se comprueba que existe una muestra considerable de la comunidad de usuarios en el estado de Hidalgo que no cuentan con los conocimientos suficientes para la protección de sus redes inalámbricas.

Para este análisis fue requerido aplicar el método denominado Wardriving, el cual consiste en la detección de redes inalámbricas dentro de una zona geográfica, este es realizado habitualmente con un dispositivo móvil, una laptop, un PDA (Asistente Digital Personal) o por teléfonos celulares [6].

El análisis simplemente se realiza con el dispositivo móvil y en el momento que se detecta la existencia de una red, procede a hacer un estudio de la misma ubicando los puntos de acceso, anidada la información de las características hardware del punto de acceso inalámbrico (AP).

Gracias al método fue posible la obtención de datos proporcionadas por las lecturas de la aplicación "Wigle Wifi Wardriving" disponible para dispositivos con Sistema Operativo Android, las cuales son tratadas en esta investigación con el proceso ETL.

Esta información proporciona a la investigación datos muy relevantes pues a manera estadística podemos determinar las áreas más vulnerables dentro del estado de Hidalgo.

Trabajos relacionados

Existe un artículo realizado en la ciudad de Santiago de Cali en el país de Colombia elaborado por grupo de investigación COMBA I+D [7], en éste se encuentra analizada la seguridad de las redes Wi-Fi, sin embargo no se menciona el proceso de distinción de los datos y se utilizan métodos de análisis convencionales.

Un segundo artículo similar al presente, es llamado "Wardriving: an experience in the city of La Plata" elaborado para LINTI, Facultad de Informática, Universidad Nacional de La Plata, La Plata, Buenos Aires, Argentina [8] en donde también se hace estudio de redes para interpretar la seguridad en dicha ciudad.

También se encuentra un trabajo realizado en Tunja, Boyacá, Colombia para la Universidad Nacional de Colombia, realizando un análisis más a profundidad y dando resultados más gráficos [9].

En este artículo y el objeto diferenciador es que se ha buscado hacer una correcta integración de la información, así como de su adecuada implementación, preservando la integridad, consistencia y disponibilidad la misma.

Pruebas de wardriving a equipos inalámbricos

El propósito es representar los datos esquemáticamente con respecto a la seguridad que se presentan en los equipos inalámbricos además de generar conciencia de los riesgos que representa no tener seguridad en ellos y que en próximos análisis esos resultados mejoren.

Para la realización del análisis, se solicitó apoyo a estudiantes para realizar las pruebas con las técnicas de WarWalking y WarDriving.

ISSN-2531-2197

Fue seleccionada la aplicación para dispositivos móviles. "Wigle Wifi Wardriving" [10], debido a que en su mayoría los estudiantes contaban con celulares con el sistema operativo Android y ésta aplicación permite obtener información de los equipos WiFi y generar mapas de los equipos detectados, en la Figura 1 se muestra una de las diferentes pantallas de las que consta esta aplicación, pudiéndose almacenar los registros obtenidos en diferentes opciones de exportación, en nuestro caso fue solicitada la exportación de los dispositivos detectados en el formato csv (comma sepparated values).

