MONOGRAFIA SOBRE LA SEGURIDAD DE WIMAX

IBETH JOHANA PACHECO SIMANCAS

RICARDO JOSE BARRO BARRIOS

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

INGENIERIA DE SISTEMAS

CARTAGENA

2008

MONOGRAFIA SOBRE LA SEGURIDAD DE WIMAX

IBETH JOHANA PACHECO SIMANCAS
RICARDO JOSE BARROS BARRIOS

Monografía presentada para optar al
Titulo de Ingeniero de Sistemas

DIRECTOR, GIOVANNY R. VASQUEZ MENDOZA
INEGNIERO DE SISTEMAS

UNIVERSITDAD TECNOLOGICA DE BOLIVAR
INGENIERIA DE SISTEMAS
CARTAGENA
2008

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

ARTICULO 105

La Universidad Tecnológica de Bolívar, se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados, y no se pueden ser explotados comercialmente sin autorización.

DEDICATORIA

Todo mi esfuerzo y trabajo es bendecido por el ser mas hermoso de todo el universo a quien le doy miles e infinitas gracias por estar conmigo en todo este camino, dé tropiezos y angustias gracias Dios por no abandonarme y por protegerme en todo momento, por guiarme por el sendero del bien.

A mis padres le quiero dedicar esta monografía por que de no ser por ellos no estaría en etapa de mi vida, gracias a ustedes por brindarme la oportunidad de tener una formación académica gracias por el amor, el apoyo, y la confianza que tuvieron en mi los amo con todo mi corazón y es por ustedes que hoy soy lo que siempre he querido ser.

A mis hermanos les agradezco por que como familia el apoyo es fundamental en todo proceso, y ese apoyo yo lo obtuve con ustedes.
A mi hermoso novio a quien amo con todas mis fuerzas por que el es un motor en mi vida, el es mi amigo incondicional gracias mi amor por estar con migo en la buenas y en las malas, por el apoyo que siempre obtuve de ti, este logro también es tuyo.

A mis compañeros de universidad, en especial a Ricardo quien es mi compañero de monografía, docentes y tutores por la paciencia, tolerancia, y comprensión que tuvieron con migo en este proceso de formación.

A mis amigos en especial a mafe y diana por tenerme paciencia y por sus consejos, que me fueron muy útiles en todo este camino.
Gracias a todos por esperar junto a mí este día los quiero a todos con todo mi corazón.

IBETH JOHANA PACHECO SIMANCAS

DEDICATORIA

Gracias Dios por no abandonarme y por protegerme en todo momento, por guiarme por el sendero del bien, por darme todas las fortalezas, por darme paciencia y por darme la oportunidad de ser un profesional.

Le agradezco a mis padres y a mi hermano, en cual les quiero dedicar esta monografía por que de no ser por ellos no estaría en etapa de mi vida, gracias a ustedes por brindarme la oportunidad de tener una formación académica gracias por el amor, el apoyo, y la confianza que tuvieron en mi los amo con todo mi corazón y es por ustedes que hoy soy lo que siempre he querido ser.

A mis amigos, especialmente ibeth mi compañera y mi amiga, a mis compañeros y a todos aquellos que han sido testigos del proceso, de la preparación y del esfuerzo para realizar esta monografía.

Y por ultimo quiero agradecer a mi abuela que en paz descanse por todas sus oraciones que yo se que desde el cielo fuero bienvenidas por mi y toda esa buena energía que también me brindo mi madrina chachi dándome muchas ganas y fuerzas para salir adelante.

Gracias a todos por esperar junto a mí este día los quiero a todos con todo mi corazón.

RICARDO JOSE BARROS BARRIOS

AUTORIZACION

Cartagena de indias D.T. y C.

Nosotros IBETH JOHANA PACHECO SIMANCAS, con cedula de ciudadanía 32.939.088 de Cartagena y RICARDO JOSE BARROS BARRIOS, con cedula de ciudadanía 8870488 de Cartagena. Autorizamos a la Universidad Tecnológica De Bolívar para hacer uso de nuestro trabajo de grado y publicarlo en el catalogo online de la biblioteca.

Cordialmente,

_____ _____

IBETH J PACHECO SIMANCAS **RICARDO J BARROS BARRIOS**

CC.32939088 de Cartagena **CC. 8.870.488 de Cartagena**

Cartagena de indias D.T. y C.

Señores

COMITÉ DE FACULTAD DE INGENIERÍA DE SISTEMAS

Universidad Tecnológica de Bolívar

Ciudad

Apreciados Señores.

Cordialmente me permito informarles que he llevado a cabo la dirección del trabajo de grado de los estudiantes IBETH JOHANA PACHECO SIMANCAS y RICARDO JOSE BARROS BARRIOS, titulado: “SEGURIDAD DE WIMAX”.

Cordialmente,

_____

GIOVANNY R. VÁSQUEZ MENDOZA

Cartagena de indias D.T. y C. 5 de agosto de 2008

Señores

COMITÉ DE FACULTAD DE INGENIERÍA DE SISTEMAS

Universidad Tecnológica de Bolívar

Ciudad

De la manera más cordial nos permitimos presentar a su consideración y aprobación el trabajo de grado titulado “SEGURIDAD DE WIMAX”. Elaborado por IBETH JOHANA PCHECO SIMANCAS y RICARDO JOSE BARROS BARRIOS.

Esperamos que el presente trabajo se ajuste a las expectativas y criterios de la Universidad para los trabajos de grado.

Cordialmente,

_____ _____

IBETH J PACHECO SIMANCAS **RICARDO J BARROS BARRIOS**

CC.32939088 de Cartagena **CC. 8.870.488 de Cartagena**

INTRODUCCION

En las primicias de las telecomunicaciones muchas de las empresas que utilizan las telecomunicaciones presentaron muchas dudas sobre la seguridad de estas ya que a la hora de hacer una mayor inversión es necesario saber si vale pena gastar en seguridad dependiendo la importancia de la información. En la actualidad en Colombia existe un avance tecnológico muy importante que va evolucionando desde el cableado hasta la convergencia de voz, datos y video en LAN´s, WAN´s además el uso de internet como una necesidad particular de movilidad en videoconferencias y tecnología Wimax.

Por último, quería denotar que mientras se redacto la presente memoria, han aparecido nuevas vulnerabilidades de diversos protocolos que más tarde serán explicados. Por lo tanto, con el deseo de que esta memoria no quede obsoleta antes de salir publicada, asi los apartados tratados sean de interés para el lector.

TITULO DE LA MONOGRAFIA

SEGURIDAD DE WIMAX

LINEA DE INVESTIGACION

Comunicaciones y redes.

CAMPO DE LA INVESTIGACION

Seguridad.

DESCRIPCION DEL PROBLEMA

La motivación de esta monografía esta basada en la falta de información y fuentes literarias donde este tema en desarrollo a pesar de el principal auge que ha tomado, obtener en si material para poder entender la tecnología en nuestro lenguaje, de una manera más amena y fácil cuando se trata de adquirir el conocimiento

Todo esto con el desenlace de dar a conocer conocimientos actuales que han cambiado la perspectiva de esta tecnología y a raíz de esta necesidad se ha desarrollado este documento el cual va a ser dirigido a la comunidad estudiantil, a los investigadores y aquellos que deseen implementar esta tecnología.

OBJETIVOS

Elaborar un documento investigativo sobre la seguridad en Wimax, con el fin de fortalecer el aspecto bibliográfico del tema, facilitando un mejor recurso de dicho tema.

OBJETIVOS ESPECIFICOS:

- Describir mecanismos de seguridad utilizados por Wimax.
- Comprender los protocolos a utilizar en la seguridad de Wimax.
- Determinar vulnerabilidad en las redes inalámbricas particularmente en la seguridad de Wimax.

JUSTIFICACION

La seguridad de una red inalámbrica en estos momentos juega un papel muy importante para la sociedad porque el auge que a tomado la tecnología lleva a que como usuarios interactuemos de una manera mas confiable y eficaz en el medio, de tal manera se a querido establecer o divulgar que esta tecnología aunque no este en su total madurez la podemos implementar de una manera optima, por eso el enriquecimiento y desarrollo de esta monografía.

Aunque en la Actualidad en Colombia son muy pocos los recursos bibliográficos sobre la seguridad en Wimax, por eso se ha desarrollado este documento para que les sirva de guía a todos los estudiantes, docentes, ingenieros de la universidad tecnológica de bolívar que quieran ampliar y difundir sus conocimientos y habilidades por este tema, ya que hasta hoy los únicos recursos existentes sobre la seguridad de Wimax son en otro idioma y costosos para adquiriros.

TIPO DE INVESTIGACION

La presente investigación es de tipo descriptiva, detallando la historia y el desarrollo tecnológico de la seguridad de Wimax.

RESUMEN

El estándar wimax esta diseñado teniendo en cuenta los aspectos relacionadas con la seguridad, y ofrece una protección mas solida mediante la encriptación basada en certificados.

Wimax es el asíncrono de Worldwide Interoperability for Microware Access (Interoperabilidad Mundial para Acceso por Microondas) No es una tecnología demasiado nueva, sino que se encontra mas ante la estandarización de la ultima y mas reciente tecnología de acceso radio OFDM (Orthogonal Frecuncy Division Multiplexing) de banda ancha. Así, se trata de un sistema pensado para proporcionar servicios triple play, de voz, video y datos, con calidad de servicio independientemente de si se opera en banda ancha regulada o banda libre.

Si Wimax sigue obteniendo más apoyo de la industria, también puede proveer acceso de banda ancha en regiones alejadas y partes del mundo en desarrollo donde el acceso básico de voz o banda ancha mediante un servicio de línea fija no es económicamente viable. Además, Wimax potencialmente puede usarse para proveer backhaul a redes celulares o puede usarse para mejorar en forma significativa el rendimiento de los puntos de acceso con redes inalámbricas Wi-Fi (Wireless Fidelity), aumentando el rendimiento de la red de backhaul y haciendo más fácil y económico desplegar Wi-Fi.

