# Seguridad en Redes Inalámbricas 802.11

Say Hood Chiu
Universidad Central de Venezuela, Fac. Ciencias
Caracas, Venezuela, 1053
schiu@tyto.ciens.ucv.ve

## Abstract

A WLAN presents a great amount of advantages, but this technology also implies security risks, between which this the fact that whatever is within the perimeter of Point Access (AP) it can try to accede to the network, if it is does not count on mechanisms and protocols that guarantee the security of the information and access to the same one.

One is due to consider that when we worked with a twisted network conventional we have a security extra, because to connect itself to the same one normally it is necessary to accede to the cable around which the data circulate or to the physical devices of communication of the same one. In the case of the WLAN, the information it travels through air, which makes more accessible people nonwished that you to their pleasure can explode. It is for that reason that next will expose methods or mechanisms that allow to create or to improve schemes of security for these radio networks.

**Keywords:** Encriptación, Security, Standard, Access, Authentication.

## Resumen

Una WLAN presenta una gran cantidad de ventajas, pero esta tecnología también implica riesgos de seguridad, entre los cuales esta el hecho de que cualquiera que se encuentre dentro del perímetro de Access Point (AP) puede intentar acceder a la red, si está no cuenta con mecanismos y protocolos que garanticen la seguridad de la información y acceso a la misma.

Se debe tener en cuenta que cuando trabajamos con una red cableada convencional disponemos de un extra de seguridad, pues para conectarse a la misma normalmente hay que acceder al cable por el que circulan los datos o a los dispositivos físicos de comunicación de la misma. En el caso de las WLAN, la información viaja a través del aire, lo que hace más accesible a personas no deseadas que puedan explotarlas a su gusto. Es por ello que a continuación se expondrán métodos o mecanismos que permiten crear o mejorar esquemas de seguridad para dichas redes inalámbricas.

**Palabras claves:** Encriptación, Seguridad, Estándar, Acceso, Autenticación.

## 1 Seguridad de las redes inalámbricas

### 1.1 Wardriving

Es un método para detector redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como una laptop o un PDA. El método es simple y consiste en que el atacante simplemente pasea con el dispositivo móvil y en el momento en que se detecta la existencia de una red, realiza un análisis de la misma ubicando los puntos de acceso con sus datos (SSID, WEP, direcciones MAC, entre otros).

Para realizar el Wardriving se necesitan pocos recursos. Los mas habituales son una laptop con una tarjeta inalámbrica, un dispositivo GPS el cual es usado para ubicar el AP en un mapa de coordenadas, opcionalmente una antena direccional para recibir el trafico de la red desde una distancia considerable y software apropiados para verificar puntos de acceso como por ejemplo: AirSnort, Kismet, AirTools o NetStumbler, entre otros.

## 1.2 Warchalking

Se trata de un lenguaje de símbolos utilizados para marcar sobre el terreno la información que fue recopilada en el Wardriving, es decir, difundir la existencia de redes inalámbricas; de forma que puedan ser utilizadas por aquellas personas interesadas que pasen por el lugar. Su simbología es la siguiente:

SSID
)(
*Nodo Abierto*
Ancho de banda

SSID
()
*Nodo Cerrado*

SSID Contacto
(W)
*Nodo WEP*
Ancho de Banda

Primeramente se identifica el nombre del nodo o el SSID, luego se identifica el tipo de red, bien sea abierta, cerrada o con WEP, y por ultimo se especifica la velocidad máxima de la red; por ejemplo:

MiRed
)(
1.5

En el ejemplo se señaliza una red inalámbrica con SSID "MiRed", abierta y dispone de un ancho de banda de 1.5Mbps.

