Universitat Oberta de Catalunya uoc.edu

Redes wifi, ¿realmente se pueden proteger?

Francisco de Borja Nafria Oñate
Titulación: Seguridad de las Tecnologías de la Información y de las Comunicaciones (interuniversitario: UOC, UAB, URV)
Área del trabajo: Ad-hoc
Realizado en colaboración con el INCIBE

Marco Antonio Lozano Merino
Víctor García Font

Junio de 2018

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:	*Francisco de Borja Nafría Oñate*
Nombre del consultor:	*Marco Antonio Lozano Merino*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2018
Titulación:	Seguridad de las Tecnologías de la Información y de las Comunicaciones (interuniversitario: UOC, UAB, URV)
Área del Trabajo Final:	*Ad-hoc*
Idioma del trabajo:	*Español*
Palabras clave	*Wifi, seguridad, red*

Resumen del Trabajo:

Las redes inalámbricas son utilizadas en todo tipo de ámbitos y, como podremos ver en este Trabajo, están ampliamente integradas en la sociedad. La seguridad de estas supone un factor fundamental para la expansión de las mismas. En la actualidad la preocupación de los usuarios sobre los ataques que pueden sufrir en sus redes inalámbricas está creciendo.

La metodología del trabajo es una combinación práctica y teórica. Inicialmente se exponen los conceptos necesarios para posteriormente comprender los detalles de los diferentes estándares de seguridad, vulnerabilidades y ataques.

Actualmente existen diferentes medios para establecer medidas de seguridad en las redes Wifi, sin embargo, se han tenido que ir renovando continuamente, a medida que se detectaban problemas de seguridad. En este trabajo, analizamos los conceptos básicos de funcionamiento las redes Wifi, para a continuación exponer los estándares de seguridad junto con los ataques sufridos más habituales, investigaremos los diferentes mecanismos que existen para protegerse. Se analizará en el nuevo estándar WPA3 y las mejoras que aporta, al igual que se analizarán las últimas vulnerabilidades descubiertas que afectan al estándar WPA. Los cuales han dado paso a los ataques tipo KRACK y Evil Twin utilizando Linset.

Finalmente, el lector podrá encontrar unas conclusiones y propuesta de trabajo futuro.

Abstract:

Wireless networks are used in all sorts of fields and, as we will see in this paper, are widely integrated into society. Their safety is a fundamental factor for their success. Users are now increasingly concerned about the attacks they may suffer on their wireless networks.

The methodology of the work is a practical and theoretical combination. Initially, the necessary concepts are exposed to later understand the details of the different security standards, vulnerabilities and attacks,

Currently, there are different means to establish security measures in Wi-Fi networks, however they have had to be updated continuously, as security problems were detected. In this work, we analyze the basic concepts of running Wi-Fi networks, to then expose the security standards, the most common attacks, we will investigate the different mechanisms that exist to protect the wireless networks. It will be analyzed the new WPA3 standard and the improvements it brings, as well as analyzing the latest discovered vulnerabilities that affect the WPA standard. Which have given way to attacks type KRACK and Evil Twin using Linset.

Finally, the reader will be able to find some conclusions and a proposal for future work.

Índice

1. Introducción 1
1.1 Contexto y justificación del Trabajo 1
1.2 Objetivos del Trabajo 1
1.4 Enfoque y método seguido 2
1.6 Planificación del Trabajo 2
1.6 Breve sumario de productos obtenidos 1
1.7 Breve descripción de los otros capítulos de la memoria 1
2. Penetrabilidad de las redes wifi en empresas y hogares 2
3. Conceptos básicos de las redes wifi 5
3.1 Qué es Wi-fi y el estándar 802.11 5
3.2 Canales Wi-fi 5
3.3 Estándares 802.11 6
3.4 Servicios en wifi 6
3.5 Topologías redes Wi-fi 7
3.5.1 Red inalámbrica modo Ad Hoc 7
3.5.2 Red inalámbrica modo infraestructura BSS 8
3.5.3 Red inalámbrica modo infraestructura ESS 8
3.6 Identificadores SSID, BSSID y ESSID 8
4. Protocolos de seguridad wifi 10
4.1 Estándar WEP 10
4.2 Estándar WPA y WPA2 11
4.3 Estándar WPA3 13
5. Vulnerabilidades WEP 16
6. Vulnerabilidades WPA/WPA2 17
7. Ataques y contramedidas WiFi: 18
7.1 Ataques comunes 18
7.2 Contramedidas Wifi 19
7.3 Ataques KRACK: 20
7.3.1 Definición 20
7.3.2 Protecciones 22
7.3.3. Análisis práctico – Detección de si un cliente es vulnerable 22
7.3 Ataques Evil Twin utilizando Linset: 24
Descripción 24
Prueba práctica 25
7.4 Ataque basados en diccionario a partir del 4-way handshake 29
8. Conclusiones 31
9. Glosario 32
10. Bibliografía 33

1. Introducción

1.1 Contexto y justificación del Trabajo

En la actualidad las redes Wifi tienen una utilización muy amplia en la sociedad. Estas redes aportan considerables ventajas y por ello se han convertido en elemento fundamental de muchas empresas y hogares. Dada su propia definición de inalámbricas, no sólo afrontan los problemas de seguridad que posee una red cableada, sino que se le suman retos adicionales. Los usuarios que utilizan estas redes no sólo se preocupan de si sus comunicaciones están siendo interceptadas, sino que además de que, si se realiza alguna actividad delictiva en sus redes, la responsabilidad inicial recae sobre el suscriptor del servicio.

Actualmente existen diferentes medios para establecer medidas de seguridad en las redes Wifi, sin embargo, se han tenido que ir renovando continuamente, a medida que se detectaban problemas de seguridad. Recientemente ha sido liberada la versión WPA3, el nuevo estándar de seguridad para redes Wifi. En este Trabajo analizaremos el estado del arte de los estándares de seguridad para estas redes incluyendo principalmente este nuevo sistema entre otros.

Después de estudiar las medidas de seguridad, nos centraremos en el estudio de los ataques más comunes a las redes con seguridad WPA/WPA2, viendo también posibles contramedidas específicas. Adicionalmente, estudiaremos los problemas de seguridad en las redes públicas realizando también una prueba de concepto.

Finalmente, se extraerán conclusiones y se propondrán posibles trabajos futuros.

1.2 Objetivos del Trabajo

A continuación, se pueden encontrar los objetivos de este Trabajo:

- Analizar los elementos fundamentales de las redes wifi incluyendo: Conceptos, Componentes, Modos de funcionamiento, Estándares actuales 802.11, Tipos de autenticación
- Analizar el estado del arte de los protocolos de seguridad Wifi actuales. Incluyendo WPA3.
- Analizar las vulnerabilidades del estándar de seguridad WEP, muy utilizado en el pasado, aunque dadas sus múltiples vulnerabilidades ha quedado en desuso.
- Analizar las vulnerabilidades del estándar WPA/WPA2, comprendiendo los principales tipos de ataques y realizar pruebas prácticas de los mismos. Viendo a su vez, las posibles contramedidas.
- Analizar los problemas de seguridad en el uso de redes wifi públicas y realizar una prueba de concepto.
- Extraer conclusiones y plantear un trabajo futuro.

1.3 Requisitos legales y éticos

Se debe tener en cuenta que este Trabajo únicamente tiene el propósito educativo de investigación, cualquier conocimiento desvelado no se podrá utilizar para cometer actos delictivos.
Se aprovecha para recordar al lector que según el Artículo 197 del Código Penal del Reino de España que, entre otros, la interceptación de cualquier comunicación o el acceso a un sistema informático sin consentimiento puede estar castigado con penas de prisión.

1.4 Enfoque y método seguido

En este Trabajo se ha decidido seguir una estrategia que combina estudio teórico y práctico. Se considera que, de esta forma, se alcanzará un análisis más profundo y, por lo tanto, los objetivos quedarán completados de forma satisfactoria.

1.5 Recursos necesarios

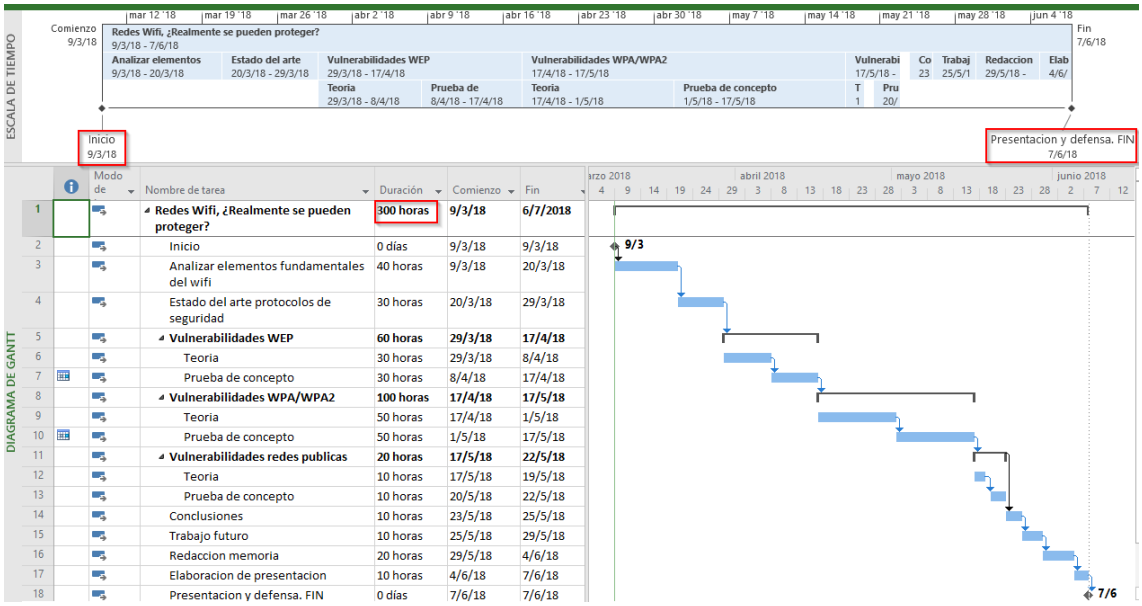
Se utilizará un ordenador personal y un router propiedad del alumno como material físico necesario para la realización del Trabajo.
Se utilizará el paquete de ofimática de Microsoft para el desarrollo de la Memoria y la presentación.
Se utilizarán herramientas especializadas para los ejemplos prácticos, siempre cumpliendo con la Licencia de Distribución de los mismos.
Se utilizará la información disponible en Internet y en los recursos de la UOC.

1.6 Planificación del Trabajo

Teniendo en cuenta mi nivel de conocimiento y experiencia se propone la siguiente planificación temporal, detallada mediante un diagrama de Gantt.

Esta planificación tiene en cuenta puentes y, por supuesto, tiempo de redacción de memoria y tiempo de elaboración de presentación.

Debido a la situación personal del alumno, la mejor planificación consiste en conseguir los objetivos con una dedicación de 3,5 horas diarias (incluyendo sábados y domingos, aunque excluyendo puentes.



1.6 Breve sumario de productos obtenidos

En este Trabajo, no se han desarrollado productos nuevos, sino que se han estudiado y puesto en práctica vulnerabilidades, ataques y nuevas especificaciones de seguridad en redes inalámbricas.

1.7 Breve descripción de los otros capítulos de la memoria

En el primer capítulo encontramos información introductoria como el contexto, objetivos y metodología del trabajo.
En el segundo capítulo se ha realizado un análisis del nivel de penetración de las redes wifi en las empresas y hogares españoles
A continuación, se ha pasado a desarrollar la parte teórica dividida en: análisis de los conceptos fundamentales de las redes wifi y el análisis de los protocolos de seguridad wifi incluyendo al nuevo estándar WPA3. (Aunque este estándar aún está en fase de desarrollo).
A continuación, se ha realizado un análisis práctico y teórico de los ataques más novedosos en las redes inalámbricas.
Por último, se han expuesto unas conclusiones.

2. Penetrabilidad de las redes wifi en empresas y hogares

En este apartado se ofrece al lector datos reales sobre el nivel de uso y seguridad sobre las redes wifi en empresas y hogares españoles.
Para ello se han utilizado fuentes oficiales como los informes del "Observatorio Nacional de Telecomunicaciones y SI" (ONTSI) y datos proporcionados por el Instituto Nacional de Estadística (INE).

Según la Nota de Prensa del 5 de octubre de 2017 proporcionada por el INE en [1], el 83,4% de los hogares españoles tiene acceso a Internet.

