UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

Algoritmos de cifrado para protocolos de autenticación en redes inalámbricas

Trabajo Monográfico

para obtener el grado de

Ingeniero en Redes

PRESENTA

Mario Rodrigo Herrera Canto

Supervisor de Monografía

MTI. Vladimir Veniamin Cabañas Victoria

MTI. Melissa Blanqueto Estrada

M.C. Javier Vázquez Castillo

Chetumal, Quintana Roo, México, Noviembre de 2009

UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

Trabajo monográfico bajo supervisión del Comité de Asesoría y aprobada como requisito parcial para obtener el grado de:

INGENIERO EN REDES

Comité de Trabajo Monográfico

Supervisor: M.T.I. Vladimir Veniamin Cabañas Victoria
Profesor – Investigador

Supervisor: M.T.I. Melissa Blanqueto Estrada
Profesor – Investigador

Supervisor: M.C. Javier Vázquez Castillo
Profesor – Investigador

Agradecimientos

A mis padres Ilmer Herrera Muñoz y Nelly Margarita Canto Lugo que siempre me apoyaron en la continuidad de mi carrera y en los momentos difíciles por los que atravesé durante mi periodo de estudios.

A mis hermanos Ilmer Herrera Canto y Jorge Carlos Herrera Canto que siempre estuvieron al pendiente en mis estudios y que en todo momento me daban consejos durante mi carrera.

A la Universidad de Quintana Roo por ser la escuela que me abrió las puertas para llevar una carrera tan exitosa.

Dedicatoria

A mi madre la Sra. Nelly Margarita Canto Lugo por ser la persona más importante de mi vida, la que ha estado conmigo en todo momento, dándome ánimos, orientándome, aconsejándome. Sin ella no hubiera podido lograr terminar mi carrera.

Resumen

El uso de las redes inalámbricas en la infraestructura de tecnologías de comunicación, se ha vuelto una pieza clave; proporcionan básicamente los mismos servicios de la red cableada, pero a diferencia de esta añade movilidad, independencia del cableado y la reducción de costos en la parte de instalación.

A través de este trabajo monográfico el tema principal fue la seguridad; en la cual los puntos más importantes que se resaltaron fueron los protocolos de estandarización (WEP, WAP y WAP2) y la criptografía simétrica.

En general este trabajo monográfico nos ofrece varias alternativas para mejorar la seguridad de una red inalámbrica que se desee implementar siendo WAP el protocolo más utilizado, sin embargo WPA2 a través del estudio que se realizó es el más viable a implementar. Por otra parte, existen otras herramientas importantes a considerar dado de que van de la mano con el funcionamiento de los protocolos de estandarización (WEP, WAP, y WAP2), entre ellas están: el vector de inicialización, los códigos MIC (Message Integrity Code) y MAC (Message Authentication Code), el protocolo TKIP (Temporal Key Integrity), el cifrado simétrico RC4, la criptografía simétrica, entre otros. Estas herramientas son relevantes para el buen funcionamiento de los estándares.

Contenido

Índice de Figuras y tablas

Índice de Tablas

Índice de Figuras

Capítulo 1

1.- Introducción

Las nuevas tecnologías de la información y las comunicaciones son la base fundamental de la infraestructura tecnológica de las organizaciones actuales., Las redes de datos o paquetes han simplificado distintas tareas en las organizaciones ya que por medio de ellas se ha podido compartir información, recursos (unidades de almacenamiento, unidades ópticas, impresoras, computadoras, servidores, etc.) y diversos tipos de servicios (como el acceso a Internet, correo electrónico, mensajería instantánea, de impresión, de voz sobre IP, etc.).

Las redes están ayudando a las organizaciones a hacer posible el mejor aprovechamiento de sus recursos tecnológicos, además, han permitido la reducción en costos y tiempo para las actividades relacionadas con su administración y operación.

Particularmente, las redes basadas en tecnologías inalámbricas hace tiempo que ofrecen un servicio equivalente de comunicación a las redes cableadas aunque los datos generalmente fluyen por las redes de cables a mayor velocidad. En algunas ocasiones, la velocidad en la transmisión resulta no ser importante, la necesidad apremiante es la movilidad y la independencia que proporcionan las redes inalámbricas.

Lo más llamativo de las redes inalámbricas es la potencialidad del concepto, la conexión de los distintos aspectos de la información con los de la transmisión las convierte en una opción atractiva e incluso insinúa la raíz de una revolución social, pues la gente puede comunicarse de formas nuevas, más flexibles, atractivas y entretenidas.

A diferencia de las redes convencionales el funcionamiento de las redes inalámbricas se basa en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo) en lugar de cableado estándar. La instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente como pasa con las redes cableadas, tampoco hay necesidad de agujerear las paredes para pasar cables ni de instalar porta cables o conectores; esto ha hecho que el uso de esta tecnología se extienda con rapidez.

El mayor atractivo de las redes inalámbricas es que ofrecen movilidad y una instalación sencilla, además permiten una fácil ampliación en la red; es decir podemos estar moviéndonos de un lugar a otro dentro y fuera de la organización y así poder comunicarnos con otros usuarios y establecer diferentes tipos de servicios (como envío de voz y datos, videoconferencias, compartir dispositivos, uso del Internet, etc.).

Entre las principales características de una red inalámbrica podemos mencionar varias como por ejemplo:

- Bajo costo en instalación y mantenimiento.
- La reducción de cableado y la consecuente facilidad de instalación.
- Permite conectar zonas a las cuales no se puede llegar utilizando cableado, ya sea por el costo o por la ubicación.
- Permite la transmisión de datos en tiempo real a usuarios, lo que proporciona grandes posibilidades del servicio y productividad.

2.- Objetivo general.

Determinar las principales características de los estándares de seguridad utilizados en los protocolos de autenticación para redes inalámbricas.

3.- Objetivos Específicos.

- Analizar los principales estándares para redes inalámbricas.
- Comparar los métodos para el aseguramiento de la privacidad en el estándar IEE 802.11.
- Realizar un estudio acerca del funcionamiento de cada uno de los protocolos de estandarización de seguridad que utilizan las redes inalámbricas.

4.- Justificación

Dar a conocer los diferentes algoritmos de encriptación de los mecanismos de autenticación del Estándar IEEE 802.11 mejora su comprensión y se pueden ofrecer soluciones más confiables en redes inalámbricas.

Capítulo 2

5.- Marco Teórico

5.1.- Introducción a los estándares IEEE802.11

La especificación IEEE 802.11 (ISO/IEC 8802-11) es un estándar internacional que define las características de una red de área local inalámbrica (WLAN). **Wi-Fi** (que significa "Fidelidad Inalámbrica", a veces incorrectamente abreviado WiFi) es el nombre de la certificación otorgada por la Wi-Fi alliance, anteriormente WECA (Wireless Ethernet Compatibility Alliance), grupo que garantiza la compatibilidad entre dispositivos que utilizan el estándar 802.11. Por el uso indebido de los términos (y por razones de mercadeo) el nombre del estándar se confunde con el nombre de la certificación. Una red Wi-Fi es en realidad una red que cumple con el estándar 802.11.

Con Wi-Fi se pueden crear redes de área local inalámbricas de alta velocidad siempre y cuando el equipo que se vaya a conectar no esté muy alejado del punto de acceso. En la práctica, Wi-Fi admite computadoras portátiles, equipos de escritorio, asistentes digitales personales (PDA) o cualquier otro tipo de dispositivo de alta velocidad con propiedades de conexión también de alta velocidad (11 Mbps o superior) dentro de un radio de varias docenas de metros en ambientes cerrados (de 20 a 50 metros en general) o dentro de un radio de cientos de metros al aire libre.

Los proveedores de Wi-Fi están comenzando a cubrir áreas con una gran concentración de usuarios (como estaciones de trenes, aeropuertos y hoteles) con redes inalámbricas. Estas áreas se denominan "**zonas locales de cobertura**".

(IEEE Standards Association, 2008).

5.1.1.- Descripción de los estándares 802.11

Estándar 802.11: El primero en existir. Llega a soportar de 1 a 2 Mbps y tiene una transmisión de 2.4 GHz. Su ventaja es que no utiliza licencia para este tipo de redes. Su desventaja son las posibles interferencias con las microondas, dispositivos Bluetooth y los teléfonos Dect (es una tecnología de teléfonos inalámbricos con más de 120 canales distintos de radios y una cobertura de hasta los 300 metros). En la actualidad existen algunos teléfonos celulares que utilizan esta tecnología.

(IEEE Standards Association, 2008).

Estándar 802.11a: Soporta un ancho de banda máximo de 54 Mbps, aunque normalmente en la práctica llega hasta los 30 Mbps El estándar 802.11a provee 8 canales de radio en la banda de frecuencia de 5 GHz. Este estándar presenta muchas desventajas como son: no resiste la inclemencia del tiempo, disminuye la calidad de la red y se hace incompatible con los otros estándares como son el 802.11b y 802.11g. No necesita licencia y utiliza una modulación OFDM (Orthogonal Frecuency Division Multiplexing).

(IEEE Standards Association, 2008).

Estándar 802.11b: Este estándar es el más utilizado actualmente. Ofrece un rendimiento total máximo de de 11 Mbps, aunque en la práctica funciona normalmente hasta 6 Mbps y tiene un alcance hasta los 300 metros en un espacio abierto. Utiliza el rango de frecuencias de 2.4 GHz con tres canales de radio disponibles. Ofrece compatibilidad con el estándar 802.11g.

(virusprot.com, 2006).

Estándar 802.11g: Aprobado a mediados del año 2003 y se popularizó rápidamente por su compatibilidad con el estándar 802.11b.El estándar 802.11g soporta velocidades de 20 a 54 Mbps, con una transmisión de 2.4 GHz. Funciona sin licencia, utiliza una modulación de DSSS (Direct Sequence Spread Spectrum) y OFDM (Orthogonal Frecuency Division Multiplexing). Lo que muchos desconocen es que al mezclar equipos del estándar 802.11b con equipos del estándar 802.11g la velocidad la fija el equipo más lento. Con el estándar 8022.11g se pueden utilizar 3 canales no superpuestos de los 11 disponibles.

(virusprot.com, 2006).

Estándar 802.11n: El nuevo estándar 802.11n promete una tasa de transferencia de hasta 100 Mbps, superando a todas sus antecesoras y pudiendo obtener hasta 5 veces más. Para alcanzar estas velocidades se utilizan una serie de antenas 4x4 con una transmisión de 40 MHz, siendo compatible con la de 20 MHz y los equipos Wi-Fi actuales. Esto es importante ya que existen algunos países actuales donde se prohíben los 40 MHz.

Uno de los problemas más recientes al momento de enviar datos es la disminución de la velocidad, ya que se ve afectada por todo el preámbulo que hay que seguir para el envío de los datos y esto genera una sobrecarga, el estándar 802.11n promete solucionarlo.

El estándar 802.11n utiliza la tecnología MIMO (Múltiples Entradas Múltiples salidas) que es más confiable que la Wi-Fi, especialmente para el envío de multimedia, esperando superar velocidades de conexión Ethernet.

(IEEE Standards Association, 2008).

5.1.2.- Complementos de los estándares 802.11, 802.11b, 802.11g y 802.11n

Estándar 802.11c: Combinación del estándar 802.11 y 802.11d. No ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos)

(piurawifi.com, 2008).

Estándar 802.11d: Complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.

(piurawifi.com, 2008).

Estándar 802.11e: Está destinado a mejorar la calidad del servicio en el nivel de la *capa de enlace de datos*. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo.

(piurawifi.com, 2008).

Estándar 802.11f: El 802.11f es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.

(piurawifi.com, 2008).

Estándar 802.11h: El estándar 802.11h tiene por objeto unir el estándar 802.11 con el estándar europeo (HiperLAN 2, de ahí la h de 802.11h) y cumplir con las

regulaciones europeas relacionadas con el uso de las frecuencias y el rendimiento energético.

(piurawifi.com, 2008).

Estándar 802.11i: El estándar *802.11i* está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el AES (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.

(piurawifi.com, 2008).

Estándar 802.11r: El estándar *802.11r* se elaboró para que pueda usar señales infrarrojas. Este estándar se ha vuelto tecnológicamente obsoleto.

(piurawifi.com, 2008).

Estándar 802.11j: El estándar *802.11j* es para la regulación japonesa lo que el 802.11h es para la regulación europea.

(piurawifi.com, 2008).

Estándar	Velocidad	Frecuencia de Operación
802.11	2 Mbps	2.4 GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	100 Mbps	40 MHz

Tabla 1.- Tabla comparativa de los principales estándares 802.11.

Es necesario mencionar los elementos básicos y características de las redes inalámbricas para poder tener un mejor entendimiento de los algoritmos de cifrado utilizados en los principales estándares (WEP, WAP y WAP2).

5.2.- Puntos débiles en Redes Inalámbricas

La instalación de una Red Inalámbrica presenta diversos desafíos de seguridad y como sucede muchas veces, varias de sus ventajas y funcionalidades se convierten en puntos débiles muy difíciles de proteger:

Amenazas a solucionar en Redes Inalámbricas:

- Todos los que estén en un radio de 100 ms. aproximadamente son intrusos potenciales.
- La información se transmite por el aire y, por lo tanto, puede ser "vista" por cualquiera que esté en el radio de 100 ms.

- Nuestros usuarios pueden conectarse equivocadamente (o voluntariamente) a redes que se encuentren abiertas en el radio de 100 ms y esto puede ser muy peligroso para la seguridad de nuestra organización.
- Cualquier "vecino" puede captar los login y las contraseñas cuando los usuarios intentan conectarse.

(virusprot.com, 2006)**.**

5.3.- Elementos básicos de una Red Inalámbrica.

Antes de entrar a fondo sobre los temas posteriores en seguridad en Redes Inalámbricas (Necesidades, problemas y mecanismos de seguridad) se comentarán brevemente los elementos básicos que se manejan en las redes inalámbricas con la finalidad de entender con mayor claridad los temas posteriores.

A) Punto de Acceso (Access Point)

Es un dispositivo inalámbrico central de una Red Inalámbrica WI-FI (Wireless) que por medio de ondas de radio frecuencia (RF) recibe información de diferentes dispositivos móviles y la transmite a través de cable al servidor de la Red cableada.

El estándar 802.11 es bastante ambiguo y no define con claridad todas las funciones que debería realizar un Punto de Acceso y sólo lo describe de una manera muy superficial. Esto dio lugar a que cada fabricante lo diseñara según su criterio y, por lo tanto existen en el mercado decenas de Puntos de Acceso con características y funcionalidades muy dispares.

(virusprot.com, 2006).

B) Dispositivos Móviles

Los hay muy diversos como computadoras portátiles (Notebooks), PDAs, teléfonos celulares. Estos tienen instalados tarjetas PCMCIA o dispositivos USB con capacidades WI-FI y pueden por lo tanto, reciben o envían información a los Puntos de Acceso o a otros dispositivos de manera inalámbrica (RF). En la actualidad ya abundan los que tienen la tecnología WI-FI incorporada en el procesador (Intel, Atheros, etc.) y por lo tanto no necesitan de agregados USB o PCMCIAs.

(virusprot.com, 2006).

C) Dispositivos Fijos

Los computadores de sobremesa o fijos (desktops), las impresoras, cámaras de vigilancia, etc., también pueden incorporar tecnología WI-FI y, por lo tanto, ser parte de una Red Inalámbrica.

(virusprot.com, 2006).

D) Otros elementos

También existen amplificadores y antenas que se pueden agregar, según las necesidades, a instalaciones WI-FI y sirven para direccionar y mejorar las señales de RF transmitidas.

(virusprot.com, 2006).

5.4.- Tipos de Redes Inalámbricas WI-FI

Las Redes Inalámbricas WI-FI se pueden conectar, básicamente, de 2 maneras muy diferentes:

A) Red WI-FI de Infraestructura

Esta arquitectura se basa en 2 elementos: uno o más Puntos de Acceso y Estaciones Cliente (fijas o móviles) que se conectan al servidor a través del Punto de Acceso como se observa en la figura 1.

(virusprot.com, 2006).

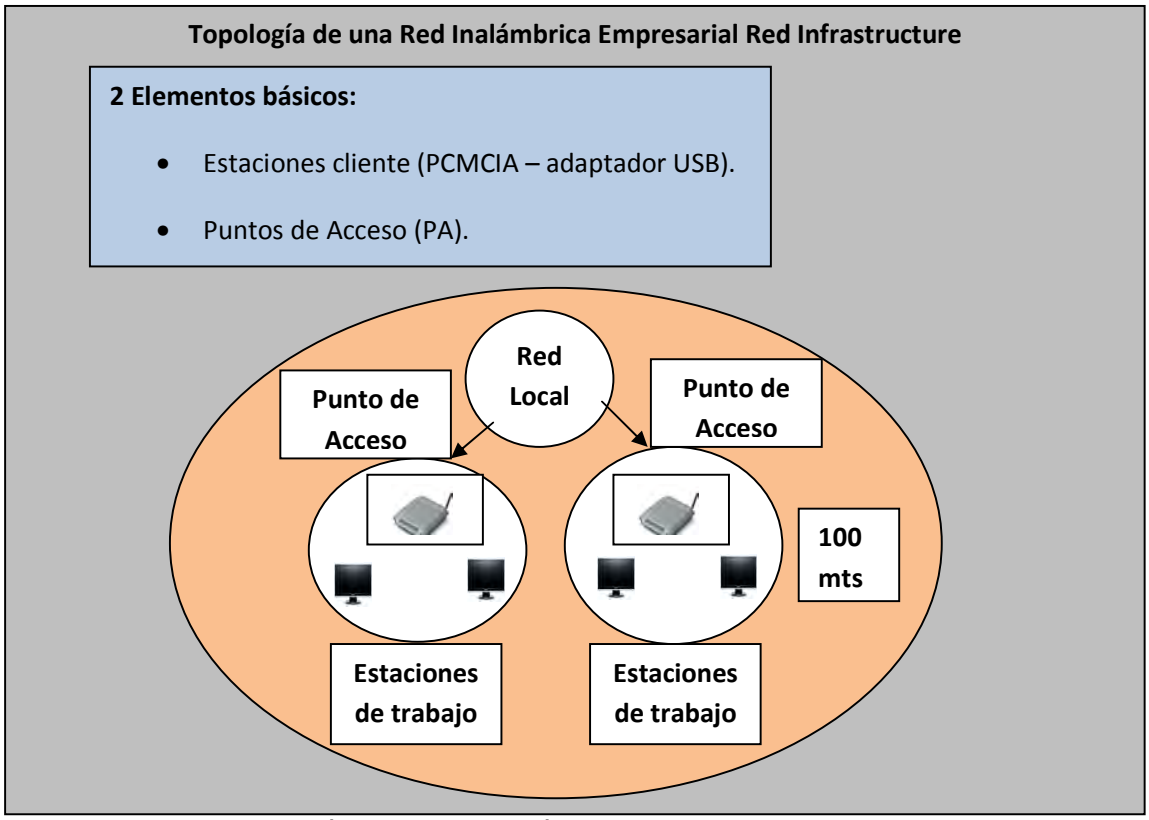

Figura 1.- Topología de una Red Inalámbrica Empresarial Red Infraestructura.

B) Red WIFI Ad-Hoc

Esta arquitectura se basa en un sólo elemento: Estaciones cliente (fijas o móviles). Éstas se conectan entre sí para intercambiar información de manera inalámbrica como se observa en la figura 2.

(virusprot.com, 2006).

