Universitat Oberta de Catalunya

uoc.edu

Redes WiFi: ¿realmente se pueden proteger?

Encarna Pau García
Máster Interuniversitario en Seguridad de las TIC (UOC-UAB-URV)
Seguridad en el Internet de las cosas

Helena Rifà Pous
Jorge chinea López

Junio de 2019

Licencias alternativas (elegir alguna de las siguientes y sustituir la de la página anterior)

A) Creative Commons:

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento 3.0 España de Creative Commons

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Redes WiFi:¿realmente se pueden proteger?*
Nombre del autor:	*Encarna Pau García*
Nombre del consultor/a:	*Jorge Chinea*
Nombre del PRA:	*Helena Rifà*
Fecha de entrega (mm/aaaa):	04/06/19
Titulación::	*Máster Universitario en seguridad de las TIC*
Área del Trabajo Final:	*El Internet de las cosas*
Idioma del trabajo:	*Castellano*
Palabras clave	*Seguridad, WiFi, Protección*

Resumen del Trabajo

Las redes WiFi, hoy en día, se han convertido en una herramienta imprescindible para la gran mayoría de procesos que se usan en la vida cotidiana, tanto a nivel privado como empresarial.

Es por ello que los cibercriminales tienen como objetivo atacarlas para obtener todo tipo de datos, personales y económicos, incluso delinquir mediante usurpación de identidad.

De ahí surge la necesidad de preguntarse si las redes WiFi realmente se pueden proteger.

Con este trabajo se pretende estudiar el entorno WiFi y analizar si nuestras redes están bien protegidas y son altamente seguras.

Se analizan los diferentes mecanismos de protección WiFi tales como WPE/ WPA/ WPA2 y sus correspondientes ataques por los que se demuestra que tan vulnerables son. Además también se analiza el nuevo estándar WPA3 con las mejoras sobre su predecesor.

De este estudio se llega a la conclusión que la existencia de métodos de protección hacen securizar nuestras redes, hasta que se descubren vulnerabilidades que obligan a

encontrar nuevos mecanismos de robustez.

Abstract

Nowadays, the Wifi Networks, have become an essential tool for the majority of processes that are used in everyday of our life, both on a personal and business areas.

Because of that, cybercriminals aim to attack them to obtain all kinds of data, private and economic, including committing a illegal actions though identity theft.

Hence the need to ask whether WiFi networks can really be protected.

This Work aims to study the WiFi environment and analyze if the networks are well protected and highly secure.

The different WiFi Protection mechanisms such as WPE/ WPA /WPA2 and their corresponding attacks are analyzed by demonstrating how vulnerable they are. In addition, the new WPA3 standard is also analyzed with the improvements over its predecessor.

This study concludes that the existence of protection methods make our networks secure, until vulnerabilities are discovered that force us to find new mechanisms of robustness.

ÍNDICE

1. Introducción

1.1 Contexto y justificación del Trabajo

La finalidad de este Trabajo es el análisis de la tecnología WiFi en general, centrándome en el ámbito industrial en particular.

La necesidad de focalizar el trabajo en esta área es debido en gran parte a la actual revolución industrial que estamos viviendo de forma acelerada –Industria 4.0- la cual conecta millones de dispositivos entre sí –IoT, Internet of Things- y que lo hace mediante alguna de las tecnologías inalámbricas existentes, en su gran mayoría a través de redes WiFi.
Es por ello que surge la necesidad de analizar los diferentes mecanismos de Seguridad para poder securizar al máximo la red WiFi.

1.2 Objetivos del Trabajo

- Estudiar los conceptos básicos, tipología y funcionalidad de la tecnología WiFi (qué es y cómo funciona)
- Analizar los diferentes mecanismos de seguridad existentes aplicables en entornos domésticos, públicos e industriales. (Autenticación y cifrado)
- Analizar también las vulnerabilidades y ataques existentes en este tipo de redes inalámbricas.
- Indagar sobre dispositivos del ámbito industrial que trabajan mediante red WiFi –PLCs, *gadgets* IoT-
- Comprobar qué diferentes tecnologías inalámbricas existen paralelas a las redes WiFi

1.3 Enfoque y método seguido

El enfoque que se le dará a este trabajo será de investigación y análisis teórico de la materia, aplicando paralelamente el know-how adquirido en laboratorio de test dentro de un entorno doméstico e industrial, y así poder dar solución al título del mismo: ***Redes WiFi: ¿Realmente se pueden proteger?***

1.4 Planificación del Trabajo

El trabajo se planifica teniendo en cuenta la dedicación a la búsqueda de información, a la realización de pruebas físicas en entorno de test dentro de un entorno industrial y también a la elaboración de la memoria.

Para la realización de este trabajo se utilizará un ordenador personal con Windows 7, Microsoft Word y aquellos softwares necesarios para llevar a cabo el análisis de seguridad en la red WiFi -éstos siempre con licenciamiento vigente u openSource-, además de diferentes entornos físicos de test tanto domésticos como industriales –Routers, Access Points WiFi, dispositivos inalámbricos industriales-

El trabajo se distribuirá en diferentes fases:

- Fase 1: Planificación del Proyecto
- Fase 2: Investigación y documentación teórica del tema que atañe a este trabajo
- Fase 3: Comprobación y aplicación práctica del conocimiento adquirido en entornos de test.
- Fase 4: Obtener conclusiones
- Fase 5: Exposición visual de la memoria

1.5 Breve sumario de productos obtenidos

La finalidad de este trabajo es investigar, de forma teórica, si las redes WiFi son seguras, estudiando y aplicando técnicas prácticas en entorno de test para abordar el análisis de campo. Por lo tanto no se desarrollará ningún producto físico.

1.6 Breve descripción de los otros capítulos de la memoria

El trabajo se distribuirá de la siguiente manera:

1. Introducción (objetivos, enfoque y planificación del proyecto)
2. Las redes inalámbricas: conceptos básicos
3. Redes WiFi
4. Mecanismos de Seguridad WiFi
5. Vulnerabilidades y Ataques en redes WiFi
6. La red WiFi en entornos domésticos, públicos e industriales
7. Cómo securizar al máximo nuestra red WiFi *(caso práctico)*
8. Conclusiones
9. Bibliografía

1.7 Pequeña revisión del estado del arte

Durante la elaboración del este trabajo, se pretende investigar sobre la tecnología WiFi y su seguridad. Pero hay que ser conscientes que es un paradigma muy efímero, con lo que en este periodo de estudio puede aparecer algún protocolo o vulnerabilidad nueva, y se deberá tener en cuenta.

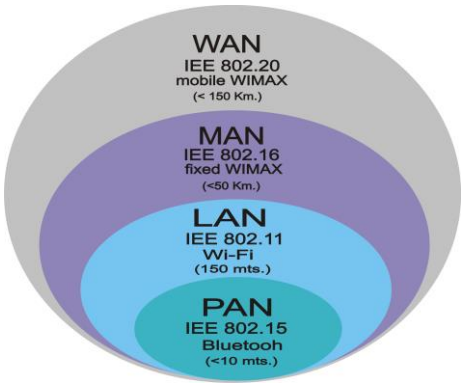
En la parte motivacional, se dedicará más esfuerzo a la investigación en entornos industriales, debido a qué es una revolución que estamos viviendo hoy en día, y en la que muchos sectores industriales no han parado a pensar en qué hay más allá de colocar sensórica o PLCs en sus plantas de producción. Se trata pues de securizar esos dispositivos para evitar posibles ataques externos.