En este sentido, Wimax es la solución más efectiva y económica para suministrar banda a escala universal. La estandarización cambiara la situación del mercado BWA, pasando de la condición limite de mercado a convertirse en un mercado masivo, aportando todos los beneficios económicos que acompañan a un producto al mercado de masas.

De igual modo, a la larga, Wimax permitirá eliminar la barrera permanente para ofrecer acceso de banda ancha a millones de usuarios potenciales de mercado a los que es difícil llegar o que cuenten con un servicio de baja calidad en todo el mundo.

Una vez que los equipos certificados de wimax estén disponibles en una cierta cantidad de proveedores, puede haber una mayor competencia y alcanzando un volumen de unidades despachadas, que conllevan a precios más atractivos

Desde el comienzo de 2006 se ha sentido la disponibilidad de equipamiento WIMAX certificado de acuerdo con el estándar 802.16-2004 para el acceso inalámbrico de banda ancha móvil fijo. A finales de este año es mas que probable que este lista la certificación del equipamiento para WIMAX móvil, 802.16e.

Wimax ofrece equipamiento de banda ancha inalámbrica lo que significa, menor precio en el equipamiento para proveedores de servicio y operadores, lo que permite a los operadores poner en marcha redes inalámbricas ya sea en banda libre o licenciada, para suministrar servicios, en que se despliegue con anterioridad ha sido inviable por cuestiones económicas; interoperabilidad, lo que derivará en su momento en productos plug and play. Los proveedores de servicio serán capaces de combinar equipamiento de otros proveedores de soluciones, asegurándose la compatibilidad.

En su evolución, Wimax da el mayor salto sobre Wi-FI, proporcionando conectividad de banda ancha en la ultima milla sobre un área geográfica significativa mas extensa, abarcando un radio de mas de diez kilómetros y ofreciendo características estables, cumpliendo de forma rigurosa los requerimientos de los operadores en una amplia variedad de escenarios de despliegue.

CONTENIDO

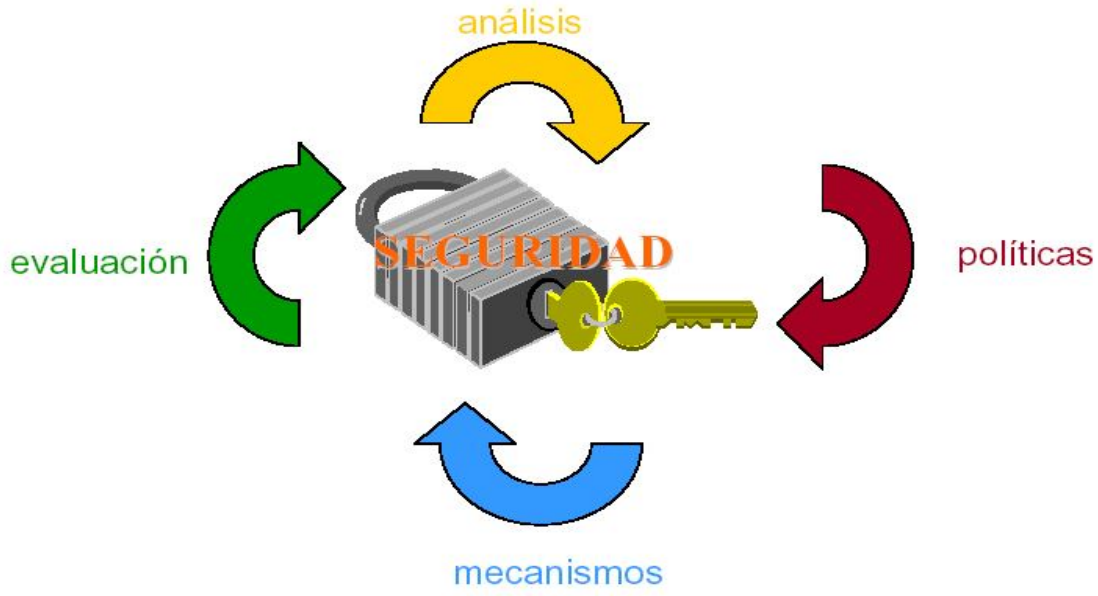
Pág.

LISTAS DE FIGURAS

Pág.

Lista de Figuras.

1. SEGURIDAD DE WIMAX.



La seguridad de los datos se ha convertido en un problema importante en la mayoría de protocolos de red. Esto se debe a la creciente importancia de la información. Debido a esta importancia, los diferentes protocolos de seguridad se han diseñado, desplegado y con las normas de red con el fin de añadir la seguridad. Esta publicación aborda los protocolos de seguridad definido por uno de los modernos estándares de comunicación inalámbrica, el acceso inalámbrico de banda ancha, comúnmente conocida como Wimax, es una rápida evolución de la tecnología que se utiliza para formar amplia gama de redes inalámbricas, dramáticamente de datos a alta velocidad de transferencia de información.

Wimax abre la puerta a miles de aplicaciones que hacen uso de la columna vertebral sólida inalámbrico para conectar los pueblos. Con la alta velocidad de

[1] Tomado de la referencia bibliográfica No 10 Pag.16

transmisión de datos, las aplicaciones incluyen la transferencia de vídeo, llamadas de voz, y otros servicios. Todos los tipos de solicitudes requieren, un medio seguro para operar e intercambiar información. Esto es lo que el IEEE decidió añadir a la norma Wimax en sus dos versiones, fijas y móviles acceso inalámbrico de banda ancha.

Desde el punto de vista de un usuario final, los principales problemas de seguridad son la privacidad e integridad de los datos. Los usuarios necesitan tener garantías de lo que no se puede escuchar en sus períodos de sesiones y que los datos enviados a través del enlace de comunicación no son manipulados. Esto se suele lograr mediante el uso de la encriptación.

Desde el punto de vista del proveedor de servicios, una importante consideración de seguridad es prevenir el uso no autorizado de los servicios de red. Esto normalmente se hace utilizando autenticación fuerte y los métodos de control de acceso. Autenticación y control de acceso se pueden aplicar en los distintos niveles de la red, tales como la capa física, y la capa de servicio. El proveedor de servicios ve la necesidad de prevenir el fraude el cual debe ser equilibrado contra las molestias que pueda imponer a los usuarios.

1.1 ¿QUÉ SE NECESITA PARA ESTAR PROTEGIDO?

Como cualquier otra red de comunicación al servicio de empresas y usuarios individuales que desean mantener su información segura, los sistemas Wimax necesitan aplicar medidas para asegurar la privacidad de sus usuarios finales y prevenir el acceso a información confidencial o sensible a personas que no están autorizadas.

Desde que los sistemas Wimax utilizan el interface radio como medio de transmisión, la pregunta que conviene hacerse es cómo prevenir que los intrusos no intercepten información sensible y confidencial transmitida por ondas hertzianas ya sea en banda libre o banda licenciada.

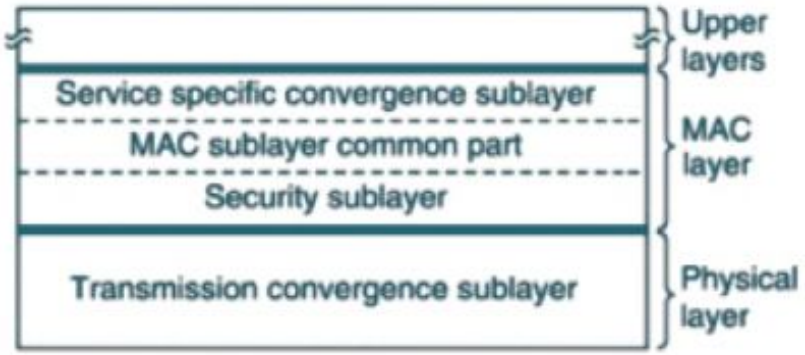


Figura 2. Estructura de una red Wimax[2]

Tanto los clientes como los operadores deberían sentirse protegidos y confiar en que su sistema es privado y seguro, y que las medidas apropiadas están disponibles para minimizar los riesgos de seguridad, incluyendo:

- ✓ **Escuchar/espionaje**: interceptar información de forma intencional cuando se está transmitiendo.
- ✓ **Privacidad**: Asegurarse de que la información transmitida es solamente leída por los destinatarios a los que va dirigida.
- ✓ **MAC Spoofing**: evitar que un atacante copie las direcciones MAC de CPE legítimas con el fin de conseguir el acceso a la red.
- ✓ **Robo del Servicio**: prevenir que los agresores puedan acceder a Internet u otros servicios utilizando CPE robadas y advirtiendo a los usuarios legítimos de obtener los servicios de forma gratuita.

[2] Tomado de la referencia bibliográfica No.6

1.2 PROTOCOLOS EN LA SEGURIDAD DE WIMAX.

A medida que trascurre el tiempo, las innovaciones tecnológicas van siendo mayores y junto a esto las reglas y normas que permiten el buen funcionamiento de estas innovaciones; los protocolos fueron creados con el fin de describir las normas que le ayudan a los dispositivos de la red a intercambiar información haciendo de esta manera que los trabajos tengan una mayor aceptación en el mercado global de las tecnologías. Con la aparición de la seguridad los protocolos tenían que estar suficientemente actos para su uso ya que con la presencia de nuevos métodos de hackeo se ha tratado de crear protocolos que reúnen las características esenciales y necesarias para este trabajo. Esos protocolos son capaces de garantizar no solo la confidencialidad de la información sino también la integridad de la misma.

1.2.1 PKM (Privacy Key Management Protocol).

La estación de subscriptora (SS) hace uso de la PKM para obtener la autorización y tráfico del material de las claves desde estación Base (BS), para mantener la reautorización y actualización periódica de las claves[3].

