UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA
UNAN-MANAGUA
RECINTO UNIVERSITARIO RUBÉN DARÍO
FACULTAD DE CIENCIAS E INGENIERÍAS
DEPARTAMENTO DE TECNOLOGÍA
INGENIERÍA EN ELECTRÓNICA

SEMINARIO DE GRADUACIÓN 2012

TEMA:

Análisis de la gestión de seguridad de los protocolos WPA y WPA2 en el tráfico de datos de una red LAN con tecnología WiFi.

Elaborado por:

Br. José Antonio Ulloa Santana

Br. Víctor Hugo Fonseca Sánchez

Tutor:

Msc. Álvaro Segovia

DEDICATORIA

Este camino largo y de esperanza,
Se lo he de dedicar a mis padres: Wilfredo y Yolanda
que con su apoyo me llevaron a superar esta mi gran meta;
Los amo mucho.
Víctor Hugo Fonseca Sánchez

Especialmente a mi madre Modesta Santana,
por ser mí apoyo, ejemplo y fortaleza siempre,
a toda mi familia que siempre confió en mí;
Los quiero.
José Antonio Ulloa Santana

AGRADECIMIENTO

A DIOS por su amor y bendiciones siempre;
a nuestros padres por el apoyo incondicional
en cada etapa de nuestras vidas.
A todos los docentes que ayudaron
en nuestra formación profesional

Gracias!

INDICE DE CONTENIDO

INDICE DE FIGURAS Y TABLAS

RESUMEN

Este documento pretende explicar paso a paso el sistema utilizado por los protocolos de seguridad de acceso e intercambio de datosWPA Y WPA2 utilizados por el sistema de comunicaciones WiFi.

En primera instancia, debemos comprender el funcionamiento y régimen que lleva consigo una red LAN, tratando de enfocarnos en lo que es la tecnología WiFi. Hablaremos de los estándares que rigen la tecnología WiFi y su evolución lo cual nos permite tener una introducción al tema principal y que veremos reflejado en lo que llamamos el Capítulo 1.

En el capítulo 2, llevamos a cabo la explicación del funcionamiento y gestión que realizan los protocolos WPA y WPA2, los cuales utilizan sistemas conocidos e implementados desde hace muchos años y aplicados a lenguaje de computadora como es la encriptación y la autenticación que serán las principales herramientas en la defensa de una red WiFi.

El paso a seguir ahora, será, el de identificar los ataques que podemos tener en nuestra red casera o empresarial, puesto que desde la implementación de las redes inalámbricasse han generado una serie de ataques con enfoque malicioso,por lo que es indispensable el uso de sistemas de protección.También mostraremos la gestión y los pasos que debemos seguir para minimizar estos riesgos.

INTRODUCCIÓN

Las redes de computadoras, han constituido una gran herramienta en las comunicaciones modernas, tanto telefónicas, como computacionales, en especial con la implementación de las redes inalámbricas, las cuales se han logrado volver una gran oportunidad de crecimiento por su viabilidad tanto económica como de cobertura y movilidad. No obstante, la aparición de estos nuevos servicios implica nuevas necesidades y requerimientos, entre los cuales uno de los más críticos es la seguridad.

El problema de la seguridad, ve su enfoque de acuerdo a la necesidad en cuanto a mantener la información resguardada. Una red inalámbrica publica no necesita alta seguridad de acceso para el usuario, en cambio una red empresarial tiene que tener un alto nivel de autenticación, debido a la información confidencial que posee y hasta una red doméstica necesita una manera de resguardar su integridad y tenemos que tener muy en cuenta que estas pueden estar sujetas a ataques e infiltraciones no autorizadas, lo que todos conocemos es más común en sistemas inalámbrico que en los cableados.

Podemos dividir la seguridad en las redes inalámbricas en dos categorías: la seguridad al momento de autenticar los usuarios e identificar sus correspondientes permisos, y la seguridad al momento de transmitir los datos entre dispositivos inalámbricos usando ondas de radio.

La mayor parte de las acciones a desarrollar para la planificación de la seguridad deben de realizarse a partir del conocimiento claro que se tenga del funcionamiento y los objetivos particulares de los protocolos relacionados con la protección de los datos.

Centraremos el trabajo en los protocolos de seguridad WPA Y WPA2, utilizados en sistemas de comunicaciones inalámbricas que utilizan la tecnología WiFi. Describiremos mecanismos, características, y medios utilizados por estos protocolos para la defensa de las redes**.**

ANTECEDENTES

En los últimos años una de las tecnologías que más ha evolucionado son las Redes de área local inalámbricas (Wireless Local Área Networks), las cuales tienen la funcionalidad de brindar conexión a una Red de computadoras local o a internet sin necesidad de una conexión física, como sucedía con las redes cableadas. Sin embargo desde su estandarización uno de los grandes retos que presentó fue la seguridad, puesto que son más difíciles de proteger debido a que utilizan ondas de radio y por tanto el espacio libre como medio de transmisión.

Para enfrentar esta problemática de las redes inalámbricas el instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers, IEEE) manifestó mecanismos de encriptación y autenticación en su estándar 802.11, en 1999. Sin embargo, en 2001 fueron publicados una serie de documentos que evidenciaban vulnerabilidades en este mecanismo de encriptación y ponían en duda la seguridad de las redes WiFi, puesto que el método de autenticación del estándar 802.11 no era el más seguro.

Para solucionar esta problemática y las necesidades de seguridad en redes inalámbricas el IEEE público su estándar certificado 802.11i en 2004, el cual presentaba mejoras significativas para la seguridad, como era la incorporación de una capa de seguridad especifica.

Siendo la seguridad uno de los grandes inconvenientes en las comunicaciones inalámbricas no ha sido un obstáculo para el crecimiento en masa que ha tenido la tecnología WiFi en los últimos años y se estima que siga en crecimiento, puesto que los equipos portátiles representan una amplia facilidad de movilidad y estabilidad.

JUSTIFICACIÓN

Sabemos que la seguridad en las redes, en especial en las que usan la tecnología WiFi, es un tema aun en desarrollo, ya que actualmente no se dispone de normas de trabajo para la gestión de seguridad que cumplan con todos los requerimientos específicos para cubrir todas las necesidades de quienes utilizan las redes de telecomunicaciones modernas WiFi para cualquier tipo de ataques, y es por eso que le damos la importancia de la aplicación de protocolos que se han desarrollado hasta ahora para ese propósito.

Las debilidades de las tecnologías inalámbricas y más en concreto de la tecnología WiFi son la falta de seguridad atribuida más que a la seguridad física, a la seguridad de la información, su integridad y la no accesibilidad a terceros.

La idea de centrarse en los protocolos WPA y WPA2, es debido a que son protocolos que en la actualidad tienen las mejores herramientas en el sistema de accesibilidad que tienen las redes Wi Fi, protocolos que con el tiempo han realizado mejoras en su utilidad y aplicaciones en comparación a su predecesor WEP.

En WPA y WPA2 se definen características que los hace capaces de resguardar cualquier red tanto pública como privada, tomando en cuenta que cada uno se ha diseñado de manera que atienda las necesidades de los tipos de redes WiFi mencionadas.

Con este estudio se pretende analizar el funcionamiento de estos protocolos para la gestión de seguridad de redes Wi-Fi, como una forma de organizar las labores de seguridad no como una combinación de mecanismos de defensa sino, como un estudio continuo de planificación, implantación y mantenimiento de la seguridad de la red.

OBJETIVOS

Objetivo general:

Analizar el funcionamiento de los protocolos de seguridad WPA y WPA2 en el tráfico de datos de las redes LAN con tecnología WiFi.

Objetivos específicos:

- Evaluar la evolución de la seguridad en redes inalámbricas con tecnología WiFi.
- Describir el funcionamiento general de los protocolos WPA y WPA2, determinando los métodos para la prevención y protección de amenazas.
- Presentar los posibles ataques que sufren las redes WiFi e indicar las deficiencias en la seguridad que puedan presentar los protocolos WPA y WPA2.

CAPITULO 1

SEGURIDAD EN REDES LAN

1.1 LAS REDES

Cuando se hace mención a una "red" estamos hablando de un conjunto de entidades ya sea (personas, objetos, etc.) que se encuentren interconectadas. En definición una red nos da a entender que en dichas entidades se dará un intercambio y/o retroalimentación de elementos materiales o inmateriales según como se dé el caso.

Una red es un conjunto de ordenadores conectados entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los distintos dispositivos. A través de una red se puede ejecutar procesos en otro ordenador o acceder a sus ficheros, enviar mensajes, compartir programas.

La tendencia de las *redes de área local LAN* implica el uso de medios de transmisión o conmutación compartidos para lograr altas velocidades de transmisión de datos en distancias relativamente cortas. Conceptos como medios de transmisión, topologías y técnicas de control de acceso al medio surgen por sí mismos.

La industria de las redes LAN en cuanto a comunicación de datos se refiere, ha sido la que mayor crecimiento ha tenido; esto se debe a que las empresas en su afán de automatizarse han escogido esta tecnología que les brinda facilidad de compartir recursos tanto de hardware como de software, sus altas velocidades aseguran a las empresas un incremento en su eficiencia y productividad.

1.1.1 Aplicaciones de las redes LAN

Las redes LAN constituyen la base de casi todas las redes de comunicación de datos comerciales, por tanto, a medida que se ha ampliado el campo de aplicaciones de las LAN también ha crecido lo que se exige de ellas en términos de volumen de transmisión de datos y confiabilidad.

La aplicación más extendida de las redes LAN es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. Por otra parte, algunas de las áreas de aplicación generales más importantes de este tipo de redes son:

- **Redes LAN de computadores personales**

Una configuración de red LAN común es aquella que consta de computadores personales. Con frecuencia, algunos gerentes administradores adquieren PC´s personales para aplicaciones departamentales como hojas de cálculo, herramientas de gestión de proyectos y acceso a Internet; esto debido al bajo costo del sistema.

Este conjunto de procesadores departamentales no cubren todas las necesidades de un organismo ya que muchos de los programas usados para sus actividades diarias son demasiado grandes para una PC, requiriendo por tanto, de un proceso centralizado y al mismo tiempo que sea accesible para distintos usuarios. Los miembros del equipo de un proyecto u organismo necesitan compartir trabajo e información, resultando eficiente el uso de la tecnología digital para hacerlo.

Recursos caros como una impresora láser puede ser compartida por todos los usuarios de la red LAN, esta puede ser a nivel de edificio; además la red puede servir de nexo entre servicios de red corporativos mayores. Un servidor de comunicaciones puede dar acceso controlado a estos recursos.

- **Redes de respaldo y almacenamiento**

Las redes de respaldo conectan grandes sistemas como computadoras centrales, supercomputadores y dispositivos de almacenamiento masivo en un espacio reducido con una transferencia elevada de datos en un número limitado de dispositivos.

Permiten manejar adecuada y eficazmente la información que se genera constantemente dentro de una empresa, sin excederse en sus presupuestos establecidos, es uno de los mayores retos que las organizaciones tienen hoy en día.

Características:

- *Alta velocidad*: para satisfacer la de demanda de volumen de tráfico, precisan velocidades de 100 Mbps o más.

- *Interfaz de alta velocidad*: se usa interfaces de entrada/salida en paralelo de alta velocidad debido a las operaciones de transferencia de datos. El enlace físico entre la estación y la red debe ser de alta velocidad.

- *Acceso distribuido*: permite que varios dispositivos compartan el medio mediante un acceso eficiente y fiable.

- *Distancia limitada*: las redes de respaldo se emplean en salas de computadoras.

- *Número limitado de dispositivos*: es el número de computadoras principales o dispositivos de almacenamiento. Están en el orden de las decenas.

- **Redes LAN troncales**

El uso de aplicaciones y computadores personales provoca la necesidad de una estrategia flexible para el uso de redes LAN. El soporte de comunicaciones de datos entre oficinasprecisa de un servicio de red capaz de cubrir distancias e interconectar equipos situados en uno o varios edificios.

El uso de una única LAN presenta varios inconvenientes, aunque es posible desplegar una sola LAN para interconectar todos los equipos de procesamiento de datos necesarios en una oficina. Los inconvenientes de usar una única LAN pueden ser:

- *Fiabilidad:* una interrupción del servicio podría provocar un trastorno importante para los usuarios.

- *Capacidad*: la red LAN se podría saturar si el número de dispositivos de la red crece con el tiempo.

- *Coste*: una única LAN no es óptima para los numerosos requisitos de interconexión y comunicación. Las redes que admiten conexiones de muy bajo coste no son adecuadas para satisfacer los requisitos globales.

1.2 REDES LAN: INALÁMBRICA

Una LAN inalámbrica es una red en donde un usuario móvil puede conectarse a una LAN a través de enlaces de radiofrecuencia sin cables. La norma IEEE 802.11 especifica las tecnologías WLAN.

La tecnología LAN Inalámbrica le ofrece a las Empresas en Crecimiento la posibilidad de tener redes sin problemas, que sean rápidas y fáciles de configurar. En la figura 1.1 se muestra una configuración sencilla de una red LAN inalámbrica.

Figura. 1.1. Red Inalámbrica sencilla

1.2.1Tecnologías

- **HiperLAN2 (*High Performance Radio LAN 2.0*)**

Estándar europeo desarrollado por ETSI (*EuropeanTelecommunicationsStandardsInstitute*). HiperLAN2 permite a los usuarios alcanzar una velocidad máxima de 54 Mbps en un área aproximada de cien metros y transmite dentro del rango de frecuencias de 5150 y 5300 MHz.