2. Las redes inalámbricas: conceptos básicos

Las redes inalámbricas son todas aquellas conexiones entre nodos que se dan por medio de ondas electromagnéticas, sin necesitar ningún tipo de cableado.

Las redes inalámbricas se pueden clasificar según su cobertura:

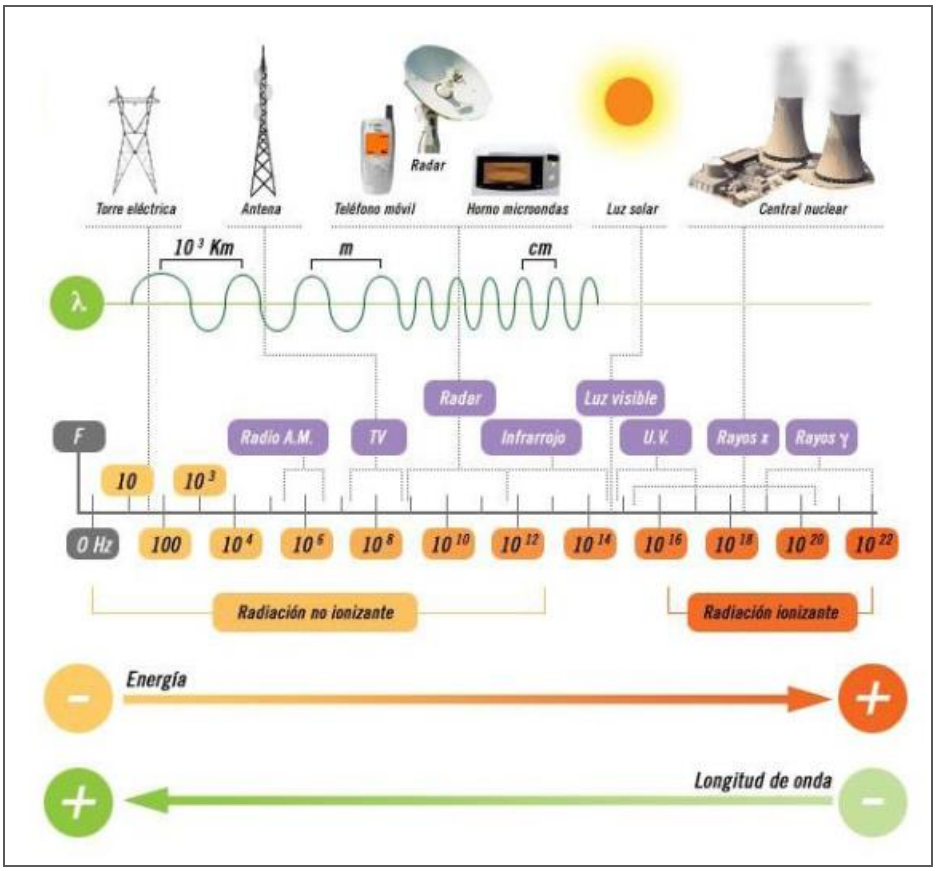
- WPAN: Wireless Personal Area Network
- WLAN: Wireless Local Area Network
- WMAN: Wireless Metropolitan Area Network
- WWAN: Wireless Wide Area Network



[1]. Clasificación redes WiFi según cobertura

Y según el rango de frecuencias en las que operan:

- *Microondas terrestres*, las cuales utilizan antenas parabólicas para enviar y recibir la señal entre emisor y receptor.
- *Ondas de radio*, son ondas electromagnéticas que se propagan a través del espacio transportando energía de forma omnidireccional, sin necesidad de antenas parabólicas.
- *Microondas por satélite*, las cuales se hacen enlaces entre dos o más estaciones terrestres que se denominan estaciones base. El satélite recibe la señal en una banda de frecuencia, la amplifica y la retransmite en otra banda.
- *Infrarrojos*: se enlazan transmisores y receptores que modulan la luz infrarroja.



[2]. Frecuencias espectro WiFi

Para que una red inalámbrica se considere segura debería cumplir con los siguientes puntos:

- Las ondas de radio deben limitarse tanto como sea posible con la ayuda de antenas direccionales.
- Debe existir algún mecanismo de autenticación de doble vía que permita al cliente verificar que se está conectando a la red correcta, y a la red que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el medio aéreo para evitar captura de datos de equipos no autorizados a hacerlo.

Este trabajo de final de máster se centrará, tal y como indica el título del proyecto, en la seguridad de redes WiFi.

3. Redes WiFi

3.1 Breve Historia: WiFi Alliance

Las redes WiFi son un tipo de red inalámbrica que aparecieron a principios de los años 90, para conectar dispositivos electrónicos entre sí sin necesidad de cableado.

La entrada de esta tecnología fue un tanto desordenada ya que cada fabricante desarrollaba sus propios modelos generando dificultades entre ellos, y para evitar este desorden, se creó unos años más tarde una asociación entre varias compañías del sector de las telecomunicaciones llamada **WECA (Wireless Ethernet Compatibility),** la cual en el año 2003 pasó a ser la actual **Wi-Fi Alliance**.

Sus objetivos fueron el del fomento de la tecnología WiFi y establecer estándares para que los equipos que utilizan esta tecnología sean compatibles entre sí.

[3]. WiFi Alliance Logo.

3.2 Frecuencias, canales y estándares de la tecnología WiFi

El entorno WiFi al tratarse de ondas de radio convive con el resto de ondas que se propagan por el medio aéreo. Éstas, operan dentro de las frecuencias 2,4 GHz y 5GHz.

Actualmente los estándares asignados y certificados por la ***WiFi Alliance*** son el IEEE 802.11b,g,n para interfaces WiFi que operan en la frecuencia de los 2,4GHz y el IEEE 802.11A para los que operan en la frecuencia de los 5GHz.
Dependerá de la velocidad y del alcance operar en una frecuencia o en otra. A mayor frecuencia menor alcance.

