RIESGOS DE SEGURIDAD Y METODOS DE DEFENSA PARA REDES DE AREA LOCAL INALAMBRICA IEEE 802.11

RICARDO ANTONIO AGUIRRE PEDROZA
JAIME MAURICIO VILLARREAL RESTREPO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE CIENCIAS DE INGENIERÍA
DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
CARTAGENA DE INDIAS D.T. Y C.
2007

RIESGOS DE SEGURIDAD Y METODOS DE DEFENSA PARA REDES DE AREA LOCAL INALAMBRICA IEEE 802.11

RICARDO ANTONIO AGUIRRE PEDROZA
JAIME MAURICIO VILLARREAL RESTREPO

Monografía para optar al titulo de
Ingeniero Electrónico

Director
David Senior Elles
Magíster en Ingeniería Electrónica

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE CIENCIAS DE INGENIERÍA
DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
CARTAGENA DE INDIAS D.T. Y C.
2007

Nota de aceptación

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Cartagena, 10 de Julio 2007

Cartagena de Indias D. T. y C, 10 de Julio 2007

Señores:

Comité Evaluador

Departamento de Ingeniería Eléctrica y Electrónica

La Ciudad

Respetados Señores

Tengo el agrado de presentar a su consideración el trabajo de grado del cual me desempeño como director de la monografía titulada **"RIESGOS DE SEGURIDAD Y METODOS DE DEFENSA PARA REDES DE AREA LOCAL INALAMBRICA IEEE 802.11"** desarrollada por los estudiantes RICARDO ANTONIO AGUIRRE PEDROZA Y JAIME MAURICIO VILLARREAL RESTREPO, como requisito para obtener el titulo de ingenieros electrónicos.

Atentamente

David Senior Elles

Cartagena de Indias D. T. y C, 10 de Julio 2007

Señores:

Comité Evaluador

Departamento de Ingeniería Eléctrica y Electrónica

La Ciudad

Respetados Señores

Con mucha atención nos dirigimos a ustedes para presentar la monografía titulada: **"RIESGOS DE SEGURIDAD Y METODOS DE DEFENSA PARA REDES DE AREA LOCAL INALAMBRICA IEEE 802.11"** para su estudio y evaluación como requisito fundamental para obtener el titulo de Ingeniero Electrónico.

En espera que esta cumpla con las normas pertinentes establecidas por la institución nos despedimos

Atentamente

---------- ----------

Ricardo Antonio Aguirre Pedroza **Jaime Mauricio Villarreal Restrepo**

AUTORIZACIÓN

Yo **Ricardo Antonio Aguirre Pedroza**, identificado con número de cédula 73.200.951 de la ciudad de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de grado y publicarlo en el catálogo online de la Biblioteca.

_____

Ricardo Antonio Aguirre Pedroza

C.C.: 73.200.951 de Cartagena

AUTORIZACIÓN

Yo **Jaime Mauricio Villarreal Restrepo**, identificado con número de cédula 73.008.278 de la ciudad de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de grado y publicarlo en el catálogo online de la Biblioteca.

_____

Jaime Mauricio Villarreal Restrepo

C. C.: 73.008.278 de Cartagena

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

- ACK (**ACK**NOWLEDGMENT): Son tramas de gestión de control y coordinación en 802.11, ACK chequea paquetes en búsqueda de errores, el envío de este mensaje significa que el paquete ha llegado correctamente y una vez que esto sucede el canal esta libre para continuar la transmisión de paquetes.
- AES (**A**dvanced **E**ncryption **S**tandard): AES es bloque de cifrado, basado en el algoritmo Rijndael de Joan Daemon y Vincent Rijmen, AES recibe bloques de datos y los convierte en bloques cifrados de igual tamaño 128bits con la información encriptada.
- BEACONS: Son tramas de gestión de para establecer y mantener la comunicación en 802.11, son enviados los APs anunciando su disponibilidad aproximadamente cada 100mS, envía parámetros como el SSID.
- CBC-MAC (**C**ipher **B**lock **C**haining – **MAC**): Es una técnica que utiliza los bloques de mensajes AES y realiza una operación XOR subsiguiente con cada bloque de mensaje, resultando en el bloque final de 128bits.
- CCK (**C**omplementary **C**ode **K**eying): Es una técnica de modulación utilizada en WiFi junto con las técnicas de espectro distribuido.
- CCMP (Counter-Mode / **C**ipher Block **C**haining **M**essage Authentication Code **P**rotocol, protocolo de encriptación utilizado en WPA2, basado en la suite de cifrado de bloques AES.

- CRC (**C**yclic **R**edundancy **C**heck): Es un Pseudo-algoritmo utilizado en el protocolo WEP para el chequeo de errores de integridad en la transmisión.
- DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol): Es un protocolo que permite la asignación automática de direcciones IP a las terminales clientes que requieren acceso.
- EAP (**E**xtensible **A**uthentication **P**rotocol): Protocolo que flexibilidad en la elección de protocolos de autenticación entre suplicantes y servidores de autenticación.
- EAPOL (**EAP O**ver **L**AN): protocolo usado en redes inalámbricas para transportar EAP.
- EAP-SIM (**EAP S**uscriber **I**dentity **M**odule): Permite incorporar dispositivos celulares a la interfaz WiFi y autenticarse utilizando 802.11X.
- EAP-TLS (**EAP T**ransport **L**ayer **S**ecurity): Es un esquema de autenticación empleado en RSN.
- GATEWAY: Puerta de enlace este permite transferir datos entre dos aplicaciones o redes incompatibles entre si, sirviendo como traductor.
- GEK (**G**roup **E**ncryption **K**ey): Clave para la encriptación de datos multicast
- GIK (**G**roup **I**ntegrity **K**ey): Clave de encriptación para trafico multicast utilizada en TKIP.
- GTK (**G**roup **T**ransient **K**ey): Clave derivada de la GMK.

- HSRP (**H**ot **S**tandby **R**outer **P**rotocol): Protocolo de redundancia de Cisco para establecer tolerancia ante fallas de gateway
- ICV (**I**ntegrity **C**heck **V**alue): Es un valor de 4bytes que previene la modificación de mensajes en transito detectando bits corruptos, los bits del mensaje se combina con el CRC para la transmisión.
- KCK (**K**ey **C**onfirmation **K**ey): Clave de integridad que protege los mensajes en el handshake.
- KERBEROS V5: Protocolo que provee servicios de seguridad para redes IP, con el uso de credenciales de acceso que pueden ser utilizadas con 802.1X.
- Keystream: El cifrado de flujo es una secuencia de datos pseudo aleatorios para crear el texto cifrado, en el proceso de TKIP.
- Group Key Key ID: Es una clave encontrada en la cabecera del CCMP no encriptada para ser utilizada en la computación del MIC en WPA2.
- MIC (**M**essage **I**ntegrity **C**ode): Es un campo de datos para la integridad de los datos, basado en el Algoritmo Michael.
- MK (**M**aster **K**ey): Clave principal conocida por el suplicante y el autenticador tras el proceso de autenticación 802.1X.
- MPDU: **MAC P**rotocol **D**ata **U**nit, paquete de datos antes de la fragmentación.
- MSDU: **MAC S**ervice **D**ata **U**nit, paquete de datos después de la fragmentación.
- OSP: Open Short Path.

- PEAP (**P**rotected **EAP**): Se encarga que el proceso de autenticación de EAP sea realizado de manera privada al momento de establecer una conexión segura y completar la negociación. En la actualidad es susceptible a ataques.
- PMK (**P**airwise **M**aster **K**ey) clave principal de la jerarquía de pares de claves.
- PN (**P**acket **N**umber): Contador de tramas en el CCMP.
- **P**robe **R**equest: Mensaje inicial para el inicio del establecimiento de comunicaciones.
- PSK (**P**re **S**hared **K**ey): Clave derivada de una frase clave, sustituye a la PNK enviada por un servidor de autenticación.
- PTK (**P**airwise **T**ransient **K**ey): Clave derivada de la PMK.
- RC4: Algoritmo de encriptación utilizado por WEP.
- RSN (**R**obust **S**ecurity **N**etwork): Mecanismo de seguridad de 802.11i (TKIP, CCMP etc.).
- RSNA (**R**obust **S**ecurity **N**etwork **A**ssociation): Asociación de seguridad usada en una RSN.
- Nonce: Es un número o cadena de bits utilizada en procesos de autenticación para evitar su reutilización en ataques de retransmisión de mensajes.
- TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol): Protocolo de encriptación usado en WPA basado en el algoritmo RC4 (como en WEP).
- Trafico de red: Este puede ser ***unicast*** dirigido hacia una sola estación, ***multicast*** hacia grupos de estaciones y ***broadcast*** dirigido hacia toda la red.

- TSC (**TKIP S**equence **N**umber): Contador de repetición en TKIP similar al Extended IV.
- TSN (**T**ransitional **S**ecurity **N**etwork) Sistemas de seguridad previos a 802.11i.
- UNII (**U**nlicensed **N**ational **I**nformation **I**nfraestructure): Banda de frecuencias de los 5GHz, utilizada en 802.11a

INTRODUCCION

El presente documento tiene como objetivo presentar el uso de la familia de estándares IEEE802.11 b/g/a para el despliegue seguro de redes de área local inalámbricas. Ente sus características básicas están posibilidad de posicionar o extender redes en lugares de difícil o imposible uso de redes cableadas, compatibilidad de equipos de diversos fabricantes, uso de roaming o itinerancia entre puntos de acceso inalámbrico sin que el usuario móvil pierda conexión mientras se desplaza entre las celdas, incluir nuevos usuarios sin modificar la arquitectura física de la oficina u hogar donde se ubica la red; a las cuales se les suma el bajo costo de dispositivos necesarios para la puesta en marcha de la red. Todas estas características básicas de este tipo de redes y la topología manejada son descritas en el primer capitulo.

IEEE 802.11 utiliza como medio de transmisión ondas de radio, este medio de transmisión brinda algunas de las características que han popularizado su uso en las redes actuales, pero también hay que tener en cuenta que este medio de transmisión es susceptible a recibir ataques inalámbricos, clasificados según la meta elegida por el intruso o hacker. La descripción de los posibles ataques en redes WiFi se estudia en el capitulo 2.

Todo administrador de red debe cumplir con responsabilidad el mantenimiento de la seguridad, por lo cual debe tener en cuenta los posibles ataques a los que se encuentra susceptible la red y las amenazas dirigidas hacia los dispositivos autorizados por parte de personal ajeno a la red que por curiosidad, diversión o dinero intentan ingresar. Es necesario que el administrador conozca el funcionamiento y existencia de esos ataques con el fin de establecer y usar políticas de gestión de la seguridad que eviten o replieguen los ataques realizados, protejan la integridad de las comunicaciones de la red con uso de protocolos de encriptación y autenticación de dispositivos que desean establecer comunicación, proteja la integridad de la información y mantenga confidencialidad en la red. El capitulo 3 muestra un estudio de técnicas de seguridad, válidas y complementarias en WiFi.

Para finalizar en el último capitulo, se encuentra un sumario de los programas y herramientas empleadas por los hackers o intrusos en el momento de realizar ataques y algunos programas de defensa para proteger redes inalámbricas; estos programas deben ser objeto de estudio para comprender los riesgos a los que puede estar expuesta una red con políticas de seguridad, también se muestran medidas complementarias de seguridad.

1. REDES INALAMBRICAS

Estas palabras hacen referencia a cualquier red de telecomunicaciones cuyas interconexiones entre nodos esté implementada sin el uso de cables, como lo es una red de computadores y cualquier otro equipo informático que tenga un sistema de transmisión que utilice ondas electromagnéticas como capa física de transmisión de la red, según el modelo OSI, y así establecer la conexión de estos equipos. Estas redes, en teoría, permiten manejar mayores velocidades que una red cableada y con la posibilidad de obtener movilidad en áreas que pueden abarcar cientos de metros para crear el entorno de red local entre ordenadores o terminales situados en un mismo edificio o grupo de edificios, sin tener que modificar la arquitectura de forma drástica en el lugar donde será implementada.

1.1 Modelo OSI

El modelo de Interconexión de Sistemas Abiertos OSI[1], es un modelo de referencia creado en 1984 por la ISO con el objetivo de encontrar un conjunto de reglas guías en la creación de nuevos equipos de redes por parte de los fabricantes, y de este modo mejorar la compatibilidad de los equipos. El modelo OSI se encuentra divido en 7 capas que poseen funciones especificas, que indica su tarea en la red. En la tabla 1, se describe brevemente la función de las capas.

[1] Open Systems Interconnection.

Tabla 1. Descripción Modelo OSI

MODELO OSI			
#	**Capas**	**Unidad de Datos PDU**	**Descripción**
1	Física	Datos	Conexión Física hacia la red por Medios guiados (Cables) o Medios no guiados (inalámbricas), la forma de transmisión y las características del medio.
2	Enlace de datos	Tramas	Suministra direccionamiento físico MAC, distribuye las tramas, detecta, corrección y notificación de errores, mantiene control de flujo y define la topología de la red. LLC
3	Red	Paquetes	Determina las rutas para el envió de datos, crea dirección lógicas IP y proporciona gestión en la gestión de redes.
4	Transporte	Segmentos	Confiabilidad en las conexiones punto a punto sin errores TCP, transporta los datos dentro de paquetes sin importar la red física que se utilice y aísla las capas superiores de distintas implementaciones de tecnología de red en las capas inferiores.
5	Sesión	Datos	Es la responsable de la administración, inicio, mantenimiento y terminación de las sesiones lógicas entre usuarios finales. Mantiene el enlace entre terminales que transmiten archivos.
6	Presentación	Datos	Representación de la información a datos reconocibles, encriptación de los datos.
7	Aplicación	Datos	Ofrece acceso a los servicios de las demás capas y aplicaciones a los procesos de red

1.2 IEEE 802.11

El protocolo IEEE[2] 802.11 o Wi-Fi, es un estándar publicado en 1997 que contiene el conjunto de protocolos de comunicaciones para redes de área local inalámbrica, basado en las primeras dos capas del modelo OSI: la capa física y la de enlace. Define velocidades de transmisión de 1 y 2 Mbit/s por señales infrarrojas IR y en la banda de frecuencias ISM[3] de 2.4GHz. También define el protocolo CSMA/CA[4] como método de acceso. El estándar original tuvo problemas con la

[2] Institute of Electrical and Electronics Engineers
[3] Industrial Scientific and Medical
[4] Carrier Sense Multiple Access with Collision Avoidance

interoperatibilidad entre equipos de diferentes fabricantes, por lo que ha sido modificado en otras ampliaciones que aportan mejoras de servicio, extensiones y correcciones a las especificaciones anteriores, incluyendo cambios en la frecuencia, velocidad y modulación. Por lo anterior, fue remplazado por el 802.11b.

1.2.1 IEEE 802.11b

Esta revisión del estándar original fue publicada en 1999, tiene una velocidad de transmisión máxima de 11Mbit/s, las velocidades de transferencia pueden ser adaptables a 11Mbit/s, 5.5Mbit/s, a 2Mbit/s y 1Mbit/s. Esta opción de elegir velocidades de transferencia de datos es una solución posible si la calidad de la señal se convierte en un problema, dado que a menor velocidad la tasa de datos utiliza métodos menos complejos y mas redundantes para codificar los datos, que serán menos susceptibles a la corrupción por interferencia o atenuación. El IEEE 802.11b funciona en la banda de 2.4GHz y utiliza como método de acceso al medio CSMA/CA.

1.2.2 IEEE 802.11a

El 802.11a también fue publicado en 1999, y a diferencia de los anteriores opera en la banda UNII de los 5GHz, utilizando 52-Subportadoras con OFDM[5] con una máxima tasa de transferencia de 54Mbit/s; las velocidades de transferencia pueden ser reducidas a 48Mbit/s, 36Mbit/s, 24Mbit/s, 18Mbit/s, 18Mbit/s, 12Mbit/s, 9Mbit/s y 6Mbit/s si se requiere. Los equipos 802.11a no son compatibles con 802.11b por la diferencia de bandas, exceptuando aquellos equipos que tengan

[5] Orthogonal Frequency Division Multiplexing.

capacidad dual de bandas. Los productos de 802.11a, debido a la banda en que operan, poseen menor rango de cobertura de red que 802b/g, por la absorción en paredes y otros objetos sólidos. Entre las ventajas de operación que se destacan, gracias a la banda en la que trabaja, se encuentran la menor interferencia por equipos y el requerimiento de antenas más pequeñas pero con sistemas de RF de mayor ganancia.

1.2.3 IEEE 802.11g

Este estándar fue publicado en junio de 2003, funciona en la banda de los 2.4GHz y su tasa máxima de transferencia es de 54Mbit/s. Las velocidades de transferencia son de 48Mbit/s, 36Mbit/s, 24Mbit/s, 18Mbit/s, 12Mbit/s, 9Mbit/s y 6Mbit/s con modulación OFDM, 11Mbit/s y 5.5Mbit/s con CCK para obtener compatibilidad con 802.11b, por último 2Mbit/s y 1Mbit/s utilizando modulación DBPSK/DQPSK+DSS. Los equipos 802.g son compatibles con 802.b reduciendo la velocidad de los primeros, posee problemas de interferencia con otros equipos de la banda de los 2.4GHz, tales como equipos Bluetooth, hornos microondas, teléfonos inalámbricos, micrófonos, etc.

1.2.4 IEEE 802.11n

En la actualidad el IEEE se encuentra trabajando en la publicación de una enmienda al estándar llamada IEEE 802.11n, el cual se espera estar finalizado en Septiembre de 2008. Este estándar contempla el uso de antenas MIMO[6], las cuales utilizan múltiples transmisores y receptores para incrementar la tasa de

[6] Multiple Input Multiple Output

transferencia de datos, utilizando varios canales a la vez e incrementando el rango de cobertura de la red. En enero de 2007 se aprobó el segundo borrador de la enmienda propuesta, 802.11n no esta aún limitado al rango de frecuencia de los 2.4GHz o 5GHz, esto depende del producto especifico que desee implementar compatibilidad con las anteriores enmiendas. Es valido aclarar que el único estándar es el 802.11, las otras versiones son enmiendas que poseen adiciones y correcciones del documento original.

1.3 Wi-Fi Alliance

Es la organización comercial que tiene por funciones probar y certificar los productos que cumplen las especificaciones del grupo IEEE 802.11 y promover el uso de esta tecnología. WiFi es un conjunto de estándares para redes de área local inalámbricas basados en las especificaciones 802.11. Los equipos que poseen la marca registrada de WiFi, superan las pruebas de la alianza incluyendo no solo la interoperabilidad de datos y formatos, sino además los protocolos de seguridad. La Figura 1, muestra el logotipo de Wi-Fi Alliance y el logotipo empleado para las certificaciones de los equipos con WiFi.

Figura 1. Logotipo WiFi Alliance y WiFi Certified[7]

[7] http://www.wifialliance.com/files/WFA_Brand_StyleGuide_May2007.pdf , Página 6

En la tabla 2, se encuentran implementaciones a la familia IEEE 802.11, exceptuando los de prácticas recomendadas 802.11F y 802.11T.

