UNIVERSIDAD DON BOSCO
VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACION

ANALISIS DE SEGURIDAD EN LA COMUNICACIÓN INALAMBRICA

PARA OPTAR AL GRADO DE MAESTRO EN SEGURIDAD Y RIESGOS INFORMATICOS

ASESORA:
DRA. MARÍA DE LOURDES LÓPEZ GARCÍA

PRESENTADO POR:
HECTOR ROGELIO DORATH MORALES

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica.
Febrero 2015

Análisis de seguridad en la Comunicación inalámbrica

Héctor Rogelio Dorath Morales
Universidad de Don Bosco, El Salvador

***Resumen*— Actualmente, la ventaja principal en el uso de los dispositivos móviles en combinación con los protocolos de comunicación inalámbrica es la facilidad de los usuarios para comunicarse en cualquier lugar de una manera fácil y eficiente. Por otro lado, la desventaja es la inseguridad en la comunicación a través de la red pública Internet.**

En este trabajo, se presenta una investigación sobre la funcionalidad de los protocolos existentes en la comunicación inalámbrica, de tal manera que el usuario tenga la certeza de su funcionalidad, las vulnerabilidades y los mecanismos que puede utilizar para mantener una comunicación libre de cables de manera segura.

Index terms ü Wireless communication, network security, security protocols.

Índice de Términos ü Comunicación inalámbrica, seguridad en redes, protocolos de seguridad.

I. Introducción

Las redes por computadora han evolucionado de manera exponencial desde el momento de su concepción volviéndose ahora una parte importante en muchas áreas de nuestra vida, incluso muchas veces sin darnos cuenta, al acceder a Internet consultando en algún motor de búsqueda, cuando se retira dinero de un cajero electrónico, cuando se conecta el dispositivo móvil a alguna red inalámbrica, o incluso cuando se escribe el usuario y contraseña en el lugar de trabajo.

Lo que muchas veces se desconoce es que esta de fondo cuando se hace clic para efectuar una petición. En general las redes se encuentran en cualquiera de los ámbitos ya sea laboral o personal.

Dentro del ámbito laboral, las redes por computadora han sido de una gran ayuda, facilitando la compartición de documentos y recursos, además de proveer una mejora sustancial en la administración de recursos, usuarios y demás dispositivos periféricos.

Dentro del ámbito personal va desde conectar la computadora a la red inalámbrica, compartir documentos entre familiares o la navegación por cualquiera de las páginas web.

De acuerdo con el avance tecnológico la manera de comunicarse ha evolucionado, los usuarios tienen como preferencia interactuar a través de dispositivos móviles tales como los celulares, las iPads, las Tablets, aún más que sobre los dispositivos cableados como las computadoras personales. De tal manera, que la comunicación que requiere cables como por ejemplo los teléfonos fijos, no puede ser implementada de la misma forma que para los dispositivos libres de cables. Por tal necesidad, aparecen los protocolos de comunicación inalámbrica que pretenden establecer la transferencia de información de un punto a otro usando como canal de comunicación el aire. La principal ventaja de la comunicación inalámbrica es la flexibilidad en su uso, la desventaja es la inseguridad de la transmisión sin cables.

Hasta este momento, se han propuesto protocolos para la comunicación inalámbrica como lo son el IEEE 802.11 en sus versiones a, b y g, principalmente.

Por lo anterior, este trabajo se enfoca en el análisis de la funcionalidad de los protocolos de comunicación inalámbrica, las vulnerabilidades y sus beneficios. Para lo cual, es necesario, presentar los conceptos básicos de las redes convencionales, las redes de comunicación inalámbrica y los servicios de seguridad.

El resto del documento se encuentra organizado como sigue. En la sección II se presenta una breve historia, definiciones y topologías de las redes convencionales. En la sección III, los conceptos básicos de las redes inalámbricas. En la sección IV y la sección V se presentan los protocolos de comunicación y de seguridad inalámbrica, respectivamente. En las secciones VI y VII se listan los ataques más comunes de las redes inalámbricas y algunas técnicas de prevención para evitarlos. Finalmente, en la sección VIII se presentan las conclusiones de este trabajo.

II. Redes de computadoras

En 1957 se forma la Agencia de Investigación de Proyectos Avanzados (ARPA, por sus siglas en inglés) como parte del departamento de defensa de los Estados Unidos para impulsar el desarrollo tecnológico. En 1965, ARPA patrocinó un programa que permitió que la máquina TX-2 en el laboratorio Lincoln del MIT y la AN/FSQ-32 del System Development Corporation de Santa Mónica en California se enlazaran directamente mediante una línea dedicada de 1200 bits por segundo. Cuatro años después, nace la ARPANET compuesta por cuatro nodos situados en la UCLA (Universidad de California en Los Ángeles), el SRI (Stanford Research Institute), la UCBS (Universidad de California de Santa Bárbara, Los Ángeles) y la Universidad de UTA. En 1973, esta red llegó a tener más de 40 computadoras conectadas.

La comunicación entre los nodos en la red inicialmente se realizaba con el protocolo de control de red (NCP). Ante la gran demanda de correos y cuentas personales entre los usuarios de la red, se desarrolló un protocolo de emergencia el TCP/IP que se estableció en 1980. Actualmente, existen dos estándares importantes en la industria de la comunicación ya sea inalámbrico o por cable, y es que aun en la comunicación humana es necesario ponerse de acuerdo en un mismo lenguaje, es acá donde aparecen los estándares de comunicación como lo son el protocolo TCP/IP y el modelo OSI. Estos protocolos han ido evolucionando poco a poco mejorando cosas como lo son el control de errores y el control de flujo [1].

El modelo OSI tiene siete capas y no todas son implementadas en los dispositivos de comunicación. Las capas son definidas en la Tabla I.

Como se puede notar, cada capa tiene su propia función. La capa física es la encargada de mover la información a través del medio de comunicación fijo, ya sea teléfono, cable, el aire en caso de las redes inalámbricas. La capa de enlace es la encargada de establecer la conexión con el otro par al que se está queriendo conectar. La capa de Red es la encargada de manejar los paquetes, hacia donde se dirige y provee un estándar o plantilla de paquetes para que estos puedan ser usados por la capa de enlace. Hasta este punto las capas son implementadas por los fabricantes de hardware de cada dispositivo y no son a nivel lógico en cada host, a partir de la capa 4 hacia arriba, son implementadas por cada nodo en la red.

La capa de transporte es la encargada de llevar sin errores los datos entre el emisor y receptor así como mantener el orden de los paquetes. La siguiente capa es la de sesión, que como su nombre lo indica, es la encargada de mantener las sesiones, cuando usamos cookies en el navegador de Internet, es también la capa encargada de expirar (cerrar) la sesión además de reiniciarla en caso de ser necesario. La siguiente capa que es la de presentación encargada de codificar y decodificar la información. Además para los protocolos de Internet es la capa encargada de implementar la capa de aplicación.

Por otro lado, un ámbito importante en el cual se han explotado las redes por computadora es la programación, llevando el concepto de tener que procesar todo en la computadora local a transferirlo

para procesarse en un ordenador central dejando las computadoras como “terminales tontas”, y dando paso a un concepto muy usado en la actualidad como lo es el paradigma “Cliente/Servidor” en el cual la computadora cliente hace peticiones por medio de la red para poder obtener un dato o efectuar una acción determinada y esta es procesada por un servidor el cual devuelve un valor.

TABLA I. CAPAS DEL MODELO OSI

No. capa	Nombre	Descripción
1	Física	Especifica conectores, la frecuencia en la que pasan los datos y como los bits son codificados, también incluye corrección de errores a bajo nivel
2	Enlace	Especifica métodos de comunicación a través de un enlace, incluyendo el acceso a medios cuando estos son compartidos (WIFI, Ethernet, ISO 13239)
3	Red	Especifica métodos de comunicación de múltiples saltos de diferentes enlaces. Para redes con paquetes define la estructura del paquete
4	Transporte	Especifica los métodos de conexión o asociaciones entre diferentes programas corriendo bajo el mismo sistema operativo (Internet, TCP, etc.).
5	Sesión	Especifica métodos para múltiples conexiones constituyendo una sesión de comunicación. Se incluye cerrar conexiones, reiniciarlas y poner puntos de verificación. ISO X.225 es un ejemplo en esta capa.
6	Presentación	Especifica métodos de conversión de datos y las reglas para conversión de las aplicaciones. Un ejemplo puede ser EBCDIC a ASCII
7	Aplicación	Especifica métodos para completar las tareas iniciadas por el usuario, estas son desarrolladas por desarrolladores, ejemplo Skype, FTP, etc.

En un comienzo, si se quería tener una red, era necesario tener todo el equipo desde el cable hasta la tarjeta de red, y equipos y hardware del mismo fabricante, esto debido a que el protocolo que usaban para comunicarse entre sí era el mismo y ningún otro fabricante lo tenía. La forma en que las redes se comunicaban se definía de acuerdo a la topología de red, de la cual se desprenden seis tipos:

1. Punto a punto
2. En bus
3. En estrella
4. En anillo o circular
5. En malla
6. En árbol

La topología punto a punto es la más simple y se define como el enlace entre dos nodos (Fig. 1). En este tipo de redes los nodos trabajan como “Cliente” y como “Servidor” ya que no existe una centralización de la administración, siendo eso la mayor desventaja cuando la red crece en número de nodos.

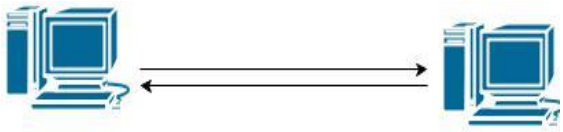

Figura 1. Topología punto a punto

La topología de bus se caracteriza por compartir un sólo canal de comunicación denominado Bus (Fig. 2). En cada uno de los extremos del cable que conecta a los nodos, existen unas resistencias llamadas *terminadores.* Básicamente el concepto es que cuando un nodo intenta mandar un mensaje a otro este tiene que esperar que no exista ninguno otro nodo usando el canal de comunicación. Entre las ventajas de este modelo es que es de fácil la escalabilidad de crecimiento e implementación. Entre las desventajas se menciona el límite de equipos debido a que la señal se debilita en el cable, además de una compleja detección de fallos en caso que un nodo falle.

