Diseño de una arquitectura de seguridad para redes MESH en entornos comunitarios o rurales de Colombia

A. C. Lozano & F. Blanco

I. INTRODUCCIÓN

A medida que pasa el tiempo la forma de usar las redes tecnológicas tienden a ser inalámbricas, evitando infraestructuras de alto costo o complicaciones de las mismas, de igual manera se habla de tener la información al instante con la mayor movilidad y comodidad del caso en un mundo empresarial o laboral, comunitario e inclusive personal, donde lleva al uso de tecnologías enfocadas a las redes inalámbricas para lograr el acceso de los servicios ofrecidos por parte de los usuarios de forma rápida, así que es momento de hablar de las redes MESH o también conocidas como redes en malla trabajadas en una frecuencia determinada de 2.4 GHz y 5.4 GHz, posibilitando a los usuarios disponer del 80% más de los canales libres para un mayor uso, además aumentando el número de usuarios concurrentes en un 60-80%.

A comparación de las redes WIFI que presentan algunas falencias en su manejo frente a dispositivos y dependiendo de los sectores comunitarios y rurales del país, además con la deficiencia frente a la prestación de los servicios de las redes de computadores, debido a los altos costos y los diferentes problemas que se presentan en su conectividad.

Hechos que dan importancia de conocer y dar uso de las características de las redes MESH, pues requieren de otra alternativa para realizar interconectividad de las comunidades y de las áreas rurales de Colombia, independientemente de la existencia de algunos intereses económicos por parte de los diversos actores que llegan a intervenir, factor que favorece la configuración de las redes en malla.

Son varias las características que benefician las comunicaciones remotas entre los equipos y a su vez las tecnologías de información que son gran apoyo de las aplicaciones de INTERNET, las cuales brindan sus servicios, para la trasferencia de archivos, el acceso, subida y descarga de contenidos de todo tipo sin restricciones.

Así como cuenta con características especiales que hacen de las redes MESH la mejor alternativa, existe un camino que permite la desconfianza para su uso, la cual es la seguridad que se presenta en estas, motivo por el cual se lleva a cabo este proyecto con el objetivo general de Diseñar una arquitectura de seguridad para redes MESH en entornos comunitarios o rurales de Colombia, el cual se enfocara a la investigación de los protocolos de seguridad que se llevan a cabo en las redes MESH o Malla

A.C. Lozano. Universidad Libre de Colombia. Andreac.lozanol@unilibre.edu.co

F. Blanco Garrido. Docente Investigador Universidad Libre de Colombia, Bogotá – Colombia Fabian.blancog@unilibre.edu.co

Corresponding author: A.C. Lozano

I. RED EN MALLA O MESH

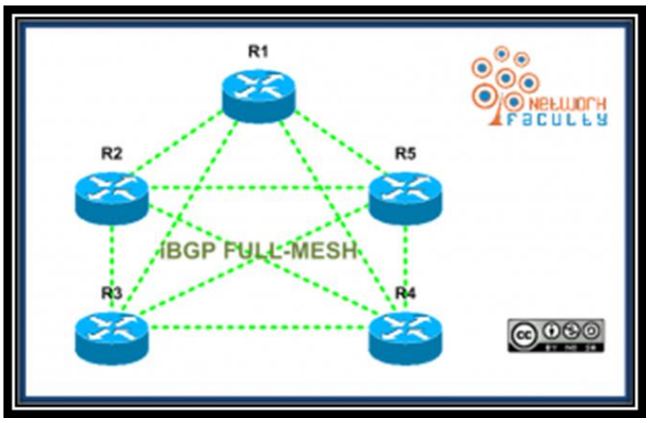
Estas redes también conocidas como redes acopladas o redes de malla inalámbricas de infraestructura. Son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas, la topología Ad-hoc y la topología infraestructura. Básicamente son redes con topología de infraestructura pero que permiten unirse a la red a dispositivos que a pesar de estar fuera del rango de cobertura de los puntos de acceso están dentro del rango de cobertura de alguna tarjeta de red (TR) que directamente o indirectamente está dentro del rango de cobertura de un punto de acceso (PA). [1]

La tecnología MESH siempre depende de otras tecnologías complementarias, para el establecimiento de backhaul (red de retorno) [2] debido a que los saltos entre nodos MESH, provoca retardos que se van añadiendo uno tras otro, de forma que los servicios sensibles al retardo, como la telefonía IP, no sean viables (Ver Figura 1, Ver Figura 2).