Tabla 2. Versiones del Estándar IEEE 802.11x

IEEE	CARACTERÍSTICAS
802.11	Estándar original para WLAN de 1Mbit/s y 2MBits. En la banda de 2.4GHz con RF.
802.11a	Señal pico de trabajo de 54Mbps por mercadotecnia, Velocidad real bajo condiciones ideales de 23Mbps en la banda de 5GHz. Modulación BPSK, QPSK, 16QAM y 64QAM.
802.11b	Señal pico de trabajo de 11Mbps por mercadotecnia, Velocidad real bajo condiciones ideales de 6Mbps en la banda de 2.4GHz. Modulación DSSS y CCK.
802.11c	Procedimientos de operación en modo Bridge; incluida en IEEE 802.1D
802.11d	Extensión de Roaming Internacional de país a país.
802.11e	Mejoras de QoS, incluyendo la inyección de paquetes.
802.11F*	Inter-Access Point Protocol, removido en febrero de 2006.
802.11g	Señal pico de trabajo de 54Mbps por mercadotecnia, Velocidad real bajo condiciones ideales de 23Mbps en la banda de 2.4GHz. Modulación OFDM, CCK y DBPSK/DQPSK+DSSS. Compatibilidad con 802.11b
802.11h	Manejo del espectro 802.11a en 5GHz para compatibilidad en Europa.
802.11i	Corrección de seguridad, mejora en los protocolos de codificación y autenticación originales.
802.11j	Extensiones para Japón.
802.11k	Mejoras en el manejo de recursos de radio. Propuesto en 2007.
802.11l	Reservado y no será utilizado.
802.11m	Mantenimiento del estándar. Correcciones y remanentes
802.11n	Señal pico de trabajo de 128Mbps por mercadotecnia, Velocidad real bajo condiciones ideales 60Mbps con canales de 20MHz. Frecuencia de 2.4GHz o 5GHz, Antenas MIMO. Septiembre 2008
802.11o	Reservado y no será utilizado.
802.11p	WAVE – Wireless Access for the Vehicular Environment. 2009
802.11q	Reservado y no será utilizado.
802.11r	Fast Roaming. En proceso 2007
802.11s	ESS Extended Service Set Mesh Networking.
802.11T*	Wireless Performance Prediction WPP – Métodos de prueba y recomendaciones métricas. Trabajando 2008.
802.11u	Evaluación propuesta para la compatibilidad con redes que no son 802
802.11v	Wireless Network Management. Propuesta inicial.
802.11w	Protected Management Frames. Propuesta inicial.
802.11x	Reservado y no será utilizado.
802.11y	Operación en los Estados Unidos. Propuesta inicial.

* Estos son documentos independientes, más que correcciones al estándar 802.11

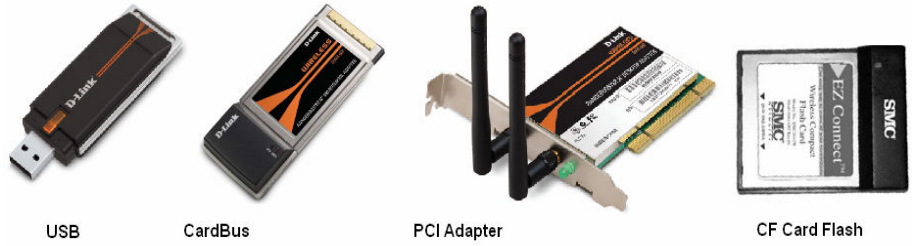
1.4 Dispositivos Wi-Fi

- AP: punto de acceso inalámbrico (Ver figura 2) que conecta clientes a una red LAN cableada, funciona como un Hub Ethernet, permitiendo la transmisión de datos entre los dispositivos inalámbricos y los dispositivos pertenecientes a la red cableada.

Figura 2. Puntos de Acceso Inalámbrico (AP)[8].

- Adaptador de red Inalámbrica: permiten la conexión a la red inalámbrica, estos pueden conectarse a diversos puertos como: CardBus o PCMIA[9] se utiliza en portátiles, CF Card[10] se utiliza en PDAs, las PCI son de uso interno en los puertos de expansión de la motherboard y las USB son de uso externo del Terminal. La figura 3 muestra adaptadores de red inalámbrica.

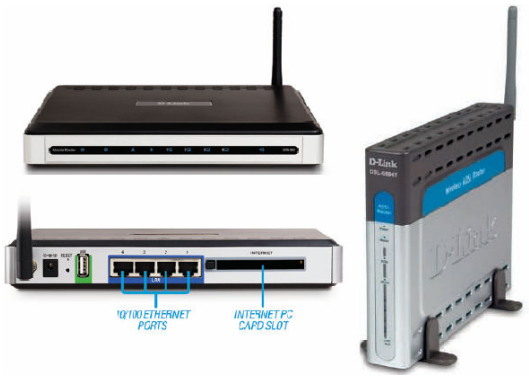
Figura 3. Adaptadores de red inalámbrica[8].



[8] Catalogo de productos DLINK http://www.dlink.com/products/category.asp
[9] Personal Computer Memory Card International Association.
[10] Compact Flash Card Adapter.

- Router Inalámbrico: Es la combinación de AP, con un Switch Ethernet que utilizan el firmware de un router (Ver figura 4). Permiten la conexión a redes Ethernet cableadas e inalámbricas y también incluyen un puerto para la conexión a redes WAN como un cable MODEM o un MODEM DSL.

Figura 4. Ejemplo Routers inalámbricos[8].



- Wireless Ethernet Bridge: El Wireless Ethernet Bridge (Ver figura 5) puede conectar dos redes cableadas separadas físicamente en único enlace inalámbrico, se diferencia del AP porque este conecta dispositivos inalámbricos con cableados a nivel de la capa de enlace.

Figura 5. Ejemplo de Wireless Ethernet Bridge[8].

- Repetidores Wireless o Extensiones de rango inalámbrico: permiten extender el rango de una red inalámbrica para llegar a áreas de difícil acceso inalámbrico como paredes muy gruesas o corredores en forma de L. La figura 6 muestra potenciadores de señal inalámbrica.

Figura 6. Equipos de extensión de rango inalámbrico[8].

- Antenas: Las antenas se dividen dependiendo del rango que cobertura, estas pueden ser direccionales para enviar la señal hacia un punto en concreto, con mayor o menor precisión o pueden ser omnidireccionales emitiendo la señal hacia por lo general 360º grados en el plano horizontal y 75º en el plano vertical cubriendo una mayor área. La figura 7 muestra ejemplos de antenas externas empleadas en equipos WiFi.

Figura 7. Ejemplos de antenas[8].

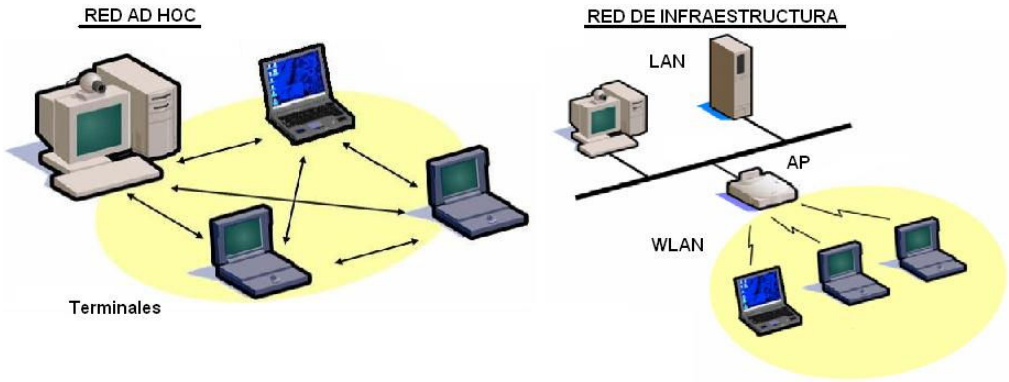
- Otros dispositivos: Aparte de los dispositivos anteriormente mencionados existen teléfonos, PDAs, consolas de videojuegos, cámaras de video, impresoras, lectores de IR, entre otros compatibles con WiFi.

1.5 Topologías de redes WiFi

Existen dos tipos de topología de redes WiFi Ad Hoc o Peer to Peer y de Infraestructura (Ver Figura 8).

- Topología Ad Hoc o Peer to Peer: Cada estación de trabajo se conecta con todos los demás equipos sin ningún tipo de jerarquía, no hay control de acceso y las dimensiones están limitadas al cubrimiento que posean las tarjetas inalámbricas de cada equipo.
- Topología de Infraestructura: Los equipos se conectan a un Access Point (AP) el cual administra el acceso, tiene mayor cobertura que las redes Ad Hoc porque el AP actúa como repetidor, posee mayor control de seguridad que la configuración Ad-Hoc y permiten la conexión a redes cableadas. Un Hotspot es una zona de cobertura WiFi con uno o varios AP que proveen servicios de Internet en lugares públicos de manera gratuita o pagando una suma dependiendo del proveedor.

Figura 8. Redes Ad hoc e Infraestructura[11]



El término BSS es utilizado en redes de infraestructura que utilizan un AP, ESS es cuando se utilizan más de un AP y el término IBSS para redes Ad Hoc.

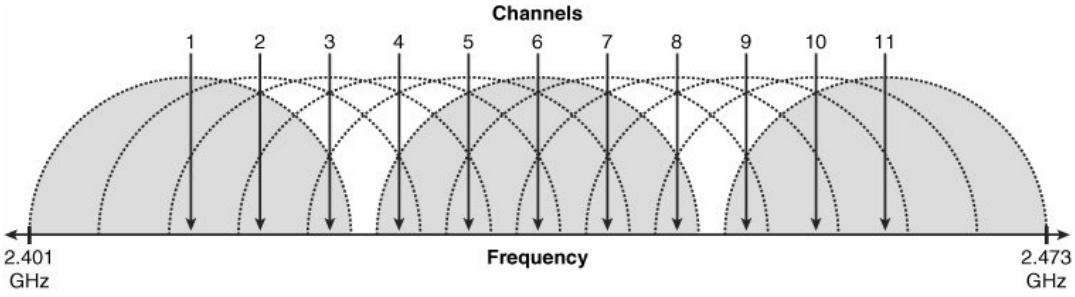
[11] Ohrtman, Frank, Roeder Konrad, WiFi Handbook-Building 802.11b Wireless Networks, Capitulo 2

1.6 Parámetros y Configuraciones de red

SSID: Identificador de Servicios de Red o SSID (también suele llamarse *Network ID* y *Service Area*), puede ser una cadena alfanumérica de hasta 30 caracteres. El fabricante del AP provee un SSID de fábrica, se recomienda cambiar el nombre del SSID, esto permite diferenciar el AP inalámbrico de AP vecinos en el área. Cuando se configuran terminales inalámbricas, se debe utilizar el mismo SSID que se asignó en el AP.

Canales: Este es el canal de radio sobre el cual el AP establecerá la comunicación, si se planea utilizar más de un AP en un área de trabajo se deben asignar diferentes canales para evitar la interferencia de señales. Para el IEEE 802.11b/g existen 14 canales distanciados por intervalos de 5 MHz, el segmento de canales utilizados varía de país en país, en Colombia se permite el uso de los primeros 11 canales. La frecuencia real de transmisión se ensancha a 22MHz por motivos de potencia. Para permitir roaming en una red se deben utilizar los canales 1,6 y 11 como se muestra en la figura 9, ya que estos no interfieren.

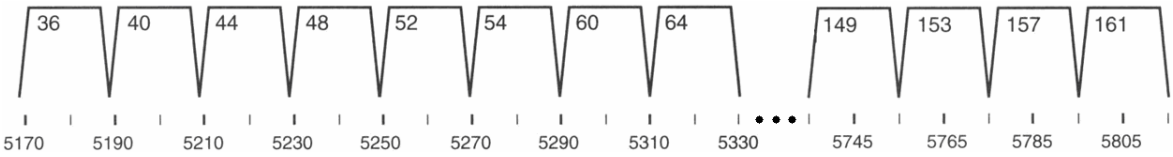
Figura 9. Canales empleados en 802.11b/g[12]



[12] Ohrtman, Frank, Roeder Konrad, WiFi Handbook-Building 802.11b Wireless Networks, Capitulo 7, Secc. 8

En el caso del IEEE 802.11a, existen 12 canales distanciados por intervalos de 20MHz (Figura 10), el ancho de banda ocupado por cada canal es alrededor de 16.6MHz, esto permite que los canales no tengan traslapes entre otros. Algunos países del mundo están permitiendo la operación en las bandas de frecuencia de 5.470 a 5.725GHz para aumentar 12 canales nuevos y poder ofrecer 24. En Colombia se permite el uso de los canales 149 hasta el 161.

Figura 10. Canales empleados en 802.11a[13]



La tabla 3, contiene las frecuencias de los canales para las diferentes redes inalámbricas.

Tabla 3. Canales empleados en 802.11a/b/g

2,4GHz 802.11b/g		5 GHz 802.11a		
Canal	**Frecuencia (GHz)**	**Frecuencia**	**Canales**	**Frecuencia (GHz)**
1	2,412		36	5,180
2	2,417	U-NII Lower Band	40	5,200
3	2,422	5,15 - 5,25	44	5,220
4	2,427		48	5,240
5	2,432			
6	2,437		52	5,260
7	2,442	U-NII Middle Band	56	5,280
8	2,447	5,25 - 5,35	60	5,300
9	2,452		64	5,320
10	2,457			
11	2,462		149	5,745
12	2,467	U-NII Upper Band	153	5,765
13	2,472	5,725 - 5,825	157	5,785
14	2,483		161	5,805

[13] Ohrtman, Frank, Roeder Konrad, WiFi Handbook-Building 802.11b Wireless Networks, Capitulo 7, Secc. 8

Algunos AP ofrecen la opción de selección automática del canal basándose en el ancho de banda utilizado y en la interferencia de canales adyacentes.

Esquema de seguridad: La red inalámbrica siempre debe emplear protocolos de encriptación para la seguridad como WPA2 o WPA. Sin el uso de un esquema de protección la red puede ser vulnerable o utilizada por personal no autorizado. Algunos equipos como AP tienen contraseñas por defecto para su administración, estas contraseñas deben ser cambiados para evitar brechas en la seguridad. La seguridad de la red será tratada con mayor profundidad en el capitulo 3.

Dirección MAC: La dirección MAC es la dirección física del dispositivo de radio en el AP. Este número se encuentra impreso en una etiqueta adjunta al dispositivo. Es posible necesitar este número por problemas de configuración.

Direccionamiento IP dinámico o estático de red WAN: Si la red esta conectada al Internet, se debe tener una IP asignada por el ISP. En la mayoría de casos el ISP asigna la dirección IP de manera dinámica, el router o gateway de Internet debe estar configurado para aceptar direcciones IP asignadas dinámicamente por el servidor DHCP. Es posible, pero poco probable que el ISP requiera direcciones IP estáticas.

Dirección IP local: Aparte de la dirección MAC, el AP necesita tener su propia dirección IP, esta dirección será necesaria para acceder a la página de configuración del equipo mediante un navegador Web. La dirección IP del producto se encuentra en la documentación, en la mayoría de los casos la

dirección será 192.168.xxx.xxx. También es posible que el AP pueda elegir una dirección IP por defecto que este utilizando el router DSL o el cable MODEM, de cualquier forma si ocurre un conflicto de direcciones IP, es recomendable tener los equipos en redes separadas mientras se configura el AP.

Transmisión de potencia del AP: Este es la transmisión de potencia de salida del AP, a mayor potencia mayor rango de cobertura, los AP transmiten a una potencia de salida menor de 30dBm (Un Vatio), esto esta regulado por las agencias gubernamentales de cada país. En redes internas la potencia de salida es usualmente de 13dBm (20mW) a 15 dBm (31.6mW).

Atenuación de la señal: La señal de radio puede volverse más débil como resultado de la interferencia causada por otras señales de radio, la reducción de la señal por otros dispositivos es llamada atenuación. La sensibilidad de receptor es la medida de que tan fuerte es la señal para poder recibir otra señal de radio y poder establecer una comunicación confiable.

Cobertura: La cobertura de la red depende de los elementos en donde trabaje la red, paredes, puertas, ventanas, la potencia de transmisión de los equipos y antenas y del nivel de sensitividad de los equipos receptores. Un alcance común de una red puede estar entre 30M hasta 150M, siendo la primera una oficina con muros gruesos de ladrillo y la segunda una oficina abierta.

2. CLASIFICACIÓN DE ATAQUES A REDES INALÁMBRICAS

Los ataques perpetrados a las redes inalámbricas se pueden dividir en diversas categorías, en la práctica los atacantes pueden emplear combinaciones de ataques de distintas categorías.

- **Ataques al Acecho**
- **Ataques sin conocimiento de las claves**
- **Ataques hacia las claves**

En la tabla 4, se observan una clasificación de los distintos ataques realizados y los nombres de las técnicas empleadas en contra de las redes Wi-Fi.

Tabla 4. Clasificación de ataques en redes Wi-Fi

CLASIFICACION DE ATAQUES EN REDES WI-FI	
TIPO DE ATAQUE	**TÉCNICAS EMPLEADAS**
Ataques de acecho	• Asociación Accidental • Warxing
Ataques sin conocimiento de las claves	• Snooping • Puntos de Acceso Maliciosos • Man-in-the-Middle • Wi-Phishing y Evil Twin • Masquerading y MAC Spoofing • Negación de Servicio (DoS) • Inyección de tráfico
Ataques hacia las claves	• Ataque de Fuerza Bruta • Ataque de Diccionario • Ataques Algorítmicos

2.1 Técnicas Empleadas Por Ataques de Acecho

Se realizan con el fin de brindar información preliminar de la red inalámbrica, la información recopilada por el atacante puede ser utilizada en un futuro para atentar con la integridad de los equipos, la integrad de los datos manejados en la red y ser la base para ataques más avanzados.

- **Asociación Accidental:** Esta sucede cuando el usuario de una Terminal establece conexión a una red wireless privada, mediante un AP o una Terminal con Wi-Fi, sin el conocimiento por parte del usuario del evento ocurrido; sin embargo, la facilidad con la que se realizó la conexión puede ser considerada como una brecha de seguridad por parte del administrador de la red privada, donde los datos de la red se encuentran expuestos al acceso del público. Es un ataque malintencionado hacia una red que en todo caso no es de uso público y no pretende prestar un servicio de *hotspot*.
- **Warxing:** Es el conjunto de actividades que consisten en detectar redes inalámbricas en una ciudad, se divide en diferentes clases generando actividades más específicas. Los usuarios de estas prácticas hacen uso de GPS[14] para determinar la ubicación de las redes con el fin de registrarlos en mapas de redes inalámbricas por ciudades o barrios, emplean modificaciones en las antenas de sus dispositivos para aumentar el rango de búsqueda de las redes. La idea de realizar mapas con redes inalámbricas no se considera como

[14] GPS: Global Positioning System, Sistema de Posicionamiento Global

un ataque, el problema es el uso que se le puede dar a la información obtenida porque ésta puede ser utilizada por la comunidad hacker para la violación de la seguridad en redes inalámbricas privadas; además, la recopilación de información se realiza sin el conocimiento del propietario de la red, de manera secreta hasta que se publican los mapas o bases de datos con la ubicación de las redes. A partir de esta técnica se derivan otras como: Wardriving, Warbiking, Warwalking, Warspying, Warchalking cuyas características se encuentran en la tabla 5.

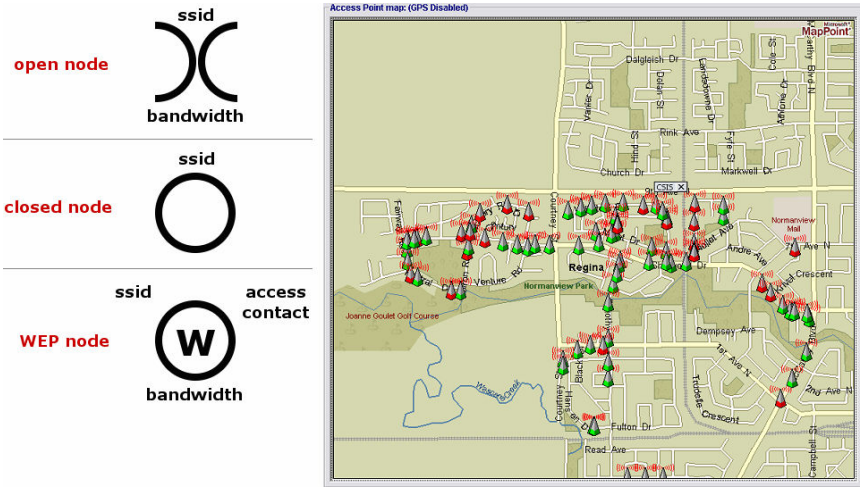
Tabla 5. Clasificación de ataques Warxing

ATAQUE	CARACTERISTICAS
Wardriving	Búsqueda de redes inalámbricas desde un automóvil en movimiento con el uso de un equipo portátil o una PDA
Warbiking	Búsqueda de redes inalámbricas desde un motocicleta en movimiento con el uso de un equipo portátil o una PDA
Warwalking	Búsqueda de redes inalámbricas con el uso de un equipo portátil o una PDA, realizada sin el uso de vehículos.
Warspying	Búsqueda de cámaras inalámbricas instaladas en grandes ciudades, para el control de tráfico, seguridad o webcams. Los hackers observan la transmisión utilizando receptores de video, pantallas LCD, y potenciadores de señal.[15]
Warchalking	Marcado de la red Wi-Fi encontrada con tizas en paredes y/o andenes indicando las características de la red.