[3] Security: Privacy Key Management (PKM) Protocol [en línea]. [Consulta: 10 Junio. 2008]. Disponible en: http://www.freewimaxinfo.com/pkm-protocol.html

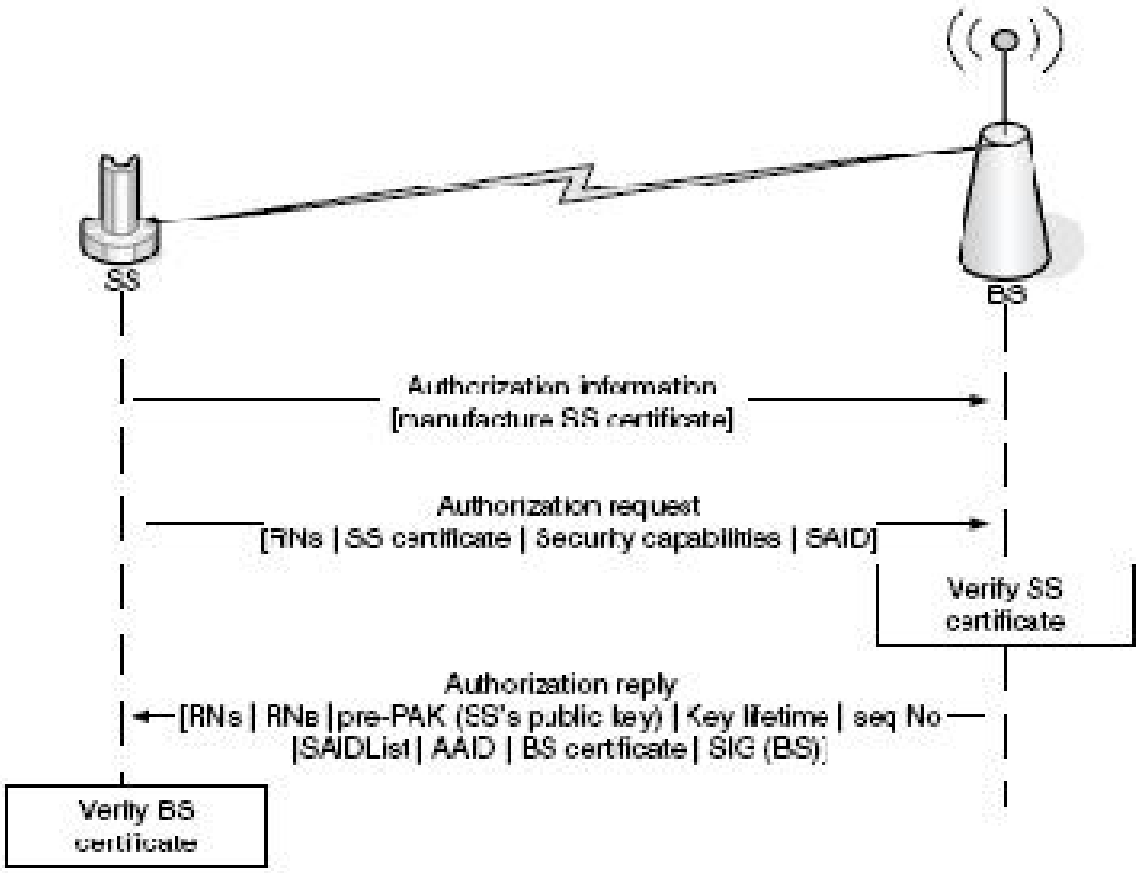


Figura 3. Autorización de Procesos entre una SS y la BS.[4]

El protocolo PKM utiliza certificados digitales X.509, y el sistema (DES), para el intercambio seguro entre una estación subscriptora dada (SS) y la estación base (BS), siguiendo el modelo cliente-servidor. Aquí, las (SS) como cliente solicita el materia de las claves, mientras que el BS como servidor actúa en respuesta a esas peticiones, asegurando que SS cliente sólo reciba el material de las claves para las cuales esta autorizado.

[4] Tomado de la referencia bibliográfica No.9 Pág.241

El protocolo PKM primero crea una clave de autorización (AK), la cual es una clave simétrica secreta compartida entre la SS y BS. Entonces el AK se utiliza para proteger el PKM con un intercambio de claves de encriptado de trafico (TEK). El uso de la AK y un sistema de clave simétrica de cifrado reduce la sobrecarga debido a la costosa implementación de clave pública.

Base Station (BS) es una autenticadora estación de Suscriptora, durante la primera autorización de cambio. El dispositivo SS adjunta la clave pública certificada RSA y otro dispositivo específico de información, como su dirección MAC, número de serie, fabricante y número de identificación. Dentro de la autorización de cambio, la SS luego envía una copia de este dispositivo certificado a la BS. La BS debe autenticar la sintaxis y la información en la SS certificada y posiblemente, llevará a cabo los controles de validación. Si se ha verificado, la BS como parte de sus respuestas a las SS encripta la clave de autorización (AK), utilizando la clave pública de la SS con el certificado recibido de la estación de subscripción. Puesto que sólo la SS contiene la clave privada, la SS sólo puede encriptar el mensaje y obtener la AK que le ha sido asignado.

Es importante señalar que la estación de subscripción (SS) certificada, está abierta al público o al usuario malintencionado, sólo el SS tiene acceso similar a la clave privada, es decir la clave pública certificada. Como tal, para proteger un dispositivo y su certificado de ser duplicada, es importante apreciar que la clave privada sea insertada dentro del dispositivo de hardware. Es decir, el costo de un atacante para la eliminación de la clave privada del dispositivo debe ser mayor que el posible valor obtenido del atacante utilizando el dispositivo craqueado.

1.2.2 TKIP (Temporal Key Integrity Protocol).

Con este protocolo se pretende resolver las deficiencias del algoritmo WEP, encargado de comprimir y cifrar los datos que se envían a través de las ondas,

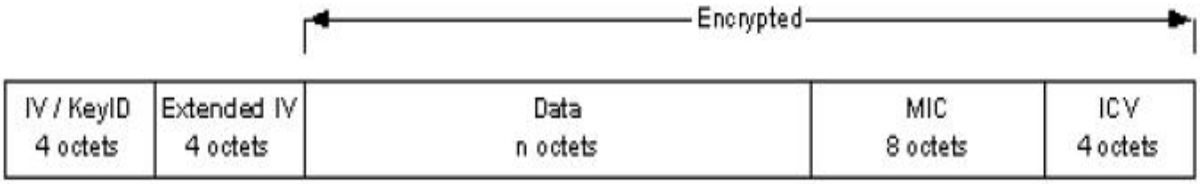


Figura 4. Estructura de encriptación TKIP[5].

El protocolo TKIP está compuesto por los siguientes elementos:

- ✓ Un código de integración de mensajes (MIC), que encriptar el checksum incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11. Esta medida protege contra los ataques por falsificación.
- ✓ Contramedidas para reducir la probabilidad de que un atacante pueda aprender o utilizar una determinada llave.
- ✓ Utilización de un IV (vector de inicialización) de 48 bits llamado TSC (TKIP Sequence Counter) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden.

La utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de redecodificar la llave temporal durante una sola asociación. Solo Pueden intercambiarse 2 paquetes utilizando una sola llave temporal antes de ser reusada.

[5] Tomado de la referencia bibliográfica No.8 Pág. 12

En el proceso de encapsulación TKIP mostrada a continuación:

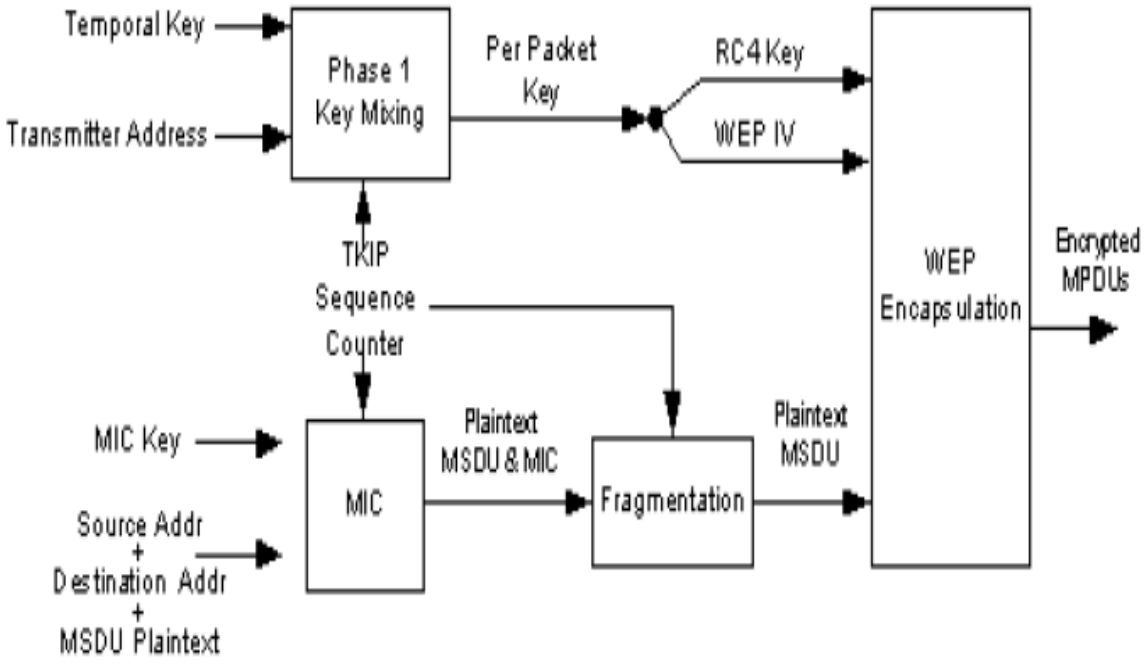


Figura 5. Proceso de encapsulación TKIP[6]

Se combinan en dos fases la llave temporal, la dirección del emisor y el TSC para la obtención de una llave de 128 bits por paquete, dividido en una llave RC4 de 104 bits y en una IV[7] de 24 bits para su posterior encapsulación WEP. El MIC final se calcula sobre la dirección física origen y destino y el MSDU (MAC Servicie Data

Unit o texto plano de los datos en la trama 802.11) después de ser segmentado por la llave MIC y el TSC.

[6] Tomado de la referencia bibliográfica No.8 Pág. 12
[7] Vector de iniciación

La función MIC utiliza una función hash unidireccional, si es necesario, el MSDU se fragmenta incrementando el TSC para cada fragmento antes de la encriptación WEP.

