INDICE

Seguridad en Redes Inalámbricas, para hogares y empresas pequeñas.

Harold Alfaro Castillo[1]

Resumen:

Está dirigido a personas en sus casas y a empresas pequeñas que necesitan hacer uso de la tecnología de redes inalámbricas, y que por falta de información o de asesoramiento no cuentan con la seguridad recomendable.

Presenta de manera general y sencilla lo que es Seguridad Inalámbrica, tratando que las redes inalámbricas sean más seguras al seguir algunas recomendaciones.

Analiza aspectos importantes que se deben tomar en cuenta cuando se instalan dispositivos inalámbricos, para garantizar que la información esté segura ante vulnerabilidades o ataques de hackers.

Finalmente, señala buenas prácticas para aplicarlas en el uso de la tecnología inalámbrica y, recomienda algunos equipos que ofrecen diferentes servicios de acuerdo a las necesidades del usuario.

Palabras clave: Seguridad Inalámbrica, redes cableadas, WLAN, IEEE, 802.11b, 802.11g, 802.11b, 802.11i

Abstract:

It is directed to people in its houses and small companies that need to make use of the technology radio networks, and that by lack of information or advising do not count on the recommendable security.

It displays of general and simple way what is Wireless Security, treating that the radio networks are safer when following some recommendations.

It analyzes important aspects that they are due to take into account when wireless devices settle, to guarantee that the information is safe before vulnerabilities or attacks of hackers.

[1] Bachiller en Ingeniería Informática, candidato a Licenciado en Informática con Énfasis en Redes y Sistemas Telemáticos

Finally, it indicates good practices to apply them in the use of the wireless technology and, it recommends some equipment that offers different services according to the necessities of the user.

Keywords: Wireless Security, redes cableadas, WLAN, IEEE, 802.11b, 802.11g, 802.11b, 802.11i, seguridad

Introducción.

En los últimos años la tecnología ha ido en avanzada y los mercados buscan las mejores formas para innovar y hacer que ésta sea de ayuda para que las empresas puedan tener mayor productividad.

Es así como de una forma silenciosa las redes inalámbricas o Wireless Network, que es el término más tradicional para señalar a las redes de telecomunicaciones cuyas conexiones entre cada punta de intersección es implementada sin usar cables, se han estado introduciendo en el mercado de consumo, gracias a su bajo costo y facilidad de utilización.

El objetivo primordial de las redes inalámbricas es proporcionar las facilidades de conexión donde el cableado normal no está disponible, lo que conlleva a tener un ahorro por instalación del tradicional cableado de redes.

Pero como toda tecnología, tiene riesgos inherentes a la utilización del medio de transmisión, como son las ondas de radio, por lo que se deben tomar medidas para asegurar que los riesgos en cuanto a seguridad sean los mínimos para aquellos clientes de hogares y pequeñas empresas que desean utilizar esta tecnología y así abaratar los costes de sus redes caseras.

Aunque hay muchos libros en los cuales se habla profundamente acerca del tema de Seguridad Inalámbrica, el objetivo de este trabajo es introducir los conceptos básicos de Seguridad y buenas prácticas que se deben tomar en cuenta a la hora de pensar en hacer una red inalámbrica doméstica o para una empresa pequeña.

I. ¿Qué son las redes inalámbricas?

Una red de área local inalámbrica se define como una red de alcance local o doméstica, que usa medios no guiados, para hacer transmisiones a través del aire, lo cual brinda movilidad sin usar cables. Estas redes cubren un contorno limitado, con una tasa o carga de transferencia de datos relativamente alta mayor o igual a 10 Mbps.

Utiliza ondas electromagnéticas para transmitir la información que viaja a través del canal inalámbrico enlazando los diferentes dispositivos o terminales móviles asociados a la red. Estos enlaces se implementan básicamente a través de tecnologías de microondas y de infrarrojos.

Por su movilidad y rápido acceso, el sistema inalámbrico se usa más a menudo en lugares públicos, como restaurantes, aeropuertos, hoteles, etc., y como complemento en una red LAN (Local Area Network).

El auge que ha tenido esta tecnología en los últimos años se ha ido incrementando y, próximamente, desde el hogar y sentado en el escritorio de trabajo, se podrá tener acceso a Internet inalámbrico; aunque no es la única tecnología que permite el acceso a Internet desde el hogar, es una solución para aquellas localidades donde el acceso es difícil por la infraestructura que pueda tener el proveedor de servicios.

Tratar el tema de redes inalámbricas, es referirse a un sistema que permite la conexión a Internet sin hilos; pero, no es necesariamente una red con acceso a Internet, ya que los equipos inalámbricos pueden ser utilizados en una empresa pequeña o red doméstica para hacer uso de servidores de impresión, transferencia de archivos; sin embargo al igual que cualquier otra red inalámbrica, debe llevar su seguridad para evitar que personas no autorizadas hagan uso de las mismas o puedan utilizar herramientas para descodificar información relevante de la empresa. Además, hay otras tecnologías para utilizar la Internet como los son ADSL y Cable Modem, que son conexiones que utilizan los cables de tendido telefónico; no obstante cuando se utilizan estos dispositivos de conexión, la red se torna vulnerable a ataques y; por lo tanto, se deben de tomar las medidas de seguridad necesarias.