En la figura 11 se muestran los símbolos utilizados en el warchalking, estos indican el tipo de red, identifican el nombre del nodo o SSID, el tipo de red abierta o cerrada, el tipo de protección empleada y la velocidad de conexión de la red.

[15] Systm tiene un video realizando Warspying en el siguiente enlace http://revision3.com/systm/warspyingbox

Figura 11. Símbolos warchalking y mapeo de red de una ciudad[16]



2.2 TÉCNICAS EMPLEADAS POR ATAQUES SIN CONOCIMIENTO DE LAS CLAVES

Se realizan por usuarios malintencionados que no tienen conocimiento de las contraseñas de ingreso a la red. En esta categoría de ataques se incluye la modificación de datos por parte del atacante, negar el acceso de la red de los dispositivos autorizados en la verdadera red y detener el flujo de datos de la red imposibilitando su uso.

- **Snooping:** Este ataque es realizado con tarjetas Wi-Fi modificadas por software o hardware para obtener datos de la red inalámbrica victima, protegida con clave. El hacker puede obtener la información valiosa de la red con la captura de paquetes del AP, algunos de los datos obtenidos se encuentra en la tabla 6:

[16] Barrios, Jesús; Conceptos Básicos de Telecomunicaciones Diapositivas DLINK 2005

Tabla 6: Datos Obtenidos a partir de la captura de paquetes

Datos obtenidos por medio de la captura de paquetes
Nombre de la red o el SSID con el que se puede obtener una idea general de lo que pueden realizar los usuarios de la red.
Con los primeros 3 bytes se conoce la dirección MAC del Access Point y el fabricante con la dirección MAC
El numero del modelo basado en la capacidad de información del propietario incluida en los *beacons*[17]. Se pueden buscar fallas y debilidades posibles del dispositivo.
Posible conocer estimado de dispositivos wireless conectados en una red de varios Access Points, observando las diversas direcciones MAC asociadas.
Si la red utiliza WEP, posible conocer si se utiliza una llave compartida o si cada dispositivo posee una clave distinta, por el análisis de los bits de cabecera de la trama IEEE 802.11
Con el análisis de tráfico se puede conocer la frecuencia de la comunicación y el tamaño. El tamaño puede identificar el protocolo empleado al corroborar la distancia.
La longitud de los paquetes da el protocolo utilizado, por ejemplo ciertos mensajes TCP/IP como las tramas ACK[18], tienen una longitud fija y ocurren con regularidad típica.
Los mensajes DHCP[19] descubiertos pueden dar la dirección IP de la red. Certeza si un usuario se encuentra utilizando un navegador Web o trabajando en el servidor local, con los tiempos de ida y venida de los mensajes.

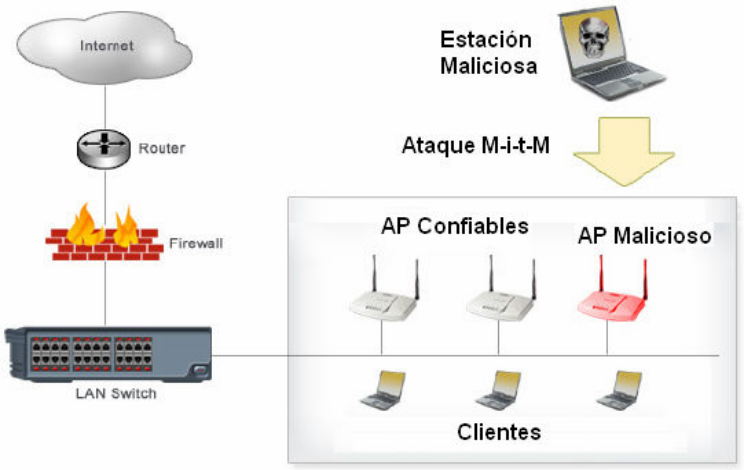
El flujo de la cantidad de datos transmitidos brinda una noción de lo que sucede en la red, aunque no es posible conocer el tipo exacto del suceso por el análisis de la longitud de los paquetes y el tiempo de envío, sin conocer el mensaje enviado. Esta información por si sola tiene un uso limitado, pero combinada con otras herramientas, el atacante puede generar ataques de mayor riesgo para la red.

[17] Los paquetes beacon hacen parte de los paquetes de Management del estándar IEEE 802.11, estos se envían periódicamente aproximadamente cada 100mS para saber cual AP esta disponible.
[18] Las trama ACK (Acknowledgment) o de reconocimiento hacen parte del paquete de control, cuando un paquete es recibido y no posee errores se envía un mensaje ACK y el canal queda disponible.
[19] Dynamic Host Configuration Protocol Protocolo de Asignación de Clientes dinámicos.

- **Puntos de Acceso Maliciosos:** Son AP (Ver Figura 12) instalados en cercanías de una red inalámbrica sin la debida autorización de los propietarios de la red local, usualmente colocados para realizar un ataque del tipo *Man-in-the-middle*. Los AP Maliciosos se clasifican en dos tipos:

  1. Primer tipo: Son colocados de manera arbitraria por el usuario en la empresa para extender la cobertura de su red, si este AP es mal configurado de manera inofensiva o de manera maliciosa conociendo el resultado de sus acciones, puede permitir el acceso a redes seguras por parte de personal no autorizado.
  2. Segundo tipo: Son colocados por Hackers para atacar redes que no emplean autenticación mutua (Cliente-Servidor, Servidor-Cliente) y puede ser utilizado en conjunto con un servidor RADIUS malicioso, dependiendo de la configuración de seguridad de la red victima.

Figura 12. Ataque Man-in-the-middle con un AP Malicioso[20]



[20] Tlatzer, Presentation_ID, Cisco Systems 2003

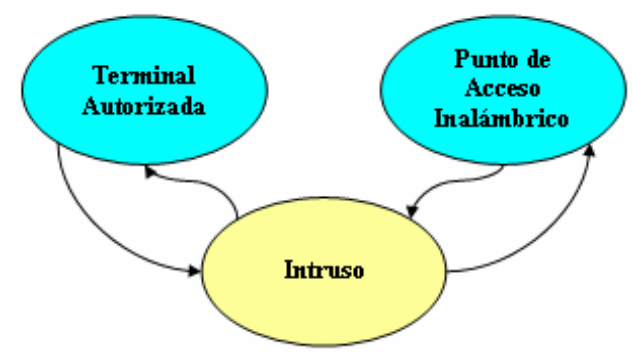
- **Modificación y Man in the Middle:** El atacante puede modificar información enviada como e-mails o números en una transferencia electrónica bancaria, por ejemplo si intercepta una transmisión inalámbrica y cambia la dirección IP de destino, puede enviar la información a cualquier IP conocida mediante el Internet sin cambiar la dirección e-mail de destino, con esto recibe la versión desencriptada del mensaje enviado. Existen dos modos de modificar un mensaje:

  1. Se puede modificar el mensaje en vuelo, lo que es realmente difícil, ya que requeriría del envío de ráfagas de transmisión por radio en el momento exacto para causar que el receptor interprete un bit incorrectamente. Los datos enviados por Wi-Fi no viajan con bits de manera individual, sino en grupos codificados en conjunto para que la tarea de cambiar un único bit en la transmisión sea una tarea difícil, esta modificación puede ser posible en teoría pero es muy difícil de realizar un ataque de este tipo de manera satisfactoria.
  2. Se puede capturar, modificar y reenviar el mensaje, esta técnica es conocida como método de *store and foward*[21], este es llamado ataque de modificación ***man-in-the-middle***. Este ataque es el resultado de la combinación del snooping y de la modificación, en esté el atacante recibe toda la información y reenvía cuidadosamente a los dispositivos terminales

[21] Almacenamiento y Reenvió

extremos la información sin que estos tengan conocimiento que su información ha sido interceptada, como se muestra en la figura 13.

Figura 13. Ataque de modificación "*Man in the Middle*"



En este tipo de ataques, el enemigo detiene la recepción del mensaje por parte del receptor, cuando captura el mensaje, lo modifica y luego lo reenvía al receptor.

El procedimiento utilizado por el atacante se muestra en la tabla 7:

Tabla 7. Procedimiento utilizado en el ataque Man in the Middle

PROCEDIMIENTO UTILIZADO POR EL ATACANTE	
1	Escuchar el mensaje desde el dispositivo autorizado hacia el AP inalámbrico
2	Leer el mensaje hasta que encuentre la *checkword*, esta es utilizada por el receptor para detectar errores en los datos
3	Transmitir una ráfaga de ruido con el fin de corromper la *checkword* con esto el AP desecha el mensaje, pero el atacante ha obtenido una copia del mensaje valido, en esta primera transmisión
4	Falsificar un mensaje *ACK* con la dirección del AP, este mensaje se envía hacia el dispositivo móvil
5	Recalcular la *checkword* correcta y enviar el mensaje capturado hacia el AP; el AP supone que el mensaje proviene del dispositivo móvil
6	Esperar el reconocimiento del AP, enviar una ráfaga de ruido al dispositivo móvil para que este no obtenga el mensaje y no reciba dos mensajes ACK por el mismo paquete

Como se observa el procedimiento no es tan sencillo de realizar, pero si es posible una variación de este ataque, la más sencilla de ejecutar por los atacantes es la de colocar AP maliciosos siguiendo los siguientes pasos:

- El AP malicioso identifica el AP verdadero por adelantado.
- Cuando un dispositivo móvil intenta la asociación con el AP malicioso, este copia los mensajes recibidos y los envía al AP verdadero, substituyendo su dirección MAC.
- Cuando el AP recibe el mensaje de asociación reenviado por el AP malicioso, este le da acceso y el mensaje es capturado por el AP malicioso y luego reenviado hacia el dispositivo móvil.
- Como resultado todo flujo de datos del dispositivo móvil al AP verdadero serán interceptados por el AP malicioso, sin tener las claves de acceso a la red, porque la dirección MAC la cual es alterada no se encuentra encriptada.

Una vez que el enemigo se establezca en medio de las comunicaciones, el atacante tiene una oportunidad de cambiar los datos de los mensajes individuales, a menos que tenga conocimiento del contenido de los mensajes antes de que sean encriptados. El atacante puede intentar modificar la dirección IP de destino, aunque esto puede ser detectado rápidamente por el emisor porque es difícil más no imposible recibir una respuesta ACK.

Un atacante utilizando *man-in-the-middle* puede obtener un mensaje *ICMP*[22] viajando desde el dispositivo móvil hasta el servidor de la red, el atacante puede suponer el tipo de mensaje *ICMP* por la longitud del mismo. La mayoría de mensajes *ICMP* requieren una respuesta del servidor que el enemigo capturara de manera encriptada, este tampoco podrá leer el mensaje por la encriptación pero puede enviar el mismo mensaje *ICMP* encriptado y el servidor le responderá cada vez que este lo haga pensando que provino de un dispositivo valido. El mensaje ICMP contiene un checkword, si el atacante cambia un solo bit y reenvía el mensaje, la palabra clave indicara un error y el mensaje será desechado por no recibir respuesta del servidor. Un atacante puede modificar entonces bits en los datos y en la checkword del mensaje ICMP y enviar esa información de manera sucesiva en miles de combinaciones distintas hasta que se obtenga respuesta del servidor, luego de miles de intentos es posible que el servidor envíe respuesta y pueda obtener la dirección IP del dispositivo móvil y del servidor[23]. En una red que emplee como medio de seguridad WEP, los ataques activos poseen grandes porcentajes de éxito, por su parte los métodos seguridad de WPA y WPA2 son más resistentes a este tipo de ataques.

- **Wi-Phishing:** Ataque de ofrecimiento de conexión de servicio inalámbrica a Internet gratis en lugares públicos, estos AP no son colocados por un proveedor de servicios de Internet ISP sino por un hacker que busca

22 Internet Control Message Protocol. El mensaje ICMP pertenece al protocolo de control de Internet en la capa de red del modelo OSI. Este es enviado entre dispositivos de redes TCP/IP
23 Descripción mas extensa de ataques Man-in-the-Middle con uso de AP maliciosos Borisov, N,I. Goldber and D. Wagner 2001. Intercepting mobile communications: The insecurity of 802.11

aprovecharse de la falta de conocimientos de un usuario. Si este accede el ofrecimiento sin comprobar la procedencia del servicio, los datos que utilice el cliente mientras navega en la red como: contraseñas, cuentas bancarias o números de tarjetas de crédito pueden ser fácilmente capturados por el AP malicioso con un keylogger[24].

- **Masquerading y MAC Spoofing:** El ataque de *Masquerading*[25] es cuando el dispositivo atacante roba la identidad de un dispositivo valido de la red, esto es realizada por atacantes que desean tener ingreso a la red privada sin ser detectados, obteniendo los derechos de acceso que posee el dispositivo real cuando establece una sesión en la red. Cuando el administrador de la red realice el análisis de ingreso a la red puede que no encuentre la presencia del intruso a menos que el atacante notifique su presencia en la red o que este se comporte de manera irregular a cómo lo haría el usuario legitimo, al intentar acceder a áreas restringidas de la red o copiar archivos masivos que puedan verse en el tráfico de la red del sistema.

  El *MAC Spoofing* es el robo de identidad que ocurre cuando el atacante luego de escuchar el tráfico de la red mediante *snooping*, identifica las direcciones MAC de una terminal valida de la red. Los paquetes de la red son obtenidos por programas llamados "*sniffers*", estos capturan los paquetes y los analizan para obtener una dirección MAC, al combinar estos programas con otro tipo de

24 Los Keyloggers son programas que guardan una copia de las teclas presionadas por un usuario.

25 Masquerading significa personificación, hacerse pasar por otra entidad.

software que permita cambiar la dirección MAC del equipo del atacante por la dirección MAC obtenida previamente, el atacante puede ingresar a la red, si el único medio de protección de la red es el filtrado de direcciones MAC. El proceso de obtención de la dirección MAC se muestra en la Figura 14.

Figura 14. Procedimiento en un ataque MAC Spoofing[16]

Los pasos empleados en el ataque son:

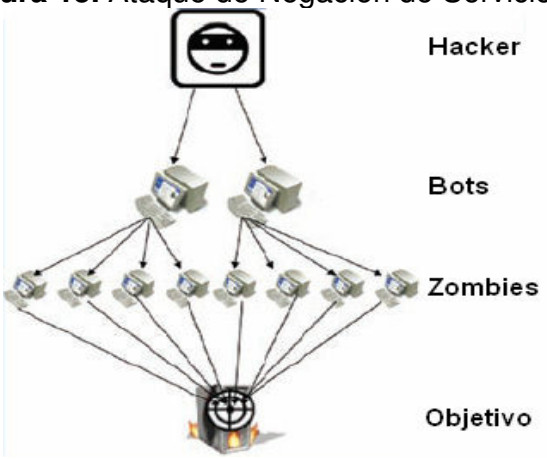
1. El usuario legítimo envía la petición de entrada a la red.
2. El Intruso obtiene la dirección MAC y la hace propia con el uso de un sniffer y de software para alterar su dirección MAC.
3. El intruso accede a la red por que la única protección empleada en esta, es el control de acceso de direcciones MAC.

- **Negación de Servicio (Denial of Service DoS):** En este tipo de ataque, se bombardea a un AP con peticiones de manejo de red falsas como peticiones de asociación, des-asociación, mensajes de conexión satisfactoria prematuros, mensajes de error y otros comandos, causando que los usuarios legítimos no puedan acceder a la red, incluyendo al atacante y deshabilitando el uso de la

red por cierto intervalo de tiempo. Estos ataques son difíciles de prevenir en Internet y usualmente dependen del agotamiento de los recursos del buffer del servidor para que no se pueda generar conexiones validas.

La figura 15 muestra un ataque de DoS en el cual el hacker utiliza un ejército de terminales controladas por Terminales Bots que controlan terminales Zombies las cuales se encargan de realizar los ataques de agotamiento hacia el AP.

Figura 15. Ataque de Negación de Servicios[16].



- **Inyección de tráfico a la red:** Se realiza en contra de los AP expuestos al tráfico de red no filtrado, específicamente a transmitir el trafico de la red como el protocolo "*Spanning Tree*[26]", OSP, RIP y HSRP. El atacante ejecuta un comando de reconfiguración falso en la red afectando a todo equipo de conexión de redes: routers, switches y hubs inteligentes. Como resultado la red

26 Este protocolo es utilizado para evitar la duplicación de datos en la red y que se realice el envío por múltiples vías en la red, agotando recursos innecesarios.

se congestiona, termina cayendo y requiere reprogramar todos los dispositivos inteligentes para su puesta en funcionamiento.

2.3 TÉCNICAS EMPLEADAS POR ATAQUES HACIA LAS CLAVES

Se realizan por usuarios malintencionados en contra de redes protegidas, con el fin de conocer la clave de ingreso desconocida y acceder a la red, el ataque se dirige hacia las claves o el protocolo de protección empleado.

Salvo a los ataques de DoS y de inyección de tráfico el resto de ataques tiene como meta final tener acceso a los datos obteniendo las claves o rompiendo el algoritmo de protección.

Para una red que no posea una infraestructura avanzada de seguridad y no emplee rotación de claves de ingreso de manera continúa, un atacante puede capturar mensajes que viajen en la red y analizarlos. Con este estudio se pueden obtener datos útiles que servirán como medio de comparación para romper la protección en la red.

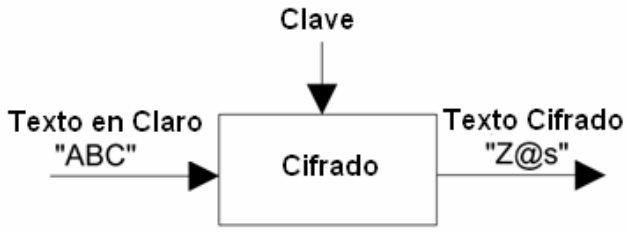
Antes de continuar con los ataques introduciremos los siguientes términos de criptografía:

- Texto en Claro (*Plaintext*): Esta es la información original que se desea proteger mediante el uso de la encriptación.
- Texto cifrado o criptograma (*Ciphertext*): Es la versión encriptada que se envía mediante los enlaces de radio.

- Cifrado (*Cipher*): Es el proceso de convertir el texto claro a texto cifrado mediante la aplicación de las reglas de un algoritmo dado para encriptar y desencriptar el texto.
- Clave (Key): Es el valor secreto utilizado para encriptar y desencriptar un mensaje.

La figura 16 muestra el proceso de encriptación de mensajes utilizando los anteriores términos.

Figura 16. Proceso de encriptación de mensajes[27]



El texto cifrado es el resultado del procesamiento del texto claro con el cifrado, empleando una clave para activar el proceso. Este puede ser comprendido con la siguiente formula:

Texto Cifrado = Cifrado (Clave, Texto en Claro)

Regresando al escenario de la red y el atacante, este último puede obtener una copia del texto cifrado mediante el *snooping*.

Una de las reglas de la criptografía moderna es asumir que el atacante conoce el algoritmo utilizado para la encriptación[28]. Aunque él atacante conoce el texto cifrado y el cifrado empleado, no puede obtener el texto en claro porque le hace

[27] Lehtinen Rick, Computer Security Basics, 2 edición. Sección 6.2
28 Esto se conoce como el criterio de Kirchoff

falta la clave, aun así, puede obtener una muestra del texto en claro del encabezado MAC de la trama IEEE 802.11 ya que este no se encuentra encriptado, con el uso del protocolo TCP/IP parte de la cabecera del mensaje es texto en claro que es convertido en texto cifrado. La cabecera siempre se encuentra al inicio de cada paquete.

Algunos mensajes IP tienen un formato de trama conocido como el DHCP, utilizado en la asignación de direcciones de red, estos están encriptados pero pueden ser identificados por su longitud. En este caso, el atacante puede adivinar correctamente el resto del texto claro.