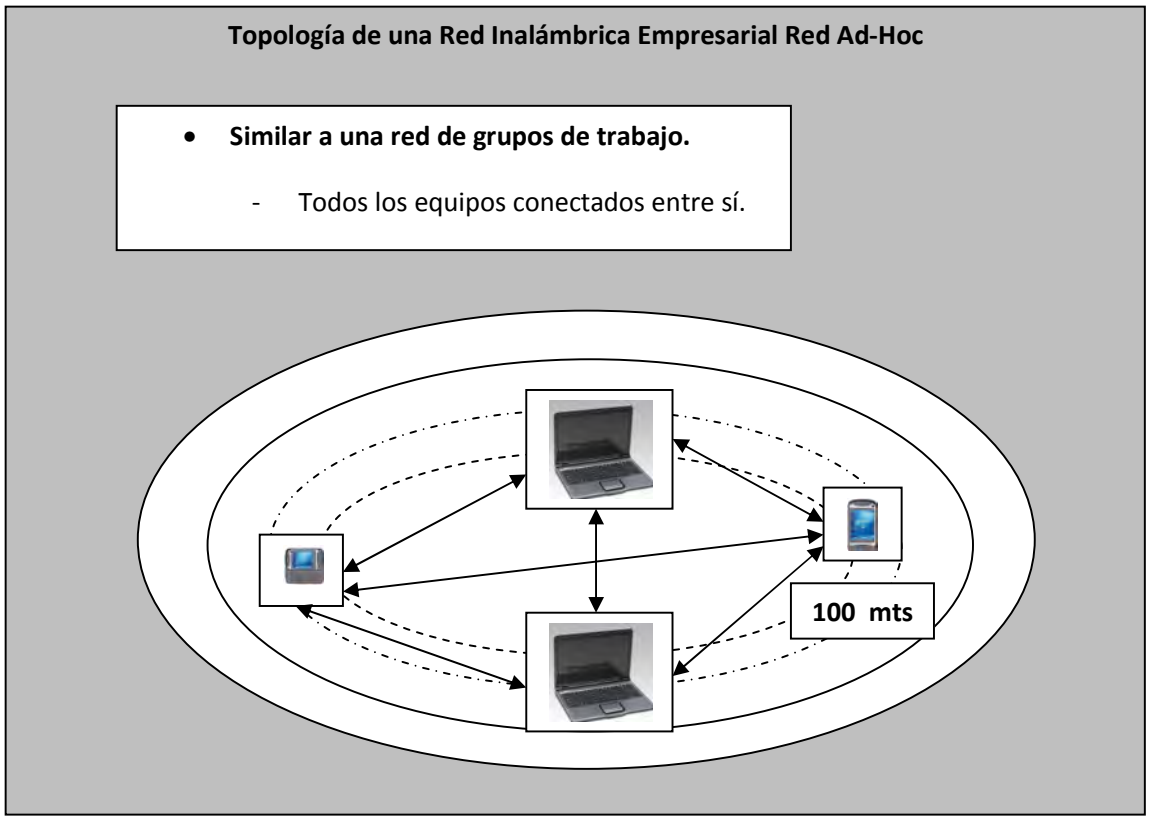

Figura 2.- Topología de una Red Inalámbrica Empresarial Red Ad-Hoc.

5.5.- Identificación de Puntos de Acceso y Estaciones WIFI en Redes Inalámbricas

De acuerdo a la identificación de puntos de acceso y estaciones WIFI se realiza a través de:

1) Direcciones MAC (MAC – Media Access Control – Address): Es un número de 48 bits asignado por el fabricante a los dispositivos inalámbricos: Puntos de Acceso, tarjetas WI-FI, USBs WI-FI, etc. Aunque está grabado en el hardware, se puede modificar por software.

2) SSID (Service Set Identifier): Cada AP tiene uno de hasta 32 bytes. Sirve para identificar a la red inalámbrica.

3) IBSS (Independent Basic Service Set): Identifica a las redes Ad-Hoc pues hay que recordar que en éstas no hay Punto de Acceso.

(virusprot.com, 2006).

5.6. Necesidad de seguridad en comunicaciones Inalámbricas

Las redes inalámbricas, nos libran de la dependencia que impone el cable a permanecer en un lugar fijo sin poder movernos apenas, y a realizar la conexión bien a nuestra red local o a Internet, solamente en aquellos lugares donde haya una toma de conexión, de modo que esta característica se convierte en su principal ventaja, y a su vez en su principal problema en lo que a la seguridad se refiere.

En primer lugar, se debe considerar que en una WLAN todos las computadoras radian información de forma interrumpida, e incluso anuncian su presencia a cualquiera que pase dentro de su radio de alcance, este hecho hace que sea muy fácil espiar la red, por lo tanto, nos encontramos con el problema de que a

diferencia de red cableada (en la que el intruso necesita un acceso físico al edificio u oficina donde se encuentra la red interna que trata de asaltar), las señales de radio utilizadas por los dispositivos inalámbricos navegan con libertad a través del aire, al alcance de aquel que esté dispuesto a interceptarlas.

Debido a que las redes inalámbricas no ofrecen la misma seguridad que las redes tradicionales y son más vulnerables a los ataques informáticos se han desarrollado muchas estrategias para intentar evitar estos problemas, la mayoría basadas principalmente en el cifrado de las comunicaciones (WEP, WPA). Diversos estudios muestran la debilidad de estos mecanismos de seguridad. También existen otros tipos de medidas de protección como el filtrado de direcciones MAC, o bien medidas de protección más robustas basadas en el estándar 802.1x que permiten la autenticación y autorización de usuarios, a través del protocolo extendido de autorización (EAP). Todas estas medidas de protección, y algunas adicionales se detallarán más adelante analizando las ventajas e inconvenientes de cada una.

(taringa.net, 2008).

Capítulo 3

6.- Desarrollo

6.1.- Protocolos de estandarización

6.1.1.- WEP (Wired Equivalent Privace)

En una red inalámbrica existe una mayor necesidad con respecto a otros tipos de redes, de que la información transmitida por radio sea protegida frente a la pérdida de confidencialidad; vista la facilidad con la que un intruso puede capturar la información intercambiada entre las estaciones que forman la WLAN en cuestión. Es por ello, que hay que hacer uso de la encriptación de la información, y para ello se describirá y analizará el sistema de encriptación WEP, como forma de protección de los datos, porque este protocolo provee de un mecanismo de cifrado débil, siendo considerablemente sencillo comprometer la clave de encriptación.

(TECH-FAQ, 2008).

Definición

WEP Es un cifrado simétrico de flujo con un tamaño de clave arbitraria RC4 (creada por Ron Rivest de RSA Security en 1987) con cifrado de flujo de 40 o 104 bits, claves de 24 bits y un vector de inicialización.

(TECH-FAQ, 2008)**.**

Objetivo de WEP

El objetivo de utilizar el vector de inicialización (IV*)* es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave.

Como es lógico, se debe conocer tanto la clave secreta como el vector de inicialización (IV*)*. Lo primero es conocido puesto que está almacenado en la configuración de cada elemento de red. El vector de inicialización (IV*)* en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Al viajar el vector de inicialización (IV*)* en cada trama es sencillo de interceptar por un posible atacante.

La mayoría de los dispositivos de 802.11 WEP permiten que se introduzcan claves utilizando una contraseña ASCII o en formato hexadecimal. La conversión entre estos dos formatos es un estándar de la industria, que es compartida por casi todos los proveedores de equipo de 802.11.

(virusprot.com, 2008).

Funcionamiento

• Existe una clave secreta compartida entre emisor y receptor que puede valer 40 o 128 bits.

• A la trama que queremos enviar, se le aplica un código de integridad denominado “Integrity Check Value” (ICV) mediante el algoritmo CRC-32. Este código va a actuar como “checksum”, para asegurar que la recepción se corresponda exactamente con lo que envió el emisor, es decir, que la trama no haya sido modificada durante su trayecto.

• Lo siguiente es concatenar la clave secreta con un número aleatorio llamado vector de inicialización, (IV) que tendrá una longitud de 24 bits. Si se utilizará siempre una misma clave para cifrar las tramas entonces, dos tramas iguales darían lugar a tramas cifradas similares. Esto ayudaría a cualquier intruso, a descifrar los datos sin conocer la clave secreta, por ello, este vector irá cambiando en el envío de cada trama.

• El algoritmo de encriptación RC4 dispondrá de dos entradas; por una parte la clave secreta + IV (semilla) y por otra parte los datos modificados con el código de integridad (CRC-32). Dicho algoritmo, basándose en un proceso de XOR bit por bit generará la trama cifrada.

• Se enviará al receptor la trama cifrada (datos + CRC) junto con IV e ICV sin cifrar.

• El receptor utilizará la clave secreta que tiene compartida con el emisor, junto con el IV enviado para generar la semilla. Por medio de la semilla calculada y el algoritmo RC4 se generará la trama en claro junto con el ICV.

• Por último, el receptor calculará el ICV de los datos recibidos, y lo comparará con el ICV recibido, y si no concuerdan, descartará tanto a la trama como al emisor de la misma.

La siguiente figura nos mostrará detalladamente el modo de transmisión de algoritmo WEP:

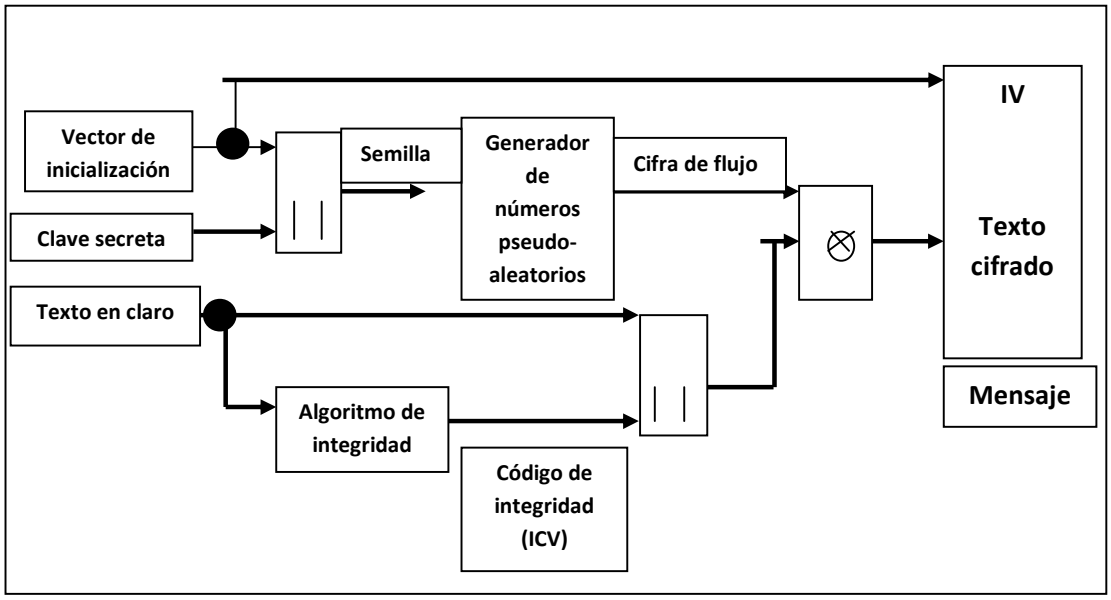

Figura 3.- Transmisión de algoritmo WEP.

(virusprot.com, 2008).

Algoritmo utilizado

La Privacidad Equivalente a Cableado *WEP* (por sus siglas en inglés) es el algoritmo de cifrado estándar incluido en el 802.11 (Wi-Fi). El cifrado en RC4 con claves (seed) cuando usa 64 bits, están conformados por 24 bits correspondientes al vector de inicialización, más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente.

El vector de inicialización (IV*)* por sus siglas en inglés), en cambio, es generado dinámicamente y debería ser diferente para cada trama.

(virusprot.com, 2008).

Características

• Forma parte de la especificación del estándar 802.11.

• Opera en el nivel 2 del modelo OSI (subcapa MAC).

• Soportado por una amplia mayoría de fabricantes de soluciones inalámbricas.

• Utiliza el algoritmo de encriptación RC4.

(virusprot.com, 2008)**.**

Debilidades

- La clave secreta compartida entre las estaciones que intercambian tráfico tiene varios problemas:

  1. Utilización de clave estática, no modificada.
  2. La modificación de la clave ha de hacerse de forma manual.
  3. El password del administrador es directamente la clave. Por ello la clave puede ser descubierta por ataques de diccionario (método que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario).
  4. Todas las estaciones que comparten PA (Punto de Acceso) utilizan la misma clave.
  5. Por todas estas cosas resulta bastante sencillo romper la clave por fuerza bruta cuando se acumulan grandes cantidades de tráfico cifradas con la misma clave.

- El IV utilizado es de longitud insuficiente (24 bits). El número total de vectores de inicialización será entonces 224. Esto quiere decir, que en una red con alto tráfico (recordando que se utiliza un IV distinto por cada trama enviada) el espacio de IV distintos se agotará en un plazo relativamente corto de tiempo, de modo que la captura de dos tramas con un mismo IV no será demasiado improbable. Esto hace que con

métodos estadísticos, se pueda obtener el texto en claro de una trama y con él, aplicando el algoritmo RC4, se pueda llegar a descubrir la clave secreta entre las dos estaciones.

- También existen problemas con el código de integridad (ICV). Dicho código, sirve para solucionar problemas del medio de transmisión, pero no permiten evitar modificaciones maliciosas, cambiando ciertos bits de datos y calculando los cambios del CRC-32 para mantenerlo coherente.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso, el estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red.

Esto genera varios inconvenientes, por un lado, la clave está almacenada en todas las estaciones aumentando las posibilidades de que sea comprometida, y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

(virusprot.com, 2008).

6.1.2. - WPA (Wi-Fi Protected Access)

Debido a los problemas que presenta el estándar WEP, en la cual constituye un mecanismo débil de cifrado, pero que sin embargo puede constituir una solución adecuada para redes domésticas o de pequeñas oficinas, debemos habilitar mecanismos de protección más robustos en entornos que precisen protección profesional. Por ello se ha desarrollado el estándar WPA, para

subsanar las debilidades de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autentificación.

(TECH-FAQ, 2008).

Definición

Es un estándar de la Wi-Fi Alliance. WPA fue creado en respuesta a las serias debilidades de otros protocolos como WEP (Wired Equivalent Privacy). Implementa la mayoría de lo que conforma el estándar IEEE 802.11i y fue diseñado para funcionar con todos los dispositivos para redes inalámbricas, excepto los puntos de acceso de primera generación.

WPA fue creado por el grupo industrial y comercial Alianza Wi-Fi, dueños de la marca registrada Wi-Fi y certificadores de los dispositivos que ostenten dicho nombre.

(TECH-FAQ, 2008).

Objetivos

Además de proporcionar autenticación y cifrado, WPA tiene como objetivo proporciona mejor integridad de la carga útil. La verificación de redundancia cíclica (CRC o Cyclic Redundancy Check) utilizada en WEP es insegura porque permite alterar la carga útil y actualizar el mensaje de verificación de redundancia cíclica sin necesidad de conocer la clave WEP.

En cambio WPA utiliza un Código de Integridad de Mensaje (MIC o Message Integrity Code) que es en realidad un algoritmo denominado *«Michael»*, que fue el más fuerte que se pudo utilizar con dispositivos antiguos para redes inalámbricas a fin de no dejar obsoletos a éstos. El Código de Integridad de Mensaje de WPA incluye un mecanismo que contrarresta los intentos de

ataque para vulnerar el protocolo TKIP (Temporal Key Integrity Protocol) y bloques temporales.

(Universidad de Buenos Aires (Departamento de computación), 2006).

Funcionamiento

Desde el punto de vista del funcionamiento, WPA incorpora por un lado mecanismos definidos dentro del estándar 802.11i como por ejemplo en lo que respecta al proceso de autenticación y por otro lado hace uso del mismo algoritmo de confidencialidad que utiliza WEP, aunque le incorpora procesos adicionales para subsanar las deficiencias de WEP.

Con respecto a Autenticación, WPA soporta dos modos de operación:

1. Enterprise.
2. Pre-shared Key (PSK).

(Universidad de Buenos Aires (Departamento de computación), 2006).

Modo Enterprise

En el modo Enterprise se opera contra un servidor de Autenticación (por ejemplo un servidor RADIUS) para el establecimiento de la autenticación. De esta manera se establece un proceso de autenticación centralizado.

Este proceso de autenticación se basa en el estándar definido dentro de la norma 802.1X. La definición y abordaje sobre este último estándar excede el alcance de este informe pero a grandes rasgos el mismo tiene por objetivo establecer un contexto seguro de comunicación, definiendo las siguientes fases:

- Acuerdo sobre política de seguridad entre ambas partes.

- Autenticación de Terminal (certificados, pregunta secreta, etc.)

- Derivación y distribución de claves que serán utilizadas dentro de la conexión (claves de sesión, claves de cifrado de paquetes, claves de encriptación de mensajes multicast, etc.). Las mismas están basadas en una estructura jerárquica.

La norma 802.1X está basada en el framework de autenticación Extensible Authentication Protocol (EAP). Para poder certificar un producto como WPA o WPA2 el dispositivo debe proveer los siguientes métodos:

- EAP-TLS: Fue el primero en ser certificado, y es considerado uno de los más seguros. Requiere certificados por parte del Cliente y del Servidor (es decir, se necesita de una infraestructura de claves). Hasta abril de 2005, los distintos fabricantes sólo necesitaban soportar éste método de autenticación para certificar WPA o WPA2.

- EAP-TTLS: EAP-Tunneled Transport Layer Security utiliza certificados sólo del lado del servidor.

- PEAPv0 / EAP-MSCHAPv2: Protected EAP / Microsoft Challenge Handshake Authentication Protocol. Diseñado en forma conjunta por Microsoft, Apple y RSA. Similar a TTLS. Es el más utilizado.

- PEAPv1 / EAP-GTC: Creado por Cisco como alternativa a PEAPv0. No posee soporte nativo en sistemas Windows.

- EAP-SIM: Utiliza el Subscriber Identity Module (SIM) de los celulares GSM para proveer autenticación a una WLAN.

(Universidad de Buenos Aires (Departamento de computación), 2006).

Modo PSK (Pre Shared Key)

En el modo Pre Shared Key no se opera con un servidor de autenticación sino que utiliza la técnica de "secreto compartido" para autenticarse con el servidor. Cabe aclarar que en este modo también se realizan las fases mencionadas en el modo anterior como el acuerdo de política de seguridad, derivación de jerarquía de claves, etc.

Con respecto a la confidencialidad, WPA sigue haciendo uso del algoritmo RC4 como mecanismo de cifrado en sus comunicaciones. Esto a priori es preocupante, puesto que ya se ha visto que una de las debilidades más fuertes de WEP es la utilización del RC4.

Una de las razones por las que se sigue utilizando este algoritmo en WPA es que uno de los objetivos de este estándar era evitar que se realice un cambio de hardware forzoso. Por esta razón se hace uso del mismo algoritmo que se estaba utilizando en WEP, pero incorporando mejoras en el mismo.

Esos avances e incorporaciones en la forma de utilizar RC4 dentro de WPA se denominan TKIP (Temporal Key Integrity Protocol). Este nuevo protocolo incorpora nuevas técnicas tales como:

- **Extiende el tamaño del vector de inicialización utilizado en el algoritmo RC4**. En WEP el tamaño de los IV es de 24 bits, que resultan en 16.777.216 valores diferentes, algo totalmente inaceptable cuando se sabe que una red con un volumen razonable será necesario reutilizar los IV. Por esa razón, en WPA se decidió extender el tamaño del IV a 48 bits, dando un espacio de valores más grande.

  (Universidad de Buenos Aires (Departamento de computación), 2006).

- **Se incorporan nuevas reglas para la selección de los IV.** En WEP no hay reglas para evitarla reutilización de los IV y por esa razón la mayoría de los fabricantes elegían, en el momento de seleccionar un IV, uno al azar. Esto en conjunto con el corto tamaño de los mismos hacía que la probabilidad de que un IV se repitiera sea grande. En cambio en WPA se especifican reglas para la asignación de los IV.

  En particular se define iniciar en el número 1 e incrementar en uno con cada paquete que se transmite. De esta forma la reutilización del IV es mucho más espaciada, sobre todo combinando esto con el incremento del tamaño del IV a48 bits.

  Esta política de incremento secuencial de IV trae un beneficio adicional que se basa en que el mismo es utilizado como contador de paquetes recibidos y por ende se puede utilizar para evitar el tipo de ataque denominado “replay attack”.

