La seguridad informática y su impacto en las conexiones del estándar IEEE 802.11

Computer security and its impact on IEEE 802.11 standard connections

José Danilo Villares Pazmiño[1,*], Monica Patricia Acurio Acurio[1,†],
Carlos Julio Soto Valle[1,‡].
[1]Universidad Técnica de Babahoyo.
{macurio@utb.edu.ec, jvillares@utb.edu.ec, carlos.soto@babahoyo.gob.ec}

Fecha de recepción: 03 de octubre de 2017 — **Fecha de aceptación:** 16 de octubre de 2017

Resumen: La presente investigación trata sobre el tema seguridad informática y las normas que se encargan de diseñar los métodos para que el sistema sea más confiable en un ambiente de red, el cual tiene como objetivo identificar y eliminar vulnerabilidades existentes. En la experiencia de wifi se dice que admite ordenadores portátiles equipos de escritorio, asistentes digitales personales o cualquier otro dispositivo de alta velocidad y de conexión tanto en lugares cerrados como al aire libre. Una red wifi es en realidad una red que cumple con el estándar 802.11. En general el estándar 802.11 establece modelos inferiores del modelo OSI para las conexiones inalámbricas que utiliza ondas electromagnéticas. Una gran parte significativa de la velocidad de transmisión se utiliza en la necesidad de codificación para perfeccionar la eficacia de trasmisión bajo ciertas situaciones ambientales diversas, lo cual se cambió en dificultades de interoperabilidad entre equipos de diferentes marcas. La metodología utilizada en la presente investigación se llevó a cabo mediante la revisión de documentos de referencia y un análisis comparativo de datos, teniendo como conclusión la importancia de adoptar medidas de seguridad para que la información no sea vulnerada en a red.

***Palabras Clave*—Seguridad informática, Wifi, Vulnerabilidades.**

Abstract: This research deals with the subject of computer security and the rules that are responsible for designing methods to make the system more reliable in a network environment, which aims to identify and eliminate existing vulnerabilities. In the Wi-Fi experience, it is said that it supports laptops, desktop computers, personal digital assistants or any other high-speed and connection device both indoors and outdoors. A Wi-Fi network is actually a network that complies with the 802.11 standard. In general, the 802.11 standard establishes lower models of the OSI model for wireless connections that use electromagnetic waves. A large part of the transmission speed is used in the need for coding to improve the efficiency of transmission under certain environmental situations, which changed into difficulties of interoperability between equipment of different brands. The methodology used in the present investigation was carried out through the review of reference documents and a comparative analysis of data, having as a conclusion the importance of adopting security measures so that the information is not violated in the network.

***Keywords*—Computer security, Wifi, Vulnerabilities.**

INTRODUCCIÓN

A medida que pasa el tiempo el uso del internet va aumentando y las compañías admiten a sus proveedores acceder a sus sistemas de información. Por lo cual es necesario que su sistema de información este protegido para el control al acceso al mismo.

También debido a que en la actualidad se puede acceder a sistemas de información desde cualquier lugar se pide a sus empleados a que lleven parte de la información fuera de su área segura es por ellos y otros factores que se debe proteger los sistemas de información.

Por otro lado, el IEEE 802.11 se lo define como estándar internacional que define una red de área local inalámbrica (WLAN). Con wifi se puede construir redes inalámbricas de alta velocidad siempre y cuando el equipo que se va a conectar no esté muy lejano al punto de acceso. Los proveedores de wifi están comenzando a cubrir áreas con gran concentración de usuarios y a estas áreas se les denomina zonas locales de cobertura.

El estándar 802.11b admite como máximo de trasferencia de datos 11Mbps en un rango de 100 metros en ambientes cerrados y más de 200 metros al aire libre. El estándar 802.11g permite como máximo de trasferencia de datos 54 Mbps en rangos comparables a los del estándar 802.11b.

La seguridad informática tiene como objetivo proteger los sistemas de información de las compañías ya que en la información incluyen todos los datos de una compañía por considerarlo de esta manera.

DESARROLLO

¿Qué es seguridad informática?

También se lo conoce como ciberseguridad rama que se encarga en la protección tanto lógica como física del sistema informático computacional. Para lo cual existen patrones para disminuir los posibles peligros que por lo general estos riesgos suelen proceder desde programas dañinos instalados en la misma computadora como un virus o filtrarse en las computadoras de los usuarios al ingresar al internet e ingresar a distintos sistemas. Actualmente a un sin número de virus que vulneran cualquier equipo o sistema informático como

[*]Ingeniero en Sistemas, Magíster en Gestión de Bases de Datos
[†]Ingeniera en Sistemas, Magíster en Gerencia Educativa
[‡]Ingeniero en Sistemas

tenemos por ejemplo se puede decir que los virus residentes son los que generalmente se caracterizan por estar ocultos en la memoria RAM lo cual le da la oportunidad de controlar las operaciones que son efectuadas en el ordenador ocasionando la contaminación de los programas que son parte de ella. Así también tenemos los virus de acción que se caracterizan por ejecutarse rápidamente por todo el equipo contaminando a todo lo que se encuentre a su paso (ACISSI, 2015).

También se hace énfasis a que la seguridad de información no debe ser confundida con la seguridad informática, ya que la seguridad informática es la que se faculta de proteger o como su palabra lo dice asegurar el sistema informático.

Historia de la Seguridad Informática

Todo inicio a partir del año 1980 época en la que el uso de un computador personal se volvió común, con ella la preocupación por la integridad de los datos empezó a florecer en el año 1990 se toma conciencia del peligro que crea no tener protección que hacía falta a los usuarios de Pc's y en la misma época los famosos virus y gusanos causaban estragos en internet empezando a generalizarse las amenazas hacia la integridad de los dato; A partir del año 2000 se comienza a tomar muy en serio la parte de seguridad informática , volviéndose una necesidad principalmente por el uso masivo del internet (Rascagneres, 2016).

Seguridad informática en las conexiones Wireless 802.11

Las redes inalámbricas en la actualidad han sufrido un sin número de cambios para ser acoplada a los intereses de los usuarios dentro de esta serie de cambios hay que recalcar todos los aspectos que violan la seguridad, con la aparición del WPA y del estándar 802.11 la seguridad informática se ha visto reforzada al dificultar las técnicas utilizadas para poder comprometer la seguridad de las mismas, por lo que hoy en día se cuenta con tecnologías para solucionar las redes inalámbricas (Banerji & Singha Chowdhury, 2013).

La seguridad es el tema más importante al momento de hablar de redes inalámbricas, siempre desde sus inicios se ha tratado de que los protocolos garanticen la comunicación, pero ha tenido muchas fallas. Dentro de los procesos de gestión de seguridades de redes, cabe recalcar que los accesos a todos los espacios físicos deben estar salvaguardados, evitando la intromisión de personal no autorizado (León Acurio, Bastidas Zambrano , & Vera Mora , 2016).

¿Qué es Wireless 802.11?

802.11 es un estándar internacional que define las características de una Red de área Local también conocida como WLAN, muchas personas quizá no conozcan del tema, en realidad una Red Wifi es una red que cumple con el estándar 802.11. Se preguntará porque hablamos de esto, pues las redes que tenemos en nuestras casas son redes Wifi o WLAN que utilizan este estándar.

Nuestras redes WLAN aunque parezca mentira pueden ser vulneradas con facilidad, en nuestros hogares la integridad de nuestros datos podrían ser sustraídos para cualquier fin, es nuestro deber y obligación poder blindar nuestra red Wifi, normalmente no se trata de hackers o ciberespias que tratan de robar nuestra información (no en todo los casos), lo común es que sea algún "vecino" que trate de infiltrarse en nuestra Red.

¿Cómo evitar infiltraciones en Redes WLAN?

Como probablemente sepan es imposible tener la seguridad al 100 %, podríamos aplicar algo una especie de blindaje extra a nuestra Red para asi evitar infiltraciones. A continuación, se muestran algunos tipos de blindajes:

- **Blindaje del acceso al Router:** Fijarnos en que nadie más pueda ingresar a nuestro Router depende de nosotros, tener actualizado el Firmware a nuestro Router es un paso primordial para evitar vulnerabilidades existentes, cambia tu nombre y clave de acceso al sistema de tu Red.
- **Cambiar el SSID del Router:** Cambiar el identificador de Red nos ayudara en un leve porcentaje a proteger nuestra Red, ya que nuestra compañía de servicios muchas veces revela más información de la necesaria.
- **Elegir el mejor sistema de cifrado (Wpa, Wpa2):** El sistema de cifrado WEP quedo para el pasado, es muy sencillo vulnerar ese tipo de cifrado, recomendamos que se usen cifrados Wpa, Wpa2 para mayor seguridad.
- **Utilizar algún tipo de cifrado MAC:** Dicho cifrado es como hablar de una dirección IP pero de más bajo nivel, nos permitirá organizar un listado de dispositivos permitidos para conectarse a nuestra Red, dependiendo de la versión o modelo se puede hacer BlackList o listas negras de dispositivos.
- **Limitar la potencia de emisión:** A través de esta opción podremos levantar una muralla de protección, ya que si solo conectaremos dispositivos conocidos, con esta opción daríamos un rango de emisión para dichos dispositivos.

Hablando de infiltraciones es importante recalcar que:

Las redes con estándar 802.11 son seguras, pero como conocemos, en la actualidad la tecnología avanza día a día y poco a poco será más fácil infiltrarse a la red de una persona desconocida, lo que queremos dar a conocer es que la seguridad informática es muy útil al momento de integridad de datos, proporcionar una buena muralla o configuración a nuestra red nos ahorrara muchos inconvenientes. A continuación mostraremos una tabla de estándares 802.11, con su respectiva frecuencia, DER y el rango de emisión, para poder tener un poco más de conocimiento de características Wireless (Rascagneres, 2016).

Protocol	Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)
Legacy	1997	2.4 -2.5 GHz	1 Mbit/s	2 Mbit/s	?
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	25 Mbit/s	54 Mbit/s	~30 meters (~100 feet)
802.11b	1999	2.4-2.5 GHz	6.5 Mbit/s	11 Mbit/s	~30 meters (~100 feet)
802.11g	2003	2.4-2.5 GHz	25 Mbit/s	54 Mbit/s	~30 meters (~100 feet)
802.11n	2008 (projected)	2.4 GHz or 5 GHz bands	200 Mbit/s	540 Mbit/s	~50 meters (~160 ft)

Figura 1. especificaciones de estándares IEEE 802.11
Fuente: (Galeon, 2004).

Tabla 1. Comparación de las características del estándar 802.11n vs 802.

	IEEE 802.11n	**IEEE 802.11ac**
Frecuencia de operación	2.4 GHz y 5 GHz	5 GHz
Canales	20,40 MHz	20, 40, 80 y hasta 160 MHz
Streams	1 a 4	1 a 8
MU-MIMO	2003	Si
Máxima tasa de transferencia por radio (1x1)	150 Mbps	450 Mbps
Máxima tasa de transferencia por radio (3x3)	450 Mbps	1.3 Gbps

Fuente: (Pimentel, 2004)

Algunos Estándares inalámbricos

Estándar 802.11a.

Según Ariganello, E. & Barrientos, E. (2010) manifiestan que el estándar 802.11a define el uso de WLAN en la banda de 5 GHz que puede dividirse en tres grupos:

- **Banda baja:** Implementaciones en interiores con un manejo de frecuencia de 5,15 a 5,25 GHz.
- **Banda media:** Implementaciones en interiores y exteriores con un manejo de frecuencia de 5,25 a 5,35 GHz.
- **Banda alta:** Implementaciones en exteriores con un manejo de frecuencia de 5,725 a 5,825 GHz.

Además, el estándar 802.11a permite que los valores de transferencia sean desde 6, 9, 12, 18, 24, 36, 48 y 54 Mbps, interpretando un intervalo de rendimiento máximo de 28 Mbps, y dependiendo del acercamiento a los AP, su velocidad podría aumentar como también disminuir.

Estándar 802.11b

Según Radvan, S. (2010) manifiesta que es una expansión del estándar original, el estándar 802.11b se caracteriza por alcanzar una velocidad máxima de hasta 11 Mbps, prácticamente fue publicado como IEEE Std. 802.11b, el mismo que define la utilización con una banda de 2.4 GHz, cabe destacar que una de las principales motivaciones era el aumento del valor de las tasas de datos.

Estándar 802.11c

Banerji, S. & Singha, R. (2013) mencionan que el estándar IEEE 802.11c son características que utilizan los AP (puntos de accesos), formalmente denominados bridge (puentes) que enlazan dispositivos mediantes las topologías de las redes de área local dotando a las capas MAC (Control de Acceso al Medio) de otras normas de conectividad y cabe destacar que dicha norma es compatible con la 802.11a, 802.11b y a su vez siendo un complemento del estándar 802.11d.

El estándar mencionado es utilizado generalmente en el ámbito estudiantil universitario para el desarrollo de prácticas de telecomunicaciones y utilización de un alto despliegue de cobertura para las implementaciones de bridging.

RESULTADOS

El impacto que hasta ahora ha generado la seguridad informática en redes Wlan es muy alto, pero aun asi existen personas que logran infiltrarse en dichas redes ya sea por desconocimiento de parte de los dueños de las redes o por simple mala configuración de sus dispositivos, los cuales no cuentan con la seguridad necesaria para contrarrestar ataques informáticos. La integridad de los datos es uno de los factores principales que nosotros como usuarios debemos saber proteger, la implementación de blindajes o configuraciones avanzadas disminuirán en un tanto por ciento las infiltraciones de hackers o aficionados al hacking que intenten robar información de su red.

La debida capacitación autónoma nos dara la facilidad de blindar más nuestras conexiones, a medida que la tecnología avanza nosotros debemos seguir capacitando y engrandeciendo nuestros conocimientos para poder tener segura nuestra información, cualquier persona puede ser víctima de hacking.

Con esto nuestro estudio determino que un 62 % de datos en la red se encuentras seguros con alguna medida de seguridad implementada, mientras que la diferencia no cuentan con sistemas netamente seguros para evitar ataques informáticos, los cuales quedan expuestos a posibles amenazas, las cuales rompen de manera directa conexiones de redes existentes y de preferencias las inalámbricas.

¿Se puede evitar ser víctima de hacking?

Sí, pero no en su totalidad ya que siempre habrá nuevas formas de infiltrarse en las redes privadas, nuestras redes se encuentran a vista y gusto de todo mundo, la encriptación, configuración MAC, la configuración de Router todos estos componentes nos mostraran buenos resultados al momento de evitar perdida de integridad de datos.

CONCLUSIONES

Como se ha comprobado a lo largo de la investigación, la seguridad informática forma parte de nuestra vida tecnológica en el internet, ya que si no la sabemos utilizar creara inconvenientes, disgustos, y problemas sociales, aunque parezca mentira es real, ser propietario de una red wireless ocasiona problemas,

y es nuestro deber blindar y proteger nuestra infraestructura tecnológica.

Por tanto, los factores que intervienen al momento de hablar de infiltraciones, hacking, sustracción de datos son muchos: vulnerabilidad en las barreras del Router, puertas de acceso abiertas a todo público, mala configuración de Router, mala utilización de Direcciones MAC, rango de emisión WLAN muy extensa u otros.

Según el apartado de desarrollo, la seguridad informática es la parte fundamental de toda conexión a internet, ya que desde los momentos que fue creado el internet hasta el dia de hoy siguen existiendo mejoras, actualizaciones de virus y malware que han ido siendo desarrollados. Es importante dar a conocer todas estas situaciones para saber a qué nos enfrentamos a diario.

REFERENCIAS BIBLIOGRÁFICAS

ACISSI. (2015). Seguridad Informática Hacking Ético. España: ENI.

British Standards Institution. (2008). Norma Iso 27002. BSI Publications.

Buffalo. (2003). Obtenido de http://www.buffalo-technology.com/es/tecnologia/software-asociado/wireless-80211-technologies/

Buffalo. (2007). buffalo-technology. Obtenido de http://www.buffalo-technology.com/es/tecnologia/software-asociado/wireless-80211-technologies/

Díaz, G. O. (2014). Procesos y Herraminetas para la seguridad en redes. España: Universidad Nacional de Educacióon a Distancia.

Fiscalia General del Estado. (13 de 6 de 2015). Los delitos infomaticos van desde el fraude hasta el espionaje. Obtenido de Los delitos infomaticos van desde el fraude hasta el espionaje: http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform %C3 %A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

Gabriel, B. U. (2016). Introducción a la Seguridad Informática . Grupo Editorial Patria.

Galeon. (16 de 05 de 2004). galeon.com. Obtenido de http://ieeestandards.galeon.com/aficiones1573579.html

León Acurio, J., Bastidas Zambrano, L., & Vera Mora, G. (2016). Red metropolitana segura y la gestión de sucursales en la infraestructura tecnológica: Caso de Estudio GADM de la Ciudad de Babahoyo. Journal Of Science And Research: Revista Ciencia E Investigación, 7-12.

Pimentel, F. (15 de 07 de 2004). http://www.wni.mx/. Obtenido de http://www.wni.mx/index.php?option=com_content&view=article&id=75:80211ac&catid=31:general&Itemid=79

Rascagneres, P. (2016). Seguridad Informática y Malwares. España: ENI.

Suárez, R. C. (2010). Tecnologías de la Información y la Comunicación. España: Ideaspropias.