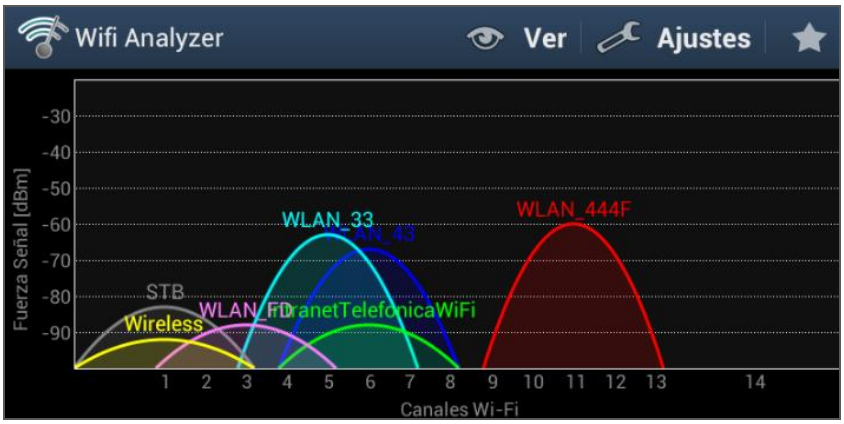
Norma 802.11			
Estándar	Frecuencia	Velocidad (En Megabits)	Alcance (Metros en lugar cerrado)
A	5.86 GHz	54 Mbs	45
B	2.4 GHz	11 Mbs	91
G		54 Mbs	91
N		600 Mbs	70

[4]. Frecuencias espectro WiFi.

Se espera durante el año 2019 que haga aparición un nuevo estándar, el IEEE 802.11AX, operando en frecuencias que van desde 1GHz hasta los 7GHz.

El hecho de que todos los dispositivos trabajen dentro de estas dos frecuencias hace que en entornos muy masificados se puedan experimentar interferencias. Es por ello que existen diferentes canales para que los espectros no se solapen unos con otros.

A continuación se muestra captura de pantalla del software WiFi Analyzer donde se escanea y analiza todo el espectro WiFi de un área, representando la potencia de cada red y en qué canales operan cada uno.
De esta forma se minimizan las interferencias entre conexiones.



[5]. Representación gráfica Wifi Analyzer.

3.4 Topología de la red WiFi

Según el estándar IEEE 802.11, las redes inalámbricas Wifi contemplan tres topologías distintas:

- Modo infraestructura BSS (Basic Service Set)

  Este tipo de infraestructura se caracteriza por disponer, además de tarjeta Wifi en el dispositivo, de un Punto de acceso en el que los usuarios se registran en la red mediante él.

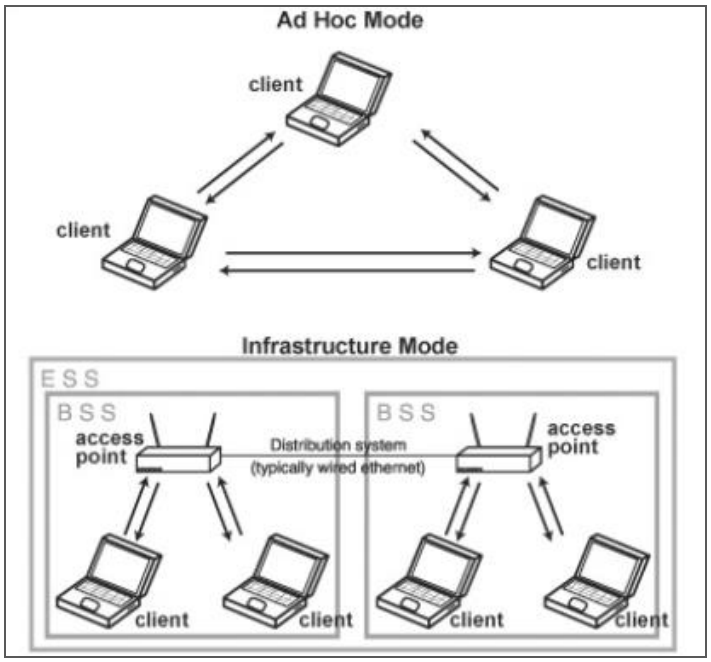
- Modo Ad-Hoc IBSS (Independent Basic Service Set)

  Esta segunda topología conecta dispositivos entre sí sin necesidad de disponer de un Punto de acceso intermedio.

  Los equipos pueden realizar la conexión directamente desde sus tarjetas inalámbricas.

- Modo infraestructura ESS (Extended Service Set)

  Esta topología sigue la misma estructura que la tipo BSS pero utiliza varios puntos de acceso, formando una WLAN. Los usuarios pueden conectarse a varios de ellos para acceder a la red.



[6]. Topología de Redes WiFi.

4. Métodos de Autenticación y Cifrado

Tal y como se ha enumerado en capítulos anteriores, para que una comunicación inalámbrica tenga un nivel alto de seguridad deben existir ciertos mecanismos de seguridad garantizando el control de acceso, autenticación, disponibilidad, confidencialidad e integridad de la información.

A continuación se muestran diferentes métodos de Autenticación y Cifrado, los cuales evitan que personas no autorizadas accedan a la información cuando ésta se transmite de forma inalámbrica, añadiendo complejidad a las contraseñas para que éstas sean más complicadas de descifrar.

Los protocolos de cifrado existentes son:

4.1 WEP (Wired Equivalent Privacy) 1999

El objetivo de este protocolo fue el de proteger la confidencialidad de los usuarios de escuchas no autorizadas, mediante la aplicación de 3 propiedades: *Confidencialidad, autenticación y control de acceso.*

En sus inicio usaba 64bits para cifrar sus contraseñas y más tarde aumentó a 128bits, pero rápidamente se descubrieron fallos de seguridad que hacían que ésta se pudiera romper en cuestión de minutos.

En la actualidad no se recomienda su uso debido a que es altamente vulnerable.

WEP proporciona dos tipos de autenticación:

Open System, el cual deja autenticarse a todos los usuarios en el punto de acceso.

Y ***Shared Key***, la cual trabaja requiriendo al usuario que envíe un mensaje al punto de acceso solicitando la conexión. Éste le contesta con un reto, el cual debe ser cifrado por el usuario y reenviado nuevamente al punto de acceso.

Finalmente, si el punto de acceso es capaz de descifrarlo, se valida la autenticación.

Respecto a la confidencialidad, WEP utiliza la misma clave secreta para usuario y punto de acceso, y el estándar no especifica ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de la red. Esto provoca que la clave esté almacenada en todos los dispositivos, aumentando las posibilidades de visibilidad frente a un atacante. Además la distribución manual de claves provoca un aumento de mantenimiento y gestión para los administradores de la red, con lo que la clave no es cambiada con frecuencia.

Funcionamiento de cifrado del sistema WEP.

El algoritmo de cifrado utilizado es RC4 con claves (seed), según el estándar, de 64 bits.

Estos 64bits están formados por 24 bits correspondientes al ***IV - vector de inicialización***- más 40 bits de la clave secreta.

Los 40 bits se deben distribuir manualmente, en cambio el IV es generado dinámicamente y debería ser diferente para cada trama.

Así, el objetivo con el IV es cifrar con claves diferentes para impedir que un atacante pueda capturar suficiente tráfico cifrado con la misma clave.