Los ataques contra la seguridad de la red inalámbrica crecen día tras día por lo que, si se instala este servicio en un hogar o una empresa pequeña, se deben de tomar medidas para evitar las amenazas a la confidencialidad de los datos importantes y de la información de los usuarios.

II. ¿Surgimiento de las redes inalámbricas?

Los primeros indicios de comunicación inalámbrica datan del año 1901 con el descubrimiento por el físico Gluglielmo Marconi, del teléfono inalámbrico de barco a costa utilizando el código Morse. Más adelante en el año 1979 se publican los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

III. Estándares de protocolo inalámbrico.

En febrero de 1980 el IEEE (Instituto de Eléctricos y Ingenieros Electrónicos) comenzó un proyecto llamado estándar 802 basado en conseguir un modelo para permitir la intercomunicación de ordenadores para la mayoría de los fabricantes, y que se desarrolló paralelamente con el modelo OSI, pero que es específicamente para hardware. (Fernández, 2007).

IEEE 802.X, es un conjunto de normas que definen las características físicas y de enlaces de las redes LAN, dictadas por el IEEE, que es una asociación internacional formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de computación e ingenieros en telecomunicación.

Este artículo se centra en el apartado sobre la normativa 802.11 y sus subapartados que describen una interfaz inalámbrica y que es compatible con la norma IEEE 802.

802.11 Redes Inalámbricas.

El comité de la 802.11 es un comité que define estándares para las redes inalámbricas, como son: el ancho de banda, las frecuencias y las modificaciones que se le puedan hacer a esta tecnología

Estas normas pretenden que las tecnologías sean concomitantes entre ellas para poder minimizar los problemas al usar las tecnologías juntas, como son los costes por instalación y la protección.

La IEE ha confirmado tres tipos de normas como lo son: 802.11b, 802.11g, 802.11a.

802.11b

- Tiene una velocidad máxima de datos de hasta 11 Mbps por canal.
- Ofrece una penetración mejor a través de muros y otros obstáculos, y mayor alcance en la oficina, el hogar y otros entornos cerrados.

Es el estándar inalámbrico más ampliamente usado.

802.11g

- Ofrece todas las ventajas del 802.11b, y además una velocidad de transferencia de datos de hasta 54 Mbps.

Compatible con 802.11b; constituye una buena opción para empresas cuyos usuarios utilicen portátiles con el estándar 802.11b y que necesiten más velocidad para futuras aplicaciones.

802.11a

- También ofrece una velocidad de datos de hasta 54 Mbps, pero funciona en una banda de frecuencia independiente de 5 GHz
- Cuenta con un número adicional de canales sin solapamiento que aumenta el rendimiento al tiempo y la facilidad de ampliación.

No es compatible con 802.11b ni con 802.11g, pero puede coexistir con estos estándares sin afectar en el rendimiento

Como en las primeras tecnologías se detectaron fallas a nivel de seguridad, la IEEE se ha dado a la tarea de definir el estándar 802.11i, para contrarrestar la vulnerabilidad de los protocolos de autenticación y de codificación. Estas mejoras incluyen varios protocolos como lo son TKIP (Temporal Key Integrity Protocol) y AES (Estándar de Cifrado Avanzado), que uno se refiere a codificar claves íntegras, seguras y temporales, y; el otro es un protocolo de encriptamiento avanzado.

Tabla de los estándares inalámbricos

Característica	**Definición**	**802.11b**	**802.11g**	**802.11a**
Canales de radiofrecuencia disponibles	Numero de enlaces de comunicaciones	3 sin solapamiento	3 sin solapamiento	8 o más sin solapamiento (varía según el país)
Velocidad máxima de datos por canal	Velocidad máxima por canal de radiofrecuencia	11 Mbps	54 Mbps	54 Mbps
Banda de frecuencia	Rango de frecuencia de transmisión	2,4 GHz	2,4 GHz	5 GHz
Alcance habitual	Distancia que pueden recorrer los datos y a qué velocidad	30 m a 11 Mbps 90 m a 1 Mbps	15 m a 54 Mbps 45 m a 11 Mbps	12 m a 54 Mbps 90 m a 6 Mbps

Fuente: Intel, 2007.

IV. Ventajas y Limitaciones de las Redes Cableadas (LAN) y Redes Inalámbricas (WLAN).

Redes Cableadas:

Se entiende por redes cableadas aquellas que son usadas con cable UTP (UTP (del inglés: Unshielded Twisted Pair, par trenzado no apantallado) es un tipo de conductor utilizado, principalmente para comunicaciones), que es el tipo de cable más usado en las redes y que puede ser de diferentes categorías como por ejemplo: categoría 5e o categoría 6 y, que dependiendo de su diseño, se pueden construir redes simples como poder interconectar dos o tres computadoras entre sí, o tan complejas como interconectar miles de ellas.

Entre los diferentes tipos de redes se pueden encontrar las Redes personales (PAN), Red de área Local (LAN), Red del área de campus (CAN), Red de área Metropolitana (MAN) y Red de área amplia (WAN).