Existe un ataque llamado ***Evil Twin***, el cual es empleado para obtener el texto en claro, utilizando AP maliciosos que ofrecen servicio de conexión a Internet gratis, en donde el hacker envía un correo electrónico a la victima, persuadiéndola a utilizar un enlace a una pagina Web y obtener así la muestra del texto en claro, una vez que el usuario acepta el link, redirigen al usuario a otras páginas para introducir spyware, troyanos y keyloggers. Las técnicas empleadas por ataques hacia las claves son:

- **Ataque mediante Fuerza Bruta:** Funciona básicamente probando cualquier posible clave hasta encuentra la clave real. Se conoce el texto y el protocolo de cifrado, se inicia el ataque con un valor inicial de ceros y se desencripta el mensaje, se compara con el texto plano o cualquier fragmento que se haya obtenido hasta que estos dos textos coincidan, se continuara el ataque incrementado un bit en la clave hasta encontrarla. El

tiempo requerido para que el ataque funcione depende de la longitud de la clave o mas correctamente de la *entropía de la clave.* Para romper una clave de 40-bits, como la utilizada en el estándar original WEP, se necesitaría intentar con 2^{39} claves distintas[29], el cual equivale a 550 mil millones de claves distintas. Si se realizara el ataque desde una Terminal que pruebe una combinación de claves cada microsegundo, se obtendría la clave en aproximadamente una semana.

Debido a que la clave de 40-bits es débil, muchos sistemas utilizan 128 bits para mejorar la seguridad, el uso de claves más extensas hace que los ataques por fuerza bruta sean completamente inútiles, asumiendo que el algoritmo criptográfico utilizado no posea alguna otra debilidad. Con una clave de 104 bits (Como algunas versiones de WEP) se necesitaría en promedio de 3,200,000 millones de años para encontrar la clave secreta, a razón de probar 100 claves en un microsegundo[30].

- **Ataques de Diccionario:** Derivado del ataque de fuerza bruta, limita el número de intentos de ataque asumiendo que el usuario incluirá exclusivamente letras y números en su clave, reduciendo la entropía de la clave de 104-bits a 78-bits porque estos caracteres solo utilizan 6 bits de cada byte. Estos 78 bits aún siguen siendo difíciles de descifrar por un

29 El número total de combinaciones es 240 pero en promedio se necesita intentar la mitad de ellas antes encontrar la clave verdadera, por lo tanto el número es 239

30 La fórmula empleada para realizar el calculo es la siguiente:

Tiempo Promedio= 2103 /(Intentos por segundo) / (Número de segundo en un año)

ataque de fuerza bruta, esta reducción en el número de claves da inicio a la tarea de utilizar un diccionario de ataques, en la que se utiliza un diccionario o base de datos con diversas contraseñas, nombres, apellidos, calles, números telefónicos, códigos postales, e-mails, faxes, fechas del año, etc.

Con millones de posibles entradas, estos diccionarios son utilizados por el atacante con la muestra del texto cifrado y el texto en claro hasta que coincida con la clave real. Este ataque solo funciona con contraseñas que contengan caracteres alfanuméricos con palabras de uso común o derivadas de estas, omitiendo los caracteres extraños. Existen formas de ocultar la palabra clave, como la **derivación de claves** *(Key derivation)* utilizada por la mayoría de los sistemas de seguridad modernos y que no son susceptibles a ataque con diccionario.

- **Ataque Algorítmicos:** Empleado por aquellos atacantes que intentan romper el algoritmo, en la búsqueda de fallas del proceso de encriptación que puedan exponer el valor de la clave. Este tipo de ataques fueron realizados de manera satisfactoria en contra de WEP, donde se pudo atacar byte por byte a la clave. El tiempo para descubrir la clave es proporcional al numero de bytes empleado por ella. Estos son los ataques más peligrosos ya que una vez que se descubre el método para romper el algoritmo, es fácil para la comunidad hacker escribir programas para descubrir las claves que serán distribuidas masivamente por Internet atentando la seguridad de las redes que empleen dichos algoritmos.

3. MEDIDAS DE DEFENSA Y PROTECCIÓN EN WIFI

El riesgo por parte de enemigos de la red inalámbrica siempre existirá, el reto de los fabricantes y desarrolladores es estar un paso delante de los enemigos, estudiar las técnicas que éstos utilizan y estar constantemente desarrollando mecanismos de seguridad robustos que no den lugar a brechas en los sistemas, en este caso especifico, WiFi.

Este capitulo se divide en tres secciones (ver Tabla 8), donde se muestran el estudio de diversas medidas de seguridad disponibles, primero se mostrarán las medidas de seguridad inalámbrica invalidas, medidas validas y por último, medidas complementarias para asegurar una red inalámbrica WiFi.

Existen una gran diversidad de métodos para asegurar la red, pero ningún método es absolutamente infalible en contra de todos los ataques existentes, por lo tanto la mejor estrategia de defensa es combinar diversas medidas de seguridad teniendo en cuenta los siguientes parámetros:

- Toda red inalámbrica debe estar asegurada.
- El administrador de la red debe conocer como asegurar su red.

- Todas las redes deben estar monitoreadas activamente para descubrir debilidades y brechas en su seguridad.

Tabla 8. Medidas de seguridad en redes WiFi

MEDIDAS DE SEGURIDAD EN REDES WI-FI	
NIVEL DE SEGURIDAD	**MEDIDA UTILIZADA**
Soluciones Invalidas	• Filtrado de direcciones MAC • Direccionamiento IP Estático • Ocultación SSID • Disminución del nivel de señal • Autenticación LEAP • Encriptación WEP • VPN
Soluciones Validas	• Encriptación WPA • Encriptación WPA2
Soluciones Complementarias	• Wireless Protected Setup • WAPI • Firewalls • Tarjetas Inteligentes y Tokens • Redes Honeypots • Wireless Intrusion Detection Systems • Wireless Intrusion Prevention Systems

3.1 Medidas de seguridad inválidas.

Las siguientes medidas son inválidas si se desea imponer un esquema de seguridad robusta en la red para el sistema Wi-Fi, estas se consideran como una pérdida de recursos, tiempo y dinero al momento de ser utilizadas o sencillamente no ofrecen seguridad alguna en su implementación.

3.1.1 Filtrado de direcciones MAC

El principio de funcionamiento del filtrado de direcciones MAC, es el de permitir el ingreso de terminales a la red cuya dirección MAC es conocida, esta dirección se debe incluir en una lista de direcciones MAC en el AP que funciona como filtro de ingreso a la red. La dirección MAC es un número de 12 dígitos hexadecimales, que puede ser capturado por un sniffer, una vez que el intruso obtiene la dirección MAC de cualquier dispositivo autorizado modifica la dirección MAC de su adaptador inalámbrico, acabando por completo con la seguridad de la red.

3.1.2 Direccionamiento IP estático

Esta consiste en deshabilitar DHCP, el cual permite asignar direcciones IP automáticas aparte de otras opciones de configuración, para colocar manualmente las direcciones IP en los equipos autorizado en la red. Deshabilitar DHCP consiste en una pérdida de tiempo más que una medida de seguridad, un hacker puede encontrar el esquema de direcciones IP utilizado en la red en cuestión de segundos y asignar una dirección IP valida en la WLAN.

3.1.3 Ocultación del SSID

La ocultación del SSID consiste en dejar de transmitir las tramas *beacons* del AP, pero quienes emplean esta medida de seguridad, desconocen que existen otros cuatro mecanismos de gestión y mantenimiento de la comunicación en WiFi, que transmiten el SSID sobre el espectro, estos mecanismos son: *Probe Request*, *Probe Response, Asociation Request* y *Re-Association Request*. Ocultar el SSID

elimina uno de los 5 mecanismos de transmisión del SSID, hace más difícil el *roaming* entre AP a AP y hace a la red menos amigable al usuario.[31]

3.1.4 Disminución del nivel de señal

La disminución o supresión de la señal de la antena del AP como medida de seguridad para minimizar el área de cobertura de la red inalámbrica justo hasta donde se encuentra la terminal que utilizara la red, es inútil como una medida de seguridad en contra de ataques hackers, como se describió en los ataques de *warxing* los hackers pueden realizar modificaciones en las antenas de sus equipos para ampliar su rango de cobertura a cientos de metros de distancia.

3.1.5 Autenticación LEAP

La autenticación LEAP[32] creada por Cisco, es un mecanismo de autenticación empresarial para minimizar las falencias de WEP. LEAP esta basado en 802.1x, utiliza autenticación de direcciones MAC, compromete la seguridad (un hacker puede romper las contraseñas de la red en cuestión de horas sin importar la longitud de la clave empleada) siendo susceptible a recibir ataques de diccionario. Cisco decide actualizar LEAP a una nueva versión llamada EAP-FAST, levemente superior pero al igual a la primera versión del protocolo, ambos se basan en la complejidad de las contraseñas empleadas en vez de encriptación. Existen

[31]Para mayor información acerca de esta técnica de seguridad, visite el siguiente enlace: http://www.icsalabs.com/icsa/docs/html/communities/WLAN/wp_ssid_hiding.pdf

[32] LEAP significa Lightweight Extensible Authentication Protocol

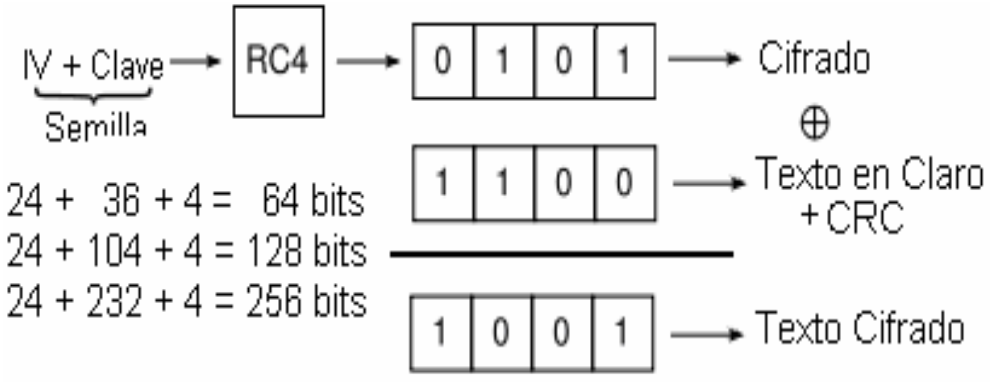
alternativas basadas en Protocolos de Autenticación Extensible (EAP) como EAP-TLS y PEAP lo cuales son mecanismos de seguridad superiores.

3.1.6 Encriptación WEP

WEP *Wired Equivalent Privacy* (Privacidad equivalente a un red cableada), es el mecanismo de seguridad implementado por el estándar 802.11 en septiembre de 1999. Utiliza un algoritmo de encriptación ***RC4*** para cifrar el tráfico de información entre AP y las terminales móviles, empleado una clave secreta que se combina con un Vector de Inicialización (IV) para encriptar el mensaje enviado y su ***checksum***[33] o ICV ***Integrity Check Value.***

La clave secreta puede variar de tamaño, para WEP 64 bits se utiliza una clave de 40-bits, WEP 128-bits utiliza una clave de 104-bits y WEP 256-bits utiliza una clave de 232-bits, los 24 bits restantes para cualquiera de los anteriores casos hace parte del IV, el IV es la clave para la seguridad de WEP, a continuación (figura 17) se muestra el funcionamiento de cifrado:

Figura 17. Proceso de Encriptación WEP[34]



[33] La *checksum* es una forma de control de redundancia para verificar la integridad de los datos y que estos no hayan sido corrompidos.
[34] Lehtinen Rick, Computer Security Basics, 2 edición. Sección 6.2

- El Vector de inicialización (IV) se concatena con la contraseña formando la semilla de entrada al algoritmo RC4 de cifrado de flujo.
- RC4 es un algoritmo de flujo este se encarga de expandir una semilla, para generar una secuencia de números pseudo-aleatorios.
- A la secuencia de salida de números se le aplica una operación XOR con en el texto en claro y su ICV generando el texto cifrado.

Dentro de las debilidades de WEP encontramos:

- El vector de inicialización utiliza 24 bits, el cual es muy pequeño y no tienen protección en contra de rehúso. Aumentar los bits de la clave de encriptación solo incrementa el tiempo para romper la clave WEP.
- La forma de construcción del IV lo hace susceptible a ataques contra de las claves, no tiene protección contra repetición de mensajes.
- Algunos dispositivos USB y tarjetas de red inalámbrica de primera generación WEP, generan el IV como un contador con incrementos de 1bit siendo esta secuencia fácil de descubrir para los hackers.
- No posee un sistema de control de secuencia de paquetes, estos pueden ser modificados o robados sin que el cliente sepa.
- El ICV, previene la corrupción de datos, este se combina con el texto en claro creando el CRC que es un valor de 4bytes al final de la trama enviada para la transmisión. Si un bit ha sido alterado, el CRC indicaría el error y el mensaje se rechaza, el problema con este esquema es que solo se puede

detectar errores accidentales, pero los errores intencionales como los creados por un hacker que ha enviado un mensaje alterado con un nuevo valor CRC, no pueden ser detectados.

Las primeras fallas fueron publicadas en 2001, en el artículo científico de FMS mostrando las vulnerabilidades de la no variación del IV. Luego de esta publicación, se inicio un lanzamiento de programas para romper claves WEP analizando una cantidad de tráfico suficiente, los ataques de inyección de tráfico disminuyen el tiempo para romper las claves.

Existen soluciones propietarias como *WEP2* que incrementa el valor del IV, *WEP+* de *Agere Systems* que evita el uso de IV débiles y *WEP Cloaking* de *Air Defense* que remueve las debilidades de WEP transmitiendo tráfico simulado, confundiendo programas de rompimiento de claves WEP empleados por hackers.

Un paper publicado por Eric Tews, Ralf Philipp Weinmann y Andrei Pyshkin demuestran como romper una clave WEP de 104 bits en 60 segundos[35], realizando ataques hacia las claves y mostrando como capturando 85000 paquetes la probabilidad de obtener la clave es del 95%, lo que se puede realizarse con un ataque de inyección en menos de un minuto.

Algunas de las debilidades conocidas de WEP como la reducción del tiempo o la necesidad de paquetes empleados para obtener la clave, crean la necesidad de emigrar a una nueva estrategia de protección como WPA o WPA2 si se desea administrar un red Wi-Fi segura.

[35] http://eprint.iacr.org/2007/120.pdf

3.1.7 Virtual Private Networks con IPSEC

El uso de VPN refuerza la seguridad de la red y funciona como una alternativa al uso de WEP. Las VPN forman un esquema de canales similares a túneles para proteger la conexión empleando con ***IPSEC***[36], el cual permite servicios de autenticación, este utiliza un conjunto de protocolos de cifrado para asegurar flujos de paquetes de datos e intercambiar claves de la siguiente forma:

- ESP: Encapsulating Security Payload, el cual provee autenticación, confidencialidad de datos e integridad del mensaje.
- AH: Authentication Header, este provee autenticación e integridad de datos, pero no de confidencialidad.

IPSEC tiene dos modos de empleo diferenciados por la unidad de información que protegen, el primer modo de transporte protege la carga útil del paquete IP y el segundo modo de túnel se protegen los paquetes IP completos, el modo de túnel es más utilizado en VPN aunque el modo de transporte sea más confiable que el de túnel.

El uso de VPN como mecanismo de seguridad, para WiFi no es fundamentalmente seguro porque desde sus orígenes estas fueron diseñadas para proteger cableadas punto a punto, protegiendo paquetes pero dejando la capa de enlace vulnerable a ataques hacia las tramas, siendo el menos complejo la búsqueda de puertos abiertos en el firewall y en el peor de los casos un ataque de Negación de Servicios. Adicionalmente VPN no tiene soporte con todos los dispositivos WiFi,

[36] IPSEC Internet Protocol Security

como impresoras WiFi o PDAs, entre otros esta es una medida alternativa pero no una solución definitiva de seguridad, por ello se debe utilizar WPA o WPA2.

3.2 Medidas de seguridad validas

Las siguientes medidas de seguridad son validas en la actualidad, para asegurar una red inalámbrica en el hogar, oficinas y empresas.

3.2.1 Encriptación WPA

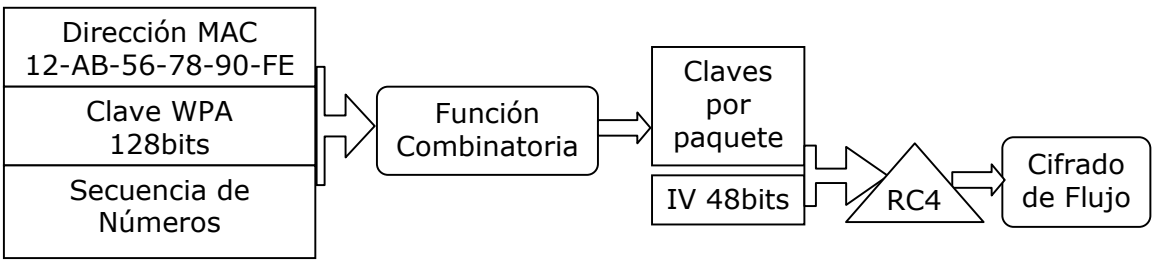
Wi-Fi Protected Access (Acceso Protegido de Wi-Fi), desarrollada por la *Wi-Fi Alliance* como una medida correctiva para reemplazar WEP y solución intermedia mientras se finalizaba el estándar de seguridad IEEE 802.11i. Fue lanzado en Abril de 2003 utilizando el borrador de la versión preliminar del estándar de seguridad 802.11i. WPA corrige deficiencias de WEP, utiliza una distribución de claves de manera dinámica e incrementa el tamaño del vector de inicialización IV, agrega técnicas y conceptos para la integridad y autenticación.

WPA utiliza el cifrado de flujo RC4 con claves de 128bits y un IV de 48bits para la encriptación, el uso de RC4 fue por motivos de compatibilidad con los equipos existentes de la época, los cuales con una actualización de firmware podrían implementar el uso de WPA.

También se introduce un nuevo protocolo de seguridad de claves llamado ***TKIP Temporal Key Integrity Protocol,*** el cual cambia las claves dinámicamente durante la sesión, esto previene la repetición de claves. TKIP utiliza una disciplina de secuencia de paquetes y una función de combinación de claves de dos fases

por paquete, esto significa que cada clave de encriptación esta asociada a una secuencia de números (previniendo *ataques de replay*), la función de combinación de paquetes toma la secuencia de número en conjunto con la clave WPA y la dirección MAC del emisor como entradas y por salida se obtienen nuevas claves WPA por cada paquete, esta nueva clave WPA es utilizada con el IV para generar la secuencia de cifrado. La figura 18 muestra el proceso de TKIP.

Figura 18. Proceso de TKIP para la creación del cifrado de flujo



WPA mejora la integridad de los paquetes utilizando el MIC (Message Integration Check), este campo se encarga de proteger a los paquetes y verificar que no han sido manipulados, el valor del MIC se computa con un algoritmo llamado Michael este utiliza una clave de 64bit y divide a los paquetes en bloques de 32bit, los paquetes pasan por procesos de registro, XOR y adiciones para agregar a cada bloque en dos registros, finalizando en una autenticación de 64bit. MIC fue el algoritmo más fuerte que se pudo crear con la premisa que debía funcionar en tarjetas inalámbricas más antiguas, sin embargo, este es susceptible a ataques. Como característica adicional posee un mecanismo de contraataque, si este detecta dos intentos de ataque durante un minuto, las comunicaciones se bloquearan por 60 segundos.

Existen varios cambios en la transición de WEP a WPA como son:

- El vector de inicialización se incrementa de 24bits a 48bits, las claves de seguridad de 40bits y 104bits se incrementan a 128bits.
- WEP no posee integridad de mensajes, MIC corrige esto previniendo la manipulación de mensajes.
- Anteriormente se utilizaba una única clave, en el nuevo esquema se utilizan nuevas claves de encriptación por cada trama en cada paquete transmitido, eliminando la susceptibilidad a los ataques de claves.
- Mecanismo para distribuir y cambiar las claves transmitidas.
- Protección contra ataques de repetición al incluir un contador de tramas.