Fases del algoritmo de cifrado de WEP

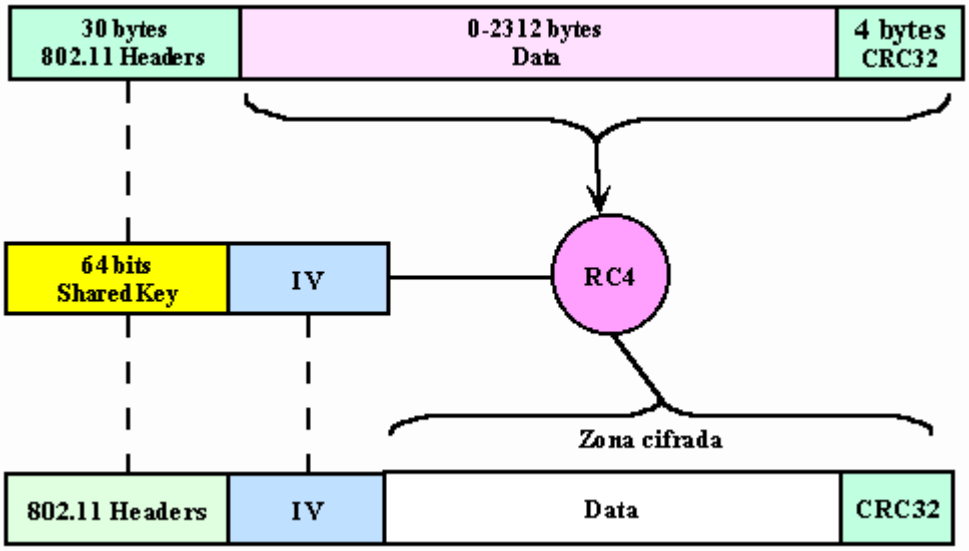
Fase 1.Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (***ICV*** -***Integrity Check Value***-

Fase 2. Se concatena la clave secreta a continuación del IV formando el seed

Fase 3.***El PRNG*** -***Pseudo-Random Number Generator***- de RC4 genera una secuencia de caracteres pseudo-aleatorios (***Keystream***) a partir del *seed*, con la misma longitud que los bits obtenidos en la fase.

Fase 4. Se calcula la XOR de los caracteres de la fase 1 con la del 3. Y el resultado es el mensaje cifrado.

Fase 5. Por último se envía el IV sin cifrar y el mensaje cifrado dentro del campo de datos (frame body) de la trama.



[7]. Algoritmo de Cifrado WEP

4.2 WPA (WiFi Protected Acces) 2003 y WPA2 2004

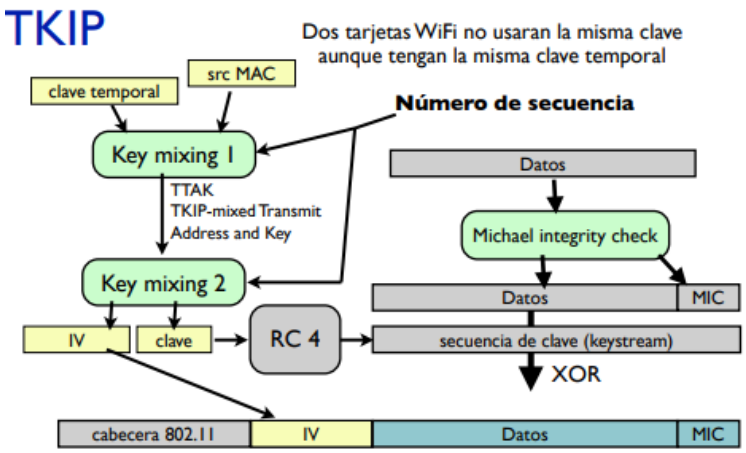
Este cifrado surgió de la necesidad de encontrar una nueva seguridad al cifrado WEP.

Su actualización fue rápida y fácil para proveedores y usuarios de con cifrado WEP, ya que bastaba con una simple actualización del firmware del dispositivo.

Sus principales características son:

.-Mejor Cifrado e integridad de los datos, ya que utiliza una distribución dinámica de claves de duración limitada, llamada ***TKIP***, usando un algoritmo de cifrado de 256bits, y aunque continua empleando RC4, lo hace sin compartir la clave entre todos los clientes,

TKIP implementa una clave por paquete, lo que hace que se genere una nueva clave de 128 bits por cada paquete, dando mayor complejidad ante un ataque.



[8]. Algoritmo de Cifrado TKIP.

También, utiliza técnicas de integridad y autenticación como ***MIC,*** acrónimo de Message Integrity Check.

Se trata de un MIC de 64 bits que sirve para proporcionar integridad a todo el sistema.

.-El vector de iniciación (IV) es más robusto que en el protocolo WEP, siendo éste de 48 bits y minimizando la reutilización de claves.

.- Mayor Autenticación del estándar 802.1X, controlando el acceso por puerto y permitiendo únicamente el tráfico EAP hasta la autenticación.

Este protocolo aporta frente a su antecesor WEP dos sistemas diferenciables según su escenario:

.- WPA Personal: utilizando una clave Pre-Shared Key

.- WPA Enterprise: WPA + RADIUS (802.1x), el cual se explica en el apartado 4.6.

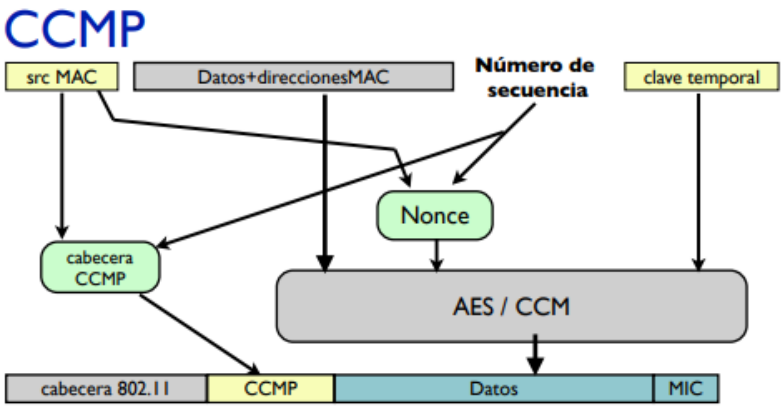
En breve, surgió la necesidad de avanzar un paso más en el cifrado del protolo, y es entonces cuando se estandariza WPA2.

La diferencia entre ambos cifrados (WPA y WPA2) es la sustitución del algoritmo de cifrado TKIP con RCA4 por AES, usando el protocolo ***CCMP***.

Éste está completamente rediseñado para nuevo Hardware y basado, como ya se ha mencionado, en ***AES*** (Advanced Encryption Standard)

AES es un “cifrador” de bloque de clave secreta, el cual cifra bloques de 128bits con una clave de 128 bits, y utiliza un modo de funcionamiento llamado Counter CRT, con código de autenticidad de mensaje (integridad) mediante Cipher Block Chaining.

Con lo que AES proporciona un cifrado capaz de generar códigos de integridad.



[10]. algoritmo de Cifrado CCMP en WPA2.

4.3 WPA3 (WiFi Protected Acces) 2018

De igual forma que con WEP, WPA y WPA2, surge la necesidad de estandarizar un nuevo protocolo de seguridad para evitar las vulnerabilidades descubiertas, en este caso en WPA2, denominado WPA3.

Las diferencias más notables de este cifrado frente al predecesor son las siguientes:

WPA3 pasa de usar una clave de 128bits a una de 192bits, añadiéndole mayor seguridad.