A continuación, podemos ver un gráfico extraído de la Nota de Prensa mencionada en [1] en la que podemos observar la evolución del equipamiento TIC en las viviendas españolas:

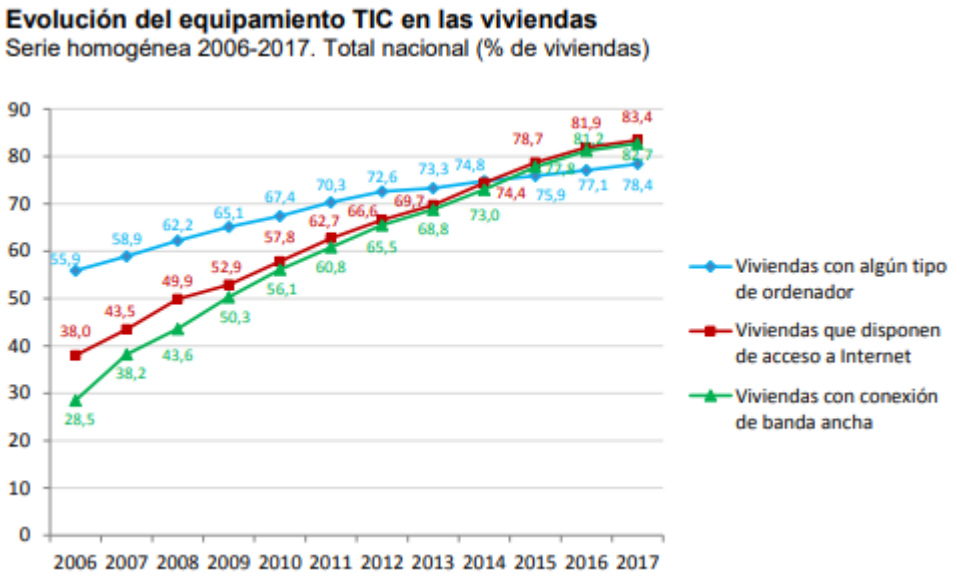


Ilustración 1. Viviendas con acceso a internet

El ONTSI afirma que existe una penetración de conexión a internet en los hogares del 77.3% en [2]. En este mismo informe, de entre los usuarios de internet destaca que el lugar de acceso más frecuente suele ser el hogar (91.8%), seguido del trabajo y las casas de amigos o familiares.
Podemos observar que el 75% de los usuarios que realizan gestiones electrónicas con la administración publica lo hacen a través de la conexión a internet que disponen en el hogar y que un 80.8% de los que acceden a la banca electrónica también prefieren hacerlo a través de la red fija del hogar.

Esta misma organización publica otro informe en el que podemos encontrar datos interesantes en [3].
De este documento hemos extraído el siguiente gráfico:

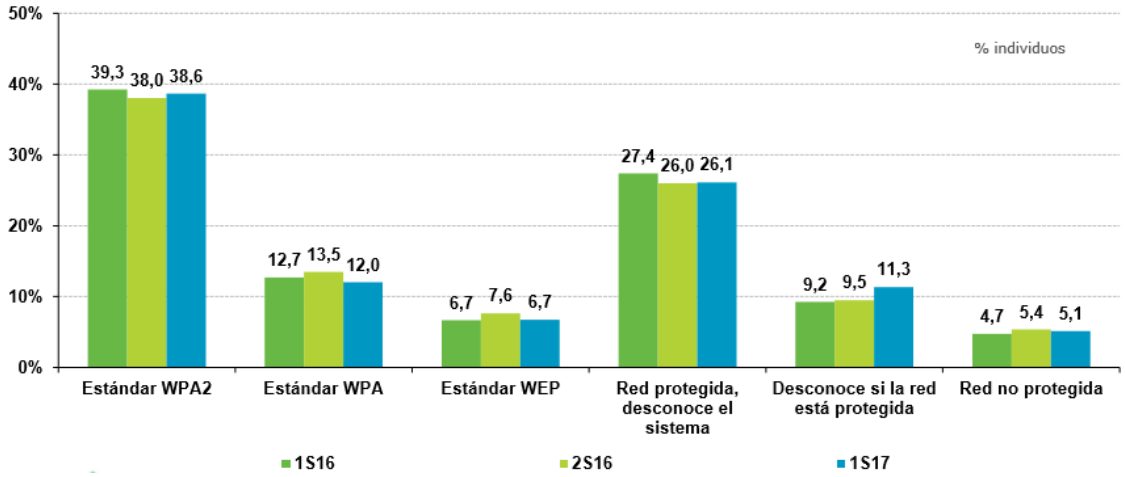


Ilustración 2. Medidas de seguridad utilizadas en redes Wifi

Nota sobre la imagen:
1S16 corresponde al estudio realizado en el primer semestre de 2016 (enero - junio), 2S16 al estudio realizado en el segundo semestre de 2016 (julio - diciembre) y 1S17 al estudio realizado en el primer semestre de 2017 (enero - junio).

Del grafico observamos, entre otros, que existe una gran mayoría de redes con seguridad WPA2, que ha incrementado en el 2017 un 1.8% los usuarios que desconocen el estado de su red inalámbrica.

En la sección Hábitos de uso de las redes inalámbricas Wifi, observamos que el 17,5% de los internautas se conecta a una red inalámbrica Wi-Fi pública y un 13,4% a una red de un tercero y lo hace siempre que lo necesita y en cualquier lugar (39,1%).

De este mismo documento podemos observar que un 14.1% de los usuarios sospecha haber sufrido una intrusión en su red wifi durante el 2017, lo que supone un incremento del 2% respecto al 2016.

En cuanto a datos más específicos de las empresas, el ONTSI publica el informe [4]. Del cual extraemos el siguiente gráfico:

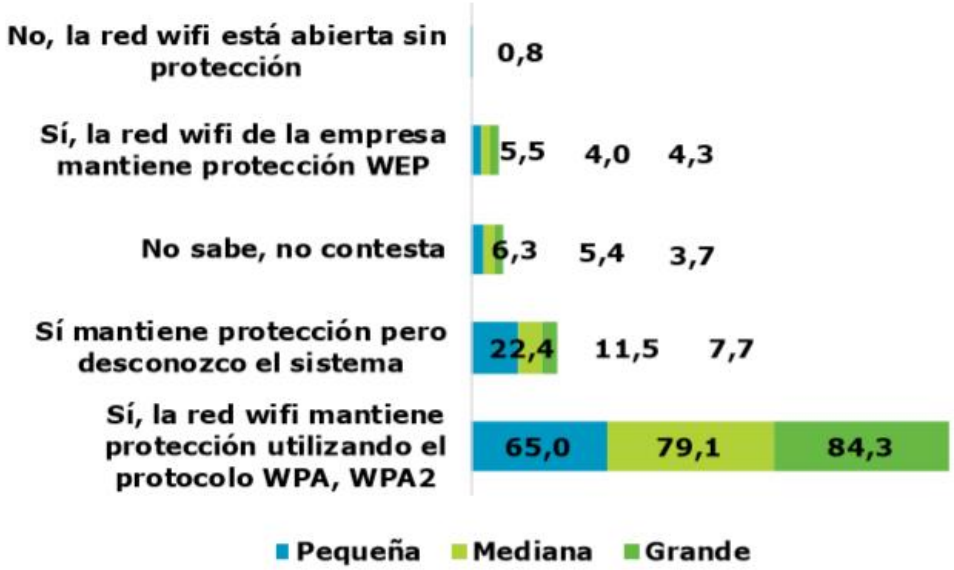


Ilustración 3. Seguridad en conexiones Wifi por tamaño de empresa

De este podemos destacar:

- que se encuentra una relación indirectamente proporcional entre el tamaño de la empresa y la seguridad en su red Wifi. Cuanto más pequeña la empresa, menor control sobre la seguridad del wifi
- el 77.3% de las empresas utiliza seguridad WPA/WPA2, el 4.5% reconoce utilizar seguridad WEP, un 0.2% no dispone de seguridad y el 13% desconoce qué tipo de protección tienen.

Como resumen a este apartado, tras el análisis de los documentos de estadísticas sobre las conexiones Wifi en la sociedad española, observamos un crecimiento tanto en las conexiones Wifi de los usuarios, como en su preocupación por estar siendo atacados o tener intrusos en sus redes.

3. Conceptos básicos de las redes wifi

En este apartado se pretende mostrar los conceptos teóricos básicos de las redes inalámbricas wifi, que ayudarán al lector a comprender los siguientes capítulos de este Trabajo.

3.1 Qué es Wi-fi y el estándar 802.11

El término red inalámbrica (en inglés: Wireless Network) se utiliza para designar la conexión de nodos que se da por medio de ondas electromagnéticas, sin necesidad de una red cableada o alámbrica. La transmisión y la recepción se realizan a través de puertos.
Wi-fi es una marca comercial de Wi-fi Alliance, que únicamente permite el uso de Wi-fi Certified a productos que completan con éxito pruebas de certificación de operabilidad. Aunque popularmente se piensa que Wi-fi es un acrónimo de "Wireless Fidelity", esto nunca ha sido confirmado, y es desmentido desde múltiples fuentes, ver [5] y [6]. Cuando hablamos de Wi-fi nos referimos a la tecnología de redes de ordenadores basada en el estándar IEEE 802.11.

Wi-fi Alliance es una asociación mundial de compañías entre las que encontramos actores tan destacados como Apple, Cisco, Intel y Microsoft.

Ilustración 4. Logotipo Wi-fi

El estándar IEEE 802.11 trabaja en las capas de Enlace de datos y Físico del modelo OSI.

3.2 Canales Wi-fi

La tecnología Wi-fi actualmente utiliza dos bandas de frecuencia, la de 2,4GHz y la de 5GHz.
Ambas bandas, se pueden utilizar sin solicitar permiso a instituciones como FCC (Federal Communications Commision, o Comisión Federal de Comunicaciones en español). Esto supone que pueden ser utilizadas por distintos tipos de comunicaciones y por lo tanto se pueden dar escenarios donde haya un elevado nivel de interferencias.

Para intentar aliviar las interferencias, existen los canales. Tal como sucede con la modulación FM que es dividida en diferentes canales, podemos encontrar 14 canales Wi-fi. Aunque este número puede variar dependiendo del país ya que hay en determinados países que se ha reservado un ancho de banda menor para esta tecnología.
El ancho de cada canal se mide en los MHz que transmite el canal. El ancho exacto de cada canal puede variar dependiendo de que estándar de Wi-fi se use, pero el ancho de canal básico es de 20 o 22 MHz.

A continuación, se puede observar un gráfico con los canales y su frecuencia central y ancho de banda.

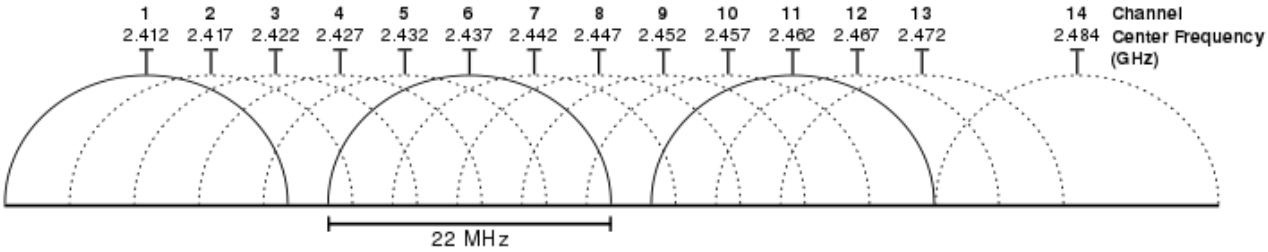


Ilustración 5. Representación gráfica de canales Wifi en la banda de 2,4GHz. Fuente: [8]

En cuanto a los canales en la banda de los 5 GHz, el número de canales difiere mucho más entre países, y no tienen tanto nivel de solapación entre sí.

3.3 Estándares 802.11

La familia 802.11 consiste en una serie de técnicas de modulación por aire half-duplex que se basan en el mismo protocolo básico. El estándar siempre empieza por “802.11” seguido de una o varias letras, aunque a veces pueden ser números.

802.11-1997 fue el primer estándar de red inalámbrica de la familia, pero 802.11b fue el primero ampliamente aceptado, seguido por 802.11a, 802.11g, 802.11n y 802.11ac.

A continuación, podemos observar una tabla de los estándares más populares:

Protocolo 802.11	Frecuencia (GHz)	Ancho de banda (MHz)	Velocidad de transmisión (Mbps)
a	5	20	6, 9, 12, 18, 24, 36, 48, 54
b	2.4	22	1, 2, 5.5, 11
g	2.4	20	6, 9, 12, 18, 24, 36, 48, 54
n	2.4/5	20/40	A 2.4GHz hasta 288.8 A 5GHz hasta 600
ac	5	20	346.8
		40	800
		80	1733.2
		160	2466.8

3.4 Servicios en wifi

Para poder ofrecer un nivel de seguridad alto, en una red inalámbrica deberíamos encontrar los siguientes servicios garantizados:

SERVICIO	DESCRIPCION
Control de Acceso	Limitar el acceso únicamente a entidades autorizadas

Autenticación	Identificar la entidad que generó la información, evitando suplantaciones de identidad.
Disponibilidad	La red o la información se debe encontrar disponible siempre que se requiera, siendo capaz de protegerse u optimizar recursos para evitar denegaciones de servicio.
Confidencialidad	Asegura el acceso a la red o a la información únicamente por aquellos que estén autorizados a ello.
Integridad	Impide cualquier modificación no autorizada de la información.