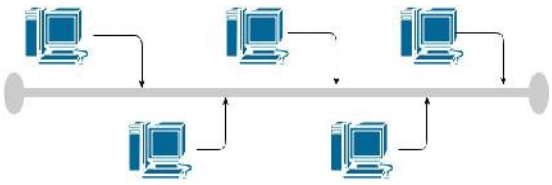

Figura 2. Topología de bus

La topología estrella es la más usada actualmente, en esta topología los nodos se conectan a un dispositivo central que es el encargado de enviar el paquete a su nodo destino (Fig.3).

Entre las ventajas que posee es su fácil administración, prevención de colisiones y centralización de la administración.

Entre sus desventajas se citan la dependencia del dispositivo central ya que si este falla interrumpe la comunicación de la red completa.

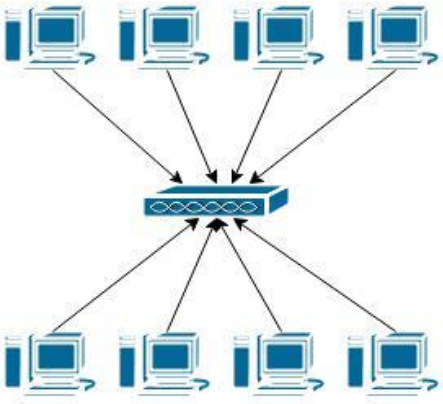

Figura 3. Topología de estrella

En la topología de anillo o circular la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones, (Fig.4).

De entre las ventajas que se pueden mencionar es que cada nodo posee un acceso equitativo a la red y que el rendimiento no recae cuando hay muchos equipos en la misma.

Entre sus desventajas se puede mencionar lo difícil que se vuelve el diagnosticar alguna falla en la red y reparar problemas.

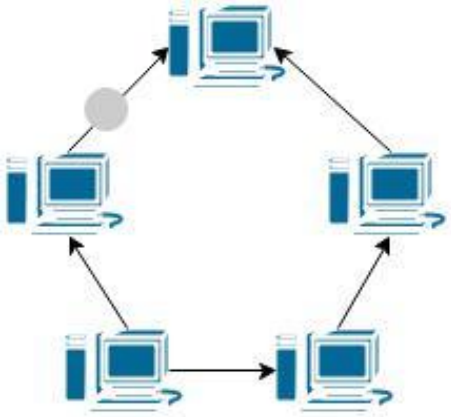

Figura 4. Topología de anillo

La Fig. 5 muestra la topología de malla que es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar el tráfico de un nodo a otro por distintos caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones.

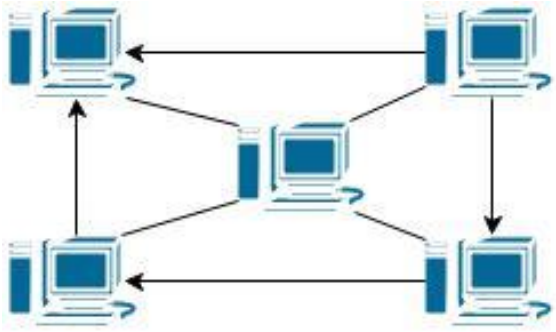

Figura 5. Topología de malla

La topología de árbol, mostrada en la Fig. 6, es muy parecida a la red estrella excepto que un extremo está conectado a otro switch o router donde se ramifican más nodos.

Entre las ventajas es la fácil solución de problemas debido a su centralización, además de que es soportado por casi todos los vendedores de software y hardware

Entre sus desventajas se menciona que tiene difícil configuración y además un extremo uso de cable.

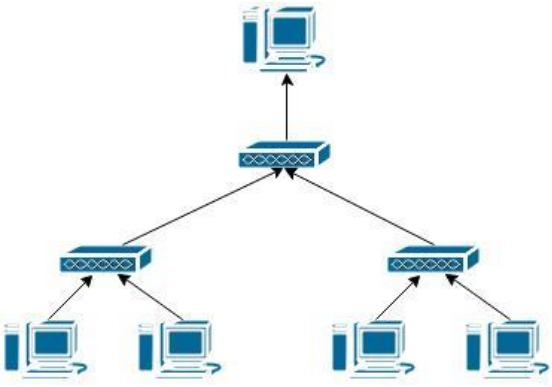

Figura 6. Topología de estrella

III. REDES INALÁMBRICAS

Las redes inalámbricas son un mecanismo de conexión inalámbrica que nace tras la creciente necesidad de conectar dispositivos entre sí, sin el uso de cables. Es un término usado en informática para la interconexión de nodos sin necesidad de una conexión física, sino más bien por ondas electromagnéticas.

Una red inalámbrica posee una gran cantidad de ventajas como la de tener ahorro de cables, flexibilidad de conexión y hasta incluso comodidad, pero así también posee muchas desventajas entre las cuales esta una de las más importantes: la seguridad.

La seguridad fue, es, y será uno de los más grandes desafíos para este tipo de redes ya que están más expuestas a ser interceptadas. A lo largo de este trabajo se estarán presentando diferentes tipos de ataques y vulnerabilidades, además de cómo funcionan cada uno de los tipos de cifrados y protocolos para la comunicación de estas redes.

Otro gran reto que acompañó al nacimiento de las redes inalámbricas fue la forma en la que estas se comunicarían entre sí sin importar la compañía que fabrique el dispositivo, es ahí donde nace el estándar IEEE 802.11.

Existen diferentes tipos bajo el estándar 802.11. El 802.11a se refiere al modo de acceso que alcanza hasta 54Mbps en un rango de frecuencia de 5Ghz, mientras que el 803.11b define un acceso de 11Mbps en el rango de frecuencia de 2.5Ghz entre otros como el estándar 802.11g que poco a poco va tomando cada vez más auge [2].

Las redes inalámbricas son clasificadas de acuerdo a su cobertura, como se muestra en la Fig. 7.

Las redes personales o (Personal Area Network), son redes de corto alcance, generalmente usadas para interconectar dispositivos de corto alcance típicamente no más de 10 metros. Un ejemplo de esta tecnología puede ser el Bluetooth, o el láser infrarrojo.

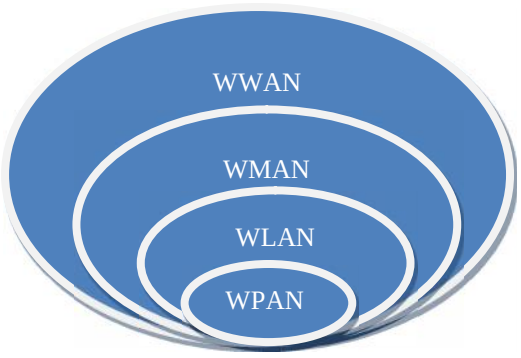

Figura 7. Cobertura de las redes inalámbricas

En el mejor caso, como es una red generalmente utilizada para conectar dispositivos como mouse, teclados, audífonos, etc. Es común que la conexión sea automática cuando el dispositivo entre en el rango de acción.

Wireless Local Area Network es una red es en la cual los usuarios pueden conectare a la LAN (Local Area Network) sin hacerlo de forma alámbrica. Esta forma de comunicación está regida por el estándar de la IEEE 802.11

La forma en la que se transmiten los datos de un lado a otro no es por medio de un medio físico guiado sino a través de ondas de radio portadoras de información. A este proceso se le llama modulación.

En una red LAN (con cable) los puntos de acceso se conectan a la red cableada de un lugar fijo mediante cableado normalizado. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del y las ondas, mediante una antena.

Otro de los problemas que presenta este tipo de redes es que actualmente (a nivel de red local) no alcanzan la velocidad que obtienen las redes de datos cableadas debidas entre otros factores al medio por el cual se mueven y la velocidad de las ondas.

Además, en relación con el apartado de seguridad, el tener que cifrar toda la información supone que gran parte de la información que se transmite sea de control y no información útil para los usuarios, por lo que incluso se reduce la velocidad de transmisión de datos útiles y no se llega a tener un buen acceso.

La naturaleza de la conexión sin cable es transparente a la capa del cliente que previamente se mencionó en el modelo OSI.

Las WMAN (Wireless Metropolitan Area Network) son usadas en su mayoría para conectar diferentes redes WLAN y están regidas por el estándar de la IEEE 802.16.

Esta red está pensada para abarcar un rango de cobertura de una ciudad y tienen mayor cobertura que una WLAN pero menor que una WWAN.

La WMAN es normalmente manejada por proveedores, por ejemplo el ISP (Internet Service Provider), entidades gubernamentales, o grandes corporaciones.

Wireless Wide Area Network es un tipo de rede que posee una cobertura mayor que las WLAN y las WPAM y es normalmente usada para tener un alcance a nivel nacional o incluso internacional.

Además de diferir en el alcance, también lo hace en su tecnología ya que las redes de telefonía celular pueden ser catalogadas bajo esta categoría. Algunos ejemplos de esta categoría son CDMA2000, GSM, cellular digital packet data (CDPD) and Mobitex para la transferencia de datos.

IV. PROTOCOLOS DE COMUNICACIÓN INALÁMBRICA

Antes de comenzar de lleno con los protocolos de comunicación inalámbrica, convendría definir el concepto de protocolo. Según la enciclopedia británica, protocolo se define como un conjunto de reglas o procedimientos para la transmisión de datos entre dispositivos electrónicos, como los ordenadores. A fin de que los equipos intercambien información, debe haber un acuerdo preexistente en cuanto a cómo la información se estructura y cómo cada lado enviará y recibirá [3].

El protocolo utilizado para la comunicación de redes impuesto por la IEEE es el 802 siendo el 802.3

para la comunicación por cable y el 802.11 para la comunicación inalámbrica [4]. Dentro de este estándar se definen técnicas para modular las cuales están definidas por las letras a, b y g siendo estas tres las más comúnmente usadas, los demás estándares como el *c, f, h , j, n* son mejoras o extensiones hechas a los estándares principales [4].