Otra novedad aportada por este cifrado es que WPA3 trabaja con ***Wi-Fi Easy connect.***

Se trata de un nuevo modo de configurar y conectar a la red dispositivos que no gozan de una pantalla o no botones físicos, como es el caso de los dispositivos IoT (Internet of things).
La forma de conectarse de estos dispositivos a la red WiFi se realiza mediante la lectura de un código QR.

y por último la incorporación de una nueva tecnología llamada ***Forward Secrecy***. Dicha tecnología cerraría el paso a los piratas informáticos si consiguiesen acceder a la conexión consiguiendo la clave del router.
Una vez que el atacante cambia la contraseña del router, no logrará acceder a la información registrada con fecha anterior al cambio del password.

	WEP	**WPA**	**WPA2**	**WPA3**
Año salida	1997	2003	2004	2018
Cifrado	RC4	TKIP con RC4	AES-CCMP	AES-CCMP y AES-GCMP
Tamaño de clave	64 y 128 bits	128 bits	128 bits	128 y 256 bits
Tipo de cifrado	Flujo	Flujo	Bloque	Bloque
Autenticación	Sistema abierto y clave compartida	Clave precompartida (PSK) y 802.1x con variante EAP	Clave precompartida (PSK) y 802.1x con variante EAP	Simultaneous Authentication of Equals (SAE) y 802.x con variante EAP

[11]. Protocolos de Autenticación y Cifrado WiFi

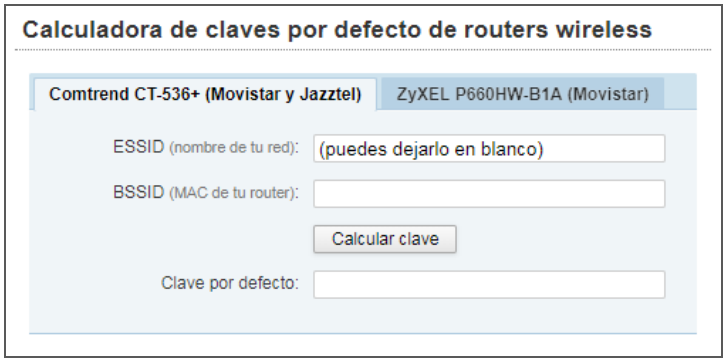
5. Mecanismos de Seguridad WiFi

5.1 Ocultación de la red WiFi

Nuestra red WiFi tiene un **SSID (service Set Identifier)** o nombre de red para identificarla. En cada punto de acceso o Router se puede decidir propagar el nombre de la red y hacerla visible, u ocultarla para que cualquier atacante no pueda penetrar a ella si no la conoce.

En los Routers domésticos, es muy aconsejable cambiar el SSID y contraseña que viene definido de fábrica ya que muchos de ellos están almacenados en bases de datos que se pueden encontrar por internet con gran facilidad.
Además el SSID y contraseña de estos dispositivos en algunos proveedores de internet (ISP) están asociados a su dirección MAC, por lo que un atacante puede tardar pocos minutos en descifrarla conociendo las siguientes premisas:
.-La contraseña por defecto está basada en que la primera letra se corresponde con la identificación del fabricante del Router.
.-El resto de caracteres proceden del principio de la dirección MAC y los dos últimos de sus últimos dos dígitos.
.-Por último, los 4 números restantes se generan al azar, así que con un ataque por diccionario se descifra en pocos minutos.

En internet se pueden encontrar páginas web dedicadas a resolver la contraseña por defecto indicando la MAC del Router.



[12]. Calculadora de claves por defecto en Routers

5.2 Filtrado de direcciones MAC

Con este mecanismo se añade una capa de seguridad a la red, ya que permite restringir el acceso a los recursos de la red mediante la dirección MAC de los dispositivos.

Se puede definir mediante dos políticas de acceso.

Listas blancas: Son las que mayor seguridad ofrecen, ya que en ellas se recogen una serie de direcciones MAC que serán las únicas que estarán autorizadas para conectarse a nuestra red WiFi.

Listas negras: En este tipo de listas también se tiene una recopilación de direcciones MAC, pero éstas no pertenecen a los dispositivos autorizados sino a aquellos no autorizados para conectarse a nuestra red WiFi.

5.3 Servicio WPS

WPS es el acrónimo de **Wifi Protected Setup** y se trata de un estándar promovido por la WiFi Alliance para hacer más sencilla la creación de una red WiFi segura para usuarios domésticos o de oficinas en el hogar.

Ésta define los mecanismos a través de los cuales los dispositivos de red obtienen las credenciales de acceso a la red mediante un PIN aleatorio para cada usuario, siendo éste fácilmente descifrable.

Motivo por el cual es aconsejable deshabilitar esta función.

[13]. Redes WiFi con WPS activo

5.4 Conexión a través de VPN

VPN es el acrónimo de **Virtual Private Network** y se caracteriza por ser una tecnología de red que permite conectar uno o más ordenadores en una red privada virtual, a través de una red pública como lo es internet, y sin la necesidad de que los dispositivos estén conectados físicamente entre sí.

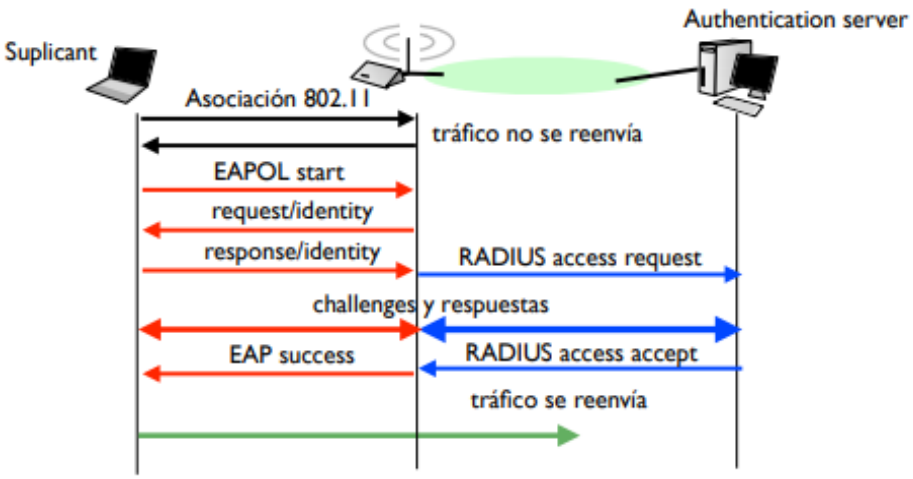
Los datos dentro de este "túnel virtual" viajan completamente cifrados y los usuarios además deben acceder mediante usuario y contraseña, por lo que a un posible atacante se le haría muy difícil tarea conseguir acceder.

5.5 Servidor RADIUS

El término **Radius** corresponde a **Remote Access Dial in User Service**, y se trata de un protocolo destinado a ofrecer seguridad en las comunicaciones WiFi ofreciendo un mecanismo de autenticación de usuarios para acceder a la red.