## 1.3 Mecanismos y Protocolos de Seguridad de IEEE 802.11

### 1.3.1 Mecanismos de autenticación OSA y SKA

El estándar 802.11 ofrece dos métodos de autenticación:
OSA (Open System Authentication, Autenticación de Sistema Abierto)
SKA (Shared Key Authentication, Autenticación de Clave Compartida)

#### 1.3.1.1 OSA

Este mecanismo consiste en autenticar todas las peticiones de los usuarios. OSA consta de dos pasos; el primero consiste en que la estación que quiere autenticarse con otra o con el AP, le envía una trama que contiene la identidad (SSID Service Set Identifier) de esta estación emisora. El segundo paso, la otra estación (receptora) o el AP envía a la estación emisora otra trama que indica si se reconoció o no la identidad proporcionada por ella.

El principal problema de este mecanismo es que no realiza ninguna comprobación y, además, todas las tramas de gestión son enviadas sin ningún tipo de encriptación.

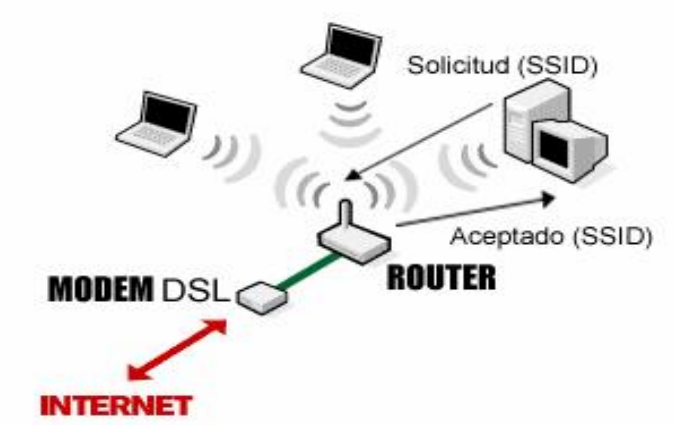


Figura 1.1: Autenticación de Sistema Abierto

1.3.1.2 SKA

Este mecanismo se basa en cada estación debe poseer una clave compartida, la cual es recibida a través de una canal seguro e independiente de la red 802.11; por lo que cada estación que posea una clave va a poder autenticarse con otra por medio de un conociendo (secreto) compartido. WEP es el algoritmo de encriptación utilizado en este mecanismo.

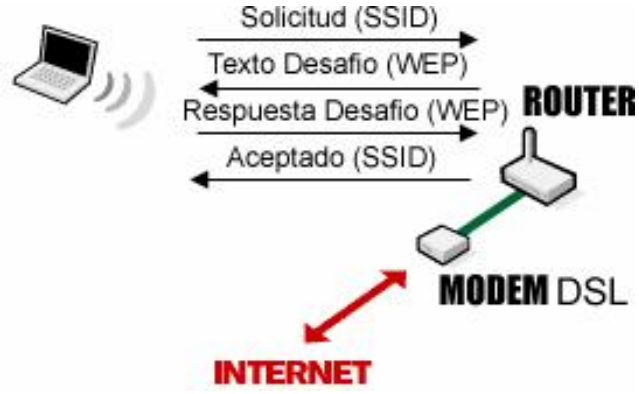


Figura 1.2: Autenticación de Clave Compartida

1.3.2 Protocolos de encriptación WEP

El protocolo WEP (Wired Equivalent Privacy, Privacidad Equivalente a la Cableada), es un estándar por el comité 802.11, implementado en la capa MAC y soportado por la mayoría de los fabricantes de dispositivos inalámbricos; WEP comprime y cifra todos los datos que se envían a través de ondas de radio, encriptando el cuerpo y el CRC de cada trama 802.11 antes de la transmisión, utilizando un algoritmo de encriptación simétrico RC4; la estación receptora, ya sea un punto de acceso o una estación cliente, es la encargada de desencriptar la trama.

WEP se diseño para cumplir con los siguientes objetivos de seguridad:

- Confidencialidad: la meta fundamental de WEP es prevenir escuchas casuales que puedan robar información.
- Control de Acceso: proteger el acceso a la infraestructura de la red inalámbrica, lo cual se logra a través del descarte de paquetes que no están debidamente encriptados.
- Integridad de los Datos: este objetivo se logra previniendo la manipulación (por terceras personas) de los mensajes transmitidos. Un campo de Checksum es incluido en el WEP para este propósito.