En la desencriptación se examina el TSC para asegurar que el paquete recibido tiene el valor TSC mayor que el anterior. Sino, el paquete se descartará para prevenir posibles ataques por repetición. Después de que el valor del MIC sea calculado basado en el MSDU recibido y desencriptado, el valor calculado del MIC se compara con el valor recibido.

1.2.3 CCMP (Counter-Mode/CBC-MAC Protocol)

Este protocolo es complementario al TKIP y representa un nuevo método de encriptación basado en AES (Advanced Encryption Standards), cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC. Así como el uso del TKIP es opcional, la utilización del protocolo CCMP es obligatorio si se está utilizando el estándar 802.11i[8]

En la siguiente figura podemos observar el formato tras la encriptación CCMP:

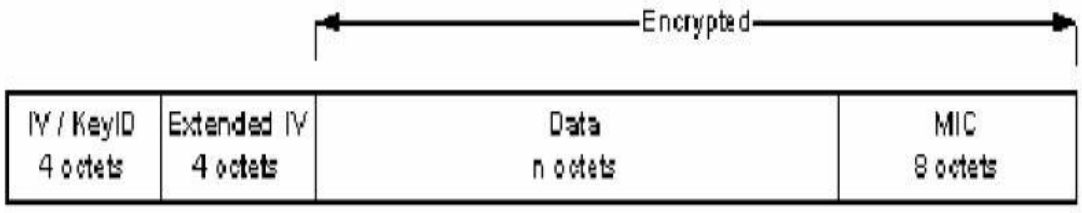


Figura 6. Estructura de encriptación CCMP[9].

[8] SEGURIDAD WIRELSS [en línea]. [Consulta: 03 Julio. 2008]. Disponible en: http://documentos.shellsec.net/otros/SeguridadWireless.pdf

[9] Tomado de la referencia bibliográfica No.8 Pág. 13

CCMP utiliza IV de 48 bits denominado Número de Paquete (PN) utilizado a lo largo del proceso de cifrado, junto con la información para inicializar el cifrado, AES para calcular el MIC y la encriptación de la trama.

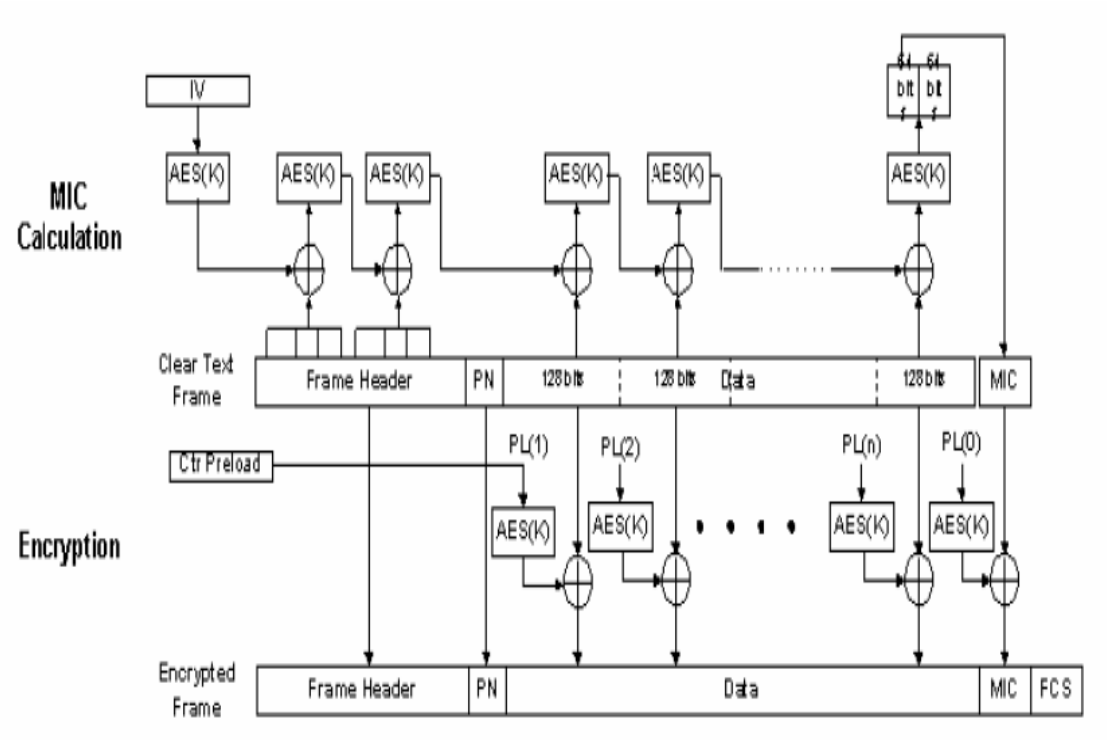


Figura 7. Proceso de encriptación CCMP[10]

En el proceso de encriptación CCMP, la encriptación de los bloques utiliza la misma clave temporal tanto para el cálculo del MIC como para la encriptación del paquete. Como en TKIP, a clave temporal se deriva de la llave principal obtenida como parte del intercambio en 802.1x. El cálculo del MIC y la encriptación se realizan de forma paralela. El MIC se calcula a partir de un IV formado por el PN y datos extraídos de la cabecera de la trama. El IV se convierte en un bloque AES y su salida a través de la operación XOR conformará el siguiente bloque AES.

[10] Tomado de la referencia bibliográfica No.8 Pág.13

1.2.4 Protocolo de autenticación extensible (EAP, Extensible Authentication Protocol).

El Protocolo de autenticación extensible (EAP) es una extensión del Protocolo punto a punto (PPP), que es un protocolo que proporciona un método estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto estableciendo una conexión de par evitando que intrusos entren en la comunicación. Es un protocolo punto a punto que soporta métodos de autenticación múltiples.

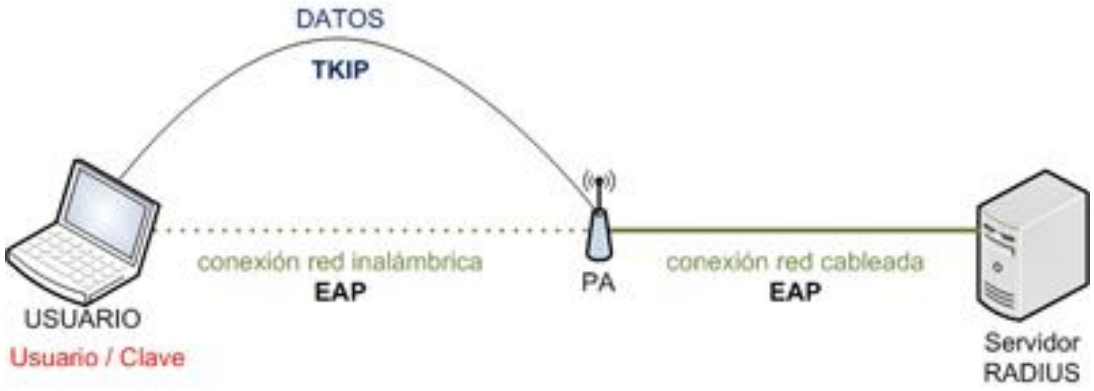


Figura 8. Sistema de Autenticación EAP[11].

Este protocolo se desarrolló como respuesta al aumento de la demanda de autenticación de usuarios de acceso remoto que utilice otros dispositivos de seguridad.

EAP proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un solo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros. EAP, junto con los métodos de autenticación EAP de alto nivel,

[11] Tomado de la referencia bibliográfica No.7

es un componente tecnológico crítico para las conexiones seguras a través de una red privada virtual (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, que otros métodos de autenticación.

Existen diferentes variantes del protocolo EAP, según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas.

1.3 MECANISMOS UTILIZADOS POR WIMAX PARA SU SEGURIDAD.

Los mecanismos de seguridad que poseen los actuales estándares son diferentes, la descripción de cada uno de ellos es la siguiente:

1) IEEE 802.16-2004: Provee manejo de privacidad de llaves para autenticación e intercambio de llaves (PKM) y un protocolo de encapsulación de datos para el manejo de confidencialidad e integridad. Entre las principales debilidades detectadas se pueden mencionar:

- ✓ No existe autenticación de red, por lo que es posible realizar ataques usando estaciones base falsas.
- ✓ No se especifica la forma de manejar certificados.
- ✓ Utiliza DES para la encriptación, lo cual es considerado inseguro.
- ✓ Existen potenciales ataques de denegación de servicio debido a la no existencia de protección de integridad en los paquetes.
- ✓ El método de generación de números pseudo-aleatorios es potencialmente débil comparado con otros métodos estándares.

2) IEEE 802.16e: Este estándar es un gran paso en términos de seguridad con respecto al estándar anterior, ya que la mayor parte de las debilidades fueron corregidas. El estándar provee mejoras en los mecanismos de autenticación (EAP, PKMv2), la mayoría de los paquetes de control son firmados para protección de integridad, se usan mecanismos basados en AES para encriptación de datos y se efectúa una pre-autenticación para proveer un inicio de sesión más eficiente para movilidad. Los análisis han detectado algunas probables debilidades:

- ✓ Es posible un ataque de DoS en la autenticación debido a que no todos los paquetes EAP están protegidos.
- ✓ El manejo de certificados es aún poco claro, ya que no se han resuelto asuntos como el almacenamiento de los mismos y sus llaves privadas.

1.3.1 MECANISMO DE INGRESO A LAS REDES.

Todo sistema posee un mecanismo de ingreso a las redes, pero solo es para el personal autorizado, por que no todos pueden tener acceso a estas, esto se realiza con el fin de acabar con los hacker que de alguna u otra manera buscan las maneras de romper los sistemas de seguridad e ingresar y destruirlos haciendo así que la integridad quede obsoleta. Es importante destacar que la seguridad es útil y necesaria en todos los aspectos existentes, ya que juega un papel muy importante en el campo de las redes y las telecomunicaciones.