WPA tiene dos modos de uso, el primer modo es utiliza una clave PSK Pre-Shared Key para usuarios en casa y redes de oficina, el segundo modo es utilizado con un servidor de autenticación RADIUS que distribuye claves diferentes a cada usuario, este método esta enfocado a brindar seguridad a nivel empresarial.

WPA-PSK o Modo Personal: Este modo es para usuarios en el hogar y pequeñas oficinas que no puedan costear un servidor de autenticación. En este modo la autenticación se realiza con el AP con una clave llamada ***passphrase*** o palabra clave, que puede ser de 8 a 63 caracteres ASCII o 64 dígitos hexadecimales, esta clave también debe ser introducida en cada terminal autorizada. La clave debe ser aleatoria (recomendable utilizar mínimo 10 caracteres), existe un estudio en donde

se estima que una clave con esta longitud y aleatoria, puede ser descubierta por 1000 terminales trabajando en paralelo en 500 años[37].

WPA-PSK utiliza una encriptación de claves modificadas automáticamente en un proceso llamado ***rekeying***[38], la autenticación entre dispositivos sucede luego de un periodo de tiempo específico o de un número de paquetes transmitidos. Este proceso se llama ***rekey interval***[39]. TKIP obtiene esta clave inicial de los dispositivos autorizados y se encarga de la encriptación y el ***rekeying*** automático.

WPA Empresarial: Este utiliza el protocolo EAP (Extensible Authentication Protocol) en conjunto con autenticación mutua con un servidor, para que el usuario no pueda conectarse de manera accidental a redes maliciosas.

EAP no es propiamente un mecanismo de autenticación sino más bien un mecanismo de autenticación de tramas, provee funciones comunes y negociación de un mecanismo deseado de autenticación, que en este caso se realiza con un Servidor de autenticación, este funciona siguiendo los siguientes principios.

- El servidor de autenticación debe aceptar las credenciales del usuario.
- El servidor de autenticación utiliza, tramas 802.1x y EAP para generar un clave maestra única.
- 802.1X distribuye la clave al AP y al cliente.

[37] http://blogs.zdnet.com/Ou/?p=127
[38] Re-claveado
[39] Intervalo de Re-Claveado

- TKIP establece una jerarquía de claves y un sistema de gestión, utilizando la clave maestra. En otras palabras, las claves de encriptación empleadas con cada paquete, son generadas a partir de la clave maestra.

El modo WPA-Empresarial requiere la existencia de un servidor de red, el AP emplea 802.1X y EAP para utilizar autenticación y el servidor suministra claves para el cifrado.

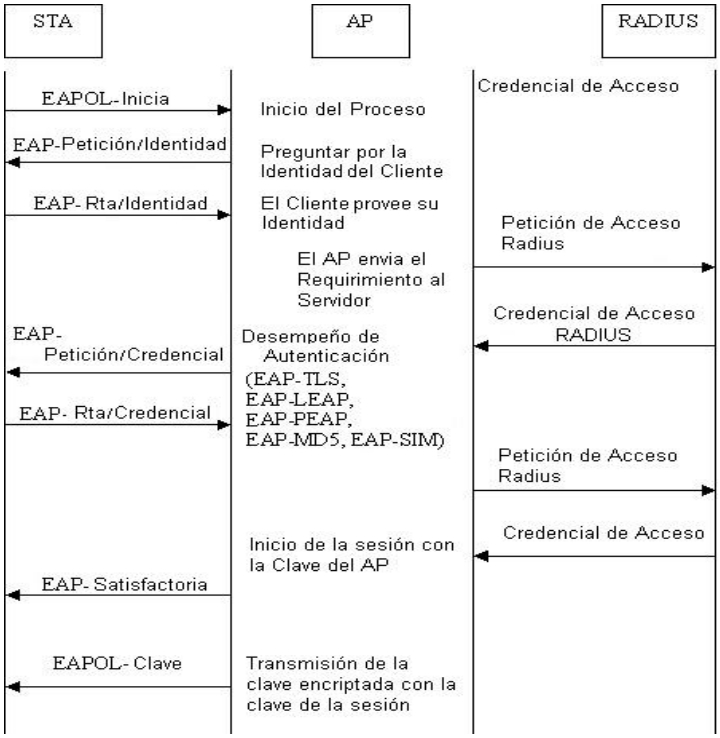
- 802.1X[40] es un estándar que proporciona control de acceso en redes basadas en puertos. Este permite autenticar a los dispositivos inalámbricos estableciendo conexiones o previniendo el acceso a la red si la autenticación falla, utilizando EAP con un servidor **RADIUS** para autenticación central, hasta que no se autentique el usuario, el AP mantendrá el acceso bloqueado a la red.
- **RADIUS**[41] es un protocolo de autenticación, autorización y conteo para aplicaciones de acceso a la red o movilidad IP, RADIUS corrobora la identidad del usuario con un nombre de usuario y contraseña usuario predeterminadas.
- EAP se utiliza para permitir el transporte de un protocolo de autenticación, autorización y contabilidad de clientes, este protocolo fue diseñado para protocolo punto a punto, que en Wi-Fi serán la conexión entre estación y servidor RADIUS. Si la autorización es positiva el servidor autoriza el acceso al sistema, otorgándole luz verde al AP para que el Terminal acceda a la red. La autenticación puede ser con el uso de EAP-TLS, EAP-TTLS, PEAP, Kerberos V5, EAP-SIM, etc. Cuando finaliza el proceso la Terminal suplicante y el

[40] Página oficial del 802.1X: http://www.ieee802.org/1/pages/802.1x.html
[41] Remote Authentication Dial In User Service

servidor de autenticación tendrán una clave maestra secreta. El protocolo para transportar EAP en redes inalámbricas se denomina EAPOL (EAP over LAN).

El proceso de autenticación utilizado con una Terminal suplicante (STA), un AP y el servidor RADIUS, se encuentra en la figura 19.

Figura 19. Autenticación con RADIUS[42]

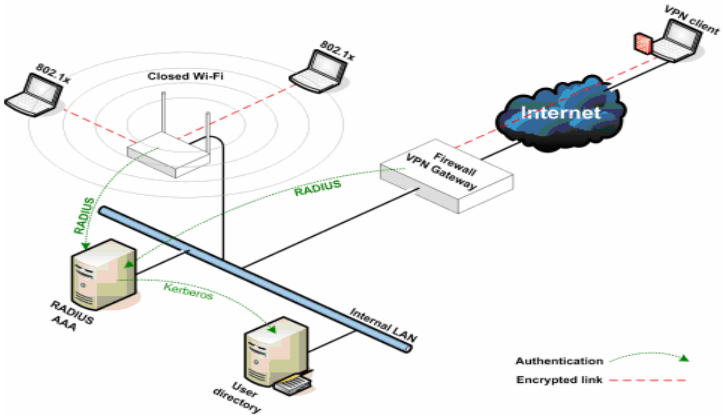


Existe una solución empleando WPA y VPN a nivel empresarial, el **gateway** VPN provee conexiones encriptadas para usuarios remotos desde Internet, mientras los AP proveen control de acceso y autenticación antes de realizar asociación con los dispositivos de la red local. La topología (Figura 20) emplea un modelo de

[42] Edney, Jon; Arbaugh, William A. Real 802.11 Security: Wi-Fi Protected Access and 802.11i, 2003

autenticación en donde cada AP y gateway VPN, se autentican con el servidor RADIUS para la verificación de usuarios. Esta es solución con el uso de VPN no tiene desperdicio de recursos en la red y es valida para implementar seguridad a la red.

Figura 20. WPA Empresarial y acceso remoto con VPN[43]



3.2.2 Encriptación WPA2

WPA2 es la versión final del estándar 802.11i fue publicada en Junio de 2004, los equipos creados a partir de Marzo de 2006, tiene soporte de fabrica de WPA2. Entre los cambios que se introducen se encuentran:

- Aparte de emplear TKIP, MIC y el algoritmo Michael, se presenta un nuevo algoritmo llamado **AES-CCMP**[44], el cual reemplaza el cifrado RC4, el CCMP utiliza el IV de 48bits para evitar ataques hacia las claves.
- La derivación de claves por paquetes utiliza una única clave AES, para proteger confidencialidad e integridad en los mensajes.

[43] Ou, George; Why Can't VPN replace WiFi Security http://blogs.zdnet.com/Ou/?p=489

[44] AES Advanced Encryption Standard y CCMP Counter Mode with Cipher Block Chaining Message Authentication Code Protocol.

- Separación del proceso de autenticación de usuario con el proceso de la integridad y privacidad de los mensajes. Esta nueva arquitectura se llama **RSN**[45] y se emplea para gestionar las asociaciones.
- Las RSN proporciona soluciones seguras y escalables con **TSN**[46], permitiendo interoperatibilidad con sistemas RSN y WEP en una red.
- Se reduce la cabecera en la derivación de las claves y la autenticación en roaming para evitar la captura de claves, por hackers oportunistas.
- Se implementa una autenticación llamada **4-Way Handshake**, la arquitectura de asociación de este proceso entre terminales, recibe el nombre de **RSNA**[47].

El establecimiento de un contexto seguro de comunicación con WPA2, consta de cuatro fases:

- Acuerdo de políticas de seguridad
- Autenticación 802.1X
- Derivación y distribución de claves
- Confidencialidad e integridad de datos RSNA.

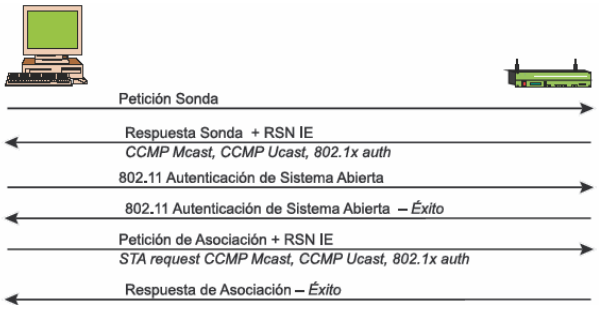
Fase1 Acuerdo de políticas de seguridad

La primera fase (Figura 21) requiere un acuerdo de políticas de seguridad a utilizar, esto se inicia con un *Probe Request* por parte del usuario, las posibles políticas se responde por el AP con un mensaje *Beacon o Probe Response*, luego

[45] Robust Security Network.
[46] Transitional Security Network.
[47] Robust Security Network Association

se realiza una autenticación abierta, la respuesta del cliente incluye una petición y finalmente el proceso finaliza con una Respuesta de Asociación por el AP. La respuesta de políticas de seguridad, que se envía en el campo RSN IE (*Information Element*) muestra información como el método de autenticación soportado (802.1X o PSK), el protocolo de seguridad (CCMP, TKIP) y soporte para pre-autenticación antes de realizar de AP en roaming.

Figura 21. Fase 1: Acuerdo de Políticas de seguridad[48]



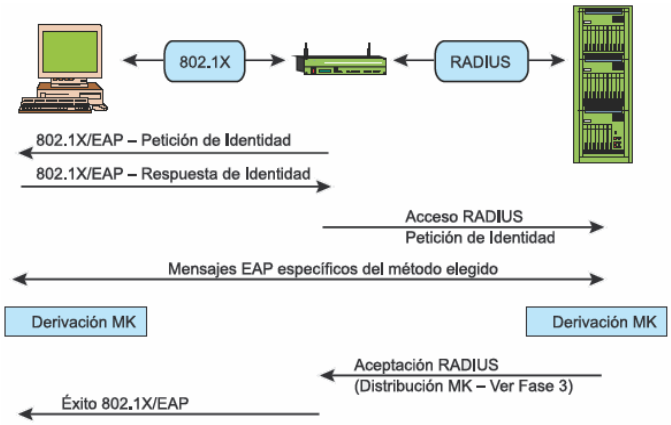
Fase 2 Autenticación 802.1X:

Esta segunda fase (Figura 22) es la autenticación 802.1X basada en EAP y el método especifico de autenticación decidido: EAP/TLS con certificados de cliente y servidor utilizando una infraestructura de claves públicas o PEAP con autenticación hibrida, etc. La autenticación 802.1X inicia con una petición de identidad del AP hacia el cliente, este último responde el método de autenticación a utilizar, luego se intercambian mensajes entre cliente y servidor para generar la MK o Master Key común, al final de este proceso, se envía desde el servidor de

[48] Lehembre, Guillaume; WiFi Security, WEP, WPA, WPA2; www.hakin9.org

autenticación al AP un mensaje de aceptación con la MK y un mensaje final de conexión exitosa para el cliente.

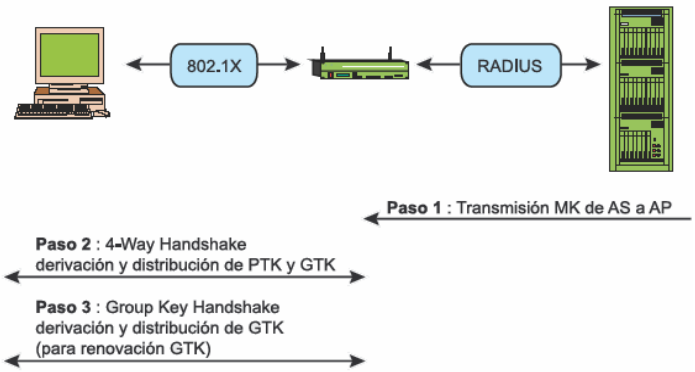
Figura 22. Fase 2: Autenticación 802.1X[48]



Fase 3 Jerarquía y distribución de claves

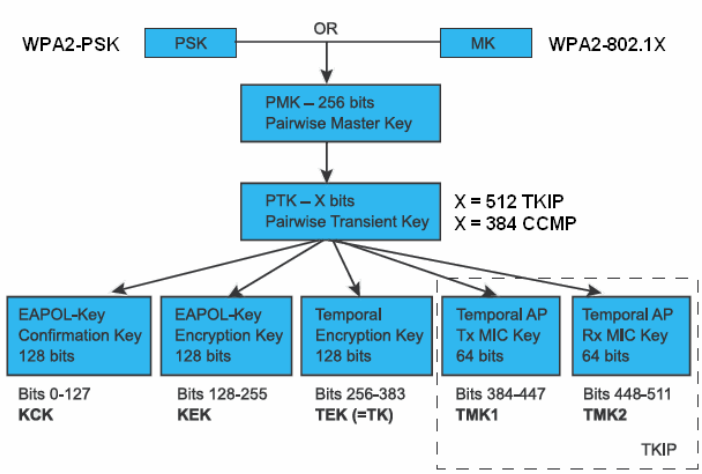
La seguridad de la conexión se basa en las claves secretas. En RSN cada existen diversas claves organizadas por jerarquía, se crean claves temporales de sesión y se actualizan regularmente hasta que se cierra el contexto de seguridad. Durante la derivación de claves (Figura 23), se producen dos handshakes: el primero es el 4-Way Handshake para derivar la **PTK** Pairwise Transient Key y la **GTK** Group Transient Key, el segundo Handshake es para renovar la GTK.

Figura 23. Fase 3: Derivación y distribución de claves[48]



La derivación de la clave **PMK** Pairwise Master Key depende del modo de autenticación, para redes en el hogar y oficinas se utiliza una PSK utilizada como PMK y para redes empresariales con servidores de autenticación, la PMK se deriva de la MK en la autenticación 802.1X. La PMK no se utiliza para la encriptación o comprobación de integridad, sino para la generación de un clave de encriptación temporal que puede ser de 512 bits con TKIP y 384bits con CCMP. La jerarquía de claves temporales de PTK, se muestra en la figura 24.

Figura 24. Jerarquía y Formación de la PTK[48]



KCK Key Confirmation Key – 128bits: Esta autentica mensajes MIC durante el 4-Way Handshake y el Group Key Handshake.

KEK Key Encryption Key – 128bits: Esta asegura la confidencialidad de datos como RSN IE, durante el *4-Way Handshake* y el *Group Key Handshake*.

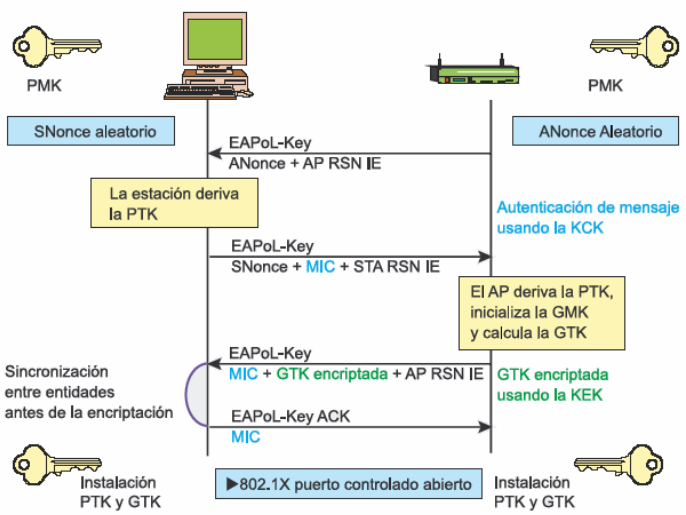
TEK Temporary Key – 128bits: Esta encripta y desencripta paquetes de transmisión única con TKIP o CCMP.

TMK Temporary MIC Key –2x64bits: Esta es utilizada solo por Michael con TKIP, utiliza una clave dedicada en cada extremo de la comunicación.

El 4-Way Handshake iniciado por el AP permite, confirmar el conocimiento del cliente de la PMK, derivar una nueva PTK, instalar claves de encriptación e integridad, encriptar el transporte de la GTK y confirmar la selección de cifrado.

En este procedimiento se intercambian cuatro mensajes EAPOL-Key entre el cliente y el AP, se muestra en la figura 25.

Figura 25. Procedimiento de 4-Way Handshake[48]



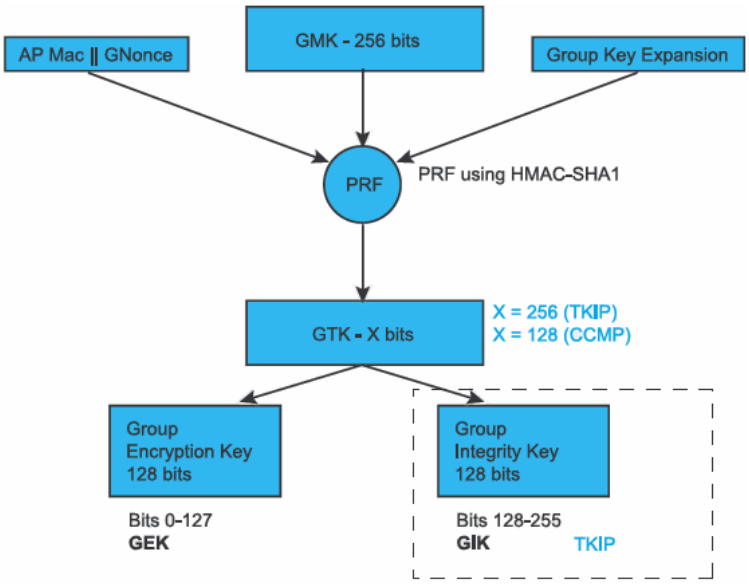
- En el 4-Way Handshake, la PTK se deriva de la PMK, una cadena fija, la dirección MAC del AP y dos números aleatorios llamados ANonce[49] por parte del autenticador y el SNonce por parte del suplicante.
- El AP inicia el primer mensaje seleccionando el ANonce y lo envía al suplicante sin encriptarlo.

[49] Un nonce es un número o cadena de bits utilizada una sola vez en procesos de autenticación para evitar su reutilización en ataques de retransmisión de mensajes

- El suplicante genera SNonce, calcula la PTK y las claves derivadas, envía el SNonce y la clave MIC calculada utilizando la clave KCK.
- El autenticador extrae el SNonce que no se encuentra encriptado, calcula la PTK y las claves temporales derivadas. Luego verifica el MIC y se asegura que el suplicante conoce la PMK, ha calculado correctamente la PTK y las claves temporales derivadas por último envía la GTK encriptada con KEK, derivada de un GMK aleatorio y GNonce (Ver Figura 26) junto con MIC utilizando KCK.
- El suplicante recibe el mensaje comprueba que el autenticador conoce el PMK y ha calculado correctamente la PTK y derivado las claves temporales. Este último mensaje certifica la finalización del handshake y el suplicante instalará la clave y empezará la encriptación.
- El autenticador instala sus claves tras verificar el valor MIC, en este momento los dos sistemas han calculado e instalado claves de integridad y encriptación para comunicarse a través de un canal seguro para tráfico **unicast**.