  (Universidad de Buenos Aires (Departamento de computación), 2006).

- **Integridad del Mensaje**. Incorpora un protocolo de integridad de los mensajes para prevenir, que puede ser producido en software sobre

microprocesadores lentos. Se modifica el usado por WEP (CRC-32) por el Message Integrity Code (MIC). El MIC en WPA está basado en un algoritmo denominado Michael, que realiza un hash (función o método para generar claves o llaves que representen de manera casi unívoca a un archivo, documento o registro) unidireccional e involucra la clave del paquete, por lo que no es susceptible a ataques como el CRC-32.

(Universidad de Buenos Aires (Departamento de computación), 2006).

- **Clave de Paquetes**. Se establece que las claves de encriptación de los paquetes son temporales. Es decir que cada paquete transmitido es encriptado utilizando una clave diferente, derivada de la jerarquía de claves generada en el proceso de autenticación mencionado anteriormente.

  (Universidad de Buenos Aires (Departamento de computación), 2006).

- **Mecanismo de generación y distribución de claves**. La seguridad de la conexión se basa en gran medida en las claves secretas. En WPA y WPA2, cada clave tiene una vida determinada y la seguridad global se garantiza utilizando un conjunto de varias claves organizadas según una jerarquía. Cuando se establece un contexto de seguridad tras la autenticación exitosa, se crean claves temporales de sesión.

  El proceso de generación de esta jerarquía involucra varios intercambios y negociaciones entre partes, así como también procesos de derivación de claves en función de otras. El proceso de derivación es un proceso bastante complejo pero a modo de ejemplo describiremos algunos procesos y claves que se generan**:**

- 4-Way Handshake para la derivación de la PTK (Pairwise Transient Key) y GTK (Group TransientKey).
- Group Key Handshake para la renovación de GTK.

(Universidad de Buenos Aires (Departamento de computación), 2006).
En la figura 4 se muestran tres llaves móviles temporales de sesión que están agrupadas en el grupo llamado pareja de llave (Pairwise Key), colocando las tres llaves de manera ordenada (key 1, key 2 y key 3).

Posteriormente en el siguiente ejemplo de la misma figura nos muestra las misma tres llaves móviles como en el ejemplo anterior; pero a diferencia de este los va agrupar en el grupo llamado llave de grupo (Group Key); de tal manera que a través de generación y distribución de llaves los va a reagrupar y compactar a través de una llave creada con el nombre de Key G con la finalidad de que las llaves sean más difíciles de descifrar.

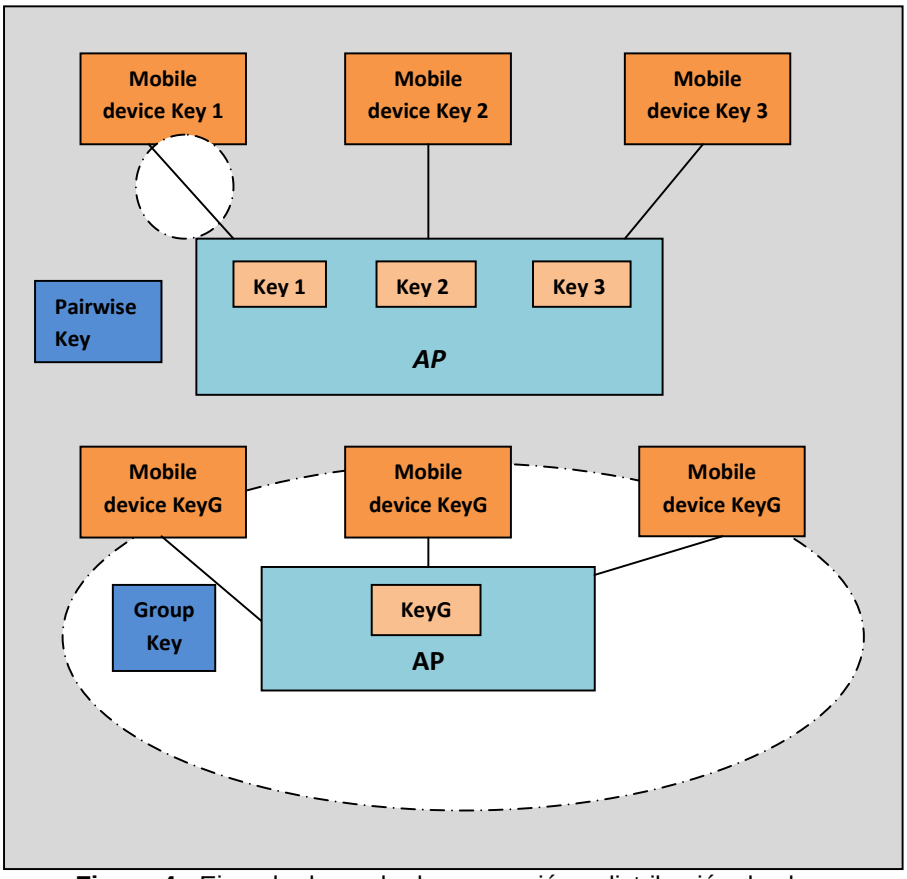

Figura 4.- Ejemplo de modo de generación y distribución de claves.

(Scribd, 2009).

La derivación de la clave PMK (Pairwise Master Key) depende del método de autenticación:

- Si se utiliza una PSK (Pre-Shared Key), PMK = PSK. La PSK es generada desde una passphrase (de 8 a 63 caracteres) o una cadena de 256 bits y proporciona una solución para redes domésticas o pequeñas empresas que no tienen servidor de autenticación.

- Si se utiliza un servidor de autenticación, la PMK es derivada de la MK de autenticación 802.1X.

La PMK en sí misma no se utiliza nunca para la encriptación o la comprobación de integridad. Al contrario, se utiliza para generar dos claves de encriptación temporales: la PTK (Pairwise Transient Key) para el tráfico unicast y la GTK (Group Transient Key) para el tráfico mulitcast.

La PTK consiste de varias claves temporales dedicadas:

- KCK (Key Confirmation Key – 128 bits): Clave para la autenticación de mensajes (MIC) durante el 4-Way Handshake y el Group Key Handshake.

- KEK (Key Encryption Key – 128 bits): Clave para asegurar la confidencialidad de los datos durante el 4-Way Handshake y el Group Key Handshake.

- TK (Temporary Key – 128 bits): Clave para encriptación de datos (usada por TKIP o CCMP en WPA2).

- TMK (Temporary MIC Key – 2x64 bits): Clave para la autenticación de datos (usada sólo por Michael con TKIP en WPA). Se usa una clave dedicada para cada lado de la comunicación.

Esto se resume en la figura 5.

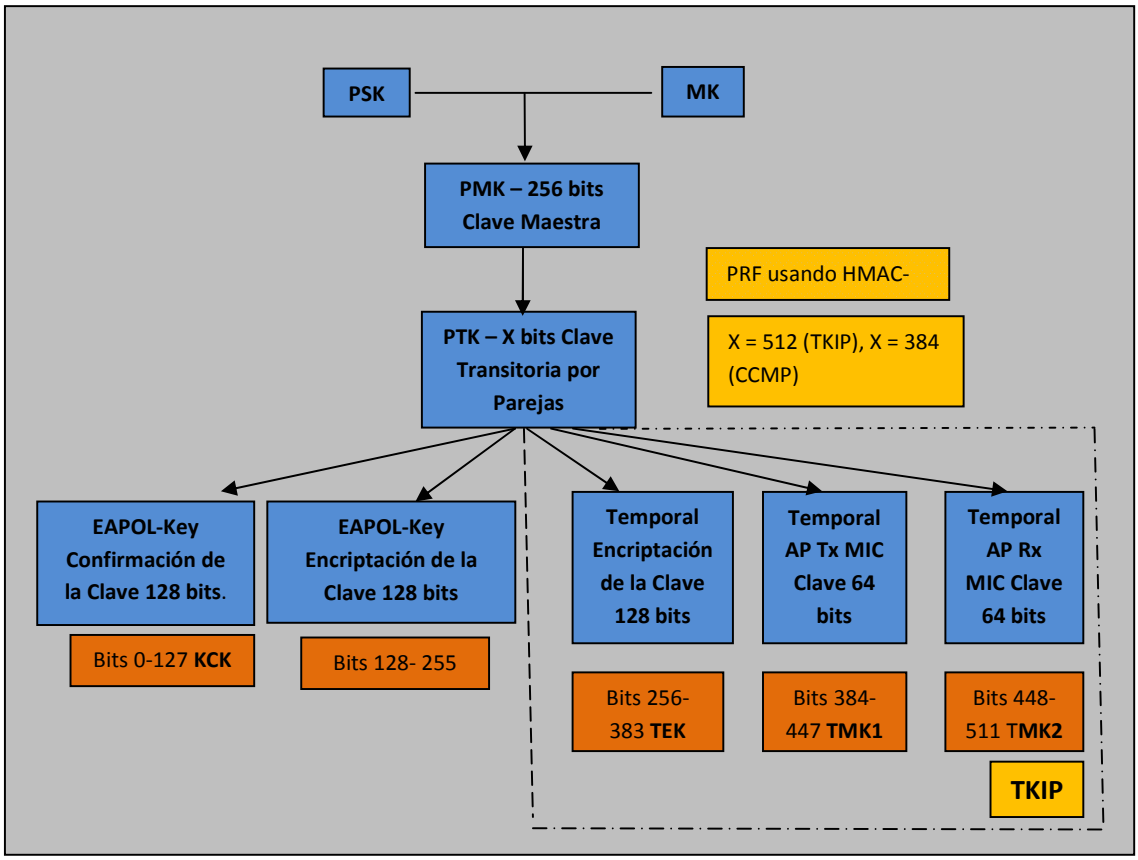

Figura 5.- Jerarquía de claves por parejas.(Scribd, 2009)**.**

El 4 –Way Handshake iniciado por el punto de acceso, hace posible:

- Confirmar que el cliente conoce PMK.
- Derivar una PTK nueva.
- Instalar claves de encriptación e integridad.
- Encriptar el transporte de la GTK.
- Confirmar la sesión de la suite de cifrado.

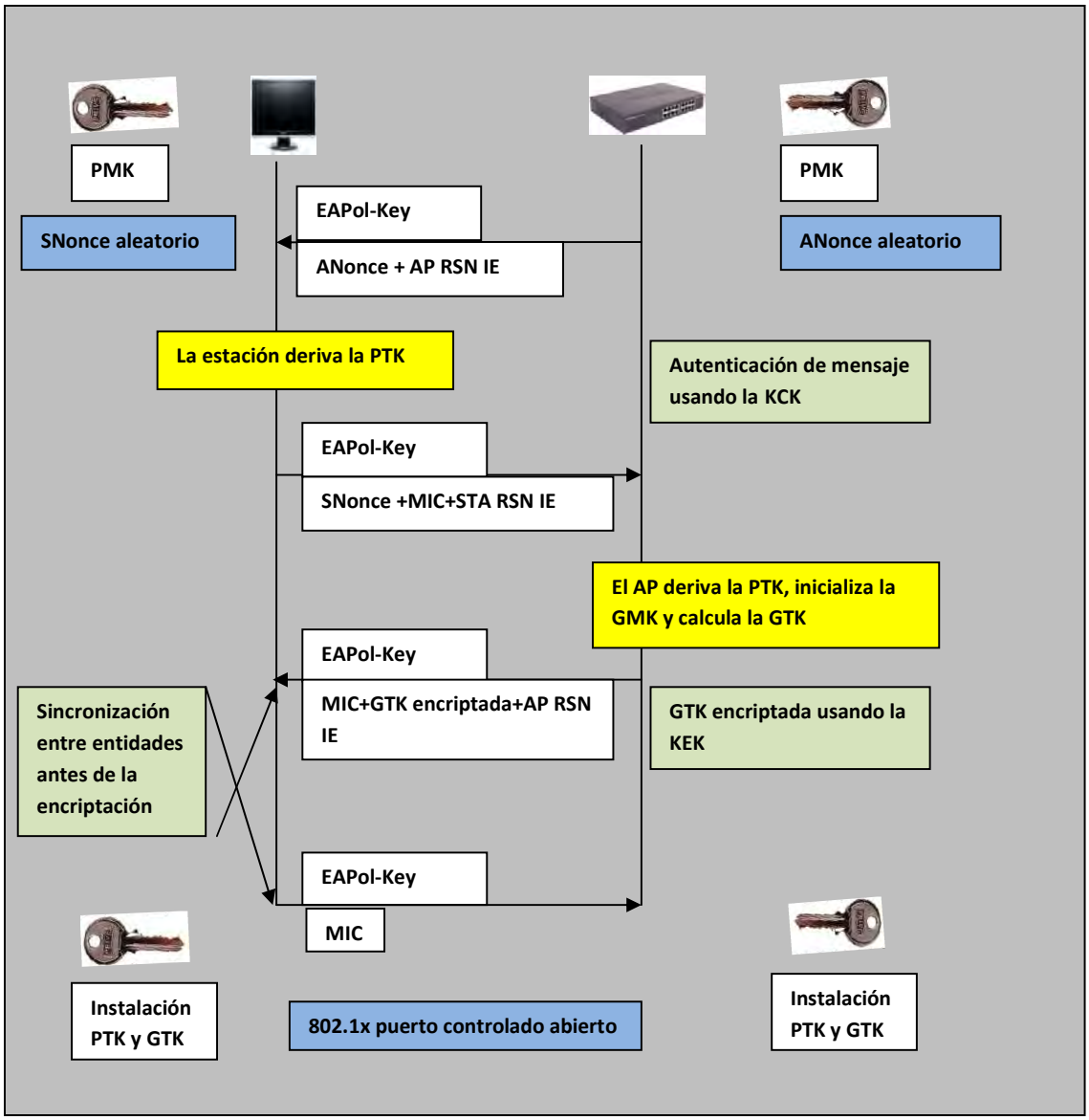

Figura 6 .- 4-Way Handshake. (Scribd, 2009)**.**

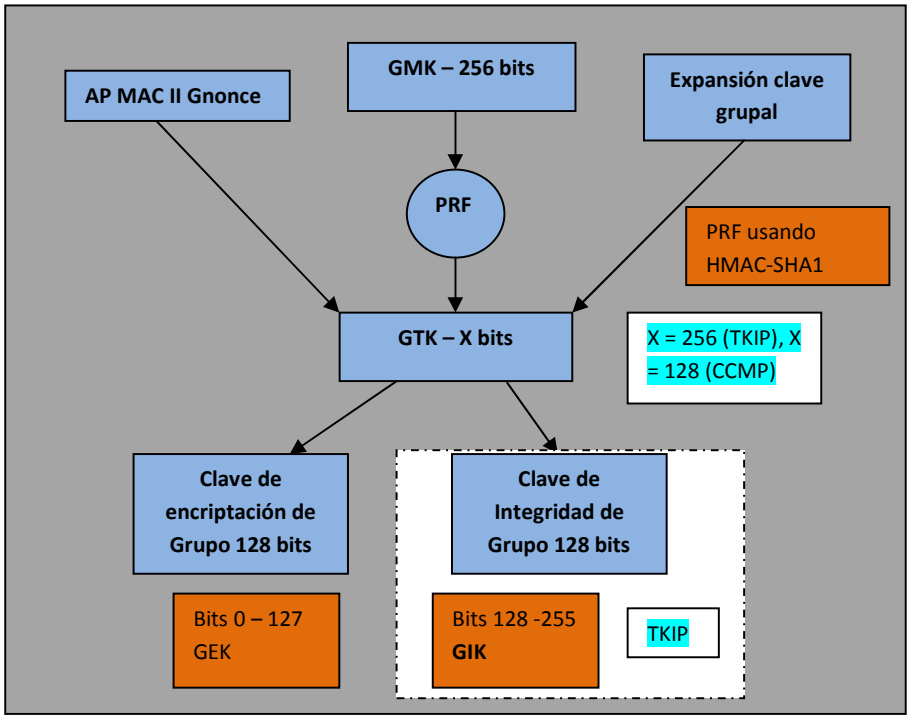

Figura 7.- Jerarquía del Group Key **(**Funcionamiento del GMK y GTK).

(Scribd, 2009).

En la figura 6 se explica esquemáticamente como se intercambian cuatro mensajes EAPOL Key entre el cliente y el punto de acceso durante el 4-Way Handshake.

La PTK se deriva de la PMK, una cadena fija, la dirección MAC del punto de acceso, la dirección MAC del cliente y dos números aleatorios (ANonce y SNonce, generados por el autenticador y el suplicante, respectivamente. El punto de acceso inicia en el primer mensaje seleccionando el número aleatorio ANonce y enviándoselo al suplicante, sin encriptar el mensaje o protegerlo de las trampas. El suplicante genera su propio número aleatorio Snonce y ahora puede calcular la PTK y las claves temporales derivadas, así que envía el Snonce y la clave MIC calculada del segundo mensaje usando la clave KCK.

Cuando el autenticador recibe el segundo mensaje, puede extraer el SNonce (porque el mensaje no está encriptado) y calcular la PTK y las claves temporales derivadas. Ahora puede verificar el valor del MIC en el segundo mensaje y estar seguro del que el suplicante conoce la PMK y ha calculado correctamente la PTK y las claves temporales derivadas.

El tercer mensaje enviado por el autenticador suplicante contiene el GTK (encriptada con la clave KEK), derivada de un GMK aleatorio y Gnonce (Ver figura 7), junto con el MIC calculado del tercer mensaje utilizando la clave KCK. Cuando el suplicante recibe este mensaje, el MIC se comprueba para asegurar que el autenticador conoce el PMK y ha calculado correctamente la PTK y derivado claves temporales.

El último mensaje certifica la finalización de handshake e indica que el suplicante ahora instalará la clave y empezará la encriptación. Al recibirlo, el autenticador instala sus claves tras verificar el valor MIC. Así, el sistema móvil y el punto de acceso han obtenido, calculado e instalado unas claves de integridad y encriptación y ahora pueden comunicarse a través de un canal seguro para tráfico unicast y multicast.

El tráfico multicast se protege con otra clave: GTK (Group Transient Key), generada de una clave maestra llamada GMK (Group Master Key), una cadena fija, la dirección MAC del punto de acceso y un número aleatorio GNonce. La longitud de GTK se divide en claves temporales dedicadas:

GEK (Group Encryption Key): Clave para encriptación de datos (usada por CCMP para la autenticación y para la encriptación y por TKIP).

GIK (Group Integrity Key): Clave para la autenticación de datos (usada solamente por Michael con TKP).

Esta jerarquía se resume en la figura 7.

A continuación en la siguiente tabla se explicará las características y diferencias entre WPA Enterprise con WPA PSK:

Modo WPA Enterprise	Modo WPA PSK (Pre-Shared Key)
Requiere un servidor de autenticación.	No necesita un servidor de autenticación.
Utiliza protocolos RADIUS para la autenticación y distribución de claves.	Secreto compartido se utiliza para la autenticación.
Centraliza la gestión de las credenciales de los usuarios.	Dispositivo orientado a la gestión de los usuarios.

Tabla 2.- Características y diferencias de WPA Enterprise y WPA PSK.

(Universidad de Buenos Aires (Departamento de computación), 2006).

Algoritmo utilizado

WPA utiliza el algoritmo RC4 con una clave de 128 bits y un vector de inicialización de 48 bits. Una de las mejoras más sobresalientes sobre su predecesor WEP, es TKIP (Temporal Key **I**ntegrity Protocol, o Protocolo de integridad de clave temporal), el cual consiste en el cambio dinámico mientras se utiliza el sistema. Cuando se combina con Vectores de Inicialización mayores, hace considerablemente más difícil realizar ataques para la obtención de llaves, como ocurre con WEP.

(TECH-FAQ, 2008).

Características y diferencias con respecto a WEP

- Propuesto por los miembros de la Wi-Fi Alliance en colaboración con la IEEE.

- Basado en el protocolo para cifrado TKIP (Temporary Key Integrity Protocol).

- La longitud de las claves pasa de 40 a 128 bits y el vector de inicialización, de 24 a 48 bits.