1.3.1.1 WEP (Wired Equivalent Protocol).

El protocolo WEP es un sistema de encriptación estándar propuesto por el comité 802.11, implementada en la capa MAC y soportada por la mayoría de vendedores de soluciones inalámbricas.[12] En ningún caso es comparable con IPSec. WEP comprime y cifra los datos que se envían a través de las ondas de radio. Con WEP, la tarjeta de red encripta el cuerpo y el CRC de cada trama 802.11 antes de la transmisión utilizando el algoritmo de encriptación RC4 proporcionado por RSA Security. La estación receptora, sea un punto de acceso o una estación cliente es la encargada de desencriptar la trama.

Como parte del proceso de encriptación, WEP prepara una estructura denominada 'seed' obtenida tras la concatenación de la llave secreta proporcionada por el usuario de la estación emisora con un vector de inicialización (IV) de 24 bits generados aleatoriamente. La estación cambia el IV para cada trama transmitida.

A continuación, WEP utiliza el 'seed' en un generador de números pseudo-aleatorio que produce una llave de longitud igual al payload (cuerpo más CRC) de la trama más un valor para chequear la integridad (ICV) de 32 bits de longitud.

El ICV es un checksum que utiliza la estación receptora para recalcularla y compararla con la enviada por la estación emisora para determinar si los datos han sido manipulados durante su envío. Si la estación receptora recalcula un ICV que no concuerda con el recibido en la trama, esta queda descartada e incluso puede rechazar al emisor de la misma.
WEP especifica una llave secreta compartida de 40 o 64 bits para encriptar y desencriptar, utilizando la encriptación simétrica.

[12] Seguridad [en línea]. [Consulta: 03 Julio. 2008]. Disponible en: http://rinuex.unex.es/modules.php?op=modload&name=Textos&file=index&serid=39

Antes de que tome lugar la transmisión, WEP combina la llave con el payload/ICV a través de un proceso XOR a nivel de bit que producirá el texto cifrado, Incluyendo el IV sin encriptar sin los primeros bytes del cuerpo de la trama. La estación receptora utiliza el IV proporcionado junto con la llave del usuario de la estación receptora para desencriptar la parte del payload del cuerpo de la trama.

Cuando se transmiten mensajes con el mismo encabezado, por ejemplo el FROM de un correo, el encabezado de cada payload encriptado será el mismo si se utiliza la misma llave. Tras encriptar los datos, el encabezado de estas tramas será el mismo, proporcionando un patrón que puede ayudar a los intrusos a romper el algoritmo de encriptación. Esto se soluciona utilizando un IV diferente para cada trama.

La vulnerabilidad de WEP reside en la insuficiente longitud del Vector de Inicialización (IV) y lo estáticas que permanecen las llaves de cifrado, pudiendo no cambiar en variación del tiempo. Si utilizamos solamente 24 bits, WEP utilizará el mismo IV para paquetes diferentes, pudiéndose repetir a partir de un cierto tiempo de transmisión continúa. Es a partir de entonces cuando un intruso puede, una vez recogido suficientes tramas, determinar incluso la llave compartida.

En cambio el estándar 802.11 no proporciona ninguna función que soporte el intercambio de llaves entre estaciones. Como resultado, los administradores de sistemas y los usuarios utilizan las mismas llaves durante días o incluso meses. Algunos vendedores han desarrollado soluciones de llaves dinámicas distribuidas.

A pesar de todo, WEP proporciona un mínimo de seguridad para pequeños negocios o instituciones educativas, si no está deshabilitada, como se encuentra por defecto en los distintos componentes inalámbricos.

1.3.1.2 OSA (Open System Authentication)

Es otro mecanismo de autenticación definido por la norma 802.11 para autentificar todas las peticiones que recibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aún activando WEP, por lo tanto es un mecanismo poco fiable.

1.3.1.3 ACL (Access Control List)

Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autenticación, la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que consten en la Lista de Control de Acceso.

1.3.1.4 CNAC (Closed Network Access Control)

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID) actuando este como contraseña.

1.4 FUNCIONES DE SEGURIDAD.

A diferencia de Wi-Fi, los sistemas de Wimax fueron diseñados al principio con una robusta seguridad en mente. La norma incluye, los métodos para garantizar la privacidad de los datos de usuario y prevenir el acceso no autorizado, con la optimización adicional de los protocolos para la movilidad. La seguridad es manejada por una sub capa de privacidad en el Control de Acceso al Medio. Los aspectos claves que utiliza Wimax para su seguridad son los siguientes:

Apoyo a la privacidad: Los datos del usuario son encriptados usando esquemas de criptografía de robustez probada para proporcionar privacidad. Tanto la tecnología AES y 3DES están soportadas. La mayoría de los sistemas de implementación usaran AES, ya que es un nuevo estándar de encriptación aprobado por la (Federal Information Processing Standard –FIPS) y es mas fácil de implementar. Los 128 bits o 256 bits de clave usados para derivar el cifrado es generado durante la fase de autenticación y es periódicamente renovado para una protección adicional.

Autenticación: Wimax ofrece una manera flexible para autenticar la estación de subscripción y usuario, para prevenir el uso no autorizado. La estructura de autenticación esta basada en el sistema Internet Engineering Task Force (IETF) EAP, la cual brinda una variedad de identificaciones, como nombre de usuario, contraseña, certificados digitales y tarjetas inteligentes. Los dispositivos terminales de Wimax vienen con certificados digitales incorporados, que contienen sus claves publicas y direcciones MAC. El operador Wimax puede aplicar los certificados para los dispositivos de autenticación usando un nombre de usuario, contraseña o una tarjeta inteligente sobre el, para la autenticación del usuario.

***Protocolo de gestión de clave*:** La privacidad y el protocolo de gestión de clave versión 2(PKIv2) son usados para transmitir la información de las claves en forma segura, de una estación base a una estación móvil. PKM también es usado para reautorizar y renovar las claves periódicamente. PKM es un protocolo cliente-servidor, la estación móvil actúa como cliente y la estación base como servidor, este usa certificados digitales x.509 y RSA que son algoritmos de encriptación de clave publica, las cuales son usadas para el intercambio seguro de la información de las claves entre la estación base y la estación móvil.[13]

Protección de mensajes de control: La integridad de los mensajes de control que van sobre el aire es protegida usando esquemas de resumen de mensajes tales como AES basado en CMAS o Message Digest 5 basado en HMAC (Hash-based Message Authentication).

Apoyo para una rápida entrega: Para apoyar rápida entrega, Wimax permite a la estación móvil usar una pre-autenticación con la estación base destino particular para asistir en re entrada acelerada. Un esquema de apretón de manos (hanshake) de tres formas, es soportado para optimizar el mecanismo de re autenticación para soporte de entrega rápida, además de que previene de cualquier ataque de hombre en el medio.

[13] Security: WIMAX Security Functions [en línea]. [Consulta: 03 Julio. 2008]. Disponible en: http://www.freewimaxinfo.com/security-functions.html

1.5 INFRAESTRUCTURA DE SEGURIDAD

Además de encriptar el tráfico de la red más allá de la autenticación predeterminada del PKI, OEMs (Productor den Equipos Original) aplica varias características adicionales dentro de un equipo de redes para asegurar la infiltración de los paquetes de datos procedentes de los servidores de señalización, dirigiendo el tráfico a su destino. Varias características se destacan aquí en el contexto de la VoIP, cada uno de los cuales deben ser tratadas por OEM en el desarrollo de una plataforma de convergencia de red.

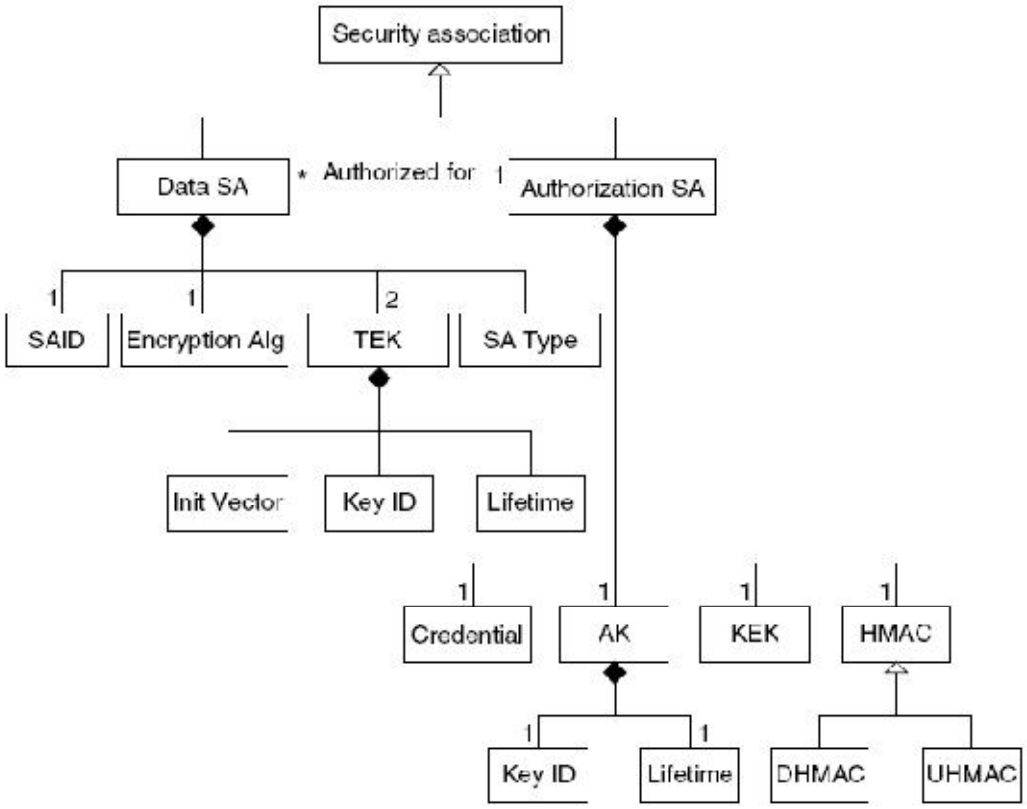


Figura 9. Diagrama Estructura de Seguridad[14].