El tráfico **multicast** se protege con otra clave la **GTK** Group Transient Key, generada de una clave maestra llamada **GMK** Group Master Key, una cadena fija, la dirección MAC del AP y un número aleatorio GNonce. La longitud de GTK depende del protocolo de encriptación 256bits para TKIP y 128bits para CCMP. La jerarquía de claves temporales de GTK, se muestra en la figura 26.

Figura 26. Jerarquía y formación de la GTK[48]



GEK Group Encryption Key: Esta encripta datos utilizados en CCMP para la autenticación y por TKIP en la encriptación.

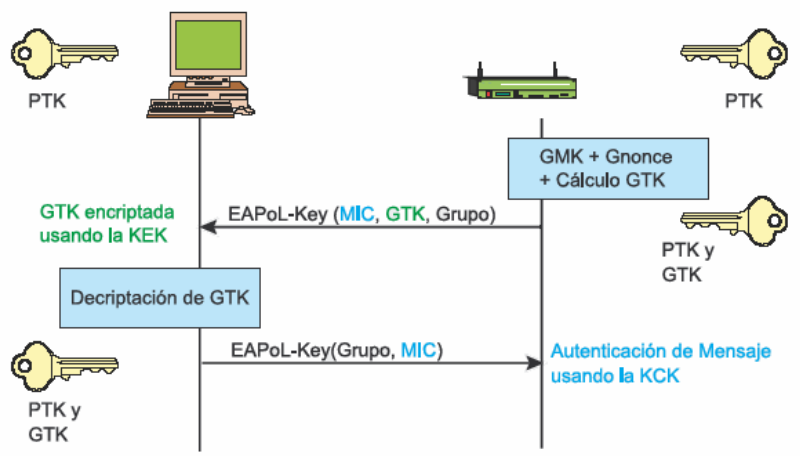
GIK Group Integrity Key: Esta autentica datos, es utilizada por el algoritmo Michael con TKIP.

En el proceso de Group Key Handshake (Figura 27), se intercambian dos mensajes EAPOL-Key entre el cliente y el AP. Este handshake hace uso de claves temporales generadas durante el 4-Way Handshake KCK y KEK. En el procedimiento se requiere desasociar una estación para renovar la GTK, a petición del cliente.

- El AP escoge un número aleatorio GNonce y calcula una nueva GTK, envía la GTK encriptada usando KEK, el número de secuencia de la GTK y el MIC calculado de este mensaje usando KCK hacia el suplicante.

- El suplicante certifica la finalización del Group Key Handshake, enviando el número de secuencia de GTK y el MIC calculado del mensaje del suplicante

Figura 27. Procedimiento Group Key Handshake[48]



Fase 4 Confidencialidad e integridad de datos RSNA

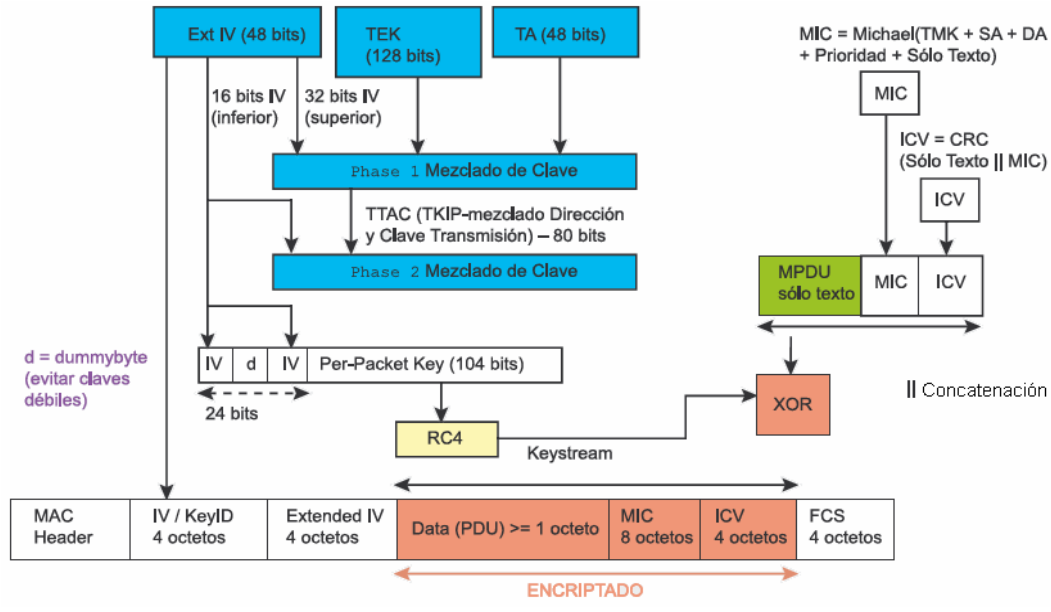
Las claves generadas anteriormente son utilizadas en protocolos que soportan confidencialidad e integridad de datos RSNA:

- **TKIP** Key Mixing
- **CCMP** Counter-Mode / Cipher Block Chaining Message Authentication Code Protocol

Existen dos términos **MSDU** MAC Service Data Unit y **MPDU** MAC Protocol Data Unit. Estos se refieren a único paquete de datos, pero MSDU representa a los datos antes de la fragmentación donde TKIP calcula el MIC, mientras las MPDUs son múltiples unidades de datos tras la fragmentación y es aquí donde CCMP calcula el MPDU.

TKIP: El esquema de combinación de claves se divide en dos fases: La primera fase se ocupa de datos estáticos, la clave TEK de sesión secreta, **TA** de la dirección MAC del transmisor para prevenir colisiones IV y los primeros 32bits del IV (Ver figura 28). La segunda fase incluye el resultado de la primera fase y los bits restantes del IV, se cambian los bits del campo *Per Packet Key* por cada nuevo IV. El IV empieza en 0 y es incrementado como contador por cada paquete, los mensajes cuyo **TSC** o TKIP *Sequence Counter* (Es un contador de tramas para evitar la reutilización de IVs) no es mayor que al último mensaje son rechazados. El resultado de la segunda fase y el IV sirven de entrada para RC4, generando un flujo de claves que se combina con un XOR con el MPDU y el ICV de WEP.

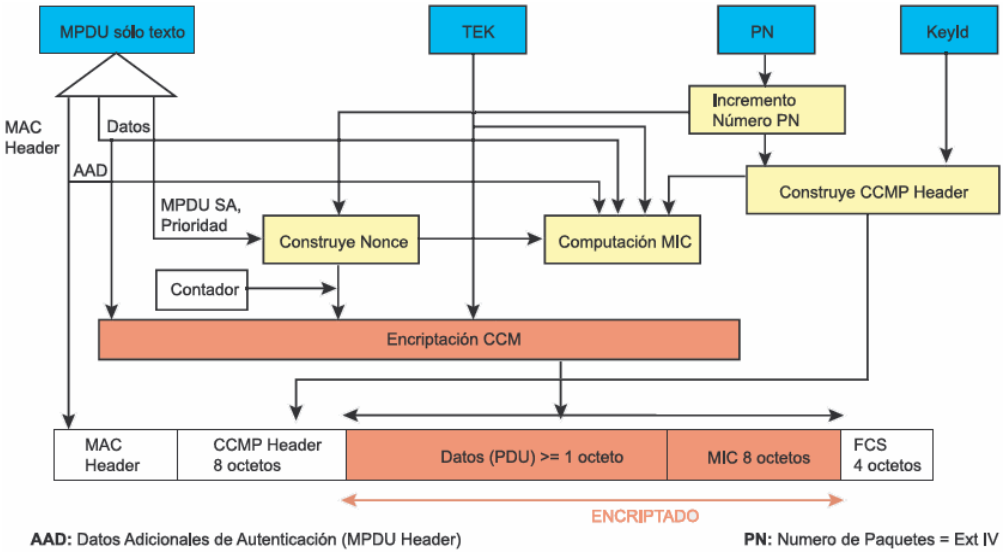
Figura 28. Esquema de encriptación TKIP Key Mixing[48]



CCMP utiliza el cifrado de bloques **AES** Advanced Encryption Standard (Figura 29), existe un modo de conteo en conjunto a un método de autenticación de mensajes llamado *Cipher Block Chaining* **CBC-MAC** para producir un MIC.

MIC utiliza el algoritmo **CBC-MAC** que encripta un nonce de inicio, la dirección fuente de MPDU y el PN, operaciones XOR sobre los bloques subsiguientes para obtener un MIC de 64bits, el MIC final es un bloque de 128bits, donde se descartan los últimos 64bits, se añaden datos de texto para encriptación AES en modo contador de un nonce similar al de un MIC, pero con un campo de contador extra. Se utiliza una clave única para la encriptación y autenticación con diferentes IVs y por último se añaden 16bytes al MPDU: 8 para el encabezamiento CCMP y 8 para el MIC. El encabezamiento CCMP es un campo no encriptado incluido entre el encabezamiento MAC y los datos encriptados, incluye el **PN** *Packet Number* (IV extendido) y la *Group Key Key ID*. El PN funciona como contador con incrementos de uno, para cada MPDU subsiguiente.

Figura 29. Esquema de encriptación CCMP[48]



3.3 Medidas de Seguridad Complementarias

Las siguientes medidas complementan la seguridad de las redes inalámbricas a parte del empleo de WPA o WPA2.

3.3.1 Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS[50]) es una certificación opcional de la Wi-Fi Alliance (Figura 30) desde Enero de 2007, para facilitar la configuración de los parámetros seguridad en la red. WPS aplica para redes que emplean comunicación con un AP o router inalámbrico, no tiene soporte para redes Ad Hoc, configura el nombre de la red SSID y la clave de seguridad WPA2 para el AP y los clientes WPS de la red.

Figura 30: Logotipo de Wi-Fi Protected Setup[50]

WPS introduce el concepto de **Registrar**, el cual es una entidad lógica con la autoridad para otorgar y revocar credenciales necesarias para incluir nuevos clientes en la red, Registrar puede estar integrado al AP o ejecutarse en un dispositivo separado del AP, en una WLAN pueden existir múltiples Registrars.

La configuración de WPS actuales son **PIN** *Personal Information Number* y **PBC** *Push Button Configuration*, se pretende extender la configuración con dos nuevos métodos en el transcurso del presente año llamados **NFC** *Near Field*

[50] http://www.wi-fi.org/files/uploaded_files/wp_18_20070108_Wi-Fi_Protected_Setup_WP_Final.pdf

Communications y **USB** *Universal Serial Bus*. La especificación obliga que los dispositivos incluyan PIN y PBC en el AP y al menos PIN en el dispositivo cliente.

- PIN viene incluido desde una calcomanía o se genera un PIN dinámico desde el dispositivo, este se introduce en el AP en una interfaz gráfica llamada Registrar. El PIN asegura que el dispositivo agregado a la red es el correcto y evitar asociaciones accidentales o intentos maliciosos de agregar otros dispositivos no autorizados en la red.
- PBC habilita el cifrado oprimiendo botones (físicos o virtuales) en el AP y el dispositivo cliente para dar acceso a la red. El usuario debe saber que utilizando este método, existe un periodo de tiempo en el que otros equipos no autorizados podrían unirse a la red.
- NFC utiliza interacciones para intercambiar las credenciales de la red entre el AP y el cliente. Las credenciales se intercambian cuando el usuario acerca el cliente basado en NFC y lo aproxima AP o trae al dispositivo cliente a una proximidad de 10Cm. El dispositivo Registrar lee la credencial de identificación del cliente incluida en el dispositivo y envía el SSID de la red y el código PSK al cliente, autorizándole la entrada a la red.
- USB intercambia credenciales, se conecta una unidad USB para transferir los datos al dispositivo Registrar en este caso el AP. Las credenciales se copian al disco, el cual es insertado en el nuevo dispositivo para completar la transferencia de credenciales.

El soporte a estos últimos modelos de configuración es opcional, también son conocidos como métodos fuera de banda, porque la transferencia de credenciales emplea un canal de autenticación distinto al de WiFi.

El procedimiento se inicia con ejecutar el menú de configuración e introduciendo el PIN o presionando el PBC para solicitar acceso. Se inicia un intercambio de información entre el dispositivo y el Registrar, este último otorga credenciales con el SSID y la clave de acceso a la red utilizando EAP y un handshake para autenticar el cliente a la red.

3.3.2 WAPI

WAPI *WLAN Authentication and Privacy Infrastructure)*, es un estándar de seguridad nacional del gobierno chino para WLAN, esta diseñado para operar sobre Wi-Fi la compatibilidad con el protocolo de seguridad utilizado por IEEE 802.11 esta en debate. WAPI utiliza un servicio de autenticación **ASU** Authentication Service Unit, conocida por el dispositivo Terminal y el AP, este actúa como unidad central de verificación autorizada. El estándar requiere del uso de un algoritmo de encriptación simétrico *SMS4*, el cual fue eventualmente descalificado en enero de 2006, de cualquier forma el estándar y su implementación criptográfica no ha sido publicada.

La Asociación de Estándares Chinos (SAC) presento WAPI a la Organización de Estándares Internacionales ISO para su reconocimiento como un estándar internacional, casi al mismo tiempo que el estándar IEEE 802.11i. Luego de debatir ambos procesos y problemas técnicos, la secretaria genera IEC/ISO

decidió enviar las propuestas a votación, en marzo de 2006 la propuesta IEEE 802.11i fue aprobada y la propuesta WAPI fue rechazada. En julio de 2006 se publico el estándar 802.11i y WAPI dejo de ser considerado por la ISO.

A principios de 2007 el gobierno chino reporto que utilizara WAPI en sistemas de seguridad para el gobierno, aunque el mercado no gubernamental sigue utilizando equipos certificados con WPA2.

La **WAPIIU**[51], fue establecida para promover el uso y certificación WAPI, con el apoyo de 22 miembros incluyendo empresas como Lenovo, Huawei y Beijing Founder Electronics, así como también los 4 mayores operadores de telecomunicaciones en China. Este grupo ha promovido el uso de WAPI en china durante 2006 y 2007.

3.3.3 Firewalls

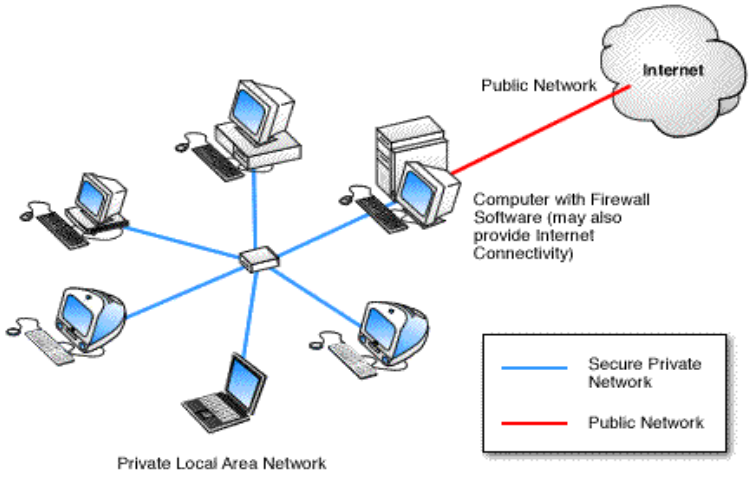
Los Firewalls son elementos de hardware o software que restringen la entrada y salida de la información o fijan limites para limitar distintas redes. Estos proporcionan protección contra ataques, complementando las medidas de seguridad en garantías a la protección de la información, no solamente por ataques externos sino también internos y el bloqueo de aplicaciones que puedan generar agujeros significativos en los puertos de acceso a la red.

Los Firewalls pueden funcionar a nivel de enlace de datos capa 2 filtrando direcciones MAC; a nivel de red capa 3 filtrando paquetes IP por dirección de origen y dirección IP de destino; a nivel de transporte capa 4 con el puerto de

[51] Unión Industrial de Autenticación Cableada y Privacidad de Infraestructura

origen y destino; y por último también a nivel de aplicación capa 7 filtrando el tráfico http, a diferentes direcciones URL a las que se pretende acceder, estos firewalls llevan el nombre de Proxy. El firewall puede permitir el paso de tráfico a menos que este cumpla cierto criterio o negar el acceso a tráfico que no cumpla ciertos criterios, estos criterios pueden ser la dirección IP de destino, el tipo de paquete o el puerto empleado. En la figura 17 se observa un firewall protegiendo el acceso a Internet.

Figura 31. Firewall en una red privada[52].



3.3.4 Tarjetas Inteligentes y USB Tokens

Los Tokens de seguridad electrónicos son dispositivos de hardware o software que posee un usuario autorizado para autenticar su identidad personal y obtener acceso a la red. Estos son una forma de autenticación de seguridad de alto nivel, pueden poseer claves criptográficas como firmas digitales o datos biométricos, con pruebas de alteraciones e incluir teclados para la digitación de un PIN.

[52] Barnes, Christian; Hack Proofing Your Wireless Network; Capitulo 6.

Las tarjetas inteligentes basadas en USB tokens contienen un chip con que posee un código único de identidad para cada usuario y es chequeado por un software en el servidor interno en conjunto con un PIN de ingreso del usuario esto verifica la autenticidad de un usuario y que la tarjeta no ha sido robada, creando un nuevo código de cifrado en la transmisión de la red inalámbrica. Estas medidas son altamente costosas y su empleo es limitado a nivel empresarial para la protección de espionaje industrial, generando redes con un nivel de seguridad y vulnerabilidad prácticamente nula, por sus niveles de autenticación para confirmar la identidad del usuario.

Figura 32. USB Tokens y Tarjetas Inteligentes[53]

3.3.5 Redes tipo Honeypot

Las redes Honeypot son trampas colocadas para detectar o atraer el interés de los hackers, simulando ser vulnerables o débiles para ataques. Esta herramienta distrae a los atacantes de la verdadera red inalámbrica y advierten al administrador de la red la ejecución de un ataque, este tipo de redes recopilan información útil de los hackers y sus técnicas de empleo antes, durante y después

[53] http://en.wikipedia.org/wiki/Wireless_security

del ataque dependiendo de la complejidad del honeypot. Existen varios tipos de redes Honeypot según su nivel de interacción e intervención:

Honeypot de baja interacción: Estos se limitan a simular grandes redes en una simple Terminal, emulando otras terminales ejecutando distintos procesos[1] como sucedería en una red real y con direcciones IP no utilizadas en la red verdadera. Este tipo de Honeypot es empleado para alertar la presencia de un ataque. Honeyid[54] es software de simulación de este tipo de redes.

Honeypot de alta interacción: Estos operan sobre sistemas de redes reales, estos se ocultan en la red real monitoreando y controlando el flujo de datos de la red. Esta red puede capturar una mayor cantidad de datos que las redes de baja interacción, como el tráfico de la red, registros de eventos e información capturada por **keyloggers** ocultos. Estas redes se utilizan para investigar el comportamiento de hackers.

Con el análisis de estas redes se puede encontrar fallas en los sistemas de seguridad, encontradas por hackers y crear herramientas para contraatacar esas fallas. Las redes Honeypot no son una solución concreta para el problema de seguridad, exceptuando el la alerta de un ataque en ejecución al administrador y este pueda ser detenido a tiempo, por el personal de seguridad de la empresa, la red honeypot muestra posibles vulnerabilidades y riesgos a los que se pueden estar expuestos en la red[55].

---

[54] http://en.wikipedia.org/wiki/Honeyd

[55] http://project.honeynet.org es un proyecto de investigación de tácticas de herramientas y tácticas de hackers

3.3.6 Wireless Intrusion Detection Systems

Wireless Intrusion Detection Systems (**WIDS**) son dispositivos de red que monitorean el espectro de radio para la búsqueda de Access Points Maliciosos.