Las LAN inalámbricas se clasifican generalmente de acuerdo con la técnica de transmisión usada. Las actuales se encuentran en las siguientes categorías:

- **Redes LAN de infrarrojos**

Las redes de luz infrarroja están limitadas por el espacio y casi generalmente la utilizan redes en las que las estaciones se encuentran en un solo cuarto o piso, algunas compañías que tienen sus oficinas en varios edificios realizan la comunicación colocando los receptores/emisores en las ventanas de los edificios.

Técnicas de transmisión

Un haz dirigido puede utilizarse para crear enlaces punto a punto, donde el alcance depende de la potencia de emisión y el grado de enfoque. Un enlace de datos IR dirigido puede alcanzar distancias de hasta kilómetros utilizando este tipo de enlace en la interconexión de edificios a través de puentes o dispositivos encaminadores entre los que haya línea de visión.

En una configuración omnidireccional existe una estación base aislada que se encuentra en la línea de visión del resto de estaciones que conforman la LAN; por lo general esta estación se ubica en el techo y actúa como un repetidor multipunto.

El transmisor del techo difunde una señal omnidireccional que es recibida por el resto de transceptores IR en la zona En una configuración de difusión todos los transmisores IR están enfocados hacia un punto en un techo reflectante. La radiación IR que alcanza el techo es reflejada omnidireccionalmente y recogida por todos los receptores en la zona.

- **Redes LAN de espectro expandido**

En la mayoría de los casos estas LAN operan en las bandas ISM que no necesitan licencia FCC para su uso en los E.E.U.U. Estas LAN hacen uso de la tecnología de transmisión de espectro expandido

Configuración

Este tipo de redes LAN hacen uso de una disposición de celdas múltiples en donde las celdas adyacentes utilizan diferentes frecuencias dentro de la misma banda para evitar interferencias. Si se usa una topología basada en un concentrador, éste puede controlar el acceso actuando como un repetidor multipunto. Por otra parte cada estación puede difundir usando una antena omnidireccional de tal forma que el resto de estaciones en la celda pueda recibir.

1.2.2 Especificaciones

- **WiFi (*IEEE 802.11*)**

Cuando hablamos de WIFI nos referimos a una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día.

La familia de especificaciones ***802.11*** para una WLAN fue desarrollada por un grupo de trabajo internacional del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) [1]. Dentro de la familia 802.11 se encuentran los estándares:

- **802.11a:** El estándar 802.11a conocido también como WiFi 5, se introdujo al mismo tiempo que 802.11b, con la intención de constituirla en la norma para redes inalámbricas para uso empresarial. Ofrece velocidades de hasta 54 Mbps, en la práctica alcanza hasta 22 Mbps, su rango de operación óptima es menor a la del 802.11b y opera en la banda de 5 GHz, Es por esto que los dispositivos 802.11a son incompatibles con los dispositivos 802.11b. Sin embargo, existen dispositivos que incorporan ambos chips, los 802.11a y los 802.11b y se llaman dispositivos de "banda dual". En la tabla 1.1 se muestra el flujo de datos del estándar 802.11a

Velocidad hipotética (en ambientes cerrados)	Rango
54 Mbit/s	10 m
48 Mbit/s	17 m
36 Mbit/s	25 m
24 Mbit/s	30 m
12 Mbit/s	50 m
6 Mbit/s	70 m

Tabla 1.1Flujo de datos802.11a

- **802.11b:** La norma ***802.11b*** (a menudo llamada Wi-Fi) es retrocompatible con la 802.11 que es la primera de toda esta familia de normas. Introducido en 1999 para redes domésticas y pequeños negocios, permite lograr una velocidad límite de 11 Mbps, tiene un rango de operación óptima de 50 metros en interiores y 100 metros en exteriores. interferencia causada por otros dispositivos. La interferencia es el factor más crítico, porque los equipos 802.11b operan en la banda libre de 2.4 GHz.

Velocidad hipotética	Rango (en ambientes cerrados)	Rango (al aire libre)
11 Mbit/s	50 m	200 m
5,5 Mbit/s	75 m	300 m
2 Mbit/s	100 m	400 m
1 Mbit/s	150 m	500 m

Tabla 1.2 Flujo de datos802.11b

- **802.11c**: El estándar combinado 802.11c 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)

- **802.11d:**El estándar 802.11d es un 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.

- **802.11e:** El 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.

- **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 deacceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.

- **802.11g:** Surgió en 2003, como una evolución del estándar 802.11b, por lo que son compatibles. Esta norma ofrece velocidades hasta de 54 Mbps en la banda de 2.4 GHz. En la tabla 1.3 se denota el flujo de datos del estándar 802.11g

Velocidad hipotética	Rango (en ambientes cerrados)	Rango (al aire libre)
54 Mbit/s	27 m	75 m
48 Mbit/s	29 m	100 m
36 Mbit/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m

Tabla 1.3 Flujo de datos802.11g

- **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.
- **802.11i:**El estándar 802.11i está destinado a mejorar la seguridad en la transferencia de datos (administrar, distribuir claves, 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.

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

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

En la tabla 1.4 se muestran las características principales de los estándares más conocidos de la familia 802.11

Estándar	Velocidad	Frecuencia de operación
802.11	2 Mb/s	2.4 GHz
802.11b	11 Mb/s	2.4 GHz
802.11a	22 Mb/s	5 GHz
802.11g	54 Mb/s	2.4 GHz

Tabla 1.4 Familia 802.11

1.2.3 Beneficios

Las redes LAN inalámbricas (WLAN) ofrecen diversas ventajas sobre las redes LAN convencionales (Ethernet, Token-Ring, fibra óptica) porque pueden ser móviles.
Los beneficios son evidentes para computadoras portátiles y computadoras de escritorio dado que el usuario puede verdaderamente trasladarse de un punto a otro y permanecer conectado a la red LAN y a sus recursos.

La red puede establecerse sin incurrir en los gastos y las exigencias de colocar cables e instalar conectores en paredes, además, las redes inalámbricas son flexibles dado que las máquinas de escritorio pueden cambiarse de lugar sin ningún trabajo de infraestructura. Esto resulta particularmente útil al instalar sitios temporales o al trabajar en lugares "fijos" que periódicamente cambian de ubicación tales como: las empresas que se trasladan a otra oficina más grande cuando exceden la capacidad de sus instalaciones actuales.

1.3 MODELO DE REFRENCIA OSI

OSI: Open System Interconnections: fue creado a partir del año 1978, con el fin de conseguir la definición de un conjunto de normas que permitieran interconectar diferentes equipos, posibilitando de esta forma la comunicación entre ellos. El modelo OSI fue aprobado en 1983. Un sistema abierto debe cumplir las normas que facilitan la interconexión tanto a nivel hardware como software con otros sistemas (arquitecturas distintas).

Este modelo define los servicios y los protocolos que posibilita la comunicación, dividiéndolos en 7 niveles diferentes, en el que cada nivel se encarga de problemas de distinta naturaleza interrelacionándose con los niveles contiguos, deforma que cada nivel se abstrae de los problemas que los niveles inferiores solucionan para dar solución a un nuevo problema, del que se abstraerán a su vez los niveles superiores. [2]

NIVELES	FUNCIÒN
Aplicación	Semántica de los datos
Presentación	Representación de los datos
Sesión	Diálogo ordenado
Transporte	Extremo a extremo
Red	Encaminamiento
Enlace	Punto a punto
Físico	Eléctrico / mecánico

Tabla 1.5 Niveles y funciones-modelo OSI

Cada capa individual del modelo OSI tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino.

1.3.1 capas del modelo OSI

Para poder simplificar el estudio y la implementación de la arquitectura necesaria, la ISO divide el modelo de referencia OSI en capas, entendiéndose por "capa" una entidad que realiza de por sí una función específica. Cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas. Esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI.

Este modelo considera 7 capas:

- Aplicación
- Presentación
- Sesión
- Transporte
- Red
- Enlace de datos
- Física [2]

La división de la red en siete capas presenta las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí de una forma totalmente definida.
- Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

En esta sección veremos con mayor énfasis la capa Transporte y la capa de Red para así ver el tráfico y luego comprender mejor la gestión de seguridad a nivel de capa.

1.3.1.1 La capa de Red

La capa de Red se ocupa de la obtención de paquetes procedentes de la fuente y de encaminarlos durante todo el camino hasta alcanzar su destino.

La función real de la capa de red consiste en el encaminamiento de paquetes, desde la maquina origen hasta la destino. En la mayoría de las subredes, los paquetes necesitaran realizar múltiples saltos para terminar el viaje. Los algoritmos que seleccionan las rutas y las estructuras de datos que utilizan representan una de las aéreas principales del diseño de la capa de red.

El funcionamiento de la red puede funcionar por datagramas o por circuitos virtuales. En pocas palabras, todo lo que a esta capa le interesa es un camino de comunicación y no la forma en que este se construye. Se necesita presentar un esquema de direccionamiento para direcciones de la red.

La función de esta capa va crucialmente ligada a la capa de transporte, esto se debe a que, en conjunción con la cuarta capa (transporte), es decir, la capa de transporte tomará parte de los datos y la capa de red se encargará de establecer el camino por donde viajarán. Otra característica interesante de esta capa es que es la capa más inferior en cuanto a manejo de transmisiones punto a punto.

1.3.1.2 La capa de Transporte

La capa de transporte ofrece a los usuarios de sus servicios un transporte extremo a extremo de los datos. Este transporte se realiza mediante un protocolo o dialogo también extremo a extremo con la entidad homóloga de la capa de transporte en el nodo destinatario.

La capa de transporte es la encargada de controlar el flujo de datos entre los nodos que establecen una comunicación; los datos no solo deben entregarse sin errores, sino además en la secuencia que proceda. La capa de transporte se ocupa también de evaluar el tamaño de los paquetes con el fin de que estos Tengan el tamaño requerido por las capas inferiores del conjunto de protocolos. El tamaño de los paquetes 10 dicta la arquitectura de red que se utilice.

1.4 LA TRAMA DEL ESTÁNDAR IEEE 802.11

Para analizar el funcionamiento de una WLAN basada en 802.11, debemos comprender los distintos tipos de paquetes que circulan y cuál es su función específica.

En forma general, podemos decir que el estándar 802.11 define una serie paquetes que son usados por los nodos y los AP para establecer la comunicación entre ellos y mantener el link entre ellos.

1.4.1 Trama MAC 802.11

El protocolo MAC del estándar IEEE 802.11 distingue tres tipos de tramas: tramas de control, de datos y de gestión. Los mensajes de gestión se utilizan para soportar los servicios de 802.11. Los mensajes de control se utilizan para la correcta entrega de tramas y los mensajes de datos transportan la información de los usuarios. En la figura 1.2 se muestra el formato de la trama IEEE 802.11

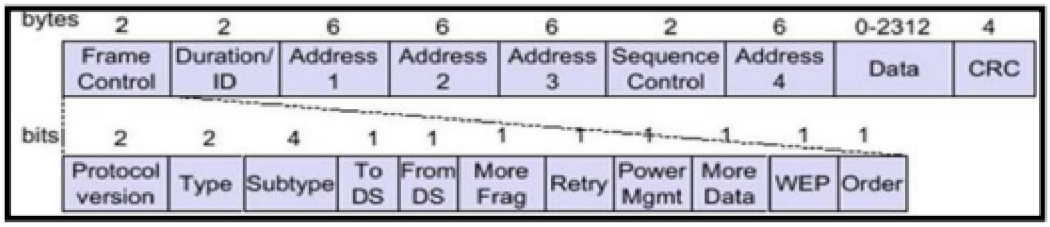


Figura. 1.2. Formato trama 802.11

FC: Frame Control:

- Tipo de trama + subtipo:

- Control: ACK, RTS, CTS...

- Gestión Entre estaciones y AP's para acceso a servicios

- Datos.

- Trama dentro de la BSS o hacia/desde otra BSS.

- Bit que indica si hay más fragmentos en la secuencia.

- Bit que indica si es retransmisión.

- Cifrado / No cifrado.

D/ID: Duración (CTS, RTS) / ID (conexión).

Direcciones:

- Source Adress.

- Destiniy Adress.

- Transmissor Adress - BSS externos en la misma ESS.

- Receptor Adress - BSS externos en la misma ESS.

- BSSID

SC: Sequence Control

- Controla fragmentos.

Datos: En la práctica <1500 bytes.

- CRC: 32 bits.

1.4.1.1 Servicios

El estándar IEEE 802.11 define nueve servicios MAC (Medium Access Control). Seis de estos servicios están destinados a la transmisión de paquetes. Los tres servicios restantes se utilizan para controlar el acceso a la LAN 802.11 y para proporcionar confidencialidad a la transacción de datos

- **Servicios de Transmisión y distribución de los mensajes**

  Asociación: Relación Estación-AP (SSID).
  Reasociación: Transferencias de asociación entre AP's de la ESS.
  Disociación: Fin asociación.
  Entrega MSDUs (Unidad de datos del servicio MAC)
  - Con confirmación (ACK).
  - Fragmentación MAC.
  - Entrega en la misma BSS o en otras (Distribución).
  DFC: Función de coordinación distribuida:
  - SIFS: Intervalo corto.
  - DIFS: Intervalo distribuido.

  PFC: Función de coordinación puntual:
  - Coordinador (Punto de acceso).
  - Tiempo dividido en "Supertramas" de dos partes:
  - Libre de contienda (PFC).
  - Con contienda (DFC).

- **Servicios de Control de acceso y seguridad:**

  Autenticación: SSID (Service Set ID) o técnica de cifrado.
  Fin de autenticación.
  Privacidad -> Cifrado de datos:
  - WEP (Wire Equivalent Privacy) - Vulnerable.
  - WPA2 (802.11i) (Wi-Fi Protected Access 2) - Comrade AES.