Funcionamiento

El cifrado WEP utiliza una clave secreta compartida y el algoritmo de cifrado RC4 como se dijo anteriormente. El punto de acceso y todas las estaciones que están conectadas a el deben utilizar la misma clave compartida. A continuación se detalla el proceso:

Se utiliza una palabra clave para autenticarse, por lo que muchos AP piden una frase y luego a partir de ella, se generan claves distintas para garantizar al máximo el azar en la elección de la misma, o simplemente se pide clave que respete las restricciones de longitud que se configure.

Para el cifrado de cada trama se añadirá una secuencia cambiante de bits, que se llama vector de inicialización (IV), con el fin de que no se utilice siempre la misma clave de cifrado y descifrado. Así, dos mensajes iguales no generaran el mismo resultado de cifrado, ya que la clave va cambiando.

Si se utiliza calves WEP de 64 bits, cinco octetos (40 bits) son clave y 24 bits restantes son el IV, para el caso de claves WEP de 128 bits, 104 bits son clave y 24 son IV.

Proceso de Cifrado:

Se elige el IV (24 bits)
Se unen la clave WEP y el IV para generar una secuencia de 64 o 128 bits, a este valor se e llama RC4 keystream.
Se pasa esa secuencia por un algoritmo RC4 para generar un cifrado de esa clave en concreto, que tiene una longitud igual al payload (cuerpo + CRC) de la trama mas un valor de integridad del mensaje a transmitir (ICV), el cual es usado para comprobar que el mensaje ha sido descifrado correctamente y se añade al final del mensaje.
Se hace un XOR (Exclusive OR) entre el mensaje y RC4 keystream generando el mensaje cifrado.
Se añade al mensaje cifrado el IV para que el destinatario sea capaz de descifrar el mensaje.

Proceso de descifrado:

Se lee el IV del mensaje recibido
Se une el IV a la clave WEP
Se genera el RC4 keystream
Se hace XOR entre el mensaje cifrado y el RC4 keystream y se obtiene el mensaje y el ICV
Se comprueba el ICV para el mensaje obtenido.

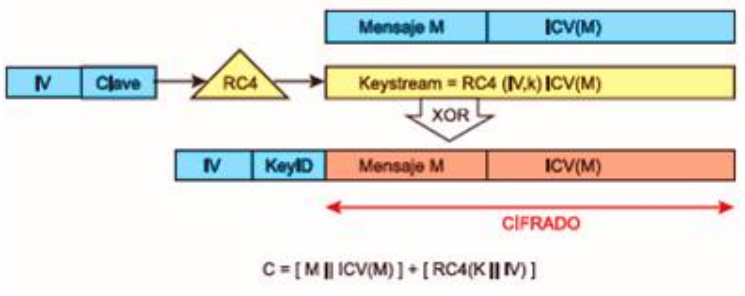


Figura 1.3: Encriptación WEP

### 1.3.3 Filtrado por direcciones MAC

Como parte del estándar 802.11, cada interfaz de radio o dispositivo tiene una única dirección MAC asignada por el fabricante. Para incrementar la seguridad inalámbrica es posible configurar el AP para que acepte solo ciertas direcciones MAC y boquee todas las demás, es decir, se crea una lista de direcciones MAC que serán permitidas por el AP para conectarse. Esta técnica puede ser muy compleja si es implementada en grandes organizaciones, pues puede llegar a consumir mucho tiempo en configuración y mantenimiento, por lo que se recomienda usar en redes pequeñas.
El filtrado MAC es una medida básica para evitar que el primero que se encuentre dentro del área de captación del AP, pueda acceder a la red, lo cual resulta muy efectivo para prevenir accesos no autorizados.