- La clave es generada de forma dinámica, para cada usuario, para cada sesión, y para cada paquete enviado, así como la distribución de claves, que también es realizada de forma automática.

- El mecanismo de autentificación basado en WPA emplea 802.1x/EAP. Se detallará brevemente el funcionamiento del protocolo de cifrado TKIP.

- Basado en el algoritmo “Michael” para garantizar la integridad.

- Genera un bloque de 4 bytes (MIC) a partir de la dirección MAC de origen, de destino, y de los datos.

- Añade el MIC calculado a la unidad de datos a enviar.

- Posteriormente los datos se fragmentan y se les asigna un número de secuencia.

- La mezcla del número de secuencia con la clave temporal, genera la clave que será utilizada para cada fragmento.

(Saulo.Net, 2008).

Mejoras de WPA respecto a WEP

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados.

El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (replay).

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC. (Message Integrity Codeo Michael) (Código que verifica la integridad de los datos de las tramas).

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

(Saulo.Net, 2008).

Debilidades y técnicas de ataques

A pesar que WPA resuelve problemáticas muy puntuales de seguridad que WEP tiene, no por eso es un sistema infalible y se han descubierto algunas vulnerabilidades sobre este método.

Como se ha mencionado anteriormente, WPA subsana las vulnerabilidades provenientes en WEP. En WEP no importa que tan buena o mala, larga o corta sea la clave WEP puesta, esta puede ser comprometida. Sin embargo, en WPA es diferente.

Una clave WPA puede construirse lo suficientemente buena como para hacer su descifrado casi imposible. Como contrapartida, el descifrado de WPA es mucho más amigable y sencillo, pues capturando los paquetes adecuados se puede realizar un ataque offline. Esto significa que sólo en un momento muy corto es necesario tener acceso al tráfico que llega al AP (Access Point).

La vulnerabilidad principal radica en tratar de vulnerar la clave maestra de donde se deducen el resto de las claves. Esta clave se genera en el proceso de autenticación inicial y por ende sería necesario capturarlos mensajes de ese proceso para tratar de vulnerar la misma. Para ello existen herramientas que provocan autenticaciones forzadas de las estaciones que las mismas vuelvan a generar el proceso de autenticación correspondiente.

Cuando las claves preestablecidas utilizadas en el modo PSK de WPA utilizan palabras presentes en el diccionario y la longitud es inferior a los 20 caracteres, el atacante sólo necesitará interceptar el tráfico inicial de intercambio de claves. Sobre este tráfico, realizando un ataque de diccionario o de fuerza bruta, el atacante puede obtener la clave preestablecida, que es la información

necesaria para obtener acceso a la red. Esto se debe a que en el modo PSK, la clave secreta compartida coincide con la clave maestra generada (PMK) en el proceso de generación de claves.

A diferencia de WEP es necesario capturar un volumen significativo de tráfico para poder identificar las claves, en WPA alcanza con capturar el tráfico de intercambio de claves para poder realizar este ataque.

(Saulo.Net, 2008)**.**

6.1.3. -WPA2 (Wi-Fi Protected Access 2)

Definición

WPA2, es el nombre que le dio la WIFI Alliance a la segunda fase del estándar IEEE 802.11i. La seguridad es muchísimo más robusta que la que ofrece WPA. WPA2 ya no se basa en un parche temporal sobre el algoritmo RC4 y en su lugar, utiliza el algoritmo de encriptación AES - recomendado por el NIST (National Institute of Standards, Instituto Nacional de Estándares y Tecnología), de los más fuertes y difíciles de comprometer en la actualidad. Este algoritmo de encriptación requiere un hardware más robusto, por lo tanto los Puntos de Acceso antiguos no se pueden utilizar con WPA2. Las primeras certificaciones de Puntos de Acceso compatibles con WPA2, se han hecho en Septiembre de 2004. Esto era voluntario, pero WPA2 es requisito obligatorio para todos los productos WIFI, desde Marzo de 2006.

(Seguridad Informática en 802.11, 2006).

Algoritmo que utiliza

Utiliza el algoritmo de encriptación AES y es de los más fuertes y difíciles de comprometer en la actualidad. Este algoritmo de cifrado requiere un hardware más robusto, por lo tanto los Puntos de Acceso antiguos no se pueden utilizar con WPA2. Las primeras certificaciones de Puntos de Acceso compatibles con WPA2 se han hecho en Septiembre de 2004. Esto era voluntario, pero WPA2 es requisito obligatorio para todos los productos WIFI, desde Marzo de 2006.

La implementación de protección que se aplica en el estándar de seguridad Wifi 802.11i, se conoce con el acrónimo CCMP (CounterMode with CBC-MAC Protocol) y está basada, como ya se comentó, en el algoritmo de encriptación AES .El cifrado que se utiliza es simétrico de 128 bits y el Vector de Inicialización (IV) tienen una longitud de 48 bits.

- El nuevo estándar exigió cambios en los paquetes que utilizan las redes inalámbricas WIFI para transmitir la información. Por ejemplo en los paquetes de "Beacons" o "Association Request" hubo que incluir datos sobre el tipo de encriptación: WEP, TKIP, CCMP, o sobre el tipo de autenticación: 802.1x o contraseña. Esto explica una vez más, porque los Puntos de Acceso y dispositivos Palm o PDA muy antiguos no funcionan con WPA2.

  (Seguridad Informática en 802.11, 2006).

Funcionamiento

Del mismo modo que en WPA, la autenticación se realiza utilizando o bien EAP (denominado comercialmente Enterprise Mode) o bien una clave compartida por todas las estaciones (Pre-Shared KeyMode o PSK).

Las principales diferencias con WPA son la utilización del Advanced Encription Standard (AES) en lugar de RC4 y del Counter-mode / Cbc Mac Protocol (CCMP) de AES en lugar de TKIP y MIC.

La utilización de AES, considerado uno de los algoritmos más seguros hasta el momento, es una mejora muy importante en la seguridad de las redes inalámbricas. El Advanced Encryption Standard es un cifrador por bloque, a diferencia del RC4 que es un cifrador por flujo. AES se utiliza en WPA2 con una longitud de clave de 128 bits. La arquitectura especificada por el estándar 802.11i se denomina Robust Security Network (RSN).

Además, se define una Transitional Security Network (TSN) en la que pueden participar sistemas RSN (es decir WPA o WPA2) y WEP. Cuando el proceso de autenticación utiliza el 4-way handshake, la asociación recibe el nombre de Robust Security Network Association (RSNA). Las fases utilizadas son las mismas que las descritas en el apartado de WPA.

La primera fase requiere que los participantes estén de acuerdo sobre la política de seguridad a utilizar. Sigue a esto una autenticación abierta estándar (igual que en las redes TSN, donde la autenticación siempre tiene éxito). La respuesta del cliente se incluye en el mensaje de *Association Request* validado por una *Association Response* del punto de acceso. La información sobre la política de seguridad se envía en el campo RSN IE (*Information Element*) y detalla:

- Los métodos de autenticación soportados (802.1X, Pre-Shared Key (PSK)).
- Protocolos de seguridad para el tráfico unicast (CCMP, TKIP etc.) – la suite criptográfica basada en pares.

- Protocolos de seguridad para el tráfico multicast (CCMP, TKIP etc.) – suit criptográfica de grupo.
- Soporte para la pre-autenticación, que permite a los usuarios pre-autenticarse antes de cambiar de punto de acceso en la misma red para un funcionamiento sin retrasos.

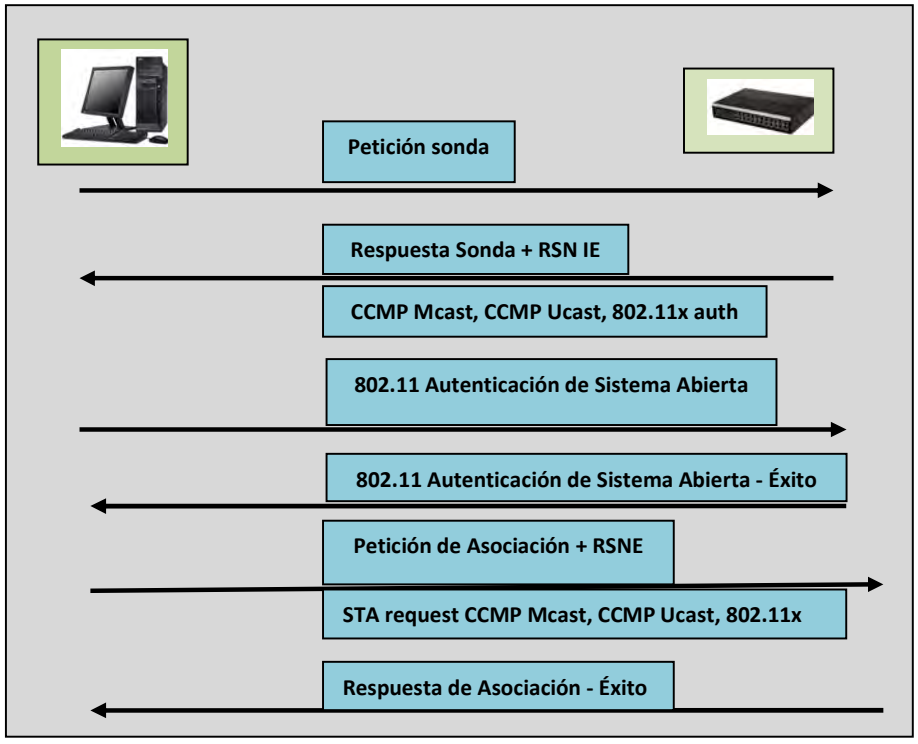

Figura 8.- Fase 1 WPA2.

La segunda fase es la autenticación 802.1X basada en EAP y en el método específico de autenticación decidido: EAP/TLS con certificados de cliente y servidor (requiriendo una infraestructura de claves públicas), EAP/TTLS o PEAP para autenticación híbrida (con certificados sólo requeridos para servidores), etc. La autenticación 802.1X se inicia cuando el punto de acceso pide datos de

identidad del cliente, y la respuesta del cliente incluye el método de autenticación preferido. Se intercambian entonces mensajes apropiados entre el cliente y el servidor de autenticación para generar una clave maestra común (MK). Al final del proceso, se envía desde el servidor de autenticación al punto de acceso un mensaje *Radius Accept*, que contiene la MK y un mensaje final *EAP Success* para el cliente.

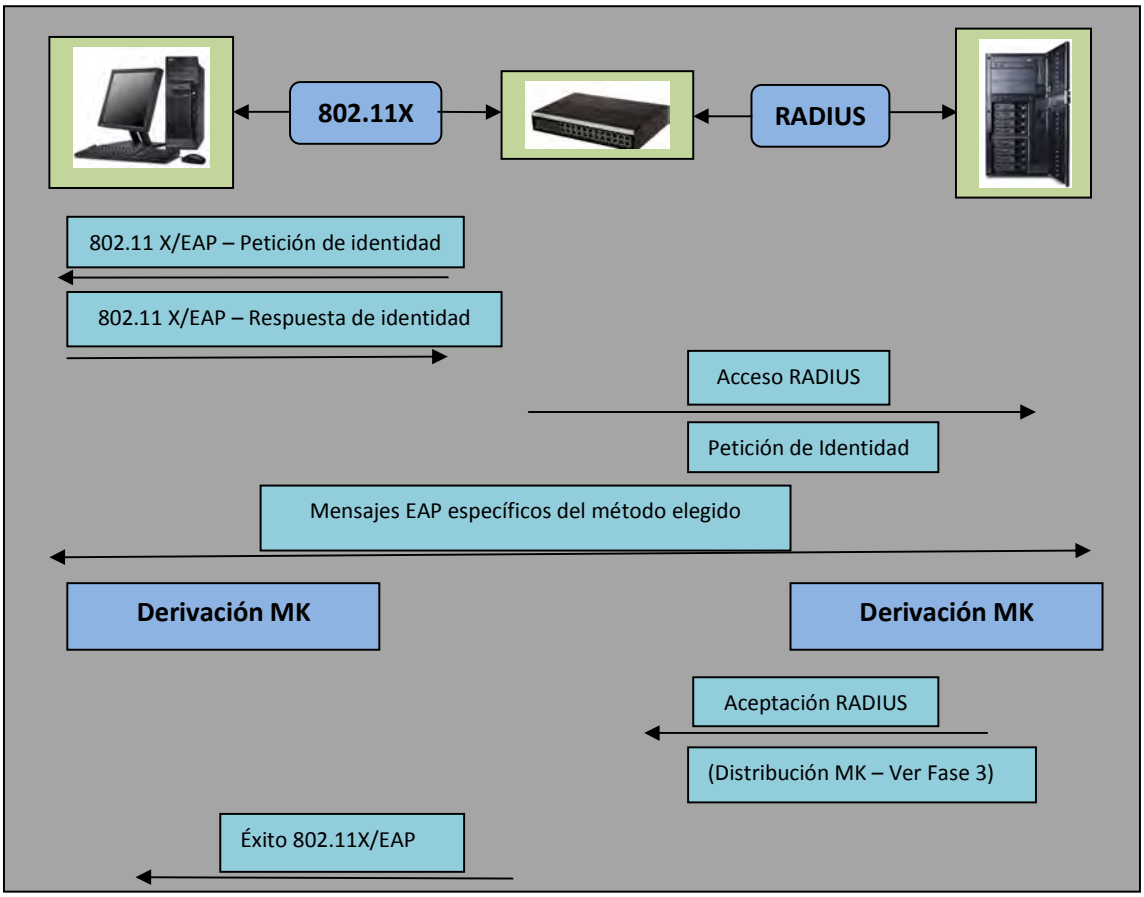

Figura 9.- Fase 2 WPA2.

La tercera fase trata la distribución y jerarquía de las claves. La seguridad de la conexión se basa en gran medida en las claves secretas. En RSN, cada clave

tiene una vida determinada y la seguridad global se garantiza utilizando un conjunto de varias claves organizadas según una jerarquía. Cuando se establece un contexto de seguridad tras la autenticación exitosa, se crean claves temporales de sesión y se actualizan regularmente hasta que se cierra el contexto de seguridad.

La cuarta fase habla sobre la confidencialidad e integridad de datos RSNA**.** Todas las claves generadas anteriormente se usan en protocolos que soportan la confidencialidad e integridad de datos RSNA:

- TKIP (*Temporal Key Hash*).
- CCMP (*Counter-Mode / Cipher Block Chaining Message Authentication Code Protocol*).
- WRAP (*Wireless Robust Authenticated Protocol*).

(Seguridad Informática en 802.11, 2006)**.**

Características

- WPA2 implementa todo el estándar IEEE 802.11i.
- Usa AES en lugar de RC4 para el cifrado de datos.
- Usa CCMP en lugar de TKIP y MIC
- Usa EAP como protocolo de autenticación.

(Universidad de Buenos Aires (Departamento de computación), 2006).

Debilidades y técnicas de ataques

- La utilización del mismo mecanismo de autenticación hace vulnerable a WPA2 al mismo tipo de ataque que WPA para el modo PSK: si un

atacante logra interceptar los paquetes de autenticación puede intentar un ataque de diccionario o de fuerza bruta sobre la clave PMK (que es la misma que la PSK). A partir de esta clave puede derivarse el resto de las claves utilizadas por el algoritmo.

Es importante recordar que para minimizar la posibilidad de la explotación de esta vulnerabilidad deben utilizarse claves mayores a 20 caracteres que incluyan caracteres especiales.

- Ciertas vulnerabilidades conocidas del protocolo 802.1X afectan obviamente a WPA y WPA2.

- Ningún protocolo inalámbrico está protegido frente a un ataque de denegación de servicio con un jammer (estafador).

(Universidad de Buenos Aires (Departamento de computación), 2006).

Protocolo	Tipo de Algoritmo	Características	Debilidades
WEP	• Algoritmo de cifrado estándar 802.11. • RC4 con claves (seed) 64 bits. • Vector de inicialización de 24 bits (RC4). • Clave secreta de 40 bits (RC4).	• Forma parte del estándar 802.11. • Opera en la capa 2 del modelo OSI (Subcapa MAC). • Soportado por una amplia mayoría de fabricantes de soluciones inalámbrica. • Utiliza el algoritmo de encriptación RC4.	• Utiliza clave estática (no se puede modificar). • La configuración de la clave ha de hacerse de forma manual. • El password del administrador es directamente la clave. Por ello la clave puede ser descubierta por ataques de diccionario. • La clave es bastante sencillo de romper.

WAP	• Algoritmo RC4 con clave de 128 bits. • Vector de inicialización de 48 bits. • Protocolo TKIP (Temporal Key Integrity Protocol).	• Propuesta por la Wi-Fi Alliance. • Basado en el protocolo de cifrado TKIP. • La longitud de la clave pasa de 40 a 128 bits y el vector de inicialización de 24 a 128 bits en comparación de WEP. • Clave generada de forma dinámica, es decir, cada usuario tiene su propia sesión y la distribución de claves se genera de forma automática. • Mecanismos de autenticación 802.1x/EAP. • Algoritmo Michael. • Genera bloques de 4 bits (MIC) a partir de la dirección MAC de origen, de destino y de los datos. • Añade MIC calculado a la unidad de datos a enviar. • Los datos se fragmentan y se les asigna un número de frecuencia. • La mezcla del número de secuencia con la clave temporal, genera la clave que será	La vulnerabilidad principal radica en tratar de vulnerar la clave maestra de donde se deducen el resto de las claves. Esta clave se genera en el proceso de autenticación inicial y por ende sería necesario capturar los mensajes de ese proceso para tratar de vulnerar la misma. Para ello existen herramientas que provocan autenticaciones forzadas de las estaciones que las mismas vuelvan a generar el proceso de autenticación correspondiente.

		utilizada para cada fragmento.	
WAP2	• Algoritmo de encriptación AES. • Cifrado simétrico de 128 bits. • Vector de inicialización de 48 bits.	• WPA2 implementa todo el estándar IEEE 802.11i. • Usa AES en lugar de RC4 para el cifrado de datos. • Usa CCMP en lugar de TKIP y MIC • Usa EAP como protocolo de autenticación	• La utilización del mismo mecanismo de autenticación hace vulnerable a WPA2 al mismo tipo de ataque que WPA para el modo PSK. • Ningún protocolo inalámbrico está protegido frente a un ataque de denegación de servicio.

Tabla 3.- Tabla comparativa de los principales protocolos de estandarización.

6.2. -Protocolo EAP

Al utilizar el Protocolo de autenticación extensible (EAP, Extensible Authentication Protocol), un mecanismo de autenticación arbitrario autentica las conexiones de acceso remoto. El cliente de acceso remoto y el autenticador (el servidor de acceso remoto o el servidor del servicio de usuario de acceso telefónico de autenticación remota [RADIUS]) negocian el esquema de autenticación exacto que se va a utilizar.

EAP permite que se establezcan conversaciones abiertas entre el cliente de acceso remoto y el autenticador. Esta conversación se compone de las solicitudes de información de autenticación realizadas por el autenticador y las respuestas del cliente de acceso remoto.

Por ejemplo, si se utiliza EAP con tarjetas de testigos de seguridad (en el que los usuarios escriben los datos que aparecen en un dispositivo de tarjeta de testigo al iniciar la sesión en la red inalámbrica) el autenticador puede consultar al cliente de acceso remoto el nombre, el PIN y el valor del testigo de la tarjeta por separado. Con cada consulta realizada y respondida, el cliente de acceso remoto atraviesa otro nivel de autenticación. Una vez respondidas correctamente todas las preguntas, se autentica al cliente de acceso remoto.

Los esquemas de autenticación específicos de EAP se denominan tipos de EAP. El cliente de acceso remoto y el autenticador deben admitir el mismo tipo de EAP para que la autenticación se lleve a cabo correctamente.

(Microsoft Tech Net, 2009).