[14] Tomado de la referencia bibliográfica No.9 Pág.200

- ✓ Firewall y NAT transversal, topología de la clandestinidad: El firewall proporciona acceso a dispositivos autorizados para el registro haciendo llamadas VoIP a través de servidores, dinámicamente abriendo y cerrando múltiples puertos de señalización, mientras que la manipulación no solicita los períodos de sesiones. Un recorrido de NAT permite a ambas señales y medios de comunicación que corren desde los dispositivos con las direcciones IP cubiertas.

- ✓ DoS y ataques de inundación de detección: La sesión de control de fronteras (SBC) deberá detectar los ataques de DoS, UDP, ICMP y TCP.

- ✓ Señalización de seguridad y los medios de comunicación, robo de servicio de prevención: Señalización de seguridad se basa en MD-5 y la autenticación TLS / IPsec. Los medios de seguridad se basan en garantizar RTP / IPsec. El tipo de seguridad es negociable a través de señalización SIP o por medio de un proceso de dotación.

- ✓ Control de acceso granular: De acuerdo con la política de control de acceso granular provee una facilidad para el administrador creando la política de administrador especifica.

- ✓ Sesión de control de admisión, al margen de la ley RTP detección, control y configuración: La SBC permitirá a los medios de comunicación de tráfico pasar por válidos los períodos de sesiones y aplicar normas de gestión y control para evitar el exceso de tráfico. Del mismo modo, la SBC deberá proporcionar a la QoS deseada por la configuración del tráfico en la salida.

- ✓ Firewalls especialmente diseñados para aplicaciones específicas puertas de entrada: Estos firewalls tienen mayores capacidades de cortafuegos más convencionales porque son parte de los gateways VoIP / IP PBX. El firewall puede proporcionar seguridad a estos elementos y detectar fraudes en tiempo real en las redes distribuidas, que no es posible en los sistemas de legado PSTN centralizado que adoptar sistemas de gestión.

- ✓ De detección de intrusos y sistemas de prevención: Un sistema de detección de intrusos es de vital importancia en la detección basada en firma y ataques de intrusos. Este sistema no supone demoras y señalización del tráfico que fluye a través de la red.

Para acelerar su despliegue y mantener una ventaja competitiva en términos de innovación de productos, OEMs se convertirá en software de terceros fabricantes de diseño original, para incorporar amplia convergencia de plataformas de software que comprende el apoyo a las mencionadas características de seguridad. Estas plataformas son:

- ✓ Lo suficientemente amplio como para acomodar las exigencias de la empresa;
- ✓ Completamente probado y aprobado por la industria consorcios y grupos de seguridad, lo que permite a los OEM somerterse a rigurosas normas de certificación, y Plenamente interoperables con herencia (es decir, 802.11) y futuras (por ejemplo, 802.16e) las normas, aseguran los productos siguen siendo preparada para el futuro.

Además, estas plataformas de software son lo suficientemente maduras para la integración en cualquier dispositivo Wimax, que permite diseñar e implementar soluciones al mercado a una mejor reacción para el usuario final o empresa.

1.6 ELEMENTOS ESENCIALES DE LA SEGURIDAD.

La seguridad es un elemento clave de los sistemas de acceso inalámbrico de banda ancha. Cualquier red que transmite sus datos a través de señales inalámbricas es de por sí más abierto a la injerencia, de intrusión o asalto. Esto no significa que la solidez de la seguridad de la banda ancha inalámbrica, es imposible, sólo es más difícil.

Afortunadamente, las redes inalámbricas de banda ancha han madurado características de seguridad en su funcionamiento, siendo estas mejor. Incluso la verdadera Wi-Fi y redes de propiedad han mejorado ampliamente sus protocolos de seguridad.

Con la llegada de Wimax, la seguridad de redes, se ha puesto a disposición de los proveedores de servicios inalámbricos de banda ancha ha alcanzado todos los tiempos máximos de funcionalidad. Hoy las redes Wimax se pueden garantizar de manera más eficaz. Sin embargo, para la obtención de la red Wimax existen consideraciones adicionales que deben evaluar los carrier como parte de un fondo de seguridad de aplicación. De hecho hay cinco aspectos principales de la seguridad de Wimax que deben considerarse en el diseño de un plan de seguridad para su red Wimax. Estos van desde técnicas de reducción en la capa física, a la mejora de la autenticación inalámbrica de intrusos, el cifrado de datos y la protección de la seguridad del transporte.

En cada nivel, las opciones de la aplicación y los niveles de seguridad se pueden hacer, aunque en el caso de la capa física las opciones son limitadas. Empecemos por examinar algunos de los ataques que se pueden suministrar junto con algunas de las herramientas que en particular Wimax ofrece.

1.6.1 Capa Física de Seguridad.

Hay dos tipos básicos de los ataques que pueden afectar a la capa física de Wimax. Una de ellas es interferencias y paquetes de codificación. La primera es relativamente sencilla, y es a veces el resultado de la interferencia en lugar de un ataque, fue diseñada para frecuencia 10-66 Mgz, sin embrago solo puede utilizarse en la línea de visibilidad directa, con el fin de ofrecer un mayor rendimiento a distancia máxima al tiempo que ofrece 99,999 por ciento de fiabilidad, también maneja diversas técnicas, tales como el Jamming, que consta de una señal más fuerte de la red Wimax, , ya sea en los canales o con intermitentes ráfagas sostenidas.

Dado que la mayoría de los servicios de red Wimax son suministrados a través de las bandas con licencia (en la actualidad, 3,5 GHz y 2,5 GHz internacionalmente tanto a nivel internacional como en los EE.UU.), ofrece este espectro relativamente tranquilo de la interferencia accidental; esta interferencia no siempre pueden ser totalmente descontado ya que hay una posibilidad de que lo que se llama segunda y terceras olas de interferencia armónica, es de menor frecuencia de las señales, si ellos están en una estrecha proximidad a los sistemas de antenas o Wimax, la señal opera con ellos lo suficientemente cerca por la proximidad física a nivel local, llevando a la sobrecargada la señal Wimax.

También a veces, las fugas de otros equipos transportadores, ocasionalmente, se producen dentro de las salas de torres de pc. Estos por lo general puede ser detectada en la planificación de los barridos con un analizador de espectro antes de la instalación y filtros de supresión o filtro para banda de algún tipo, sobre los equipos específicos se puede aclarar estas cuestiones rápidamente. Interferencias constantes, ya sea dañino o no, se encuentran bastante rápido usando un analizador de espectro y antenas direccionales para triangular la señal, intermitente atascos o interferencia, pueden ser más difícil para encontrar la ubicación, pero también es menos intrusiva a la red, por lo que en algunos paquetes de retransmisión y desaceleraciones, pero con menos frecuencia en los cortes de manta. Un buen análisis de espectro realizadas antes del despliegue y de esa forma intermitente, pueden contribuir en gran medida a derrotar a este problema. En algún momento la mayoría de los proveedores de servicios Wimax se enfrentará a algún tipo de interferencia o problemas.

El paquete de codificación es un ataque que se produce cuando los paquetes de control en los respectivos enlaces ascendente y descendente son codificados y luego regresados a la red. Este ataque es más difícil de montar que un ataque de interferencias.

"Dado que la mayoría de las redes Wimax hoy por división de tiempo de uso de la doble cara (TDD), en el que las señales son rodajas de tiempo a través de un paquete atacante puede analizar este momento y la secuencia de captura de datos de control, en el preámbulo y de ruta, y enviar de vuelta en el momento correcto para interrumpir legítimo Señal, lo que resulta en demoras y reduce el ancho de banda de manera efectiva.

Los paquetes codificados son interceptados con dúplex por división de frecuencia (FDD), que transmite el enlace ascendente y descendente de manera simultánea, pero es aún más difícil de explotar este ataque que con los sistemas TDD.

Aunque pueda parecer la capa física es inherentemente más vulnerables como los elementos de seguridad de Wimax se encuentran en las capas superiores, la realidad es a menudo los hackers pueden encontrar las rutas y entrar a los sistemas, en términos de utilidad explota más alto en la pila, porque como Wimax soporta múltiples selecciones en que los proveedores de servicios pueden optar por aplicar en términos de autenticación, múltiples acciones.

1.6.2 Autenticación De Las Transmisiones Inalámbricas.

En el control de acceso a medios (MAC) Wimax en la capa de control o cabecera MAC parte de las transmisiones no está encriptado. Esto es deliberado, a fin de facilitar el trabajo de la capa MAC. Con esto no significa que Wimax es inseguro, pero sí presenta algunas debilidades para las transmisiones.

Figura 10. Autenticación de Procesos[15].

[15] Tomado de la referencia bibliográfica No.9 Pág.237

Tradicionalmente el primer nivel de seguridad de autenticación para las tecnologías inalámbricas de banda ancha de más edad ha sido MAC y autenticación Wimax, esta técnica permite a los proveedores de servicios de registro tener direcciones MAC y permitir sólo las direcciones para acceder a la red. Una segunda, más nueva y mejor elección es el construido en el dispositivo de apoyo a los certificados X.509.

Por último el protocolo de autenticación extensible utiliza la capa de seguridad de transporte, método (EAP-TLS), añadió con el estándar 802.16e, agrega una capa adicional de seguridad para la autenticación de la mezcla. "Si una estación base no es suficiente con establecer las medidas de autenticación, un atacante puede capturar los paquetes de control y plantean como una forma legítima de abonado de más edad, incluso con dispositivo de autenticación MAC permitido".

Sin embargo, el certificado X.509 hace que sea muy difícil para un intruso suplantala identidad de un suscriptor. El certificado X.509 está integrado en las unidades de suscriptor y Wimax incorpora un cifrado de clave pública de autenticación. Esto significa que una estación base Wimax puede detectarlo en forma rápida y sencilla.

El protocolo X.509 es muy bueno, sin embargo no hay manera de verificar si una estación base es auténtica, con el X.509 el cual captura los paquetes de control de una estación para la transmisión legítima, entonces el momento de la secuencia TDD señal a la unidad para el abonado que espera recibir, posiblemente dependiendo del tráfico.

Esta técnica, se añadió al estándar 802.16e, permite que tanto el abonado y la estación base, para autenticar mutuamente tienen que utilizar el protocolo X.509.