Figura 1 Red MESH, distribución de internet en zonas urbanizadas o rurales.

http://www.grssistemas.com.ar/productos-servicios.htm

Figura 2 Ilustración de la red MESH con el protocolo Border Gateway Protocol



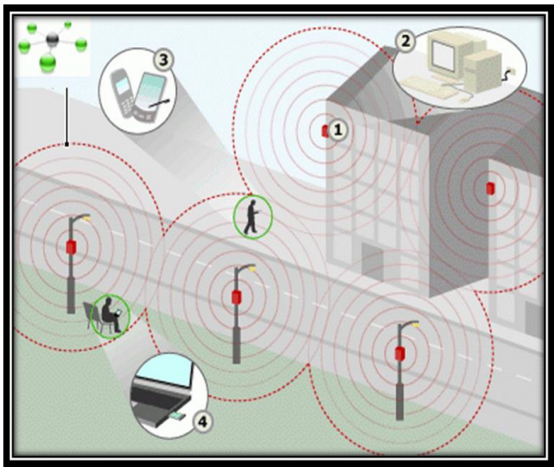
http://www.webopedia.com/TERM/I/iBGP.html

La tecnología MESH utiliza los estándares establecidos de una forma totalmente novedosa. El conjunto de nodos proporciona una zona de cobertura inalámbrica muy extensa. Los nodos son capaces de establecer comunicación entre ellos en cuanto sus zonas de cobertura se solapan entre sí. Por otro lado, si se solapan varias zonas de cobertura, aunque fallen uno o más nodos, la red se sustenta y sigue operando. El usuario probablemente ni se enterará de esto, ya que su equipo se conectará automáticamente (*roaming*) con el nodo más próximo operativo. Cuantos más puntos de acceso a Internet disponga, más fiable y rápida será la red [3].

Así es como es posible reconocer que el uso de las redes MESH traen más ventajas que desventajas, que su distribución hace de la trasmisión y uso de esta sea de manera segura y confiable.

La Figura 3 ilustra cómo se distribuye las redes MESH.

Figura 3 Ilustración del beneficio de las redes MESH



http://www.nodalis.es/sobre-nodalis-por-que-una-red-mesh-o-mallada.htm

II. ATAQUES A REDES WLAN

Una de las características poco mencionadas al hablar de las redes inalámbricas WLAN, es la inseguridad que estas pueden contener este tipo de redes, pues son vulnerables a ataques en el transcurso de la información, esto por la propagación que se presenta en la señal ya que esta se genera a todas las direcciones.

Para poder brindar seguridad en redes es importante reconocer primero cuales son los posibles ataques que pueden sufrir las redes WLAN. Dichos ataques se dividen en dos grandes grupos, ataques pasivos y ataques activos.

A) Ataques pasivos

Su principal objetivo para atacar las redes es lograr obtener información, suponiendo un primer paso para poder atacar posteriormente, ejemplo monitorizaciones y escuchas de la red. [4]

Dentro del mismo se pueden encontrar ataques como los siguientes:

a. Espionaje o Surveillance

Consiste en observar el entorno en el que se relaciona dicha red para así recopilar información relacionada con la topología de la red. Datos que se usan para un próximo ataque, sin necesidad de un hardware o un software especifico, simplemente se genera ataque teniendo acceso a la instalación.

Información usada para su favor, con motivos de daños al usuario principal.

b. Escuchas o Sniffing

Su objetivo final es monitorizar la red para asi poder tener el acceso a información sensible como la dirección IP de origen y destino, contraseñas, Clave WEP [5], con el modo de inyectar o modificar los mensajes.

Al obtener información comprometida son considerables ataques de gran impacto y peligrosos, difícilmente detectables.