El estándar 802.11 define dos modos de operación, el modo **infraestructura**, en el que los clientes de tecnología inalámbrica se conectan a un punto de acceso y el modo **ad-hoc** en el que los clientes se conectan entre sí sin ningún punto de acceso [5].

En el modo de infraestructura, cada estación informática (que abreviaremos EST) se conecta a un punto de acceso a través de un enlace inalámbrico. La configuración formada por el punto de acceso y las estaciones ubicadas dentro del área de cobertura se llama *conjunto de servicio básico* o BSS. Estos forman una célula. Cada BSS se identifica a través de un BSSID (identificador de BSS) que es un identificador de 6 bytes (48 bits). En el modo infraestructura el BSSID corresponde al punto de acceso de la dirección MAC [5].

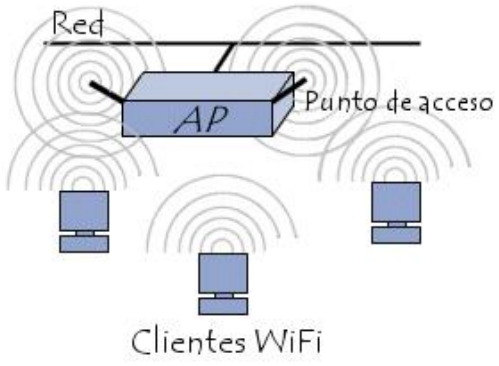

Figura 8. Modo de operación de infraestructura

TABLAI II. VERSIONES PROTOCOLO 802.11

Protocolo	Descripción
802.11a	Llamado también WiFi5. Tasa de 54 Mbps Trabaja a 5 GHz, frecuencia menos saturada que 2,4. Este estándar posee 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto.
802.11b	Conocido como WiFi. El más utilizado actualmente. Las mismas interferencias que para 802.11 ya que trabaja a 2,4 GHz. Tasa de 11 Mbps
802.11c	Es una versión modificada del estándar 802.1d, que permite combinar el 802.1d con dispositivos compatibles 802.11 en el nivel de enlace de datos.
802.11d	Este estándar es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
802.11e	Define los requisitos de ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo. Está destinado a mejorar la calidad del servicio en el nivel de la capa de enlace de datos.
802.11f	Su objetivo es lograr la interoperabilidad de puntos de acceso (AP) dentro de una red

	WLAN multiproveedor. El estándar define el registro de puntos de acceso dentro de una red y el intercambio de información entre ellos cuando un usuario se traslada desde un punto de acceso a otro.
802.11g	Ofrece un ancho de banda de 54 Mbps en el rango de frecuencia de 2,4 GHz. Es compatible con el estándar 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.
802.11h	El objetivo es que 802.11 cumpla los reglamentos europeos para redes WLAN a 5 GHz. Los reglamentos europeos para la banda de 5 GHz requieren que los productos tengan control de la potencia de transmisión y selección de frecuencia dinámica.
802.11i	Aprobada en Julio 2004, se implementa en WPA2. Destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el protocolo de encriptación AES.
802.11n	Se basa en la tecnología MIMO. Trabajará en la frecuencia de 2.4 y 5 GHz. Soportará tasas superiores a los 100Mbps.
802.11s	Redes Mesh o malladas.

Cada una de las celdas a las que dan cobertura los APS, permite crear redes que den cobertura en zonas amplias, permitiendo así la movilidad de desplazarse sin perder conectividad.

En el **modo ad hoc** los equipos clientes inalámbricos se conectan entre sí para formar una red punto a punto, es decir, una red en la que cada equipo actúa como cliente y como punto de acceso simultáneamente.

La configuración que forman las estaciones se llama conjunto de servicio básico independiente o IBSS.

Un IBSS es una red inalámbrica que tiene al menos dos estaciones y no usa ningún punto de acceso. Por eso, el IBSS crea una red temporal que le permite a la gente que esté en la misma sala intercambiar datos. Se identifica a través de un SSID de la misma manera en que lo hace un ESS en el modo infraestructura.

En una red ad hoc, el rango del BSS independiente está determinado por el rango de cada estación. Esto significa que si dos estaciones de la red están fuera del rango de la otra, no podrán comunicarse, ni siquiera cuando puedan "ver" otras estaciones. A diferencia del modo infraestructura, el modo ad hoc no tiene un sistema de distribución que pueda enviar tramas de datos desde una estación a la otra. Entonces, por definición, un IBSS es una red inalámbrica restringida.

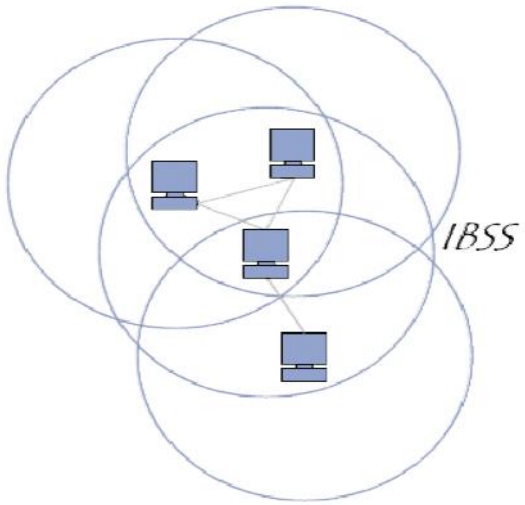

Figura 9. Modo de operación Ad hoc

i) Espectros de difusión

Espectro ensanchado de difusión es una familia de métodos para transmitir una sola señal de radio utilizando un amplio segmento del espectro de radio. Las redes inalámbricas utilizan varios sistemas de transmisión ondas de radio, Espectro ensanchado por ondas de frecuencia (FHSS), Espectro ensanchado por secuencia directa (DSSS), y división de frecuencia ortogonal (OFDM). La Tabla III muestra la frecuencia para cada espectro.

Algunas redes de datos más antiguos utilizan el sistema FHSS que es más lento, pero las primeras redes inalámbricas utilizaban DSSS, y sistemas más recientes utilizan OFDM. La siguiente tabla enumera cada uno de los estándares y el tipo de modulación de espectro ensanchado que utilizan [6].

TABLA III. ESPECTROS PARA LA TRANSMISIÓN INALÁMBRICA

Estándar	Frecuencia	Modulación
802.11 a	5Ghz	OFDM
802.11b	2.4 Ghz	DSSS
802.11g	2.4Ghz	OFDM

El espectro ensanchado por ondas de frecuencia (FHSS) divide la señal de radio en pequeños segmentos y saltos de una secuencia a otra múltiple vez por segundo mientras va transmitiendo. El que envía y el que recibe establecen un canal sincronizado de saltos en el cual usan diferentes subcanales.

Este sistema supera la problemática de la interferencia de otros usuarios utilizando un sistema más reducido que cambia muchas veces por segundo.

Para algunos dispositivos antiguos 802.11 la banda de 2.4 Ghz es divida en 75 canales cada uno con un ancho de 1Mhz [6].

El Acceso múltiple por división de frecuencias ortogonales (OFDM) consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias donde cada una transporta información, la cual se modula entre QAM y PSK.

Esta técnica divide la frecuencia en un número de bandas de frecuencia, en cada una de estas se transmite una porción de información del usuario, cada una de los sub portadores es ortogonal al resto y es por eso el nombre de esta técnica [7].

El Espectro ensanchado por secuencia directa (DSSS) genera un patrón de bits redundante para cada uno de los bits que componen la señal. Cuanto mayor sea este patrón de bits, mayor será la resistencia de la señal a las interferencias. El estándar IEEE 802.11 recomienda un tamaño de 11 bits, pero el óptimo es de 100. En recepción es necesario realizar el proceso inverso para obtener la información original [8].

V. PROTOCOLOS DE SEGURIDAD

Hablar de seguridad en las redes inalámbricas es sumamente importante debido a que la información es transmitida por medio de un canal público como lo es el aire, por lo tanto es necesario definir protocolos de comunicación segura para el tráfico de información. Esta información puede ser: tarjetas de crédito, datos privados de empresas, etc.

A continuación se detallan los diferentes protocolos diseñados para poder solventar la problemática que representa la comunicación segura.

i) WEP (Wired Equivalent Privacy)

Este protocolo basado en RC4 que utiliza claves de 64 bits o de 128 bits, con una clave secreta de 40 bits o 104 bits. Este protocolo fue presentado para igualar el nivel de privacidad que se obtiene en las redes cableadas y fue presentado en 1999.

Este protocolo utiliza un patrón de redundancia cíclica CRC – 32 que es utilizado para verificar la integridad del paquete a la hora que es entregado.

La base del WEP se encuentra en la operación lógica XOR, el cual dice que si se aplica dos veces

esta operación a un valor se obtendrá el valor original.

El WEP no protege la conexión por completo sino solamente el paquete de datos. Este sistema posee dos tipos de autenticación los cuales son el Sistema abierto y el de clave compartida.

En el sistema abierto, el cliente no debe autenticarse con el router o punto de acceso.

En el sistema de clave compartida, se poseen cuatro fases:

1. La estación cliente envía una petición de autenticación al Punto de Acceso.
2. El punto de acceso envía de vuelta un texto modelo.
3. El cliente tiene que cifrar el texto modelo usando la clave WEP ya configurada, y reenviarlo al Punto de Acceso en otra petición de autenticación.
4. El Punto de Acceso descifra el texto codificado y lo compara con el texto modelo que había enviado. Dependiendo del éxito de esta comparación, el Punto de Acceso envía una confirmación o una denegación. Después de la autenticación y la asociación, WEP puede ser usado para cifrar los paquetes de datos.

Estas fases definidas anteriormente se pueden ver en el Figura 10.