Infraestructura EAP

El protocolo EAP es un conjunto de componentes internos que proporciona la compatibilidad de arquitecturas con cualquier tipo de EAP en forma de módulo de complemento. Para que la autenticación se realice correctamente, el cliente de acceso remoto y el autenticador deben tener instalado el mismo módulo de autenticación EAP. A continuación se describirá en forma detallada toda la familia del protocolo EAP:

EAP-TLS

El tipo de EAP Seguridad del nivel de transporte EAP (EAP-TLS, EAP-Transport Level Security) se utiliza en entornos de seguridad basados en certificados. Si se está utilizando tarjetas inteligentes para la autenticación de acceso remoto,

se debe utilizar el método de autenticación EAP-TLS. El intercambio de mensajes EAP-TLS permite la autenticación mutua, la negociación del método de cifrado y la determinación de claves cifradas entre el cliente de acceso remoto y el autenticador. EAP-TLS proporciona el método de determinación de claves y autenticación más eficaz.

EAP-TLS sólo se admite en servidores que ejecutan Enrutamiento y acceso remoto, que están configurados para utilizar la Autenticación de Windows o RADIUS, y que son miembros de un dominio. Los servidores de acceso remoto que se ejecutan como servidores independientes o miembros de un grupo de trabajo no admiten EAP-TLS.

(Microsoft Tech Net, 2009).

EAP- TTLS

Un tipo de método de autenticación que utiliza EAP y seguridad del nivel de transporte canalizado (TTLS). EAP-TTLS utiliza una combinación de certificados y otro método de seguridad, como las contraseñas

(DELL, 2009).

EAP-SIM

La autenticación de Protocolo de autenticación ampliable - Módulo de identidad de abonado (EAP-SIM) se puede utilizar con:

- Los tipos de autenticación de red: Abierta, Compartida y WPA2-Empresa.
- Los tipos de codificación de datos: Ninguna, WEP y CKIP

La tarjeta SIM es una tarjeta inteligente que se utiliza en redes celulares digitales basadas en GSM (Global System for Mobile Communications). La tarjeta SIM se utiliza para validar sus credenciales en la red.

(DELL, 2009).

EAP-RADIUS

EAP-RADIUS no es un tipo de EAP, sino el paso de mensajes EAP de cualquier tipo de EAP a un servidor RADIUS por parte de un autenticador para su autenticación. Por ejemplo, si se configura un servidor de acceso remoto para la autenticación RADIUS, los mensajes EAP enviados entre el cliente y el servidor de acceso remoto se encapsulan y formatean como mensajes RADIUS entre el servidor de acceso remoto y el servidor RADIUS.

EAP-RADIUS se utiliza en entornos en los que RADIUS se usa como proveedor de autenticación. La ventaja de utilizar EAP-RADIUS es que no es necesario instalar los tipos de EAP en todos los servidores de acceso remoto, sino sólo en el servidor RADIUS. En el caso de los servidores IAS (Internet Authentication Service (Servicio de Autenticación de Internet)), sólo debe instalar tipos de EAP en el servidor IAS.

Por lo general, al utilizar EAP-RADIUS, el servidor que ejecuta Enrutamiento y acceso remoto se configura para utilizar EAP y un servidor IAS para la autenticación.

Cuando se establece una conexión, el cliente de acceso remoto negocia el uso de EAP con el servidor de acceso remoto. Si el cliente envía un mensaje EAP al servidor de acceso remoto, éste encapsula el mensaje EAP como un mensaje RADIUS y lo envía al servidor IAS configurado.

El servidor IAS procesa el mensaje EAP y devuelve un mensaje EAP encapsulado como RADIUS al servidor de acceso remoto. A continuación, el servidor de acceso remoto reenvía el mensaje EAP al cliente de acceso remoto. En esta configuración, el servidor de acceso remoto sólo funciona como dispositivo de paso a través. Todo el procesamiento de los mensajes EAP se lleva a cabo en el cliente de acceso remoto y en el servidor IAS.

Se puede configurar enrutamiento y acceso remoto para realizar la autenticación localmente o en un servidor RADIUS. Si se configura Enrutamiento y acceso remoto para realizar la autenticación localmente, todos los métodos de EAP se autenticarán localmente.

Si se configura enrutamiento y acceso remoto para autenticar un servidor RADIUS, todos los mensajes EAP se reenviarán al servidor RADIUS con EAP-RADIUS.

(Microsoft Tech Net, 2009).

6.3.- Protocolo PEAP

El Protocolo de autenticación extensible protegido (PEAP) es un nuevo miembro de la familia de protocolos de Protocolo de autenticación extensible (EAP). PEAP utiliza Seguridad de nivel de transporte (TLS) para crear un canal cifrado entre un cliente de autenticación PEAP, como un equipo inalámbrico, y un autenticador PEAP, como un Servicio de autenticación de Internet (IAS) o un servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS). PEAP no especifica un método de autenticación, sino que proporciona seguridad adicional para otros protocolos de autenticación de EAP, como EAP-MSCHAPv2, que pueden operar a través del canal cifrado de TLS que proporciona PEAP. PEAP se utiliza como método de autenticación para los equipos cliente inalámbricos 802.11, pero no se admite en clientes de red privada virtual (VPN) u otros clientes de acceso remoto.

Para mejorar los protocolos EAP y la seguridad de red, PEAP proporciona:

- Protección de la negociación del método EAP que se produce entre el cliente y el servidor mediante un canal TLS. Esto ayuda a impedir que un intruso inserte paquetes entre el cliente y el servidor de acceso a la red (NAS) para provocar la negociación de un método EAP menos seguro. El canal TLS cifrado también ayuda a evitar ataques por denegación de servicio contra el servidor IAS.
- Compatibilidad con la fragmentación y el reensamble de mensajes, lo que permite el uso de tipos de EAP que no lo proporcionan.
- Clientes inalámbricos con la capacidad de autenticar el servidor IAS o RADIUS. Como el servidor también autentica al cliente, se produce la autenticación mutua.
- Protección contra la implementación de un punto de acceso inalámbrico (WAP) no autorizado cuando el cliente EAP autentica el certificado que proporciona el servidor IAS. Además, el secreto principal TLS creado por el autenticador y el cliente PEAP no se comparte con el punto de acceso. Como consecuencia, el punto de acceso no puede descifrar los mensajes protegidos por PEAP.
- Reconexión rápida de PEAP, que reduce el tiempo de retraso entre la solicitud de autenticación de un cliente y la respuesta del servidor IAS o RADIUS, y que permite a los clientes inalámbricos moverse entre puntos de acceso sin solicitudes de autenticación repetidas. De esta forma, se reducen los requisitos de recursos del cliente y el servidor.

(Microsoft TechNet, 2009).

Proceso de autenticación PEAP

El proceso de autenticación PEAP entre el cliente y el autenticador PEAP tiene lugar en dos etapas. En la primera etapa se configura un canal seguro entre el cliente PEAP y el servidor de autenticación. En la segunda se proporciona la autenticación EAP entre el cliente y el autenticador EAP.

(Microsoft TechNet, 2009).

Canal cifrado TLS

El cliente inalámbrico se asocia con un punto de acceso inalámbrico. Para poder crear una asociación segura entre el cliente y el punto de acceso, una asociación basada en IEEE 802.11 proporciona una autenticación de sistema abierto o de clave compartida. Una vez establecida correctamente la asociación basada en IEEE 802.11 entre el cliente y el punto de acceso, la sesión TLS se negocia con el punto de acceso. Después que la autenticación finalice correctamente entre el cliente inalámbrico y el servidor (por ejemplo, un servidor IAS), se negocia la sesión TLS entre ellos. La clave obtenida durante esta negociación se utiliza para cifrar todas las comunicaciones posteriores.

(Microsoft TechNet, 2009).

Comunicación autenticada por EAP

La comunicación EAP completa, que incluye la negociación EAP, tiene lugar a través del canal TLS. El servidor IAS autentica al usuario y al equipo cliente con el método que determina el tipo de EAP y que se ha seleccionado para utilizar en PEAP (EAP-TLS o EAP-MS-CHAPv2). El punto de acceso sólo reenvía mensajes entre el cliente inalámbrico y el servidor RADIUS; el punto de acceso (o una persona que lo supervise) no puede descifrar estos mensajes porque no es el extremo TLS.

(Microsoft TechNet, 2009).

Implementaciones inalámbricas 802.11 con PEAP

Puede elegir entre dos tipos de EAP para usar con PEAP: EAP-MS-CHAPv2 o EAP-TLS. EAP-MS-CHAPv2 usa credenciales (nombre de usuario y contraseña) para la autenticación de usuarios, y un certificado del almacén de certificados del equipo servidor para la autenticación del servidor. EAP-TLS utiliza los certificados instalados en el almacén de certificados del equipo cliente o una tarjeta inteligente para la autenticación de usuarios y equipos cliente, y un certificado del almacén de certificados del equipo servidor para la autenticación del servidor.

(Microsoft TechNet, 2009).

PEAP con EAP-MS-CHAPv2

PEAP con EAP-MS-CHAPv2 (PEAP-EAP-MS-CHAPv2) es más sencillo de implementar que EAP-TLS porque la autenticación de usuarios se realiza con credenciales basadas en contraseñas (nombre de usuario y contraseña) en lugar de certificados o tarjetas inteligentes; sólo es necesario que el servidor IAS o RADIUS tenga un certificado. Además, el certificado de servidor puede emitirlo una entidad emisora de certificados (CA) pública en la que confíe el equipo cliente (es decir, el certificado de la CA pública ya existe en la carpeta de la entidad emisora de certificados raíz de confianza en el almacén de certificados del equipo cliente). En este caso, el certificado de servidor no se descarga ni se agrega al almacén de certificados raíz de confianza del cliente, y no se pide al usuario que tome la decisión de confiar o no en el servidor.

El uso de autenticación mutua por parte de PEAP-EAP-MS-CHAPv2 supone una mayor seguridad que la que proporciona MS-CHAPv2, pues impide que un servidor no autorizado negocie el método de autenticación menos seguro y

permite generar claves con TLS. PEAP-EAP-MS-CHAPv2 requiere que el cliente confíe en los certificados que proporciona el servidor.

(Microsoft TechNet, 2009).

PEAP con EAP-TLS

Los certificados de clave pública proporcionan un método de autenticación más seguro que los que utilizan credenciales basadas en contraseñas. PEAP con EAP-TLS (PEAP-EAP-TLS) utiliza certificados para la autenticación de servidores y certificados o tarjetas inteligentes para la autenticación de usuarios y equipos cliente. Para utilizar PEAP-EAP-TLS, debe implementar una infraestructura de claves públicas (PKI).

(Microsoft TechNet, 2009).

6.4. - Protocolo TLS (Transport Layer Security)

Es un protocolo para establecer una conexión segura entre un cliente y un servidor. TLS (Transport Layer Segurity) es capaz de autenticar el cliente y el servidor y la creación de una conexión cifrada entre los dos.

El protocolo TLS es extensible, en el sentido de que los nuevos algoritmos se pueden añadir para alguno de estos fines, siempre y cuando el servidor y el cliente tengan el conocimiento de los nuevos algoritmos.

(TECH-FAQ, 2008).

6.5.- Código de Autenticación de Mensaje (MAC):

Un código de autenticación de mensajes (MAC - Message Authentication Code) consiste en una etiqueta de autenticación (también llamada suma de comprobación) obtenida de aplicar un algoritmo de autenticación, junto con una clave secreta, a un mensaje. Los MAC se computan y comprueban con la

misma clave de manera que sólo puedan ser comprobados por el destinatario específico, a diferencia de las firmas digitales.

Los MAC basados en una función hash (HMACS) utilizan una o varias claves junto con una función hash para generar una suma de comprobación que se adjunta al mensaje. Un ejemplo es el método MD5 con claves para la autenticación de mensajes.

Los MAC también pueden obtenerse de codificadores de bloques. Los datos se cifran en bloques de mensajes con DES CBC y el bloque final en el texto cifrado se utiliza como la suma de comprobación. El MAC DES-CBC es una norma de uso generalizado en EE. UU. y en el ámbito internacional.

(HP, 2008).

6.6.- Código de Integridad de Mensaje (MIC):

Se utiliza con frecuencia como un término para sustituir el MAC, sobre todo en las comunicaciones, donde MAC es el acrónimo utilizado tradicionalmente por los medios de comunicación de control de acceso. Sin embargo, algunos autores MIC usa como diferente plazo de un MAC en una clave secreta que no se utiliza en el Centro de operación, por lo que una MIC debe ser siempre cifrados durante la transmisión para que sea utilizado como un indicador fiable de mensaje integridad.

Un mensaje dado siempre produce el mismo MIC asumiendo que el mismo algoritmo se utiliza para generar tanto. Por el contrario el mismo mensaje solo puede generar la misma clave secreta y el vector de inicialización son utilizados con los mismos algoritmos para generar ambos. PRM no utiliza claves secretas y, cuando se toma por su cuenta es mucho menos fiable de medir la integridad del mensaje. Un Mac que utiliza una clave secreta no necesariamente tienen que ser codificadas para proporcionar el mismo nivel de fiabilidad.

La computación del MIC utiliza el algoritmo Michael de Niels Ferguson. Se creó para TKIP y tiene un nivel de seguridad de 20 bits (el algoritmo no utiliza multiplicación por razones de rendimiento, porque debe ser soportado por el viejo hardware de red para que pueda ser actualizado a WPA). Por esta limitación, se necesitan contramedidas para evitar la falsificación del MIC. Los fallos de MIC deben ser menores que 2 por minuto, o se producirá una desconexión de 60 segundos y se establecerán nuevas claves GTK y PTK tras ella. Michael calcula un valor de comprobación de 8 octetos llamado MIC y lo añade a la MSDU antes de la transmisión.

El MIC se calcula de la dirección origen (SA), dirección de la TMK apropiada (dependiendo del lado de la comunicación, se utilizará una clave diferente para la transmisión y la recepción).destino (DA), MSDU de sólo texto y CCMP se basa en la suite de cifrado de bloques AES (*Advanced Encryption Standard*) en su modo de operación CCM, con la clave y los bloques de 128 bits de longitud. AES es a CCMP lo que RC4 a TKIP, pero al contrario que TKIP, que se diseñó para acomodar al hardware WEP existente, CCMP no es un compromiso, sino un nuevo diseño de protocolo. CCMP utiliza el counter mode junto a un método de autenticación de mensajes llamado *Cipher Block Chaining* (CBC-MAC) para producir un MIC.

Se añadieron algunas características interesantes, como el uso de una clave única para la encriptación y la autenticación (con diferentes vectores de inicialización), el cubrir datos no encriptados por la autenticación. El protocolo CCMP añade 16 bytes al MPDU, 8 para el encabezamiento CCMP y 8 para el MIC. El encabezamiento CCMP es un campo no encriptado incluido entre el encabezamiento MAC y los datos encriptados, incluyendo el PN de 48-bits (*Packet Number* = IV Extendido) y la *Group Key KeyID*. El PN se incrementa de uno en uno para cada MPDU subsiguiente.

La computación de MIC utiliza el algoritmo CBC-MAC que cifra un bloque de inicio (son bloques de datos generados por el servidor) (computado desde los campos de *Priority*, la dirección fuente de MPDU y el PN incrementado) y hace XORs sobre los bloques subsiguientes para obtener un MIC final de 64 bits (el MIC final es un bloque de 128-bits, ya que se descartan los últimos 64 bits). El MIC entonces se añade a los datos de texto para la encriptación AES en modo contador. El contador se construye de un nonce similar al del MIC, pero con un campo de contador extra inicializado a 1 e incrementado para cada bloque.

(Seguridad Informática en 802.11, 2006).

Ejemplo

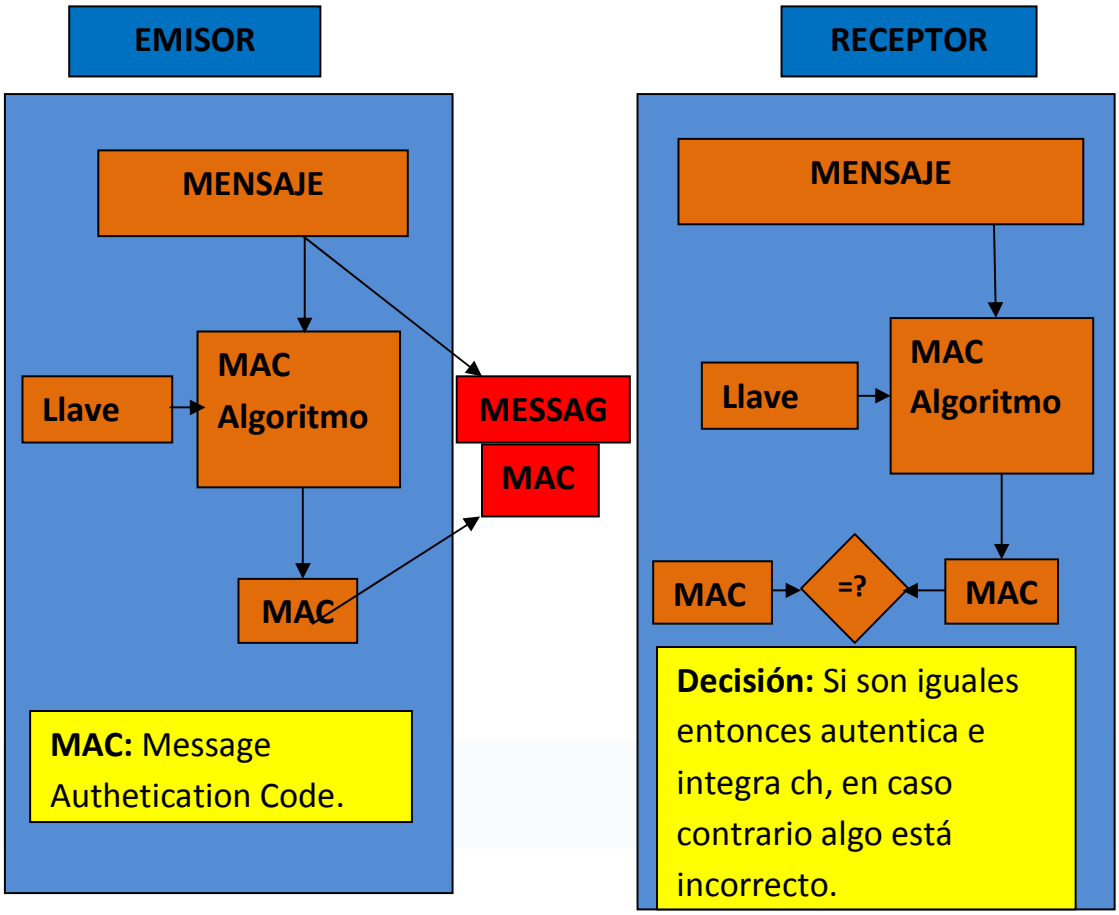

Figura 10.- Funcionamiento del MAC.

6.7.- PSK (PRE-Shared Key)

La PSK es generada desde una *passphrase* (de 8 a 63 caracteres) o una cadena de 256-bit y proporciona una solución para redes domésticas o pequeñas empresas que no tienen servidor de autenticación.

(Seguridad Informática en 802.11, 2006).

6.8.- PTK (Pairwise Transient Key)

Para el tráfico unicast esta es la PTK (*Pairwise Transient Key*). La longitud de la PTK depende el protocolo de encriptación: 512 bits para TKIP y 384 bits para CCMP. La PTK consiste en varias claves temporales dedicadas:

• KCK (*Key Confirmation Key* – 128 bits): Clave para la autenticación de mensajes (MIC) durante el *4-Way Handshake* y el *Group Key Handshake*,
• KEK (*Key Encryption Key* – 128 bits): Clave para asegurar la confidencialidad de los datos durante el *4-Way Handshake* y el *Group Key Handshake*,
• TK (*Temporary Key* – 128 bits): Clave para encriptación de datos (usada por TKIP o CCMP),
• TMK (*Temporary MIC Key* – 2x64 bits): Clave para la autenticación de datos. Se usa una clave dedicada para cada lado de la comunicación.