- Las herramientas que permiten obtener estos datos son los sniffers y los analizadores de protocolos.
- Un sniffer o rastreador de red es un proceso que olfatea el tráfico que se genera en la red a nivel de enlace; de este modo puede leer toda la información que circule por el tramo (segmento) de red en el que se encuentre.
- Un analizador de protocolos es un sniffer que ha extendido su funcionalidad para comprender ciertos

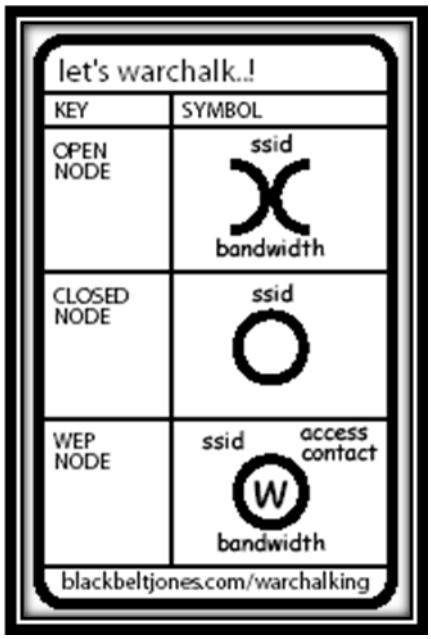
protocolos y permiten analizar la información contenida en los paquetes enviados por la red.

- Un ordenador conectado a una red mediante un hub puede ver el tráfico de toda la red poniendo su tarjeta en modo promiscuo y analizarlo con programas como tcpdump, dsniff, wireshark, etterca [6]

c. Warchalking

Este hace referencia al lenguaje de símbolos normalmente utilizados para señalar el sitio donde se encuentra la red inalámbrica de la forma que aquella persona que pase por allí pueda utilizarla. La simbología de esta es sencilla y clara (Ver Figura 5). El objetivo es identificar si esta es cerrada con clave de acceso o si es abierta sin clave de acceso, claro está especificar que la misma indica el nombre del red SSID además indicando que velocidad es manejada para dicha red.

Figura 2 Simbología



http://www.wi-fiplanet.com/columns/article.php/1402401

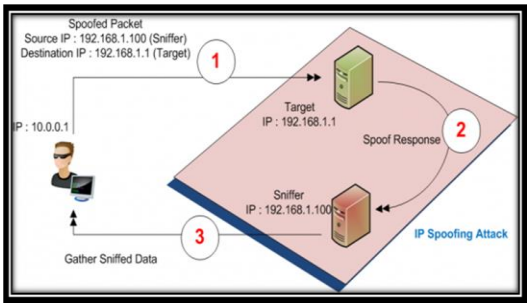
B) Ataques activos.

Este ataque hace referencia a la modificación en el flujo de datos o la creación de falsos flujos en la trasmisión de datos. Teniendo dos objetivos generales, uno suplantar al usuario para así obtener información ajena o dos colapsar la red para así bajar la funcionalidad de los servicios que este mismo puede prestar.

a. Spoofing

Consiste en la creación de trampas TCP/IP Utilizando una dirección IP Falsa para así suplantar la red y obtener información (Ver Figura 6). Para esto entran en juego tres maquinas: un atacante, un atacado y un sistema suplantado con que se relaciona con el atacado [7].

Figura 3 Relación con la que se modifica las IP



http://www.opensourceforu.com/2011/12/cyber-attacks-explained-packet-spoofing/

En la figura 7 se observa la información con la que la red se vuelve vulnerable y los atacantes pueden llegar a modificar para así tener el acceso a la red que desean suplantar.

Figura 4 Validadores suplantantes mediante Spoofing.