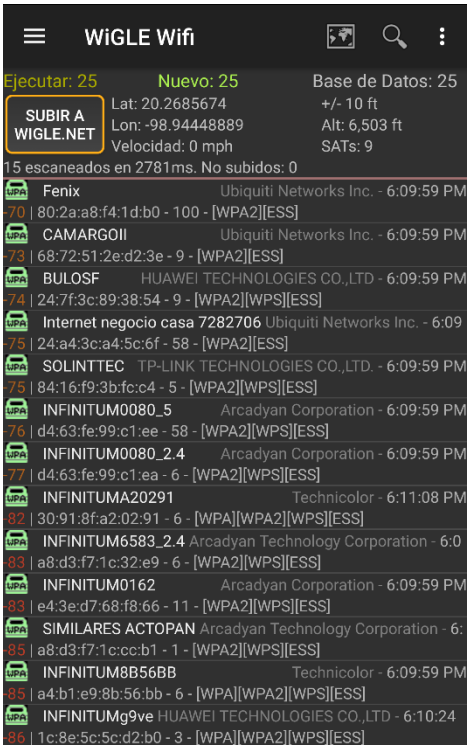


Figura 1 Aplicación WiGLE WIFI

Realización de pruebas de wardriving dentro del estado de Hidalgo

Se recolectó información utilizando wardriving en los distintos municipios donde los estudiantes residen, a fin de conocer el grado de seguridad que se maneja en los equipos existentes con tecnología WiFi, y lograr una conciencia más profunda de la seguridad en redes inalámbricas, se analizaron 60 localidades del estado, pertenecientes al 17.8% de los municipios que existen en el estado de Hidalgo [11], aunque se logró una muestra de los municipios más importantes, faltó el municipio de Tulancingo uno de los más importantes del estado, debido a que de los estudiantes seleccionados ninguno residía en ese municipio.

En la Tabla 1 se muestran los municipios analizados en la prueba del Wardriving, y las colonias pertenecientes a dicho municipios.

Municipios	No. Loc.	Localidades
Actopan	3	Actopan, Cañada Chica Antigua, La Palma
Atotonilco el grande	2	La Puebla, Atotonilco el grande
El Arenal	4	El Jiadi, El Arenal, El Pozo (Santa Ana), San José Tepenene
Huasca de Ocampo	3	Cruz Blanca, Huasca de Ocampo, La mora
Ixmiquilpan	1	Ixmiquilpan
Mineral del monte	2	Barrio del Agua Escondida, Mineral del monte
Pachuca de Soto	15	Cerro de Guadalupe, El Venado, Colonia las Campanitas., Pachuca de Soto, Ejido San Antonio, Ejido San Bartolo, El Huixmí, El Roble, Fraccionamiento Valle del Sol, Hilario Monzalvo Roldán, La Rabia, Los Chávez, Maluco, Pitayas, San Pedro Nopancalco
Zapotlán de Juárez	2	Acayuca, Santa María
Zempoala	2	La Isla, Zempoala
Mineral de la Reforma	19	Azoyatla de Ocampo, Bosques del Mineral, Carboneras, El Popolito, Guadalupe Minerva, La Colonia, San Miguel la Higa, Privada Quinta Bonita, Privadas del Parque, Real de Oriente, Rinconada los Álamos, Rinconadas de San Francisco, Rincones del Paraíso, San Guillermo la Reforma, San José Palma Gorda, Santiago Jaltepec, Unidad Habitacional CTM, Unidad Minera 11 de Julio, Valle Dorado.
San Salvador	2	Caxuxi, San José Doxey
Tepeapulco	2	Fray Bernardino de Sahagún (Ciudad Sahagún), Guadalupe
San Agustín Tlaxiaca	1	San Juan Solís
Cuautepec de Hinojosa	1	Santa Rita
Francisco I. Madero	1	Tepatepec

Tabla 1 Municipios y localidades analizadas

ISSN-2531-2197

Preparación de Datos utilizando ETL

Para el proceso de ETL (Extraction, Transformation and Loading) el equipo que realizó el wardriving, entregó un archivo de cada uno de los sitios analizados en formato CSV, al haber utilizado todos el mismo software y la misma opción de almacenamiento, hubo una estandarización en los datos, lo que facilitó el proceso de integración de la información recolectada, sin embargo aún así se encontraron archivos con datos corruptos u opciones que se salieron de lo especificado, sin embargo fueron muy pocos estos casos. Una vez que se tuvieron los archivos corréctos se unieron estos registros en uno solo para hacer el proceso de análisis. Las principales actividades llevadas en la realización del proceso ETL fueron las siguientes:

- Identificar y eliminar archivos fuera de lo solicitado o corruptos.