El *4-Way Handshake*, iniciado por el punto de acceso, hace posible:

• Confirmar que el cliente conoce la PMK.
• Derivar una PTK nueva.
• Instalar claves de encriptación e integridad.
• Cifrar el transporte de la GTK.

• Confirmar la selección de la suite de cifrado.

La PTK se deriva de la PMK, una cadena fija, la dirección MAC del punto de acceso, la dirección MAC del cliente y dos números aleatorios (*ANonce* y *SNonce*, generados por el autenticador y el suplicante, respectivamente). El punto de acceso inicia el primer mensaje seleccionando el número aleatorio *ANonce* y enviándoselo al suplicante, sin cifrar el mensaje o protegerlo de las trampas. El suplicante genera su propio número aleatorio *SNonce* y ahora puede calcular la PTK y las claves temporales derivadas, así que envía el *SNonce* y la clave MIC calculada del segundo mensaje usando la clave KCK. Cuando el autenticador recibe el segundo mensaje, puede extraer el *SNonce* (porque el mensaje no está encriptado) y calcular la PTK y las claves temporales derivadas. Ahora puede verificar el valor de MIC en el segundo mensaje y estar seguro de que el suplicante conoce la PMK y ha calculado correctamente la PTK y las claves temporales derivadas.

(Seguridad Informática en 802.11, 2006).

6.9.- GTK (Group Transient Key)

El tráfico multicast se protege con otra clave: GTK generada de una clave maestra llamada GMK (Group Master Key), una cadena fija, la dirección MAC del punto de acceso y un número aleatorio GNonce. La longitud de GTK depende del protocolo de encriptación – 256 bits para TKIP y128 bits para CCMP. GTK se divide en claves temporales dedicadas:

- GEK (*Group Encryption Key*): Clave para encriptación de datos (usada por CCMP para la autenticación y para la encriptación, y por TKIP).

- GIK (*Group Integrity Key*): Clave para la autenticación de datos (usada solamente con TKIP).

(Seguridad Informática en 802.11, 2006).

6.10.-TKIP (Temporal Key Integrity Protocol)

Es un protocolo de seguridad usado en WPA (Wi-Fi Protected Access) para mejorar el cifrado de datos en redes inalámbricas. WPA es utilizado en redes Wi-Fi para corregir deficiencias en el antiguo estándar de seguridad WEP.

TKIP fue diseñado para reemplazar el WEP sin cambiar el hardware (tal vez solamente el firmware). Esto era necesario, porque la seguridad del WEP fue quebrada, dejando a las redes Wi-Fi sin una buena seguridad en su capa de enlace y la solución a este problema no podía esperar a que se cambie todo el hardware fabricado.

La principal diferencia entre WEP y TKIP, es que WEP utiliza periódicamente la misma clave para cifrar los datos; en cambio TKIP comienza con una clave temporal de 128 bits que comparte entre los clientes y puntos de accesos. TKIP combina la clave temporal con la dirección MAC del cliente. Luego añade un valor de inicialización relativamente largo (de 16 octetos) para producir la clave final con la cual se cifrarán los datos. Tanto WEP como TKIP utilizan el RC4 para hacer el cifrado.

TKIP se considera una solución temporal, pues la mayoría de los expertos creen necesaria una mejora en el cifrado.

(Diccionario Informático, 2008).

TKIP Key-Mitin Scheme se divide en dos fases. La primera se ocupa de los datos estáticos – la clave TEK de sesión secreta, el TA de la dirección MAC del transmisor (incluido para prevenir colisiones IV) y los 32 bits más altos del IV. La fase 2 incluye el resultado de la fase 1 y los 16 bits más bajos del IV, cambiando todos los bits del campo *Per Packet Key* para cada nuevo IV. El valor IV siempre empieza en 0 y es incrementado de uno en uno para cada paquete enviado, y los mensajes cuyo TSC no es mayor que el del último mensaje son rechazados. El resultado de la fase 2 y parte del IV extendido (además de un bit dummy) componen la entrada para RC4, generando un flujo de clave que es XOR-eado con el MPDU de sólo texto, el MIC calculado del MPDU y el viejo ICV de WEP.

(Seguridad Informática en 802.11, 2006)**.**

6.11.-CCMP (Counter Mode With CBC – MAC): Modo de contador con protocolo CBC-MAC (Counter Mode with CBC-MAC Protocol). 802.11i define el uso de AES con el modo de operación CCM como CCMP. Es el protocolo de cifrado más fuerte disponible para su uso con las LAN inalámbricas.

(WIFI, 2009).

CCMP utiliza claves de 128 bits, con una de 48 bits del vector de inicialización (IV) para la detección de reproducción.

Contra el modo de (CM) de componente CCMP es el algoritmo de proporcionar la privacidad de los datos.

El Cipher Block Chaining Código de autenticación de mensaje (CBC-MAC) de componente CCMP ofrece la integridad de los datos y autenticación.

(TECH-FAQ, 2009).

6.12.- Vector de inicialización

En criptografía, un **vector de inicialización** (conocido por sus siglas en inglés IV) es un bloque de bits que es requerido para permitir un cifrado en flujo o un cifrado por bloques, en uno de los modos de cifrado, con un resultado independiente de otros cifrados producidos por la misma clave. El tamaño del IV depende del algoritmo de cifrado y del protocolo criptográfico y a menudo es tan largo como el tamaño de bloque o como el tamaño de la clave.

Los vectores de inicialización son implementados en cifrados por bloques y cifrados en flujo. Por ejemplo, el modo *Electronic Code Book* (ECB), el cifrado del mismo texto con la misma clave da como resultado el mismo texto cifrado, lo cual es una considerable vulnerabilidad. El uso de un vector de inicialización añadido linealmente (mediante una operación XOR) o incluido delante del texto plano antes del cifrado resuelve este problema.

En los cifrados en flujo, los vectores de inicialización se cargan en estado interno en clave del cifrador, después del cual se ejecuta cierto número de rondas de cifrado antes de emitir el primer BIT cifrado. Por razones de rendimiento, los diseñadores de los cifrados en flujo intentan mantener el número de rondas en las mínimas posibles, pero debido a que determinar el número de rondas para que sea seguro no es una tarea trivial, y considerando otros temas como la pérdida de entropía, dependiente del diseño del cifrador, ataques criptográficos relacionados con los IV son un problema de seguridad conocido para estos cifradores en flujo. Esto hace que el uso de IV en estos algoritmos un tema que debe ser aún desarrollado e investigado.

(Schneir, 1996).

6.13.- Criptografía simétrica

Utiliza una misma clave para cifrar y para descifrar mensajes. Las dos partes que se comunican se ponen de acuerdo de antemano sobre la clave a usar. Una vez que ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y este lo descifra con la misma.

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un hacker o cracker conocer el algoritmo que se está usando. Solo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Los algoritmos de cifrado usados por ejemplo en el sistema GNU, GnuPG tienen estas propiedades.

Dado que toda la seguridad está en la clave, es importante que sea muy difícil descifrar el tipo de clave. Esto quiere decir que el abanico de claves posibles, es decir, el espacio de posibilidades de claves, debe ser amplio.

Actualmente los computadores y servidores pueden adivinar claves con extrema rapidez, y esta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos. El algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 2 elevado a 56 claves posibles. 2 elevado a56 son 72.057.594.037.927.936 claves.

Esto representa un número muy alto de claves, pero una PC de uso general puede comprobar todo el espacio posible de claves en cuestión de días. Una máquina especializada lo puede hacer en horas. Por otra parte, algoritmos de cifrado de diseño como 3DES, Blowfish e IDEA usan claves de 128 bits, lo que significa que existen 2 elevado a 128 claves posibles.

Esto representa muchas más claves, y aún en el caso de que todas las PCs del planeta estuvieran cooperando, todavía tardarían más tiempo que la misma edad del universo en encontrar la clave. Incluso en la actualidad se pueden encontrar en el mercado claves a 256 bits, 512 bits y más.

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse la clave entre sí? Sería mucho más fácil para un atacante intentar interceptar una claveque probar las posibles combinaciones del espacio de claves. **Es aquí donde entran la criptografía asimétrica y la criptografía híbrida.**

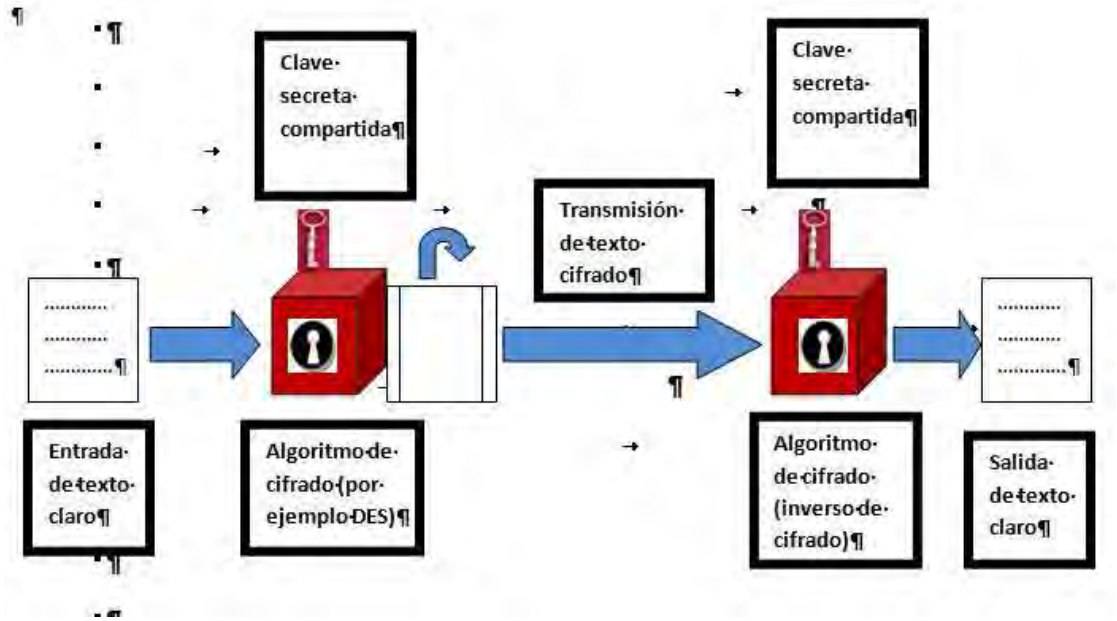

Figura 11.- Modelo simplificado del cifrado convencional.

(Componentes de Seguridad, 2009).

6.14.- Algoritmos de cifrado simétrico

Los algoritmos de cifrado simétrico más comúnmente usados son los cifradores de bloques. Un cifrador de bloques procesa la entrada de texto claro en bloques de tamaño fijo y genera un bloque cifrado del mismo tamaño para cada texto claro.

(Componentes de Seguridad, 2009).

DES (Data Encryption Standard)

El esquema de cifrado más extendido se basa en el DES (Data Encryption Standard) adoptado en 1977 por el Nacional Bureau of Standards, ahora el NIST (Nacional Institute of Standards and Technology), como Federal Information Processing Standard 46.

(Componentes de Seguridad, 2009).

Descripción del algoritmo

El texto claro tiene una longitud de 64 bits y la clave, de 56; si el texto en claro es más largo se procesa en bloques de 64 bits. La estructura del DES consiste en una pequeña variación de la red de Feistel, que se muestra en la figura 11. Hay 16 etapas de proceso. Se generan 16 subclaves partiendo de la clave original de 56 bits, una para cada etapa.

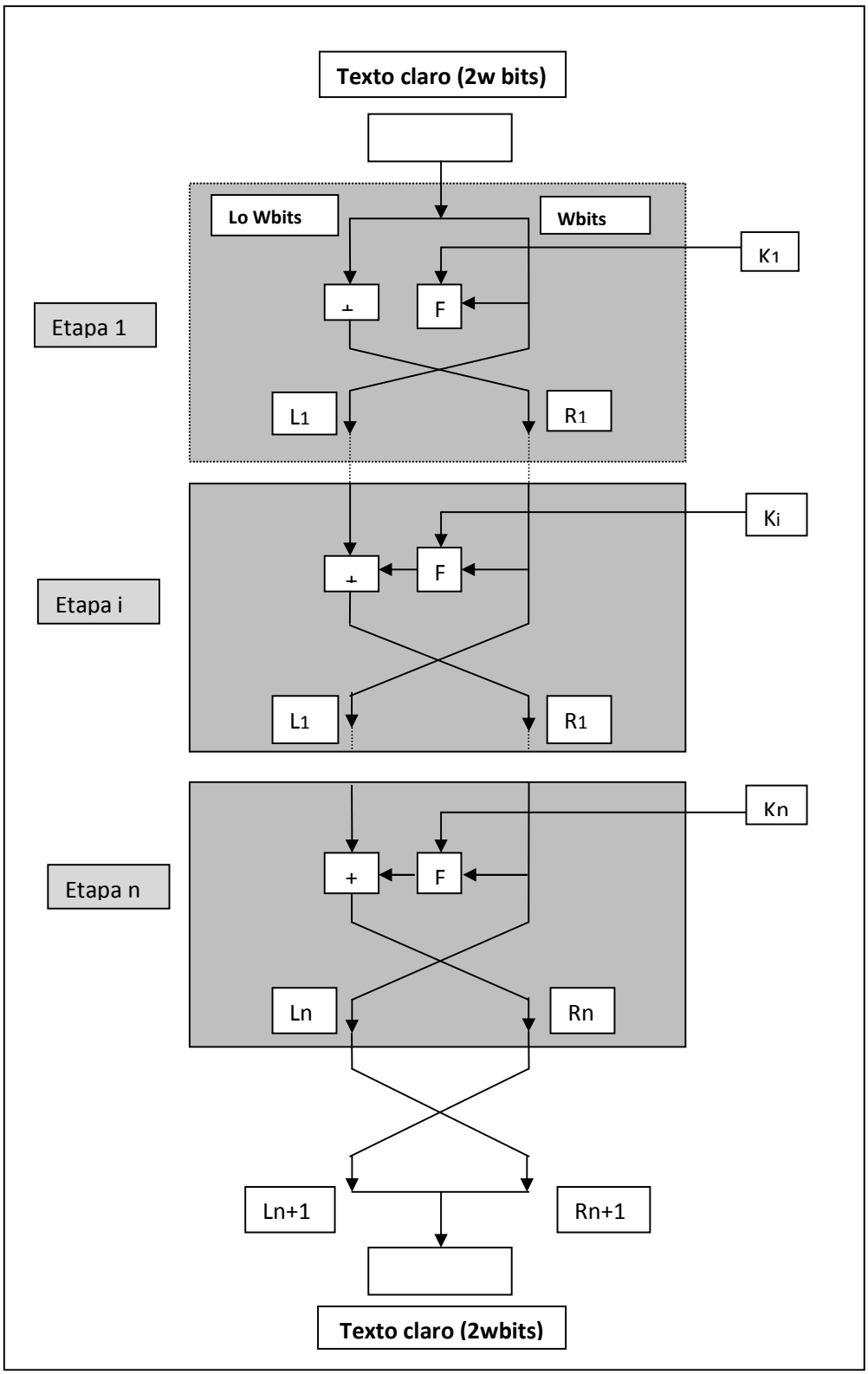

Figura 12.- Red clásica de Feistel.

El proceso de descifrado con el DES es básicamente el mismo que el de cifrado. La regla es la siguiente: usar el texto cifrado como entrada al algoritmo del DES, pero las subclaves K_i se pasan en orden inverso.

Es decir, en la primera etapa se usa K16, K15 en la segunda y así sucesivamente hasta K1 en la 16ª y última.

(Componentes de Seguridad, 2009).

Robustez del DES

Los aspectos de robustez del DES se engloban en dos categorías: aspectos sobre el algoritmo mismo y aspectos sobre el uso de una clave de 56 bits. Los primeros se refieren a la posibilidad de que el criptoanálisis se realice explotando las características del algoritmo DES. A lo largo de los años, se han intentado encontrar debilidades que explotar en el algoritmo, lo que ha hecho del DES el algoritmo de cifrado existente mas estudiado. A pesar de los numerosos enfoques, nadie había conseguido descubrir ninguna debilidad grave en el DES.

Un aspecto de mayor importancia es la longitud de la clave. Con una clave de 56 bits, hay 256 claves posibles, que es aproximadamente 7,2 X 1016 claves. Por este motivo, no parece práctico un ataque de fuerza bruta. Suponiendo que, en promedio, se tiene que intentar la mitad del espacio de claves, una única máquina que realice un cifrado DES por microsegundo tardaría mas de mil años en romper el cifrado.

En cualquier caso, la suposición de un cifrado por microsegundo es demasiado conservadora. En julio de 1998, se probó que el DES no era seguro, cuando la

Electronic Frontier Foundation (EFF) anunció que había roto un cifrado DES utilizando una máquina especializada DES cracker, construida por menos de 250.000 dólares. El ataque duro menos de tres días. La EFF ha publicado la descripción detallada de la máquina, haciendo posible que cualquiera construya su propia cracker. Naturalmente, los precios del hardware continuarán bajando mientras la velocidad seguirá aumentando, haciendo al DES prácticamente inútil.

Es importante tener en cuenta que para que un ataque de búsqueda de clave no basta con probar todas las posibles claves. A menos que se suministre el texto claro, el analista debe ser capaz de reconocer el texto claro como tal. Si el mensaje es texto claro en inglés, entonces el resultado se obtiene fácilmente, aunque la tarea de reconocimiento del inglés tendría que estar automatizada.

Si el mensaje de texto se ha comprimido antes del cifrado, entonces el reconocimiento es más difícil. Y si el mensaje es de un tipo más general de datos, como un fichero numérico, y ha sido comprimido, el problema es aun más difícil de automatizar. Pero eso, para complementar el enfoque de fuerza bruta, se necesita algún grado de conocimiento sobre el texto claro esperado y alguna forma de distinguir automáticamente el texto claro de lo que no lo es.

El enfoque de la EFF trata también este tema, e introduce algunas técnicas automatizadas que serían efectivas en muchos contextos, por ejemplo, si la única forma de ataque a un algoritmo de cifrado es la fuerza bruta, entonces la manera de contrarrestar este ataque sería obvia: usar claves más largas. Para tener una idea del tamaño de clave necesario, se puede usar el cracker de la EFF como base de estas estimaciones. El cracker de la EFF era un prototipo, y se puede suponer que con la tecnología actual es rentable construir una máquina más rápida.

Si se asume que un dispositivo como el cracker puede realizar un millón de descifrados por us, [Dominio de nivel superior geográfico o Dominio de nivel superior de código de país (en inglés ccTLD, *country code Top-Level Domain*) es un dominio de Internet usado y reservado para un país o territorio dependiente; el dominio us pertenece a EUA], entonces tardaría alrededor de diez horas en descifrar un código DES. Esto constituye un incremento de velocidad aproximadamente un factor de siete comparado con los resultados de la EFF.

La figura 12 muestra cuánto tardaría en romper un algoritmo del estilo del DES en función del tamaño de la clave. Por ejemplo, para una clave de 128 bits, que es común entre los algoritmos actuales, tardaría 1018 años en romper el código usando el cracker de la EFF. Incluso, aunque se aumentará la velocidad del cracker en un factor de un trillón (1012), todavía se tardaría un millón de años en romper el código. Así que una clave de 128 bits garantiza que el algoritmo es inexpugnable por la fuerza bruta.