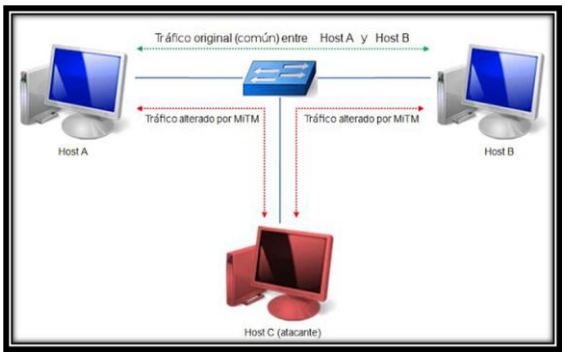
Libro virtual Redes WLAN

b. Man in the Middle (MITM)

Como su nombre lo indica “Hombre en el medio” es un tipo de amenaza que se aprovecha de un intermediario. El atacante en este caso, tiene la habilidad de desviar o controlar las comunicaciones entre dos partes. Por ejemplo, si se tratase de un ataque MITM a algún correo electrónico, el perpetrador podría desviar todos los e-mails a una dirección alterna para leer o alterar toda la información antes de enviarla al destinatario correcto. [8]

Con el fin en general de obtener información y a su vez modificar para algún mal en específico (Ver Figura 8).

Figura 5 Ilustración del ataque MITM



http://infyseg.blogspot.com/2013/11/ataque-man-in-middle-con-ettercap.html

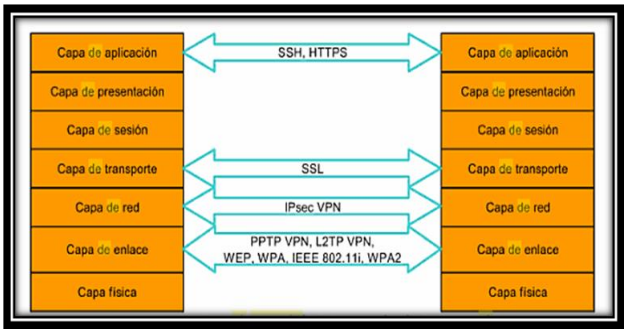
III. DISEÑO INGENIERIL

Al momento de reconocer la mejor alternativa para brindar seguridad a las redes MESH, es necesario conocer las características, ventajas y desventajas de los protocolos de seguridad en redes MESH.

IV. PROTOCOLOS DE SEGURIDAD

Para llegar a mencionar a detalle los protocolos de seguridad ideales para proteger las redes MESH de cualquier ataque, anteriormente mencionados, los cuales como uso de mecanismos de seguridad actúan en diferentes capas del modelo OSI. (Ver Figura 9).

Figura 9 Mecanismos de seguridad Existentes de las distintas capas de OSI



Libro virtual Redes WLAN

Se reconoce que en cualquier red la seguridad puede ser comprometida en dos aspectos: Autenticación el cual pueden ser empleados para la identificación de usuario inalámbrico ante un punto de acceso y viceversa y como segundo esta el Cifrado los cuales aseguran que no sea posible decodificar el tráfico de usuarios.

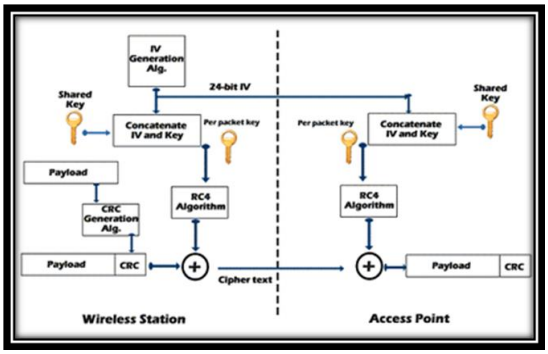
Así mismo que los protocolos de seguridad para las redes WLAN, deben proteger estos dos puntos vulnerables ante posibles ataques anteriormente mencionados. Los protocolos del nivel de enlace desarrollados específicamente para dotarlas de seguridad han sido WEP, WPA, IEE 802.11i y WPA2[9]

C) WEP (Wired Equivalent Privacy, privacidad equivalente al cable)

Es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN (Ver Figura 10).