Cada una de ellas tienen sus propias características y su propio diseño. Algunas ventajas y limitaciones de usar redes cableadas son:

Ventajas

1- Flexibilidad en la localización de la estación.
2- Fácil instalación.
3- Menores tiempos en la reconfiguración.
4- Menor coste.
5- Diseño.

Limitaciones

1- Reparaciones costosas.
2- El tiempo medio entre fallas es menor.
3- El tiempo de reparación es mayor.
4- Dificultad para el tendido del cableado o la reutilización de éste.
5- Mayor tiempo de instalación.

Redes Inalámbricas:

Como se ha dicho anteriormente es una red que no utiliza cables; usa el aire como medio de transmisión y, lo interesante al usar estas redes es que no es necesario que el otro punto de referencia sea visible para poder conectarse. Además puede ser usada para accesar a Internet o como una red Lan doméstica. (WLAN).

En sus inicios esta red que en su principio fue evolucionando lentamente debido a factores como falta de normas, la oferta y la demanda y por problemas de la misma tecnología; pero en los últimos años se ha visto afectado por el avance tecnológico y su crecimiento va en aumento. Algunas ventajas y limitaciones que se pueden encontrar son:

Ventajas:

1- Buenas características de desempeño.
2- Resistencia a la interferencia externa.
3- Seguridad.
4- Bajos costos de operación.
5- Facilidad de instalación.
6- Facilidad en el mantenimiento y detección de fallas.
7- Útil en ciertas circunstancias geográficas.
8- Menor tiempo de instalación.
9- Buen nivel de integración con redes tradicionales existentes.
10- Mínima capacitación para la instalación.

Limitaciones

1- Calidad de servicio.
2- Velocidad de transmisión limitada.
3- Potencia y distancias limitadas.
4- Alto costo por unidad.

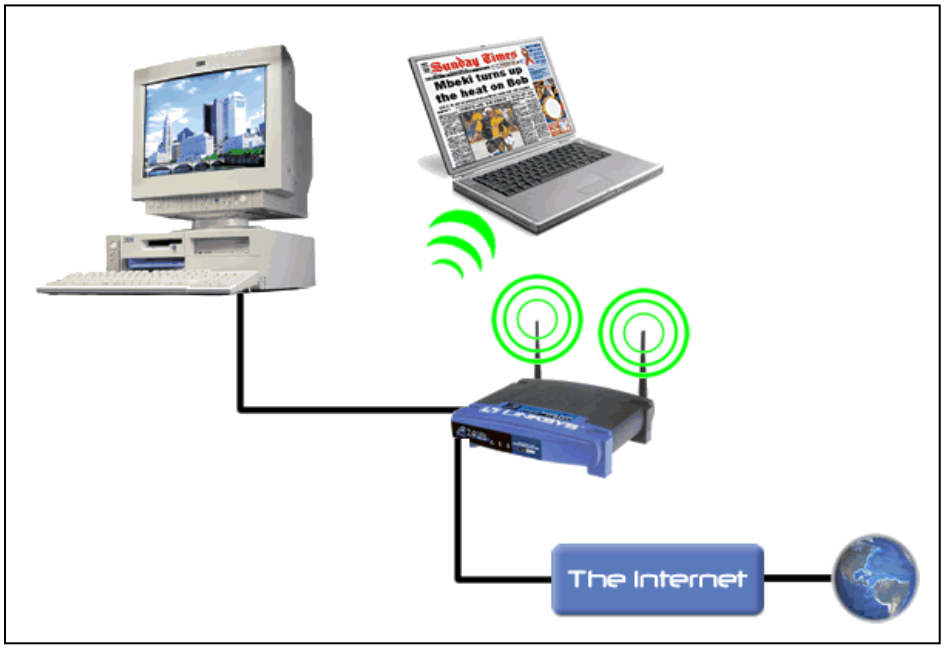

Figura No. 1. Acceso inalámbrico doméstico

V. Principios de Seguridad

El aspecto de seguridad en las redes es una necesidad vital; esto implica que se deriven ciertos aspectos importantes que se deben tomar en consideración como:

- La Confidencialidad: este aspecto tiene que ver con las comunicaciones entre el cliente y el punto de acceso garantizado por el proveedor de servicios de la comunidad. Los datos importantes y la información de los clientes se tienen que mantener en confidencia y no tienen que estar disponibles para otras entidades.

- Integridad: significa la confianza en la información del negocio y los clientes.

- Disponibilidad: indica que los objetos del Sistema tienen que permanecer accesibles a elementos autorizados.

Por lo tanto, cuando se hace un diseño de seguridad, se debe tratar de reducir las vulnerabilidades de los sistemas inalámbricos ante posibles ataques cibernéticos o incidentes negativos que puedan producirse.

VI. ¿Qué es Seguridad?

Para iniciar este tema se citará la opinión de varios expertos en seguridad:

> Vivimos en una sociedad en que los recursos no son muchos para poder enfrentarse a cualquier problema que pueda ocurrir. El conocimiento del riesgo proporciona los medios necesarios para priorizar y asignar los recursos limitados de los que disponemos con el fin de llevar a la practica ciertas medidas para lograr reducir al máximo los riesgos de seguridad. (Martínez, 2006).