## 1.4 Estándar de seguridad IEEE 802.1x

IEEE 802.1x es un estándar propuesto por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), que es implementado ampliamente por los fabricantes de redes de área local tanto cableadas como inalámbricas. Dicho estándar fue diseñado para ofrecer seguridad perimetral de la red, específicamente en autenticación y control de acceso a nivel de puerto, para usuarios LAN cableadas e inalámbricas; cabe destacar que el estándar originalmente fue diseñado para redes cableadas pero totalmente adaptables a las redes inalámbricas empleando claves dinámicas en lugar de claves estáticas utilizadas en la autenticación WEP por lo que el sistema se compone de:

Estaciones clientes
Puntos de Accesos
Servidores de Autenticación (AS)

### 1.4.1 Protocolo de autenticación extensible EAP

Es uno de los elementos básicos del 802.1x desarrollado como mejora del Point to Point Protocol PPP, el cual usa como método de autenticación “username” y “password”.

EAP utiliza métodos de autenticación arbitrarios, que sirve como soporte a protocolos propietarios de autenticación, gestiona las contraseñas en mecanismos de desafió-respuesta y es capaz de trabajar con tecnología de clave publica, pudiendo así utilizar métodos de autenticación a través de certificados, tarjetas inteligentes o credenciales.

El estándar IEEE 802.1x describe como encapsular mensajes de EAP en tramas Ethernet, es decir, el funcionamiento del protocolo EAP en redes LAN ya sea cableadas o inalámbricas (EAP over LANs, EAPOL).

Adicionalmente, para contrarrestar las debilidades de 802.11, diversos fabricantes crearon varios métodos EAP, entre los cuales encontramos:

EAP-LEAP (Light EAP), desarrollado por Cisco y el cual provee un mecanismo de autenticación mutua basada en password, es decir, se requiere que la estación del usuario se autentique contra la red, pero que también la red se autentique contra el usuario, asegurando de esta manera que los usuarios son los que dicen ser, también se introduce el uso de claves dinámicas por sesión.

EAP-TLS (Transport Layer Security EAP) desarrollado por Microsoft, el cual ofrece autenticación mutua, credenciales seguras y claves de encriptación dinámicas; requiere de la distribución de certificados digitales por lo que puede llegar a producir overhead .

EAP-TTLS (Tunneled TLS) permite solo certificados del servidor, no de cliente; permite que los usuarios sean autenticados dentro de las WLANs con las credenciales existentes, utilizando criptografía de clave publica/privada, es mas sencillo de gestionar y económico que EAP-TLS.

Además de los ya mencionados existen numerosas variantes de EAP, como por ejemplo: EAP-md5, EAP-AKA, EAP-Fast, EAP-PEAP, etc.

### 1.4.2 Servidor de autenticación RADIUS

RADIUS (Remote Authentication Dial-UP User Service), es un servidor de punto final que es responsable de recibir solicitudes de conexión y de la autenticación de los usuarios para luego retornar toda la información de configuración necesaria para el cliente. Este servidor desempeña la autenticación utilizando EAP. Una de las características importantes es la capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, pudiendo utilizar estos valores para generar estadística.

Actualmente existen muchos tipos de servidores RADIUS, tanto comerciales como de código abierto.

### 1.4.3 Funcionamiento de 802.1x

El proceso de autenticación se lleva a cabo de la siguiente manera (ver figura 1.4), el cliente establece una conexión al AP (una tarjeta de red conectada a un punto de datos o una tarjeta de red inalámbrica asociada con un punto de acceso). En este punto el cliente se encuentra en un estado no autorizado, ya que ninguna dirección IP le es asignada o no se le permite de ninguna manera el acceso a la red, es decir, que el AP solo le permite al cliente enviar mensajes 802.1x necesarios para su autenticación (estos son mensajes EAP sobre Wireless EAPOW). Entonces es