3.5 Topologías redes Wi-fi

A continuación, se detallan las topologías más comunes en las redes inalámbricas:

3.5.1 Red inalámbrica modo Ad Hoc

Las redes Ad hoc, también se pueden denominar en inglés “Independent Basic Service Set” (IBSS), o lo que es lo mismo en español: Conjunto independiente de servicios básicos.
En este tipo de tipología se crea una red descentralizada, todos los nodos se disponen conectados entre sí unos a otros mediante conexiones inalámbricas sin utilizar puntos de acceso que centralicen las conexiones. La conexión entre los dispositivos es punto a punto.
Este tipo de topología no es la más habitual, pero si puede ser muy práctico en ciertos escenarios, ya que aporta las siguientes ventajas: alto rendimiento, sin coste en elementos centrales de red, uso de frecuencias que no requieren licencia para su uso, no disponen de punto único de fallo. Sin embargo, requiere dispositivos más inteligentes y protocolos más versátiles y adaptables por los constantes cambios de ruta.
A continuación, podemos ver un ejemplo sencillo de una red Ad-hoc:

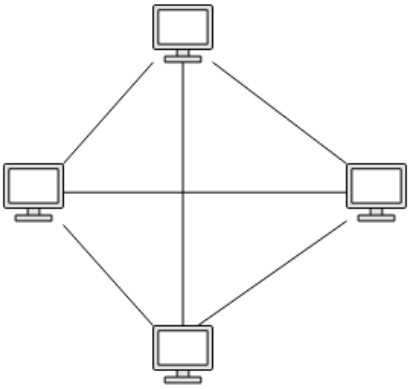


Ilustración 6. Ejemplo red Ad-Hoc

3.5.2 Red inalámbrica modo infraestructura BSS

Estas redes se denominan en inglés “Basic Service Set” (BSS), o en español: Conjunto de servicios básicos.
Esta tipología se caracteriza por disponer de un Punto de Acceso, o “Access Point” (AP) en inglés. Los clientes se unen a la red mediante este AP. Este tipo de topología es común en ámbitos de diferente índole.
Al final de este capítulo, podemos ver un pequeño esquema de un ejemplo sencillo de esta topología.

3.5.3 Red inalámbrica modo infraestructura ESS

Esta tipología se denomina en inglés “Extended Service Set” (ESS), o en español: Conjunto de Servicios Extendidos o Área de Servicio Extendida.
Esta tipología es como la BSS, pero escalable dado que, en vez de contar con un único AP, se dispone de varios. Los clientes pueden conectar a distintos AP para acceder a la red.
Se podría hacer una equiparación de: un BSS corresponde a la red inalámbrica creada por un AP y un ESS corresponde a una WLAN completa creada por todos los AP.
Al final de este capítulo, podemos ver un pequeño esquema de un ejemplo sencillo de esta topología.

3.6 Identificadores SSID, BSSID y ESSID

Los términos SSID, BSSID y ESSID son utilizados para describir secciones de una red inalámbrica o en inglés “Wireless Network” (WLAN). Los 3 términos son similares, y aunque no difieren demasiado, en posteriores capítulos el lector podrá denotar que si tienen cierta importancia en cuanto a evitar algunos tipos de ataques.

SSID: “Service Set Identifier” o en español servicio identificador de conjunto.
El SSID se podría definir como el nombre de la red. Es necesario identificar a las diferentes redes inalámbricas con su correspondiente nombre y que así puedan existir diferentes redes en el mismo medio y que los usuarios las puedan identificar sencillamente por su nombre.
Cuando un usuario se quiere conectar a una red, busca el SSID de la red objetivo en la lista mostrada en su dispositivo.

BSSID: “Basic Service Set Identifier” o en español servicio básico identificador de conjunto.
El BSSID es un elemento utilizado para identificar el AP dentro una WLAN especifica. Mientras que el SSID nos servía para identificar diferentes WLAN, el BSSID nos sirve para identificar diferentes AP dentro, o no, de la misma WLAN. Esta información se debe incluir en todos los paquetes inalámbricos.
Los usuarios normalmente no se deben preocupar del BSSID y nunca lo llegan a visualizar, ya que únicamente se preocupan del SSID o del ESS al que están conectados.
Cuando un usuario se desplaza y se cambia de AP dentro de la misma WLAN, se cambia el BSSID.

Normalmente, el BSSID corresponde a la dirección física MAC del AP, pero suele ocurrir que un mismo AP está radiando diferentes redes, con diferentes SSID. Por lo tanto, a este AP se le asignaran múltiples MAC, una para cada BSS que está ofreciendo. Todas las direcciones MAC secundarias del AP, se crean basadas en la primaria.

Como resumen a este apartado, se muestra un gráfico a continuación, en el que se pueden ver todos los conceptos explicados anteriormente:

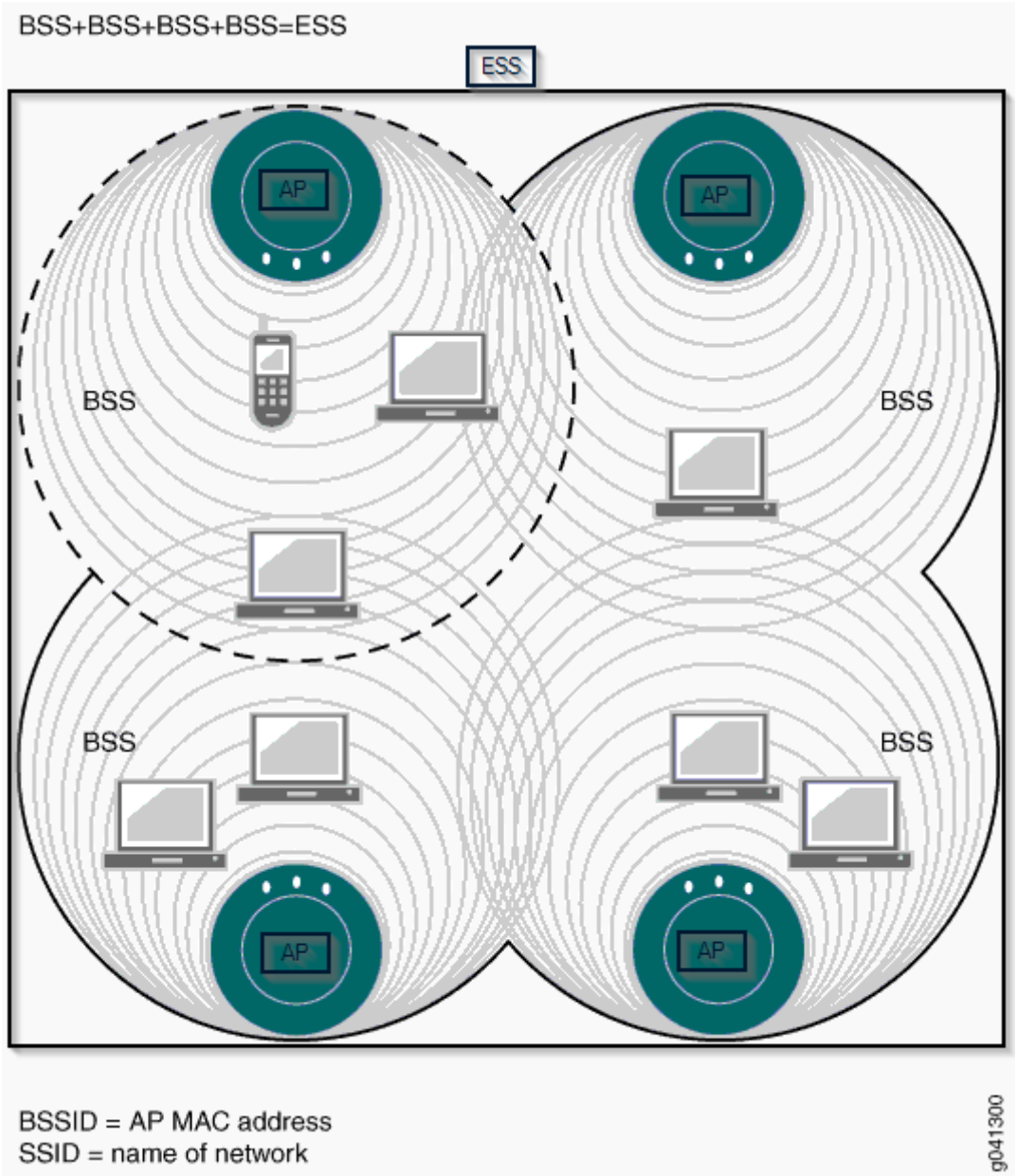


Ilustración 7. Resumen conceptos del apartado. Fuente grafico Juniper Networks [12]

4. Protocolos de seguridad wifi

Uno de los factores que afecta directamente a la usabilidad de las redes inalámbricas es la seguridad. Este factor gana importancia respecto a las redes alámbricas debido a que el medio de transmisión de ondas de radio a través del espacio es accesible a todos aquellos que se encuentren en zona de cobertura.

En wifi encontramos diferentes estándares de seguridad, los cuales se han ido desarrollando a medida que se descubrían vulnerabilidades.

En este capítulo, se expone cuáles son los principios de funcionamiento de los estándares de seguridad: WEP, WPA/WPA2 Y WPA3.

4.1 Estándar WEP

WEP, es el acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", incluido en el estándar IEEE 802.11 como protocolo para redes Wireless. El principal objetivo de este estándar es proteger la confidencialidad de los usuarios de escuchas no autorizadas. Esto se hace mediante la aplicación de 3 propiedades: confidencialidad, control de acceso e integridad. (Conceptos explicados en 3.4 Servicios en wifi)

Todas estas propiedades son obtenidas mediante una clave secreta. Toda la seguridad del protocolo WEP reside en la dificultad de conseguir la clave secreta.

Para comprender el proceso de cifrado/descifrado de WEP, antes es necesario definir algunos términos:

- PRNG: Pseudo random-number generator o Generador de pseudo números aleatorios.
  Se debe recordar que en todo proceso criptográfico siempre se necesita algún tipo de número origen aleatorio. En WEP, el cifrado de secuencia RC4 permite crear una secuencia de números pseudo-aleatorios. Pero como todos los cifradores de streams, creará el mismo flujo de salida ante la misma entrada.
- IV: Initialization Vector o Vector de Inicialización.
  El IV es la entrada que se introduce en el PRNG. Está compuesto de 24 bits y se concatena a la clave secreta de 40 bits. Para que el PRNG cambie y no produzca siempre el mismo número aleatorio, el IV debe de cambiar lo más a menudo posible. Teniendo en cuenta que está formado por 24 bits, únicamente existen 2^24=16.777E3 IVs diferentes.
- ICV: Integrity Check Value o Comprobador de Integridad.
  Para proveer integridad en WEP se utiliza el algoritmo CRC32. Antes de que un paquete se encripte se genera un “valor comprobante de redundancia cíclica” y se concatena al mensaje. Este valor es de longitud 32 bits. De forma más sencilla, ICV es un identificador único para cada paquete. Se debe tener en cuenta que CRC32 es una funcional lineal y por lo tanto no provee ningún tipo de seguridad criptográfica.

Antes de proceder a encriptar un mensaje, es necesario ejecutar los procesos de autenticación y asociación. Esto consiste en que un AP anuncia su existencia y permite a un cliente comunicarse con este. Primero el AP escuchara todos los APs disponibles en el entorno. Cuando encuentre uno y desee conectarse, le mandara un mensaje de solicitud de autenticación. El AP responde con una trama de autenticación conteniendo un reto de texto, que el cliente debe encriptar usando la clave secreta y devolvérselo al AP. EL AP se asegura de que el cliente tiene la clave WEP correcta descifrando la respuesta, y si el texto coincide exactamente, le permitirá autenticarse. Procediendo a asociarse y el AP le reservara memoria y le asignara un ID.

El procedimiento de encriptado consiste en:

1. El PRNG se alimenta con la clave secreta y el IV.
2. El PRNG genera lo que se denomina “key sequence” o secuencia de clave.
3. Se calcula la O exclusiva de esta secuencia de clave y una concatenación del texto en plano y su ICV.
4. Finalmente, el mensaje encriptado es concatenado con el IV en texto plano y transmitido.

El receptor del mensaje únicamente necesita hacer el mismo proceso, pero al revés:

1. Tomar el IV que se acaba de recibir, concatenarlo con la clave secreta y alimentar el PRNG.
2. El PRNG genera la “key sequence”.
3. Se calcula la OR de esta “key sequence” y del texto cifrado. Obteniendo el texto en plano y el ICV original.
4. Finalmente, se genera el ICV del texto desencriptado y se comprueba la integridad del mismo.

En siguientes capítulos analizaremos las vulnerabilidades que afectan al protocolo de seguridad WEP.