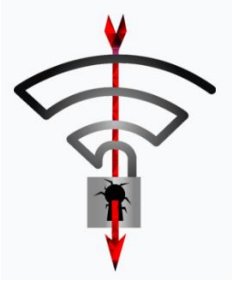
Este tipo de protocolo trabaja con arquitectura Cliente-Servidor. Es decir, que el usuario con unas credenciales de acceso a la red se conecta contra el servidor RADIUS, y éste es el encargado de verificar la autenticidad de la información.

[14]. Servidor RADIUS



[15]. Autenticación RADIUS.

6. Vulnerabilidades y Ataques en redes WiFi



6.1 Vulnerabilidades WEP

El protocolo WEP, es en la actualidad, el más vulnerable y motivo por el cual la mayoría de fabricantes de Routers ya no lo incluyen en sus dispositivos.
Esta afirmación es gracias a que en Julio de 2001, los criptógrafos *Scott Fluhrer*, *Itsik Mantin* y *Adi Shamir* describieron una vulnerabilidad en el algoritmo de cifrado RC4, donde se puede recuperar la clave empleada si la inicialización del algoritmo cumple determinadas premisas, muy comunes, y se interceptan el suficiente número de mensajes.

Esta vulnerabilidad la descubrieron realizando dos tipos de ataques sobre RC4.

El primero de ellos está basado en patrones invariante, donde existen patrones, que de existir la clave, se propagan también al estado interno del algoritmo, debilitándolo considerablemente.
El resultado es que los primeros bytes generados por RC4 pueden ser muy predecibles.

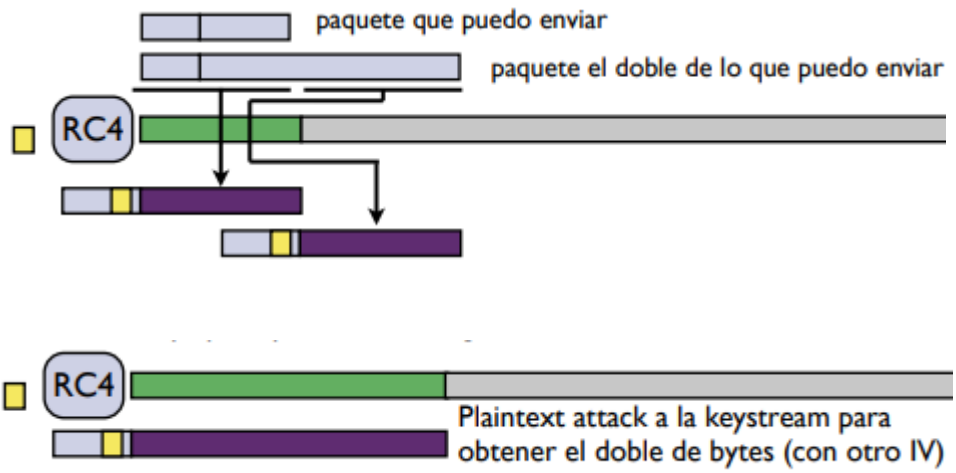
El segundo ataque describe la recuperación de la clave secreta, cuando la clave del algoritmo se deriva de la concatenación de dicha clave secreta y del vector inicial público y conocido.

Otra vulnerabilidad no menos importante y que también reside en el algoritmo RC4, es la que permite reducir la longitud efectiva del cifrado a 24bits, en lugar de los 128 bits que forma este tipo de cifrado.

También cabe destacar la facilidad de inyección de tramas por parte de un atacante, ya que este protocolo no dispone de ningún sistema para detectar tramas duplicadas.

6.1.1 Ataque de Fragmentación

El objetivo de este ataque es generar un archivo XOR, el cual necesita la captura de un paquete de datos como mínimo para ser iniciado.
Paulatinamente se extrae la información del paquete acerca del PRGA, para luego validarlo reenviando al Punto de acceso WiFi un paquete ARP o también paquetes LLC. Si la respuesta obtenida es válida, se añade más información y el ataque continúa.
Esta operativa se repite tantas veces hasta llegar a los 1500 bits del PRGA.



[16]. Ataque de Fragmentación

6.1.2 Ataque CHOPCHOP

El ataque CHOPCHOP es un ataque al protocolo WEP aparecido en el año 2004, mediante el cual se puede conocer el contenido de un paquete cifrado, capturado de una red WEP, descifrándolo byte a byte por la cola.

Cada byte es probado por fuerza bruta, generándose cada vez, tras una serie de pasos, un paquete nuevo es enviado al punto de acceso, y éste determina si el paquete posee un checksum válido. En caso afirmativo, el byte probado corresponde al byte concreto.

6.2 Vulnerabilidades WPA/WPA2

Tal y como se ha comentado anteriormente en este trabajo, el protocolo WPA surge de la necesidad de contrarrestar la falta de seguridad que presenta el protocolo WEP, y más tarde aparece WPA2 para añadir un step más de seguridad a WPA. Aun así este protocolo también se ha visto vulnerado, siendo sus principales problemas de seguridad la Inyección de paquetes, descifrado, y Contraseñas débiles, donde las claves compartidas o Shared Key, son totalmente vulnerables a ser hackeadas cuando éstas tienen una complejidad baja, y mediante un ataque de fuerza bruta se pueden conseguir fácilmente.

6.2.1 Ataques BECK-TEWS y OHIGAHI-MORRI

Este tipo de ataques permiten realizar inyección y descifrado de paquetes cuando se utiliza el protocolo WPA juntamente con el cifrado TKIP.

WPS o WiFi Protected Setup: Los fallos de seguridad permiten al atacante descubrir el PIN WPS para luego obtener la clave WPA/WPA2.

Gestión de reinstalación clave de Hadshake de 4 vías. Debido a que el protocolo WPA no especifica cómo debe ser la gestión de la clave secreta durante el proceso de Handshake de 4 vías de WPA, se ha estado implementando de forma no segura por los fabricantes, y mediante el ataque de tipo KRACK se puede vulnerar la comunicación.

6.2.2 Ataque KRACK

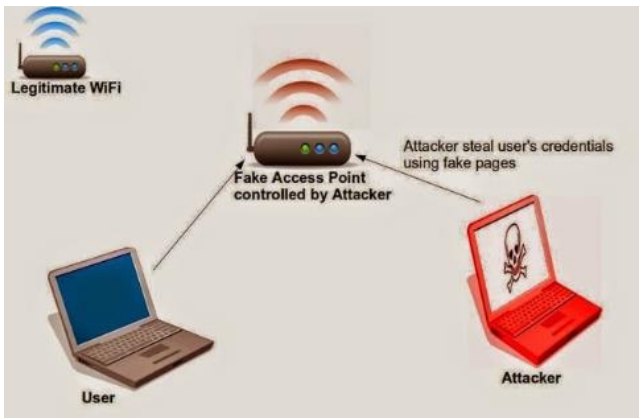
El ataque de tipo KRACK, (de sus siglas Key Reinstallation Attacks), es la combinación de 10 vulnerabilidades encontradas en los dos agentes integrantes, 1 en el Punto de acceso y 9 en el cliente.