cuando el cliente envía una solicitud de acceso a la red (Mensaje "EAP start") al AP (802.1x define el uso de este protocolo) mandando las credenciales al usuario, estas pueden ser el nombre de usuario y contraseña (u otra forma de identificación). Luego, el AP reenvía esta petición al servidor de autenticación RADIUS para su aprobación y si las credenciales son validas, envía de regreso un desafió al autenticador y este desempaqueta el datagrama IP y lo reempaqueta dentro del EAP, sobre un protocolo LAN (EAPOW), para luego enviar el mensaje al cliente. Si el cliente responde de manera exitosa, el servidor le responde a través del AP, con un mensaje de éxito ("EAP Succes"), de lo contrario responde con un mensaje de fallo ("EAP Failure"). De esta manera queda establecida la autenticación, aunque el autenticador también pueda prepararse para imponer diferentes atributos o reglas en cada cliente, proveyendo así varios niveles de restricciones de acceso a los mismos.

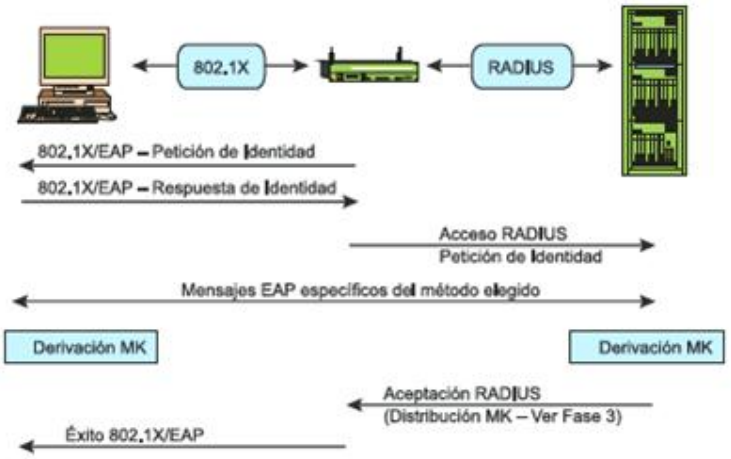


Figura 1.4: Proceso de Autenticación

## 1.5 Acceso Protegido Wi-Fi

Wi-Fi (Wireless Fidelity), es un estándar para redes inalámbricas desarrollada por la IEEE basada en las especificación de la IEEE 802.11 y es una marca que pertenece a la Wi-Fi Alliance, organización comercial que se encarga de probar y certificar los equipos que cumplen con los estándares IEEE 802.1x

Existen tres tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11 (802.11 a/b/g), un cuarto estándar se espera que este listo para este ano 802.11n

Este estándar surge como solución provisional a la aprobación final de estándar 802.11i y para resolver los inconvenientes de encriptación WEP , utilizando TKIP (Protocolo de Integridad de Clave Temporal), para prevenir ataques de repetición, proveer integridad en los mensajes, privacidad entre otras nuevas funcionalidad.

### 1.5.1 WPA-PSK y WPA-Enterprise

WPA (Wireless Protected Access), es un sistema para proteger las redes inalámbricas Wi-Fi, creado para corregir las deficiencias del sistema previo WEP.

WPA usa un password maestro a través del cual el sistema genera claves para cifrar el tráfico de la red, que cambian continuamente usando el protocolo TKIP; además las claves nunca son rehusadas eliminando el riesgo de que puedan ser descubiertas. Incluye también los beneficios de autenticación del estándar 802.1x, lo que le permite al sistema chequear quien se esta registrando contra una base de datos central de usuarios conocidos.
Este sistema ofrece dos métodos de autenticación de usuario y manejo de claves:

- WPA-PSK (WPA Pre-Shared Key): normalmente usado en ambientes donde no se cuenta con servidores de autenticación (RADIUS). Se usan claves pre-compartidas estáticas a partir de las cuales se generan nuevas claves de encriptación usando el protocolo TKIP. Con la autenticación PSK, los usuarios deben introducir la clave maestra manualmente en los puntos de acceso e introducir la misma clave en cada dispositivo cliente que accede a la red inalámbrica.

- WPA-Enterprise (WPA Empresarial): para este caso se requiere de un servidor de autenticación como punto final y el uso de EAP, teniendo en cuenta que también usa TKIP.