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca. [10]

Figura 60 Funcionamiento de WEP para Cifrar y Descifrar



http://www.sniferl4bs.com/2012/09/seguridad-en-redes-inalambricas-i-wep.html

a. Características

- Cifra los datos de red de forma que solo el destinatario pueda acceder.
  - Cuenta con dos niveles de seguridad, clave de 64 (5 Caracteres o 10 dígitos hexadecimales) y 128 bits(13 Caracteres o 26 dígitos hexadecimales)
  - Codifica los datos mediante una clave de cifrado antes de ser enviado a su destinatario.
  - Utiliza el algoritmo de flujo RC4 y el algoritmo de chequeo de integridad CRC. Junto una llave secreta y un vector de iniciación.
  - Forma parte de la especificación 802.11.
  - Opera al nivel 2 del modelo OSI.

- Los dos puntos de acceso deben tener la misma clave.

b. Ventajas

- El cifrado de 128 bits evita que el intruso informático acceda a sus archivos y conexión de alta velocidad. Bloqueando sus accesos por el alto consumo de este cifrado.
- Compatibilidad entre distintos fabricantes
- Superior a la seguridad en redes LAN
- Existe un tráfico interrumpido de datos durante un tiempo determinado al momento de cifrar la clave.

a. Desventajas

- Vector inicial
- Sistema de integridad
- Claves de cifrado estáticas, el atacante accede varias veces con el mismo texto cifrado.
- No brinda servicio de autenticación.
- Existen varias herramientas (Software) para romper la clave secreta.
- Es probable que el vector inicial se repita a las 5 horas en redes de alto tráfico. Reutilización del vector.
- El cliente no puede autenticar a la red.
- Su algoritmo permite la modificación de datos sin ser notado.
- El punto de acceso y los clientes deben estar programados con la misma llave, hecho que debilita la red.

D) WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) [11]

Es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

El IEEE tiene casi terminados los trabajos de un nuevo estándar para reemplazar a WEP, que se publicarán en la norma IEEE 802.11i a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaba suficientemente maduras y publicar así WPA.

WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

a. Características

- Implementa la mayoría del estándar IEEE 802.11i
- Resiste Sistemas operativos desde Windows 98 – XP y Linux.
- Distribución Dinámica de claves, utilización mas robusta en el vector inicial.
- Propone un nuevo protocolo para cifrado TKIP (Temporary Key Integrity Protocol.) el cual se encarga de cambiar la clave compartida entre el punto de acceso y cliente cada cierto tiempo.
- Basada en servidores de autenticación (Radius Remote Authentication Dial-In User Server) el cual distribuye claves diferentes entre los usuarios.

b. Ventajas

- Subsana los problemas de WEP
- Establece nuevos protocolos para cambiar clave compartida.
- Trabaja en dos modalidades caseras y corporativas.
- No es necesario el conocimiento técnico, sin introducir manualmente una contraseña ni clave asociada.
- Claves dinámicas, autenticaciones mediante claves generadas por el sistema.
- Se genera autenticación evitando la verificación de las direcciones MAC. De las estaciones por la terna

c. Desventajas

- No todos los dispositivos son capaces de implementarlo.
- No todas las tarjetas inalámbricas son compatibles con este estándar.

- No cumple la norma IEEE 802.11i
- Vulnerable ante claves cortas.
- Las claves preestablecidas utilizan palabras presentes en el diccionario y longitud menor a 20 caracteres, lo cual permite un ataque más fácilmente.

E) WPA2 (802.11i)

Es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Se espera que esté concluido todo el proceso de estandarización para mediados de 2004. Wi-Fi está haciendo una implementación completa del estándar en la especificación WPA2.

Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.

WPA2 incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC.

Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc)

a. Características

- Versión de migración de WPA, pues esta es la segunda generación y es la versión certificada del estándar 802.11i
- Incluye el algoritmo de cifrado AES (Advanced Encryption Standars) el cual es un algoritmo cifrado de bloque con claves de 128 bits, con un máximo de 256 bits.
- Luego de la autenticación del usuario el servidor crea una pareja de claves maestras PMK las cuales se distribuyen entre el punto de acceso y cliente. Así se protegerá el tráfico entre estos.

b. Ventajas

- Ideal para sector privado y público.
- Utiliza protocolos para el aseguramiento de la integridad y autenticidad de los mensajes.
- Asigna a cada usuario una clave única de identificación.
- Cifrado por paquete, asi que cada paquete utiliza una clave generada específicamente para ese mismo.
- Reduce la complejidad y el tiempo de los usuarios de un punto de acceso a otro.

c. Desventajas

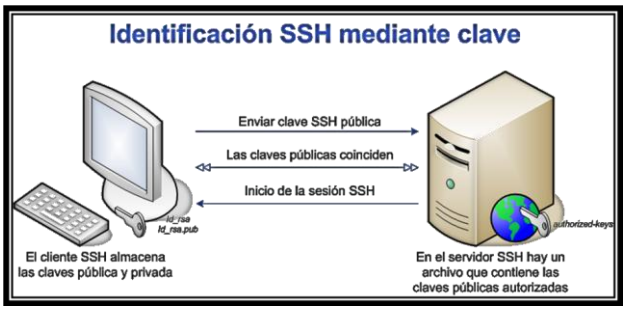
- Es necesario de equipos potentes pues no todos podrán soportar el protocolo.
- Vulnerabilidad en la información pues esta va en formato de texto, hecho que permite ser más fácil su manipulación.
- No se puede controlar el área de cobertura de una conexión.
- No todos los dispositivos pueden adquirir el protocolo.

F) SSH (Secure Shell) [12]

Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través de la shell de comando, tales como telnet o rsh. Un programa relacionado, el scp, reemplaza otros programas diseñados para copiar archivos entre hosts como rcp. Ya que estas aplicaciones antiguas no encriptan contraseñas entre el cliente y el servidor, evite usarlas mientras le sea posible. El uso de métodos seguros para registrarse remotamente a otros sistemas reduce los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto (Ver Figura 20).

Figura 7 Representación de la identificación SHH mediante clave.



http://www.ehu.es/ehusfera/ghym/2010/10/15/identificacion-automatica-en-ssh-usando-claves-rsa/

a. Características

- Su conexión se establece en una primera instancia donde se determina la identidad entre el servidor y el cliente para así tener un canal seguro. Y como segunda instancia, el cliente inicia sesión en el servidor.
- El cliente y el servidor se autentica uno a otro para asegurar que las dos maquinas que se comunican, se identifiquen y así adquirir información.
- Su objetivo es iniciar sesiones en maquias remotas que ofrecen autenticación, confidencialidad e integridad.

b. Ventajas

- Sencillo de usar y habilitar.
- Comprime los datos lo más posible antes de ser transferidos.
- Permite que un cliente abra sesión interactiva en una maquina remota y lograr el envío de comandos o archivos.
- Comunicación cifrada, en todos sus componentes sean datos, archivos o comandos. Entre cliente servidor.
- Inicia sesiones login en servidores remotos, ejecutar aplicaciones graficas desde Shell. Realizar túneles IP.

c. Desventajas

- Imposibilidad para dar acceso anónimo al repositorio.
- Trasmite la información en texto plano lo que deja que este vulnerable sin ser notado ante cualquier intruso.
- Por medio de una herramienta rastreadora logra capturar paquetes, obteniendo el nombre de acceso y la contraseña para acceder remotamente.
- No soporta cambio de contraseña.

G) SLL (Secure Sockets Layer) [13]

Es un protocolo diseñado para permitir que las aplicaciones para transmitir información de ida y de manera segura hacia atrás. Las aplicaciones que utilizan el protocolo Secure Sockets Layer sí sabe cómo dar y recibir claves de cifrado con otras aplicaciones, así como la manera de cifrar y descifrar los datos enviados entre los dos.