1.5 SEGURIDAD EN REDES WIRELESS

Las redes inalámbricas consta de dos elementos clave: las estaciones y los puntos de acceso, la comunicación puede realizarse entre estaciones o a través de puntos de acceso. Un punto de acceso transmite señales de gestión periódicamente, una estación después de recibir esta señal inicia la autenticación mediante el envío de una trama. Una vez realizada la autenticación se produce la asociación entre los dos equipos.

El estándar IEEE 802.11 provee la seguridad mediante dos métodos primarios: autenticación y cifrado. Además, define dos tipos de servicios de autenticación: sistema abierto y claves compartidas:

- **sistema abierto:**

Primeramente hablaremos de las llamadas redes abiertas, estas redes se caracterizan por no implementar ningún sistema de autenticación o cifrado, las comunicaciones entre terminal y AP (punto de acceso) viajan en texto plano (sin cifrar) y no se necesita ningún dato para acceder a la red. Este sistema se utiliza normalmente en puntos de acceso públicos y se describe en la figura 1.3

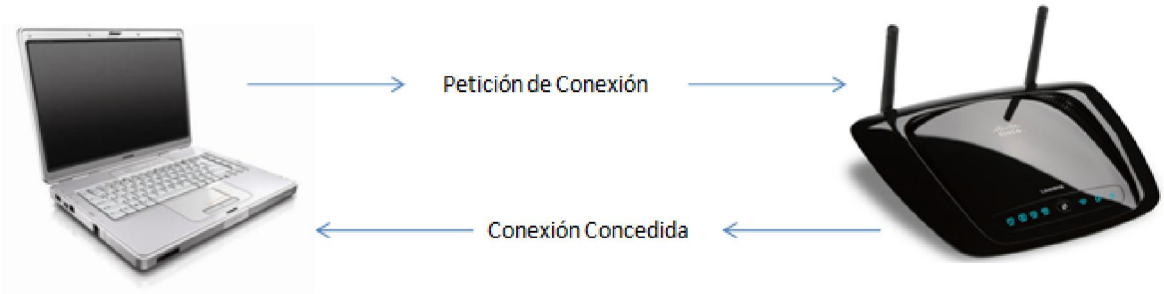


Figura. 1.3. Sistema Abierto

- **Claves Compartidas:**

En este servicio de autenticación existen claves que son compartidas entre el AP y la terminal. La autenticación se muestra en la figura 1.4

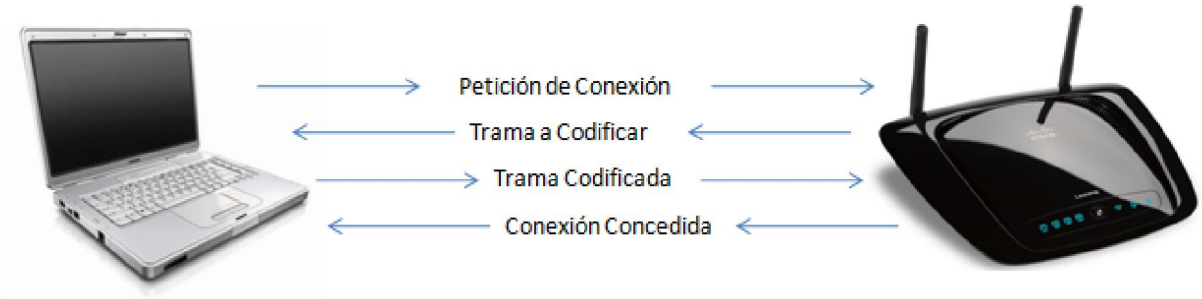


Figura. 1.4. Usando Claves Compartidas

En este tipo de servicio se sigue una serie de pasos:

1. El AP pide a la terminal que se autentique mediante el envío de una trama de datos.

2. Una vez recibida, la terminal debe codificar dicha trama y reenviarla al AP.

3. El AP decodificará la trama retransmitida por la terminal.

4. Si la trama es igual a la original, el AP permitirá a la terminal establecer una asociación, en caso contrario se niega el acceso.

1.6. RIESGOS EN LAS REDES WIFI

El utilizar el espacio libre como medio de transmisión en un factor que pone en riesgo la información confidencial. Hay taques dirigidos a la seguridad de una red inalámbrica, entre los cuales podemos mencionar algunos:

- **Romper Access control Lista basados en MAC:** entre las primeras medidas de seguridad usadas en redes wireless fue el filtrado de conexiones por dirección MAC. para ello se crea una lista de direcciones MAC en el AP indicando solo las direcciones que podrán tener acceso permitido o denegado. este método es poco seguro debido a la sencillez de cambiar la dirección MAC de nuestra tarjeta por otra valida previamente obtenida mediante un sniffer.

- **ataque de denegación de servicio:** conocido como ataque DoS, el objetivo de este ataque consiste en impedir la comunicación entre un terminal y un AP, para lograr esto solo debemos hacernos pasar por el AP poniéndonos su dirección MAC (obtenida con un sniffer) y negar la conmutación al terminal mediante el envío continuo de notificaciones de desasociación.

- **Suplantación:** se hace creer a la terminal victima que el atacante es el AP, y al mismo tiempo, convencer al AP que el atacante es el cliente. se usa un sniffer para obtener los siguientes datos necesarios:
    - El ESSID de la red
    - La dirección MAC del AP
    - la dirección MAC de la terminal

  Conociendo estos datos se emplea la misma técnica del ataque DoS para romper la conexión entre terminal y AP, tras la ruptura la tarjeta de la terminal comenzara a buscar un nuevo AP empleando su MAC y ESSID en un canal diferente, de manera paralela el atacante ha de suplantar la identidad de la terminal con el AP empleando para esto la dirección MAC de la terminal, de esta manera ni AP ni terminal se dan cuenta de la infiltración.

Como se mencionó en la sección de “seguridad de redes”, las medidas de seguridad que se implementaban se centran en impedir el acceso a la red a usuarios no autorizados. Sin embargo ninguna de las medidas anteriores se emplea para evitar la obtención de información intercambiada entre el AP y las terminales.

Para solucionar esto se implementa el cifrado de las comunicaciones de tal forma que si alguien captura las comunicaciones entre una terminal y el AP no pueda acceder a la información concreta enviada.

A continuación se explica el funcionamiento de uno de los primeros sistemas para la protección de redes inalámbricas WiFi en donde se hace uso de sistemas de cifrado y también se denota algunos de los problemas que este presentó.

1.7 ALGORITMO WEP

La Privacidad Equivalente al Cableado WEP fue el primer mecanismo de seguridad que se implementó bajo el estándar 802.11 aprobado por la IEEE y opera en la capa dos del modelo OSI. Este algoritmo permite codificar los datos que se transfieren a través de una red inalámbrica y autenticar los dispositivos móviles que se conectan al AP.

La seguridad ofrecida por WEP tiene como pilar fundamental el uso de una clave compartida entre todas las terminales y el AP la cual se emplea para cifrar los datos enviados, lo que reduce en gran medida la seguridad que puede ofrecer este sistema.

Para codificar los paquetes de información, WEP se basa en el algoritmo de encriptación RC4, el cual utiliza a la entrada 4 claves estáticas de 40 bits junto con un vector de inicialización aleatorio de 24 bits, haciendo un total de 64 bits.

La figura 1.5 muestra el proceso de cifrado del algoritmo WEP.

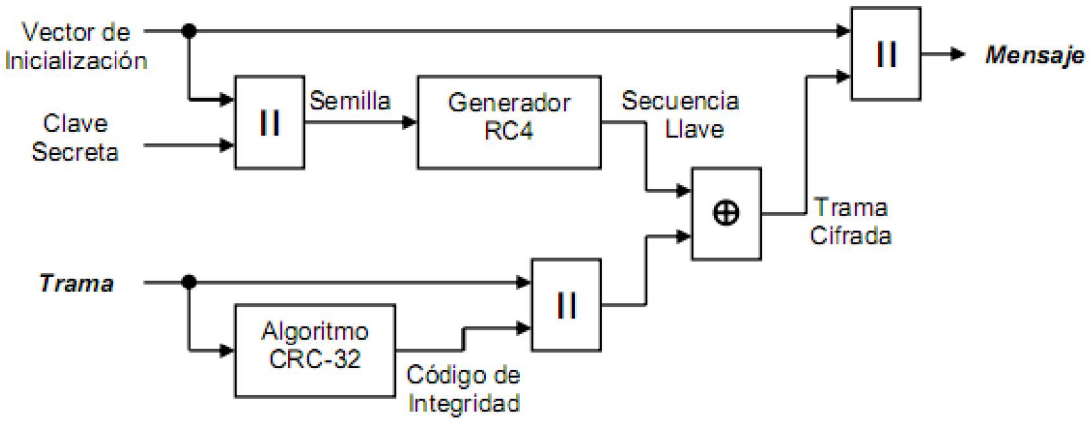


Figura. 1.5 diagrama de bloque del cifrado WEP

El proceso realizado fue el siguiente:

- A la trama original se le agrega un código de integridad ICV (IntegrityCheckValue) mediante el algoritmo CRC-32. Este código de integridad se concatena con la trama, y es empleado por el receptor para comprobar si la trama ha sido alterada durante la transmisión.

- Se escoge una clave secreta compartida entre emisor y receptor.

- Para evitar que las tramas cifradas sean similares, la clave secreta se enlaza con un número aleatorio llamado Vector de Inicialización (Initialization Vector - IV) de 24 bits, este enlace se conoce como semilla. El vector de inicialización al ser aleatorio es distinto para cada trama.

- El enlace de la clave secreta y el vector de inicialización se emplea como la entrada de un generador RC4 de números pseudo-aleatorios. El generador RC4 es capaz de generar una secuencia pseudo-aleatoria tan larga como se desee a partir de su entrada, en nuestro caso el generador RC4 origina una secuencia pseudo-aleatoria, denominada secuencia llave, del mismo tamaño de la trama a cifrar.

- Se ejecuta una operación XOR bit por bit con la trama y la secuencia llave, obteniéndose como resultado la trama cifrada.

- El vector de inicialización y la trama cifrada se transmiten juntos.

En la figura 1.6 se muestra el proceso que se lleva a cabo en el receptor para el descifrado.

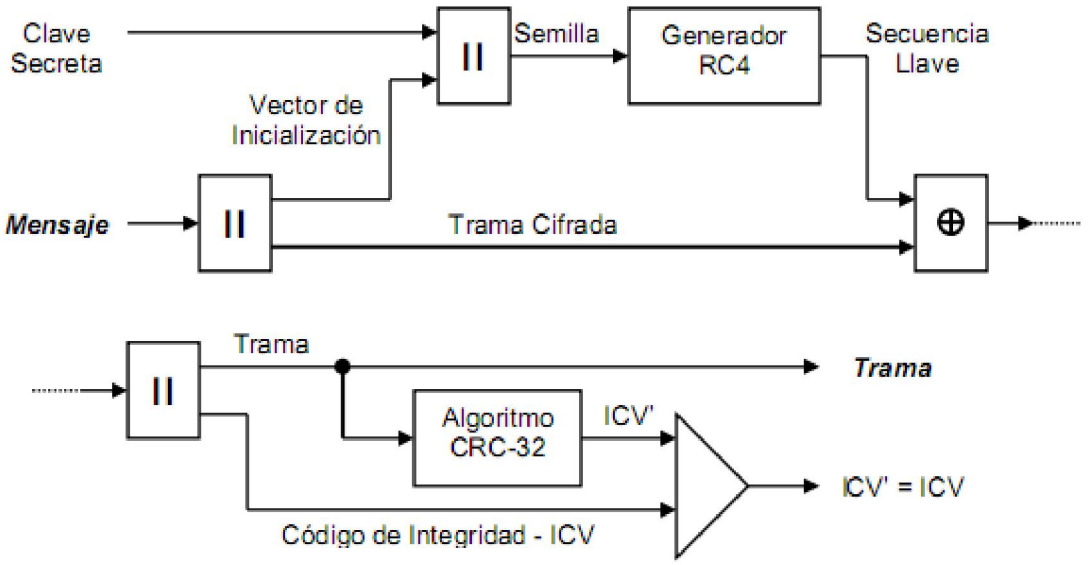


Figura. 1.6. Diagrama de bloque del descifrado WEP

- Se concatenan el vector de inicialización recibido y la clave secreta compartida para generar la misma semilla que se utilizó en el transmisor.

- Un generador RC4 produce la secuencia llave a partir de la semilla.

- Se ejecuta la operación XOR bit por bit entre la secuencia de clave y la trama cifrada, para obtener la trama original y el código de integridad.

- Finalmente, a la trama obtenida se le aplica el algoritmo CRC-32 para obtener un segundo código de integridad, que se compara con el código de integridad recibido.

- Si los códigos de integridad coinciden, la trama se acepta; en caso contrario se rechaza.

En la figura 1.7 se muestra la estructura de encriptación del algoritmo WEP.

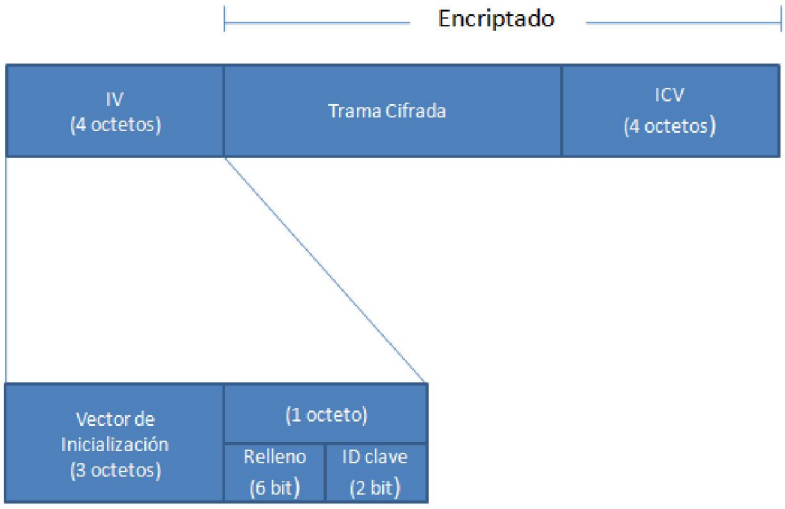


Figura. 1.7 Encriptación WEP

ICV es una secuencia de verificación de grupo sobre la trama cifrada, calculada con el algoritmo CRC-32. El vector de inicialización tiene una longitud de tres octetos, más seis bits de relleno y dos bits que indican la llave compartida que se utilizó en el cifrado.