> La rápida expansión y popularización de Internet ha convertido a la seguridad en redes en uno de los tópicos más importantes dentro de la Informática moderna. Con tal nivel de interconexión, los virus y los hackers acampan a sus anchas, aprovechando las deficientes medidas de seguridad tomadas por administradores de red doméstica y empresas pequeñas a los que esta nueva revolución ha cogido por sorpresa. (Lucena, 1999).

Seguridad, enfocado desde un punto de vista tecnológico es el conjunto de políticas, procedimientos, controles y herramientas orientados a garantizar la confidencialidad, integridad y disponibilidad de la información. Para cumplir con este objetivo existen mejores prácticas, estándares y guías de implementación como la provista por BSI 7799 orientadas a la implementación de un SGS Sistema de Gestión de Seguridad. Esto por cuanto la simple adquisición de herramientas no es suficiente para garantizar la seguridad está debe gestionarse de forma integral. (Sebiani, 2007).

VII. Seguridad Inalámbrica en el mundo real

Las redes inalámbricas ofrecen la conveniencia de no requerir la instalación de los cables y de ofrecer movilidad a los usuarios, sin embargo desde el punto de vista de seguridad el medio se considera por defecto, inseguro, esto por que ante la aparición de una vulnerabilidad el nivel de exposición es mayor, dado que no requiere de acceso físico a las instalaciones de la empresa y de forma remota y cómoda se podría explotar una eventual vulnerabilidad.

Para efectos de los usuarios, es importante evitar el uso de redes públicas o gratuitas, dado que se desconoce el nivel de seguridad de ellas y podrían estar siendo utilizadas para capturar información. Muchas veces el usuario piensa que se está aprovechando de un vecino que tiene un enlace no asegurado, pero podría ser que éste se esté aprovechando de esa conexión ilícita para capturar y obtener información sensible tal como claves de acceso bancarias. Es importante que los equipos de los usuarios se mantengan debidamente actualizados y tengan un firewall personal, un antivirus y un antispyware activados.

VIII. Buenas prácticas en Seguridad Inalámbrica

En este apartado se pretende dar algunas herramientas para los hogares o empresas pequeñas que quieran utilizar algún sistema inalámbrico que les permita minimizar los riesgos y evitar daños en el diseño de su red.

Al tratar el tema de Seguridad Inalámbrica para hogares y empresas pequeñas esté donde esté, ya sea hacia la red interna o su acceso a la

red de Internet, se busca proteger su inversión y la información ante los peligros de pérdidas o robos de identidad, virus o gusanos, spam, spyware y redes zombis entre otros.
Pero, ante estos peligros, los hogares y empresas pequeñas deben de tener en cuenta antes de instalar su red inalámbrica la ecuación de la seguridad que implica: seguridad va a ser igual a tecnología adquirida más el factor humano, que será al final el que defina las políticas de seguridad que eventualmente se configurarán y darán protección a la información de la empresa o del hogar.

Ante este panorama en las redes inalámbricas, se debe planificar su seguridad ante algunos desafíos como lo son:

- Que cualquier persona con su portátil inalámbrica en un radio de 100 metros, potencialmente puede ser un intruso.
- Brindar los accesos a los usuarios de la red, deben darse con la implementación debida en seguridad.
- Las configuraciones hacia la red de conexión, deben asegurarse que sean las correctas, para evitar una conexión errónea o ser un intruso potencial en otra red.
- La información se debe transmitir con seguridad implementando la utilización apropiada de las llaves de encriptamiento necesarias.

Ante estos desafíos, y la falta de implementación de políticas de seguridad en algunos hogares o empresas pequeñas debido a su falta de capacitación o información, se muestran a continuación varios mecanismos de seguridad para proteger las redes inalámbricas:

- SSID (Service Set Identifier)

El SSID es una norma incluida en todos los equipos de acceso inalámbrico y sirve para reconocer a los equipos que pertenecen a esa red en particular. La norma consta de un máximo de 32 caracteres alfanuméricos; por lo que, todos los equipos que intentan interactuar entre ellos se deben identificar con el mismo SSID. Ésta es una contraseña simple que identifica la red inalámbrica, no es, en sí, una medida de seguridad ya que no está encriptada, sino que es una unidad para organizar y gestionar una WLAN en diferentes sectores de llegada donde tengan que entenderse los diferentes equipos en el mismo canal; esto permite la creación de grupos de trabajo 'lógicos' aislados en el mismo sector (parecido a las redes virtuales VLANs). Tanto los dispositivos que se conectan como el punto de acceso se identifican con el mismo SSID. El uso del SSID como procedimiento único de control de

seguridad de entrada a la infraestructura es peligroso, ya que, en sí mismo, este mecanismo no es seguro.

- Filtrado por dirección MAC (Media Access Control)

La dirección MAC (Media Access Control) es un número que se encuentra incluido y codificado en cada tarjeta de los dispositivos de la red y que lo identifica como único.

Está constituida por seis pares divididos por un guión, los cuales representan la identificación, el modelo de la tarjeta y el fabricante.

Es uno de los métodos de protección de redes inalámbricas WIFI más antiguo y menos eficaz que existen, debido a que tiene muchas desventajas y puntos débiles.