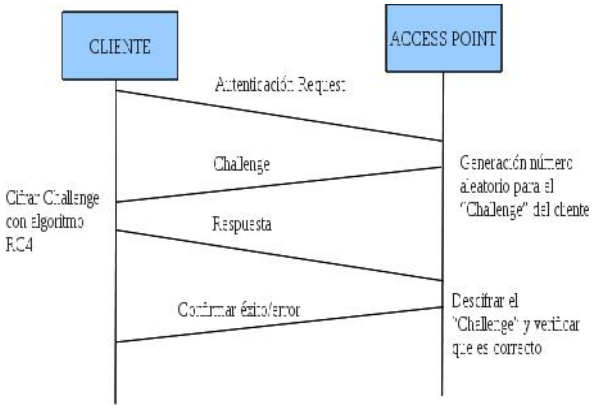

Figura 10. Funcionamiento de clave compartida

Este protocolo no contempla un mecanismo de distribución automática de claves por lo cual es obligatorio escribir la clave en cada dispositivo, lo que puede provocar que la transmisión sea vulnerable, además de que aumenta el costo de mantenimiento en caso que se desee cambiar la clave.

El algoritmo usado por WEP es el siguiente:

1. Se calcula un CRC de 32 bits esto para garantizar la integridad de los mensajes. (integrity check value)
2. Se concatena el ICV al mensaje que se desea enviar y se concatena la clave secreta a continuación del vector de inicialización formado la semilla (Seed).
3. El PRNG (Pseudo-Random Number Generator) de RC4 genera secuencia de caracteres aleatorios a partir de la semilla (seed) de la misma longitud obtenido en el punto 2.
4. Se calcula el XOR de lo que se formó en el punto 2 con el resultado del punto 3 y este es el mensaje cifrado.
5. Se envía el vector de inicialización sin cifrar y el mensaje cifrado del campo de datos.

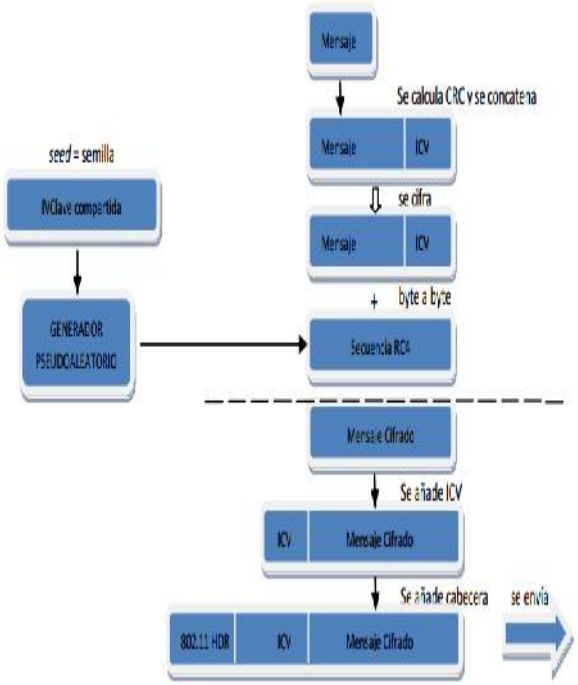

Figura 11. Algoritmo usado por WEP

Vulnerabilidades de WEP

Los problemas de vulnerabilidad de WEP recaen en los problemas del algoritmo RC4 y en el vector de inicialización. El Vector de inicialización no es especificado su uso por la norma 802.11 por lo tanto queda abierto al fabricante de los productos, esto implica que el fabricante fija el vector a 0 y se incrementa en 1 para cada trama por lo cual esto ocasiona que el comienzo tanto del vector como de la clave de repitan frecuentemente.

Otro problema que posee es la cantidad de vectores posibles a generar es bien poco el universo 2^{24} que son aproximadamente 16 millones por lo cual se repite este vector. En el escenario ideal no debería nunca de repetirse [9].

ii) WPA (WiFi Protected Access)

Este Sistema nace debido a las fallas presentadas por WEP, este estándar implementa la mayoría de los estándares de la 802.11i.

Este sistema trabaja con un servidor de autenticación, normalmente RADIUS, que es el encargado de distribuir las claves a los diferentes usuarios a través del protocolo que se esté utilizando de la familia 802.11x, presentando también la opción de usar una clave pre compartida (que normalmente es menos seguro).

La mejora quizá más importante sobre el protocolo WEP es la adición del Protocolo de Integridad de Clave Temporal (TKIP - Temporal Key Integrity Protocol), lo que hace es cambiar las claves guardadas en el servidor de autenticación cada cierto tiempo para evitar ser un ataque de recuperación de claves estático. WEP es vulnerable a este ataque.

WPA implementa un código de integridad del mensaje (MIC - Message Integrity Code), también conocido como "Michael". Además, WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas.

Otra vulnerabilidad a la cual está expuesto este algoritmo es a lo que se llama “Keystream” que tiene como finalidad obtener varios mensajes con igual vector de iniciación lo que permitirá conocer el mensaje original.

Una vulnerabilidad más asociada es que como este protocolo utiliza un CRC para verificar la integridad del mensaje, este puede ser alterado al igual que el mensaje sin necesidad de conocer el mensaje original sino cambiando algunos de los bits en el bloque del mensaje.

También puede asociársele la vulnerabilidad que no existe protección contra mensajes repetidos, esto es que si el atacante captura un paquete de la red lo puede volver a inyectar a ella momentos después de la transmisión.

Al usar el WPA en su forma PSK (Pre Shared Key), también conocido como WPA Personal, no requiere de un servidor de autenticación sino que utiliza una clave compartida en las estaciones y el punto de acceso, lo que lo diferencia del WEP en este punto es que esta clave sólo sirve para el inicio de la autenticación pero no para cifrar los datos. Esta forma es usada mucho para usuarios domésticos o con redes pequeñas debido a su complicada administración.

La otra forma de uso es con un servidor de autenticación (RADIUS), este también es conocido como WPA Enterprise, donde un servidor es el encargado de efectuar las tareas de autenticar a las estaciones, además de autorizarlas y contabilizarlas. La forma en la que funciona este protocolo es que mantiene el puerto bloqueado en el servidor hasta el que usuario se autentica, esto lo hace usando el protocolo EAP y un servidor de autenticación (RADIUS). Si la autenticación es correcta entones el servidor abre el puerto.

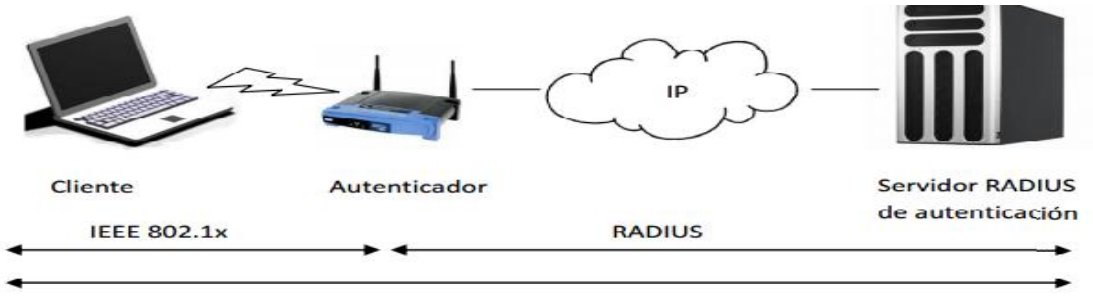

Figura 12. Funcionamiento de WPA

Algunos de los elementos que entran en consideración en este sistema son:

- Solicitante: usuario que solicita tener acceso a la red.
- Autenticador: su función es forzar el proceso de autenticación y enrutar el tráfico hacia los dispositivos adecuados en la red, típicamente este rol lo hace el Access Point.
- Servidor de Autenticación: Autentica al usuario.

Vulnerabilidades de WPA

Quebrar un sistema como el WPA es mucho más complejo que el WEP, debido a su fuerte algoritmo de cifrado, pero no está exento de ello. Una de sus vulnerabilidades es en el momento del handshake (protocolo donde se ponen de acuerdo los dispositivos para crear una sesión segura) ya que haciendo uso de un ataque de diccionario se puede obtener la clave, este diccionario puede ser tan pequeño como 100 Mb y puede llegar hasta 10Gb dependiendo del universo de palabras. Básicamente utilizando un algoritmo de fuerza bruta.

iii) WPA2 (WiFi Protected Access 2)

Este Sistema es una mejora del antes mencionado WPA con el Sistema de cifrado AES (Advanced Encryption Standard, véase apéndice A).

Este estándar cumple el estándar de la IEEE 802.11i que son mejoras que no estaban incluidas en el estándar WPA, este estándar pretendía admitir el sistema de cifrado AES que es mucho más seguro y a diferencia del WPA anterior puede también asegurar redes Ad-hoc.

Otra de las mejoras que se le hicieron fue el uso opcional de la memoria cache de la clave maestra en pares (PMK) siendo de este modo el acceso a los usuarios mucho más rápido. En la tabla IV se muestra la comparativa entre el WPA y el WPA2.

TABLA IV. WPA vs WPA2

	WPA	**WPA2**
Modo Enterprise	Autenticación 802.1x EAP	Autenticación: 802.1x / EAP
	Cifrado: TKIP/MIC	Cifrado AES- Comp
Modo Personal	Autenticación PSK	Autenticación PSK
	Cifrado: TKIP/MIC	Cifrado AES- Comp

Vulnerabilidades de WPA2

Este protocolo es el más fuerte de los protocolos existentes tanto en autenticación como en transmisión de datos cifrados al usar AES. Pero quizá solo era cuestión de tiempo que se encontraran vulnerabilidades ya que se ha encontrado una llamada “Hole 196” descubierta por la compañía AirTight Networks. Esta vulnerabilidad es muy parecida a un ataque de “man in the middle” o “ataque de hombre en el medio” donde se puede inyectar paquetes y tráfico para comprometer la autenticación de los dispositivos. Actualmente no existe nada que se pueda hacer para parchar esta vulnerabilidad.

VI. ATAQUES A REDES INALÁMBRICAS

Las redes inalámbricas, como se mencionó previamente, están más expuestas a ataques ya que ocupan un medio público de transporte de información como lo es el aire.

Algunas de las formas más comunes de ataque a las redes inalámbricas son las siguientes: ARP Poisoning, MAC spoofing, Denial of service, WLAN escáners , Wardriving y Warchalking [10].

i) ARP Poisoning

ARP, un protocolo muy simple, consiste en simplemente cuatro tipos de mensajes básicos:

Una petición ARP. El equipo A solicita a la red: "¿Quién tiene esta dirección IP?"