- Eliminar registros de sitios que habían sido analizados por otra persona, este caso fue muy frecuente, debido a que, aunque cada persona tenía una ruta diferente asignada, había traslape en algunas zonas, principalmente en los municipios con más habitantes, de maś de 14000 equipos analizados, se redujo la cantidad a 7562 equipos.

- Se eliminaron columnas que eran innecesarias para el análisis de vulnerabilidades.

- Se eliminaron datos de equipos que no fueran de tipo WiFi.

- Se procedieron a identificar las localidades analizadas en base a sus coordenadas proporcionadas por el GPS, este proceso requirió hacer una búsqueda de una aplicación que nos diera esta posibilidad, utilizando para esto Maplarge [12].

- Posteriormente se requirió que las localidades proporcionadas se ubicaran a los municipios del estado.

Uno de los procesos mas consumidores de tiempo fue la identificación mediante la posición absoluta de las localidades y su posterior ubicación a uno de los 60 municipios del estado, este proceso se debió relizar manualmente debido a que no se encontró una aplicación gratuita que nos realizara esta operación de manera automática, el proceso se puede apreciar en la Figura 2 mostrada a continuación.

Figura 2 Proceso ETL

Otra herramienta utilizada fue el software Pentaho [13] para poder realizar la transformación de nuestro archivo CSV a un archivo ARFF del acrónimo en ingles (Attribute-Relation File Format) utilizado por el software de Weka [14], de donde se procedió a generar los resultados reportados en este trabajo, en la Figura 3 se muestra el proceso realizado con Pentaho y su correcta transformación de 7562 registros.

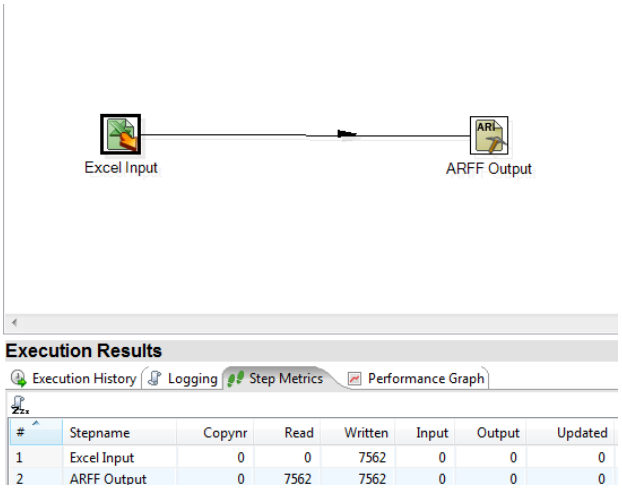


Figura 3 Proceso de transformación a un archivo ARFF

Resultados Obtenidos

En la Tabla 2 se muestra la clasificación utilizada para ubicar los equipos analizados con respecto a su seguridad.

Seguro Equipos con cifrado WPA o WPA/2.
Inseguro Oculto Equipos con SSID Oculto con cifrado WEP
Seguro Oculto Equipos con SSID Oculto y cifrado WPA y WPA2
Inseguro Equipos con cifrado WEP o ESS

Tabla 2 Clasificación de tipos de vulnerabilidades utilizadas para análisis de APs

En la Tabla 3 se muestran los resultados obtenidos por municipio de la clasificación de seguridad realizada:

– Pachuca la capital de Hidalgo, de 3771 AP's, el 65.23% son seguros, el 24.48% son seguros con el SSID oculto, el 9.25% son inseguros y el 1.03 son inseguros con SSID oculto.

– Mineral de la Reforma los 1240 AP's el 70.48% son seguros, el 20.81% son seguros con el SSID oculto, el 8.15% son inseguros, y el 0.56% son son inseguros con SSID oculto.

– Tepeapulco con 1207 AP's el 47.39% son seguros, el 29.41% son seguros con el SSID oculto, el 6.88% son inseguros, y el 16.32% son inseguros con SSID oculto.