1.7.1 debilidades

- La encriptación WEP no cubre las transmisiones desde el principio hasta el final, solamente protege la información de los paquetes de datos, pero no protege a nivel físico. Esto implica que datos de control necesarios para gestionar la red pueden ser capturados por dispositivos móviles extraños.

- El vector de inicialización es de longitud insuficiente. En una red de alto tráfico se pueden agotar los vectores de inicialización en corto tiempo. Si un atacante logra conseguir dos tramas con los vectores de inicialización idénticos, puede efectuar un XOR entre ellas y obtener los textos de ambas tramas mediante un ataque estadístico. Con el texto de una trama y su respectivo texto cifrado se puede obtener la secuencia de clave. Teniendo esta información y utilizando el algoritmo RC4 es posible obtener la clave estática compartida y descifrar toda la transmisión.

- WEP emplea claves de cifrado estáticas, las cuales son configuradas manualmente y deben ser cambiadas periódicamente. Un intruso puede acumular grandes cantidades de texto cifrado con la misma clave e intentar un ataque por fuerza bruta.

- No existe una comprobación de integridad apropiada (se utiliza CRC32 para la detección de errores y no es criptográficamente seguro por su linealidad.

CAPITULO 2

WPA Y WPA2

2.1 INTRODUCCIÓN

En enero de 2001, el grupo de trabajo i taskgroup fue creado en IEEE para mejorar la seguridad en la autenticación y la encriptación de datos. En abril de 2003, la Wi-Fi Alliance (una asociación que promueve y certifica Wi-Fi) realizó una recomendación para responder a las preocupaciones empresariales ante la seguridad inalámbrica. Sin embargo, eran conscientes de que los clientes no querrían cambiar sus equipos.

En junio de 2004, la edición final del estándar 802.11i fue adoptada y recibió el nombre comercial WPA2 por parte de la alianza Wi-Fi. El estándar IEEE 802.11i introdujo varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos.

2.2 WPA (WIFI PROTECTED ACCESS)

El algoritmo de Acceso Protegido Wifi (Wifi Protected Access) se desarrolló para mejorar el nivel de seguridad existente en WEP, fue propuesto por los miembros de la Wi-Fi Alliance en colaboración con el grupo de trabajo 802.11i de la IEEE.

WPA implementa como método de autenticación el estándar 802.1x y el Protocolo de Autenticación Extensible (Extensible AuthenticationProtocol - EAP). Además, utiliza el protocolo de integridad de clave temporal (Temporary Key Integrity Protocol - TKIP), como método de encriptación.

2.2.1 Características WPA

Las principales características de WPA son la distribución dinámica de claves, utilización más robustadel vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad yautentificación. WPA incluye las siguientes tecnologías:

- EEE 802.1X. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos presentado en el apartado anterior.
- EAP. EAP, definido en la RFC 2284, es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Trataremos más en detalles este protocolo en un apartado siguiente.
- TKIP (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave dinámica para cada trama, mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización.
- MIC (Message Integrity Code) o Michael. Código que verifica la integridad de los datos de las tramas.

2.2.1.1 Mejoras de WPA con 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 de cifrado utilizado por WPA sigue siendo RC4 como en WEP, aunque más tarde se ha demostrado inseguro. 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: Integrity Check Value), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

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, los desarrolladores modificaron los métodos de autenticación y cifrado para proporcionar más seguridad: los clientes utilizan claves previamente compartidas o (en las grandes redes LAN inalámbricas) un servidor RADIUS para asociarse con el punto de acceso.

Después de la autenticación, el cliente y el punto de acceso negocian una clave individual de 128 bits para evitar que otras estaciones en la WLAN rastreen el tráfico de datos. La renegociación periódica de la clave entre el cliente y el punto de acceso añade más seguridad a la WPA estándar, eliminando la posibilidad de que un intruso ponga en marcha un ataque de fuerza.

Según la complejidad en la autenticación, un punto de acceso que implementa el algoritmo WPA puede operar en dos modalidades:

- Modalidad 802.1x: Para operar en esta modalidad se requiere de un servidor de autenticación RADIUS (RemoteAuthentication Dial-In UserService) en la red. El punto de acceso emplea 802.1x y EAP para la autenticación, mientras que el servidor RADIUS suministra las claves compartidas que se usarán para encriptar las tramas.

- Modalidad Pre-Clave Temporal: WPA opera en esta modalidad cuando no se dispone de un servidor de autenticación en la red. Simplemente se requiere introducir una clave compartida en el punto de acceso y en los dispositivos móviles. Únicamente los dispositivos móviles cuya clave compartida estática coincida con la del punto de acceso podrán asociarse.

2.2.2TKIP (Temporal Key Integrity Protocol)

Para solucionar los problemas de encriptación descubiertos en WEP, WPA implementa el protocolo TKIP que se encarga de cambiar la clave compartida entre el AP y el dispositivo móvil periódicamente. Entre las características a destacar se encuentra la ampliación de la clave a 128 bit y el cambio del carácter de la misma de estática a dinámica; cambiando por usuario, sesión y paquete y añadiendo temporalidad. El vector de inicialización pasa de 24 a 48 bits, minimizando la reutilización de claves.

TKIP utiliza el algoritmo "Michael" para garantizar la integridad, generando bloques de 4 bytes (llamado MIC) a partir de la dirección MAC de origen, de destino y de los datos y añadiendo el MIC calculado a la unidad de datos a enviar. Posteriormente los datos (que incluye el MIC) se fragmentan y se les asigna un número de secuencia.

La mezcla del número de secuencia con la clave temporal genera la clave que se utiliza para el cifrado de cada fragmento.

TKIP extiende la estructura de encriptación WEP agregando doce octetos, cuatro octetos para el vector de inicialización extendido y ocho octetos para el código de integración de mensajes, como se muestra en la figura 2.1. La secuencia de conteo TSC se construye con los primeros dos octetos de vector de inicialización original y los cuatro octetos del vector de inicialización extendido. En la encriptación se utilizan la clave temporal y la clave MIC, que son claves compartidas generadas en el proceso previo de autenticación.

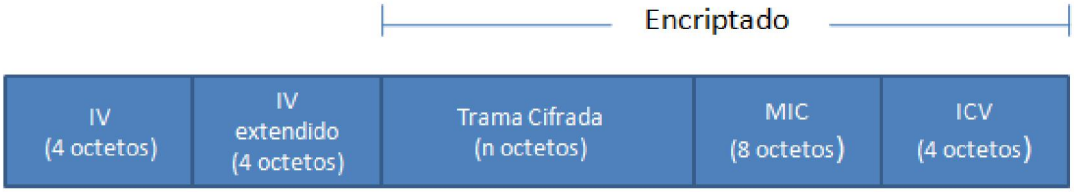


Figura. 2.1. Estructura de Encriptación TKIP

La clave temporal, la dirección del emisor y la secuencia de conteo TSC se combinan para obtener una clave temporal de 128 bits. Esta clave se divide para generar las entradas en la encriptación WEP, es decir, el vector de inicialización de 24 bits y la clave secreta de 104 bits.

El código de integración de mensajes MIC se calcula sobre la dirección física origen y destino y la trama original, utilizando la clave MIC y la secuencia de conteo TSC. Si es necesario, la trama original puede ser segmentada incrementando la secuencia de conteo TSC para cada segmento, antes de pasar a la encriptación WEP. En la figura 2.2 se describe el proceso de cifrado TKIP:

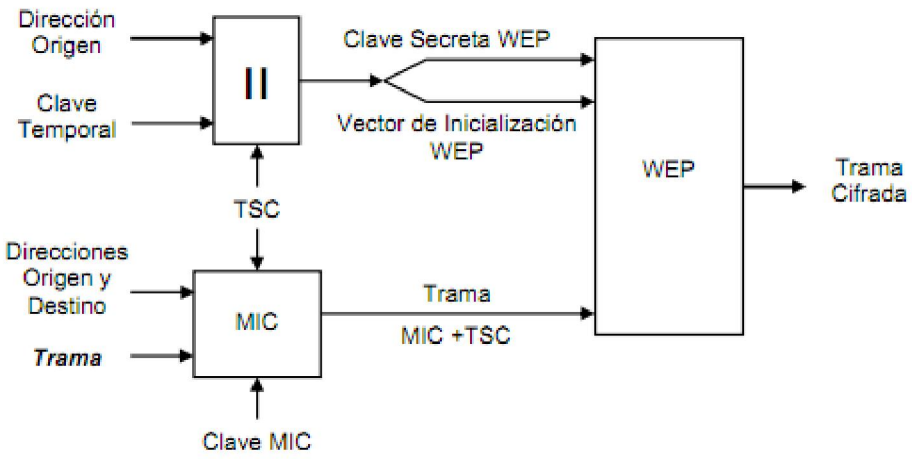


Figura. 2.2. Diagrama en Bloque del Cifrado TKIP

En la desencriptación se examina la secuencia de conteo TSC para asegurar que el paquete recibido tiene un valor mayor que el anterior, en caso contrario se descarta el paquete para prevenir posibles ataques.

El código de integración de mensaje MIC se vuelve a calcular utilizando la trama recibida desencriptada, este nuevo valor se compara con el recibido para verificar la integridad del mensaje.

Sin embargo, cuando las claves compartidas utilizadas son de una longitud corta, WPA se vuelve inseguro, porque un intruso sólo necesita interceptar el tráfico inicial de intercambio de claves y con un ataque de diccionario se puede obtener la clave compartida.

2.3 WPA2

2.3.1 Estándar 802.11i

El estándar de seguridad 802.11i propuesto por la IEEE fue ratificado en junio de 2004. Este nuevo estándar incorporará una capa de seguridad específica para redes inalámbricas, la cual se divide en tres categorías:

1. Protocolo de Integridad de Clave Temporal. El protocolo TKIP se implementó en la encriptación WPA como una solución a los problemas de la encriptación WEP. TKPI puede ser usada en los viejos equipos 802.11 para proveer integridad y confidencialidad.

2. El reemplazo del algoritmo Michael por un código de autenticación conocido como el protocolo "Counter-Mode/CBC-Mac" (CCMP), que es considerado criptográficamente seguro. El protocolo CCMP está documentado en el RFC2610, utiliza en el proceso de encriptación el Estándar de Encriptación Avanzado (AdvancedEncryption Standard - AES) con el algoritmo CBC-MAC.

3. 802.1x Control de Acceso a Red Basado en Puerto (Port-Based Network Access Control). En este control de acceso se puede utilizar los protocolos TKIP o CCMP para la encriptación y se utilizará el estándar IEEE 802.1x para la autenticación.

2.3.2 Estándar 802.1x

802.1x es un estándar de control de acceso y autenticación basado en la arquitectura cliente / servidor, que restringe la conexión de equipos no autorizados a una red. Este estándar fue inicialmente creado por la IEEE para uso en redes de área local cableadas, pero se ha extendido a las redes inalámbricas. En la figura 2.3 se muestra la arquitectura de un sistema de

Figura. 2.3. Arquitectura de un Sistema de Autenticación 802.1x

2.3.3Autenticación 802.1x

El contenido principal del estándar 802.11 es encapsular los protocolos de autenticación sobre los protocolos de la capa de enlace de datos y permite emplear el protocolo de autenticación extensible (EAP) para autenticar al usuario de varias maneras.

El protocolo 802.1x involucra tres participantes:

- El Solicitante, o equipo del usuario que desea conectarse con la red.
- El Servidor de Autenticación, que contiene toda la información necesaria para saber qué equipos o usuarios están autorizados para acceder a la red.
- El Autenticador, es un equipo de red que recibe la conexión del suplicante, actúa como intermediario entre el suplicante y el servidor de autenticación, solamente permite el acceso del suplicante cuando el servidor de autenticación lo autoriza.

EAP comprende cuatro tipos de mensajes:

- Petición (Request Identity): empleado para enviar mensajes desde el AP a la terminal.
- Respuesta (Identity Response): empleado para enviar mensajes desde la terminal al AP.
- Éxito (Success): emitido por el AP, significa que el acceso está permitido.
- Fallo (Failure). emitido por el AP cuando al solicitante se le niega la conexión.

El funcionamiento básico del estándar 802.11x se centra en la denegación de cualquier tráfico que sea hacia el servidor de autenticación hasta que el cliente no se haya autenticado correctamente. Para ello el Autenticador crea un puerto por cliente que define dos caminos, uno autorizado y otro no; manteniendo el primero cerrado hasta que el servidor de autenticación le comunique que el cliente tiene acceso al camino autorizado.

El solicitante, cuando pasa a estar activo en el medio selecciona y se asocia a una AP. El Autenticador (ubicado en el AP) detecta la asociación del cliente y habilita un puerto para ese solicitante, permitiendo únicamente el trafico 802.11x, el resto del tráfico se bloquea. El cliente envía un mensaje "EAP Start", el Autenticador responde con un mensaje "EAP RequesIdentity" para obtener la identidad del cliente, la respuesta del solicitante "EAP Response" contiene su identificador y es retransmitido por el Autenticador hacia el servidor de autenticación. A partir de ese momento el solicitante y el servidor de autenticación se comunican directamente, usando un cierto algoritmo de autenticación que pueden negociar. Si el servidor de autenticación acepta la autenticación, el Autenticador pasa el puerto del cliente a estado autorizado y el tráfico será permitido.

Existen variantes del protocolo de autenticación extensible según la modalidad de autenticación utilizada, se puede emplear certificados de seguridad o contraseñas. En la figura 2.4 se muestra el diálogo básico entre un nuevo usuario y el punto de acceso a la red, durante el proceso de autenticación.

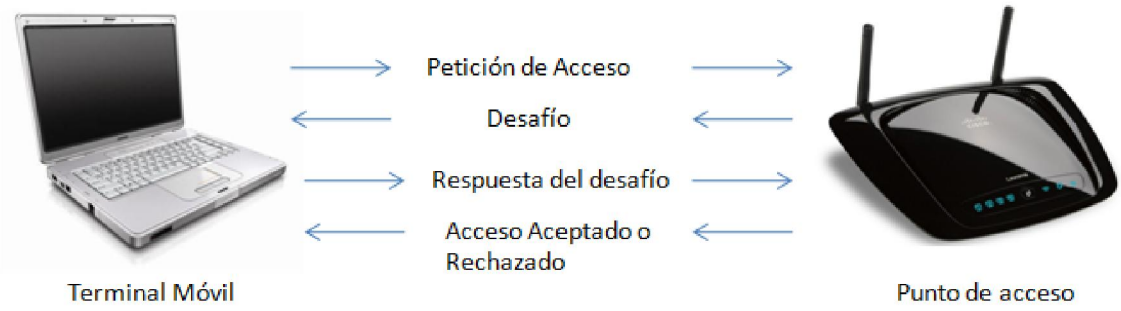


Figura. 2.4 Diálogo EAPOL - Autenticador

Los métodos de autenticación complementados en WPA son: EAP-TLS, EAP-TTLS y PEAP. Todos ellos se basan en el método de infraestructura pública (PKI) para autenticar al usuario y al servidor de autenticación mediante certificados digitales. Para ello es necesaria la existencia de certificación (CA), bien sea empresarial o pública.

2.4 PRIVACIDAD TLS

El protocolo TLS o Transport Layer Security tiene su origen en los comienzos de Internet. En esta época Netscape era el navegador dominante en el mercado, por lo que la mayoría de los avances en aquella época vinieron de él. Apareció la necesidad de realizar transferencias de información de forma segura, así que Netscape implementó una solución a la que se le llamó SSL o Secure Socket Layer. SSL se basaba en el uso de Certificados Digitales, y aunque permitía el uso de certificados en cliente y servidor, su uso más común era el de utilizar Usuario/Contraseña en el lado del cliente. Por otra parte, SSL ofrecía la posibilidad de identificar y validar entidades de Internet de forma inmediata, a la par que permitía comunicarse con ellos de forma segura, con control de integridad y privacidad garantizadas. Esto permitía trasladar a otras entidades información muy sensible como podría ser por ejemplo un número de cuenta.

SSL se convirtió rápidamente en el estándar de facto para transacciones Web seguras. Aunque lasespecificaciones de este protocolo eran conocidas, continuaba siendo una solución propietaria. Estono es algo que agrade especialmente a los fabricantes por lo que se promovió un protocoloestandarizado, a través del IETF. El resultado de este trabajo vio la luz en 1999 con la aparición deTLS. TLS proporciona más servicios que los que nosotros necesitamos de un Protocolo deAutenticación de Alto Nivel. TLS proporciona servicios como Autenticación, Cifrado y Compresión de Datos. Nuestro principal interés en TLS será su mecanismo de autenticación, que se adapta muy bien al modelo basado en 802.1X y EAP que vamos a describir a continuación.

2.4.1 Características de WPA-EAP:

En el protocolo EAP, como se muestra en la figura 4, intervienen tres tipos de elementos: el cliente que solicita acceso, el autenticador que sirve de enlace entre el cliente y el servidor de autenticación (que en el caso de redes WIFI es el punto de acceso) y el servidor de autenticación que es el que realiza la comprobación de credenciales que puede ser un servidor RADIUS.

2.4.1.1 EAP-TLS:

EAP-TLS (Extensible Authentication Protocol with Transport Layer Security) [3] se trata de una variante de EAP en la cual se realiza una negociación SSL con autenticación basada en certificadosX.509 para autenticar tanto usuario como servidor. En el caso de TLS, las credenciales corresponden al certificado de cliente, mientras que en otros tipos de EAP la conexión segura se realiza a partir exclusivamente del certificado del servidor. El certificado del usuario se puede almacenar en algún dispositivo hardware como Smart Card o USB para aumentar aún más la seguridad de la red, aunque también hace más difícil la implementación y la gestión de ésta. Además, hay que tener en cuenta que algunos usuarios necesitan extensiones específicas para certificados digitales.

El proceso a seguir en EAP-TLS es el siguiente:

1) El cliente se asocia al punto de acceso físico.
2) El punto de acceso envía una solicitud de autenticación al cliente. El cliente responde con su ID (nombre de host o login), el mensaje se transmite por el punto de acceso al servidor RADIUS.
3) El servidor RADIUS inicia el proceso de autenticación TLS con el mensaje TLS Start.
4) El cliente responde con un mensaje client_hello , que contiene:
   - Las especificaciones de cifrado, campos vacíos hasta que se negocian entre el cliente y el servidor;
   - La versión TLS del cliente;
   - un número aleatorio (reto o desafío);
   - un identificador de sesión;
   - Los tipos de algoritmos de encriptación soportados por el cliente.
5) El servidor envía una petición que contenga un mensaje server_hello seguida por:
   - su certificado (x509) y su clave pública;
   - la solicitud del certificado de cliente;
   - un número aleatorio (reto o desafío);
   - un identificador de sesión

El servidor elige un sistema de cifrado entre los que han sido propuestos por el cliente.

6) El cliente comprueba el certificado del servidor y responde con su propio certificado y la clave pública.
7) El servidor y el cliente, cada uno a su vez, definen una clave de cifrado principal que se utiliza para la sesión. Esta clave se calcula con los valores aleatorios que han intercambiado el cliente y el servidor. Los mensajes change_cipher_spec indican el cambio de clave. El mensaje TLS_finished finaliza la fase de autenticación TLS (TLS handshake), en el caso de EAP-TLS la clave de sesión no se utiliza para cifrar los siguientes intercambios.

8) Si el cliente ha verificado la identidad del servidor (con el certificado y la clave pública), devuelve una respuesta EAP sin datos. El servidor devuelve una respuesta EAP Success.
9) La clave de sesión generada en (8) se vuelve a utilizar en el punto de acceso para crear una clave WEP que se envía al cliente si se trata de una estación WiFi. La clave de sesión es válida hasta que el cliente se desconecta o su autentificación caduca, en cuyo caso se debe autenticar de nuevo.

El túnel de TLS establecido durante la creación de la clave de sesión no se ha utilizado. Solamente se usa el TLS Handshake, que permite la autenticación mutua de ambas partes. EAP-TLS es un método de autentificación de gran rendimiento. Tan sólo los problemas relacionados con la administración de claves pueden desalentar el uso de este método.

Hablar de ataques Man In The Middle en redes con seguridad EAP-TLS no tiene mucho sentido, ya que el usuario comprueba la autenticidad del servidor comparándolo con una lista de servidores autorizados, siendo realmente difícil suplantar la identidad del servidor autorizado.

EAP-TLS sigue manteniendo el problema de exposición de la identidad, puesto que los certificados son enviados por el medio (aire) sin cifrar, por lo que un atacante podría ver la identidad del cliente que está tratando de conectarse. Además, el mensaje de aceptación o denegación de la conexión es enviado sin cifrar, por lo que un atacante podría enviarlo suplantando la identidad del servidor de autenticación.

El uso de certificados tiene sus ventajas y desventajas. A menudo son considerados más seguros que las contraseñas, sin embargo, las operaciones de gestión que generan pueden ser tediosas (creación, supresión, listas de revocación, etc.) y la existencia de una infraestructura de gestión de claves (PKI) es necesaria. La distribución de los certificados a los clientes es una limitación que no debe pasarse por alto.

2.4.1.2 EAP-TTLS:

En la línea de EAP-TLS se encuentran otros métodos que resuelven los problemas de éste. EAP-TTLS (Extensible Authentication Protocol with Tunneled Transport Layer Security), desarrollado por Funk Software, está orientado a trabajar con servidores RADIUS. Puede emplear métodos de autenticación EAP adicionales o métodos como PAP y CHAP. Está integrado con una gran variedad de formatos de almacenamiento de contraseñas y sistemas de autenticación basados en contraseñas, así como con múltiples bases de datos de seguridad. Además, en el mercado existen un gran número de usuarios TTLS disponibles.

2.4.1.3 EAP-PEAP:

EAP-PEAP (Protected EAP) es un protocolo que ha sido desarrollado de forma conjunta entre Microsoft, Cisco y RSA Security como alternativa a EAP-TTLS. Su objetivo original era conseguir un sistema basado en Contraseña pero que a la par fuera más seguro respecto a los Ataques de Diccionario.

Para explicar este protocolo vamos a partir de aquellos defectos que tenía EAP. El mensaje EAP-Identity no estaba protegido, por lo que si en la primera fase del protocolo EAP había alguien observando, la identidad del cliente podría ser descubierta. De la misma forma el EAP-Success y EAP-Reject estaban desprotegidos frente a snooping.

La solución que propone PEAP es proteger el proceso de autenticación completo, incluyendo los mensajes EAP iniciales y finales mediante un túnel TLS. De esa forma PEAP pretende establecer el túnel que proporcione la privacidad del proceso, dejando luego libre toda la flexibilidad de EAP para implementar cualquier método de autenticación, eso sí, implementado desde el primer al último mensaje sobre un canal seguro.

¿Pero cómo establecer un canal seguro si precisamente uno de los propósitos de EAP era ese? La respuesta es simple. Privacidad y Autenticación son independientes, y es posible conseguir privacidad sin tener autenticación. Ese es precisamente nuestro objetivo, utilizar PEAP para proporcionar privacidad, dejando el peso de la autenticación a EAP.

El proceso se puede dividir en dos fases. En la primera de ellos se utiliza EAP del modo convencional para establecer una conexión segura TLS. En la segunda se utiliza el túnel creado para llevar a cabo una nueva negociación EAP, complementada con el protocolo de alto nivel que se desee, en la que se realice una autenticación completa. Hay que resaltar que en la primera fase sí que se produce una autenticación real del servidor, al que se le solicita un Certificado para probar su identidad. Veamos a continuación con algo más de detalle las dos fases.

EAP-TTLS y EAP PEAP son métodos muy similares y el uso de un túnel cifrado TLS les da un buen nivel de Privacidad. La principal diferencia entre EAP-PEAP y EAP-TTLS está en la forma de encapsular los intercambios durante la segunda fase. Para EAP-PEAP, los datos intercambiados entre el cliente y el servidor en el túnel de TLS se encapsulan en paquetes EAP.

2.4.1.4 EAP-MS-CHAP:

MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), también conocido como MS-CHAP versión 1 es un protocolo de autenticación de contraseñas de cifrado no reversible. Utiliza una versión de Microsoft del protocolo de desafío y respuesta de RSA Message Digest 4. Éste sólo funciona en sistemas Microsoft y activa la codificación de datos. La selección de este método de autenticación hace que se codifiquen todos los datos.

2.5 SERVIDORES DE AUTENTICACIÓN

Un servidor remoto agrupa servicios que están instalados en el mismo equipo y requieren el mismo tipo de autenticación.

2.5.1 RADIUS

El protocolo de autenticación RADIUS [4] se basa en la figura de un servidor centralizado de autenticación, encargado de autenticar las conexiones remotas de forma segura. De este modo

se independiza el proceso de autenticación, liberando de esta manera a los servidores de red o a los AP, también facilita las tareas de autorización y registros de usuarios.

La primera versión de este protocolo fue aprobada en 1997[5]. El servidor RADIUS utiliza protocolos para comprobar la identidad de usuarios tales como PAP, CHAP o EAP.

En la figura 2.5 se muestra como se da la autenticación mediante un servidor RADIUS.

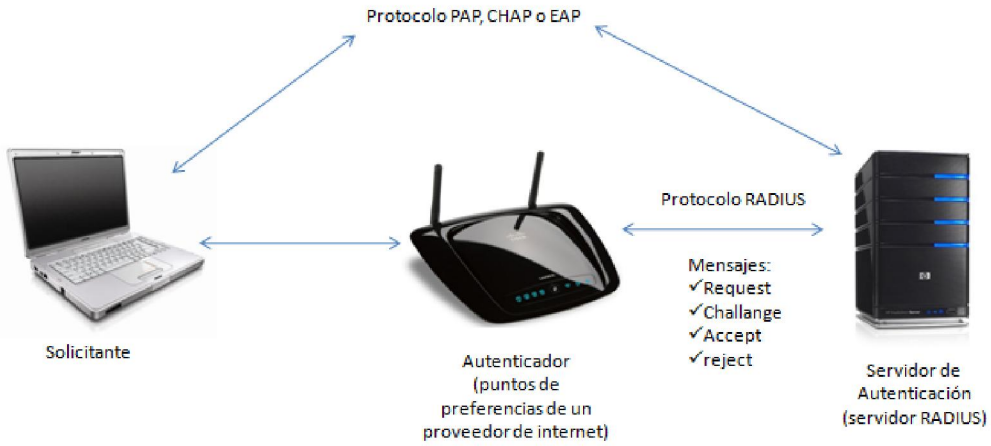


Figura. 2.5 Autenticación mediante RADIUS

Tipos de mensaje:

- Access-request: Mensajes desde el AP al servidor de autenticación.
- Access-challange: Respuestas del servidor de autenticación al AP.
- Access-accept: Enviado por el servidor de autenticación para indicar éxito en la autenticación
- Access-reject: Enviado por el servidor de autenticación para indicar fracaso en la autenticación

2.6 AUTENTICACIÓN PSK (*pre-shared key)*

El método empleado por WPA para autenticar a las estaciones Wi-Fi supone uno de los puntos débiles de este protocolo de seguridad. En entornos personales, como usuarios residenciales y pequeñas empresas, se utiliza WPA con clave pre-compartida o también llamada WPA-PSK, en estos entornos no es posible contar con un servidor de autenticación centralizado, WPA se ejecuta en un modo especial conocido como "*Home Mode*" o PSK, que permite la utilización de claves configuradas manualmente y facilitar así el proceso de configuración del usuario doméstico.

El usuario únicamente debe introducir una clave de 8 a 63 caracteres conocida como clave maestra, en su punto de acceso, módem o router inalámbrico residencial, así como en cada uno de los dispositivos que quiere conectar a la red. De esta forma sólo se permite acceso a aquellos dispositivos que son conocedores de la contraseña, lo que evita acceso de usuarios no autorizados.

2.7 CRIPTOGRAFÍA

La criptografía abarca los principios, medios y métodos para transformar los datos con el fin de ocultar el contenido, impedir su modificación y su uso no autorizado. Determina los métodos de cifrado y descifrado.

2.7.1 Cifrado

El Cifrado es la base para los mecanismos de seguridad en las redes. El cifrado consiste en escribir o leer mensajes codificados, su funcionamiento está basado en algoritmos que utilizan un valor secreto llamado llave.

Estos algoritmos son conocidos, pero el elemento que proporciona la seguridad es la llave, por esta razón se debe mantener en secreto.

El cifrado es el proceso de transformar datos. Tiene como entrada los datos originales, que se conoce como texto plano, tiene como salida un conjunto de símbolos (codificados en Hexadecimal o binario) llamado texto cifrado.

Existen dos métodos para utilizar el cifrado en comunicaciones:

- Cifrado de llave simétrica
- Cifrado de llave asimétrica

2.7.2 Cifrado de llave simétrica

Su funcionamiento consiste en utilizar una llave común y el mismo algoritmo para cifrar y descifrar el mensaje, por lo tanto si dos usuarios quieren comunicarse entre sí por este método, ambos deben ponerse de acuerdo sobre el algoritmo de cifrado y una llave secreta que será la entrada a dicho algoritmo.

2.7.3 Algoritmos de llave simétrica

WPA utiliza el cifrado de su antecesor (WEP) el RC4 y lo acopla con el PSK para mejorar deficiencias heredadas y WPA 2 utiliza el cifrado AES de mayor utilidad y fiabilidad ante los anteriores.

2.7.3.1 Algoritmo RC4

Es un algoritmo de cifrado en flujo, utilizado en protocolos de cifrado en comunicaciones como WEP y WPA, los cifrados de flujo funcionan expandiendo una llave o cadena de bits, en una clave arbitrariamente larga de bits pseudo aleatorios, el caso de claves pre compartidas la llave se forma por el vector de inicialización y la llave secreta compartida. Estas llaves alimentan al algoritmo RC4 para generar la secuencia de llaves utilizada para encriptar y desencriptar la información.

2.7.3.2 Algoritmo AES

El algoritmo AES, también conocido como Rijndael, es un algoritmo de cifrado de bloque que ha sido adoptado como estándar por el gobierno de los EE. UU.

En la figura 2.6 se muestra la estructura general del algoritmo AES. La entrada a los algoritmos de cifrado y descifrado es un solo bloque de 128 bits. En el FIPS PUB 197[6], este bloque se representa con una matriz cuadrada de bytes. Este bloque se copia en el vector Estado, que se modifica en cada etapa del cifrado o descifrado. Después de la última etapa, el vector Estado se copia en una matriz de salida. De igual manera, la clave de 128 bits se representa como una matriz cuadrada de bytes. Esta clave luego se expande en un vector de palabra para la generación de claves; cada palabra tiene cuatro bytes, y el número total de palabras para generar claves de 44 para la clave de 128 bits. El orden de los bytes dentro de una matriz se establece por columnas. Así, por ejemplo, los primeros 4 bytes de una entrada de texto plano de 128 bits al cifrador ocupan la primera columna de la matriz in, los segundos 4 bytes la segunda columna, y así sucesivamente. De igual forma, los primeros 4 bytes de la clave expandida, que forman una palabra, ocupan la primera palabra de la matriz w

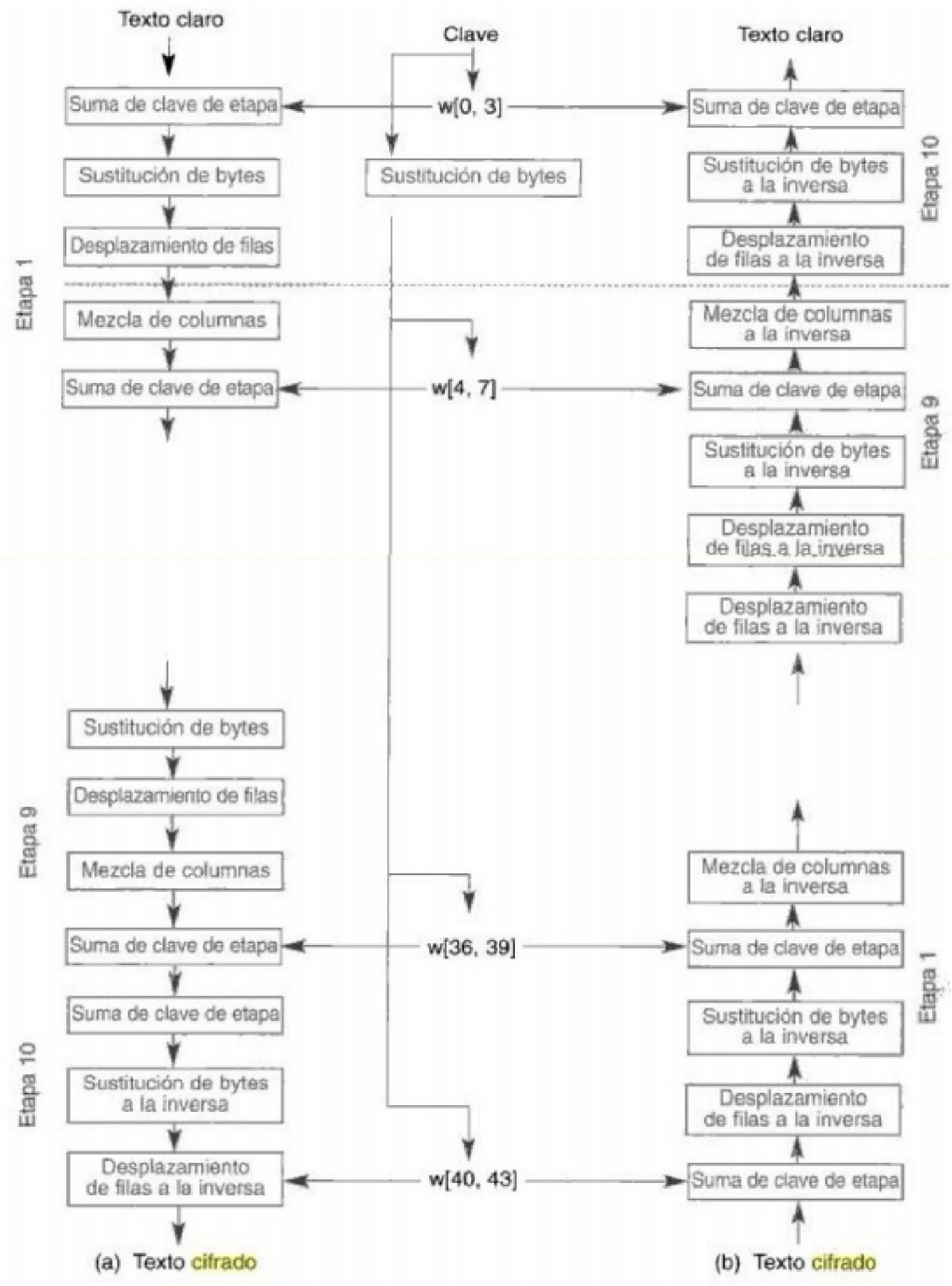


Figura. 2.6 Cifrado y descifrado AES

Algunos aspectos del algoritmo AES:

1. Una característica notable de su estructura es que no es una estructura Feistel. En la estructura clásica de Feistel, la mitad del bloque de datos se usaba para modificar la otra mitad, y entonces se intercambiaban entre sí. El algoritmo AES procesa todo el bloque de datos en paralelo durante cada etapa, realizando sustituciones y permutaciones.

2. La clave suministrada como entrada se expande en un vector de 44 palabras de 32 bits, Cuatro palabras diferentes (128 bits) sirven como clave de entrada en cada ronda.

3. Se utilizan cuatro fases diferentes, una de permutación y tres de sustitución:
    - Sustitución de bytes: se usa una tabla, denominada caja S, para realizar una sustitución byte a byte del bloque.
    - Desplazamiento de filas: una simple permutación realizada fila por fila.
    - Mezcla de columnas: una sustitución que altera cada byte de una columna en función de todos los bytes de la columna.
    - Suma de la clave de etapa: una simple operación XOR bit a bit del bloque actual con una porción de la clave expandida.

4. La estructura es muy simple. Tanto para el cifrado como para el descifrado, se comienza con una fase de suma de clave de etapa, seguido de nueve etapas de cuatro fases cada una, y acaba con una décima etapa de tres fases. La siguiente figura muestra la estructura de una etapa completa de cifrado.

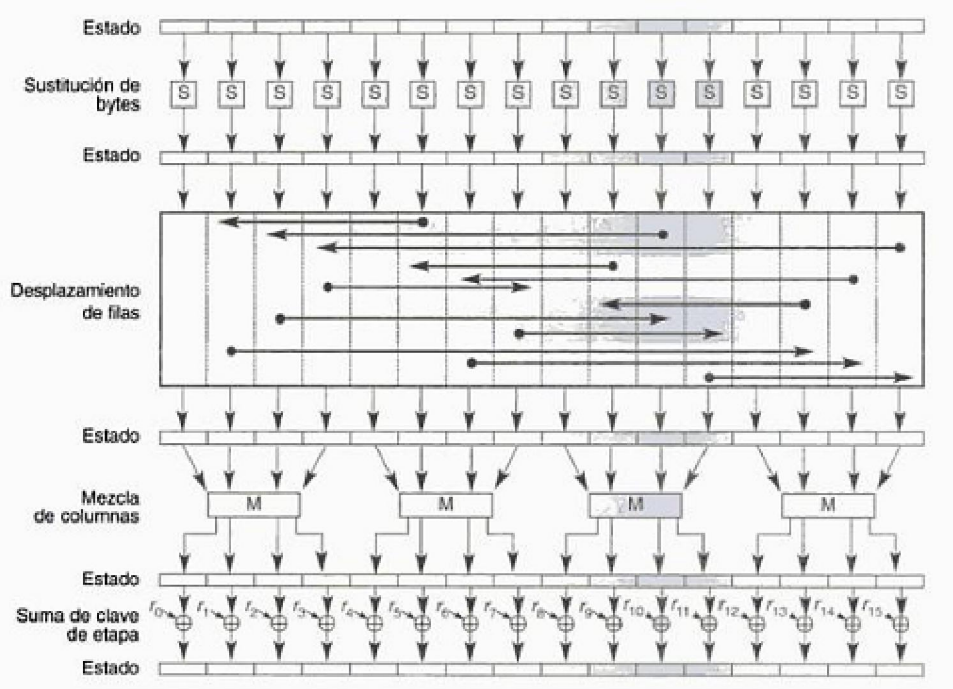


Figura. 2.7 Etapa del cifrado del AES

5. Solamente la fase de suma de la clave de etapa utiliza la clave. Por esta razón el cifrador comienza y termina con una suma de clave de etapa. Cualquier otra fase, aplicada al comienzo o al final, sería reversible sin conocer la clave y por tanto añadiría inseguridad.

6. La fase de suma de la clave de etapa no funcionaría por sí misma. Las otras tres fases juntas desordenan los bits, pero no proporcionan seguridad por sí mismos, porque no usan la clave. Se puede ver el cifrador, como una secuencia alternativa de operaciones de cifrado XOR (suma de clavede etapa) de un bloque, seguida por un desordenamiento del bloque (las otras tres fases), seguida por un cifrado XOR, y así sucesivamente. Este esquema es eficiente y muy seguro.

7. dada fase es fácilmente reversible. Para las fases de sustitución de bytes, desplazamiento de filas y mezcla de columnas, se usa una función inversa en el algoritmo de descifrado. Para la fase de suma de clave de etapa, la inversa se consigue con un XOR entre la misma clave de etapa y el bloque, usando la propiedad de que A ϴ A ϴ B = B.

8. Como la mayoría de los cifradores de bloque, el algoritmo de descifrado hace uso de la clave expandida en orden inverso. De todas formas, como consecuencia de la estructura particular del AES,el algoritmo de descifrado no es idéntico al de cifrado.
9. Una vez se ha establecido que las cuatro fases de cada etapa son reversibles, es fácil verificar que el de cifrado recupera el texto plano. La primera figura sobre AES muestra el cifrado y el descifrado desplazándose en direcciones verticalmente opuestas. En cada punto horizontal (por ejemplo, la línea discontinua de la figura), el vector estado es el mismo para el cifrado y para el descifrado.

10. La última etapa de cifrado y descifrado consiste sólo en tres fases. Otra vez, esto es consecuencia de la estructura particular del AES y es necesario que para el cifrador sea reversible.

2.8 PROTOCOLO MODO CONTADOR CON CBC-MAC

El Protocolo Modo Contador con CBC-MAC (CounterModewith CBC-MAC Protocol - CCMP) utiliza el estándar de encriptación AES con el algoritmo CBC-MAC. AES es un cifrado de bloque iterativo simétrico, encripta en bloques de 128 bits de longitud y utiliza la misma clave al encriptar y al desencriptar.

La estructura de encriptación del protocolo CCMP se muestra en la figura 2.8

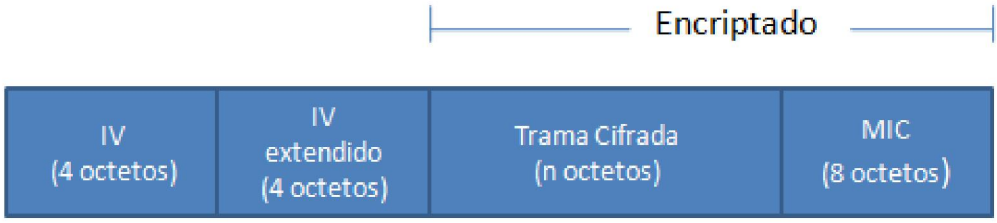


Figura. 2.8. Estructura de Encriptación CCMP

Como en el protocolo TKIP, la clave temporal se genera en el proceso previo de autenticación, también el cálculo del código de integración de mensajes y la encriptación de la trama se realizan en forma paralela. CCMP utiliza un vector de inicialización de 48 bits denominado

número de paquete PN, el cual se utiliza para el cálculo del código de integración de mensaje y para encriptar la trama.

En la figura 2.9 se muestra el diagrama de bloque del protocolo CCMP.

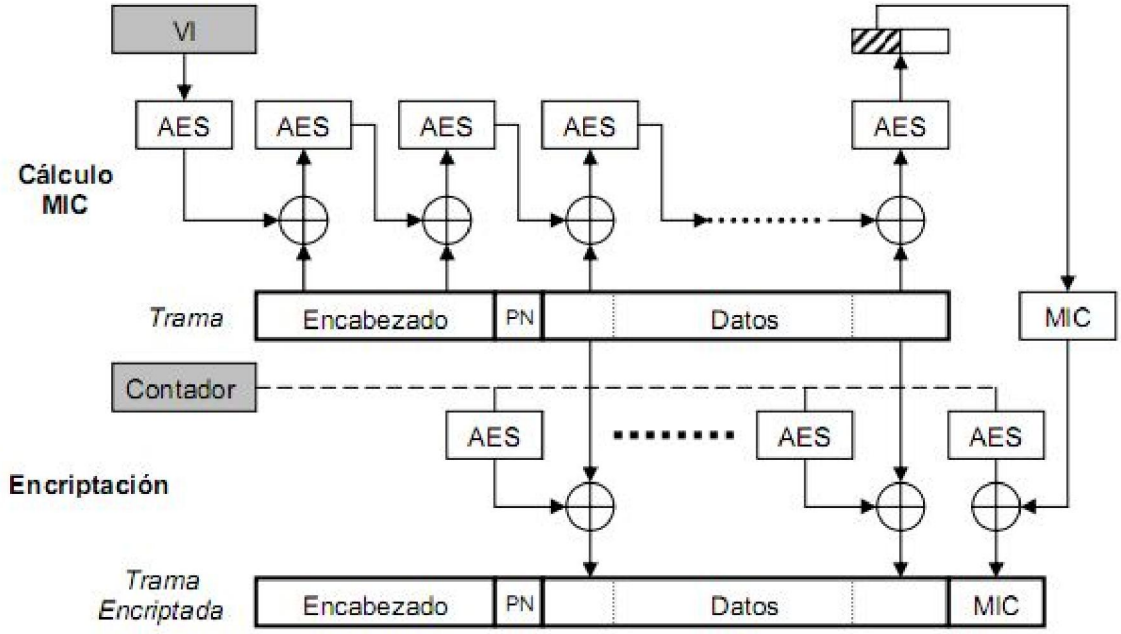


Figura. 2.9 Diagrama en Bloques de CCMP

Para el cálculo del código de integración de mensajes MIC se utiliza un vector de inicialización formado por el número de paquete, la clave temporal y datos del encabezado de la trama original. Este vector de inicialización ingresa a un bloque AESy luego pasa por un operador XOR junto a un segmento de la trama original, el resultado de este proceso pasa a ser la entrada del siguiente bloque AES y la salida de este bloque junto con el siguiente segmento de la trama original pasan por un operador XOR.

Este proceso continúa hasta capturar el último segmento de la trama original, se tomarán los primeros 64 bits del resultado final de este proceso como el código de integración de mensajes MIC final.

En el proceso de encriptación de la trama original se utiliza un contador precarga formado por el número de paquete, la clave temporal, datos del encabezado de la trama original y un contador que inicializa en 1. Este contador precarga entra en un bloque AES y su salidapasa por un operador XOR junto con un segmento de 128 bits de los datos de la trama, este proceso dará como resultado los primeros 128 bits encriptados.

Posteriormente el contador se incrementa y se repite el mismo proceso con el siguiente segmento de datos para generar los siguientes 128 bits encriptados, el procedimiento continúa hasta encriptar la totalidad de los datos. El último contador se pone en 0 y entra en el bloque AES, su salida pasa por un operador XOR junto con el código de integración de mensajes calculado anteriormente.

El proceso de desencriptación es esencialmente la reversa del proceso de encriptación. Al igual que en el protocolo TKIP, el código de integración de mensaje MIC se vuelve a calcular utilizando la trama recibida desencriptada, para compararlo con el recibido y de esta forma verificar la integridad del mensaje transmitido.

CAPÍTULO 3

SEGURIDAD. INTRUSIONES EN LA RED

3.1 SEGURIDAD

Seguridad en redes es mantener bajo protección los recursos y la información con que cuenta la red, a través de procedimientos basados en políticas de seguridad que permitan el control de dichos recursos e información. Las debilidades de las tecnologías inalámbricas y más en concreto de la tecnología Wi-Fi; son la falta de seguridad atribuida más que a la seguridad física, a la seguridad de la información, su integridad y la no accesibilidad a terceros.

3.2 CONSIDERACIONES PREVIAS

Los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio. Las ondas de radio en principio pueden viajar más allá de las paredes y filtrarse en habitaciones, casas, oficinas contiguas o llegar hasta la calle.

Si nuestra instalación está abierta, una persona con el equipo adecuado y conocimientos básicos podría no sólo utilizar nuestra conexión a Internet, sino también acceder a nuestra red interna o a nuestro equipo donde podríamos tener carpetas compartidas o analizar toda la información que viaja por nuestra red.

Si la infiltración no autorizada en redes inalámbricas de por sí ya es grave en una instalación residencial (en casa), mucho más peligroso es en una instalación corporativa. Y desgraciadamente, cuando analizamos el entorno corporativo nos damos cuenta de que las redes cerradas son más bien escasas.

3.2.1 Vulnerabilidad

Las vulnerabilidades de un sistema surgen a partir de errores individuales, nuevas y complejas vulnerabilidades surgen de la interacción entre varios componentes como el kernel del sistema, sistemas de archivos, servidores de procesos, entre otros. Estas vulnerabilidades generan problemas de seguridad para la red en cuestión; entre las más conocidas están el "fingerusername" y la notificación de mensajes de correo a través de "comsat"; además de:

- **Aumento de privilegios**. Los más terribles permiten tomar el control de los programas ejecutados con privilegios de administrador;
- **Generación de error de sistema**. El objetivo de algunos puntos vulnerables es saturar un programa informático para que "se bloquee".

Con estas prácticas el intruso puede obtener información como horarios de trabajo, claves de acceso, nombres de empleados e infiltrarse indirectamente en la organización y/0 empresa así como también acceder a la información de manera sencilla.

3.2.2 Amenaza

Las principales amenazas actuales a la seguridad son:

- *Las utilizadas para comprometer la seguridad de los sistemas*; como escanear/explorar otros sistemas para encontrar puertas traseras para obtener acceso no autorizado y los ataques del tipo DoS (Denial of Service).
- *Malware*; como virus informáticos, spyware, troyanos, gusanos, etc.
- *Spammin*; que son sistemas utilizados para enviar correos electrónicos no solicitados

3.3 PRINCIPALES ATAQUES

Cualquier equipo conectado a una red informática puede ser vulnerable a un ataque. Un "**ataque**" consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño.

Los ataques se producen en Internet, en su mayoría, se lanzan automáticamente desde equipos infectados (a través de virus, troyanos, gusanos, etc.) sin que el propietario sepa lo que está ocurriendo; en casos atípicos, son ejecutados por piratas informáticos. Para bloquear estas intrusiones es importante estar familiarizado con los principales tipos de ataques y tomar medidas preventivas.

Los ataques pueden ejecutarse por diversos motivos:

- Obtener acceso al sistema;
- Robar información (secretos industriales o propiedad intelectual)
- Recopilar información personal acerca de un usuario;
- Obtener información de cuentas bancarias u organización,
- Utilizar el sistema de un usuario como un "rebote" para un ataque;
- Usar los recursos del sistema del usuario, en particular cuando la red en la que está ubicado tiene un ancho de banda considerable.

3.3.1 Ataques redes LAN inalámbricas

3.3.1.1 Access Point Spoofing

Access Point Spoofing o "Asociación Maliciosa"; en este caso el atacante se hace pasar por un accesspoint y el cliente piensa estar conectándose a una red WLAN verdadera. Ataque común en redes ad-hoc.

El AP furtivo puede “atacar” al cliente Wifi de distintas formas:

• Espiando la conversación

• Enviando contenido falso (ej.: exploits)

• Redirigiendo los pedidos a sitios malicioso

3.3.1.2 ARP Poisoning

"Envenenamiento ARP", es el ataque al protocolo ARP como el caso del ataque denominado "Man in theMidle". Una computadora invasora X envía un paquete de ARP reply para Y diciendo que la dirección IP de la computadora Z apunta hacia la dirección MAC de la computadora X, y de la misma forma envía un paquete de ARP reply para la computadora Z diciendo que la dirección IP de la computadora Y apunta hacia la dirección MAC de X. Como el protocolo ARP no guarda los estados, las computadoras Y, Z asumen que enviaron un paquete de ARP request solicitando esta información, y asumen los paquetes como verdaderos. A partir de este punto, todos los paquetes enviados y recibidos entre las computadoras Y, Z pasan por X (hombre en medio)

3.3.1.3 WLAN Scáners

WLAN Escáners o "Ataque de Vigilancia", consiste en recorrer un local, área que se desea invadir para descubrir redes WLAN activas en dicho local, así como equipamientos físicos, para un posterior ataque o robo.

3.3.1.4 Wardriving / Warchalking

Se llama de "Wardriving" a la actividad de encontrar puntos de acceso a redes inalámbricas mientras uno se desplaza por la ciudad en un automóvil y haciendo uso de una notebook con una placa de red wireless para detectar señales.

3.4 DEBILIDADES DE WPA:

Si se emplea WPA como mecanismo de seguridad los puntos de acceso únicamente aceptan autenticación y cifrado WPA, no permitiendo conectarse a usuarios sin WPA. Por otro lado, un usuario configurado para utilizar WPA no se conecta a puntos de acceso sin WPA. El problema que aún mantiene WPA es que se basa en el algoritmo de cifrado RC4, y como se ha comentado anteriormente ya se le han encontrado vulnerabilidades.

3.5 DEBILIDADES DE WPA2:

Las redes inalámbricas basadas en WPA2 son consideradas como las más seguras. Teóricamente, la difusión y multidifusión de claves representan otra vulnerabilidad. Todos los nodos de la red necesitan conocerlas, y un atacante que descubra una de las claves puede, al menos, espiar el intercambio de claves entre el punto de acceso y la estación de trabajo.

Gracias al diseño de seguridad del estándar WPA2, las modernas redes inalámbricas disponen ahora de una seguridad bastante eficaz. El mayor factor de incertidumbre es con el usuario. Hoy en día, cuando un intruso obtiene acceso a una moderna infraestructura WLAN y consigue acceder a la red y causar daños, la causa suele ser un punto de acceso configurado de forma negligente. Por tanto, hay que tomar algún tiempo para considerar cuidadosamente cada una de las opciones del router de la red. Si deseamos reducir aún más el riesgo residual, podemos añadir a la WLAN protección basada en software. Si utilizamos un túnel, como una VPN con IPSec, podemos incluso aumentar la barrera para los atacantes experimentados. Como suele ocurrir, el sistema operativo libre Linux, con sus muchos componentes de seguridad incorporados, es una elección perfecta para la eliminación del riesgo residual.

3.6ATAQUE WPA / WPA2-PSK

WPA y WPA2 se diferencian poco conceptualmente y difieren principalmente en el algoritmo de cifrado que emplean. Mientras WPA basa el cifrado de las comunicaciones en el uso del algoritmo TKIP [Temporary Key Integrity Protocol], que está basado en RC4 al igual que WEP, WPA2 utiliza CCMP [Counter-mode/CBC-MAC Protocol] basado en AES [Advanced Encrytion System]. La segunda diferencia notable se encuentra en el algoritmo utilizado para controlar la integridad del mensaje. Mientras WPA usa una versión menos elaborada para la generación del código MIC [Message Integrity Code], o código "Michael", WPA2 implementa una versión mejorada de MIC.

Entre las vulnerabilidades de WPA/WPA2 radica la utilización de clave pre compartida para pequeñas redes, lógicamente, a la hora de elegir cómo mantener segura la red doméstica, mejor decantarse por WPA2-PSK debido a que la fortaleza de cifrado de AES es netamente superior a la de TKIP.

Aunque se han descubierto algunas pequeñas debilidades en WPA/WPA2 desde su lanzamiento, ninguna de ellas es peligrosa si se siguenunas mínimas recomendaciones de seguridad. La vulnerabilidad más práctica es el ataque contra la clave PSK de WPA/WPA2. Como ya hemos dicho, la PSK proporciona una alternativa a la generación de 802.1X PMK usando un servidor de autenticación.

Es una cadena de 256 bits o una frase de 8 a 63 caracteres, usada para generar una cadena utilizando un algoritmo conocido: PSK = PMK = PBKDF2(frase, SSID, SSIDlength, 4096, 256), donde PBKDF2 es un método utilizado en PKCS#5, 4096 es el número de hashes y 256 la longitud del resulta-do. La PTK es derivada de la PMK utilizando el 4-Way Handshake ytoda la información utilizada para calcular su valor se transmite en formato de texto. La fuerza de PTK radica en el valor de PMK, que para PSK significa exactamente la solidez de la frase.

El segundo mensaje del 4-Way Handshake podría verse sometido a ataques de diccionario o ataques offline de fuerza bruta. La utilidad cowpatty se creó para aprovechar este error, y su código fuente fue usado y mejorado por ChristopheDevine en Aircrack[4] para permitir este tipo de ataques sobre WPA.

El diseño del protocolo (4096 para cada intento de frase) significa que el método de la fuerza bruta es muy lento (unos centenares de frases por segundo con el último procesador simple). La PMK no puede ser pre-calculada (y guardada en tablas) porque la frase de acceso está codificada adicionalmente según la ESSID. Una buena frase que no esté en un diccionario (de unos 20 caracteres) debe ser escogida para protegerse eficazmente de esta debilidad. Para hacer este ataque, el atacante debe capturar los mensajes de 4-Way Handshake monitorizando.

3.7 GESTIÓN DE LA SEGURIDAD

El fin de la seguridad, y por tanto de su gestión, es mantener la confidencialidad, integridad y disponibilidad de la información (mensajes, documentos, páginas web, datos, aplicaciones.)

La gestión de la seguridad, desde este punto de vista holístico para la organización, engloba desde los mecanismos para toma de decisión de las medidas de seguridad a implantar, hasta la ejecución de los planes previstos en caso de incidente, pasando por la administración, atención y supervisión día a día de la información y su uso, y la de los equipos y dispositivos que la soportan.

En líneas generales, la gestión de la seguridad a nivel organizativo incluye la definición de la estructura y responsabilidades del equipo que se ha de ocupar de la seguridad tanto lógica como física. También comprende la definición de las políticas y los planes de seguridad en base a criterios de gestión de riesgos, contemplando las estrategias y actuaciones para alcanzar los niveles de seguridad necesarios y las acciones a realizar en caso de incidente para la recuperación de la actividad, evaluación de daños, etc.

3.8RECOMENDACIONES TÉCNICAS DE SEGURIDAD

En la tabla 1.6 se ilustran las recomendaciones básicas de seguridad que han de tomarse de manera general en la protección tanto a nivel empresarial como a nivel personal, debemos tener en cuenta que las medidas las hemos dividido por niveles que van desde bajas, medias y altas.

Nivel	Recomendaciones de seguridad
Baja	Realice la gestión y administración de cuentas de usuario y contraseñas.
Baja	Gestione el mantenimiento y actualización de los productos antimalware, antifraude, antispyware, antispam y filtros de contenidos personales
Baja	Construya redes privadas utilizando las funciones básicas del SO y de los dispositivos de red.
Media	Eliminar datos predeterminados como SSID, contraseñas de aplicaciones de administración y acceso al router desde internet.
Media	Instale, configure y gestione cortafuegos a nivel de red.
Alta	Gestione la autenticación de clientes y empleados mediante productos de certificación digital
Alta	Activar un método de cifrado de datos (mínimo de 128 bits)

Tabla 1.6 Recomendaciones de seguridad

Al momento de implementar una Red LAN WiFi se recomienda hacer uso de uno de los Protocolos de Seguridad como WPA ó WPA2 puesto que actualmente estos dos protocolos presentan las mejores herramientas de autenticación y cifrado.

CONCLUSIONES

CONCLUSIONES

Durante el desarrollo de las redes alámbricas han aparecido mecanismos, que trataban de garantizar la seguridad de dichas redes. Los equipos informáticos han ido evolucionando paralelamente, permitiendo realizar gran cantidad de cálculos en tiempos cada vez más pequeños. Por este motivo mucho de esos mecanismos han resultado ser menos seguro de lo que inicialmente se pensó.

Este caso en el sistema previo de protección WEP, sin embargo se destaca que por años fue una medida eficaz de protección de redes inalámbricas, pero con la aparición de enormes vulnerabilidades en su cifrado de datos se vio la necesidad de implementar un sistema más robusto.

Actualmente existen varios protocolos de seguridad como, WPA y WPA2 que pueden ser implementados en las Redes WLAN para prevenir ataques e intrusiones a la Red. Las variantes de WEP, WPA y WPA2, son protocolos diseñados para trabajar con y sin un servidor de manejo de llaves.

La encriptación a nivel de capa de enlace (WPA, WPA2) es una medida de seguridad comúnmente utilizada, pero no garantiza confidencialidad punto a punto. Si se se necesita seguridad a nivel de capa de enlace se recomienda el uso de IEEE 802.11 (WPA2)

El algoritmo de cifrado AES actualmente se utiliza en el cifrado de datos en las conexiones WPA2 para los dispositivos inalámbricos 802.11i, quienes a su vez son los más utilizados para conectarse a diversos servicios informáticos.

WPA/WPA2, por ahora, ha demostrado su efectividad en función de los recursos de los que disponga, si bien existen ataques de fuerza bruta contra WPA-PSK, se ha demostrado que es muy difícil conseguir la clave en un tiempo razonable siempre que la clave elegida no sea fácil de deducir.

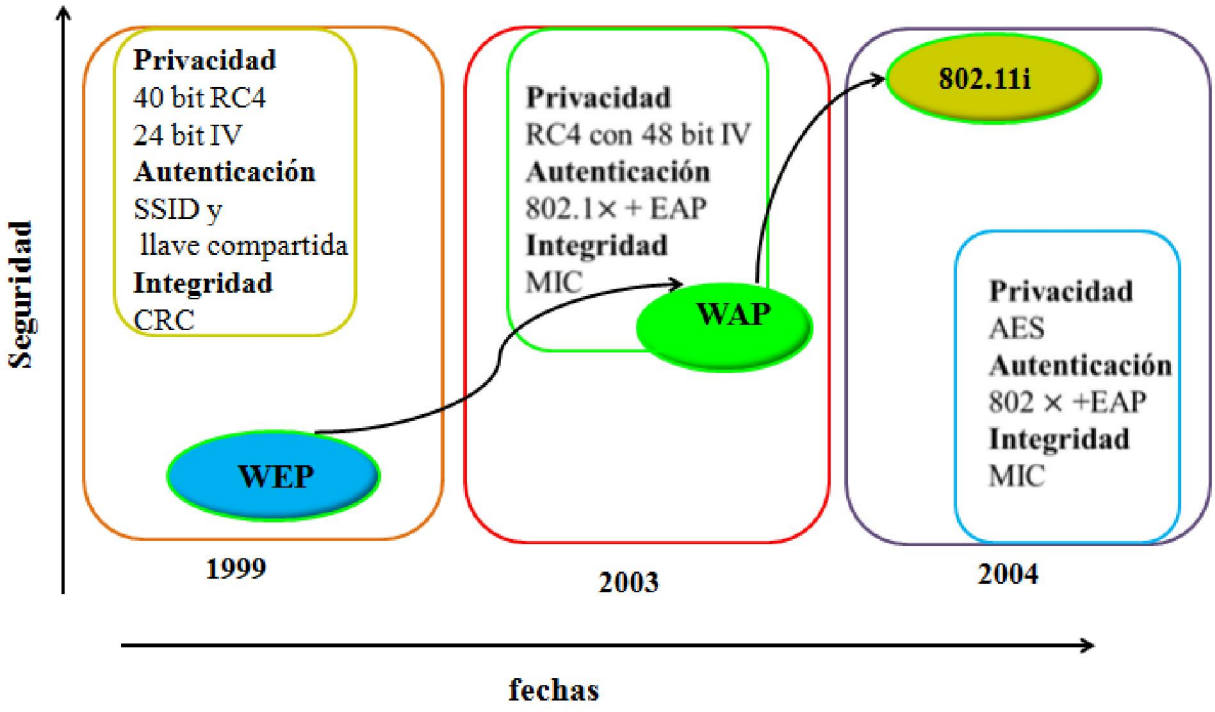
ANEXOS

		WPA	WPA2
Modo personal	Autentificación	PSK	PSK
	Cifrado	TKIP (RC4) / MIC	CCMP (AES) / CBC-MAC
Modo empresarial	Autentificación	802.1x / EAP	802.1x / EAP
	Cifrado	TKIP (RC4) / MIC	CCMP (AES) / CBC-MAC

Diferentes modos de WPA Y WPA2

	WEP	WPA	WPA2
Cifrado	RC4	RC4	AES
Longitud de la clave	40 bits	128 bits	128 bits
Duración de la clave	24- bit IV	48-bit IV	48-bit IV
Control de claves	Ninguno	EAP	EAP

Características más destacadas de los protocolos de cifrado



Mejoras en la seguridad

REFERENCIAS BIBLIOGRÁFICAS

[1] IEEEStandards association

http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[2] Fred Halsall: 1998

Comunicación de datos, redes de computación y sistemas abiertos;

Edit. Pearson Educación 4ta edición; México DF

[3] RFC 2716

[4] Protocolo de autenticación RADIUS (remoteAutentication Dial-in User Service, RFC 2865 del año 2000)

[5] RFC 2058

[6] Estándares Federales de procesamiento de la información

Páginas Web:

http//:docs.hp.com/en/T1428-90071.pdf

http//:hwagm,elhacker.net/wpa/wpa.htm

www.wirelessmundi.com

Seguridad en Redes Inalámbricas/ Alberto Escudero Pascual, LaNeta, IT +46/

www.wilac.net/tricalcar – Versión final. Octubre 2007

Maldonado López, F, 2009, Modelo de seguridad para datos y servicios de telecomunicaciones sobre redes de distribución de energía eléctrica – PLT, Universidad Nacional de Colombia.http://www.bdigital.unal.edu.co/1769/

GLOSARIO DE TÉRMINOS

LAN: Redes de área local; cualquier sistema interconectado de comunicación en un área especifico.

IEEE 802.11: Norma que especifica la tecnología WLAN

WLAN: Redes de área local inalámbrica.

WiFi (IEEE 802.11): Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica

Access Point (AP): Cualquier entidad que tiene funcionalidad de estación y provee acceso a servicios de distribución vía inalámbrica para estaciones asociadas.

XOR: Puerta lógica o-exclusiva; operador lógico que convierte a estado verdadero si, y solo si, uno de los operadores (no ambos) es verdadero. Para A y B las posibles combinaciones son:

Sniffer: Programa de captura de paquetes de red; puede ser usados con fines didácticos, maliciosos o constructivos.

WEP: Privacidad Equivalente al Cableado; fue el primer mecanismo de seguridad que se implementó bajo el estándar 802.11 aprobado por la IEEE y opera en la capa dos del modelo OSI.

RC4: Algoritmo de encriptación utilizado por WEP.

ICV: (Integrity Check Value) Código de integridad, mediante el algoritmo CRC-32. Este código de integridad se concatena con la trama, y es empleado por el receptor para comprobar si la trama ha sido alterada durante la transmisión.

CRC: Comprobación de redundancia cíclica; es un código de detección de errores usado frecuentemente en redes digitales y en dispositivos de almacenamiento para detectar cambios accidentales en los datos.

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.

WPA:(Wifi Protected Access) El algoritmo de Acceso Protegido Wifi se desarrolló para mejorar el nivel de seguridad existente en WEP.

EAP: (Extensible Authentication Protocol) es una autenticaciónframework usada habitualmente en redes WLANPoint-to-Point Protocol.

EAPOL: EAP Over LAN, protocolo usado en redes inalámbricas para transportar EAP.

TKIP: (Temporary Key Integrity Protocol)es también llamado hashing de clave WEPWPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos.

RADIUS: (*Remote Authentication Dial-In User Server*) Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.

MIC: (Modulación por impulsos codificados)MIC o *PCM* es un procedimiento de modulación utilizado para transformar una señalanalógica en una secuencia de bits (señal digital).

CCMP: Es un cifrado de datos mejorado mecanismo diseñado para la encapsulación de confidencialidad de los datos y con base en el modo de contador con CBC-MAC (MCP) de la AES estándar.

AES: También conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

CBC-MAC: un encadenamiento de bloques de cifrado código de autenticación de mensaje (CBC-MAC) es una técnica para la construcción de un código de autenticación de mensaje a partir de una cifra de bloque .

802.1x: Es un estándar de control de acceso y autenticación basado en la arquitectura cliente / servidor, que restringe la conexión de equipos no autorizados a una red.

CHAP: es un protocolo de autenticación por desafío mutuo (CHAP, en inglés: Challenge Handshake Authentication Protocol).Es un método de autentificación remota o inalámbrica.

TLS: Protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

DoS: Es un ataque de denegación de servicio (ataque DoS) o distribuido de denegación de servicio (DDoS ataque) es un intento de hacer un recurso de la máquina o de la red no esté disponible para su uso previsto usuarios .