Una respuesta ARP. Equipo B dice el equipo A, "Yo Tengo la IP. Mi dirección MAC es [XXXXX]."

Una solicitud ARP inversa (RARP). El mismo concepto como ARP Request, pero el equipo A le pregunta: "¿Quién tiene esta dirección MAC?".

Una Respuesta RARP. Equipo B dice el equipo A, "Tengo que MAC. Mi dirección IP es [XXXXX]".

Todos los dispositivos de red tienen una tabla ARP, una memoria a corto plazo de todas las direcciones IP y direcciones MAC que el dispositivo ya ha emparejado. La tabla ARP se asegura de que el dispositivo no tiene que repetir peticiones ARP para los dispositivos que ya se ha comunicado [11].

Un hacker puede explotar envenenamiento de caché para interceptar el tráfico de red entre dos dispositivos de la red. Por ejemplo, digamos que el hacker quiere ver todo el tráfico entre su equipo, 192.168.0.12, y el router de Internet, 192.168.0.1. El hacker comienza enviando un ARP malicioso "respuesta" (para los que no había ninguna petición anterior) a su router, asociar la dirección MAC de su computadora con 192.168.0.12.

ii) MAC Spoofing

La dirección MAC es una dirección física asociada al dispositivo de red, la dirección MAC está grabada a la NIC (Network Interface Controller) y esta no puede estar cambiada. Es ahí donde existen muchas herramientas las cuales hacen creer al sistema operativo que la dirección MAC asociada a la NIC es otra que la que está grabada, y es este proceso el que se conoce como MAC Spoofing.

Una de las razones principales del porque esta técnica es tan importante prevenirla es que si un hacker hacer pensar a los dispositivos de la red que su máquina es la máquina destino puede interceptar información importante de manera “legitima” [12].

iii) Denial of service (DoS)

El ataque por medio del DoS o ataque de denegación de servicio consiste en tratar de hacer una máquina o una red inaccesible a los usuarios.

Un ataque DoS puede ser perpetrado de varias formas. Aunque básicamente consisten en [13]:

- Consumo de recursos computacionales, tales como ancho de banda, espacio de disco, o tiempo de procesador.
- Alteración de información de configuración, tales como información de rutas de encaminamiento.
- Alteración de información de estado, tales como interrupción de sesiones TCP (TCP reset).
- Interrupción de componentes físicos de red.
- Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, de manera que ya no puedan comunicarse adecuadamente.

Los ataques DoS pueden clasificarse en dos categorías [13]:

- Ataques de inundaciones (Flood Attacks).
- Ataques lógicos o de software.

Ataques de inundaciones (Flood Attacks)

Este ataque consiste en cuando un equipo dentro o fuera de la red comienza a enviar tráfico dirigido al servidor de la red, atacando específicamente los ciclos del CPU, llenando la memoria RAM, o enviando tantos paquetes a la red hasta que baje su desempeño hasta incluso cesar el funcionamiento debido al alto tráfico.

Algunos de los ataques por inundación podemos mencionar los siguientes:

1) Ataque de inundación TCP SYN

Aprovechando el defecto de TCP de tres vías comportamiento apretón de manos, un atacante realiza solicitudes de conexión dirigidas al servidor víctima con paquetes con direcciones de origen inalcanzables. El servidor no es capaz de completar las solicitudes de conexión y, como resultado, la víctima pierde la totalidad de sus recursos de red. Una relativamente pequeña inundación de paquetes falsos atará memoria, CPU y aplicaciones, lo que resulta en el cierre de un servidor.

2) Smurf IP Attack

El atacante envía paquetes de eco ICMP a las direcciones broadcast de las redes vulnerables. Todos los sistemas en estas redes responden a la víctima con respuestas de eco ICMP. Esto agota rápidamente el ancho de banda disponible para el objetivo y niegan efectivamente sus servicios a los usuarios legítimos.

3) Ataque de inundación UDP

El protocolo UDP es un protocolo sin conexión y no requiere ningún procedimiento de configuración de conexión para transferir datos. Un Ataque de inundación UDP se da cuando un atacante envía un paquete UDP a un puerto aleatorio en el sistema víctima. Cuando el sistema víctima recibe un paquete UDP, determinará qué aplicación está esperando en el puerto de destino. Cuando se da cuenta de que no hay ninguna aplicación que está esperando en el puerto, se generará un paquete ICMP de destino inaccesible a la dirección de origen forjado. Si los paquetes UDP que se entregan a los puertos de la víctima son en gran cantidad, el sistema va a caer.

4) Ataque de inundación ICMP

Hay 2 tipos básicos, inundaciones y nukes.

Una inundación ICMP se hace generalmente con la difusión, ya sea mediante un grupo de pings o paquetes UDP. La idea es, para enviar tal cantidad de datos al sistema objetivo, que frena tanto que estará desconectado del IRC debido a un tiempo de espera del ping.

Los Nukes explotan errores en ciertos sistemas operativos, como Windows 95 y Windows NT. La idea es enviar un paquete de información que el sistema operativo no puede manejar. Por lo general, hacen que su sistema se bloquee.

iv) Ataques lógicos o de software.

Son pequeños paquetes mal formados con los cuales se intenta explotar un bug en el sistema objetivo.

Entre los ataques lógicos de software tenemos:

1) Ping de la muerte

El atacante envía un paquete de solicitud de eco ICMP que es mucho más grande que el tamaño máximo de paquete IP a víctima. Dado que el paquete recibido es más grande que el tamaño normal de paquetes IP, la víctima no puede volver a armar los paquetes. El sistema operativo puede ser abatido o se reinicia como resultado.

2) Ataque de Lágrima

El atacante envía dos fragmentos que no se pueden volver a armar correctamente manipulando el valor de desplazamiento de paquetes por lo se reinicia o apaga el sistema víctima. Muchas otras variantes como targa, SYNdrop, Boink, Nestea Bonk, TearDrop2 y newtear están disponibles.

v) Evil twin Networks

Este ataque es muy fácil de llevar a cabo, basta con estar en un lugar público y que el atacante tenga un punto de acceso al cual le puede poner el mismo nombre de la red legitima y al momento que el usuario intente conectarse en vez de entrar al router principal lo hará al del atacante, una vez ahí el atacante puede mostrar páginas que desee al usuario, enviar paquetes falsos, etc.

Una forma de prevenir este tipo de ataques es asegurarse de que al entrar a páginas importantes con contraseñas asegurarse que los certificados sean los correctos.

vi) Wardriving

Esta técnica implica detectar redes inalámbricas por medio de un dispositivo móvil y en un vehículo en movimiento para poder acceder a ellas quebrando su cifrado WEP.

vii) Ataques específicos contra WPA y WPA2

En el 2008 la compañía rusa ElcomSoft publicó que había logrado disminuir el tiempo para lograr obtener una clave WPA usando tarjetas de video como NVDIA usando fuerza bruta [14].

Este ataque se realiza sobre una captura de tráfico que el adversario debe conseguir en el momento de la autenticación. Esto no representaba un problema al algoritmo puesto que igual había que hacerlo por fuerza bruta y este se mantenía a salvo siempre y cuando se usase una llave lo más larga posible y con caracteres especiales.

VII. FORMAS DE PREVENIR ATAQUES A LAS REDES INALÁMBRICAS

Antes de hablar sobre las formas de prevenir un ataque, convendría hablar sobre la forma en que funcionan los hackers y algunos de los términos iniciales.

a. Intrusión

Conjunto de acciones realizadas para tratar de introducirse a una red o un sistema de forma ilícita poniendo en peligro la confidencialidad, integridad y disponibilidad de la información.

b. Amenaza

Acción o evento que puede comprometer seguridad. Una amenaza es una potencial violación de seguridad

c. Vulnerabilidad

Existencia de debilidades, diseño o errores en implementación que pueden incitar a comprometer la seguridad del sistema inesperada e indeseablemente.

d. Ataque

Un asalto en la seguridad del sistema que esta derivada desde una amenaza inteligente. Un ataque es cualquier acción que viola la seguridad.

e. Ingeniería social:

Proceso de obtener información, interactuando directamente con personas internas de la empresa, las cuales pueden proporcionar de una manera ingenua, cualquier información que le pueda servir a un hacker [15].

Luego de haber declarado estos términos, es importante definir la forma en la que los atacantes trataran de introducirse al sistema o red.

Los pasos que el atacante sigue son: Reconocimiento, escaneo, ganar acceso, mantener acceso, limpiar rastros.

a. Reconocimiento:

En esta fase el atacante recolecta toda la información relacionada a su objetivo, es donde hace un reconocimiento de su blanco antes de lanzar el ataque.Estas técnicas de reconocimiento pueden ser de 2 tipos, activas o pasivas.

El reconocimiento activo involucra una interacción directa con la víctima a diferencia del pasivo que muchas veces es ideado usando ingeniería social.

b. Escaneo:

En esta etapa el atacante escanea por medio de herramientas especializadas alguna vulnerabilidad o susceptibilidad del sistema para poder explotarla.

El escaneo incluye el uso de dialers, escáneres de puerto, mapeo de red, barridos (sweeping), escáneres de vulnerabilidad, etc., por ejemplo: Nmap, Nessus,OpenVas, Acunetix, Qualys, GFiLANguard.

Las herramientas de análisis de vulnerabilidades se basan en plugins, por lo tanto es importante mantenerlos actualizados, además configurar de forma adecuado el perfil del análisis de vulnerabilidades en base a la información recolectada en fases anteriores.

c. Ganancia de acceso:

Esta etapa es donde el atacante efectúa el ataque como tal, es donde se ejecuta la penetración explotando la vulnerabilidad detectada en la etapa anterior. Es acá donde se generan los ataques que se mencionaron en el apartado anterior como lo son: denegación de servicio, secuestro de sesión, crackeo de password, ataque man-in-the-middle (spoofing), y denegación de servicio.