Por este motivo es importante que el cliente esté actualizado con los últimos parches de seguridad que permitan evitar este tipo de ataques.

6.2.3 Ataque Evil Twin (Linset)

Este tipo de atacante consiste en crear un punto de acceso falso, copiando el SSID original. La víctima a continuación detecta 2 puntos de acceso con el mismo nombre, pero no es capaz de diferenciarlos, con lo que se conectará al que le quede más próximo.

Una vez conectada la víctima a este falso punto de acceso, se le dirige a una página web falsa en la que se le pide la contraseña WPA/WPA2. En ese momento el atacante consigue las credenciales de acceso



[17]. Ataque Evil-Twin.

6.2.4 Vulnerabilidad servidor RADIUS

Como se ha comentado anteriormente, Radius ofrece una capa adicional de seguridad a las comunicaciones de entorno empresarial, pero incluso pudo ser vulnerada. Se trata de la vulnerabilidad registrada con el código CVE-2017-9148 mediante la cual un atacante puede conectarse a una red sin autorización a través de los protocolos PEAP o TTLS, los cuales omiten la autenticación cada vez que se retoma una conexión TLS. Esto ocasiona una brecha de seguridad muy grave, ya que ningún servidor debe retomar una conexión que previamente se ha finalizado con éxito.

Para evitar esta vulnerabilidad basta con actualizar a la versión 3.0.14 de FreeRADIUS la cual evita el ataque.

6.2.5 Ataque a WPS

Este tipo de ataques se realizan contra puntos de acceso o routers que tienen esta funcionalidad activa, y consiste en el uso de la fuerza bruta para romper la clave numérica de 8 dígitos que WPS proporciona

7. La red WiFi en entornos industriales

Los entornos industriales también gozan, cada vez más, de tecnologías inalámbricas para sus procesos y sistemas, con el fin de tener un despliegue rápido de la infraestructura sin necesidad de cablear, o poder dar cobertura donde éste no puede llegar.

Motivo por el cual hace que este entorno sea más vulnerable si no se aplican unas buenas medidas de seguridad que lo proteja frente a amenazas externas como internas.

No obstante, esto tiene una contrapartida que es la velocidad de la transmisión de los datos.

Las tecnologías inalámbricas tienen mayor latencia que el cableado físico, con lo que en según qué situaciones donde se prima la transmisión de datos a tiempo real pueden no ser adecuadas. En este caso siguen primando las conexiones tipo Profibus/Profinet.

Cabe destacar la ya conocida Revolución 4.0 y el internet de las cosas (IoT), donde se emplean dispositivos y sensórica inalámbrica que ya no trabajan mediante cableado, y deben trabajar mediante redes inalámbricas.

Las más comunes en el mundo industrial son las siguientes, siendo la conexión WiFi la más frecuente.

- WiFi IEEE 802.11
- RFID
- Bluetooth IEEE 802.15-1
- ZigBee IEEE 802.15-4

Posición	Entorno doméstico	Entorno industrial
1	Redes móviles GSM/GPRS/UMTS	WirelessHART
2	Wifi	Trusted Wireless
3	BlueTooth	Zigbee
4	WiMax	Redes móviles GSM/GPRS/UMTS
5	Radiocomunicaciones	Wifi
6	Zigbee	BlueTooth
7	WirelessHART	Radiocomunicaciones
8	Trusted Wireless	WiMax

[18]. Clasificación de uso de tecnologías inalámbricas

8. Cómo securizar al máximo nuestra red WiFi

Para securizar, lo máximo posible, una red WiFi se deben tomar una serie de acciones en el momento de su configuración.

- Cambiar las credenciales de acceso del punto de acceso o Router que lleva por defecto
- Cambiar el nombre del SSID que trae el dispositivo por defecto, y ocultar la red para que la visibilidad sea algo menor. Aunque frente a un escaneo también es posible conseguir el nombre de SSIDs ocultos.
- Trabajar con cifrado WPA2, siempre que no se haya actualizado el dispositivo y se pueda trabajar con WPA3, que en ese caso sería mejor opción.
- Definir una contraseña lo más compleja posible, alternando cifras, letras mayúsculas, minúsculas, caracteres especiales y con una longitud mínima de 8 caracteres. Evitar que la contraseña contenga palabras conocidas para evitar ataques de diccionario.
- Configurar el filtrado MAC. Dependiendo de si el entorno es personal o empresarial y de su magnitud de dispositivos, se puede optar por trabajar con una política permisiva o restrictiva. Si los recursos de administración de sistemas permiten gestionar el entorno fácilmente, siempre será más segura una política restrictiva donde se denegará cualquier acceso y únicamente podrán acceder los dispositivos asignados mediante su MAC address. En el caso contrario se aceptan todas las conexiones y se deniegan las que no son autorizadas. (ROGUE)
- Si el punto de acceso o router lo permite, es aconsejable activar el Firewall interno, lo que proporciona un paso más de seguridad al entorno.
- Y si también permite activar una red virtual privada (VPN) activarla y navegar mediante ella, donde los datos quedarán cifrados e inalcanzables para un posible atacante.
- En entorno empresarial, realizar la comunicación, si no es posible aún con WPA3, mediante la combinación de WPA2-Enterprise + Servidor RADIUS.

9. Conclusiones

La premisa que resume la conclusión de este proyecto final de máster es que, ninguna red WiFi es 100% segura, pero sí puede estar lo más protegida posible.

Con esta afirmación se pretende argumentar, que todo sistema inalámbrico puede ser vulnerado, ya que los atacantes pueden emplear todo el tiempo necesario a encontrar algún fallo de seguridad que no se había contemplado durante el desarrollo de los protocolos de autenticación y cifrado.

Una vez se tiene clara esta situación, lo que se debe siempre es intentar proteger al máximo las comunicaciones para que a los atacantes, les sea lo más complicado posible, penetrar en ellas.

Durante el proyecto se ha podido ver como los diferentes protocolos de autenticación y cifrado existentes han sido todos, a la larga, vulnerados y provocando que se siga trabajando para conseguir nuevos métodos más seguros, o más difíciles de romper.
Esto da que pensar en el protocolo WPA3, catalogado en estos momentos como infranqueable. Pero, ¿hasta cuando este protocolo seguirá siendo seguro?

Por consiguiente, las mayores recomendaciones para estar lo más seguros posibles en nuestras comunicaciones WiFi son: Configurar correctamente nuestros dispositivos, como se indica en el capítulo 8, añadiendo todas las capas de seguridad existentes actualmente. Y tener alta precaución al navegar por redes WiFi abiertas en espacios públicos, ya que puede ser que esa red no sea fidedigna y la administre un pirata informático, el cual se podrá apropiar de todos nuestros datos.

Este trabajo pretendía hacer un estudio, por un lado, teórico de investigación para entender qué es la tecnología WiFi, cómo trabaja y cómo se debe proteger.
y por otro, una parte práctica para poder comprobar qué tan fácil es penetrar en una red WiFi, protegida y sin proteger. Pero esta parte no se ha podido desarrollar debido a la falta de medios para llevarla a cabo.