Grado de Seguridad por Municipio					
	INSEGUROS	INSEGUROS OCULTOS	SEGUROS	SEGUROS OCULTOS	Total
Actopan	42	11	269	120	442
Atotonilco el Grande	24	2	154	81	261
Cuautepec de Hinojosa	1	0	15	8	24
El Arenal	3	3	71	41	118
Francisco I. Madero	17	3	105	39	164
Huasca de Ocampo	7	0	35	10	52
Ixmiquilpan	4	0	23	7	34
Mineral de la Reforma	101	7	874	258	1240
Mineral del Monte	3	1	11	0	15
Pachuca de Soto	349	39	2460	923	3771
San Agustín Tlaxiaca	0	0	5	1	6
San Salvador	1	1	53	15	70
Tepeapulco	83	197	572	355	1207
Zapotlán de Juarez	1	0	1	0	2
Zapotlán de Juárez	5	0	74	40	119
Zempoala	0	1	19	17	37
Total	**641**	**265**	**4741**	**1915**	**7562**

Tabla 3 Valoración del nivel seguridad de equipos WiFi en municipios del estado de Hidalgo

Posteriormente con los datos obtenidos, se utilizó una plataforma web llamada CARTO, que nos permite subir las coordenadas obtenidas y observarlas como puntos geográficos en un mapa [15].

Se utiliza la siguiente convención para mostrar la seguridad para el tipo de equipos analizados

- Equipos Seguros (color verde)
- Equipos Seguros Ocultos (color azul)
- Equipos Inseguros (color rojo)
- Equipos Inseguros Ocultos (color amarillo)

En la Figura 4 se muestra un mapa del Estado de Hidalgo, donde se reflejan principalmente los sitios donde se encuentran equipos mal configurados (inseguros) que los hacen vulnerables a ataques por parte de usuarios maliciosos.

ISSN-2531-2197

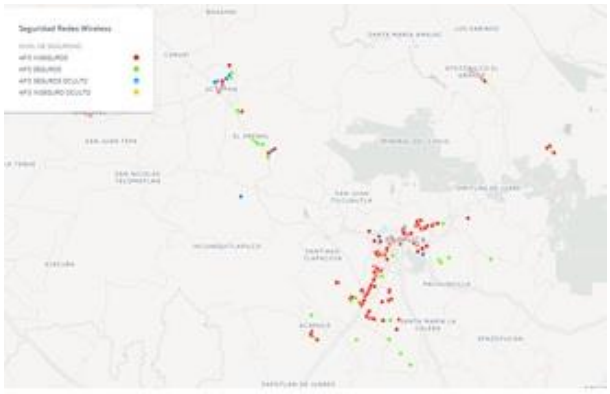


Figura 4 Mapa de seguridad en equipos WiFi analizados dentro del estado de Hidalgo (Enfatizando equipos inseguros)

En la Figura 5 se muestran los equipos que se encuentran adecuadamente configurados en el Municipio de Pachuca

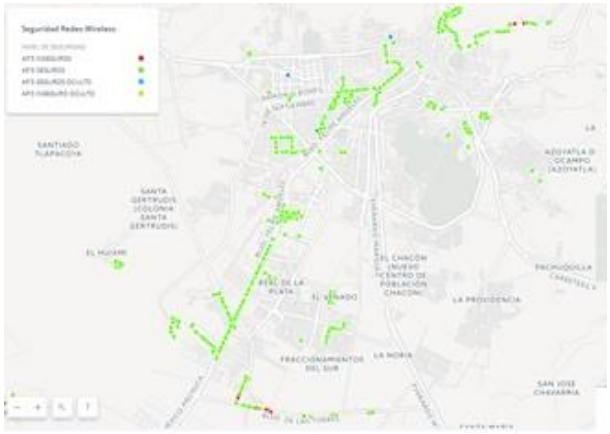
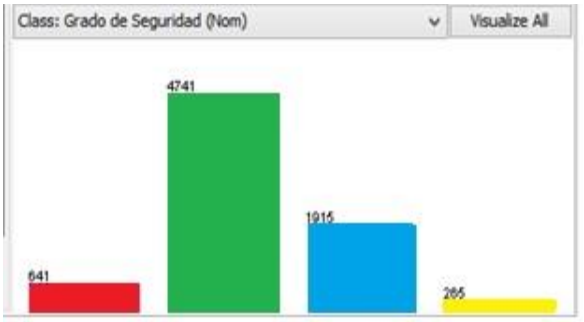


Figura 5 Mapa de seguridad en equipos WiFi analizados dentro de Pachuca (Enfatizando equipos seguros)

En la Gráfica 2 obtenida con el software de Weka pueden verse reflejados los resultados de todos los municipios del estado de Hidalgo encontrándose redes inseguras con un 8.48%, redes seguras con un 62.70%, redes seguras ocultas con el 25.32% y redes inseguras ocultas con un 3.5%.



Gráfica 2 Grado de seguridad en WiFi de municipios analizados en el estado de Hidalgo

Para la realización de minería se procedió a utilizar una clasificación utilizando algoritmos de conjuntos de datos disjuntos, probabilísticos y jerárquicos, habiéndose utilizando los métodos de agrupamiento (clustering) siguientes: (Kmeans, Xmeans y Cobweb). Para la realización de éstos métodos se utilizaron datos nominales, removiendo de los datos el grado de seguridad asignado de manera manual al momento de hacer el proceso ETL. Se analizaron diferentes grupos de datos, obteniéndose un mejor resultado con los atributos nominales (Authmode, Localidad y Ciudad-Municipio). A fin de validar con cual de los métodos se logra una mejor clasificación, se muestra en la Tabla 4 una comparación de los resultados obtenidos con el proceso de minería con respecto a la clasificación realizada manualmente. Como puede ser visto se logró una clasificación muy similar con el método SimpleKMeans utilizando Weka con 11 semillas (seeds) que son utilizadas para inicializar los clusters y que afectan el proceso de clasificación con este método. Asi mismo se establecieron 4 clusters para hacer una clasificación similar a la realizada manualmente, el método de maximización de expectación (EM) reporta una clasificación muy diferente a la obtenida con el SimpleKmeans, entregando resultados poco satisfactorios. El método Cobweb con valores de default genera un número superior a los 1000 clusters, por lo cual no se reportan los resultados.

ISSN-2531-2197

Grado de Seguridad	Manual	Simple-Kmeans (10 seeds)	Simple-Kmeans (11 seeds)	Simple-Kmeans (12 seeds)	Simple-Kmeans (13 seeds)	EM
Inseguro	641	1210	646	1109	2695	1207
Seguro	4741	4292	3488	3009	964	3676
Seguro-Oculto	1915	1975	3177	2566	3527	2561
Inseguro-Oculto	265	85	251	878	376	118
TOTAL	7562	7562	7562	7562	7562	7562

Tabla 4 Comparación de la clasificación realizada manualmente con la obtenida con algoritmos de minería

En la Figura 6 se muestran los resultados obtenidos con el método Kmeans que mejores resultados reportó.

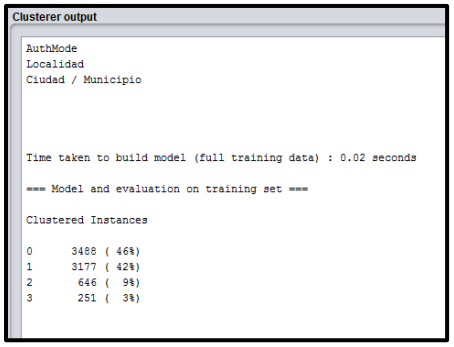


Figura 6 Resultados de minería obtenidos con la clasificación obtenida en SimpleKmeans en Weka

Aunque puede ser visto que existe una variación significativa entre la clasificación realizada automáticamente por SimpleKmeans entre equipos "seguros" y "seguros ocultos", aún así es importante considerar que todos son considerados equipos seguros. Con respecto a la clasificación realizada para equipos inseguros, la diferencia es significativamente menor, encontrándose valores casi similares, en equipos "inseguros" y en equipos "inseguros ocultos".

Puede concluirse que en los equipos analizados predominan los equipos con seguridad con un 88 % y sólo un 12 % con equipos inseguros, durante el análisis pudo ser visto que los equipos recientemente instalados vienen configurados con mejores parámetros de seguridad (encriptación WPA y WPA2).

Que ciertas empresas como Telmex y Totalplay entregan sus nuevos equipos con conexión a internet con configuraciones seguras, mientras que en lugares donde se cuenta con conexiones menos recientes las configuraciones tienden a ser más inseguras. Se encontró igualmente que hay ciertas colonias que tienden a tener configuraciones muy seguras, generalmente en fraccionamientos nuevos con servicios de internet recientemente instalados, predominando el SSID oculto y algoritmos de cifrado robustos.

Referencias

[1] Guillaume Lehembre. (Enero 2006). Seguridad Wi-Fi – WEP, WPA y WPA2. Julio 2017, de hakin9 Sitio web: http://www.zero191513wireless.net/wireless/seguridad/01_2006_wpa_ES.pdf

[2] INEGI De 2013 a 2014: INEGI. Módulo sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares.

[3] Para 2015-2016: INEGI. Encuesta Nacional sobre Disponibilidad y Uso de TIC en Hogares, ENDUTIH.

[4] Lei Z., Jiang Y., Zugao D. and Renfe Z.(2012), The security analysis of WPA encryption in wireless network, Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference. sitioweb:http://doi:10.1109/CECNet.2012.6202145

[5] Lashkari A., Mansoor M. and Danesh (2009), A., Wired EquivalentPrivacy (WEP) versus Wi-Fi Protected Access (WPA), 2009 International Conference on Signal Processing Systems. Sitioweb: http://doi:10.1109/ICSPS.2009.87

ISSN-2531-2197

[6] Universidad Central de Venezuela. (2005). Seguridad en Redes Inalámbricas 802.11. 10/08/2017, de Universidad Central de Venezuela Sitio web: http://www.ciens.ucv.ve:8080/genasig/sites/redesmov/archivos/Seguridad%20en%20Redes%20Inalambricas%20802.pdf

[7] Millán A.; Daza R.; Campiño J. (2006). Estudio de los puntos de acceso inalámbricos 802.11 en la ciudad de Cali usando las técnicas WAR-X. Sistemas & Telemática, Enero-Junio, 35-42.

[8] Díaz J., M., Venosa P., Macia N. (2017). Wardriving: an experience in the city of La Plata. 8/2017, de LINTI, Facultad de Informática, Universidad Nacional de La Plata, La Plata, Buenos Aires, Argentina Sitio web: http://sedici.unlp.edu.ar/bitstream/handle/10915/21678/Documento_completo.pdf?sequence=1.

[9] Julián Alberto Monsalve-Pulido a, Fredy Andrés Aponte-Novoa b & Fabián Chaparro-Becerra c. (November 19th, 2014). Security analysis of a WLAN network sample in Tunja, Boyacá, Colombia. DYNA, 1.

[10] Wigle Wifi Wardriving (2010).Consultado 8/Junio/2017,WiGLE.net.sitioweb:https://wigle.net/

[11] Municipios de México (2017).consultado 8/Agosto/2017,MUNICIPIOS.sitioweb:https://www.municipios.com.mx/hidalgo.

[12] MapLarge (2017).Consultado 7/Agosto/2017,MAPLARGE.sitioweb:https://www.maplarge.com.

[13] Pentaho (Septiembre 2014).Consultado 7/Agosto/2017,Pentaho A Hitachi Group Company.sitioweb: http://www.pentaho.com/

[14] Weka (1993).Consultado 10/Agosto/2017, Universidad de Waikato de Nueva Zelanda.sitioweb: http://www.cs.waikato.ac.nz/ml/weka/

[15] JAVIER DE LA TORRE (2012).Consultado 17/Agosto/2017,CARTO, sitioweb:https://www.carto.com

ISSN-2531-2197