El riesgo del negocio es alto, esta etapa es donde el hacker puede ganar acceso a los niveles de Sistema Operativo, Aplicación o nivel de red.
Existen dos tipos de lugares donde el atacante puede llevar a cabo su ataque y son: del lado del cliente y del lado del servidor, en la primera es donde se usa mayoritariamente la ingeniería social.

d. Mantenimiento del acceso:

Una vez el atacante ha entrado a la red, tratara de dejar esa vulnerabilidad abierta para poder volver a ingresar alguna otra vez. En esta etapa es donde dejan cosas como Backdoors, Rootkits o trojans, todo esto con la finalidad de permanecer oculto.

e. Cubriendo pistas o huellas

En esta etapa ya luego que el atacante ha ingresado y además tiene asegurado su ingreso y permanencia en el sistema, antes de salir del mismo, este trata de ocultar pistas y lo hace por ejemplo alterando archivos de logs, usando caballos de Troya, steganografia, etc.

Existen formas de prevenir y disminuir el riesgo de ser víctima de un ataque informático, las cuales se mencionan a continuación:

i) Hacking Ético:

Una de las mejores formas de prevenir un ataque es pensando como el atacante pensara, y tratando de penetrar la seguridad del sistema o red por lo cual las instituciones contratan personas para que traten de quebrantar la seguridad de sus instituciones.

Incluso hay casos de empresas que sacan concursos para que cualquier persona interesada en intentar quebrantar su seguridad lo intente y si logran hacerlo los remuneran, todo esto con la finalidad de mejorar su seguridad.

La mayoría de hacking ético se hace en base a la metodología ISSAF (Information System Security Assesment Framework). Este sistema es un sistema ordenado que pretende organizar y categoriza los sistemas de seguridad.

Este marco incluye los siguientes criterios de evaluación [16]:

- Una descripción de los criterios de evaluación.
- Sus metas y objetivos
- Los requisitos esenciales para dirigir las evaluaciones
- El proceso para la evaluación
- Exhibición de los resultados esperados
- Contramedidas y recomendaciones
- Referencias para documentos externos

La metodología se muestra en la Figura 13:

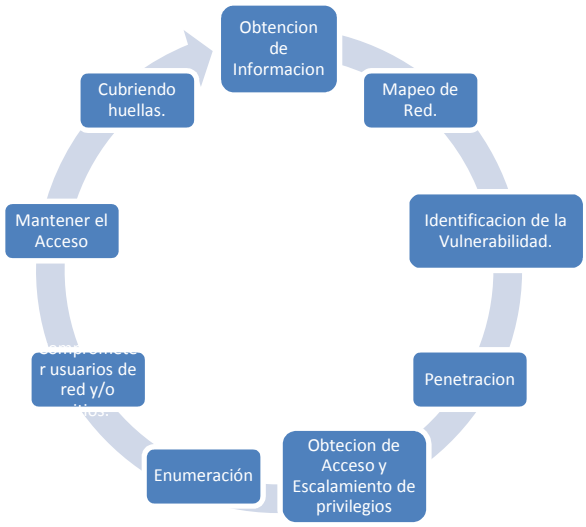

Figura 13. Metodología ISSAF

La seguridad en las redes inalámbricas se puede basar en 3 funciones principales:

1. Cifrar el canal de comunicación con métodos como el WPA2.
2. Limitar el acceso y manteniendo controles como pueden ser controles a través de filtrado por MAC.

3. Proteger con contraseñas seguras y robustas con más de 30 caracteres que combinen números, letras, símbolos, mayúsculas y minúsculas.

ii) Cifrar el canal de comunicación

La importancia de un canal de comunicación cifrado es vital debido a la falta de privacidad en el medio de comunicación inalámbrico.

iii) Cifrado de Red con clave

Hasta el momento el WPA2 es el cifrado más seguro para las redes inalámbricas, ahora bien, este solo sirve para el intercambio de llave con el punto de acceso o router. Ya que una vez la llave haya sido intercambiada este utiliza AES para el posterior tráfico.

Otra medida a tomar en cuenta es usar un servidor RADIUS para el manejo de contraseñas con el router, así cada usuario manejaría su clave con el servidor y si este usuario es vulnerado solo vulneraria la comunicación entre esos dos equipos no el resto de la red.

iv) Filtrado por dirección MAC

La dirección MAC como se mencionó previamente es el identificador único a nivel de hardware en la red. El filtrado consiste en no dejar conectar a la red inalámbrica ninguna computadora que no esté previamente registrada su dirección MAC.

Este no es un método que ofrezca un alto grado de seguridad, puesto que un atacante puede falsear su dirección y hacer que coincida con una de las permitidas, pero es una medida básica para evitar que cualquiera pueda acceder a la red de forma trivial.

v) Ocultamiento del SSID

El SSID o Service Set Identifier, como se mencionó previamente, es el nombre de red que se está transmitiendo al momento de querer conectarse a la red. Una buena práctica es tenerlo oculto y que los usuarios tengan que conectarse al punto de acceso de forma manual. Así como sucede con el filtrado por MAC el atacante también puede encontrar la red pero puede ayudar a que no se haga de forma trivial.

vi) Evitar el uso de DHCP

El servidor DHCP es el encargado de entregar direcciones IP de forma automática a los equipos que se conecten a la red.

De no ser posible quitar el uso de DHCP, se tiene que limitar el rango de direcciones IP que se entregan por parte del servidor y así limitar el uso de direcciones legítimas que el atacante pudiera hacer uso de ellas.

Al igual que las anteriores, no usar DHCP no es una medida que proteja de forma absoluta, pero sí contribuye a una implementación de una red más segura por capas.

vii) Diseño de red

Es quizá la parte más importante para la seguridad de la red. Acá es donde se establecen mecanismos para evitar que un atacante pueda entrar a la red. Dentro de un buen diseño de red es necesario considerar lo siguiente:

- Establecer redes privadas virtuales (VPN) a nivel de cortafuegos, para el cifrado adicional del tráfico de la red inalámbrica.
- Deben de existir corta fuegos entre la red inalámbrica y la red física.
- Los clientes externos deben conectarse usando conexiones seguras como IPSec, Secure Shell (SSH), o VPNs.

VIII. CONCLUSIONES

Aunque se tenga una seguridad perimetral de primer nivel, y los anillos de seguridad más apropiados para evitar ataques, estos quedan sin efecto si el usuario no está educado con respecto a temas de seguridad informática. Este ha sido y seguirá siendo el eslabón más débil en la cadena y es por eso que es donde hay que comenzar a hacer concientización.

Por la naturaleza de sus vulnerabilidades el sistema de cifrado WEP en las redes inalámbricas no debe ser utilizado.

Por el contrario, el sistema de cifrado para el intercambio de llave y transmisión de información actualmente es el WPA2 AES debido a su algoritmo WPA2 para intercambio de llaves y AES para la transmisión de información, lo que hace más difícil el trabajo de un adversario.

Además, es importante saber elegir el modelo de red a utilizar para evitar ataques a la red o sistemas de manera trivial.

En las redes inalámbricas hasta esta fecha no poseen la misma velocidad que las redes cableadas, esto debido al medio en el que se manejan y los métodos de cifrado que hay que usar para transferir la información en un canal público.

Por lo tanto, ningún sistema de red, por más anillos de seguridad que queramos implementar es 100% seguro, por lo cual también debemos estar preparados para algún imprevisto.

IX. RECOMENDACIONES

Como resultado de este estudio se recomienda el uso de WPA2 AES para el cifrado en redes inalámbricas, esto también conlleva a pensar en una solución integral teniendo en cuenta desde la parte de administración como la parte física como los dispositivos de la red.

Se recomienda, para uso institucional, manejar en la medida de lo posible un servido RADIUS para evitar que si un atacante logra descubrir la clave de un dispositivo, no corrompa la seguridad de toda la red sino solo la de ese dispositivo.

Se recomienda un buen diseño de red hecho a la medida para las necesidades de la institución para tener una mejor seguridad inalámbrica.

APENDICE A. ADVANCED ENCRYPTION STANDARD (AES).

Es un sistema de cifrado simétrico, es decir, la misma llave se ocupa para cifrar que para descifrar los bloques de datos ya que es un sistema por bloques.

Antes de hablar sobre AES, es conveniente mencionar los dos tipos de cifrado que existen: el primero es asimétrico y el segundo es simétrico.

El primero, es conocido como Criptografía de llave pública, este difiere del simétrico porque posee dos llaves.

En este cifrado, la llave pública es utilizada para cifrar la información y la privada para descifrar la información.

Otro uso que se le da a estos cifrados de llave pública es el hashing, esta es una función matemática que no tiene inversa y produce un resultado de longitud fija. A diferencia de la función de cifrado que se utiliza para garantizar la confidencialidad de la información, la función de hashing es utilizada en seguridad para garantizar la integridad de la información.

El cifrado simétrico por el contrario, maneja una sola llave. Este es conocido como Shared Key o Shared Secret.

La ventaja del cifrado simétrico es su rapidez y sencillez, en comparación con su contraparte el cifrado asimétrico. Igualmente su poca complejidad intrínseca permite la fácil implementación de esta técnica de cifrado a nivel hardware.

El cifrado simétrico fue desarrollado por dos criptólogos belgas, Joan Daemen y Vincent Rijmen, ambos estudiantes de la Katholieke Universiteit Leuven, y enviado al proceso de selección AES bajo el nombre "Rijndael".

El 23 de noviembre de 1976 se establece el primer estándar de cifrado DES. Desde ese momento se han publicado muchos ataques para criptoanalizarlo de una manera más rápida que con fuerza bruta.

En el año 1997, el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST), emprende un proceso para sustituir el ya obsoleto DES.

Entre los requisitos mínimos que debería de tener son:

- El algoritmo debía ser público.
- Debe ser algoritmo de cifrado en bloque simétrico.
- La longitud de la clave debe ser mínimo de 128 bits.
- Su diseño permite aumentar la longitud de la clave según las necesidades.
- Debía poder ser implementado en hardware y software.

Por fin en el año 2000 se celebró una tercera conferencia donde ya quedaban 5, los cuales al final de votar quedaron los siguientes algoritmos:

1. RIJNDAEL -> 86 votos
2. SERPENT -> 59 votos
3. TWOFISH -> 31 votos
4. RC6->23 votos
5. MARS -> 13 votos

Por lo tanto, en octubre de este año quedo establecido el estándar AES (rijndael), como el estándar de comunicaciones para el departamento de defensa de Estados Unidos.