Este método de filtrado de direcciones MAC / MAC Address, consiste en introducir en cada Punto de Acceso Inalámbrico un registro de hasta doce direcciones MAC de los equipos de los clientes que están autorizados a conectarse a la red. De esta manera, los equipos que no se encuentren en la lista quedan rechazados.

Las desventajas de este método son las siguientes:

1. Si hay muchos Puntos de Acceso en la empresa se pueden producir errores al teclear la dirección MAC repetidamente en todos los Puntos de Acceso. Esto producirá un falso positivo dentro de la red, ya que son usuarios "legales" que son rechazados.
2. Si hay muchos Puntos de Acceso dentro de la organización el introducir todas las MAC Address es muy trabajoso.
3. La transmisión de los paquetes de datos no va generalmente encriptada; por lo tanto, puede ser capturada por un hacker.
4. La Dirección MAC es una característica del hardware de la computadora del cliente y no directamente del usuario. Si el hardware (PC, PDA, USB, etc.) se extravía o es robado, la persona que lo encuentre podrá tener libre acceso a la red inalámbrica WIFI, ya que pasaría el control del filtro.

- Cifrado WEP (Wired Equivalency Privacy)

Cuando se desarrolló el 802.11b, se pretendía que WEP (Privacidad equivalente de cable) hiciera lo que su nombre dice: ofrecer privacidad en la red. Cualquier intruso debía de instalar algún software para rastrear todo el tráfico de la red. En ese entonces, WEP se diseñó para

que cualquier intruso pudiera penetrar en la red inalámbrica. Se comprobó que este método no es del todo eficiente, sino que se debe de acompañar de otras medidas de seguridad, por lo que este protocolo lo que hace es cifrar los datos que van a través de la red, impidiendo que se puedan rastrear.

Funcionamiento del cifrado WEP.

El algoritmo de encriptamiento WEP utiliza una llave oculta compartida basada en el algoritmo de cifrado RCA. Tanto los dispositivos desde el cliente que se quieran conectar hasta el punto de acceso (PA), deben utilizar la misma llave compartida.

En general, el usar una llave compartida es inseguridad en las redes inalámbricas, ya que si alguna persona descubre su significado, puede interceptar el tráfico y unirse a la red.

Si se va usar WEP, éste debería venir acompañado de otra herramienta de seguridad como las validaciones de los usuarios a través de VPN (Virtual Private Network) y la activación del cifrado a 128 bits; sin utilizar el cifrado WEP, cualquiera puede introducirse a la red.

- WPA (Wi-Fi Protected Access)

Es un protocolo para proteger el acceso a las redes inalámbricas, y fue creado para poder corregir las deficiencias de su antecesor WEP.

Para redes domésticas o pequeñas empresas, WAP utiliza un protocolo de integridad de clave temporal (TKIP) que se encarga de cambiar las claves dinámicamente a medida que el sistema es utilizado. Cuando se combina esta ventaja de la integridad de la clave temporal con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación de clave o ataques estadísticos a los que es susceptible el protocolo WEP.

Ventajas:

- Mejora la integridad de la información cifrada.
- Implementa un código de integridad del mensaje.
- Incluye protección contra ataques de repetición, gracias a que incluye un contador de tramas.
- Protege a las redes inalámbricas de accesos no autorizados.
- Tiene un sistema que desconecta la conexión durante 60 segundos al detectar dos intentos de ataque durante un 1 minuto.

- Recomendado para pequeñas empresas o redes domésticas.

Desventajas:

- Poco crecimiento para brindar mejores servicios.
- No soporta la autenticación de métodos extendidos (certificados, tarjetas inteligentes).
- No cumple en su totalidad con el estándar IEEE 802.11i, aunque comparable con el algoritmo WEP es más seguro.

- WPA2

WPA2 está basado en el nuevo estándar 802.11i de la IEEE. WPA2 se puede tomar como la versión certificada del estándar 802.11i, debido a que WPA es una versión previa, y no incluye todas las características del IEEE 802.11i, mientras que WPA2 sí las cumple.

WPA2; además de cumplir completamente con el estándar IEEE 802.11i también ofrece la autenticación de la conexión del lado del cliente como del servidor, haciendo más robusta la seguridad de la red inalámbrica. Por lo tanto, se recomienda configurar WPA2 modo enterprise para las empresas que deban cumplir con normas rigurosas de seguridad, y WPA para pequeñas domésticas, o para aquellos que no puedan implementar su red con la infraestructura de WPA2 empresarial.

- Uso del Protocolo RADIUS (Remoto Autenticación Dial-In User Service)

Es una tecnología de seguridad inalámbrica, que se basa en una estructura de AAA (Authentication, Authorization, Account), que consiste en autenticar, autorizar y arreglo de cuentas de usuario. Controla los accesos a las computadoras de la red, implementando políticas de seguridad y, analiza el uso de los recursos, los cuales son importantes para la administración y la implementación de la seguridad de la red.

Este protocolo está más orientado hacia aquellas empresas que tienen muchos accesos hacia la red, y que el nivel de seguridad va de la mano de normativas y buenas prácticas sugeridas por una Auditoria Interna.

El funcionamiento de la seguridad en AAA, es el siguiente: primero el usuario se comunica hacia el equipo remoto que le da acceso a la red, éste le envía la petición al servidor RADIUS, que auténtica primero la llave encriptada entre el cliente y el servidor; cuando se valida esta llave, se procede a autenticar al usuario dentro de la red; una vez

validado el usuario, se le asignan los derechos a los recursos dentro de la misma.