Los encabezados MAC nunca son cifrados en Wimax, sin embargo pueden elegir EAP para la autenticación de ellos. Este enfoque se llama código de autenticación de mensajes (Hash) que es un número generado a partir de una cadena de texto el cual usa una forma de clave privada cifrada.

"El hash se agrega al final del mensaje en sí". Cuando se reciben mensajes de la estación de base, genera su propio hash para comparar a la que se recibió de los abonados utilizando su clave privada para comparar.
Lo anterior añade una capa adicional de autenticación de confirmación. La desventaja de este es que requiere ciclos de procesador. Así que un hacker astuto puede enviar miles de mensajes de HMAC adjunto obligando a la estación de base para ejecutar los ciclos de procesador comparándolas con la eficacia resultante en un ataque de denegación de servicio.

Esto indica un dilema para los operadores inalámbricos de banda ancha Wimax, es decir, que incluso las opciones de seguridad puede traer consecuencias. Así, mientras Wimax tiene mejores herramientas y apoya la gestión de cabecera de autenticación MAC, las compañías pueden optar por trasladar algunos de los procesos de carga de la autenticación y cifrado de datos a la oficina central (CO).

1.6.3 Cifrado

Es evidente que la primera capa de defensa de los operadores Wimax se basa en la autenticación de un usuario legítimo de su red. Sin embargo, Wimax, con su ratificación 802.16e, ofrece herramientas para la línea superior de cifrado de los datos. La encriptación de datos estándar (DES), que se basó en una clave de 56 bits para el cifrado. Esto se considera en gran parte obsoletos. Wimax 802.16e ciertamente apoya DES (3DES), pero también añade soporte para el Advanced

Encryption Standard (AES) que apoya, 128-bit, 192-bit o 256-bit claves de cifrado. AES también se reúne el Federal Information Processing Standard (FIPS) 140-2 especificación, exigidas por numerosas ramas gubernamentales.

Esta tecnología exige que los procesadores de la estaciones base sean sólidos y muy eficaces. Pero una vez más, la cuestión es que dependerá en gran medida de los carrier a cargo de la transformación o el cambio de servidor de la base de soluciones de terceros que ofrecen más opciones en el cifrado.

Corresponde a los carrier de Wimax buscar en los diversos escenarios para sus necesidades de seguridad y poner un plan de migración en el lugar, si es necesario, antes de comenzar la emisión. En el pasado por ejemplo los celulares se centraron en su mayoría haciendo caso omiso a la autenticación y cifrado.

A través de este punto se ha estudiado seguridad capa física de Wimax, así como las opciones de autenticación en la capa MAC y adicionalmente AES de cifrado de datos que ahora apoya Wimax.

1.6.4 Participación De Terceros En La Protección Contra Intrusos

En varios aspectos, la revisión de opciones de seguridad Wimax, permite diagnosticar que cada vez se debe profundizar en ella. Se han estudiado las técnicas de capa física para mitigar problemas tales como interferencias y paquetes de codificación. Se examinaron los sistemas de autenticación de Wimax, que son un componente importante de una red segura y también el de cifrado de datos.

Sin embargo, existen consideraciones más allá de la simple seguridad que pueden conducir a una migración de terceros, de detección de intrusos y herramientas de protección de intrusos y no la protección de datos. Se trata de dos clases diferentes de solución. Sin duda una buena protección contra intrusos de terceros puede vigilar y asegurar una red de autenticación. Muchas de las soluciones también ofrecen protección a gusanos, caballos de Troya de protección, las defensas contra los virus, exploits puerta trasera y ataques de denegación de servicio.

1.6.5 Participación De Terceros En El Transporte De Datos De Seguridad

AES apoya claramente un sistema de cifrado de datos, Wimax ofrece excelente seguridad en este sentido. Sin embargo, otras soluciones que satisfacen las necesidades de los clientes, tales como redes privadas virtuales requieren enfoques diferentes.

Si la fuerza de todos para instalar una pequeña pieza de software de cliente puede hacer cumplir EAP autenticación basada en toda su red, Esto también permite una IPSec AES basado en la solución de cifrado de datos que soporta un túnel y encapsulación de los datos.

2 VULNERABILIDADES

VoIP está ganando cada vez más la atracción entre los consumidores y usuarios empresariales, ofreciendo una alternativa rentable, enfrentando a los medios de comunicación en contra de la tradicional red telefónica pública conmutada (RTPC). Teniendo en cuenta, la evolución del Wimax, este ofrece un protocolo llamado QoS para aplicaciones de baja latencia como VoIP, se espera que este servicio esté integrado por el grueso de ancho de banda dentro de los primeros meses de despliegue.

Sin embargo, dentro del entorno WiFi se presentan varias vulnerabilidades de VoIP con Wimax. Un sistema de VoIP utiliza protocolos como H.323, período de sesiones de iniciación y protocolos (SIP) para la señalización; son excepcionalmente populares por su facilidad de aplicación, interpretación y análisis de estado, pero si se dejan solos, son igualmente conocidos por su vulnerabilidad, RTP/ RTCP para los medios de transporte y control, servidores de medios de comunicación como puertas de entrada, los medios de comunicación (llamados *Agentes*) , los controladores de puerta de enlace, guardianes y apoderados para permitir llamadas entre los clientes de VoIP.

Los riesgos de seguridad que se mantienen dentro de los propios servidores de señalización, junto con los piratas informáticos que emplean uno o varios métodos para obtener acceso no autorizado, sin embargo OEM debe abordar cada uno de estos métodos, en forma individual y en su conjunto, al desarrollar una efectiva infraestructura de seguridad que pueden hacer frente a los hackers.

La suplantación del Cliente: El protocolo SIP puede permitir el registro de múltiples contactos para un usuario individual, con la "a" y "de" campos de cabecera única por contacto. Por suplantar la identidad de los clientes, un hacker

puede registrar sus propios contactos y hacer el nuevo correo de voz y notificaciones a las direcciones de contacto redirigido.

Servidor de suplantación: Después que un cliente se registra con el servidor de credenciales, los piratas informáticos pueden interceptar períodos de sesiones de iniciación, solicitudes del cliente y responder con una respuesta falsa dirigiendo la solicitud a un nuevo servidor. Las llamadas realizadas por el cliente, ya sea conectarse o no, los hackers definen para estos criterios de valoración, en ambos sentidos exponiendo al usuario. Del mismo modo, los piratas pueden interceptar las solicitudes, período de sesiones en el proceso de registro propio, la reorientación de las solicitudes de registro en un servidor falso y sacar a la luz la información del servidor credencial.

Mensaje manipulación: Considerado como intermediarios de confianza, los servidores proxy son a menudo empleados por los clientes para intercambiar período de sesiones de iniciación, flujo de solicitudes y los medios de comunicación. Los hackers pueden aplicar falsificación a los servidores y sin conocimiento del cliente, interceptar su período de sesiones y métodos de cifrado asociados con claves. Con esta información vital, pueden redirigir los flujos de comunicación a su dispositivo y descifrar la información, o impedir el flujo de estos para llegar a su destino real, lo que permite las escuchar las conversaciones telefónicas.

Sesión de la manipulación y el secuestro: Después de realizar el análisis a una llamada se establece que los mensajes se intercambian entre la estación base y CPE para el período de sesiones del códec (que es el encargado de codificar el flujo o la señal) de renovaciones y solicitudes de las negociaciones. Sin embargo, durante la llamada, es posible que un hacker aproveche el flujo de mensajes e ingrese. Cuando un cliente espera una sesión de mensajes la renovación es

periódica, ya que la información es manipulada para desviar el flujo de la comunicación, lo que resulta en espiar las conversaciones.

Señalización solicitudes resultantes en ataques DoS: Los servidores proxy son los encargados de los procesos de registro y apertura de los períodos, las sesiones, solicitudes, en un número de puerto estándar, a través del cual los hackers pueden ingresar con una avalancha de peticiones similares. Al mismo tiempo el servidor con múltiples período de sesiones de iniciación tendrá solicitudes como resultado a la sobrecarga del servidor y la denegación del servicio.

Para proteger la tecnología Wimax, contra cualquiera de las mencionadas vulnerabilidades, el estándar 802.16 está habilitado para los dispositivos dentro de la red Wimax, por ejemplo, adaptadores de terminal (TAS), dispositivos de acceso integrados (IADs), pasarelas, sistemas de facturación, servidores de correo de voz y mensajería unificada de sistemas, deben estar equipados con un software que puede detectar y prevenir ataques externos de infraestructura antes de que tengan éxito. La complejidad de este software varía con el tipo de dispositivo, su uso, aplicación e importancia dentro de la red.

3 RECOMENDACIONES

Es preciso saber que la evolución en la forma de cómo nos protegemos será un proceso permanente, y mas conociendo el gran impacto y lo necesario que se ha convertido la seguridad para este tipo de tecnología.

Por tal motivo los conceptos, los protocolos, las tecnologías expuestas en esta monografía dentro de unos años serán obsoletas y solo se utilizara como historia de la tecnología en ese momento.

4 CONCLUSION

Este documento fue realizado con el fin de ubicar a los estudiantes en un contexto generalizado donde la seguridad en Wimax es uno de los principales temas a nivel mundial, y que permite conocer todas sus características, conceptos, origen, vulnerabilidades y todos sus componentes, para un mayor aprendizaje de ingenieros, estudiantes, docentes y demás comunidades involucradas en el tema.

La seguridad en Wimax fue diseñada por la necesidad de encriptar y proteger los datos de esta tecnología, ¿pero que tan necesario es la protección de la información? Dependiendo del valor que cada entidad le de a la información seria necesario hacer la inversión en seguridad, por que si la información no es tan costosa no vale la pena invertir en esta. O en caso de que los datos tengan mayor validez se hace necesario implementar un sistema más robusto para la seguridad.

Así como todo proyecto, se inicia dando a conocer lo básico de las tecnologías, de quienes conforman su grupo de trabajo y desarrollo en el estándar y como se ubica dentro del espectro de servicios tecnológicos, para después empezar a fundamentar sus bases teóricas, las cuales conllevan ha tener un concepto bien definido de esta tecnología, para luego así poder penetrar dentro de las diferentes variantes que ella ofrece.

Es gratificante observar cómo se desarrolla la seguridad de Wimax, pero lo que si nos costo un poco de esfuerzo fue el poco recurso bibliográfico que existe sobre este tema, de tal manera que lo mas importante y representativo fue de que cada tema fuese expuesto de forma clara y concisa, para que cualquier persona interesada en conocer sobre este tema pueda entenderlo; al tiempo que se ofrece a la comunidad una nueva posibilidad de cubrir sus necesidades e intereses en este tema.

5 BIBLIOGRAFIA

Paginas Web:

1. http://www.wikio.com/article/39293488, WiMAX Security: Solutions for Secure 802.16

2. http://www.wimax.com/education/faq/faq27, Is Wimax technology secure?

3. http://www.clcert.cl/show.php?xml=xml/editoriales/doc_07-08.xml&xsl=xsl/editoriales.xsl, WiMAX: Desafíos de seguridad

4. http://www.nobosti.com/spip.php?article65, SEGURIDAD EN REDES WIMAX

5. http://infowimax.blogspot.com/2008/04/wimax-cinco-elementos-esenciales-de-la.html, Wimax: Cinco Elementos Esenciales De La Seguridad Wimax.

6. http://www.borrmart.es/articulo_redseguridad.php?id=1088&numero=23# Seguridad en Redes Wimax.

7. http://rinuex.unex.es/modules.php?op=modload&name=Textos&file=index&serid=3, REDES INALÁMBRICAS: Seguridad.

8. http://documentos.shellsec.net/otros/SeguridadWireless.pdf,Seguridad Wireless.

Bibliográficas:

9. Taylor & Francis Group. WIMAX: Standards and Security. Editorial SYED AHSON MOHAMMAD ILYAS, 2006. 278 p.

10. Ing. Luis Meléndez Campis. Esp. En telecomunicaciones, Diapositivas Introducción a la Seguridad, 2008, 64 p.

6 APENDICE

AAA: Abreviatura de Autenticación, Autorización y Accounting, sistema en redes IP para a qué recursos informáticos tiene acceso el usuario y rastrear la actividad del usuario en la red.

AES: Estándar de Encriptación Avanzado.

APP: Punto de Acceso

AK: Clave de autenticación, la clave activada por un BS en la red durante la autenticación con la SS de entrada.

Algoritmo de Encriptación: Codificadores de bloques de bits sobre los que iteran determinadas operaciones tales como sustitución, transposición, suma/producto modular y transformaciones lineales. Cada algoritmo utiliza bloques de distintos tamaños.

Autenticación: Proceso en el que se da fe de la veracidad y autenticidad de un producto, de unos datos o de un servicio, así como de la fiabilidad y legitimidad de la empresa que los ofrece.

Autorización: Proceso por el que se acredita a un sujeto o entidad para realizar una acción determinada.

BS: Estación Base Inalámbrica.

Códec: Los códec pueden codificar el flujo o la señal (a menudo para la transmisión, el almacenaje o el cifrado) y recuperarlo o descifrarlo del mismo modo

para la reproducción o la manipulación en un formato más apropiado para estas operaciones. Los códec son usados a menudo en videoconferencias y emisiones de medios de comunicación.

CID: Identificador de Conexión

Checksum Criptográfico: Checksum calculado mediante la utilización de un algoritmo con base criptográfica. Es imposible cambiar unos datos sin que el checksum criptográfico cambie. Ver también Checksummer.

CheckSum: Herramienta que calcula un único número asociado a determinados archivos que habitualmente no cambian para protegerlos. CheckSummer recalculará periódicamente dicho número y si se detecta que ha cambiado, será un indicio de infección.

Clave de Encriptación: Serie de números utilizados por un algoritmo deencriptación para transformar plaintext (texto sin encriptar que se puede leer directamente) en datos ciphertext (encriptados o cifrados) y viceversa.

Cliente o Usuario Inalámbrico: Toda solución susceptible de integrarse en una red wireless como PDAs, portátiles, cámaras inalámbricas, impresoras, etc.

CRC: Control de Redundancia Cíclica

Denegación de Servicio (DoS) - Denial of Service: Se trata de una ofensiva diseñada específicamente para impedir el funcionamiento normal de un sistema y por consiguiente impedir el acceso legal a los sistemas para usuarios autorizados.

DES: Algoritmo que codifica los textos haciendo bloques de datos de 64 bits y utilizando una clave de 56 bits. Existe otra modalidad más avanzada denominada 3DES que utiliza el algoritmo DES tres veces. Hay varios tipos de algoritmo 3DES en función del número de claves que utilicen y de la longitud de éstas.

DES-CBC: Estándar de Encriptación de datos con cambio de cifrado de bloques.

EAP: Extensible Authentication Protocol (Protocolo de Autenticación Extensible): Extensión del Protocolo punto a punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un sólo uso,autenticación por clave pública mediante tarjetas inteligentes, certificados y otros. Junto con los métodos de autenticación EAP de alto nivel, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virtual (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, que otros métodos de autenticación, como CHAP.

EC: Control de Encriptación.

EIK: Clave EAP integrada.

EKS: Clave de Encriptación Secuencial

FDD: Dúplex por división de frecuencia

GMH: Cabecera Genérica de MAC

HASH: Un valor hash, también conocido como "message digest", es un número generado a partir de una cadena de texto. El hash es sustancialmente más pequeño que el texto en sí, y es generado por una fórmula de tal forma que sea poco probable que algún otro texto produzca el mismo valor. Los hashes juegan un papel crucial en la seguridad donde se emplean para asegurar que los mensajes transmitidos no han sido manipulados. El emisor genera un hash del mensaje, lo encripta y lo envía con el propio mensaje. El receptor luego decodifica ambos, produce otro hash del mensaje recibido y compara los dos hashes, si coinciden, existe una probabilidad muy elevada de que el mensaje recibido no haya sufrido cambios desde su origen.

I**EEE 802,16**: Grupo de trabajo sobre acceso inalámbrico sobre las normas de banda ancha (BWA), establecida en 1999, tiene por objetos estandarizar la banda ancha inalámbrica de redes de área metropolitana (WMAN).

IETF: es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad.

IPSec - IP Security: Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtuales (VPNs), soporta dos modos de encriptación: Transporte y Túnel. El primero sólo encripta la parte relativa a los de datos (payload) de cada paquete, pero deja la cabecera intacta. Por su parte, el modo Túnel, más seguro, encripta todo.

IV: Vector de Inicialización.

KEK: clave de encriptación de clave, la clave utilizada para encriptar la clave de encriptación de tráfico.

MD5: Algoritmo de encriptación de 128-bits del tipo EAP creado en 1991 por el profesor Ronald Rivest para RSA Data Security, Inc. empleado para crear firmas digitales. Emplea funciones hash unidireccionales, es decir, que toma un mensaje y lo convierte en una cadena fija de dígitos. Cuando se utiliza una función hash de una dirección, se puede comparar un valor hash frente a otro que esté decodificado con una llave pública para verificar la integridad del mensaje. Basado en Nombre de Usuario y Contraseña, el primero se envía sin protección. Sólo autentica el cliente frente al servidor, no el servidor frente al cliente.

MPDU: Protocolo MAC Unidad de Datos

MSK: Clave Maestra de Sesión.

OFDM: Ortogonal multiplexación por división de frecuencia, un esquema de modulación digital. Se divide por flujos de bit en varias sub corrientes, y transmite en paralelo por la modulación ortogonal, sub mensajero de frecuencia.

OEMs: Fabricante de equipos originales.

PHY: Capa Física

PKM: La clave privada con manejo de protocolo definido en el las subcapas de la seguridad en wimax. Se protege la privacidad de SS o BS a través de procesos tales como la autenticación y el intercambio de claves. Tiene dos versiones: PKMv1 y PKMv2

PMP: Punto a Multipunto

QoS: *(Quality of Service) calidad del servicio*

RSA Rivest-Shamir-Adleman: Algoritmo de Encriptación de clave pública

SA: Asociación de seguridad.

SAP: Servicio de Punto de acceso.

SAID: Asociación identificador de seguridad.

SDU: Unidad de Servicio de Datos.

SFID: Servicio de Identificador de flujo.

SHA: Algoritmo de Control Seguro.

SS: Estación de subscriba inalámbrico

TDD: taller de diseño digital

TEK: Clave de Trafico Encriptado, la clave utilizada para encriptar el tráfico de Wimax.

TKIP - Temporal Key Integrity Protocol / Protocolo de Integridad de Clave Temporal: Cifra las llaves utilizando un algoritmo hash y, mediante una

herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

TLS - Transport Layer Security: Protocolo del tipo EAP que garantiza la privacidad y la seguridad de datos entre aplicaciones cliente/servidor que se comunican vía Internet. Trabaja en dos niveles: El protocolo de registro TLS - situado en el nivel superior de un protocolo de transporte seguro como TCP asegura que la conexión es privada empleado encriptación simétrica de datos y asegura que la conexión es fiable. También se utiliza para la encapsulación de protocolos de nivel superior, tales como el TLS handshake Protocol. Y, el protocolo de handshake TLS - permite la autenticación entre el servidor y el cliente y la negociación de un algoritmo de encriptación y claves criptográficas antes de que el protocolo de la aplicación transmita o reciba cualquier dato. TLS es un protocolo independiente que permite que protocolos de niveles superiores se sitúen por encima de él de manera transparente.

VPN - Red Privada Virtual / Virtual Private Network: Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado

WIFI: Tecnología que permite comunicar portátiles, PC, computadores de mano y diversos artilugios electrónicos de forma inalámbrica, y tiene varias aplicaciones.

WIMAX: Interoperabilidad Mundial para Acceso por Microondas, una tecnología especifica por el IEEE 802,16 normas para permitir la entrega de la última milla de acceso banda ancha inalámbrica.

WIMAX seguridad de subcapas: Protocolo definido en la capa MAC Wimax. Asegura SSS, SRS, transmisión y conexiones

X.509: Estándar para la infraestructura de clave pública (PKI)

XOR: exclusivo-o, Compuerta lógica conocida para unión de proposiciones lógicas.