Este cifrado puede procesar bloques de hasta 128 bits, utilizando llaves de 128, 192 y 256 bits. Está basado en una red de permutaciones y sustituciones constituida por una serie de operaciones matemáticas también llamadas S-Boxes y permutaciones llamadas P-Boxes.

Existen distintos modos de operación dependiendo de cómo se mezcla la clave con la información a cifrar:

Modo ECB (Electronic Codebook): El texto se divide en bloques y cada bloque es cifrado en forma independiente utilizando la clave. Tiene la desventaja que puede revelar patrones en los datos. La Figura 14 muestra el proceso de cifrado y descifrado.

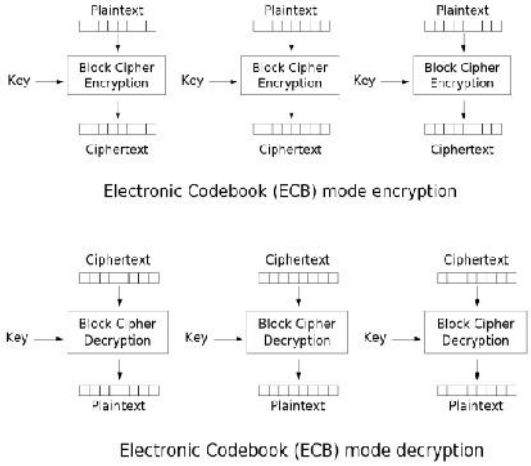

Figura 14. Diagrama de cifrado y descifrado ECB

Modo CBC (CBC): El texto se divide en bloques y cada bloque es mezclado con la cifra del bloque previo, luego es cifrado utilizando la clave. La Figura 15 muestra el proceso de cifrado y descifrado para este modo de operación.

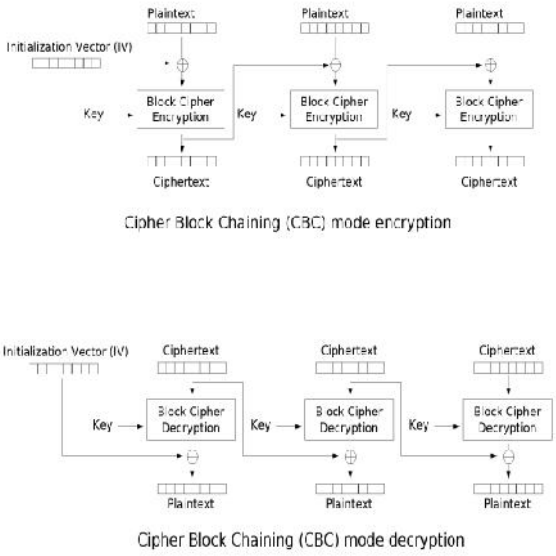

Figura 15. Diagrama de cifrado y descifrado CBC

Modo PCBC (Propagating cipher-block chaining):

El modo propagating cipher-block chaining fue diseñado para que pequeños cambios en el texto cifrado se propagasen más que en el modo CBC. El algoritmo de cifrado se ve en la Figura 16.

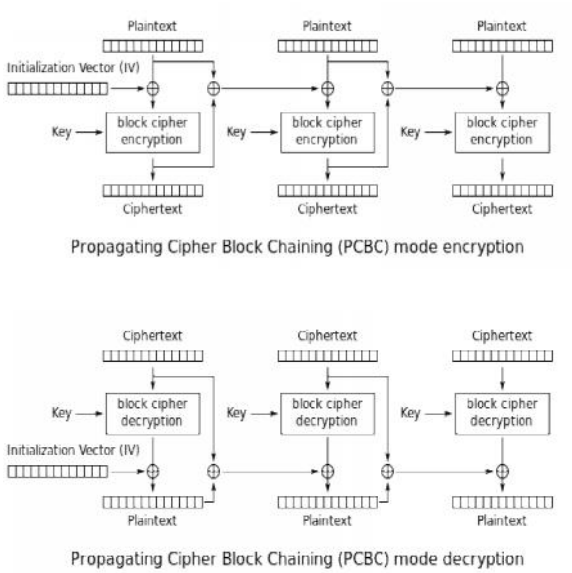

Figura 16. Diagrama de cifrado y descifrado PCBC

Modo OFB:

El modo OFB (output feedback) emplea una clave para crear un bloque pseudoaleatorio que es operado a través de XOR con el texto claro para generar el texto cifrado. Requiere de un vector de inicialización que debe ser único para cada ejecución realizada. La Figura 17 muestra ambos procesos de cifrado y descifrado.

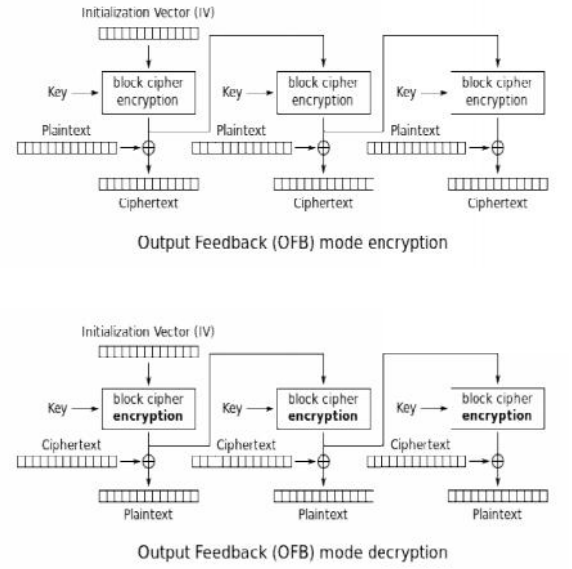

Figura 17. Diagrama de cifrado y descifrado OFB

Bloques AES

AES, al ser un algoritmo de cifrado por bloques, inicialmente fue diseñado para tener longitud de bloque variable pero el estándar define un tamaño de bloque de 128 bits, por lo tanto los datos a ser cifrados se dividen en segmentos de 16 bytes (128 bits) y cada segmento se le puede ver como un bloque o matriz de 4x4 bytes al que se le llama estado, este se organiza de la siguiente forma (Figura 18:

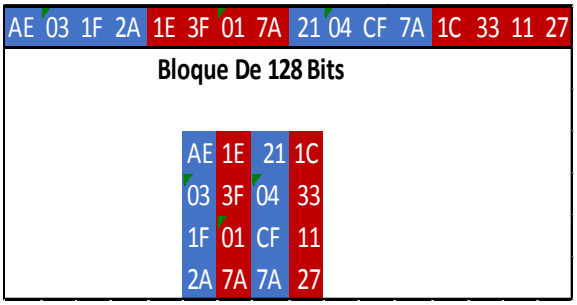

Figura 18. Bloque de Matriz 4x4 AES.

Claves AES

Por ser simétrico, se utiliza la misma clave para cifrar como para descifrar. La longitud de la clave puede ser de 128, 192 o 256 bits según especifica el estándar, esto permite tres implementaciones conocidas como AES-128, AES-192 y AES-256, el presente trabajo está basado en AES-128.

Partiendo de una clave inicial de 16 bytes (128 bits), que también se la puede ver como un bloque o matriz de 4x4 bytes, se generan 10 claves, estas claves resultantes junto con la clave inicial son denominadas sub claves.

Rondas y operaciones

El proceso de cifrado del algoritmo consiste en aplicar a cada estado un conjunto de operaciones agrupadas en lo que se denominan rondas, el algoritmo realiza 11 rondas, donde en cada ronda se aplica una subclave diferente.

Las 11 rondas se pueden clasificar en 3 tipos:

- 1 ronda inicial (se aplica la subclave inicial).
- 9 rondas estándar (se aplican las 9 subclaves siguientes, una en cada ronda).

- 1 ronda final (se aplica la última subclave).

Las operaciones que realiza el algoritmo dentro de las rondas se reducen a 4 operaciones básicas:

- SubBytes.
- ShiftRows.
- MixColumns.
- AddRoundKey.

A continuación en la figura 19, se muestra un diagrama de cómo se aplican las operaciones y claves en cada una de las rondas:

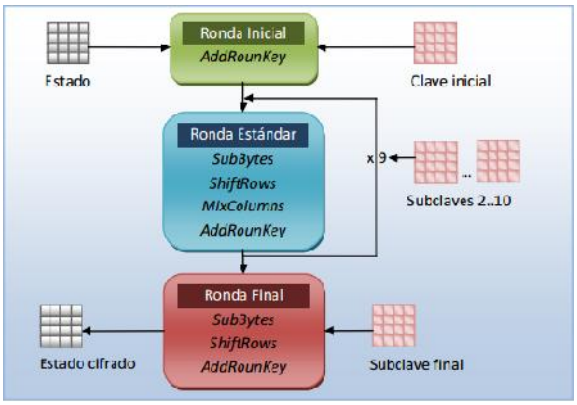

Figura 19. Bloque de Matriz 4x4 AES.

Para la ronda inicial se aplica solamente la operación AddRoundKey que es básicamente un XOR byte a byte entre el bloque a cifrar y la clave. Como se puede observar en la Figura 20, la matriz estado es operada con la clave inicial con un xor y resultan los valores presentados a la derecha.

Estado		SubClave Inicial		
32 88 31 E0		2B 28 AB 09	=	19 A0 9A E9
43 5A 31 37	XOR	7E AE F7 CF		3D F4 C6 F8
F6 30 98 7		15 D2 15 4F		E3 E2 8D 48
A8 8D A2 34		16 A6 88 3C		BE 2B 2A 08

Figura 20. Ronda Inicial

Se realizan 9 rondas estándar donde cada ronda consiste en las siguientes operaciones:

SubBytes: Cada byte del estado se reemplaza por otro valor de acuerdo a la tabla de sustitución de bytes S-Box.

ShiftRows: En cada fila del estado, a excepción de la primera, se rotan circularmente hacia la izquierda los bytes, en la segunda fila se rotan una posición, en la tercera dos posiciones y en la cuarta tres posiciones.