Cuando se usa TKIP con la configuración PSK la idea y las operaciones son las mismas que cuando se opera con un servidor de autenticación, en este ultimo caso una clave maestra llamada PMK (Pairwise Master Key), es generada vía intercambios entre el cliente y el servidor de autenticación. La clave PMK es usada para la generación de claves de encriptación a nivel de MAC.

WPA es compatible con las especificaciones de seguridad de IEEE 802.11i, es decir, WPA es un subconjunto del actual proyecto 802.11i.

Actualmente ya esta puesta en marcha WPA2, lo cual viene siendo la versión certificada del estándar 802.11i pero con mejoras.

### 1.5.2 Protocolo de integridad de clave temporal TKIP

TKIP (Temporal Key Integrity Protocol) es una alternativa a WEP que repara los problemas de seguridad y no requiere hardware diferente que el necesario para soportar a WEP. En otras palabras el hardware soportado por WEP también soporta TKIP siempre y cuando tenga el firmware del dispositivo actualizado.

Como WEP, TKIP usa el cifrado de flujo RC4 tanto para encriptar como para desencriptar y todos los dispositivos involucrados deben conocer la misma llave secreta. Esta llave secreta es de 128 bits y es llamada clave temporal o TK (Temporal Key). TKIP usa un vector de inicialización (IV) de 48 bits, el cual es suficiente para transmitir 218.474.976.710.656 paquetes sin repetir el IV, el cambio de la clave se hace cada 10.000 paquetes.

A pesar de que el TK es compartido, todos los participantes involucrados generan una clave RC4 diferente, esto es debido a que todos los participantes de la comunicación realizan dos fases de generación de una única clave por paquete (PPK PerPacket Key), para esto se usa la dirección MAC de emisor, la clave secretan el IV de 48 bits, teniendo así claves diferentes para cada dirección que opera sobre el enlace.

Por ultimo TKIP usa un MIC (Message Integrity Code), diseñado para el hardware existente. Esto es para detectar las modificaciones en el mensaje, El MIC es una función criptográfica de una sola vía y es calculado sobre las direcciones MAC origen, destino y texto plano (datos).

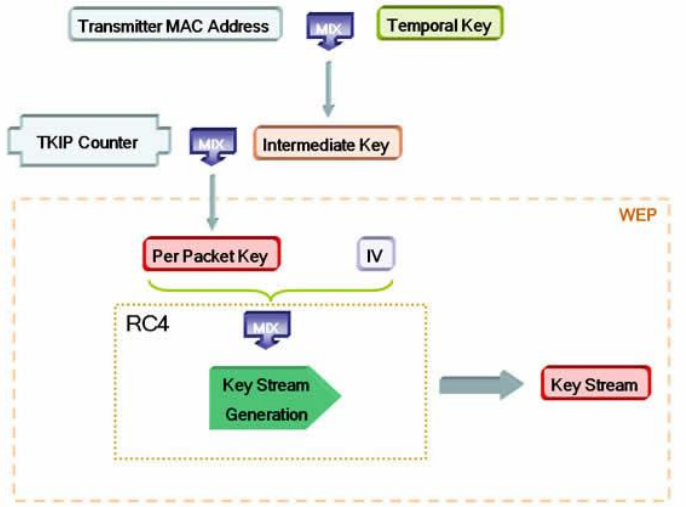


Figura 1.5: TKIP

## 1.6 Estándar 802.11i (Redes de seguridad robustas)

Es un estándar desarrollado por la IEEE y aprobado por Wi-Fi Alliance en Septiembre del 2004, también conocido comercialmente como WPA2, el cual incluye nuevos métodos de encriptación y autenticación.

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 sirte tanto para redes domesticas como para grandes empresas. La nueva arquitectura para redes wireless se llama Robust Security Network (RSN) y utiliza autenticación 802.1x, distribución de claves robustas y nuevos mecanismos de integridad y seguridad.