4.2 Estándar WPA y WPA2

Después de que se descubrieran las sendas vulnerabilidades por las que estaba afectado el estándar WEP, el IEEE creó la nueva corrección de seguridad 802.11i para neutralizar estas vulnerabilidades. En el 2003, la Wi-Fi Alliance anunció que WEP había sido reemplazado por Wi-Fi Protected Access (WPA). Finalmente, en 2004, con la ratificación del estándar completo 802.11i (conocido como WPA2), el IEEE declaró que WEP fue revocado por presentar fallos en su propósito de ofrecer seguridad.

WPA corresponde a “Wi-fi Protected Access” o “Acceso Wifi protegido”. WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida temporal para sustituir a WEP mientras 802.11i era finalizado. Una vez finalizado el nuevo estándar 802.11ie se crea el WPA2 basado en este. De este modo, WPA2 es la versión certificada del estándar.

WPA mantiene el núcleo de WEP, aunque introduce mejoras para afrontar los problemas de seguridad presentes en este.

WPA usa dos diferentes métodos de autenticación:

1. Enterprise: con clave de distribución
   Requiere un servidor RADIUS. El punto de acceso cuando detecta un cliente le mande mensaje de solicitud EAP REQUEST-ID (EAP: Extensible Authentication Protocol). En respuesta, el cliente manda el mensaje EAP RESPONSE-ID conteniendo los datos de identificación. El AP entonces encapsula la respuesta en una petición RADIUS y se lo mande al servidor RADIUS el cual básicamente permite gestión centralizada de datos de autenticación. El Servidor comprobará las credenciales contra su base de datos y entonces responderá con el mensaje permitiendo la autenticación.

2. Personal: con clave pre-compartida (PSK: Pre Shared Key)
   Diseñado para casas y redes pequeñas. No requiere autenticación de servidor. Cada dispositivo encripta el trafico de red de la clave de encriptación (desde 128 hasta 256 bits) pre-compartida. En WPA2 se introduce el 4 way handshake para permitir al AP y cliente demostrarse mutuamente de forma independiente que conocen la PSK. Este es explicado en: "The Evolution of 802.11 Wireless Security" (PDF). ITFFROC. 2010-04-18.

WPA mejora la encriptación con claves temporales para eliminar el problema de la reutilización de claves precompartidas en WEP, aunque el principio sigue siendo el mismo que en WEP. Para esto implementa el protocolo TKIP (Temporal Key Integrity Protocol). El cual cambia la clave dinámicamente en el tiempo mediante la rotación de claves y IVs para cada paquete. Genera un numero aleatorio de claves desde la contraseña. Cada cambio es sincronizado mediante los clientes Wireless y el AP. A su vez, como mejora, se ha incrementado el IV hasta 48 bits para decrementar la probabilidad de choque y/o reutilización.
En WPA 2 se introduce CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) que se basa en el uso de AES (Advanced Encryption Standard) como sustitución a TKIP de WPA.

En cuanto a la Integridad, para solucionar el gran problema de WEP de la linealidad en la función CRC32, en WPA se define una medida de seguridad denominada Michael (MIC: Michael Message Integrity Code) para mejorarla. Este permite calcular un Mensaje de Código de Integridad adicionalmente al ICV. Fue diseñado por Niels Ferguson en su trabajo titulado. “Michael: An improved MIC for 802.11 WEP,”. tech. rep., IEEE, 2002. Además, implementa contador de tramas para evitar ataques de reenvío.

4.3 Estándar WPA3

En el momento de redactar este trabajo, la única información que se encuentra disponible es la dispuesta por la WPA3 en comunicados de prensa [13]. Desafortunadamente, no incluyo demasiados detalles técnicos, aunque ya podemos conocer las bases y los problemas que intentara solucionar WPA3.

WPA3 incluirá cuatro nuevas características de seguridad principales:

Un handshake mas seguro:

En los comunicados explican que WPA3 ofrecerá protecciones fuertes incluso cuando los usuarios eligen contraseñas que no cumplen con las recomendaciones de complejidad típicas. Esto significa que las redes domésticas normales que normalmente están protegidas mediante una sola contraseña usaran SAE (Simultaneous Authentication of Equals) para realizar el handshake. Este protocolo es resistente contra los ataques de diccionario sin conexión. Esto soluciona el problema de que la mayoría de estas redes están protegidas con contraseñas débiles, ya que en WPA2 la resistencia contra ataques de diccionario sin conexión es baja.

En el siguiente trabajo: http://orbilu.uni.lu/bitstream/10993/24767/1/Dragonfly.pdf
Se demuestra que SAE proporciona seguridad en cuanto a si un atacante consigue la clave no puede usarla para descifrar el trafico capturado. Esta prueba resulta muy interesante, ya que de nuevo en WPA2 nos encontrábamos el problema de que cuando un atacante descubre la contraseña le permite descifrar todo el trafico anterior que tenga capturado.

Sin embargo, se requiere cierta precaución. Si el apretón de manos no se implementa con cuidado, es vulnerable a ataques de canal lateral. Además, debido a cuestiones de diseño, el punto de acceso (AP) debe almacenar la contraseña en texto plano. Esto supone que, si un posible atacante obtiene acceso al AP, puede leer la contraseña del texto simple. Además, es bien sabido en el mundo de seguridad, que por mucho que exista una prueba exitosa que demuestra un nivel de seguridad elevado, no garantiza que sea realmente seguro. Véase el ejemplo de que WPA2 también tenia pruebas de seguridad superadas, y aun así es necesaria una nueva actualización debido a sus vulnerabilidades.

En un nivel más técnico, el handshake SAE es una variante del presentado en RFC 7664. En una red Wi-Fi, el protocolo de enlace SAE negocia una nueva clave maestra por pares (PMK). El PMK resultante se utiliza luego en un protocolo tradicional de 4 vías para generar claves de sesión. Esto significa que el saludo SAE siempre va seguido de un apretón de manos de 4 vías.

Se sigue utilizando el procedimiento de 4 vías, ya que el PMK de 32 bytes que se negocia en SAE, tal como se ha comentado anteriormente, no puede adivinarse mediante ataques de diccionario. Además, se debe tener en cuenta que cuando se obtiene la contraseña se sigue sin poder obtener.
En el siguiente enlace se puede visualizar un fichero de captura de trafico que contiene el handshake SAE:

https://www.cloudshark.org/captures/3638626f4551

Reemplazo de WPS (Wi-fi Protected Setup):
La segunda mejora que aporta WPA3 es la sustitución de WPS (Wi-Fi Protected Setup). Este protocolo sirve para la configuración sencilla y segura de incorporación de dispositivos a la red con una interfaz limitada o nula.
Tenemos que tener en cuenta que WPS se considera que tiene un nivel muy bajo de seguridad. El reemplazo, se denomina DPP (Wi-Fi Device Provisioning Protocol). Este protocolo se puede utilizar introduciendo una contraseña, código QR, usando NFC o Bluetooth. Básicamente, DPP confía en claves publicas para identificar y autenticar dispositivos.

El protocolo DPP en sí mismo consta de tres fases principales. En la primera fase, llamada bootstrapping, se obtiene la clave pública del nuevo dispositivo (es decir, el dispositivo que se está agregando a la red). Esto se puede lograr escaneando un código QR que codifica la clave pública, o intercambiando y encriptando la clave pública de forma inalámbrica utilizando el protocolo PKEX . Como se sugirió anteriormente, también es posible transferir la clave pública mediante NFC o Bluetooth. Cada método proporciona diferentes niveles de garantías en cuanto a si la clave pública obtenida pertenece realmente al nuevo dispositivo.

En la segunda fase, llamada autenticación y aprovisionamiento, las claves públicas ahora confiables se usan para establecer una conexión autenticada (temporal), sobre la cual se pueden intercambiar credenciales. Las credenciales intercambiadas aún no son las credenciales finales para conectarse a la red. En cambio, la credencial intercambiada es un así llamada conector. Este conector se utiliza en la fase final del protocolo DPP, llamada fase de acceso a la red, para establecer las claves de redes reales. Más precisamente, la conexión se utiliza para realizar un intercambio Diffie-Hellman para establecer una clave maestra por pares (PMK). Este PMK se puede usar para acceder a la red de forma normal.

Cifrado no autenticado:
La tercera característica de WPA3 fortalece el cifrado no autenticado para redes abiertas, como por ejemplo en puntos de acceso públicos. Esto supondrá que un posible atacante que pretenda monitorear el trafico, únicamente podrá hacerlo de si mismo y no del resto de clientes. Desafortunadamente, un adversario activo aún puede crear un AP falso, engañar a las víctimas para que se conecten a este AP falso y luego leer todo el tráfico de los clientes conectados.
Aunque no lo especifican, estas mejoras parece que se conseguirán mediante el uso del protocolo Opportunistic Wireless Encryption (OWE).

En un nivel mas técnico, el handshake OWE negocia un nuevo PMK usando un intercambio de claves Diffie-Hellman. Este protocolo de enlace está encapsulado en los marcos de solicitud y respuesta de (re)asociación. El PMK

resultante se utiliza en un handshake de 4 vías, que negociará e instalará claves de cifrado de trama.

Aumento de los tamaños de clave de sesión:
Finalmente, la cuarta mejora que ofrece WPA3 es el aumento del tamaño de las claves. WPA3 admitirá AES-GCM con claves de 256 bits para cifrado basadas en criptografía de curva elíptica. Además, se usará SHA384 de la familia SHA2, y cualquier clave RSA empleada debe tener al menos 3072 bits de tamaño. Todo combinado, esto da como resultado una seguridad de 192 bits, que coincide aproximadamente con la fuerza efectiva de las curvas elípticas de 384 bits y SHA384.

Wi-Fi Alliance adicionalmente especifica que ahora exige nuevos protocolos como Protected Management Frames (PMF) como parte de su certificación. Esto evita que un atacante pueda forzar la des-autenticación de un cliente. Mediante esto también se prueba los certificados de los servidores de forma adecuada y que estén parcheados contra ataques tipo KRACK.

5. Vulnerabilidades WEP

Teniendo en cuenta la descripción del estándar WEP, a continuación, explicamos los principales problemas de seguridad por los que se ve afectado:

- El IV (Vector de Inicialización) es pequeño y siempre se transmite una parte de él en texto claro. Como ya se ha comentado, es una cadena de 24 bits. Estos 24 bits son los utilizados en la inicialización del cifrador de stream por el algoritmo RC4. 24 bits es un tamaño demasiado pequeño cuando se utiliza con propósitos criptográficos.
- El IV (Vector de Inicialización) es estático. Reutilizar el mismo IV, produce inicializar de la misma forma el cifrador de stream, y por lo tanto la misma salida. Esto en conjunto con el problema de seguridad citado anteriormente, lo convierte en una combinación que resulta ser un agujero de seguridad muy peligroso.
- Generación de IV no especificada en el estándar. El estándar 802.11 no especifica como los IV deben ser fijados o cambiados. Un adaptador wifi de una misma marca podría generar siempre los mismos IV, o incluso utilizar siempre el mismo. Como resultados, un posible atacante podría capturar tráfico de red, determinar el IV y descifrar tráfico de red.
- EL IV es parte de la clave de encriptación en RC4. El hecho de que un posible atacante obtenga 24 bits de cada clave de paquete, combinado con la debilidad del protocolo RC3, conduce a que sea posible realizar ataques basándose en interceptar una cantidad relativamente pequeña de tráfico. De ahí que los ataques a WEP siempre suelan involucrar clientes conectados.
- WEP no provee protección de integridad criptográfica. Aunque tal como se comentó el protocolo usa protocolo de redundancia cíclica no criptográfico (CRC, Cyclic Redundancy Check) para comprobar la integridad de los paquetes, en combinación con un generador de streams se ha demostrado que introduce vulnerabilidades.

Todas estas vulnerabilidades han dado lugar a múltiples ataques automatizados mediante script, que son capaces de obtener la clave WEP en menos de un minuto, sin necesidad de diccionarios.

6. Vulnerabilidades WPA/WPA2

Teniendo en cuenta la descripción del estándar WPA/WPA2, a continuación, explicamos los principales problemas de seguridad por los que se ve afectado:

- Contraseñas débiles. Las claves pre-compartidas de WPA y WPA 2 son vulnerables a crackeo de contraseñas si los usuarios configuran contraseñas con un nivel de complejidad débil. Esto quiere decir que las contraseñas se pueden averiguar con ataques de fuerza bruta.
- Falta se secreto hacia delante (forward secrecy). Este concepto quiere decir que si un adversario descubre la clave pre-compartida será capaz de desencriptar todo el trafico pasado y futuro que capture. Esto expone a los usuarios en redes publicas donde todo el mundo comparte la misma clave, ya que un atacante podrá desencriptar el trafico de todos los usuarios.
- Inyección de paquetes y desencriptación. Los ataques de Beck-Tews attack y Ohigashi-Morri permiten realizar inyección y desencriptación de paquetes cuando se utiliza WPA en conjunto con TKIP. El objetivo de este trabajo no es estudiar este tipo de ataques. Se puede encontrar más información en: http://dl.aircrack-ng.org/breakingwepandwpa.pdf
- Wifi Protected Setup (WPS). Ya en el año 2011 se descubrieron vulnerabilidades graves que afectaban a este protocolo y se podría decir que lo dejaban prácticamente inservible. Los fallos de seguridad permitían a un atacante descubrir el PIN WPS para luego obtener la clave WPA/WPA2. Como ya se ha comentado, WPA3 introduce una alternativa a este protocolo. El reemplazo, se denomina DPP (Wi-Fi Device Provisioning Protocol).
- Gestión de reinstalación clave de handshake de 4 vías. Debido a que el protocolo WPA no especifica cómo debe ser la gestión de la clave secreta durante el handshake de 4 vías de WPA, se ha estado implementado de forma insegura por los fabricantes. En el capítulo Ataques KRACK se puede encontrar una encontrar una explicación detallada y una prueba práctica.
- Uso de autenticación de clave pre-compartida (PSK) junto con claves inseguras. Un atacante podría capturar el handshake, y junto con el SSID y las direcciones MAC de cliente y AP podría obtener el secreto compartido pudiendo así conectarse a la red.

7. Ataques y contramedidas WiFi:

7.1 Ataques comunes

En este subapartado, se listan los ataques más comunes a redes Wifi.

- Suplantación de Identificador Único.
  Podemos encontrar dos tipos de ataques de suplantación de identificador único: dirección MAC y tablas ARP.
  El ataque de suplantación de MAC consiste en cambiarse la dirección de Control de Acceso al Medio (MAC) de la tarjeta de red del dispositivo.
  El ataque de suplantación de ARP consiste en que el atacante envía mensajes ARP falsos a la red de área local para conseguir vincular la dirección MAC del atacante con la dirección IP de la víctima.
  El propósito de estos ataques puede ser para diferentes fines, normalmente es para hacerse pasar por otro usuario de la red y conseguir así sus privilegios o para conseguir anonimización.
  Por ejemplo, en muchas redes públicas que son de pago, el identificador único que se utiliza para identificar a un usuario que ha pagado suele ser la dirección MAC, un posible atacante podría hacer un escaneo de red, y clonar la MAC de cualquier cliente para tener acceso a la parte de pago sin haber realizado ningún pago.
  Existen diferentes software y programas automáticos que permiten configurar la MAC deseada e incluso generarla aleatoriamente.

- Man In The Middle.
  El ataque de “hombre en el medio” consiste en que el atacante se ubica entre el cliente y el AP legítimo, de esta forma puede tanto esnifar el tráfico como modificarlo. Este tipo de ataque se puede utilizar con multitud de fines diferentes, por ejemplo, para robar credenciales de sesión, para espiar, para poner en peligro la integridad de la información, etc.

- Ataques a WPS.
  Tal como se citaba en el capítulo de vulnerabilidades WPA. Existen múltiples vulnerabilidades que afectan a WPS, debido a ello se recomienda desactivarlo. Los ataques WPS consisten en descubrir el PIN, para posteriormente obtener la clave WPA.

- Denegación de Servicio.
  Recordando que uno de los servicios que debe ofrecer cualquier red inalámbrica es el de disponibilidad, este ataque consiste en denegar esta disponibilidad. Se pueden utilizar diferentes medios para llegar a conseguirlo, normalmente se trata de abusar de los recursos para que no puedan estar disponible para un usuario legítimo.

- Ataques de reinstalación de claves.
  Los ataques de tipo KRACK, no están entre los más comunes, pero teniendo en cuenta su gravedad y su estudio son parte del propósito de este proyecto son explicados en el siguiente subapartado de este capítulo.

- Falsos AP.
  En este tipo de ataques los atacantes crean Puntos de Acceso falsos, para hacer creer al usuario que se está conectando a través un AP legítimo, sin embargo, el atacante tiene el control de todo el tráfico y, por lo tanto, puede hacer acciones de espía, modificación de información, etc.
  Dentro de esta metodología de ataque, encontramos los de tipo "Linset" o "wiphising", que se explicaran en detalle en el apartado 3 de este capítulo.

- Ataques basados en diccionario a partir del 4-way handshake.
  De la vulnerabilidad citada en el apartado de vulnerabilidades de WPA y WPA2 surge este tipo de ataque. Se ha realizado una Prueba de Concepto en el último apartado de este capítulo demostrando el peligro de establecer contraseñas débiles, ya que si el handshake es capturado por un atacante puede llegar a descifrarlo con ataques de diccionario. Ver apartado 7.4.

7.2 Contramedidas Wifi

En este apartado, se puede encontrar las medidas de seguridad adicionales que se pueden tomar para elevar el nivel de seguridad en una red Wifi. Estas medidas complementaran al nivel de seguridad ofrecido por el estándar en el caso que corresponda.

- **Cambiar y/o ocultar el SSID. Con esto conseguimos evitar que un atacante use scripts públicos que encuentran la clave de seguridad del router basándose en el SSID de la red. Se recomienda además cambiarlo por algo que sea**
- **Establecer contraseñas seguras. Se deben establecer contraseñas con un nivel de seguridad alto, (tanto para acceso a la red como a la parte de administración) algunas recomendaciones establecen que una clave debe tener 20 caracteres incluyendo números, letras y símbolos.**
- **Desactiva red inalámbrica cuando no esta en uso. Aunque esta medida pueda resultar imposible para algunos usuarios, apagar la red wifi mientras no esta en uso puede evitar posibles ataques cuando esta sin supervisión.**
- **Limitar el área de cobertura. El escenario ideal es aquel en el que únicamente existe cobertura Wifi allí donde es necesaria. Así evitaremos sobreexposición a posibles atacantes.**
- **Utilización de IPs fijas. El uso de IPs fijas puede añadir un pequeño nivel de complicación en caso de un ataque, ya que quizás el atacante piense que su ataque este fallando, mientras que sencillamente al haber IPs fijas quizás esta utilizando una dirección IP fuera de rango.**
- **Filtrado MAC: establecer un filtro de direcciones MAC nos puede ayudar a establecer que dispositivos pueden acceder a la red. Con esto, conseguimos que el atacante tenga que realizar un paso adicional de cambio de MAC.**
- **Deshabilitar WPS: Tal como ya se ha comentado varias veces, el protocolo WPS es conocido por tener vulnerabilidades criticas. Incluso**

por parte de la organización Wifi Alliance se recomienda deshabilitar este protocolo.

- **Uso de cifrado adicional. (VPN) Usar una conexión VPN para todo el trafico dirigido a través de la red inalámbrica nos permitirá cifrarlo y así conseguir que, aunque haya un atacante al menos no tenga acceso a nuestro trafico y no pueda ni interpretarlo ni modificarlo.**

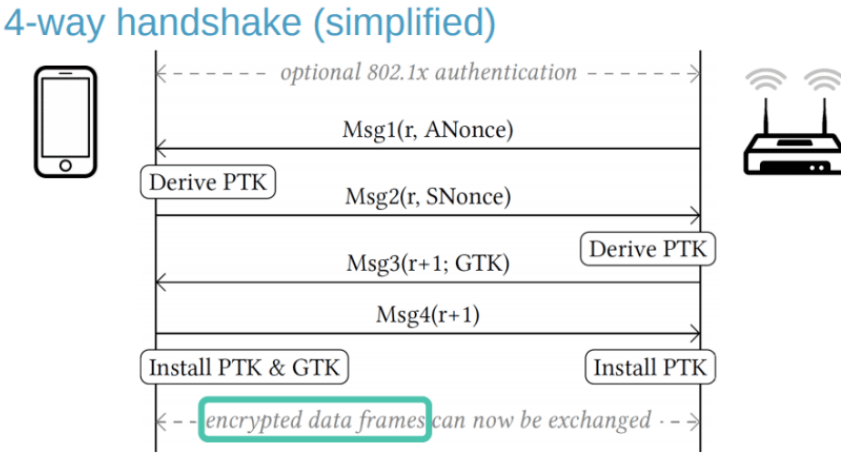
7.3 Ataques KRACK:

7.3.1 Definición

Los ataques de “Key Reinstallation Attacks” o KRACK como son normalmente llamados son los últimos y más importantes ataques descubiertos que afectan al estándar WPA2.

El investigador de seguridad Mathy Vanhoef publicó la existencia de esta vulnerabilidad en el año 2017. Cabe destacar que únicamente publicó la existencia de la vulnerabilidad con un video y posteriormente han publicado un paper en el que explican la teoría del ataque. Sin embargo, se están retrasando y no han llegado a publicar la información práctica de cómo realizar el ataque. Únicamente se han publicado unos scripts para comprobar si nuestros clientes wifi son vulnerables a este tipo de ataques.
En este capítulo, analizaremos la explicación teórica, y haremos la prueba práctica de análisis de los dispositivos cliente para observar si son vulnerables a este tipo de ataque.

Debemos de recordar, tal como se mencionó anteriormente, que en WPA2 existe lo que se denomina el handshake de 4 vías. Si un cliente quiere unirse a una red wifi con este tipo de seguridad, este proceso se ejecutará entre el cliente y el punto de acceso. El propósito de este “apretón de manos” es verificar que el cliente tiene unas credenciales válidas y generar de clave secreta que se utiliza para encriptar todo el tráfico entre el punto de acceso y el cliente conocido como PTK. (Pairwire Transfer Key)
Este ataque afecta a la generación de esta clave de secreta, y por lo tanto permite a un atacante capturar todo el tráfico y descifrarlo.
A continuación, podemos ver un ejemplo simplificado del handshake de 4 vías:



Lo que ocurre durante el proceso de encriptación es que el PTK y el Nonce (Numero de paquete) son mezclados para obtener una clave en forma de cadena de caracteres conocido como clave por paquete. (El valor de Nonce, será incrementado como un contador de uno en uno para cada paquete)
Esta clave para cada paquete se supone que debía ser única y no debía ser utilizada más de una vez. En otras palabras, el contador de paquete nunca debía repetirse, ya que en caso de que se repita, quiere decir que la misma clave se está utilizando para encriptar múltiples paquetes.

Los ataques KRACK funcionan creando un punto de acceso falso con el mismo ESSID que la red a la que está conectada la víctima, pero en un canal diferente.
Por lo tanto, la víctima se conectará a la red falsa pensando que se está conectando a la legítima.
El ataque KRACK servirá al atacante para poder realizar un ataque tipo Man In The Middle con el handshake de 4 vías.
A continuación, se puede ver un gráfico de cómo actúa este ataque:

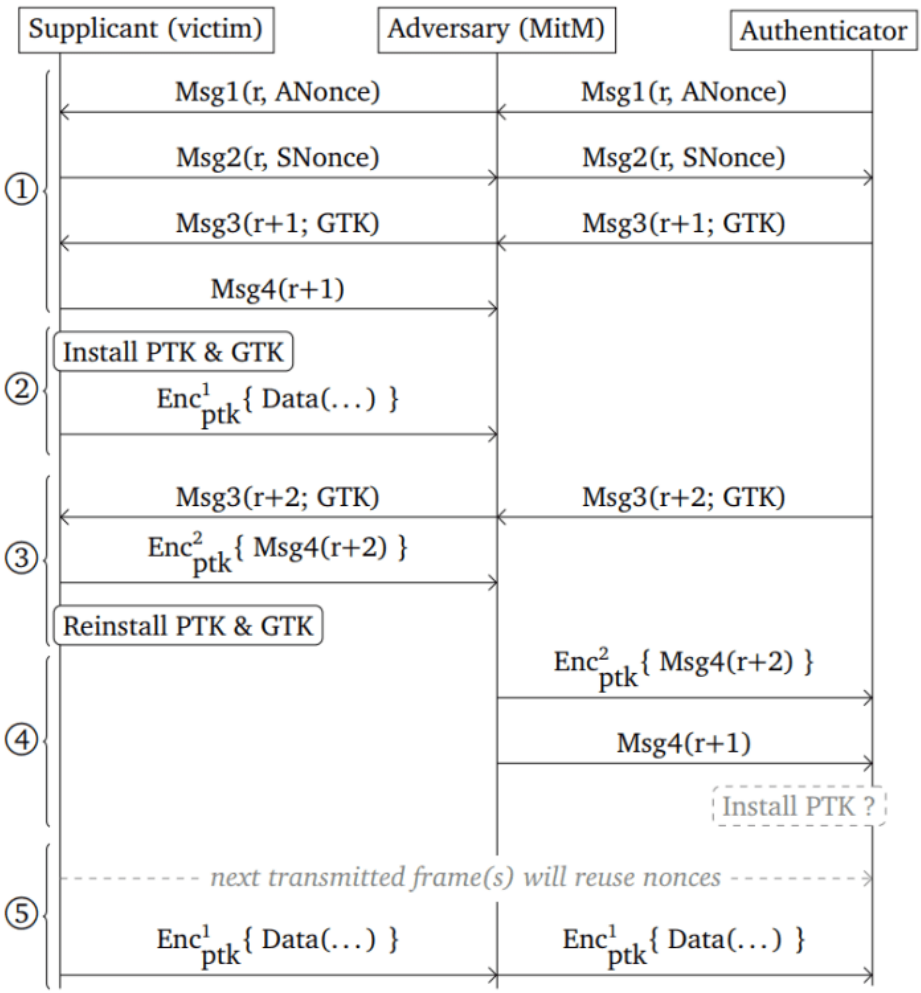


Ilustración 1. Ataque tipo KRACK

Como vemos en la imagen, una vez que el cliente recibe el tercer paquete, instala la clave en el dispositivo y manda un mensaje al Autenticador de que se ha realizado correctamente (ACK).
En este punto, la vulnerabilidad que explota el atacante es: bloquea el cuarto paquete y previene de que llegue hasta el autenticador.
El autenticador espera para recibir el ACK desde el cliente, en caso de no recibirlo el autenticador piensa que el cliente no recibió el tercer paquete y lo vuelve a mandar reiniciando el Nonce.
Esto es repetido múltiples veces. Reutilizando estos valores Nonce, permite repetir los paquetes y descifrarlo ya que al usar el mismo valor Nonce, se estaría usando la misma clave de descifrado.
Este proceso, es el que permite al atacante descifrar paquetes.

7.3.2 Protecciones

Actualizar e instalar los parches necesarios para que gestione bien la reinstalación de claves.

7.3.3. Análisis práctico – Detección de si un cliente es vulnerable

Para la prueba de la detección de si un cliente es vulnerable utilizaremos:

- Maquina física Windows 10 host
- Maquina virtual Kali Linux, hospedada dentro de la maquina física citada anteriormente
- Antena wifi USB

El esquema general que seguiremos será:

1. Mediante los scripts Python generar un AP falso
2. Conectar el dispositivo cliente que queremos testear
3. Testear el dispositivo cliente mediante los scripts Python.

Para ello ejecutamos los siguientes comandos, en los que actualizamos e instalamos las siguientes librerías:

```
apt-get update
apt-get install libnl-3-dev libnl-genl-3-dev pkg-config libssl-dev net-tools git sysfsutils python-scapy python-pycryptodome
```

A continuación, deshabilitamos la encriptación de hardware mediante el siguiente comando: (habiendo dado permisos de ejecución previamente)

```
./krackattack/disable-hwcrypto.sh
```

Recibimos un aviso de que lo ha realizado correctamente y reiniciamos la máquina.
Desactivamos Wi-fi, y a continuación usamos el siguiente comando para desbloquear Wifi únicamente para los scripts que vamos a ejecutar a continuación:

```
rfkill unblock wifi
```

```
root@ka:~/krackattacks-scripts/krackattack# rfkill unblock wifi
root@ka:~/krackattacks-scripts/krackattack#
```

Volvemos a reiniciar para evitar errores.
A continuación, compilamos hostpad con el siguiente comando:

cd hostapd
cp defconfig .config
make -j 2

Ya podemos proceder a iniciar la prueba:

```
root@ka:~/krackattacks-scripts/krackattack# python2 krack-test-client.py
[21:50:02] Note: disable Wi-Fi in network manager & disable hardware encryption. Both may interfere wit
h this script.
[21:50:02] Starting hostapd ...
Configuration file: /root/krackattacks-scripts/krackattack/hostapd.conf
Using interface wlan0 with hwaddr 30:b5:c2:10:15:32 and ssid "testnetwork"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
[21:50:06] Ready. Connect to this Access Point to start the tests. Make sure the client requests an IP
using DHCP!
```

Primero procederemos a realizar la prueba con un cliente vulnerable y otro que no debería ser vulnerable ya que está actualizado:

Procedemos a conectarnos a la red:

- SSID: testnetwork
- Password: abcdefgh

Cuando se conecta, el script comienza a ejecutarse viendo los resultados:
Es vulnerable a reinstalación de “pairwise key”:

```
[21:50:25] 9c:d9:17:d1:6e:d8: IV reuse detected (IV=1, seq=4). Client is vulnerable to pairwise key rei
nstallations in the 4-way handshake!
[21:50:26] 9c:d9:17:d1:6e:d8: Hostapd: Resetting Tx IV of group key and sending Msg3/4
[21:50:26] 9c:d9:17:d1:6e:d8: DHCP reply 192.168.100.2 to 9c:d9:17:1e:68:d1
```

Es vulnerable a reinstalación de claves de grupo:

```
[21:51:12] 9c:d9:17:d1:6e:d8: Received 5 unique replies to replayed broadcast ARP requests. Client is v
ulnerable to group
[21:51:12]                    key reinstallations in the 4-way handshake (or client accepts replayed br
oadcast frames)!
```

A continuación, probamos un dispositivo actualizado:

```
[21:52:25] f0:79:60:de:0e:05: client DOESN'T seem vulnerable to pairwise key reinstallation in the 4-wa
y handshake (using standard attack).
```

Observamos como efectivamente no parece vulnerable.

```
[21:52:35] f0:79:60:de:0e:05: client DOESN'T seem vulnerable to group key reinstallation in the 4-way h
andshake.
```

Por lo tanto, se han realizado la prueba con dos dispositivos y hemos detectado que uno de ellos es vulnerable y el otro no.

7.3 Ataques Evil Twin utilizando Linset:

7.3.1 Descripción

El ataque conocido al principio como Evil Twin, se está cambiando su nombre por “Linset” dado que es el nombre la herramienta de WifiSlax que los explota. También, a veces se denominan “wiphising”, ya que son utilizados para realizar ataques tipo “phishing”, en los que se engaña a la víctima para hacer creer que está accediendo a un sitio legítimo, mientras que realmente es un sitio falso controlado por el atacante; para por ejemplo conseguir sus contraseñas bancarias o la contraseña de la red Wifi.

WifiSlax es una distribución GNU/LINUX especializada en la auditoria de redes inalámbricas.
Linset es una herramienta para realizar auditorías de redes inalámbricas, que nos permite realizar ataques de tipo Evil Twin y así conseguir claves WPA/WPA2 sin necesidad de diccionarios ni de otros medios, ya que el propio usuario es el que termina proveyendo la clave al atacante (sin ser consciente de ello).

En el ataque Evil Twin el atacante crea un punto de acceso falso, copiando el SSID del original. La víctima detecta dos AP con el mismo SSID, pero sin embargo no es capaz de diferenciarlos, por lo tanto, se conectará al que detecte más cercano. En el momento que se detecta que la víctima se ha conectado al AP falso, se le dirige a una página web falsa en la que se solicita que escriba la contraseña WPA/WPA2 y así el atacante consigue hacerse con ella. Se recomienda ver a continuación la prueba práctica para comprender mejor este proceso.

El ataque tipo Evil Twin, no tiene fácil solución, y de hecho según lo que se ha visto en cuanto al estándar WPA3 parece que seguirá siendo un problema incluso en esta nueva versión del estándar WPA. Esto se debe, a la complicación de introducir defensas ante este tipo de ataque en el estándar.
Este tipo de ataques se ve afectado de forma negativa por la opción de los clientes wifi de conectarse automáticamente a redes preferidas. Cada vez que un cliente busca redes disponibles a su alrededor, también publica los SSID de las que conoce para ver si se encuentran en su rango, al hacer esto el cliente está exponiendo la lista de las redes que conoce y por lo tanto un atacante podría crear una red con un SSID igual al que está buscando la víctima y no ponerle contraseña, por lo que el cliente se conectaría sin ni siquiera darse cuenta. A continuación, el atacante podría realizar un ataque estilo wiphising.

A continuación, se proponen posibles defensas que nos pueden ayudar a tener un grado más de seguridad en cuanto a este tipo de ataques.

- Comprobación de BSSID. Recordemos que en el apartado 3.6 de este Trabajo, hemos definido el BSSID. (Este nos sirve para identificar el AP, dentro de una WLAN). Desgraciadamente, los clientes Wifi de los Sistemas Operativos Windows y MacOS no comprueban este valor, sino que únicamente comprueban el SSID. Cabe destacar que Windows sí que lo implementaba, pero lo dejó de hacer.

- No conectarse automáticamente a las redes preferidas. Con esto evitaríamos que un atacante pueda crear una red con un SSSID a la que el dispositivo de la víctima se vaya a conectar automáticamente. Desgraciadamente esta solución tiene un impacto muy grande en usabilidad, ya que el usuario se tendría que conectar de forma manual siempre a sus redes preferidas.
- Comprobación de parámetros adicionales. En línea con el anterior concepto de evitar conectarse a redes preferidas falsificadas, los clientes wifi al ir a conectarse a una red wifi preferida podrían comprobar parámetros adicionales como:
    - Localización GPS
    - Redes wifi cercanas
    - Redes móviles cercanas (identificadores de las antes de telefonía móvil)
- Comprobación del AP mediante los intervalos de beaconing. Para estar conectado a un AP, se produce un beaconing entre el AP y el cliente. En este paper proponen identifica los APs modelando el comportamiento del beaconing del AP: https://ieeexplore.ieee.org/document/6901631/
- Utilización de conexión VPN. Aunque la víctima esté conectándose a un AP falso, si utiliza conexión VPN ofrece una capa de cifrado adicional, además de prevenir ataques de wiphising.
- Asumir siempre que la red es insegura. En caso de redes wifi públicas se debe siempre actuar como si todo estuviese siendo controlado por un atacante.

Conclusiones: Podemos ver que la mayoría de medidas que se pueden tomar, se trata de identificar el AP falso. Estos métodos son de identificación del AP, es decir realizar un fingerprinting del AP y mantener estos datos para comprobarlos cada vez que se conecte.

7.3.2 Prueba práctica.

A continuación, se realizará una prueba de concepto, en la que se conseguirá una clave WPA2 mediante un ataque Linset.
Los pasos generales del ataque son:

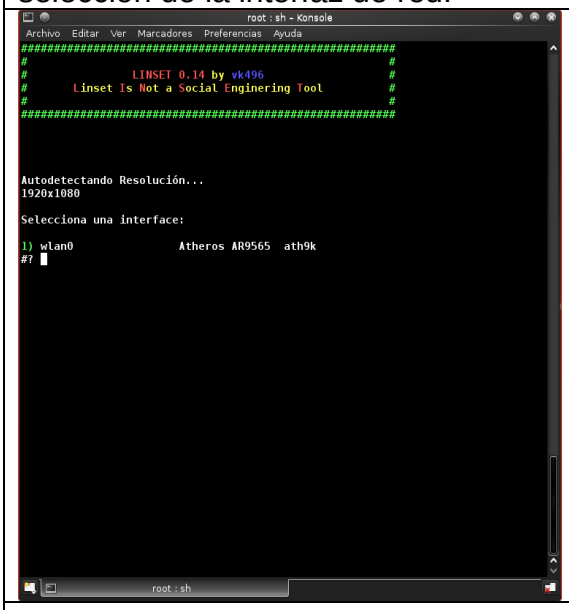
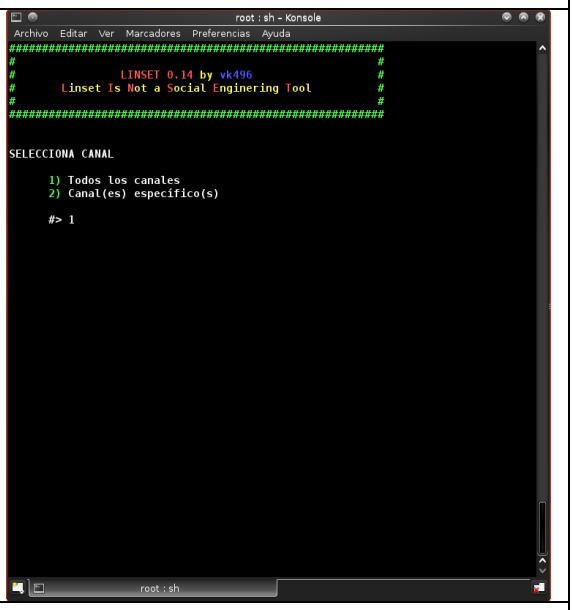
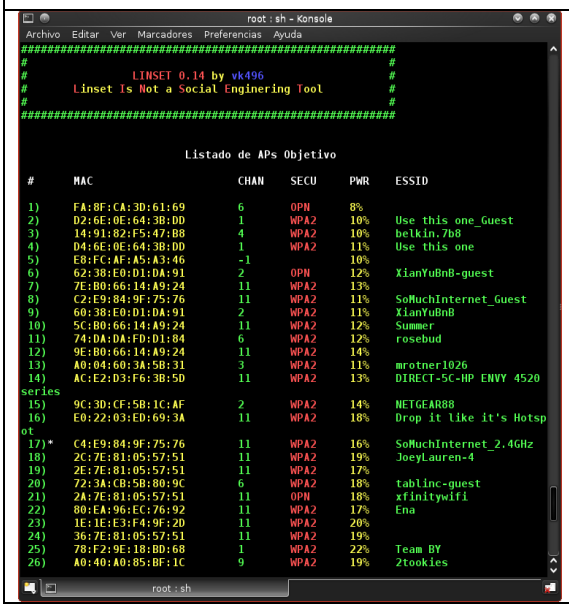
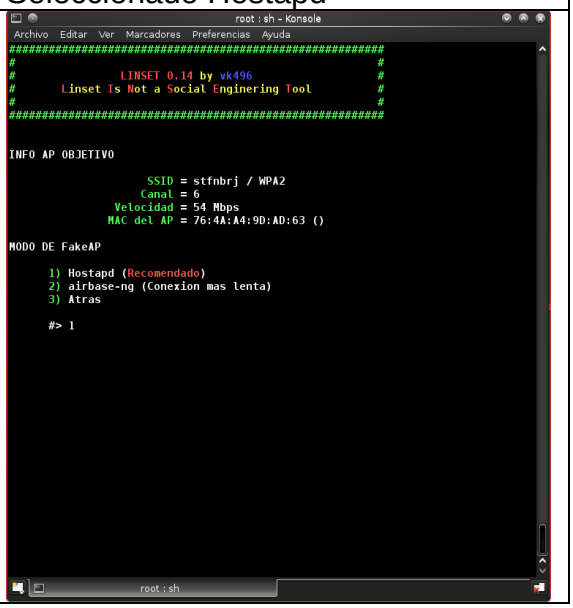
1. Escanear el espectro en busca de redes objetivo
2. Selección de la red objetivo
3. Buscar handshake
4. Configuramos la interfaz web
5. Se monta el falso AP imitando al original
6. Se crea servidor DHCP sobre el falso AP para que asigne IPs automáticamente
7. Se crea un servidor DNS para que redirija todas las peticiones a donde tenemos hospedada la interfaz web
8. Se lanza el servidor web con la interfaz web falsa
9. Se lanza el mecanismo para comprobar la validez de las contraseñas introducidas por las víctimas

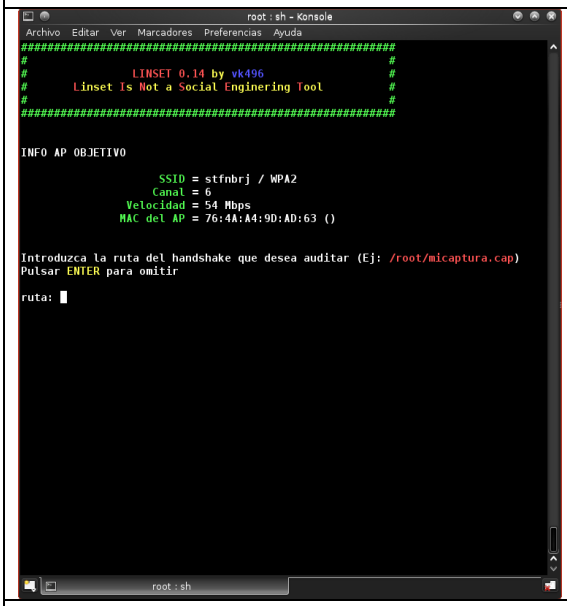
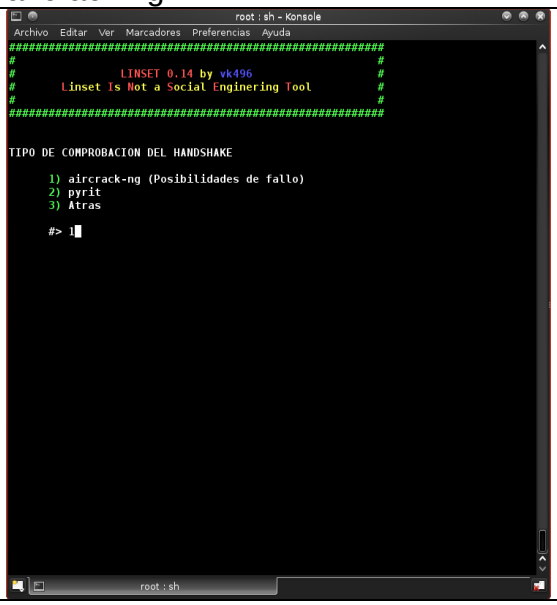
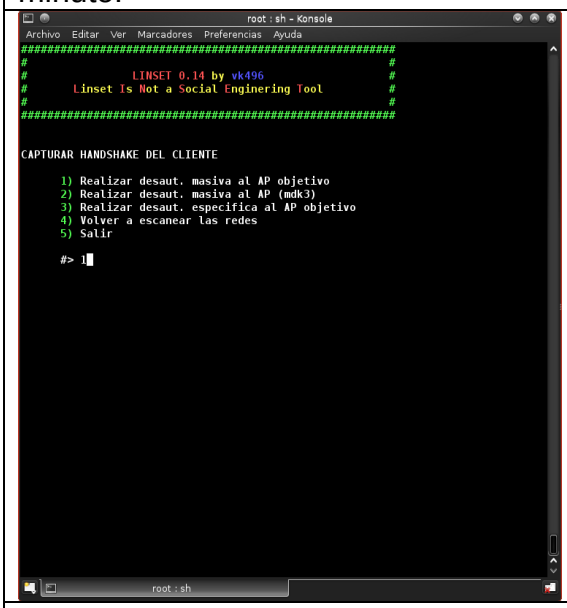
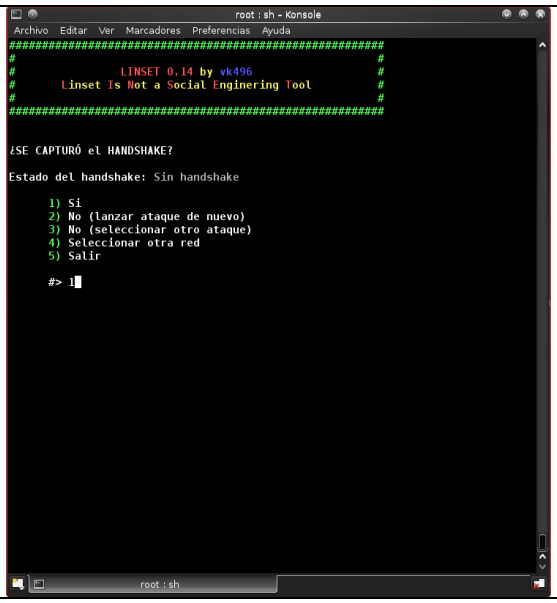
10. Se expulsa a todos los usuarios de la red, para que se conecten a nuestro falso AP
11. Obtenemos la contraseña WPA2

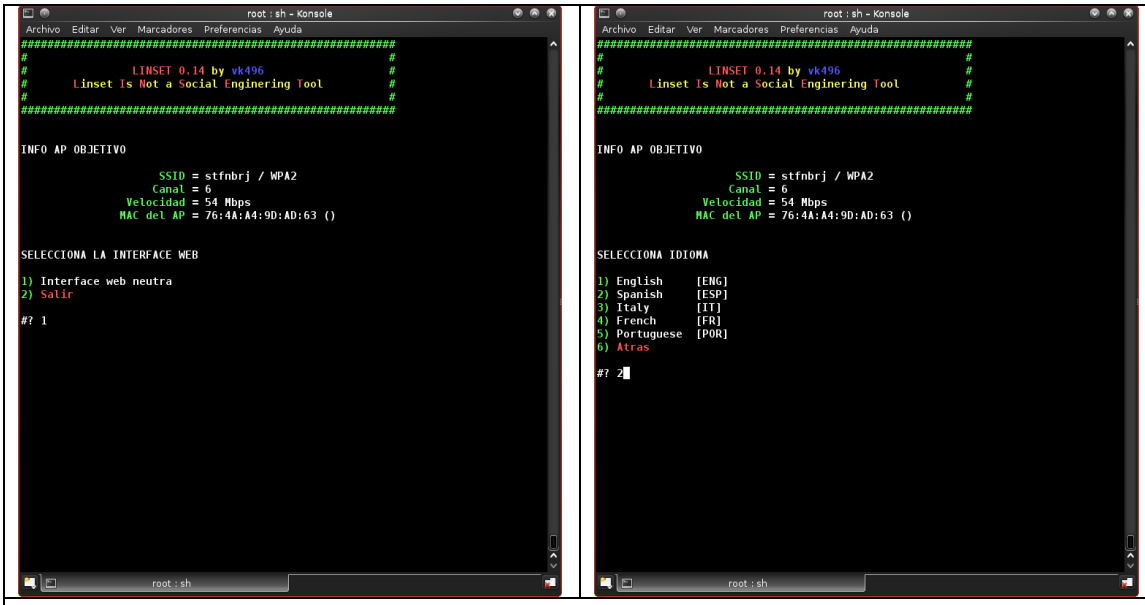
Para realizar las pruebas se ha utilizado:

- USB Live con la ultima versión de WifiSlax
- Antena wifi
- Red propia wifi como objetivo
- Cliente conectado a la red wifi objetivo. MacOS High Sierra

A continuación, se pueden observar los pasos seguidos:

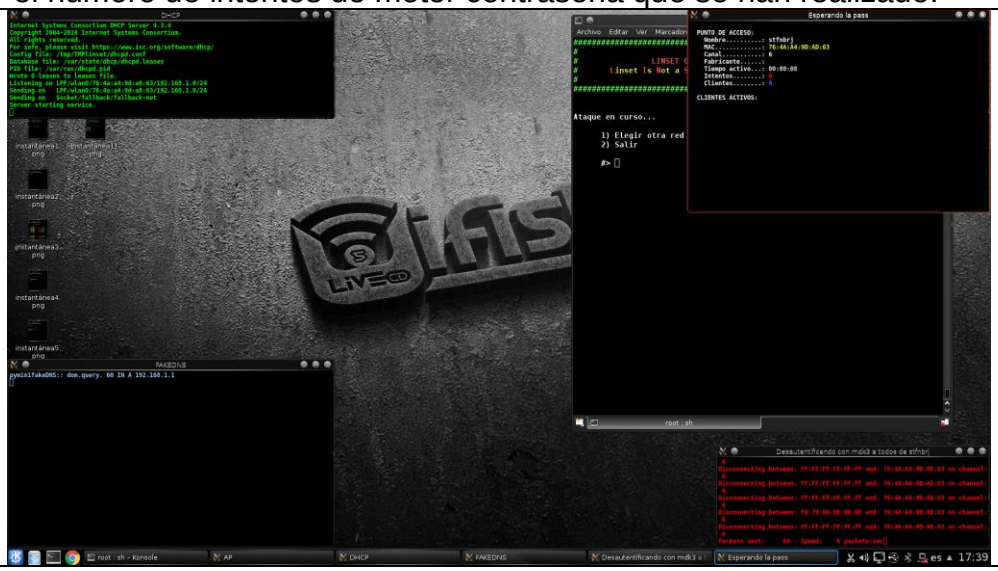
Paso 1:	Paso 2:
Ejecutar Linset (comando: Linset) y selección de la interfaz de red.	Selección de canal
	
Paso 3:	**Paso 4:**
Resultado de escaneo de red	Selección de modo del AP falso. Seleccionado Hostapd
	

Paso 5:	Paso 6:
Selección de AP objetivo	Selección de tipo de comprobación de handshake. Para ello seleccionamos aircrack-ng.
	
Paso 7:	Paso 8:
Realizar desautenticación automática masiva del AP objetivo. Al presionar enter, nos saldrá una imagen de captura de datos del canal. Esperamos aproximadamente 1 minuto.	Comprobamos que nuestro cliente objetivo (en este caso el MacOS High Sierra) y una vez conectado de nuevo al AP falso, se indica que sí se ha capturado el handshake.
	
Paso 9:	Paso 10:
Seleccionamos la interfaz web neutra básica.	Seleccionar el idioma de la página web a la que se redirigirá a las víctimas.



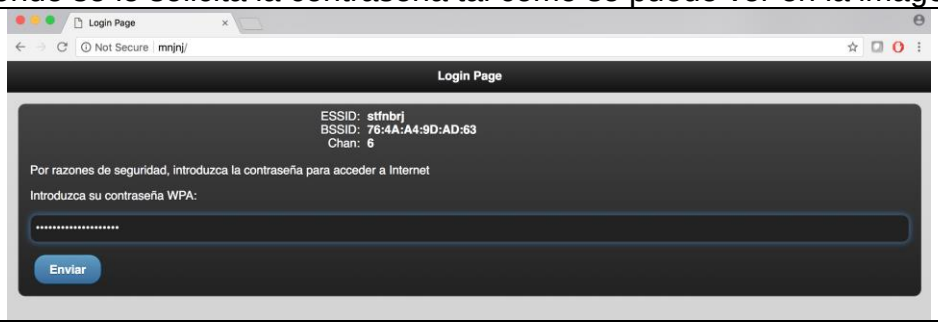
Paso 10:

Podemos ver que el ataque se está ejecutando. En la ventana de arriba a la derecha observamos el número de víctimas que tenemos conectado a nuestro AP y el número de intentos de meter contraseña que se han realizado.



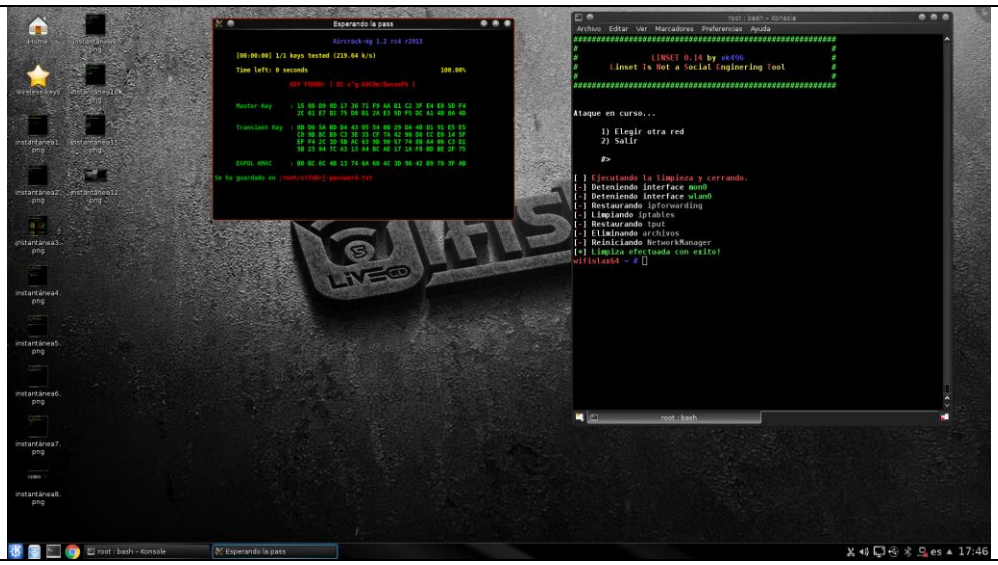
Paso 11:

El cliente intenta acceder a Google y sin embargo es redirigido a la interfaz web donde se le solicita la contraseña tal como se puede ver en la imagen:



Paso 12:

Ataque realizado con éxito y clave WPA2 conseguida.



7.4 Ataque basados en diccionario a partir del 4-way handshake

La prueba de concepto que se realiza a continuación consiste en capturar el handshake de la red objetivo y utilizar un ataque de diccionario para descifrar la contraseña de acceso a la red.

Para la realización de esta prueba práctica se utiliza:

- Máquina Kali Linux con acceso a interfaz wifi que acepte modo monitor
- Punto de Acceso a una red con seguridad:
  - WPA2/AES-PSK
- Diccionario de contraseñas

A continuación, se detallan los pasos seguidos:

Paso 1:
Activar modo monitor en la interfaz deseada. En este caso utilizaremos la interfaz wlan0.

```
root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
 1125 NetworkManager
 1174 wpa_supplicant
 2549 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k           Qualcomm Atheros QCA9565 / AR9565 Wireless Network Adapter (rev 01)

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

Paso 2:
Encontrar nuestra red objetivo y recoger información (Canal, BSSID y ESSID) El nombre de la interfaz wifi en este caso se llamaba wlan0. Al activar el modo monitor este nombre cambia a: wlan0mon Comando: airodump-ng wlan0mon En la siguiente imagen podemos ver nuestra red objetivo

```
CH  7 ][ Elapsed: 6 s ][ 2018-06-12 15:22

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

FA:8F:CA:79:E5:C9  -87        2        0    0  11  54e. OPN              <length:  0>
AE:B0:66:14:A9:24  -82        2        0    0  11  54e. WPA2 CCMP   PSK  <length:  0>
BA:CA:33:88:47:9C  -31        9        8    0   1  54e  WPA2 CCMP   PSK  iPhone
F0:99:BF:0B:43:08  -35       20        0    0  11  54e  WPA2 CCMP   PSK  Cloud 8
76:4A:A4:9D:AD:63  -42       17        2    0   6  54e  WPA2 CCMP   PSK  stfnbrj
DC:A4:CA:EC:9D:12  -53       15        0    0  11  54e  WPA2 CCMP   PSK  SinX
```

Paso 3:

Capturar el handshake: Para ello utilizaremos la herramienta airodump tal como se ve en la imagen siguiente. Para poder obtenerlo un dispositivo cliente tendría que autenticarse a la red. También se podría expulsar a los clientes para obligarles a que se vuelvan a autenticar.
Cuando se ha obtenido el handshake se puede ver en la esquina superior derecha lo recuadrado en rojo en la imagen siguiente.
Comando: aurodump-ng -c 6 --bssid 76:4A:A4:9D:AD:63 -w namefile wlan0mon

```
CH  6 ][ Elapsed: 30 s ][ 2018-06-12 15:24 ][ WPA handshake: 76:4A:A4:9D:AD:63

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

76:4A:A4:9D:AD:63  -45 100      304       47    1   6  54e  WPA2 CCMP   PSK  stfnbrj

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

76:4A:A4:9D:AD:63  F0:79:60:DE:0D:D6  -30    0e-24      0      210
76:4A:A4:9D:AD:63  50:C7:BF:95:BD:A9  -51    1e- 1e     8       97  stfnbrj
76:4A:A4:9D:AD:63  88:C2:55:2D:7A:90  -54    1e- 1e     0       12
```

Paso 4:

Realizar el ataque de diccionario al handshake capturado. Existen múltiples opciones, en este caso utilizaremos aircrack-ng y el diccionario deseado.
Comando: aircrack-ng -a2 -b 76:4A:A4:9D:AD:63 -w listapass.txt namefile.cap
Cuando se encuentre la contraseña se verá una imagen como la siguiente:

```
                    Aircrack-ng 1.2 rc4

  [00:00:00] 4/3 keys tested (263.54 k/s)

  Time left: 0 seconds                                      133.33%

                      KEY FOUND! [ 85878722 ]


  Master Key     : 91 4B 48 4E 60 BA 1E E7 C7 55 13 EA C5 DE A4 44
                   BB A2 62 10 97 2F 25 24 EF 37 6F B4 98 59 0F 6B

  Transient Key  : BC 39 B9 50 FB 38 C2 85 0F 71 3D F3 91 3B 98 0A
                   07 78 71 7E 7A 13 91 9B D1 D7 27 8F 65 2A 75 44
                   45 4F B5 66 D8 35 A9 A8 53 F9 C6 83 BC 91 EB 8E
                   F5 4A 5A 9E BC 66 0B B7 15 BF 55 21 1A 5A 87 5A

  EAPOL HMAC     : 3E 1E 24 D1 B2 CF 9B A4 4F 7E 9B B2 93 B0 0A 07
```

Con esta prueba prácticamente, queda demostrado que los estándar WPA tienen la vulnerabilidad de que la seguridad recae en un nivel alto sobre la complejidad de la clave configurada. A mayor complejidad, más segura será la red.

8. Conclusiones

En el desarrollo de este trabajo se ha adquirido gran cantidad de conocimiento sobre el funcionamiento y seguridad de las redes inalámbricas Wifi.

Con el desarrollo de este trabajo se ha demostrado la necesidad que existe del nuevo estándar WPA 3 y las garantías mínimas que debía proporcionar. Se ha encontrado que este estándar sigue aún en desarrollo y que la Wifi Alliance no ha liberado gran cantidad de información sobre el mismo. WPA 3 proveerá un handshake más seguro incluso cuando los usuarios utilicen contraseñas débiles, ofrece un reemplazo a WPS mediante un nuevo protocolo denominado DPP, proporciona una mejora en el cifrado no autenticado y un aumento en el tamaño de las claves de sesión.

Estudiando las vulnerabilidades y ataques comunes en todos los estándares de seguridad, se desaconseja eliminar el uso de WEP y al utilizar seguridad WPA2 hacerlo con contraseñas complejas, cambiándolas periódicamente.

Otro de los temas más actuales estudiados ha sido el de los ataques de reinstalación de claves, denominados KRACK (“Key Reinstallation Attacks”). Se ha visto que este ataque es potencialmente dañino ya que afecta a prácticamente todos los dispositivos. Esto es debido a que el fallo está en la propia definición del estándar. Sin embargo, con una actualización de software se ha podido solucionar en la gran mayoría de dispositivos. La vulnerabilidad se ve limitada por dos conceptos: el atacante necesitar estar cerca de la víctima, y únicamente sirve para descifrar tráfico de las víctimas, no para conseguir la clave de acceso a la red.
Aunque el equipo de investigadores se suponía que iba a liberar más información sobre la vulnerabilidad y cómo explotarla, no lo han publicado a la finalización de este proyecto. Se han realizado pruebas prácticas para detectar si un cliente Wifi es vulnerable o no, de las que hemos podido observar que efectivamente un teléfono Android sin actualizar sí que es vulnerable.

Como proposición de trabajo futuro se propone una aplicación para dispositivos cliente de redes inalámbricas wifi. Este programa debe añadir más elementos de seguridad, como añadir más controles al conectarse a redes conocidas, obligar a que todas las comunicaciones inalámbricas sean a través de VPN entre otras. Además, queda pendiente, estudiar cómo es la versión final del estándar WPA3 a su vez que los ataques tipo KRACK.

9. Glosario

AES: Advanced Encryption Standard
AP: Access Point
ARP: Address Resolution Protocol
BSSID: Basic Service Set Identifier
BSS: Basic Set Service
CRC: Cyclic Redundancy Code
EAP: Extensible Authentication Protocol
EEP: Extended Service Set
FCC: Federal Communications Commision
Hz: Hertz
ICV: Integrity Check Value
IBSS: Independent Basic Service Set
IEEE: Institute of Electrical and Electronics Engineers
INE: Instituto Nacional de Estadística
IP: Internet Protocol
IV: Initialitation Vector
ICV: Integrity Check Value
KRACK: Key Reinstallation Attacks
MAC: Media Access Control
MIC: Message Integrity Code
MiTM: Man in The Middle
ONTSI: Observatorio Nacional de Telecomunicaciones y SI
OSA: Open System Authentication
PEAP: Protected Extensible Authentication Protocol
PMK: Protected Management Frames
PMK: Clave maestra por pares
PSK: Pre-shared Key
PRGA: Pseudo Random Generation Algorithm
PRNG: Pseudo random-number generator
RADIUS: Remote Authentication Dial In User Service
RC4: Ron’s Cipher 4
RSN: Robust Security Network
SAE: Simultaneous Authentication of Equals
SKA: Shared Key Authentication
SSID: Service Set Identifier
TKIP: Temporal Key Integrity Protocol
VPN: Virtual Private Network
WEP: Wired Equivalent Privacy
WLAN: Wireless Local Area Network
WPA: Wi-fi Protected Access
WPS: Wi-fi Protected Setup

10. Bibliografía

[1] Instituto Nacional de Estadística, «Nota de Prensa. Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares,» España, 2017.

[2] Observatorio Nacional de Telecomunicaciones y SI, «Las TIC en los hogares espanoles. Estudio de demanda y uso de Servicios de Telecomunicaciones y Scoeidad de la Informacion.,» ONTSI, 2017.

[3] ONTSI, «CIBERSEGURIDAD Y CONFIANZA EN LOS HOGARES ESPAÑOLES,» 2017.

[4] https://www.wi-fi.org, marzo 2018

[5] https://superuser.com/questions/1086226/what-does-the-fi-in-wi-fi-mean, marzo 2018

[6] https://www.webopedia.com/DidYouKnow/Computer_Science/wifi_explained.asp, marzo 2018

[7] https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Alliance_2017_Annual_Report.pdf, Mayo 2018

[8] https://en.wikipedia.org/wiki/IEEE_802.11#Channels_and_frequencies, febrero 2018

[9] https://pdfs.semanticscholar.org/93dc/7c3ad36eb2e258d422185cc1593e31005570.pdf, Mayo 2018

[10]: https://www.homenethowto.com/wireless/wi-fi-standards/, abril 2018

[11]: C. Siva Ram Murthy and B. S. Manoj, Ad hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR, May 2004. ISBN 978-0-13-300706-0

[12]: https://www.juniper.net/documentation/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-ssid-bssid-essid.html, Abril 2018

[13] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements, Mayo 2018

[14] https://pdfs.semanticscholar.org/8aeb/2a27abc2a1d0a8b71047606fbeec0f711e03.pdf, Mayo 2018

[15] Arash Habibi Lashkari, Masood Mansoor, Amir Seyed Danesh. «Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). » Singapore. https://ieeexplore.ieee.org/abstract/document/5166826/

[16] http://www.elladodelmal.com/2018/03/wild-wild-wifi-dancing-with-wolves-3.html, abril 2018