Algunas aplicaciones que están configurados para ejecutarse incluyen navegadores web como Internet Explorer y Firefox, los programas de correo como Outlook, Mozilla Thunderbird, Mail.app de Apple, y SFTP (Secure File Transfer Protocol) programas, etc Estos programas son capaces de recibir de forma automática SSL conexiones.
Para establecer una conexión segura SSL, sin embargo, su aplicación debe tener una clave de cifrado que le asigna una autoridad de certificación en la forma de un Certificado. Una vez que haya una única clave de su cuenta, usted puede establecer una conexión segura utilizando el protocolo SSL.

a. Características

- Protegen del nivel de transporte hacia arriba
- Base de las comunicaciones seguras con navegadores WEB
- Integridad de mensajes, autenticando tanto del servidor de destino como del cliente.
- Instala entre los niveles de transporte y de aplicación
- Trabaja sobre el protocolo TCP y por debajo de protocolos como HTTP, IMAP.
- Intercambio de claves públicas y autenticación basada en certificados digitales.
- Encriptación del tráfico basado en cifrado simétrico.

b. Ventajas

- Es independiente del protocolo de aplicación, pues es posible ubicarlo por encima del mismo en forma transparente.
- Encripta los datos por toda la ruta desde el cliente al servidor.
- Confidencialidad (cifrado) en todo su ámbito.
- Protocolo base de seguridad en el comercio electrónico.

- Es trasparente para el usuario. No necesita de muchas modificaciones en los programas que lo utilizan.
- Elimina malware de la web, pues escanea el sitio para detectar programas dañinos.
- Funcionalidad 99% con todos los navegadores.
- Establece múltiples conexiones dentro de la misma sesión o reanudar una sesión previamente interrumpida.
- Solo el servidor es autenticado, garantizando así la identidad.

c. Desventajas

- Costoso en recursos.
- Incrementa la carga del procesador en cualquier momento, en comparación a la comunicación sin autenticación.
- Cada conexión necesita una configuración diferente,
- Claves de sesión de 40 bits, lo cual desprotege después de la trasmisión.
- Solo disponibles sus servicios para protocolo HTTP.

H) HTTPS (Protocolo Seguro de Transferencia de Hipertexto) [14]

El protocolo de Transferencia de Hiper-Texto (HTTPS) es la versión segura de el http (Hyper Text Transfer Protocool) siendo la más conocida y usada diariamente en la internet. La diferencia es que, con HTTPS se logra desarrollar ecommerce, ya que permite realizar transacciones de forma segura. Siendo esto un modelo de negocio confiable para la economía.

Crea un canal de transferencia cifrado con el que obviamente aumenta la seguridad en el tráfico de información en comparación al protocolo HTTP común.

a. Características

- La carga de documentos y archivos en la web se torna más rápido. Facilitando al usuario gracias a su lenguaje PHP y ASP.
- Comunica servidores, proxies y clientes. Permitiendo la transferencia de documentos web, sin importar cuál es el cliente o cual es el servidor.
- Basado en esquema petición/Respuesta.
- El cliente envía un mensaje de petición y el servidor contesta con un mensaje de respuesta, con el cual fue dado a petición del cliente.
- Solicita usuario y password (Confianza)
- Texto plano legible y fácil de depurar.

b. Ventajas

- Sencillez de preparación.
- No requiere de grandes recursos en el servidor.
- Los repositorios de solo lectura para así lograr transferencias encriptadas.
- Proporciona un método increíblemente simple para subir archivos al servidor, con un mínimo de conocimiento sobre la transferencia de archivos.
- El acceso a las paginas se realiza activando enlaces, sin necesidad de copiar todo el URL.
- Con variables globales permite restringir zonas de la aplicación web.

c. Desventajas

- No hay un trabajo dinámico por parte del servidor.
- Carece de potencia en el momento de carga.
- La dirección IP esta oculta si hay un proxy por medio.
- Dificultad en la administración de permisos.

V. CONCLUSIONES

En el desarrollo de este proyecto se llevo a cabo un estudio de los protocolos de seguridad para redes inalámbricas, con el fin de poder realizar un diseño de una arquitectura de seguridad en las redes MESH, el cual cumpliera con los objetivos específicos mencionados al inicio y así obtener conclusiones, representativas en el análisis, el levantamiento de información, reconociendo las características, ventajas y desventajas de cada uno de los protocolos de seguridad utilizados en las redes inalámbricas.