Estructura AAA

La estructura AAA utiliza tres aspectos importantes a la hora de identificar al usuario y validar sus credenciales:

Autenticación: es el método para identificar usuarios y comparar sus credenciales de acceso. Para que las credenciales del usuario sean autenticadas debe existir un servidor que compara las referencias de autenticación con la información almacenada; si las credenciales coinciden, se le da acceso a los recursos de la red, sino se le niega.

Autorización: Determina a cuáles recursos de la red tiene derecho el usuario.

Arreglo de cuentas de usuario: también llamado Contabilización de cuentas que consiste en: el proceso de medir y guardar el consumo de los recursos inalámbricos, permitiendo un efectivo monitoreo y reporte de los eventos que servirán para determinar una efectiva política de mantenimiento de la red.

- Llaves encriptadas, (AES-CBC-MAC, WRAP*),*

Las llaves encriptadas se usan para que la conexión entre el cliente y el servidor tenga mayor grado de seguridad y así evitar los accesos no autorizados a la red.

TKIP (Temporal Key Integrity Protocol)

En el estándar 802.11, WEP la encripción es opcional. Para WPA la encripción TKIP es requerida, por lo que TKIP remplaza a WEP con un nuevo algoritmo de encriptamiento que es más fuerte que el algoritmo WEP.

TKIP también prevé:

- La verificación de la seguridad de las llaves son determinadas después de la encripción.
- La sincronización cambia a una llave única para cada trama en la conexión.
- La determinación de una única llave de encripción para la autenticación de cada llave compartida.

- AES (Advanced Encryption Standard)

AES, también conocido como Rijndael, es un algoritmo de cifrado simétrico y que fue adoptado como un estándar de cifrado por el gobierno de los Estados Unidos en el 2001. Reemplaza a otro método de encriptamiento como lo es DES (Data Encryption Standard)

AES es más rápido en software y hardware que otros como DES. Utiliza poca memoria, por lo que también es una de las opciones de encriptamiento y seguridad para las redes inalámbrica.

Además, debido a la poca seguridad del algoritmo WEP, AES se ha convertido en una de las opciones para remplazarlo usando WPA, por lo que se considera muy seguro. A la fecha no se registra ningún ataque de éxito contra el algoritmo.

- EAP (Extensible Authentication Protocol)

Este protocolo es una extensión de Point-to-Point Protocol (PPP) que soporta múltiples métodos de autenticación, incluidos Kerberos, autenticación de clave pública (PKI) y tarjetas inteligentes. En 802.1X, EAP es encapsulado en el tráfico LAN o WAN, proporcionando el mecanismo para verificar la identidad de un usuario ante un servidor RADIUS u otra plataforma de autenticación.

Su funcionamiento es el siguiente:

Primero, entre el cliente y el servidor RADIUS, se realiza una autenticación EAP a través del protocolo 802.1x para establecer entre ambos una llave compartida llamada Pairwise Master Key (PMK). Como segundo paso, el servidor RADIUS envía la llave compartida PMK al punto de acceso; el cliente y el punto de acceso realizan un proceso denominado de "reconocimiento" en cuatro vías para establecer la llave de sesión que se llama Pairwise Transient Key (PTK).

IX. Equipos inalámbricos recomendados

En el mercado de los equipos inalámbricos para hogares y empresas pequeñas hay mucha variedad. Existen equipos que solo sirven para hacer la conexión inalámbrica hasta aquellos más inteligentes donde el equipo puede ser una pared de fuego, y hasta pueden usarse en el servicio de voz sobre ip (VOIP).

Cuando se va adquirir uno de estos equipos, lo que primero que debe analizarse es para qué quiero el equipo y cuáles son las utilidades que éste va a tener, ya que el mercado de tecnología inalámbrica se actualiza constantemente y los equipos quedan obsoletos. Se debe planificar muy bien las inversiones: compro hoy pensando en el día de mañana.

A continuación se expondrán tres marcas de equipos diferentes, sin ahondar profundamente en el detalle de los mismos, ya que lo que se pretende es dar una visión de qué equipo y características se puede adquirir y qué tipo de servicios se puede eventualmente, instalar en los mismos.

Recomendación de equipos Inalámbricos:

Las redes inalámbricas de área local (WLAN) mejoran día tras día, lo cual implica mayor productividad y nuevos equipos que vienen a solucionar en muchos casos los altos riesgos ante un ataque malicioso a la red; pero, así como mejoran estos productos, también pueden constituir una amenaza para la seguridad de las empresas.

Los puntos de acceso (AP) no autorizados en una WLAN insegura pueden ocasionar robo de información en la red por hacker potenciales, ocasionando que los bienes importantes y la información confidencial sobre la empresa, los clientes, los productos y servicios sean vulnerables. Otras amenazas, incluyendo los ataques de denegación de servicio (DoS), así como la asociación con puntos de acceso incorrectos o mal configurados pueden generar vulnerabilidades adicionales, y dolores de cabeza que no aplican una seguridad efectiva en sus accesos inalámbricos.

Ante estos escenarios de la seguridad, se presentan tres tipos de dispositivos inalámbricos, los cuales pueden ser de mucha utilidad en las redes domésticas:

- ADSL X6 ZOOM, modelo 5590

Modem ADSL2/2 + es un equipo que brinda hasta una velocidad de 125 Mbps, consta de un enrutador incorporado para acceso compartido a Internet hasta para 253 usuarios concurrentes, tiene un switch incorporado de 4 puertos Ethernet 10/100, lo cual permite hacer conexiones con redes cableadas. En cuanto a la seguridad inalámbrica incluye seguridad avanzada contra los ataques de los hackers usando:

- Inspección de Paquetes "Stateful" (SPI).
- Filtración de Paquetes.
- Prevención y detección de ataques por Negación de Servicio (DoS) y Supervisión de Puertos.
- Protección contra IP Spoofing y otros ataques comunes.

Además de su fácil instalación y manejo, cuenta con soporte de ADSL2/2, esto quiere decir que el X6 funciona con los dos protocolos de ADSL y con la nueva generación de conexiones Internet de alta velocidad.

El modelo 5590 X6 ZOOM, viene con la tecnología Prism Nitro Mode que minimiza el problema de colisión que se crea cuando se mezclan dos tipos de redes de tecnologías diferentes como 802.11b y 802.11g y aumenta el desempeño de la red. En cuanto a la seguridad inalámbrica incluye el protocolo más reciente, Acceso Protegido Wi-Fi (WPA) como también Protección Cableada Equivalente (WEP).

- Linsys Wireless –G – Broadband Router

Linksys Wireless-G Broadband Router es equipo para redes domésticas, que hace la función de cuatro dispositivos en una sola caja.

Primera función, es un punto de acceso inalámbrico, el cual permite conectar los dispositivos de ambas tecnologías: la 802.11b en 11Mbps y 802.11g en 54Mbps.

Segunda función, tiene incorporado un switch, con 4 puertos Ethernet con velocidad 10/100 Mbps, en los cuales se pueden conectar directamente cuatro dispositivos con cableado UTP, o agregar otros equipos hasta poder formar una red bastante grande.

La tercera función, es un router, lo que permite compartir el acceso de ADSL de alta velocidad de Internet para toda la red.

La cuarta función es el adaptador del teléfono con dos conectores RJ 11, que permite el servicio telefónico de alta calidad a través de la conexión, incluso se puede estar navegando en Internet y utilizar el servicio telefónico sobre Internet.

Para proteger y dar privacidad a los datos, el router de banda ancha, puede codificar todas las transmisiones inalámbricas con el cifrado de

hasta 128 bits; además, tiene soporte en protocolo de seguridad WEP, WPA.

El router puede funcionar como servidor DHCP; tiene un firewall incluido para proteger las computadoras de la red de los intrusos y de los ataques conocidos de Internet.

Con Linksys Wireless-G Broadband Router en el hogar o empresa pequeña, se puede compartir una conexión de alta velocidad de Internet, compartir archivos, impresoras, y juegos multi-usuario, y así como disfrutar del valor agregado de un servicio telefónico de alta calidad.

- 3COM AirProtect Sentry 5850

Este es un dispositivo, sensor inalámbrico, el cual escanea las ondas inalámbricas y provee a las pequeñas empresas o redes domésticas de un sistema de prevención de intrusos inalámbricos contra cualquier actividad inalámbrica no autorizada.

Los beneficios de adquirir uno de estos equipos, es la protección expuesta ante punto accesos inseguros, o cuando los usuarios se conectan a uno incorrectamente. Este dispositivo 3COM AirProtect Sentry 5850 sistema de prevención de intrusos inalámbricos, pueden controlar los accesos de todos los dispositivos, ayudando a proteger la información de la empresa.

En un contexto tradicional los firewalls o pared de fuego, tienen como función monitorear el tráfico de la red aunque no puede ver que está en el aire; pero, este equipo o dispositivo provee la solución a estos problemas y da un mayor grado de seguridad a la red.

Entre sus características están la de ser compatible con las normas de seguridad de la IEEE 802.11a, 802.11b, 802.11g y tener una línea de comandos por consola a través del protocolo SSH v2, la cual facilita su configuración, que en aproximadamente 15 minutos ya está funcionando.

Otra función de este equipo, es su compatibilidad con cualquier punto de acceso (AP) de cualquier vendedor; no necesita reemplazar el equipo y puede obtener mejor protección a su red.

Conclusiones y Recomendaciones

La seguridad de un usuario de Internet depende en gran medida de él, ya que la entidad que presta el servicio de conexión solo puede garantizar la seguridad de las aplicaciones comunes pero en lo referente a correos y transferencia de archivos en usuario, normalmente, tiene el control y la responsabilidad.

Tanto las políticas de seguridad en el acceso como los sistemas de encriptamiento dependen, en su mayor parte de la habilidad que se tengan para implementarlas; este hecho es incluso más relevante que el costo de los equipos que se utilicen para desarrollar el sistema de seguridad, sobre todo para el caso del código encriptado.

También, por la globalización que ha tenido Internet a partir de la última mitad de década, los ataques a redes privadas se han incrementado a tal punto que se puede decir que es casi de uso obligatorio la implementación de firewalls y/o proxis entre la Intranet e Internet.