Estos sistemas pueden emplear una Terminal conectada a dispositivo de procesamiento de señal inalámbrica y una antena ubicada alrededor de las instalaciones donde se localiza la red. El sistema monitorea el espectro de radio utilizado por las redes inalámbricas e inmediatamente alerta al administrador de la red, cuando un AP inalámbrico es detectado, esto se logra por la comparación de la dirección MAC de los dispositivos inalámbricos que participan. Como las direcciones MAC pueden ser suplantadas desde el dispositivo malicioso, donde se ejecuta el ataque, existen nuevas investigaciones[56] en donde se emplean huellas digitales para descartar dispositivos con direcciones MAC alteradas, comparando las firmas exhibidas por las señales emitidas por cada dispositivo inalámbrico, en contra de las firmas utilizadas por el dispositivo no autorizado.

El monitoreo del espectro de radio con WIDS, previene la instalación de AP Maliciosos en áreas cercanas a la red.

3.3.7 Wireless Intrusion Prevention Systems

Wireless Intrusion Prevention Systems o **WIPS** previenen el acceso de dispositivos inalámbricos no autorizados a la red, estos sistemas fortalecen las políticas de seguridad inalámbrica de una organización y constan de tres componentes:

[56] http://www.eetimes.com/news/latest/showArticle.jhtml;jsessionid=GPLEDVT0ZRBKUQSNDLPSKH0CJUNN2JVN?articleID=192501255

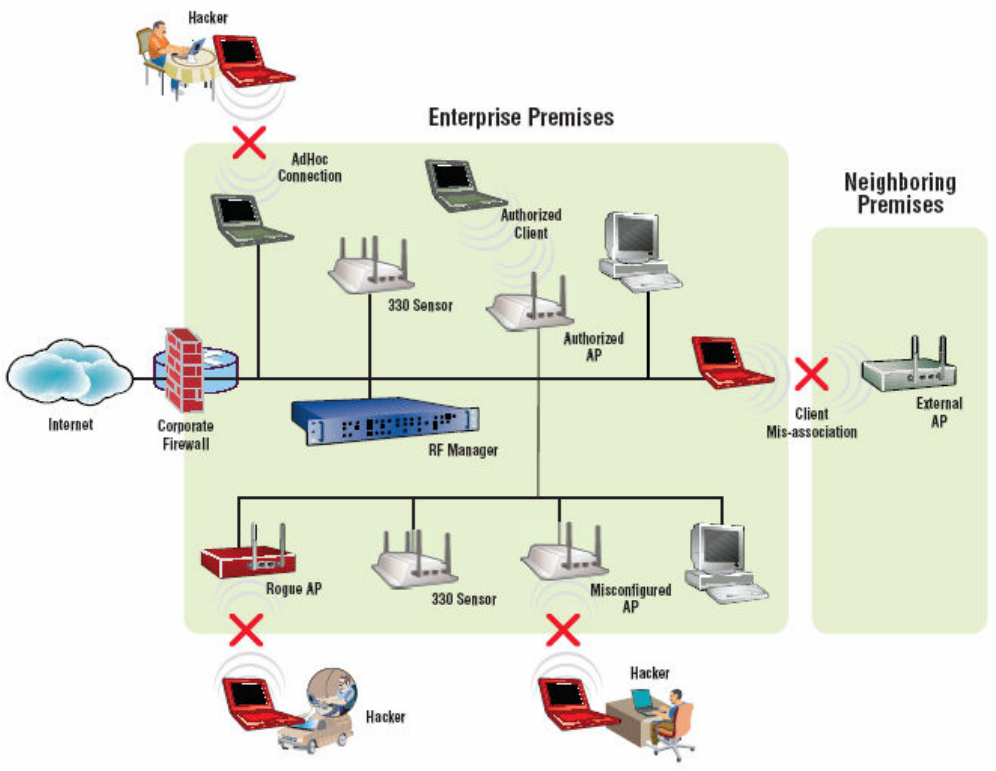
1. Sensores: Escanean el espectro en búsqueda de paquetes, son instalados en toda el área que va a ser protegida.
2. Servidor: Analiza los paquetes capturados por los sensores.
3. Consola: Provee al usuario una interfaz para reportes y administración deñ sistema.

A diferencia de WIDS, WIPS no solo detecta la amenaza también las previene de manera automática, cuando se identifica correctamente el ataque y sea clasificado como una amenaza para el sistema. El funcionamiento de WIPS consiste en:

- Definición de políticas de operación por parte del usuario, en el WIPS.
- Los sensores observan el tráfico y envían la información al servidor WIPS.
- El servidor correlaciona la información, con las políticas definidas y clasifican la amenaza de ataque.
- La amenaza se notifica al administrador de la red.
- Si la política es prevenir esa amenaza, WIPS envía una protección automática, entre las posibles amenazas se encuentran los AP maliciosos, AP configurados incorrectamente, redes Ad Hoc, asociación incorrecta de clientes, asociaciones no autorizadas, MAC spoofing y ataques Man in The Middle, Evil Twin y Negación de Servicios.

La figura 33 muestra el uso de sensores WIPS que monitorean ataques por parte de los hackers y evitan la asociación de clientes a AP externos.

Figura 33. Uso de WIPS en una red empresarial[57]



3.3.8 Pasos para asegurar una red WLAN

Los siguientes son algunos pasos básicos recomendados para tener en cuenta en el momento de asegurar una red inalámbrica, en orden de importancia:

1. Activar un método de encriptación WPA2 o WPA con contraseñas fuertes de gran longitud y caracteres aleatorias.
2. Cambiar la contraseña de fábrica para acceder al dispositivo inalámbrico, estas son conocidas por la comunidad hacker, al cambiarla se previene que estos accedan y cambien las opciones de la red del dispositivo.

[57] Aruba White Paper RF Security, Securing the Enterprise; http://manageengine.adventnet.com/products/wifi-manager/wifi-manager-software.html

3. Dividir las redes cableadas e inalámbricas en segmentos distintos, con firewall de por medio. Esto puede prevenir al cracker acceder a una red cableada mediante, luego de ganar acceso a la red inalámbrica.
4. Implementar un WIPS para monitorear el espectro inalámbrico las 24 horas del día, en contra de ataques activos por parte de dispositivos inalámbricos. Estos sistemas pueden detectar y detener el ataque más sutil con métodos de fuerza bruta, brindando un gran desempeño a la red WLAN.

4. Software utilizado en Wireless

En este capitulo se encuentra una recopilación de programas y herramientas que utilizan los hackers o intrusos en el momento de realizar los ataques, así como también algunos programas para crear redes tipo honeypot para proteger redes inalámbricas. El estudio de estos programas sirve para comprender los riesgos a los que se puede estar expuesto, estando la mayoría de estos dirigidos a realizar ataques contra WEP.

4.1 Ataques de Fuerza bruta y de Diccionario

Como se menciono en el capitulo 2, este tipo de ataques están dirigidos a aquellas palabras o frases (fácilmente recordables), que emplean los usuarios como claves para su red WiFi, facilitando los ataques.

Airsnort es un conjunto de programas con diversas herramientas que intentan desencriptar los paquetes de WEP. Una de ellas llamada *Decrypt,* esta tiene un listado de palabras (Diccionario) que utiliza en contra de los paquetes guardados que ha logrado capturar. Con cada posible clave, desencripta un paquete y computa una suma de verificación o *checksum* en los nuevos datos descifrados sumando los bytes de cada dato enviado, teniendo en cuenta su posición en el mensaje y guardando el valor. Si la suma de verificación coincide con la nueva suma de verificación transmitida en el paquete, se ha encontrado una clave

secreta potencialmente valida, si esa clave funciona con otro paquete entonces se ha encontrado la clave secreta.

Existen ataques de fuerza bruta que pueden descifrar la clave secreta de 40bits en menos de un minuto con una falla en la generación de claves WEP, descubierta por Tim Newsham[58], las claves utilizadas por WEP estan limitadas para producir claves de semillas, desde 00:00:00:00 hasta 00:7F:7F:7F. Esto reduce la cantidad de esfuerzo requerido por este tipo de ataque, **Wep_tools** utiliza este concepto. Existe un programa llamado **WEPAttack** que utiliza la eficiencia de los ataques de fuerza bruta y los de diccionario en contra de las claves. La idea es obtener un único paquete de WEP para iniciar el ataque.

4.2 Ataque de FMS

Es el ataque más conocido de WEP, se deriva de la investigación realizada por Scout Fluhrer, Itsik Mantin y Adi Shamir[59] en 2001, el trabajo describe las debilidades de RC4:

- El Vector de Inicialización IV se transmite en el texto en claro.
- El IV es relativamente pequeño (3-Bytes) lo que da como resultado un número de repetición también pequeño (16.78 Millones) de IV que son utilizados y reutilizados para encriptar los paquetes.
- Algunos de los IV son débiles en el sentido que puede ser engañados para obtener información acerca de la clave.

[58] Newsham, Tim. "Cracking WEP Keys". Presentation: Black Hat, 2001.
[59] Fluhrer, Scout, Itsik Mantin y Adi Shamir "Weakness in the Key Scheduling Algorithm of RC4". 2001 http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps

Estas debilidades han hecho posible, bajo ciertas condiciones recuperar la clave de entrada del RC4, conociendo el primer byte de salida. En los inicios del estándar el procedimiento de creación de los IV era secuencial empezando desde 00:00:00 hasta FF:FF:FF. No solo generando IV débiles sino también predecibles. **WEPCrack** fue la primera herramienta pública que utilizo un ataque FMS. **Airsnort** es más conocida y fácil de utilizar, ya que las tarjetas WiFi modernas reducen el porcentaje de IV débiles generados (bajo los contraataques de WEP+ o Advanced WEP Encryption), **Airsnort** esta declinando en importancia porque requiere una mayor cantidad de paquetes para obtener la suficiente cantidad de paquetes para romper las claves.

Utilizando este algoritmo, la búsqueda de IV débiles ha reducido el tiempo en una relación de 1/20 del tiempo que requeriría utilizar el algoritmo FMS. Estos algoritmos de estudio ayudan a reducir el tiempo de ataque en una red que utiliza WEP, no han sido ampliamente implementados, debido al bajo porcentaje de los dispositivos que utilizan WEP o a la popularidad de las herramientas WEP existentes. Estos métodos se convierten en mas populares a medida que los dispositivos evitan el uso de IV más débiles. Luego de la investigación original FMS, un número de investigadores ha descubierto otras maneras de romper los IV para agilizar el proceso de rompimiento de claves WEP, (los estudios de David Hulton[60] describen un número de aproximaciones alternativas para expandir el

[60] Hulton, David. "Practical Exploitation of RC4 Weaknesses in WEP Environments". 22 Feb 2002. http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt

concepto de FMS incluyendo métodos adicionales para encontrar IV débiles. Su algoritmo esta implementado en una utilidad llamada **dwepcrack**).

En agosto de 2004, un hacker llamado KoreK publico un código que expande los ataques FMS, este ha sido implementado en **Aircrack** afirmando romper claves WEP en tiempo record. KoreK ha lanzado otro programa llamado **chopchop**, este programa explota WEP en diferentes formas para desencriptar paquetes individuales. Cuando el paquete es capturado, puede ser descifrado byte a byte realizando ligeras modificaciones y retransmitiéndolo. El atacante remueve el último byte del paquete encriptado y lo reemplaza por otro, si el bit utilizado es correcto el paquete se envía al AP y este lo retransmite. El atacante puede utilizar este byte y el respectivo byte de cifrado para encontrar el byte del texto en claro, como solamente existen 256 alternativas para cada byte, el paquete puede ser descifrado en un periodo de tiempo relativamente corto.

En la tabla 9, se pueden observar las diferentes herramientas de ataque para encontrar las claves WEP, la dirección de la página y el sistema operativo donde se ejecutan.

Tabla 9. Búsqueda de Claves WEP

Nombre	Dirección	OS
Aircrack	http://www.cr0.net:8040/code/network/	Linux
Aisnort	http://airsnort.shmoo.com/	Linux Win
Chochop**	http://www.netstumbler.org/showthread.php?t=12489&page=1&pp=15	Linux
Dwepcrack	http://www.wi-foo.com/soft/attack/bsd-airtools-v0.2.tgz	BSD
WepAttack	http://wepattack.sourceforge.net/	Linux
WEPCrack*	http://wepcrack.sourceforge.net/	Múltiple*
Wep Tools	http://www.lava.net/%7Enewsham/wlan/	Linux

*(Si posee Perl) Cualquier Plataforma.
** Desencriptado paquete a paquete.

4.3 Inyección de Paquetes en WEP

Para romper WEP es necesario capturar cierta cantidad de paquetes, una red con gran cantidad de usuarios puede representar un gran volumen de tráfico pero en aquellas redes donde el volumen de tráfico no permite la captura de paquetes en un periodo razonable de tiempo, existen programas para incrementar el tráfico mediante la inyección de paquetes para solicitar respuestas por parte de los clientes o del AP. La respuesta de los dispositivos incrementa la probabilidad de generar vectores de inicialización débiles. Existen herramientas como **Reinj** y **Aireplay** (incluida en *aircrack*) para capturar mensajes ARP con el siguiente procedimiento:

- El atacante captura un mensaje de petición ARP (o ACK con Reinj) y lo inyecta de regreso a la red hacia el AP.
- El AP no diferencia entre el paquete capturado y el paquete inyectado, el AP responde la petición ARP, dando al AP dos paquetes con que trabajar.
- El atacante ya ha recibido dos paquetes de respuesta y continúa reenviando paquetes hasta el *AP*.

WEP utiliza el *CRC* para verificar la modificación de paquetes durante la transmisión pero no posee integridad en la protección de los datos. Cuando se envía un paquete el *CRC* se calcula del texto en claro, la salida del algoritmo *CRC* es un valor de 4bytes cuyo nombre es *ICV*[61], este *ICV* se incluye en el texto en claro y luego encriptado con *WEP*. El *ICV* se ejecuta por parte del receptor una vez que los datos han sido desencriptados. Si el valor *ICV* enviado en el paquete coincide con el valor encriptado, entonces el paquete se considera legítimo. Debido a la naturaleza de *WEP* y el cifrado, es posible crear un paquete encriptado con un *ICV* valido, sin conocer el valor de la clave *WEP*. El atacante debe determinar la combinación de texto cifrado y de texto claro para la información que se envié con *IV* particular.

El atacante toma una muestra legitima de texto en claro y texto cifrado y aplica una operación *XOR* a estos valores para recuperar el ***keystream***[62] utilizado para encriptar el texto en claro. Todos los paquetes enviados por la red inalámbrica

[61] ICV Integrity Check Value
[62] Secuencia de claves

utilizan el mismo ***keystream*** con el mismo vector de Inicialización y la clave *WEP* secreta. Debido a que la clave *WEP* secreta puede ser cambiada en un periodo razonable de tiempo, el ***keystream*** debe ser el mismo para todos los paquetes utilizando el mismo *IV*.

Existen otras herramientas como **WEPWedgie** que transmite mensajes *ICMP* hacia todas las direcciones posibles de los clientes del *AP*. Esto genera respuestas por parte de todos clientes de la red y estas respuestas pueden utilizar un *IV* débil, también es posible utilizar este ataque con otro tipos de paquetes TCP, RST, TCP, SYN/ACK, etc. También puede encontrar paquetes WEP encriptados con autenticación Shared Key empleados cuando el cliente se conecta a un AP, este enviara al cliente un nonce el cual el cliente encripta utilizando la clave WEP. Este valor encriptado es enviado de regreso al AP para verificación. Si el valor que se obtiene cuando encripta el nonce es el mismo que el cliente retorna, se concede el acceso. Este proceso provee el valor de texto en claro que necesita el correspondiente texto cifrado. En este momento **WEPWedgie** puede inyectar paquetes a la red inalámbrica.

Una vez que el atacante obtiene la habilidad de inyectar paquetes en la red inalámbrica, puede abrir conexiones en los servidores internos, inclusive si estos se encuentran aislados por firewall. El atacante también puede escanear puertos en las maquinas internas, hacer un mapa de la red interna, etc. La tabla 10 muestra diferentes programas de inyección de paquetes.

Tabla 10. Inyección de Paquetes

Nombre	Dirección	OS
Reinj	http://www.wi-foo.com/soft/attack/wnet.tgz	BSD
WEPWedgie	http://wepcrack.sourceforge.net/	Linux

4.4 Ataques a EAP-LEAP y EAP-MD5

El protocolo *EAP* verifica la identidad del autenticador/suplicante en las comunicaciones empleando un servidor para facilitar la autenticación. *EAP-LEAP* fue el primer protocolo de autenticación mediante el uso de contraseñas, emplea el algoritmo MS-CHAP, infortunadamente este posee fallas que permiten el uso de ataques de diccionario y fuerza bruta contra el servidor de autenticación para obtener la contraseña. Como resultado a esas fallas, existen varios programas que permiten realizar este tipo de ataques en contra de la autenticación, el más famoso es Asleap desarrollado por Joshua Wright. Leapcrack y Leap permiten desarrollar este ataque. También existe una forma de autenticación de respaldo llamada *EAP-MD5*, posee vulnerabilidades como: susceptibilidad de recibir ataques *Man-in-the-Middle*, carencia de distribución dinámica de claves y combinación de texto en claro/texto cifrado. El proceso empleado por *EAP-MD5* es similar al de *EAP-LEAP*.

- El servidor de autenticación envía un requerimiento al suplicante que utiliza el *MD5* y la contraseña.

- Se envía un valor **hash**[63] es enviado de regreso al servidor de autenticación.
- El valor **hash** recibido es comparado con el del servidor y si estos son equivalentes, se otorga el acceso.

Como el proceso de autenticación solamente ocurre en una sola dirección, el ataque de Man-in-the-Middle puede ser desarrollado en contra del autenticador, con el único requerimiento de colocar un AP malicioso con un software de servidor de autenticación instalado, cuando el suplicante solicite el acceso, contactara el AP malicioso en vez del AP verdadero. La tabla 11 muestra diferentes programas de búsqueda de claves LEAP.

Tabla 11. Búsqueda de claves LEAP

Nombre	Dirección	OS
Asleap	http://asleap.sourceforge.net/	Linux Windows
Leap	http://packetstormsecurity.nl/0310-exploits/leap.tgz	Linux
Leapcrack*	http://www.securiteam.com/tools/6O00P2060I.html	Múltiple

*(Si posee Perl) Cualquier Plataforma.

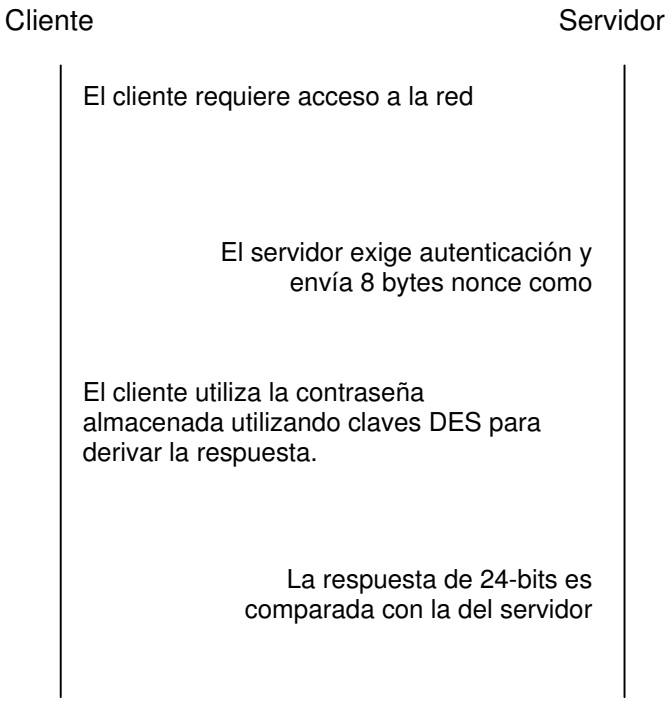
4.5 Ataques a VPN con PPTP

Las redes privadas virtuales permiten conexiones privadas entre dispositivos o redes remotas empleando cifrado en la información enviada entre los dispositivos que realizan la conexión y, utilizando autenticación entre estos. Luego de la gran decepción de WEP, las VPN fueron adoptadas como método de seguridad en

[63] Hash es una función para generar claves de gran longitud para objetos aplicando transformaciones matemáticas y operaciones lógicas.

redes WiFi, protegiendo los datos con el cifrado y limitando el ingreso a la red de personal no autorizado.