ShiftRows								
D4	E0	B8	1E	=>	D4	E0	B8	1E
27	BF	B4	41		BF	B4	41	27
11	98	5D	52		5D	52	11	98
AE	F1	E0	30		30	AE	F1	E0

Figura 21. Ronda Estándar.

A cada columna del estado se le aplica una transformación lineal, esto es multiplicarlo por una matriz predeterminada.

AddRoundKey: Se aplica la misma operación que en la ronda inicial pero utilizando otra subclave.

En la ronda final consiste en las siguientes operaciones:
SubBytes: igual al de la ronda estándar.
ShiftRows: igual al de la ronda estándar.
AddRoundKey: igual al de la ronda inicial y estándar pero aplicando la última subclave.

Descifrado AES

El proceso de descifrado aplica las mismas operaciones que el cifrado pero de forma inversa utilizando las mismas sub claves generadas en orden inverso, además se utiliza una matriz distinta en la operación MixColumns de manera de obtener la inversa de la transformación lineal aplicada en el proceso de cifrado.

Seguridad de AES

Si se trata de descifrar AES, el algoritmo conocido es por fuerza bruta.

La longitud de la llave es directamente proporcional al tiempo que tomara lograr quebrar la seguridad por fuerza bruta.

En la figura 22 se muestra un ejemplo de cómo sería romper por fuerza bruta una llave de 4 –Bits.

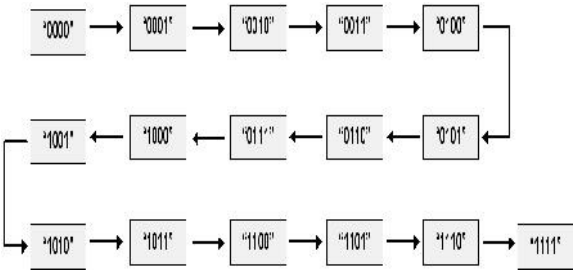

Figura 22. Romper AES 4-bit por fuerza bruta.

Como se observa en la figura se tomaría 16 para probar cada una de las posibilidades para encontrar la llave correcta.

En la tabla V se presentan las posibles combinaciones que pueden realizarse para atacar una llave según su longitud en bits.

TABLA V. COMBINACIÓN DE LLAVES VS TAMAÑO DE LLAVE.

Tamaño de Llave	Combinaciones Posibles
1-Bit	2
2-Bit	4
4-Bit	16
8-Bit	256
16-Bit	65536
32-Bit	4.2x10 ^ 9
56-Bit(DES)	7.2x10 ^ 16
64-Bit	7.2x10 ^ 19
128-Bit (AES)	3.4x10 ^ 38
192-Bit (AES)	6.2x10 ^ 57
256-Bit (AES)	1.1x10 ^ 77

Nótese que el crecimiento de las combinaciones posibles es exponencial y no tiene solución en tiempo polinomial solo exponencial lo cual hace que el tiempo para romper este algoritmo también crezca de manera exponencial.

Un atacante que desee realizar un ataque podrá verse bajo las siguientes opciones:

1. *Texto en claro desconocido y clave desconocida.*

Si el atacante solo dispone de un bloque cifrado, debería cifrar con todas las claves posibles y todos los bloques en claro posibles, para ir comparando el resultado con el bloque cifrado.

Para valores estándar del algoritmo como la clave de 256 bits y un bloque de 256 bits se demuestra que el bloque no se puede invertir. Si se toma en general el tamaño de bloque de v-bits, y la clave de n-bits. El atacante deberá probar 2^v bloques posibles y repetir este proceso para todas las claves 2^n. Actualmente es imposible computacionalmente resolver esto en un tiempo finito.

2. *Texto en claro conocido y texto cifrado conocido.*

El atacante posee el texto en claro y el texto cifrado. Para resolver esto es necesario probar el texto en claro con el texto cifrado con todas las claves posibles.

Para una clave de 128 bits, se necesitaran aplicar 2^{127} veces el algoritmo para lograr ver cuál es la clave necesaria. Para una clave de 192 bits, el ataque se necesitara aplicar 2^{191} veces. Para una clave de 256 bits, el ataque se necesitará aplicar 2^{255} veces.

También es importante notar que a medida de que la longitud de la llave crece, cuando esta es de 56-bits es un DES y este ya ha sido vulnerado en el pasado usando fuerza bruta.

Para tomar el tiempo en el que tomaría romper AES de 128 Bits, basta con ver estos cálculos:

Las computadoras más rápidas como pudieran ser las de Wikipedia procesan 10.51 Pentaflops = ($10.51x10^{15}$) (Punto flotante de operación por

segundo). Ahora bien, el número de flops que se necesitan (aproximadamente) por combinación son 1000 Flops. El número de validaciones por segundo son = $(10.51x10^{15})/1000 = (10.51x10^{12})$.

Por otro lado el número de segundos en un año son: 365 x 24 x 60 x 60 = 31, 536,000 segundos.

Ahora el número de años para romper o vulnerar con una llave de 128-Bit es: $(3.4x10^{38})$ / $((10.51x10^{12})$ x31, 536,000) = $(0.323x10^{26})$ / 31, 536,000 = 1.02 x 10^{18} = 1, 000, 000,000 millones de años.

Como puede verse, aún con una súper computadora actual tomaría esa cantidad de tiempo, que para poner un punto de comparación es más de la edad que tiene el universo actualmente [17].

Ataques a AES

El primer ataque, Nicolas Courtis y Jose Pieprzyk han demostrado que el algoritmo puede escribirse como un sistema de ecuaciones cuadráticas multi-variables. Este hecho permitirá definir un sistema de ecuaciones lineales con un gran número de variables cuadráticas que hay que resolver. Su teoría indica que podría romperse un Rijndael de 128 bits recuperando la clave secreta. Para esto solo se necesitara un bloque de texto en claro y con una representación del algoritmo con más de 8000 ecuaciones cuadráticas con 1600 incógnitas binarias. Teniendo en cuenta estas propiedades, han surgido un nuevo tipo de ataques denominados ataques XSL. Ataques que al menos en teoría, pueden ser aplicados a cualquier tipo de cifrado [18].

El segundo ataque por otro lado fue hecho por Fuller y Millan, que mostraban un documento demostrando que la S-BOX de 8x8 bit de AES era en una realidad una caja –S de 8x1 bit, demostrando que solo hay una parte de no-linealidad en el cifrado.

Un tercer ataque se dio en 2002, Murply y Robshaw, publicaron un resultado que pertenecía expresar a todo AES en un solo campo. Incluso presentaron un cifrado llamado BES que trata cada byte de AES como un vector de 8 bytes. BES opera sobre bloques de 128 bytes para un subconjunto especial de textos en claro y claves. BES es igual en forma que AES. Este método tiene varias propiedades interesantes, proporcionando al método XSL, siendo este una representación un poco más concisa [19].

Aplicando todo este algoritmo, este ataque adquiere una complejidad de 2^{100} contra AES, lo cual es un avance importante.

REFERENCIAS

[1] R. S. Kevin Fall, TCP/IP Illustrated, Volume 1: The Protocols, 2011.

[2] J. Madrid, «Universidad ICESI,» 2004. [En línea]. Available: http://www.icesi.edu.co/revistas/index.php/sistemas_telematica/article/view/934/959.

[3] Britannica, «http://www.britannica.com/,» 2014. [En línea]. Available: http://www.britannica.com/EBchecked/topic/410357/protocol.

[4] IEEE, «www.ieeeghn.org,» 2013. [En línea]. Available: http://www.ieeeghn.org/wiki/index.php/Wireless_LAN_802.11_Wi-Fi.

[5] PCMagazine, «www.pcmagazine.com,» 2014. [En línea]. Available: http://www.pcmag.com/encyclopedia/term/37204/802-11.

[6] J. Ross, «Introducion to Wireless Networks,» 2008. [En línea]. Available: http://cdn.ttgtmedia.com/searchNetworking/downloads/wireless_sample.pdf.

[7] R. Vásquez, «AnexoFG-Marcomun,» 2011. [En línea]. Available: http://www.scribd.com/doc/53039259/AnexoFG-Marcomun.

[8] J. Grim, «http://www.informit.com/,» 2000. [En línea]. Available: http://www.informit.com/articles/article.aspx?p=19825&seqNum=5.

[9] S. Barajas, «http://www.saulo.net/,» 2004. [En línea]. Available: http://www.saulo.net/pub/inv/SegWiFi-art.htm.

[10] Informatica Hoy, «Informatica Hoy,» 2010. [En línea]. Available: http://www.informatica-hoy.com.ar/redes-inalambricas-wifi/Vulnerabilidades-de-las-redes-WIFI.php.

[11] C. Nachreiner, «Watchguard,» 2011. [En línea]. Available: http://www.watchguard.com/infocenter/editorial/135324.asp.

[12] E. Cárdenas, «Giac,» 2013. [En línea]. Available: http://www.giac.org/paper/gsec/3199/mac-spoofing-an-introduction/105315.

[13] Pervasive Technology Labs at Indiana University, «archive.org/,» 2009. [En línea]. Available: http://web.archive.org/web/20100914222536/http://anml.iu.edu/ddos/types.html.

[14] Instituto Nacional de Tecnologias de Comunicacion., Riesgos de las Redes Inalámbricas, 2009.

[15] A. Pazmiño, «Aplicación de Hacking Ético para la Determinación de Vulnerabilidades de Acceso a Redes Inalámbricas».

[16] A. Pazmiño, *Aplicación de Hacking Etick para la Determinacion de Vulnerabilidades de Acceso a Redes Inalámbricas*, 2011.

[17] M. Arora, «http://www.eetimes.com/,» 2012. [En línea]. Available: http://www.eetimes.com/document.asp?doc_id=1279619.

[18] A. Pousa, «postgrado.info.unlp.edu.ar/,» 2011. [En línea]. Available: http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Pousa_Adrian.pdf.

[19] C. Nachreiner, «http://www.watchguard.com/,» [En línea]. Available: http://www.watchguard.com/infocenter/editorial/135324.asp.