**Benemérita Universidad Autónoma de Puebla**

**Facultad de Ciencias de la Computación**

**Sección 107**

**Desarrollo de Habilidades en el Uso de la Tecnología, la Información y la Comunicación**

**Alumnos**

**Ana Laura Olguín Domínguez**

**César Eduardo Plácido Velazco**

**Dolores Reyes Lezama**

**Kevin Marco Pérez Guerrero**

**“Si velocidad al navegar quieres, tu red vigilar debes”**

**Otoño 2012**

**Si velocidad al navegar quieres, tu red vigilar debes.**

**Introducción**

¿Te has enterado si te roban tu señal Wi-Fi?

Siempre que estamos en un lugar, y estamos aburridos, lo que la gran mayoría de los adolescentes y adultos hacen ahora es conectarse a Internet a través de sus celulares, y no me dejarán mentir, que siempre que estamos fuera de casa, es decir, lejos de nuestro módem, router o cable, buscamos redes gratuitas, o en otro caso, sin protección para conectarnos.

La falta de seguridad en redes inalámbricas es un problema que, a pesar de su gravedad no ha recibido la atención debida por parte de los administradores de redes y las responsables de la información. Este ensayo presenta las tecnologías existentes para mejorar el nivel de seguridad de las redes inalámbricas con sus ventajas, desventajas y escenarios de aplicación.

El acceso sin  necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere. Cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podría tener acceso a la red inalámbrica

Y esos problemas serían comunes para un usuario sin protección, destacando el mal desempeño que tendría la red al ser utilizada por personas ajenas, además de la navegación gratuita que se provee sin restricciones a nadie, ahora hablando de problemas más serios, el robo de la red inalámbrica privada es un peligro porque pueden emplear la red de la compañía (o de cualquier otro sitio) como punto de ataque hacia otras redes y luego desconectarse para no ser detectado, robar software y/o información, introducir virus o software maligno, robo de identidad, entre muchas otras terribles consecuencias.

Este ensayo va dirigido a las personas usuarias de las redes, principalmente a aquellas que tienen una red inalámbrica privada y que son o podrían ser víctimas de hurto de su red.

Vamos a analizar diferentes maneras que nos permitirían evitar la gran mayoría de los problemas arriba señalados, nuestra postura es en contra del robo de la señal  de red inalámbrica, es decir a favor de la “seguridad en las redes inalámbricas”.

**Características de una Red**

Si hay algo que define a una red WLAN son estos puntos:

* Movilidad: permite transmitir información en tiempo real en cualquier lugar de la organización o empresa a cualquier usuario. Esto supone mayor productividad y posibilidades de servicio.
* Facilidad de instalación: al no usar cables, se evitan obras para tirar cable por muros y techos, mejorando así el aspecto y la habitabilidad de los locales, y reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios temporales de la red.

* Flexibilidad: puede llegar donde el cable no puede, superando mayor número de obstáculos, llegando a atravesar paredes. Así, es útil en zonas donde el cableado no es posible o es muy costoso: parques naturales, reservas o zonas escarpadas

**El problema de seguridad en una WLAN**

Y es precisamente por esto que este tipo de redes se han vuelto tan comerciales actualmente. El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere.

Cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podría tener acceso a la red inalámbrica. Al lograr una transmisión de información en tiempo real, en caso de que la red no esté protegida, es una mina de oro para un hacker, quien con sólo un simple programa, puede obtener datos confidenciales del usuario, o usuarios, que estén utilizando la conexión.

Por ejemplo, si varias empresas tienen sede en un mismo edificio, y todas ellas poseen red inalámbrica, el equipo de un empleado podría encontrarse en cierto momento en el área de influencia de dos o más redes diferentes, y dicho empleado podría conectarse (intencionalmente o no) a la red de una compañía que no es la suya. Aún peor, como las ondas de radio pueden salir del edificio, cualquier   persona que posea un equipo móvil y entre en el área de influencia de la red, podría conectarse a la red de la empresa.

**Seguridad de una Red WLAN**

Ahora bien, revisando el problema que presenta la seguridad en las redes WLAN, probablemente se estén preguntando, ¿cómo proteger mi información? Bien, respecto a este punto, podemos contar (en algunas ocasiones) con que al contratar el servicio de Internet con algún proveedor o alguna compañía, los técnicos que realizan la instalación en la casa, oficina o empresa, proveen al usuario un módem o router, el cual viene previamente configurado con una contraseña de red, esto es principalmente para evitar que terceros puedan “colgarse” de la red, es decir, accesar de manera libre, perjudicando la estabilidad y rendimiento de la transmisión de la información, que, mientras más equipos la utilicen, mayor es el desgaste de la señal.

Desafortunadamente, no siempre es así, hay algunos casos en los que el usuario debe configurar la contraseña del módem.

Existen diversos métodos para lograr la seguridad en una WLAN, cada uno logra un nivel de seguridad distinto, y tiene sus ventajas y desventajas, nosotros nos concentraremos en aquellos que poseen un nivel de cifrado o encriptación, como son:

* Wired Equivalent Privacy (WEP)

El nivel más básico de seguridad para redes inalámbricas es WEP, o Wired Equivalent Privacy, una característica estándar de todas las redes LAN inalámbricas certificadas con la norma Wi-Fi. WEP, creado por el Instituto de Ingenieros en Electricidad y Electrónica (IEEE), ha sido diseñado para proporcionar un nivel de seguridad, prevenir posibles escuchas de la información y proteger la red mediante la encriptación de todos los datos que se envíen de forma inalámbrica. Tiene la ventaja de ser el método de seguridad más utilizado por los fabricantes, y el más fácil de configurar, pero como desventajas el cifrado WEP se ha demostrado inseguro y es posible descifrar los datos que hayan sido cifrados con este protocolo y por consiguiente se puede averiguar la clave WEP y los parámetros necesarios para poder acceder a una red protegida con este método. Dicha clave puede ser calculada mediante ingeniería inversa, disponiendo sólo del nombre de la red.

* Wireless Application Protocol (WPA)

WPA o Protocolo de aplicaciones inalámbricas, emplea el cifrado de clave dinámico, que quiere decir que la clave se está cambiando constantemente, y hace que as incursiones en la red inalámbrica sean más difíciles que con WEP. WPA está considerado como uno de los más altos niveles de seguridad inalámbrica para la red, es el método recomendado si el dispositivo es compatible con este tipo de cifrado. Las claves se insertan de dígitos alfanuméricos, sin restricción de longitud, en la que se recomienda utilizar caracteres especiales, números, mayúsculas, minúsculas, y palabras difíciles de asociar entre ellas, o con información personal.

* WPA2

Es la segunda generación de WPA, pero no fue creada para afrontar las limitaciones de WPA, y es compatible con los productos anteriores que son compatibles con WPA. La principal diferencia es que utiliza un tipo de cifrado avanzado (AES), mientras que WPA ocupa el TKIP. El cifrado de WPA2 aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas agencias federales.

**Consecuencias de no proteger la red WLAN**

Las múltiples consecuencias de no proteger una red WLAN adecuadamente varían en grados de complejidad, pueden ir desde lo más simple y común, que es que el vecino use tu Internet de manera gratuita, hasta el robo de identidad, algunas otras son que los delincuentes hagan sus “actividades” utilizando tu red, y, desafortunadamente, por medio de esto, pueden inculpar al dueño de la red. Otras cuantas incluyen enormes, y de verdad que lo son, robos a cuentas bancarias, o robo del pin de tu tarjeta de crédito, ¿cómo? Muy sencillo, al tener libre acceso a tu red, un hacker puede rastrear las contraseñas de tus cuentas, y con ellas, tiene el poder que necesita para hacerte la existencia un infierno si eres de aquellas personas que utilizar Internet para realizar pagos y hacer compras (algo muy común actualmente).

Grandes desfalcos a compañías han ocurrido por hackers que ingresaron a su sistema, quizás por que no estaba protegido, o porque su protección era muy baja, pero los usuarios sufrieron las consecuencias de no tener una red protegida. Nadie está a salvo de un hacker experto, un ejemplo reciente fue el Pentágono, que es el sistema de defensa de Estados Unidos, fue hackeado por un personaje de la Internet, un hacker muy famoso, conocido como Anonymus, creando pánico en el FBI y la policía estadounidense.

**Conclusión**

La tecnología Wi-Fi sin duda facilita la vida cotidiana de las personas. Gracias a esta, los usuarios ya no dependen de un cable para poder utilizar servicios en Internet. Y es por los múltiples beneficios que nos otorga, que tiene muchos pro’s tenerla segura. Si bien es poco probable que un hacker famoso venga a robarnos nuestra información, no estamos a salvo de los delincuentes comunes, y por eso, es de vital importancia para el usuario cotidiano el tener protegida su red.

Destaca lo inseguro que puede ser el cifrado WEP, pero hay que recordar que fue el primer tipo de cifrado para redes, y durante muchos años fue la única alternativa para mantener segura la información. Hoy día es un método muy vulnerable a los ataques externos así que conviene informarnos sobre las nuevas opciones de cifrado que nos ofrecen nuestro proveedores, desde WPA hasta WPA2, que han demostrado ser lo más eficaces en seguridad, y por tanto, los más complicados de accesar para obtener la clave.

También hay que tener en cuenta que hoy Internet provee las herramientas necesarias para burlar la seguridad, el concepto de hacker que teníamos: un experto de computadoras con un equipo sofisticado, ya no es el mismo, actualmente, hay videotutoriales que explican paso a paso como utilizar los programas diseñados para descifrar la seguridad de una red

Tanto por la tranquilidad del usuario, como la de la empresa que nos provee el servicio, la empresa en la que trabajamos, o en donde quiera que utilicemos dicha conexión. Averiguar sobre las maneras de proteger nuestra red, aunque nos parezca aburrido, es por nuestro propio bien, e incluso hay una enorme cantidad de tutoriales, manuales y consejos en Internet sobre como protegerla, variando sobre lo que busquemos, desde las configuraciones básicas, hasta los más altos protocolos de seguridad que podemos implementar en nuestro equipo.

**Bibliografía**

<http://www.eset-la.com/pdf/documento_guia_de_wifi.pdf>

(2010, 06). Seguridad en Redes. BuenasTareas.com. Recuperado de <http://www.buenastareas.com/ensayos/Seguridad-En-Redes/465169.html>

(2010, 06) Hipótesis- Seguridad en redes inalámbricas. BuenasTareas.com. Recuperado de <http://www.buenastareas.com/ensayos/Hipotesis-Seguridad-En-Redes-Inalambricas/432857.html>

(2009, 12) Tipos de Cifrados de una red WiFi. [Solodecomputacion.blogspot.mx](http://solodecomputacion.blogspot.mx/). Recuperado de <http://solodecomputacion.blogspot.mx/2009/12/tipos-de-cifrados-en-una-red-wifi.html>