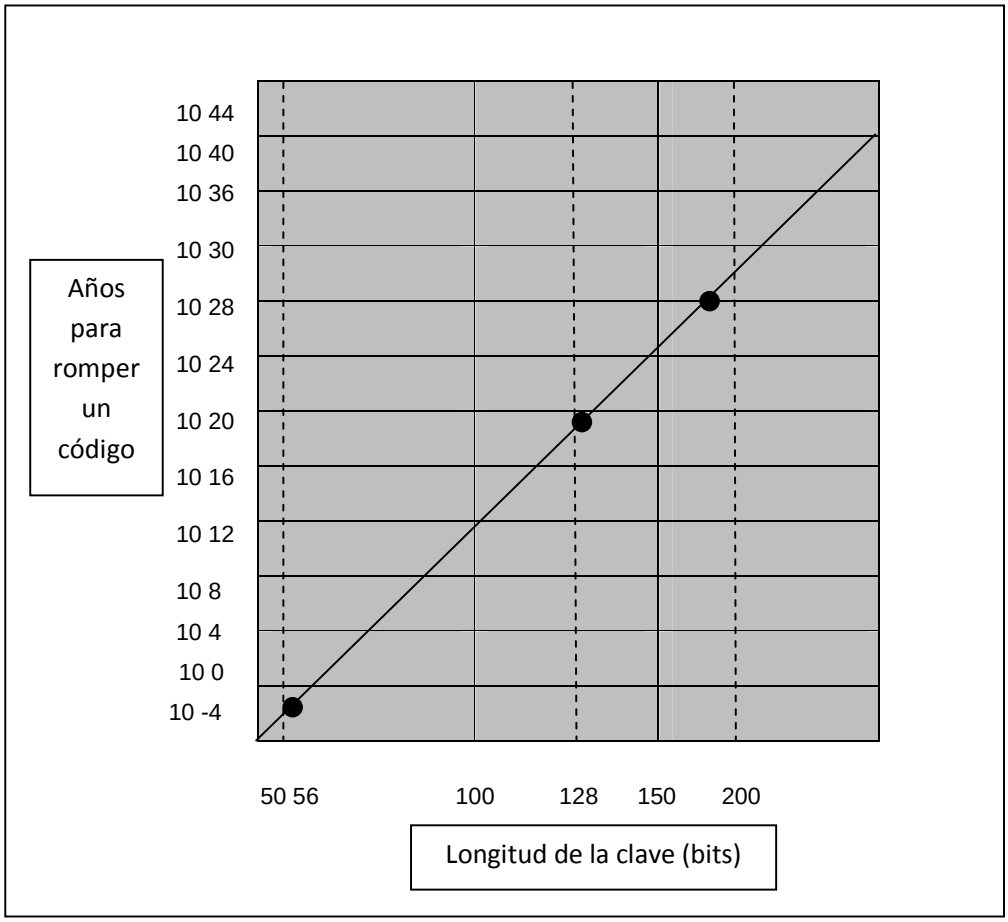

Figura 13.- Tiempo empleado en romper un código

(Suponiendo 106 descifrados/us).

(Componentes de Seguridad, 2009).

Triple DES

El triple DES (3DES) se estandarizó inicialmente para aplicaciones financieras en el estándar ANSI X9.17en 1985. 3DES se incorporó como parte del DES en 1999, con la publicación de FIPS PUB 463.

3DES usa tres claves y tres ejecuciones del algoritmo DES. La función sigue la secuencia cifrar-descifrar-cifrar (EDE: encrypt-decryptencrypt) figura 13a:

C = EK3 [DK2 [EK1 [P]]]

Donde

C = texto cifrado.

P = texto claro.

EK [X] = cifrado de X usando la clave K.

DK [Y] = descifrado de Y usando la clave K.

El descifrado es simplemente la misma operación con las claves en orden inverso (figura 13b):

P = DK1 [EK2 [DK3 [C]]]

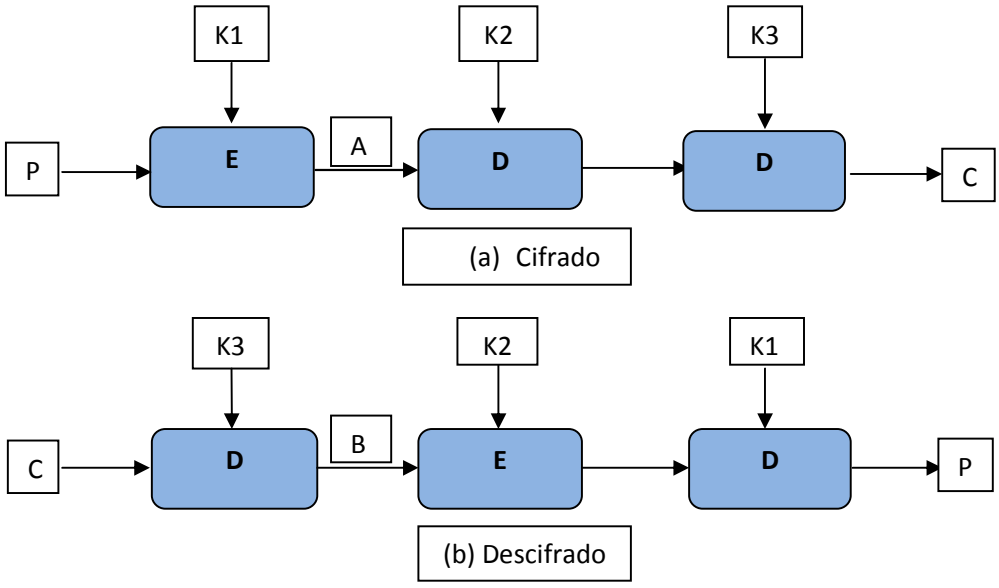

Figura 14.-Triple DES.

El descifrado del segundo paso no es significativo en términos criptográficos. Su única ventaja es que permite a los usuarios del 3DES descifrar datos cifrados por usuarios del DES:

C = EK1 [DK1 [EK1 [P]]] = EK1 [P]

Con tres claves diferentes, el 3DES tiene una longitud efectiva de clave de 168 bits. El FIPS 463también permite el uso de dos claves, con K1 = K3, lo que proporciona una longitud de clave de 112 bits. ElFIPS 463 incluye las siguientes directrices para el 3DES:

- El 3DES es el algoritmo de cifrado simétrico oficial del FIPS.
- El DES original, que usa una única clave de 56 bits, se mantiene solo para los sistemas existentes. Las nuevas adquisiciones deberían admitir 3DES.

- Se apremia a las organizaciones gubernamentales con sistemas que usan DES a migrar a 3DES.
- Se prevé que el 3DES y el AES (Advanced Encryption Standard) coexistirán como algoritmos oficiales del FIPS, permitiendo una transición gradual hacia el AES.

Es fácil observar que el 3DES es un algoritmo robusto. Debido a que el algoritmo criptográfico que lo sustenta es DES, 3DES resulta igual de resistente al criptoanálisis basado en el algoritmo que DES. Es más, con una clave de 168 bits de longitud, los ataques de fuerza bruta son efectivamente imposibles.

(Componentes de Seguridad, 2009).

AES (Advanced Encryption Standard)

AES es el nuevo estándar de cifrado simétrico dispuesto por el NIST, después de un periodo de competencia entre 15 algoritmos sometidos. El 2 de Octubre de 2000 fue designado el algoritmo Rijndael como AES, el estándar reemplazó a TDES, para ser usado en los próximos 20 años. Este reporte describe de forma detallada el algoritmo y algunas de sus características.

El algoritmo Rijndael fue elegido por el NIST (National Institute of Standards and Technology), para ser el estándar en los próximos 20 años y es llamado AES (Advanced Encryption Standar). Rijndael fue elegido después de pasar un periodo de análisis durante aproximadamente 3 años, Rijndael fue elegido como la mejor opción dentro de 15 candidatos, sus principales características fueron su fácil diseño, su versatilidad en ser implementado en diferentes dispositivos, así como ser inmune a los ataques conocidos hasta la fecha, soportar bloques

de datos de 128bits y claves de 128, 192, y 256 bits. La idea básica general es tener un estándar que mejore el “performance” de TDES y sea resistente a los ataques conocidos.

(Componentes de Seguridad, 2009).

Introducción

AES es el nuevo estándar de criptografía simétrica adoptado en el FIPS 197[34](Federal Information Processing Standards). Desde 1977 que apareció la primera versión del estándar FIPS 46, asume como estándar el algoritmo DES (Data Encryption Standar), y sus posteriores reafirmaciones en 1983, 1988, 1993, y 1999. Casi siempre se había visto opiniones controversiales de DES, sin embargo nunca fue dado un ataque que derivara por completo la clave secreta partiendo de la información pública, pero su corta longitud de clave lo comprometía poco a poco. La última reafirmación de DES en octubre de 1999 realmente fue suplantado por TDES, que es una versión múltiple de DES, designado como TDEA (Triple Data Encryption Algorithm).

Sin embargo, ya se tenían planes de encontrar un reemplazo definitivo a DES. A pesar de un número grande de algoritmos que en la época estaban presentes como: IDEA, RC5, skipjack, 3-way, FEAL, LOKI, SAFER, SHARK,... NIST decidió convocar a un concurso que tuvo como principales objetivos obtener un algoritmo simétrico que garantice su seguridad para los próximos 20 años a partir del año 2000. La convocatoria apareció el 2 de enero de 1997, se admitieron 15 algoritmos, en agosto de1998 en la primera conferencia AES se discutieron los algoritmos sometidos y posteriormente en la segunda conferencia AES en marzo de 1999, se realizaron los últimos comentarios. Para

que en agosto de 1999 se comunicaran los 5 finalistas: MARS, RC6, Rijndael, Serpent y Twofish.

En abril del 2000 se llevó a cabo la tercera conferencia AES, recibiendo los últimos análisis, para que finalmente el 2 de octubre del año 2000 se diera a conocer el ganador y se dispuso al Algoritmo RIJNDAEL como AES [46]. Esto llegó a ser asumido oficial en noviembre 26 el 2001 en el FIPS 197.

El algoritmo Rijndael fue elegido principalmente por garantizar seguridad, que significa ser inmune a los ataques conocidos, tener un diseño simple, y poder ser implementado en la mayoría de los escenarios posibles, desde dispositivos con recursos limitados, como smart cards, hasta procesadores paralelos. El tiempo ha permitido que AES sea adaptado poco a poco, desde los protocolos más usados como SSL, hasta las aplicaciones más especializadas, como VoIP.

La descripción de AES es simple si se cuentan con todos los elementos. Ésta consiste en dos partes, la primera en el proceso de cifrado y la segunda en el proceso de generación de las sub-claves, una primera aproximación se muestra la siguiente figura:

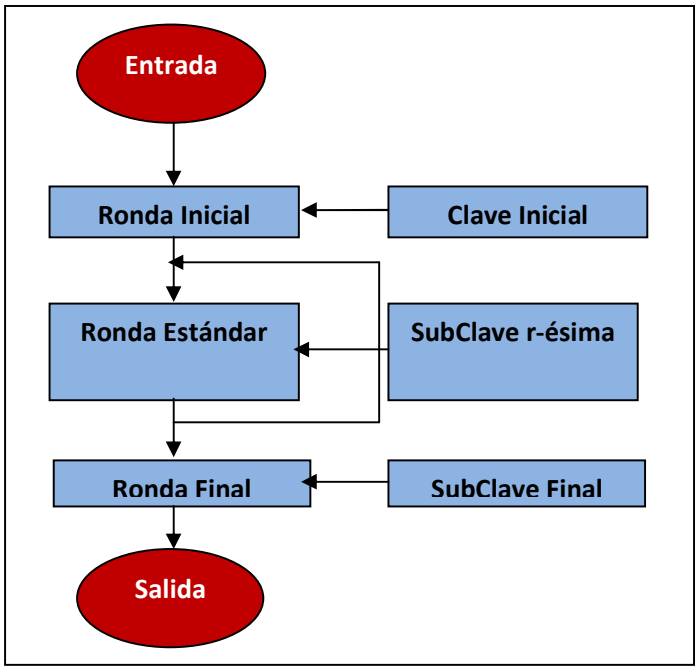

Figura 15 .- Proceso de cifrados.

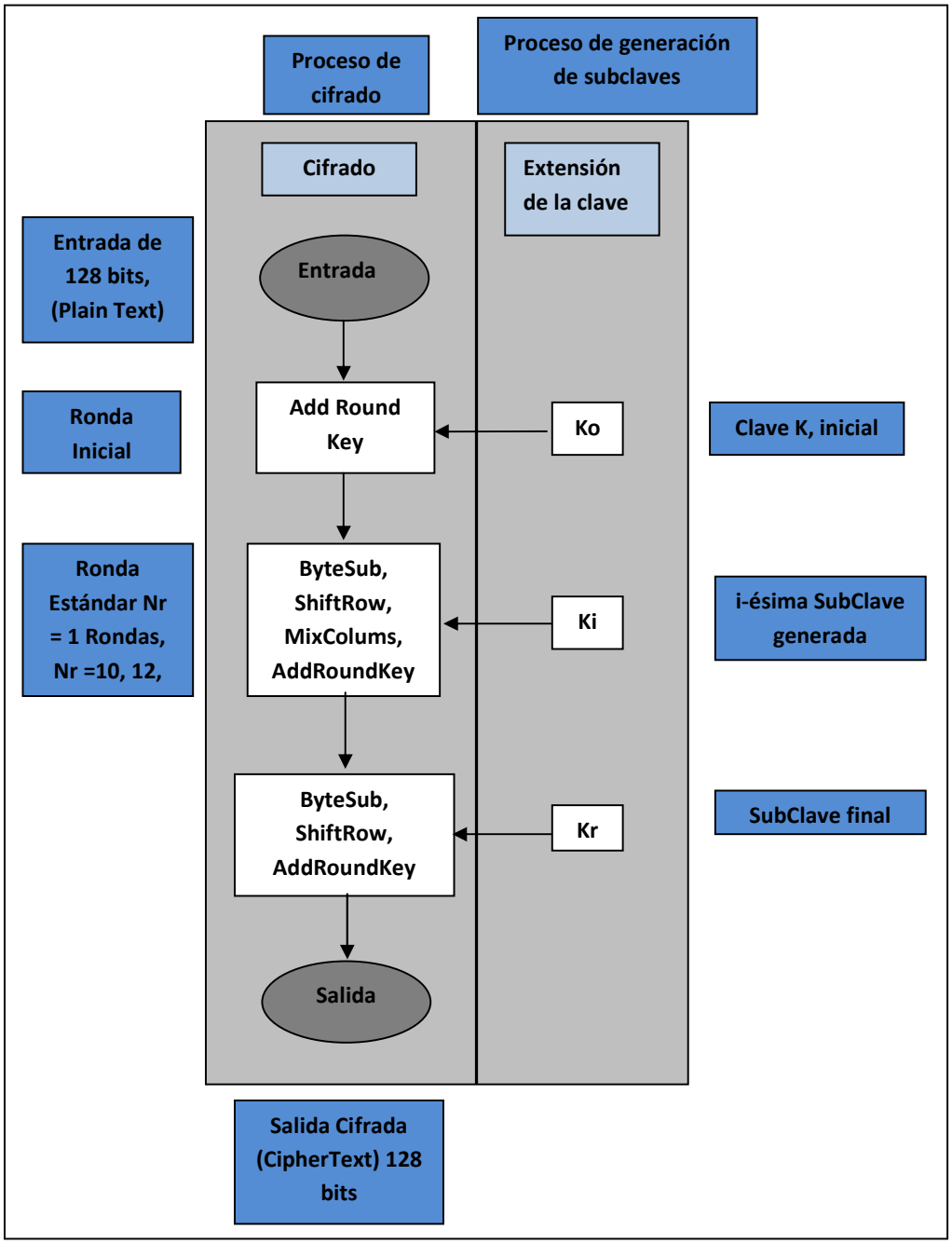

Figura 16 .- Generación de subclaves.

AES consiste de dos partes, en describir el proceso de “Cifrado”, y el proceso de “Generación de las subclaves” o “Extensión de la clave K”.
El bloque de cifrado tiene una longitud de 128 bits, la longitud de la clave K varia de 128, 192 y 256 bits, en cada caso AES tiene 10,12, y14 rondas respectivamente.

El proceso de cifrado consiste esencialmente en la descripción de las 4transformaciones básicas de AES: ByteSub, ShiftRow, MixColumns, yddRoundKey. Es importante mencionar que el caso de Rijndael las funciones o transformaciones básicas son ligeramente diferentes en el proceso descifrado, sin embargo es poco el esfuerzo necesario para poder comprender todo.

(Componentes de Seguridad, 2009).

Baby AES

Como una primera vista al algoritmo AES se puede utilizar esta versión simplificada la cual es conocida como Baby-AES, tiene la misma estructura que AES por lo tanto, puede ayudar a comprender con mayor facilidad la descripción completa de AES.

El algoritmo Baby-AES opera sobre un texto de 16 bits, y genera un texto cifrado de 16 bits, con una clave de 16 bits. Baby-AES consiste en dos procedimientos, el de cifrado dónde se aplican 4 funciones básicas tantas veces como se desee y el proceso de la derivación de las sub-claves llamado programa de claves, la idea de hacer una versión simplificada ha sido usada como un primer vistazo al algoritmo, pero también una manera de cripto-analizarlo, es decir, intentar un ataque en la versión simplificada para después extenderlo a la versión completa.

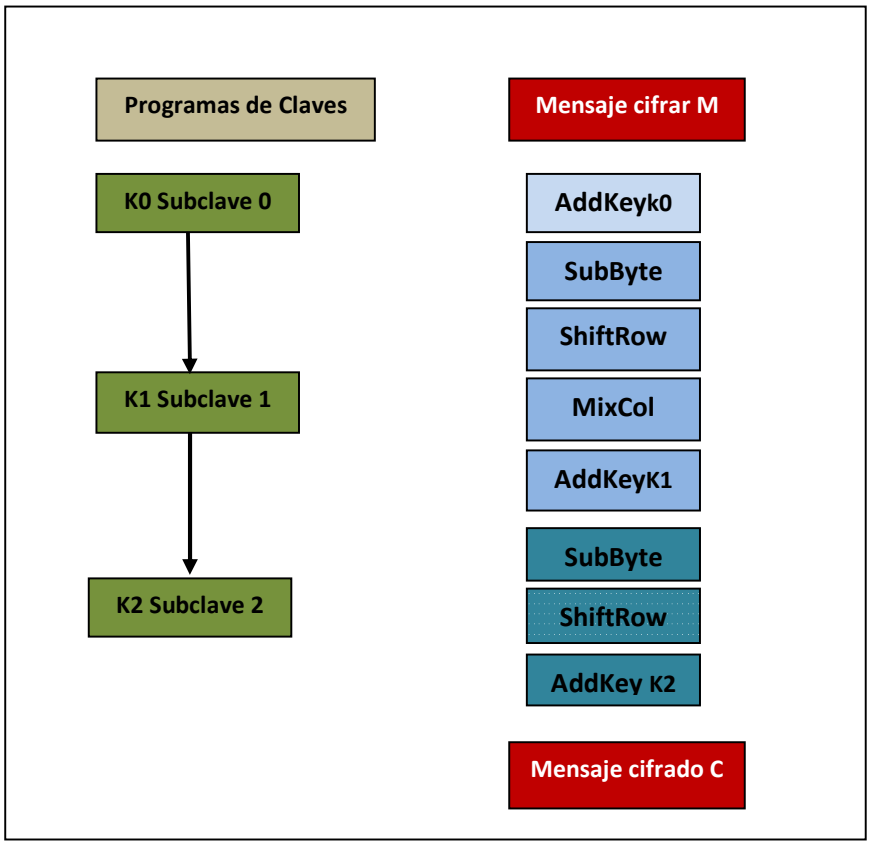

Figura 17.- Funcionamiento del Baby AES.

(Componentes de Seguridad, 2009).

IDEA

IDEA usa una clave de 128 bits. Difiere notablemente del DES en la función de etapa así como en la función de generación de subclaves. Para la función de etapa el IDEA no usa cajas S, sino que cuenta con tres operaciones matemáticas diferentes: XOR, suma binaria de enteros de 16 bits, y multiplicación binaria de enteros de 16 bits. Esas funciones se combinan de tal

forma que producen una transformación compleja muy difícil de analizar, y por ende muy difícil para el criptoanálisis.

El algoritmo de generación de sub-claves se basa solamente en el uso de desplazamientos circulares pero ejecutados de manera compleja para generar un total de seis sub-claves para cada una de las ocho etapas del IDEA. Debido a que IDEA fue uno de los primeros algoritmos de 128 bits de los propuestos para remplazar al DES, ha sido sometido a considerables exámenes y por ahora parece ser muy resistente al criptoanálisis. IDEA se usa como una alternativa en PGP (Pretty Good Privacy) y también en una serie de productos comerciales.
(Componentes de Seguridad, 2009).