RSN solo aceptara maquinas con capacidades RSN, pero IEEE 802.11i también define una red transicional de seguridad (Transitional Security Network TSN), en la que pueden participar sistemas RSN y WEP

El establecimiento de un contexto seguro de comunicación consta de 4 fases:

Acuerdo sobre la política de seguridad
Autenticación 802.1x
Derivación y distribución de las claves
Confidencialidad e integridad de los datos

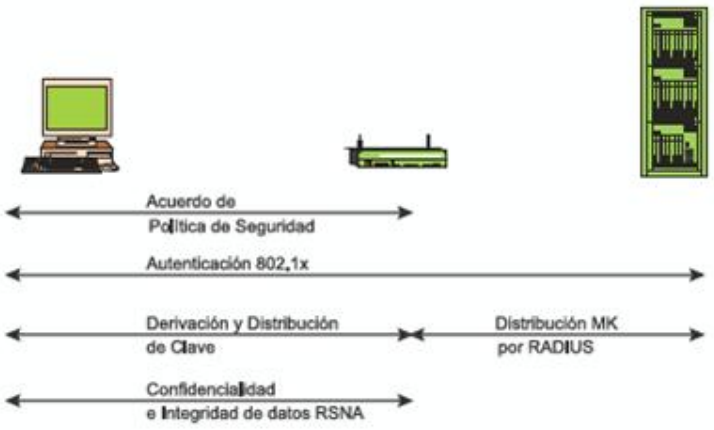


Figura 1.6: IEEE 802.11i

Finalmente se implementa un sistema para la creación de claves nuevas al inicio de cada sesión, sigue haciendo uso del estándar 802.1x, usa AES como algoritmo de encriptación con claves de 128 bits, un nuevo sistema de integridad (CCMP), soporte para redes ad-hoc y sigue siendo totalmente compatible con WPA. TPKI sigue también siendo usado

### 1.6.1 Counter Mode with CBC-MAC CCMP

Este protocolo es el complementario al TKIP y representa un nuevo método de encriptación basado en AES, cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC. Así como el uso de TKIP es opcional, la utilización del protocolo CCMP es obligatorio en 802.11i

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

En este proceso de encriptación, se utiliza la misma clave temporal tanto para el cálculo del MIC como para la encriptación del paquete. El MIC se calcula a partir de un IV formado por el PN y datos extraídos de la cabecera de la trama. El IV se convierte en un bloque AES y su salida a través de la operación XOR conformara el siguiente bloque AES.

### 1.6.2 Advanced Encryption Standard AES

Es un esquema de cifrado adoptado como un estándar de encriptación, se califica como el sucesor de DES (Data Encryption Standard), tiene un tamaño de bloque fijo de 128 bits y tamaño de llaves (Keys) de 128, 192 o 256 bits.

AES opera en un campo finito determinado, un arreglo de 4x4 de bytes, llamado state, el cifrado se forma en los siguientes 4 pasos:

SubBytes
ShiftRows
MixColumns
AddRoundKey

En la siguiente figura se muestra gráficamente los pasos para la implementación del cifrado.

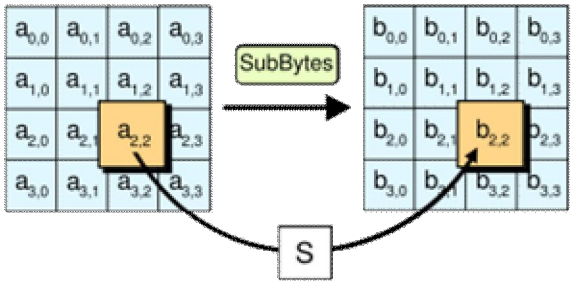


Figura 1.7: SubBytes

En la fase de SubBytes, cada byte en el state es reemplazado con su entrada en una tabla de búsqueda fija de 8 bits, $S$; $b_{ij} = S(a_{ij})$.

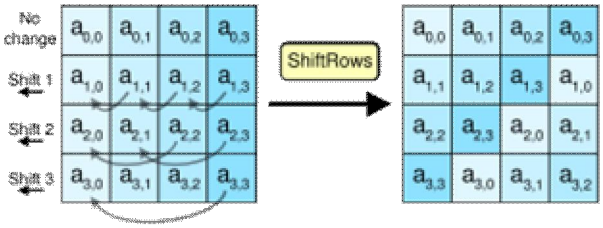


Figura 1.8: ShiftRows

En el paso ShiftRows, los bytes en cada fila del state son rotados de manera cíclica hacia la izquierda. El número de lugares que cada byte es rotado difiere para cada fila.

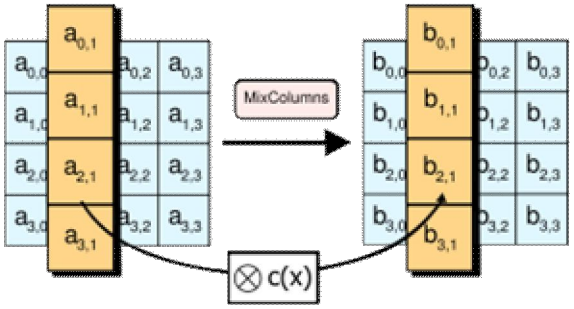


Figura 1.9: MixColumns

En el paso MixColumns, cada columna del state es multiplicada por un polinomio constante $c(x)$.

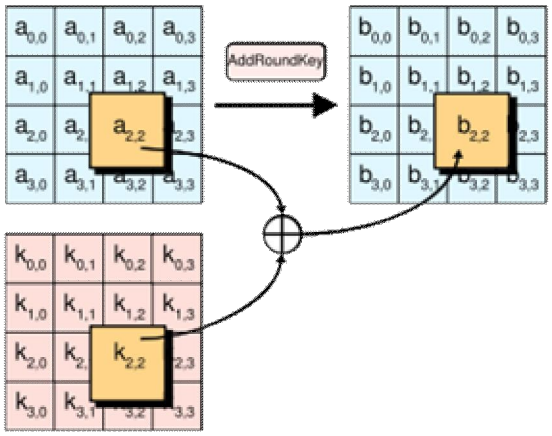


Figura 1.10: AddRoundKey

En el pasoAddRoundKey, cada byte del state se combina con un byte de la subclave usando la operación XOR.

### 1.7 Tabla Comparativa

| | WEP | WPA | WPA 2 |
|---|---|---|---|
| Cipher | RC4 | RC4 | AES |
| Key Size | 40 bits | 128 bits encryption<br>64 bits authentication | 128 bits |
| Key Life | 24-bit IV | 48-bit IV | 48-bit IV |
| Packet Key | Concatenated | Mixing Function | Not Needed |
| Data Integrity | CRC-32 | Michael | CCM |
| Header Integrity | None | Michael | CCM |
| Replay Attack | None | IV Sequence | IV Sequence |
| Key Management | None | EAP-based | EAP-based |

Figura 1.11: Tabla comparativa

## Referencias

[1] Alapont, V. Seguridad en Redes Inalambricas. E- Book (Junio, 2005), pp. 4-14.
[2] Garaizar, P. Seguridad en Redes Inalámbricas 802.11 a/b/g: Protección y Vulnerabilidades. E-Book (Marzo, 2005, pp. 71-194.
[3] Martinez, F. WEP/WAP/WAP2. E-Book (Diciembre, 2006). pp. 2-16.
[4] Morales, J. y Hontecillas, D. Seguridad en Redes Inalámbricas IEEE 802.11: Criptografía y Seguridad de redes. E-Book (Abril, 2004). pp. 16-22.
[5] Salcedo, R. y Terrones E. Evaluación de los Mecanismos de Seguridad y Protocolos de Seguridad desarrollados para Redes Inalámbricas 802.11b. TEG (Octubre, 2004), pp. 20-43.
[6] http://hwagm.elhacker.net/
[7] http://es.wikipedia.org
[8] http://www.monografias.com
[9] http://www.microsoft.com/technet
[10] http://www.saulo.net
[11] http://www.wi-fi.com/