En caso de utilizarse tecnología inalámbrica es importante considerar algunas otras recomendaciones como:

1. Utilice autenticación a nivel de red y de usuario. Antes de permitir la conexión a la red, el equipo y el usuario deberá autenticarse contra un sistema central de autenticación y no de forma local.

2. Utilice el esquema de encripción más robusto con que cuente el dispositivo de acceso, en este momento Wi-Fi Protected Access (WPA). No se debe utilizar WEP.

3. De preferencia utilice cable irradiante para limitar la cobertura del acceso y evitar que la señal llegue fuera del radio requerido.

4. Cambiar el identificador de la red no implica en sí seguridad pero podría hacer que se llame menos la atención, si el identificador de red indica algo como "Empresa-XX" lo más seguro es que, alguien intentando ingresar a la Empresa, se concentrará en ese enlace.

5. Deshabilitar las conexiones automáticas hacia las computadoras para evitar que usuarios no autorizados puedan hacer uso de la red.

6. Utilizar las conexiones encriptadas, ejemplo WPA2, la cual garantizará que realmente los usuarios que están conectados en la red son los

verdaderos y pueden hacer uso de recursos de la red interna o de internet.

7. Deshabilitar el acceso remoto hacia los Access Point, o el dispositivo que se esté usando para la conexión inalámbrica.

8. Localizar las conexiones en VLAN inalámbricas separadas para procurar la administración efectiva de red, conociendo cuáles usuarios están conectados en las diferentes redes lógicas creadas en el dispositivo.

9. Cuando se haga uso de la red inalámbrica, se debe procurar limitar la cantidad de conexiones con el fin de controlar el funcionamiento de su red y tratar de dar un mejor aprovechamiento del canal de conexión.

10. En lo que se pueda a su red y dependiendo de la cantidad de usuarios a conectar al dispositivo inalámbrico, hacer uso efectivo a través de la validación del usuario con Radius, lo cual permitirá un buen manejo de la administración de los usuarios o vecinos que comparten su red, o su acceso inalámbrico, además asegurará que ningún intruso pueda filtrarse y hacer uso de la red.

Bibliografía:

IEEE 802 Working Worgroup. (2007). *IEEE 802*. Tomado de http://grouper.ieee.org/groups/802/dots.html, el 05 de Junio 2007.

Fernández, Gonzalo. (2001). *Estándar IEEE 802*. Tomado de: http://docente.ucol.mx/al008364/public_html/redes/tarea3.htm, el 05 de Junio del 2007.

Intel. (2007). *Redes Inalámbricas para las Pymes*. Tomado de: http://www.intel.com/cd/business/enterprise/emea/spa /235485.html, el 06 de Junio 2007.

León, Jimmy. (2003). *Redes Inalámbricas*. Tomado de http://www.monografias.com/trabajos12/reina/reina.zip, el 05 de Junio 2007.

López, Edgar. *Introducción Origen de las redes inalámbricas*. Tomado de http://personales.com/colombia/bucaramanga/redeswlan/introduccion.htm, el 05 de Junio 2007.

Lucena, José. (1999). *Criptografía y Seguridad en seguridad*. Tomado de http://www.wikilearning.com/seguridad_en_redes-wkccp-15516-56.htm, el 05 de Junio del 2007.

Manuales Lucas. (2003). *¿Que es Seguridad?* Tomado de http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node8.html, el 05 de Junio 2007.

Martínez, Diana. (2006). *Protocolo de Seguridad Inalámbrica WEP*. Tomado de http://www.ofdnews.com/comentarios/2331_0_1_0/, el 05 de Junio 2007.

Padilla, Daniela. (2006). *Seguridad en redes teleinformáticas y telecomunicaciones*. Tomado de http://pdf.rincondelvago.com/seguridad-en-redes-teleinformaticas-y-telecomunicaciones.html, el 05 de Junio del 2007.

Pérez, Marta. (2005). *ADSL X6 ZOOM, modelo 5590*. Tomado de http://www.noticias.com/notaprensa/19-04-2005/sim/zoom-lanza-nuevo-modem-x6-adsl22-4kn.html, el 15 de Julio 2007.

Sebiani, Alejandro. (2007). *Seguridad Inalámbrica en el mundo real*. Banco de Costa Rica.

Varela, Carlos. Domínguez, Luis. (2002). *Redes Inalámbricas*. Tomado de www.blyx.com/public/wireless/redesInalambricas.pdf*, el 04 de Junio 2007.*

Wikimedia Foundation, Inc. (2007). *WLAN*. Tomado de http://es.wikipedia.org/wiki/WLAN#Punto_de_partida_o_inicio, el 05 de Junio 2007.

Wikimedia Foundation, Inc. *Red Inalámbrica*. (2007). Tomado de http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica, el 05 de Junio 2007.

Wikimedia Foundation, Inc. (2007). *SSID*. Tomado de http://es.wikipedia.org/wiki/SSID, el 05 de Junio del 2007.

Yanover, David. (2004). *802.11 Seguridad - Protección Wireless*. Tomado de: http://www.mastermagazine.info/articulo/3123.php, el 05 de Junio del 2007.