Blowfish

Blowfish consiguió ser rápidamente una de las alternativas más populares al DES. Se diseñó para que fuera fácil de implementar y rápido en su ejecución.

También es un algoritmo muy compacto que puede ejecutarse en menos de 5K de memoria. Una característica interesante es que la longitud de la clave es variable, pudiendo alcanzar hasta los 448 bits. En la práctica se usan claves de 128 bits. Blowfish usa16 etapas, utiliza cajas S y la función XOR, como el DES, pero también utiliza sumas binarias. Al contrario que el DES, que utiliza cajas S estáticas, Blowfish usa cajas S dinámicas generadas como una función de la clave. Las subclaves y las cajas S se generan por la aplicación repetida del propio algoritmo a la clave. Se necesita un total de 521 ejecuciones del algoritmo de cifrado Blowfish para producir las subclaves y las cajas S. Por este motivo no es adecuado para aplicaciones en las que la clave secreta cambia frecuentemente.

Este es uno de los algoritmos de cifrado simétrico más robusto hasta la fecha, porque tanto las sub-claves como las cajas S se generan por un proceso de aplicaciones repetidas del propio algoritmo, lo cual modifica totalmente los bits haciendo muy difícil el criptoanálisis. Hasta ahora, se han publicado algunos artículos sobre Blowfish, sin que se hayan encontrado debilidades.

(Componentes de Seguridad, 2009).

RC5

RC5 se diseño para tener las siguientes características:

- *Adecuado para hardware y software*: solo usa operaciones computacionales primitivas que se encuentran comúnmente en los microprocesadores.
- *Rápido*: para conseguir esto, RC5 es un algoritmo simple y orientado a palabras. Las operaciones básicas procesan palabras enteras de datos cada vez.
- *Adaptable a procesadores con diferentes tamaños de palabra*: el número de bits en una palabra es un parámetro del RC5; diferentes longitudes de palabra producen algoritmos diferentes.
- *Número variable de etapas*: el número de etapas es un segundo parámetro. Esto permite alcanzar un compromiso entre mayor rapidez y mayor seguridad.
- *Longitud de clave variable*: la longitud de la clave es un tercer parámetro. Otra vez, posibilita un acuerdo entre velocidad y seguridad.
- *Simple*: la estructura simple del RC5 es fácil de implementar y facilita la tarea de determinar la robustez del algoritmo.
- *Bajo consumo de memoria*: la poca necesidad de memoria hace que el RC5 sea adecuado para tarjetas inteligentes y otros dispositivos con restricciones de memoria.

- *Alta seguridad*: proporciona alta seguridad con los parámetros adecuados.
- *Rotaciones dependientes de los datos*: incorpora rotaciones (desplazamientos circulares de bits) cuya cantidad depende de los datos. Esto parece fortalecer el algoritmo contra el criptoanálisis.

Algoritmo	Tamaño de clave (bits)	Tamaño de bloques (bits)	Número de etapas	Aplicaciones
DES	56	64	16	SET, Kerberos.
Triple DES	112 ó 168	64	48	Financial Key management, PGP, S/MIME
AES	128, 192, 256	128	10, 12, 14	Destinados a sustituir DES y 3Des.
IDEA	128	64	8	PGP.
Blowfish	Variable hasta 448	64	16	Varios paquetes de software.
RC5	Variable hasta 2040	64	Variable hasta 255	Varios paquetes de software.

Tabla 4.- Tabla comparativa de los Algoritmos de cifrados convencional.

(Componentes de Seguridad, 2009).

7.- Conclusiones

La seguridad en las redes inalámbricas es un aspecto muy importante a mencionar que no podemos descuidar. Debido a que las transmisiones por medios no guiados de voz y datos viajan por un medio no seguro; se requieren diversos tipos de mecanismos que proporcionen confidencialidad, integridad y autenticidad de los datos que viajen a través de la red.

El uso de los protocolos de estandarización (WEP, WPA, WPA2) así como el manejo de criptografía simétrica, es una medida de seguridad comúnmente utilizada pero que no garantiza confidencialidad punto-a-punto, sino solamente proporcionan una mayor protección a nuestra red inalámbrica.

Si se necesita seguridad a nivel de capa de enlace, se debe suprimir o eliminar el uso de WEP y únicamente utilizar WPA ó WPA2, así como los propios algoritmos de cifrados simétricos (DES, Triple Des, AES, IDEA, Blowfish y RC5) y otras herramientas importantes (EAP, TKIP, CCMP, MIC y MAC, etc.) según la implementación y nivel de seguridad que se desee tener.

Una red puede ser deficiente como resultado de ataques de servicios o de software malicioso, pero también debido a nodos ocultos. Así como también presentar problemas de interferencias en la señal inalámbrica. Solo mediante el monitoreo constante del tráfico de red se pueden encontrar las causas reales de la problemática en la red inalámbrica.

A través de este trabajo monográfico se fueron cumpliendo cada uno de los objetivos planeados con anterioridad dado de que se analizó de forma clara y concisa el funcionamiento de los protocolos de estandarización, también se

realizó una comparativa mostrando sus características, ventajas y desventajas, así como la criptografía simétrica que nos proporcionaron entendimiento acerca de cómo manejar las distintas claves que nosotros generemos y administremos en las red(es) inalámbrica(s) para hacerlas más seguras a través de procesos de encriptación.

Cabe recordar que los algoritmos de encriptación también son de vital importancia para el funcionamiento y entendimiento de los protocolos de estandarización que fueron explicados detalladamente en este trabajo bajo el estándar IEEE 802.11.

En lo particular, por medio de la realización de este trabajo entendí el funcionamiento de los protocolos de estandarización (WEP, WAP y WAP2), y pude diferenciar sus ventajas, desventajas, así como sus características. Una forma de entender el funcionamiento de cada uno de los protocolos es por ejemplo que todos utilizan un vector de inicialización; el primero de 24 bits y los otros dos de 48 bits; entendiendo que el funcionamiento del vector es permitir el paso de un cifrado ya sea en flujo o por bloques de bits. También otro punto a resaltar es que cada uno de ellos maneja diferentes tipos de algoritmos y sobre todo de protocolos dando a entender que el enfoque de seguridad de los tres es muy diferente, siendo el más utilizado el WAP, pero siendo el más seguro WAP2.

Para entender claramente estos protocolos de estandarización, tuve que enfocarme a los algoritmos de cifrados simétricos (DES, Triple Des, AES, IDEA, etc.) así como a otros protocolos y herramientas (EAP, TKIP, CCMP, MIC y MAC, etc.), debido a que son parte fundamental para entender de forma clara y concisa los protocolos de estandarización que nos permiten lograr una red inalámbrica más segura.

8.- Glosario

ACL (Access Control List): Es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

AES (Advanced Encryption Standard): También conocido Rijndael. Esquema de cifrado por bloques, que fue adoptado como estándar de cifrado por el gobierno estadounidense. Reemplaza progresivamente a su predecesor (DES y Triple DES). AES es uno de los algoritmos más utilizados en criptografía simétrica.

Fue anunciado el 26 de noviembre de 2001 por el NIST (Instituto Nacional de Estándares y Tecnología), luego de un proceso de estandarización que duró 5 años. Se transformó en estándar el 26 de mayo de 2002. El cifrador fue desarrollado por Joan Daemen y Vincent Rijmen, dos criptólogos de Bélgica, estudiantes de la Universidad Católica de Leuven.

AES también es mucho más rápido que DES, tanto en hardware como en software y además, requiere poca memoria.

(Diccionario Informático, 2008).

Algoritmo Hash: Algoritmo que se utiliza para generar un valor de hash para algún dato, como por ejemplo claves. Un algoritmo de hash hace que los cambios que se produzcan en los datos de entrada provoquen cambios en los bits del hash. Gracias a esto, los hash permiten detectar si un dato ha sido modificado. Un algoritmo de hash eficiente convierte en un imposible computacional la creación de 2 entradas diferentes (por ejemplo, 2 claves diferentes o 2 correos electrónicos diferentes) que tengan el mismo hash.

Entre los algoritmos de hash más comunes están:

- SHA-1: Algoritmo de hash seguro. Algoritmo de síntesis que genera un hash de 160 bits. Se utiliza, por ejemplo, como algoritmo para la firma digital.
- MD2 y MD4: Algoritmos de hash que generan un valor de 128 bits.
- MD5: Esquema de hash de hash de 128 bits muy utilizado para autenticación cifrada. Gracias al MD5 se consigue, por ejemplo, que un usuario demuestre que conoce una contraseña sin necesidad de enviar la contraseña a través de la red.

(Cibernetía, 2008).

Checksum: Es una redundancia comprobar durante el proceso de arranque de un ordenador, que se asegura de que un ordenador de datos está intacta. Los datos se escanean y se realizarán las pruebas de la exactitud, ya sea sobre la base de qué tan bien se refiere a los datos en otro lugar o sobre la base de datos anteriores que estaba almacenada en el mismo equipo.

En esencia, todos los bits de datos en un documento o archivo se suman y un número o hash es creado. Este número de hash o puede ser en comparación con el número de hash o generados por el mismo archivo a otra persona la computadora o en un tiempo anterior en el mismo equipo.

(TECH-FAQ, 2008).

Clave pública (PKI): Es un protocolo que describe los procesos organizativos necesarios para la gestión de certificados digitales de claves públicas, para el intercambio seguro de información.

(Kioskea.net, 2009).

CNAC (Closed Network Access Control): Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.

(Saulo.Net, 2008).

CRC-32: Es el método que propone WEP para garantizar la integridad de los mensajes (ICV, Integrity Check Value).

(Saulo.Net, 2008).

Direcciones MAC: Identificador hexadecimal de 48 bits que corresponde de forma única a una tarjeta de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el OUI. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64 las cuales han sido diseñadas para ser identificadores globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

La dirección MAC es utilizada en varias tecnologías entre las que se incluyen:

- Ethernet.
- 802.5 o Redes Anillo a 4 Mbps ó 16 Mbps Token Ring.
- 802.11 Redes Inalámbricas (WIFI).
- ATM.

(Scribd, 2008)**.**

FreeBSD: Es un avanzado sistema operativo para arquitecturas x86 compatibles (incluyendo Pentium® y Athlon™), amd64 compatibles (incluyendo Opteron™, Athlon™64 y EM64T), Alpha/AXP, IA-64, PC-98 y UltraSPARC®. FreeBSD es un derivado de BSD, la versión de UNIX® desarrollada en la Universidad de California, Berkeley. FreeBSD es desarrollado y mantenido por un numeroso equipo de personas. El soporte para otras arquitecturas está en diferentes fases de desarrollo.

(FreeBSD The Power to Server, 2008).

Kismet: Es un sniffer, detector de redes inalámbricas y IDS, que permite trabajar con la tarjeta inalámbrica en modo Monitor (promiscuo). Sin duda es el mejor de su tipo.*[Usando Kismet y Airclack-ng para adivinar, descubrir y exponer claves WEP.*

MIC (Message Integrity Code) o Michael: Código que verifica la integridad de los datos de las tramas.

(Saulo.Net, 2008).

Modulación DSSS ("Direct Sequence Spread Spectrum")

El espectro ensanchado (SS) es una técnica de transmisión en la cual un código pseudoaleaotorio, independiente de los datos de información, es empleado como forma de onda modulante para “desparramar” la energía de la señal sobre un ancho de banda mucho mayor que el ancho de banda de información de la señal original.

(Transmisión de datos de red eléctrica., 2009).

Modulación OFDM (Orthogonal Frequency Division Multiplexing)

El origen del OFDM es en la década de los 50/60 en aplicaciones de uso militar que trabajan dividiendo el espectro disponible en múltiples sub-portadoras.

OFDM es una tecnología de modulación digital, una forma especial demodulación multi-carrier considerada la piedra angular de la próxima generación de productos y servicios de radio frecuencia de alta velocidad para uso tanto personal como corporativo.

(Transmisión de datos de red eléctrica., 2009).

NetBSD: Es un sistema operativo tipo Unix que es el resultado de un esfuerzo colaborativo entre diferentes grupos de personas. Es de código abierto y libre distribución. El objetivo de sus desarrolladores es crear un sistema operativo sumamente portable para un gran número de plataformas de hardware. La primera versión de NetBSD fue lanzada en abril de 1993.

(Diccionario Informático, 2008).

OpenBSD: Sistema operativo tipo UNIX, multiplataforma y descendiente del BSD (un sistema basado en Unix desarrollado en la Universidad de California). Es un descendiente de NetBSD y se destaca por la seguridad, la corrección del código, la calidad de la documentación y la insistencia en el código abierto.

OpenBSD es libre y gratuito, permitiéndose la libre distribución para uso personal y comercial. Fue fundada en 1995 por Theo de Raadt y su primer lanzamiento fue en julio de 1996. OpenBSD está disponible para plataformas como AMD64, i386, MIPS, 68000, PowePC, SPARC 32/64, VAX, Zaurus, etc.

(Diccionario Informático, 2008)**.**

OSA (Open System Authentication) y SKA (Shared Key Authentication): Cualquier interlocutor es válido para establecer una comunicación con el AP. SKA (Shared Key Authentication) es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación, entonces, el dispositivo TR pide al AP autenticarse. El AP le envía una trama al TR, que si éste a su vez devuelve correctamente codificada, le permite establecer Comunicación

(Taringa, 2009).

Portscanning: Una forma de decir escanear los puertos.

Pingscannig: Una forma de decir escanear los pings (o las direcciones).

RADIUS: Significa "Remote Authentication Dial User Services, que es un procedimiento de sistema y ofrece acceso centralizado, aprobación, así como administración de contabilidad para las personas o equipos para agregar y utilizar un servicio de red.

(TECH-FAQ, 2008).

RC4: Es un simétrico de cifrado de flujo con un tamaño de clave arbitraria. RC4 fue creada por Ron Rivest de RSA Security en 1987. RC4 se utiliza en muchas aplicaciones, incluyendo TLS (Transport Layer Security), WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), TKIP (Temporal Key Integrity Protocol), Microsoft XBOX, Oracle SQL, Microsoft PPTP, Microsoft Office , y Adobe Acrobat.

(TECH-FAQ, 2008).

Servidor IAS: IAS es la implementación de Microsoft de un servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota) y proxy que permite la administración centralizada de las operaciones de autenticación y

autorización, así como de las cuentas de los usuarios. IAS se puede utilizar para autenticar a los usuarios en bases de datos de Windows Server 2003, Windows NT® 4.0 o controladores de dominio de Windows 2000. IAS también admite una variedad de servidores de acceso a red (NAS), incluidos los servidores de enrutamiento y acceso remoto (RRAS.

(Technet, 2009).

Socket: Proporcionan una comunicación de dos vías, punto a punto entre dos procesos. Los sockets son muy versátiles y son un componente básico de comunicación entre inter procesos e inter sistemas. Un socket es un punto final de comunicación al cual se puede asociar un nombre. Este tiene un tipo y uno o más procesos asociados.

Los sockets existen en los dominios de comunicación. Un socket de dominio es una representación que da una estructura de direccionamiento y un conjunto de protocolos. Los sockets se conectan solamente con sockets en el mismo dominio [Comunicación entre procesos.

(Sockets, 2005).

SSID (Service Set IDentifier): Es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica. Los TRs deben conocer el nombre de la red para poder unirse a ella.

9.- Abreviaturas o acrónimos

ACL: Access Control List. (Lista de Control de Acceso).

AES: Advanced Encryption Standard. (Estándar de encriptación Avanzada).

DES: Data Encryption Standard. (Estándar de encriptación de Dato).

CCMP: Counter Mode With CBC – MAC

CNAC: Closed Network Access Control (Control de Acceso a Redes Cerradas).

GNSA: Generador de Números Seudo-Aleatorios.

GTK: Group Transient Key (Llave Transitorio de Grupo).

IAS: Internet Authentication Service (Servicio de Autenticación de Internet).

IV: Vector de Inicialización

MAC: Message Authentication Code (Código de Autenticación de Mensaje).

MIC: Message Integrity Code. (Código de Integridad de Mensaje).

OSA: Open System Authentication. (Sistema de Autenticación Abierta).

PSK: PRE-Shared Key (Llave Pre-Compartida).

PTK: Pairwise Transient Key (Llave Transitorio en Parejas).

RADIUS: Remote Authentication Dial User Services (Protocolo de Autenticación y Autorización para Aplicaciones de Acceso a la Red).

SKA: Shared Key Authentication. (Intercambio de autenticación de llaves)

SSID: Service Set Identifier. (Sistema Identificador de Servicio).

TKIP: Temporal Key Integrity Protocol (Protocolo Temporal de Llave de Integridad).

10.- Bibliografía

Cibernetía. (2008). Recuperado el Marzo de 2009, de http://www.cibernetia.com/enciclopedia/algoritmo_de_hash

Componentes de Seguridad. (2009). Recuperado el 23 de Marzo de 2009, de http://www.matem.unam.mx/~rajsbaum/cursos/web/resumen_seguridad_1.pdf

Cursos gratis de Redes Inalámbricas (Conceptos básicos de tecnología WIFI y best practices de Seguridad en Redes Inalámbricas). (2006). Recuperado el Febrero de 2009, de http://www.virusprot.com/cursos/Redes-Inalámbricas-Curso-gratis9.htm

DELL. (2009). Recuperado el 23 de Marzo de 2009, de http://support.dell.com/support/edocs/network/P65126/sp/glossary.htm

Diccionario Informático. (2008). Recuperado el Marzo de 2009, de http://www.alegsa.com.ar

FreeBSD The Power to Server. (2008). Recuperado el Marzo de 2009, de http://www.freebsd.org/es/about.html

HP. (2008). Recuperado el 11 de Mayo de 2009, de http://docs.hp.com/es/5992-3422/go01.html

IEEE Standards Association. (2008). Recuperado el 2008, de http://standards.ieee.org/getieee802/802.11.html

Instituto Tecnológico de Aguascalientes. (Diciembre de 2006). Recuperado el Abril de 2008, de http://desacad.ita.mx/contec/num_32/rev32-11.pdf

Kioskea.net. (2009). Recuperado el Marzo de 2009, de http://es.kioskea.net/contents/crypto/pki.php3

Microsoft Tech Net. (2009). Recuperado el Abril de 2008, de http://technet.microsoft.com

piurawifi.com. (Marzo de 2008). Recuperado el Abril de 2008, de http://piurawifi.org/proyecto/estandarwifi.htm

Saulo.Net. (2008). Recuperado el 2008, de http://www.saulo.net/pub/inv/SegWiFi-art.htm

Schneir, B. (1996). Vector de Inicialización. En B. W. Shneir, *Criptografía Aplicada.*

Scribd. (2008). Recuperado el Marzo de 2009, de http://www.scribd.com/doc/2086576/Direccion-MAC

Seguridad Informática en 802.11. (2006). Recuperado el 25 de Marzo de 2009, de http://edigital.k4k3k4.com/Docs/802.11/Seguridad/Seguridad%20en%20802.11v0.2.pdf

Sockets. (2005). Recuperado el Marzo de 2009, de http://www.fismat.umich.mx/mn1/manual/node24.html

Taringa. (2009). Recuperado el Marzo de 2009, de http://www.taringa.net/posts/downloads/1940755/Cursos-de-redes-y-muchos-manuales.html

TECH-FAQ. (Marzo de 2008). Recuperado el 2008, de http://es.tech-faq.com

Transmisión de datos de red eléctrica. (2009). Recuperado el 17 de Julio de 2009, de http://www.victorgarcia.org/files/PLC-v2.0RC.pdf

Universidad de Buenos Aires (Departamento de computación). (2006). Recuperado el 20 de Marzo de 2009, de http://www-2.dc.uba.ar/materias/seginf/material/tp_1c2006/seguridad_redes_wireless.pdf

WIFI. (2009). Recuperado el 4 de Agosto de 2009, de http://www.manual-wifi.com/ccmp.html