- Cada uno de los protocolos de seguridad utiliza algoritmos diferentes que brindan un soporte seguro, mejorando aspectos como:
    - Los datos
    - La rapidez

- Seguridad en la trasmisión de archivos remotamente
- La encriptación en la comunicación de la red

- Son varios los ataques que las redes inalámbricas pueden recibir, debido al medio de comunicación utilizado, pues al trasmitir la información pueden existir modificaciones o interrupciones en esta, de ahí que los datos pueden ser vulnerable por personas mal intencionadas, de ahí la importancia de los protocolos de seguridad, los cuales brindan confiabilidad al momento del uso en las redes, debido a la utilización de métodos de encriptación.

- Este método usa las contraseñas y autenticación con mayor frecuencia para lograr seguridad al momento del login, al realizar el análisis de dichos protocolos se concluye que su modo de encriptación para lograr una mayor confianza, en este proyecto se analizó 7 protocolos de seguridad.

- De dichos análisis se reconoce que un protocolo de seguridad como WEP, WPA o SSH, no brindan la seguridad esperada para la comunicación de las redes inalámbricas, pues son protocolos antiguos, donde son más las desventajas que las ventajas lo cual origina vulnerabilidades en la seguridad.

- Se concluye finalmente que uno de los mejores protocolos de seguridad para las redes inalámbricas como lo es las redes MESH es el protocolo de seguridad SSL (Secure Sockects Layer) el cual con sus características y modo de manejo brinda confianza en su uso, eliminando malware en el sitio de uso y a la vez detectando los intrusos debido a la forma de encriptamiento de la comunicación entre dichas redes.

RECONOCIMIENTOS

Infinitas gracias al ingeniero Fabian Blanco Garrido quien puso el empeño suficiente para sacar adelante cada una de las investigaciones aquí realizadas, asi mismo a los ingenieros Eduardo Triana y Mauricio Alonso pues dedicaron su tiempo para la corrección de diferentes fallas al momento de su realización.

REFERENCIAS

[1] Concepto extraído de: http://www.ricb.org/organizacional/que-es-una-red-inal%C3%A1mbrica-MESH

[2] Los backhaul conectan redes de datos, redes de telefonía celular y constituyen una estructura fundamental de las redes de comunicación. Un Backhaul es usado para interconectar redes entre sí utilizando diferentes tipos de tecnologías alámbricas o inalámbricas.: http://mundocontact.com/glossary/backhaul-red-de-retorno/#sthash.C3N1WctQ.dpuf

[3] Textualmente extraído de: http://www.nodalis.es/sobre-nodalis-por-que-una-red-mesh-o-mallada.htm

[4] Información tomada del libro virtual, Redes WLAN Fundamentos y aplicaciones de seguridad, Fernando Andreu Izaskun pellejero Amaia Lesta, Ediciones Marcombo, 2006

[5] Wired Equivalent Privacy o WEP, es una función de seguridad de red que se utiliza con las redes inalámbricas. La clave WEP es el código de seguridad que permite a un grupo de computadoras, impresoras u otros dispositivos en la red intercambiar información oculta de dispositivos fuera de la red http://www.ehowenespanol.com/clave-wep-info_227977/

[6] Información extraída de: http://www.ac.usc.es/docencia/ASRII/Tema_3html/node3.html

[7] Información obtenida en http://www.zonavirus.com/articulos/que-es-el-spoofing.asp

[8] Concepto suministrado por: http://bitelia.com/2014/06/ataque-man-in-the-middle

[9] Información suministrada por el . Libro virtual, Redes WLAN Fundamentos y aplicaciones de seguridad, Fernando Andreu Izaskun pellejero Amaia Lesta, Ediciones Marcombo, 2006

[10] Textualmente analizada de: http://www.saulo.net/pub/inv/SegWiFi-art.htm

[11] Textualmente analizada de: http://www.saulo.net/pub/inv/SegWiFi-art.htm

[12] Textualmente estudiado de: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html

[13] Analizado textualmente en http://www.digicert.com/es/ssl.htm

[14] Información analizada en: http://www.internetlab.es/post/888/que-significa-el-protocolo-https-y-como-funciona/