Se pretendía utilizar *Geminis Auditor, linset* y *AirCrack-ng* dentro de la herramienta Linux *WIFISLAX*, mediante una máquina virtual en Windows 7, la cual no es compatible con la antena WiFi propia del dispositivo. Motivo por el cual no se ha podido hacer el escaneo de redes ni el consiguiente intento de hackeo.

No obstante, se ha podido encontrar gran información en internet referente a la operativa y casos de uso de esta herramienta donde se puede observar cómo se pueden vulnerar las redes descifrando sus contraseñas.
[Ver anexo I]

10. Glosario

- AES: Advanced Encryption Standard
- AP: Acces Point
- ARP: Address Resolution Protocol
- BSS: Basic Service Set
- CCMP: Chaining Message Authentication Code Protocol
- CRC: Cyclic REdundancy Code
- EAP: Extensible Authentication Protocol
- ESS: Extended Service Set
- GHz: GigaHercios
- ICV: Integrity Chech Value
- IBSS: Independent Basic Service Set
- IEEE: Institute of Electrical and Electronics Engineers
- IoT: Internet of Things
- IV: Vector de Inicialización
- KRACK: Key Reinstallation Attacks
- MAC: Media Access Control
- PEAP: Protected Extensible Authentication Protocol
- PLC: Programmable Logic Controller
- PRGA: Pseudo Random Generation Algorithm
- PRNG: Pseudo Random-Number Generator
- RADIUS: Remote Authentication Dial-in User Service
- RFID: Radio Frecuency Identification
- RC4: Ron's Cipher 4
- SSID: Service Set Identifier
- TKIP: Temporal Key Integrity Protocol
- VPN: Virtual Private Network
- WECA: Wireless Ethernet Capability Alliance
- WEP: Wired Equivalent Privacy
- WiFi: Wireless Fidelity
- WLAN: Wireless Local Area Network

- WLAN: Wireless Local Area Network
- WMAN: Wireless Metropolitan Area Network
- WPA: WiFi Protected Access
- WPAN: Wireless Personal Area Network
- WPS: WiFi Protected Setup
- WWAN: Wireless Wide Area Network

11. Bibliografía

[1]. Clasificación redes WiFi según cobertura

https://www.todosobretusistemaoperativo.com/tipos-de-redes-de-computadoras/

[2]. Frecuencias espectro WiFi.

https://www.escuelasinwifi.org/que-es-wifi

[3]. WiFi Alliance Logo.

https://es.wikipedia.org/wiki/Wifi

[4]. Frecuencias espectro WiFi.

https://www.escuelasinwifi.org/que-es-wifi

[5]. Representación gráfica Wifi Analyzer.

https://comunidad.movistar.es/t5/Soporte-Fibra-y-ADSL/Mejorando-el-Wi-Fi/td-p/989996

[6]. Topología de Redes WiFi.

[7]. Algoritmo de Cifrado WEP

https://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml

[8]. Algoritmo de Cifrado TKIP.

https://www.tlm.unavarra.es/mod/resource/view.php?id=8629

[9]. Cifrado RADIUS.

[10]. algoritmo de Cifrado CCMP en WPA2.

https://www.tlm.unavarra.es/mod/resource/view.php?id=8629

[11]. Protocolos de Autenticación y Cifrado WiFi

[12]. Calculadora de claves por defecto en Routers

http://utilidades.gatovolador.net/wlan/

[13]. Redes WiFi con WPS activo

https://www.nobbot.com/tecnologia/mi-conexion/mejora-la-seguridad-de-tu-router-que-es-el-wps-y-como-deshabilitarlo/

[14]. Servidor RADIUS

https://www.redeszone.net/2017/06/02/servidor-radius-funciona/

[15]. Autenticación RADIUS.

https://www.tlm.unavarra.es/mod/resource/view.php?id=8629

[16]. Ataque de Fragmentación

https://www.tlm.unavarra.es/mod/resource/view.php?id=8629

[17]. Ataque Evil-Twin.

https://mundo-hackers.weebly.com/evil-twin-attack.html

[18]. Clasificación de uso de tecnologías inalámbricas

https://www.incibe-cert.es/blog/ciberseguridad-las-comunicaciones-inalambricas-entornos-industriales

❖ Enlaces web de consulta por sección

2. Las redes inalámbricas: conceptos básicos

https://www.escuelasinwifi.org/que-es-wifi

https://es.ccm.net/contents/818-redes-inalambricas

https://www.universidadviu.es/tipos-de-redes-inalambricas-mas-comunes/

https://www.todosobretusistemaoperativo.com/tipos-de-redes-de-computadoras/

3. Redes WiFi

https://comunidad.movistar.es/t5/Soporte-Fibra-y-ADSL/Mejorando-el-Wi-Fi/td-p/989996

https://telpromadrid.eu/que-banda-wifi-es-mejor/

https://techlandia.com/funciona-tecnologia-wifi-como_10752/

https://www.sciencedirect.com/topics/computer-science/basic-service-set

4. Métodos de Autenticación y Cifrado

http://utilidades.gatovolador.net/wlan/

https://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml

https://www.xataka.com/seguridad/caos-en-la-seguridad-wifi-un-repaso-a-las-vulnerabilidades-de-wep-wap-y-wap2

https://www.tlm.unavarra.es/mod/resource/view.php?id=8629

http://profesores.elo.utfsm.cl/~agv/elo323/2s14/projects/reports/YangRivera/Informe-Rivera-Yang.htm

https://www.muycomputer.com/2018/08/24/filtrado-mac-listas-blancas-negras/

https://elpais.com/tecnologia/2018/06/27/actualidad/1530095255_505748.html

https://www.nobbot.com/tecnologia/mi-conexion/mejora-la-seguridad-de-tu-router-que-es-el-wps-y-como-deshabilitarlo/

https://www.redeszone.net/2017/06/02/servidor-radius-funciona/

5. Mecanismos de Seguridad WiFi

http://wiki.elhacker.net/seguridad-wireless/introduccion/vulnerabilidades-del-cifrado-wep

https://www.jcea.es/artic/rc4.htm

6. Vulnerabilidades y Ataques en redes WiFi

https://www.osi.es/es/actualidad/avisos/2017/10/routers-wifi-vulnerables-han-conseguido-romper-el-protocolo-de-seguridad

http://www.el-palomo.com/2012/04/secuestro-de-sesiones-de-aplicaciones-web-session-hijacking/

https://www.esferize.com/la-vulnerabilidad-krack/

7. La red WiFi en entornos industriales

https://www.incibe-cert.es/blog/ciberseguridad-las-comunicaciones-inalambricas-entornos-industriales

http://trajano.us.es/docencia/RedesLocalesEnLaIndustria/sld/RedesIndustriales6.pdf

https://www.osi.es/es/actualidad/avisos/2017/10/routers-wifi-vulnerables-han-conseguido-romper-el-protocolo-de-seguridad

12 ANEXO I

Tutorial Wifislax

http://zoominformatica.com/blog/wifislax-el-tutorial-definitivo/

https://wifibit.com/como-robar-wifi-tutorial-wifislax/#Paso_18211_Descargar_WifiSlax