El protocolo de tunelaje punto a punto PPTP, es una extensión al protocolo punto a punto PPP utilizado por usuarios remotos para conectarse a su ISP creando una conexión segura con el servidor VPN. El estándar original PPTP especifico el uso del Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) para la autenticación. El diseño permitía la conexión al servidor, recibir autenticación basada en una contraseña y obtener acceso a los recursos de la red como muestra la siguiente figura.



Los bloques de 24-bits enviados al servidor para realizar la comparación, utilizando la contraseña almacenada por el cliente para descifrar la respuesta, si el bloque descifrado coincidía con el enviado originalmente, el acceso a la red era

otorgado. El proceso fue utilizado hasta que se implemento una nueva versión de MS-CHAP la cual debía corregir los problemas descubiertos.

MS-CHAP2 agrega seguridad al proceso con una autenticación mutua, se reemplazo el cambio de paquetes y se actualizaron las claves de cifrado aumentando el número de pasos en el proceso de autenticación, complicando el procedimiento e incrementando en poco a la seguridad del proceso.

Los ataques en la primera versión consistían en mensajes *spoofing* dirigidos hacia el servidor con la intención de cambiar la contraseña por parte del cliente. Si el cliente cambiaba la contraseña activa esta era susceptible a recibir ataques de programas como **L0phtcrack**. En la segunda versión se eliminaron las vulnerabilidades explotadas con estas herramientas cambiando el formato para el cambio de contraseñas.

Ettercap es otra utilidad que explota las debilidades de PPTP, tiene un número de *plugins* que automatizan el proceso de recuperación de contraseñas de PPTP que utilizan autenticación CHAP. La tabla 12 muestra la lista de programas para atacar la autenticación MS-CHAPv1 y v2.

Tabla 12. Ataques a VPN PPTP

Ataques a VPN PPTP empleando autenticación MS-CHAPv1 y v2		
Nombre	**Dirección**	**OS**
Ettercap	http://ettercap.sourceforge.net/	Linux
L0phtcrack	http://www.atstake.com/products/lc/	Win

4.6 Ataques de Negación de Servicios DoS

Los ataques de Negación de servicio y Negación de Servicios Distribuidos (DoS y DDoS) dejan a la red indefensa, son de los ataques más difíciles de frustrar, el ancho de banda de la red puede ser consumido por estos ataques.

Las redes inalámbricas son más susceptibles a este tipo de ataques, los atacantes pueden crear señales para saturar los recursos de la red, con transmisores poderosos que emiten señales que interfieren en la frecuencia de operación de WiFi.

Existen otros ataques a nivel de capa 2 del modelo OSI, con el envío de tramas de des-asociación y des-autenticación. Con el control de estas tramas, las conexiones serian manipuladas sin consentimiento alguno. Programas como **FakeAP, Void11** y **File2air**, son capaces de realizar este tipo de ataques.

Otro tipo de ataque es el envío masivo de tramas de autenticación en un formato irreconocible, causando la des-autenticación de clientes por la confusión del AP, este ataque ha sido implementado en la herramienta **fata_jack** de **AirJack**. Esta herramienta envía tramas de autenticación modificadas al AP, este recibe el mensaje creyendo que un nodo ha sido conectado dando como resultado una conexión fracturada, con la repetición sucesiva el cliente real no tendrá habilidad para conectarse al AP.

Cuando el cliente intenta la asociación y autenticación con el AP, este debe guardar información acerca del cliente en una tabla de estados interna, que incluye datos como la dirección MAC, IP, etc. La memoria del AP es finita, por lo que es posible enviar una cantidad de conexiones tal que el AP sufra un desborde

o **overflow**. Dependiendo del AP, esto puede provocar la caída o el bloqueo para la autenticación futura de usuarios legítimos, eliminando satisfactoriamente toda comunicación inalámbrica. Joshua Wright escribió un código en lenguaje Perl llamado **macfld.pl** que realiza este ataque. Este funciona inundando el AP con un gran número de direcciones MAC enviando tramas ACK al AP mencionando que la trama fue recibida correctamente, el AP evitaría la transmisión de información de todos los clientes.

Los ataques de negación de servicios no permiten que el atacante robe datos o que este obtenga acceso a la red, pero crea un caos significante en los recursos de la red que puede tener consecuencias desastrosas en las redes afectadas. La tabla 13 muestra la lista de programas para realizar ataques de Negación de Servicios.

Tabla 13. Negación de Servicios DoS

Nombre	Dirección	OS
Dinject	http://www.wi-foo.com/soft/attack/wnet.tgz	Linux
Fata_jack	http://www.loud-fat-bloke.co.uk/tools.html www.networkchemistry.com/news/whitepaper.pdf	Linux
FakeAP	http://www.blackalchemy.to/project/fakeap/	Linux - BSD
File2air	http://home.jwu.edu/jwright/code/file2air-0.1.tar.bz2	Linux
Macfld.pl	http://home.jwu.edu/jwright/code/macfld.pl	Linux
Omerta	http://www.securityfocus.com/archive/89/326248	Linux
Void11	http://www.wlsec.net/void11/	Linux

4.7 Ataques Man-in-the-Middle

Estos ataques suceden con la intervención de un atacante en medio del terminal cliente y el AP, el atacante puede tener control de la información para manipularla o inspeccionarla, obtener información como contraseñas y claves. Esto puede involucrar la inyección de código malicioso en el flujo de datos o comprometer los nodos de la red.

En el modo de infraestructura, los clientes y las estaciones conectadas al AP central, deben ser des-autenticadas y desasociadas, neutralizar el AP con un DoS y luego re-autenticar a los clientes con un clon bajo control del hacker.

Los programas para realizar estos ataques consisten en un software de AP y de DoS, el computador atacante debe poseer dos tarjetas inalámbricas separadas para evitar la confusión de señales y el proceso de clonado. Algunos de estos programas de emulación de AP son **HostAP y HermesAP**. La tabla 14 muestra la lista de programas para realizar ataques Man in the Middle.

Tabla 14 Software Man in the Middle

Nombre	Dirección	OS
Hostal	http://hostap.epitest.fi/	Linux
HermesAP match	http://www.hunz.org/monitoring-2_6-2.diff.bz2	Linux

4.8 Ataques a WPA-PSK

El modo WPA-PSK o personal, requiere que el cliente y el AP posean la misma clave PSK utilizada por la creación de la **Pairwise Master Key** (PMK) en el proceso de TKIP. Existe un problema con TKIP donde el atacante puede

determinar la PMK para alguno de los clientes inalámbricos, si esto sucede el atacante puede obtener acceso a la red. El investigador Robert Moskowitz, descubrió el problema con la implementación WPA-PSK[64] cuando se utilizan palabras claves cortas, cuando una clave PSK se emplea es combinada con un algoritmo de **hashing** con el SSID y la longitud del SSID, para crear una clave de 256Bits PMK. Esta clave es utilizada para derivar todas las otras claves que son empleadas en el algoritmo TKIP. La clave PSK es fijada con el SSID y la longitud del SSID datos que sirven de entrada en un algoritmo de **hashing** 4096 veces para crear la PTK. Moskowitz declaro que existe 2.5 bits de seguridad por carácter PSK con la siguiente fórmula:

2.5n + 12bits = Fortaleza de Seguridad en Bits

En donde n es el número de caracteres en la clave PSK. Esto significa que una contraseña típica de 10 caracteres provee 37 bits de seguridad. Por esta razón Moskowitz afirma que los ataques de diccionario pueden ser empleados en la recuperación de la contraseña. Existe un programa llamado **coWPAtty** para la recuperación de la PSK, el programa captura paquetes de la autenticación enviados entre el cliente y el AP para encontrar el SSID de la red, las direcciones de los AP y el cliente y mensajes **nonces** enviados entre estos. La información del SSID y la palabra frase del diccionario son utilizadas para encontrar la PMK. Utilizando el PTK, el atacante puede intentar descifrar un mensaje y verificar el ICV encontrado con los paquetes encontrados. Si estos coinciden ha encontrado

[64] MOSKOWITZ, Robert. "Weakness in Passphrase Choice in WPA Interface". 4 Nov 2003 http://wifinetnews.com/archives/002452.html

una palabra clave valida en potencia. La tabla 15, muestra la lista de programas para romper WPA-PSK.

Tabla 15. Programas para romper WPA-PSK

Nombre	Dirección	OS
coWPAtty	http://www.remote-exploit.org/downloads/cowpatty-2.0.tgz	Linux
WPA_Cracker	http://www.tinypeap.com/wpa_cracker.html	Linux

4.9 Redes HoneyPot

Las redes Honeypots son una herramienta flexible de seguridad con múltiples usos, como la prevención, detección o recopilación de información. Estas redes comparten el concepto de evitar el uso o cualquier producción de actividades no autorizadas en la red.

Existen dos tipos de honeypots los de producción e investigación. Las de producción son fáciles de utilizar, capturan información limitada y son utilizadas más que todo por compañías y corporaciones. Las de investigación son complejas de desplegar y mantener, capturan gran cantidad de información utilizada por los investigadores, entidades gubernamentales y/o militares. Programas como **mwcollect** los cuales son de libre distribución y son utilizados para recolectar información autónoma de *malware* que se esparce en la red. Estos programas extraen información de cómo el atacante obtuvo acceso a la red y como se exploto la carga de la red tomando muestras activas del proceso. Todo el proceso de

explotación es simulado en un ambiente virtual, así que el honeypot nunca es infectando con el Malware.

HoneyStick es una herramienta portátil para realizar Honeynet que son agrupaciones de redes honeypot, **HoneyStick** posee su propio OS con herramientas de respuesta ante ataques y puede ser cargado desde una memoria USB. **BackOficer Friendly** (BOF) detecta conexiones de servicios que utilizan puertos como Telnet, FTP, SMTP, POP3 e IMAP2, cuando el atacante recibe conexión de alguno de estos servicios BOF le envía mensajes falsos al atacante perdiendo este su tiempo creyendo que ha ingresado a la red. **Deception Toolkit y HoneyD** simulan sistemas vulnerables, son programables y puede generar respuestas a ataques externos simulando el comportamiento real del sistema según la herramienta empleada por el hacker. **HoneyD** puede emular servicios arbitrarios, este permite que un simple cliente obtenga múltiples direcciones LAN. Por último **Decoy Server** de Symantec da soluciones a áreas críticas de la red, aparte de servir de cortafuegos, emplea tecnología para habilitar alertas y detección de peligros. Cada acción es grabada permitiendo el análisis del administrador de cómo fue realizado el ataque e implementar políticas de respuesta ante estos eventos. Filtros de avanzada permiten habilitar soluciones ante eventos insignificantes, recopilando exclusivamente los incidentes de mayor gravedad. La tabla 16 muestra programas empleados para crear redes Honeypot.

Tabla 16. Redes HoneyPot

Software Honeypot		
Nombre	**Dirección**	**OS**
Mwcollect	http://www.mwcollect.org	Linux
Honeystick	http://www.ukhoneynet.org/honeystick.htm	Debian – USB
BackOfficer Friendly	http://www.nfr.com/resource/backOfficer.php	Win32 – Unix
Bait n Switch	http://baitnswitch.sourceforge.net	Linux
Deception Toolkit	http://www.all.net/dtk/dtk.html	Linux
Decoy Server	http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=157	Win – Solaris
HoneyD	http://niels.xtdnet.nl/honeyd/	Linux
Specter	http://www.specter.com/default50.htm	Win

4.10 Wireless Intrusion Detection Systems

Los sistemas de detección de intrusos inalámbricos (Tabla 17) están diseñados específicamente para identificar ataques apuntados hacia las redes 802.11. Los sensores detectan ataques desde una interfase inalámbrica, estos sistemas detectan específicamente el tráfico entre redes inalámbricas.

Airdefense Guard detecta intrusos en sistemas inalámbricos 802.11a/b/g, siendo una solución de seguridad al momento de identificar ataques y riesgos potenciales en la red, este posee herramientas de auditoria en tiempo real y monitoreo en la salud de la red inalámbrica para identificar y responder a fallas de hardware, interferencias a la red y degradación del desempeño de la misma. Detecta AP maliciosos, puede detectar problemas en la red inalámbrica y responder a ataques intrusos cuando estos suceden. Desempeña auditoria en tiempo real de todo el

hardware, siguiendo la huella a toda actividad inalámbrica y mejorando las políticas de seguridad y manejo en la red.

Snort-Wireless es un proyecto de detección de intrusos inalámbricos a la infraestructura IDS existente compatible con Snort 2.0.x y agregando nuevas opciones incrementando la funcionalidad de la red. Posee reglas de detección de AP maliciosos, redes AdHoc y detección de sniffers. **WIDZ** vigila las frecuencias locales en los AP en búsqueda de escáneres, AP maliciosos. **Neutrino** posee un agente de seguridad inteligente que escanea los paquetes de los dispositivos de la red y detecta las condiciones que pueden alterar la seguridad WLAN y su desempeño posee dos tipos de sensores uno inalámbrico y uno para Ethernet, cubriendo la infraestructura total de la red.

Tabla 17. Sistemas de detección de intrusos Inalámbricos WIDS

Software de WIDS	
Nombre	**Dirección**
AirDefense	http://www.airdefense.net/products/airdefense_ids.shtml
Snort-Wireless	http://snort-wireless.org
Neutrino	http://www.networkchemistry.com/products
WIDZ	http://freshmeat.net/projects/widz/?topic_id=43%2C245%2C151%2C152

4.11 Otras herramientas

Airjack: contiene un paquete de controladores para la inyección y recepción de paquetes en 802.11a/b/g necesarios para el desarrollo de aplicaciones de ataque MiTM y DoS en redes WiFi.

http://sourceforge.net/projects/airjack/ OS: Linux

Kismet: Sniffer inalámbrico, detecta intrusos en el sistema por los intentos de ataques, puede encontrar redes ocultas, AP maliciosos y clientes no autorizados. Detecta paquetes TCP, UDP, ARP y DHCP, puede dibujar las redes detectadas y estimar rango de redes en mapas de ciudades, esta herramienta es muy utilizada en Warxing.

http://www.kismetwireless.net/ OS: Win – Linux – BSD - MAC

Netstumbler: Esta es la herramienta más conocida de Windows para la búsqueda de AP 802.11a/b/g. También tiene una versión para ejecutar en PDAs con Windows Mobile llamada **MiniStumbler**. Posee aproximaciones más activas en la búsqueda de AP que Kismet, verifica el estado de configuración de la red, localiza lugares con poca cobertura inalámbrica, detectar redes que causan interferencia en la red, detecta AP maliciosos en el lugar de trabajo.

http://www.stumbler.net OS: Windows – Windows Mobile

Aircrack: conjunto de herramienta para 802.11a/b/g, romper claves WEP y WPA utilizando fuerza bruta. El paquete incluye **airodump** para la captura de paquetes,

aireplay para la inyección de paquetes, **aircrack** para romper claves estáticas WEP y WPA-PSK y **airdecap** para descifrar paquetes WEP y WPA capturados.

http://www.aircrack-ng.org/ Linux – MAC – BSD - Windows

WifiSlax: es una distribución en Linux de un Live CD basado en Slax, orientado hacia la seguridad Wireless, puede arrancar de manera booteable o ser instalado en el sistema operativo, posee también un entorno grafico de fácil manejo. Dirigido a la auditoria de seguridad inalámbrica, posee herramientas actuales para la auditoria inalámbrica y provee los controladores más comunes para tarjetas inalámbricas. Entre sus herramientas podemos encontrar:

- Escáneres de puertos: Nmap Front End 4.11, Amap, etc.
- Escáneres VPN: IKE-Scan, IKEProbe, PSK-Crack, etc.
- Escáneres de seguridad: GFI LanGuard 2.0, SuperScan, VNC auth Scanner, etc.
- herramientas: Yersinia 0.7, JTR 1.7.2, Metasploit, THC-Hydra, SQLquery, Etc.
- Recomposición de sesiones TCP: airdecap-ng y Wireshark
- Inyección de paquetes: aireplay-ng y Wireshark

El alcance de WifiSlax mejora la seguridad inalámbrica, promueve el abandono de WEP como mecanismo de defensa, potenciar la investigación de nuevos estándares de seguridad corrigiendo errores de cifrado mal implementado.

CONCLUSIONES

La gestión de políticas de seguridad en la red es un proceso que necesita ser actualizado constantemente porque los hackers o intrusos utilizan diversas técnicas, simples o sofisticadas, para explotar brechas en los protocolos de comunicaciones inalámbricas e intentar atentar contra la seguridad de la red, y de esta manera usan las técnicas para crear programas de libre distribución en Internet. El uso de estos programas maliciosos, en conjunto con malas directrices de administración de seguridad, puede acabar en resultados devastadores para la información manejada o en pérdidas de dispositivos; estas razones obligan al administrador de la red a definir políticas estrictas de seguridad necesarias para mantener el orden, minimizando en lo posible las amenazas de la red.

La labor del administrador de la red no se limita únicamente en el proceso de administrar contraseñas y elegir protocolos de autenticación. El administrador debe estar al tanto de nuevas investigaciones, de documentarse apropiadamente con revistas especializadas, foros y anuncios de los consultores e investigadores de seguridad de empresas reconocidas, con el fin de garantizar soluciones de seguridad efectivas a la altura de la red implementada y contemporáneas con las políticas de seguridad utilizadas en el resto del mundo, que tiende a ser cada vez mas pequeño por un proceso de globalización que parece no tener fronteras.

El uso de seguridad WEP, proporcionado de manera nativa con cualquier equipo WiFi, posee fallas como la ausencia de mecanismos de gestión de claves, métodos de autenticación y el ofrecimiento de confidencialidad en las comunicación. Por tal razón, se definieron en la línea del tiempo nuevas soluciones que evolucionaron y eliminan las fallas de WEP, tales como los esquemas de seguridad WPA y WPA2 que ofrecen una seguridad que puede llegar a ser infranqueable por los hackers. Sin embargo, la configuración de seguridad en los equipos puede ser confusa, por lo cual una solución complementaria para las redes WiFi corrige este aspecto de configuración de redes brindando al usuario realizar la configuración de la red de una manera amigable.

Entre las soluciones complementarias se ofrecen herramientas para proteger la red ante ataques de negación de servicios y evitar el uso de AP maliciosos y el uso de WIPS o de mecanismos de identificación de patrones en la forma de radiación de los equipos WiFi. Éstas son soluciones nuevas que aún se encuentran en desarrollo y pueden llegar a posicionarse como medidas de seguridad obligatorias en la red, por lo cual deben ser consideradas en el proceso de diseño e implementación, aunque de momento debido a los costes de implementación solo sean posibles para el uso de redes empresariales.

BIBLIOGRAFIA

- EDNEY, Jon; ARBAUGH, William A., Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison Wesley, 2003. Capítulo 4.
- LEHTINEN, Rick; Computer Security Basics, 2 Edición, O'Reilly, 2006. Capitulo 10 Section 8.
- TANENBAUM, Andrew S. Computer Networks, Fourth Edition, Prentice Hall, 2003. Capítulo 1, Sección 4.
- CARBALLAR, Jose A., Wi-Fi, como construir una red inalámbrica, Alfa Omega Ra-Ma, 2005, segunda edición
- TEWS, Erik, PYCHKINE Andrei, WEINMANN Ralf Philipp, Tecnologic University of Darmstadt, http://eprint.iacr.org/2007/120.pdf
- OU, George; Blogs Zdnet, Why Can't VPN replace Wi-Fi Security, http://blogs.zdnet.com/Ou/?p=489
- OU, George; Blogs Zdnet, The Six dumbest ways to secure a Wireless LAN, http://blogs.zdnet.com/Ou/?p=43
- MOSKOWITZ, Robert, Weakness in Passphrase Choice in WPA Interface, 2003 http://wifinetnews.com/archives/002452.html
- Wi-Fi Alliance http://www.wi-fi.org

- Scoot R. Fluhrer, Itskin Mantin. Adi Shamir, Weaknesses in the Key Scheduling Algorithm of RC4 Selected Area in Cryptography 2001
- HASSINEN, Timo; Overview of WLAN Security, Helsinki University of Technology, Thassine@cc.hut.fi
- Lehembre, Guillaurne, Wi-Fi security–WEP, WPA y WPA2, Hervé Schauer Consultants, http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf