UNIVERSIDAD Rafael Belloso Chacín

Revista Electrónica de Estudios Telemáticos

TÉLÉMATIQUE

ANÁLISIS DEL ALGORITMO DE SEGURIDAD EN REDES WIMAX

Amelia C, Colina S.
Universidad Rafael Belloso Chacín. Venezuela

Nuñez Steve
Universidad Rafael Belloso Chacín. Venezuela

RESUMEN

El presente trabajo de investigación se basa en analizar las vulnerabilidades del algoritmo de seguridad de las redes inalámbricas 802.16x (Wimax), para determinar las debilidades establecidas en el nivel de control de acceso MAC. Los defectos más obvios sobre el diseño de IEEE 802.16 son la carencia de definiciones explícitas en cuanto la autorización SA, significando que nunca recibe los mismos datos SA, la necesidad de la legitimación mutua puesto que las amenazas contra los datos SA se aplican directamente sobre la BS y la única manera de proteger al cliente contra la falsificación es sustituir el esquema de autentificación del estándar por uno que proporcione autentificación de la BS y de las asociaciones de seguridad SA. La metodología de investigación se encuentra enmarcada dentro del tipo de estudio de campo y su diseño se considera no experimental. Se concluyó que insertando valores aleatorios a las identificaciones de los certificados digitales de la BS y la SS, se mejora considerablemente la probabilidad de generar falsificaciones de BS y SS autorizadas, ya que anteriormente eran fácilmente detectados y reutilizados. Asimismo generar la llave HMAC con los valores de las llaves del downlink y el unplink se garantiza que únicamente las SS y BS que conocen el AK pueden descifrar la llave y construir el intercambio de mensaje de manera correcta.

Palabras Clave: Seguridad, Cifrado, Wimax, Confiabilidad, Integridad.

ABSTRACT

The present work of investigation this based on the analysis of the vulnerabilities of the algorithm of security of the radio networks 802.16x (Wimax), to aim to determine the weaknesses established in the level of control of access MAC. The obvious defects but on the design of IEEE 802,16 are the deficiency of explicit definitions as soon as the authorization SA, meaning that never receive data SA such, the necessity of the mutual authentication since the threats against data SA are directly applied on the BS and the only way to protect to the client against the falsification are to

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

replace the scheme of authentication of the standard by which it provides authentication of the BS and the associations of security SA. The investigation methodology is framed within the type of field study and its design is considered no experimental. One concluded that inserting random values to the identifications of digital certificates of the BS and the SS, considerably improves the probability of generating falsifications of authorized BS and SS, since previously easily they were detected and reused. Also to generate key HMAC with the values of the keys of downlink and unplink is guaranteed that solely the SS and BS that know the AK can decipher the key and construct the interchange of message of correct way.

Key words: Security, Coding, Wimax, Trustworthiness, Integrity.

INTRODUCCIÓN

El estándar **IEEE 802.16x** es conocido a nivel mundial como **WIMAX**, (*Worldwide Interoperaability for Microwave Access*) y su propósito es alcanzar velocidades de comunicación hasta los 75 Mbit/s, operando en un rango de frecuencias más bajo (2 a 11 GHz). Estas velocidades tan elevadas se consiguen gracias a utilizar la modulación OFDM (Orthogonal Frequency División Multiplexing) con 256 subportadoras, las cuales puede ser implementadas de diferentes formas, según cada operador, siendo la variante de OFDM empleada, un factor diferenciador del servicio ofrecido. [1]

La seguridad en las redes inalámbricas representa una necesidad urgente, dadas las características del medio por donde se transmite la información. La gran cantidad de redes inalámbricas actualmente instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, poniendo en peligro la confidencialidad e integridad de dicha información, lo cual pude ser grave para cualquier empresa o institución que utilice esta tecnología.

En este sentido, un atacante con un equipo correctamente configurado y con posición adecuada puede interceptar una señal, es decir, obstaculizar los mensajes que se están enviando por un canal inalámbrico y reutilizar la trama por lo tanto, hacen falta mecanismos de confidencialidad. Debido a esta vulnerabilidad, también se podría capturar tramas de lugares autorizados y formar nuevas tramas, modificarlas y retransmitirlas. En este caso el algoritmo de seguridad debe proporcionar un mecanismo de autenticidad de los datos. [2]

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

Aún más, si hablamos de la carencia de definiciones explícitas, el estándar 802.16 no define explícitamente la autorización (Security association [SA]), y por tal razón nunca se recibe los mismos datos que se envían. En este sentido, las amenazas contra los datos SAs se aplican directamente sobre autorización SA, ocasionando problemas, tales como; nunca distinguir un caso autorización SA de otro. Además, la autorización SA no incluye la identidad de la estación base (Base Station [BS]), así que los proveedor del servicio (Subscriber Station [SS]) no pueden distinguir si una estación base es autorizada ó desautorizada.

Aunque ocultar la identidad de BS del usuario pude ser deseable; sin embargo, se evitaría que el esquema de cifrado proteja los SS contra la falsificación, conllevando a nuevo ataques. Esto causa un problema relacionado con los datos SAs, porque los SS no pueden distinguir la autorización reutilizada SAs, ni reconocer los datos reutilizados SAs. El esquema por lo tanto es vulnerable al ataque con la reutilización de la llave de cifrado.

Finalmente, todo mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada y consistente; el seguimiento de esta política de seguridad evitaría que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, garantizando la calidad y confidencialidad de la información presente en los sistemas de la empresa

En este orden de ideas, el objetivo de esta investigación es proponer recomendaciones para la optimización del algoritmo encargado de la seguridad del estándar 802.16x, que utilice un mecanismo de cifrado avanzado como un modo de operación, donde se maneje un esquema más flexible de autentificación basado en la autorización SA, y que garantice la autenticación de cada una de las entidades involucradas en una conexión.

El objetivo general de la presente investigación, plantea analizar el algoritmo de seguridad en redes inalámbricas wimax a fin de proponer recomendaciones técnicas, para ello se debe identificar las características del protocolo encargados de la seguridad en redes inalámbricas 802.16x, explicar el funcionamiento del algoritmo de seguridad en redes wimax 802.16x, determinar los ataques de seguridad de redes más comunes en las mismas. Definir las principales vulnerabilidades del algoritmo de seguridad de las redes wimax, y elaborar las recomendaciones para la optimización del algoritmo.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

La presente ponencia corresponde según el tipo, a una investigación de campo, ya que el objetivo es un análisis sistemático de la problemática que presentan las redes wimax, en cuanto a la seguridad de los datos, a fin de describir sus causas y posibles consecuencias, y según su diseño se clasifica como no experimental, ya que consiste en la elaboración de una propuesta viable, o una posible solución a un problema de tipo práctico, para dar respuesta a una problemática planteada.

METODOLOGÍA

Para el desarrollo de la investigación se utilizó una metodología por fases, en donde la primera involucró un proceso de documentación teórico conceptual que permitió describir, explicar las vulnerabilidades como la falta de autenticación de los SA y el manejo de la privacidad y administración de llaves del algoritmo. En la segunda etapa se definió de manera concreta las fallas del algoritmo como se describe a continuación, Y por último se propusieron las recomendaciones para la de seguridad e intercambio de datos.

VULNERABILIDADES DEL ALGORITMO SEGURIDAD

Autorización de los SA

Luego del análisis del algoritmo de seguridad de 802.16x, se pudo detectar que unos de los defectos más obvios sobre el diseño de IEEE 802.16 es la carencia de definiciones explícitas en cuanto la autorización SA, significando que nunca recibe los mismos datos SA. Las amenazas contra los datos SA se aplican directamente a la autorización SA, así que esta falta conduce a los problemas graves como son: [1]

Nunca distinguir el estado del SA con un caso de autorización SA, dejando el protocolo una puerta abierta para nuevos ataques. Además, autorización SA no incluye la identidad de BS, así que los SS no pueden distinguir un BS autorizado de uno desautorizado. Aunque ocultar la identidad de BS pude ser deseable, ocultársela a los SS evitaría que la administración y el cifrado de llaves protejan a los SS contra la falsificación y nuevo ataques.

Esto causa un problema relacionado para los datos SAs. Porque los SS no pueden distinguir la autorización de los SA reutilizada, tampoco puede reconocer los datos SA, es decir las llaves de cifrado que han sido

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

reutilizadas. El esquema del cifrado es por lo tanto vulnerable al ataque con la reutilización de la llave del cifrado. [2]

La manera más segura de corregir la vulnerabilidad, es agregar un valor al azar a la BS y a los SS para la autorización de SA. Requerir la entrada de ambas partes puede proteger sus contribuciones. Una identificación de BS autenticada también eliminaría las amenazas contra las SS, causadas por la asimetría de las credenciales.

Autenticación Mutua

Otra debilidad notable es la necesidad de la legitimación mutua, al momento de la autenticación de un certificado digital de BS. La única manera de proteger al cliente contra la falsificación es sustituir el esquema de la autentificación del estándar por uno que la proporcione de manera mutua. La cual, para cualquier medio inalámbrico; se traduce en la reducción de costos.

Las constantes vulnerabilidades de autorización el SA, provienen del protocolo de administración de llaves (PKM) el cual es abierto a ataques de falsificación, ya los SS no pueden verificar cuando un mensaje de autorización proviene de un BS autorizada. El BS construye las respuestas de autenticación y la envía a los SS usando información pública, así que cualquier BS puede crear una respuesta. Requerir los SS autenticar al BS puede eliminar esta vulnerabilidad

LA PROPUESTA

En virtud que el protocolo de autenticación PKM sujeta los SS a nuevos ataques. Un camino simple para prevenir estos ataques es requerir a los SS generar un número aleatorio en el intercambio del mensaje 2 del protocolo de autenticación, y la BS deberá incluirlo al momento de responder a la SS con su mensaje de autenticación.

Este proceso consiste en el intercambio de tres mensajes entre una estación del suscriptor (SS) y una estación base (BS). Los SS inician el protocolo enviando los primeros dos mensajes, y BS responde con el tercer mensaje como se muestra en la figura 1.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

Mensaje1:

SS → BS: Cert (Manufacturer (SS))

Mensaje 2:

SS → BS: Cert (SS) | Capabilities | SAID

Mensaje 3:

BS → SS: RSA-Encrypt (PubKey(SS), AK) |
Lifetime | SeqNo | SAIDList

Figura 1: Autenticación del PKM
Fuente IEEE 802.16 Security (2004)

Los SS (Subscriber station, Estación del suscriptor) utilizan el primer mensaje para enviar su certificado X.509 Cert (Manufacturer (SS), certificados del fabricante) a la BS (Base Station, Estación Base), donde se utiliza para decidir si la SS (Estación del Suscriptor) es un dispositivo confiado. El algoritmo asume que todos los dispositivos de un fabricante reconocido pueden ser confiados.

El estándar 80216 deja que la BS (Estación Base) ignore este mensaje, lo asuma como un dispositivo seguro. Las SS envían el mensaje 2 inmediatamente después del mensaje 1. El mensaje 2 consiste en el certificado Cert (SS) de X.509 de los SS, incluyendo su capacidad y el identificador SAID. Los Cert (SS) se envían a la BS, quien determina si la SS se autoriza, construyendo una llave pública con el certificado de la SS (Cert (SS)) el cual se envía en el mensaje 3.

Sólo la BS puede verificar el Cert (SS) (certificado de la SS) que está autorizado, respondiendo con el mensaje 3, para establecer una autenticación de SA entre las dos estaciones. El correcto uso de esta llave demuestra quien puede acceder a la red. El estándar asume que solamente la BS y las SS poseen esta llave (AK), la cual nunca deberá ser revelada a terceros.

La intención a colocar un valor aleatorio en la definición datos SA es porque el estándar maneja los 2 bits del identificador de la llave como un buffer repetitivo, permitiendo que un atacante pueda interceptar una llave y reutilizarla, tal como se muestra en la figura 2.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

Tabla 1: Términos usados en los mensajes de autenticación PKM.

Término	**Descripción**
A $\rightarrow$ B: M	La entidad A envía un mensaje a B con el valor M.
Cert (Manufacturer(SS))	Un certificado X.509 que identifica el fabricante de los SS
Cert(SS)	Un certificado X.509 con la llave publica de los SS
SAID	Es un identificador de seguridad entre la SS y la BS. (Fijo)
RSA-Encrypt (k, a)	Llave cifrada
PubKey(SS)	Es la llave pública de la SS
Authorization key	Es la llave de autorización
Lifetime	Es un valor de 32 bits dado en segundos, representa el tiempo de vida de la llave
SeqNo	Es un valor de 4 bit para la AK
SAIDList	Es una lista con las descripción de las SA , que incluye el identificador de seguridad SAID, el tipo de SA

Fuente: IEEE 802.16 Security (2004)

Se propone ampliar el tamaño del identificador de la llave (KEY) para que más identificadores puedan ser transportados a lo largo valor del tiempo de vida de AK. Si un AK dura por lo menos hasta 7 días, mientras que el tiempo de vida de TEK puede ser tan corto como 30 minutos, entonces los datos SA pueden consumir hasta 3.360 TEKs sobre el tiempo de vida del AK, permitiendo que el tamaño de SAID crecer de 2 a12 bits.

Esto plantea la situación de cuando un TEK debe expirar. En el estándar actual, el TEK expira después de un período del tiempo configurable, aunque esto es necesario, no es suficiente, el tiempo de vida por defecto TEK de IEEE 802.16 es mitad del día, y el estándar permite un tiempo de vida del máximo de siete días. Estos números pueden conducir a los problemas.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

Mensaje1:
SS → BS: Cert (Manufacturer (SS))
Mensaje 2:
SS → BS: Cert (SS) | Capabilities | SS-Random
Mensaje 3:
BS → SS: RSA-Encrypt (PubKey(SS), AK) |
Lifetime | SeqNo | SAIDList
SS-Random | BS-Random

Figura 2: Propuesta de Autenticación del PKM
Fuente El autor (2006)

Es importante recordar que IEEE 802.16 utiliza el DES en el modo de CBC para el cifrado. El DES utiliza un bloque 64 bits, para efectuar cada operación del cifrado o del desciframiento de los datos. El modo de CBC usa segmento de cifra (block cipher) con n bits de block chipher se pierde su seguridad después de funcionar en $2^{n/2}$ bloques con la misma llave de cifrado.

Para DES, n = 64, así que IEEE 802.16 puede proteger con seguridad 2^{32} bloques de 64 bits. Obteniéndose un rendimiento de procesamiento medio de 6.36 Mbps producidos por 2^{32} bloques de 64 bits en la mitad al día; mientras que el rendimiento de procesamiento medio de 2^{32} bloques de 64 bits en un plazo de siete días es de 455 que Kbps. Si estos datos exceden el ajuste del parámetro del tiempo de vida, la utilidad del esquema del cifrado se disminuye grandemente.

Tabla 2: Términos usado en la propuesta de autenticación PKM

TÉRMINO	DESCRIPCIÓN
SS-Random	Un valor impredecible, que tiene dos funciones: identificar el protocolo de los SS al momento de establecer la conexión y ser utilizado para generar la nueva llave de autenticación y además garantizar a las SS que se ha generado una llave nueva.
BS-Random	Un valor impredecible generado por la BS que mantiene las mismas dos funciones que el SS-Random pero para la BS.
pre-BS	Es la llave base BS a los SS. Esto es idéntico al estándar actual, sólo que con el valor agregado los pre-BS están siendo generados aleatoriamente (es decir, es impredeciblemente)
Cert (BS)	Un certificado digital X.509 que identifica el BS. Puede ser puesto en ejecución con el perfil usado para los SS, pero se utiliza solamente para las firmas en el par de llaves pública/privadas de la BS.
Sig (BS)	Excedente de la firma de BS los otros artículos en el mensaje 3.

Fuente: El autor (2006)

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

Con respecto a generar números al azar públicos, y asignándoselos a las BS y SS los participantes pueden identificar el una BS autorizada. Con el uso de un valor que contenga: la identidad certificada de la BS (BS's certified identity), la identidad certificada de la estación del suscriptor (SS's certified identity), el número generado aleatoriamente para esta entidad (BS's public random number for this instance) y el número generado aleatoriamente que identifique la SS (SS's public random number for this instante), los participantes podrían utilizar esta información para administrar sus llaves con las entidades autorizadas.

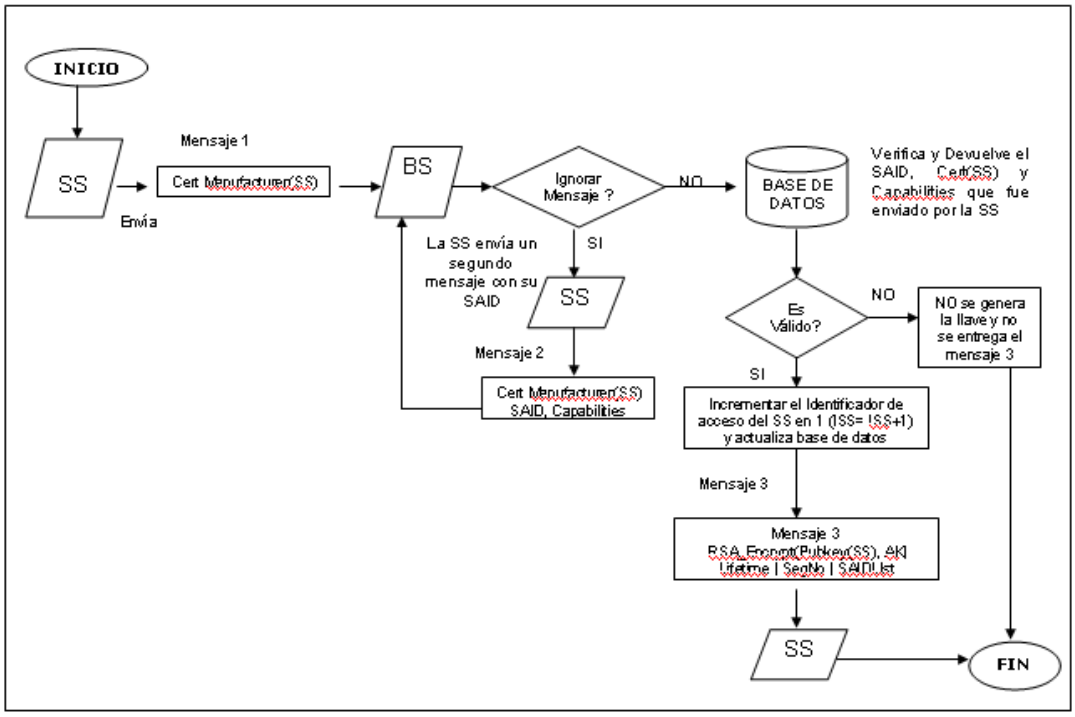

Figura. 3 Algoritmo de Autorización del PKM
Fuente: Autor (2006)

Con respecto a la otra debilidad que existe, referida a la privacidad y administración de AK. El protocolo PKM establece una asociación de seguridad de datos entre la Bs y SS.

Este proceso consiste en el intercambio de dos ó tres mensajes entre la SS y la BS. Cada BS utiliza el primer mensaje, el cual es opcional para solicitar y enviar la llave, la SS establece el protocolo y envía un segundo mensaje a la BS y ésta responde con un tercer mensaje y la nueva llave creada.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

Mensaje 1:
BS → SS: SeqNo | SAID | HMAC(1)
Mensaje 2:
SS → BS: SeqNo | SAID | HMAC(2)
Mensaje 3:
BS → SS: SeqNo | SAID | OldTEK |
NewTEK | HMAC (3)

Figura 4: Privacidad y Administración de Llaves
Fuente IEEE 802.16 Security (2004)

La BS nunca utiliza el mensaje 1 a menos que desee reenviar datos SA o crear un SA nuevo. Computando el valor HMAC (1), se permite que los SS detecten falsificaciones.

Los SS utilizan el mensaje 2 para solicitar parámetros del SA. Los SS deben tomar la lista de los protocolos autorizados (SAIDList) y con el valor del HMAC (1) válido enviado en el primer mensaje Los SS generan un segundo mensaje para cada dato SA. Cada HMAC (1) valido permite a la BS detectar falsificaciones.

Si el valor de HMAC (2) y el identificador SAID son valores válidos, la BS configura la SA creando un tercer mensaje. El valor de OldTEK reitera los parámetros activos del SA mientras que el valor del NewTEK predice los valores de parámetro que se utilizarán en el vencimiento del TEK actual.

El triple DES de BS cifra el TEKs viejo y nuevo bajo autorización SA KEK, usando modo electrónico del código (ECB). El estándar no impone ningún requisito de la generación de TEK. Computar el valor HMAC (3) con los valores del HMAC (1) y el HMAC (2) permitiría a las SS detectar falsificaciones.

Un valor de HMAC (2) válido autentica cada SS para cada BS. Solamente los SS correspondiente puede desempaquetar el AK enviado en el mensaje 3. Actualmente el protocolo no admite ninguna autentificación de BS a los SS; de hecho, con los correctos valores de HMAC (1) y HMAC (3) se afirman que solamente las entidades que sabe el valor de AK recibió por SS en el mensaje 3 podrá concatenar los mensajes completos del 1 al 3.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

Mensaje 1:
BS → SS: SeqNo | SAID | HMAC (1)
Mensaje 2:
SS → BS: SeqNo | SAID | HMAC (2)
Mensaje 3:
BS → SS: SeqNo | SAID | OldTEK |
NewTEK | HMAC (3) = (HMAC (1) y HAMC (2)

Figura 5: Propuesta de Privacidad y Administración de llaves
Fuente: El autor (2006)

Tabla 3: Términos usados en el intercambio del mensaje de la llave de autorización

Término	**Descripción**
SeqNo	La AK usada para el intercambio
SAID	La identificación datos SA que son creados o reenviados
HMAC(1)	El resumen de HMAC-SHA1 de la llave usada con el identificador de la conexión durante el downlink
HMAC(2)	El resumen de HMAC-SHA1 de la llave usada con el identificador de la conexión durante el uplink
OldTEK	Es un vector de la inicialización del TEK generado previamente, contiene el tiempo de vida restante (en segundos), y el número de serie para datos SA especificados por SAID (el número de serie de TEK es una cantidad 2-bit)
NewTEK	El vector de la inicialización del TEK siguiente, contiene el tiempo de vida (en segundos), y el número de serie para datos SA especificado por SAID.
HMAC(3)	El resumen HMAC-SHA1 de la llave usada, con el SAID, el OldTEK | NewTEK y la llave del downlink HMAC1 y del unplink HMAC 2

En este caso se recomienda computar al AK con los bits de ambas partes por ejemplo: AK = HMAC- SHA 1 (el cual contiene la llave de la BS). Incluyendo este valor en el cómputo de AK certificaría a los SS que sus llaves han sido generadas nuevamente.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

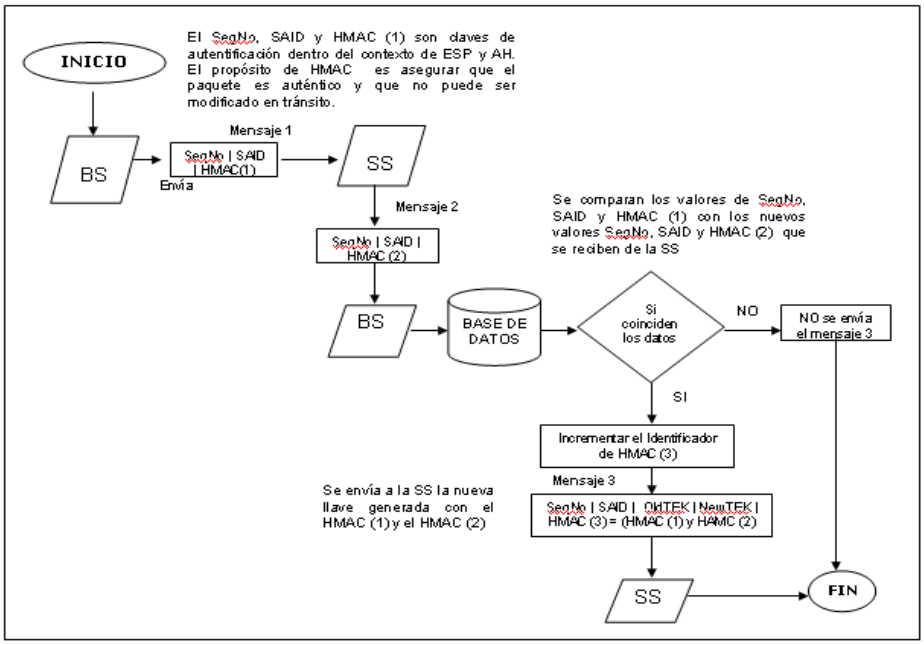

Figura 6: Algoritmo de Administración y Privacidad de Llaves
Fuente: El Autor (2006)

CONCLUSIONES

El estudio realizado permitió generar de manera puntual las siguientes conclusiones:

En cuanto al protocolo de seguridad de las redes inalámbricas específicamente el protocolo de privacidad y administración de llaves (PKM), se identificaron las siguientes características: [2]

- Autoriza a un SS registrado, y verificar la identidad de cada SS autorizado, a fin de evitar falsificaciones.
- Entrega a cada SS autorizado una llave encriptada y un mensaje de autenticación de la misma.
- Proporciona a cada SS autorizado información de las asociaciones de seguridad para poder obtener información de la llave.
- Cada SS debe estar en contacto periódico con la BS, a fin de verificar la autorización su identidad y así poder reutilizar la llave suministrada.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

- La Información de los certificados X.509 que se envían a la BS, contiene el certificado del fabricante de los SS, el cual es estrictamente informativo y cada BS válida puede ignorarlo, si así lo cree conveniente. Sin embargo, esto representa un método para que cada BS almacene los certificados de fabricantes de sus clientes.

El funcionamiento del algoritmo de seguridad en redes wimax, se pone en ejecución en la subcapa MAC; y su meta es proporcionar el control de acceso y la transmisión secreta de los datos. Las aplicaciones de seguridad de wimax incluyen cinco componentes; como son: asociaciones de la seguridad (SAs) las cuales mantienen el estado de la seguridad en una conexión; los datos SA, son los datos que se transmiten; autorización SA, es un secreto compartido entre un BS particular y los SS particulares; un certificado X.509 que identifica el fabricante de un dispositivo de IEEE 802.16, el cifrado para las administración de llaves y el protocolo de autorización de PKM que distribuye la llave a los SS acreditados.

Los ataques de seguridad más comunes en 802.16 operan generalmente a nivel MAC, y son la captura de tramas para modificarlas, reenviarlas y reutilizarlas causando vulnerables, entre una SS y BS válida.

Las principales vulnerabilidades del algoritmo de seguridad de las redes wimax están basadas en la necesidad de mecanismos de autenticidad de datos, carencia de definiciones explícitas en la autorización de los SA, significando que nunca recibe los mismos datos SAs que se envían, y la falta de autenticación mutua entre la BS y la SS.

En relación a esto, la autenticación en el algoritmo de seguridad de la redes 802.16x es una operación primordial, ya que por utilizar un medio inalámbrico donde se generan llaves públicas y privadas, que pueden ser atacadas en cualquier momento por persona no autorizadas. Con el fin de romper la integridad y confidencialidad de los datos. Por otra parte, la seguridad del protocolo no esta en el AK ni TEK de BS; si no, en la identificación debidamente autorizada de cada BS con la SS correspondiente durante el transcurso de la sesión.

Finalmente, se elaboró una propuesta con respecto a los problemas detectados específicamente en cuanto a la autenticación mutua y autorización de los SA, la cual consistió en asignar valores aleatorios a las identificaciones de los certificados digitales de la BS y la SS, lo cual mejora considerablemente la probabilidad de generar falsificaciones de BS autorizadas y SS autorizadas, ya que anteriormente los valores de identificación de cada entidad eran fijos, fácilmente detectados y reutilizados.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007

Asimismo el reducir el valor de tiempo de vida de la llave, trae como consecuencia menor probabilidad de ser atacada, porque en la actualidad el valor por defecto de este parámetro es de siete días, lo cual se considera un valor bastante riesgoso para los administradores de seguridad.

RECOMENDACIONES

Luego de finalizada la presente investigación y analizadas las conclusiones de la misma, se sugieren las siguientes recomendaciones.

Seguir realizando futuras investigaciones en al área de seguridad de la información, específicamente el cómo pueden ser protegidos los datos contra escritura y reutilizados. Los ataques de este tipo siguen siendo un desafío para los investigadores.

Se recomienda realizar pruebas al algoritmo de seguridad propuesto, a fin de verificar el desempeño y hacer mejoras de ser necesarias.

Evaluar el nivel de vulnerabilidad que pueda presentarse en el algoritmo original y en el propuesto a fin de verificar y comparar la integridad de los datos recibidos en cada uno de los escenarios descritos en la investigación.

REFERENCIAS BIBLIOGRÁFICAS

[1] But Bates Regis J. “Comunicaciones Inalámbricas de Banda Ancha” Departamento de Conmutación Ericsson España, S.A, pp. 211, 2003.

[2] David Johnston, Jesse Walter, White Paper: “Overview of IEEE 802.16 Security” Ieee Security & Privacy, 2004.

[3] Eugene Crozier , White Paper: WiMAX NLOS Features, WiMax Forum – Año 2004.

[4] IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, White Paper: “IEEE Standard for Conformance to IEEE 802.16”, June 2004.

[5] Luís Kaen, “Trabajo Final Integrador” Instituto Tecnológico de Buenos Aires, pp.51-53, 65-67, 2005

[6] IEEE Std. 802.16-2004, White Paper IEEE, 2004, IEEE Standard for Local and Metropolitan Area Networks, part 16, “Air Interface for Fixed Broadband Wireless Access Systems”.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 1 – Año 2007