Redes de Computadores

Proyecto: Seguridad en Redes Wifi

Alumnos:

- Gonzalo Vera Portilla
- Cristian Wiche Latorre
- Pedro Zepeda Pozo

Profesor: Agustín González

Redes de Computadores

Índice

1. Introducción **3**

2. Descripción tecnologías existentes y su seguridad **3**
2.1. WEP . . . 3
2.2. WPA . . . 4
2.3. WPA2/802.11i . . . 4

3. Vulnerabilidades, ataques y recomendaciones de seguridad **4**
3.1. WEP . . . 4
3.1.1. Debilidad del vector de inicialización . . . 4
3.1.2. Ataques a redes WEP . . . 5
3.2. WPA . . . 5
3.3. WPA2/802.11i . . . 5
3.3.1. WPS . . . 5
3.4. Recomendaciones generales de seguridad para redes Wifi . . . 6

4. Resultado de los ataques **7**
4.1. WEP . . . 7
4.2. WPA2 con WPS . . . 8

5. Conclusiones **8**

6. Anexos **9**

Resumen

En la sociedad actual las comunicaciones juegan un rol fundamental, ya sea para hablar por celular, descargar información de internet, ver televisión satelital o escuchar radio, el humano está rodeado de señales inalámbricas. Por ese motivo es que a grandes rasgos en este proyecto se analizó la seguridad de una de las redes más usadas, que es la Wifi. En particular, se estudiará las redes WEP, WPA, WPA2 además mencionaremos la tecnología WiMax. Se explicará a grandes rasgos la teoría detrás de cada encriptación y como ha sido la evolución desde WEP hasta la encriptación actual, y porqué se siguen usando métodos poco seguros hasta el día de hoy. Ya que sabemos que a través del uso malicioso de cada una de estas redes, un hacker o un atacante pueden dañar de manera significativa no solo al dispositivo atacado, sino al propio usuario que hace uso de él. Evidentemente no nos estaremos refiriendo a un daño físico, sino a un daño de robo de identidad, de dinero, de información personal u otros. Analizaremos cuáles son los posibles ataques que se pueden hacer a las distintas seguridades, y cómo funcionan, así como también probar la seguridad de nuestra propia red casera, mencionando finalmente cuales son las posibles medidas de seguriad a tomar para disminuir el riesgo de ataques.

1. Introducción

La intención o finalidad de este proyecto ha sido la de realizar un estudio completo de las seguridades típicamente usadas en Wifi, y hacemos mensión a la seguridad WiMax. Asimismo también se ha querido demostrar y explicar cómo defenderse de estos ataques y que pautas o medidas son recomendables para evitar todos estos. Es decir, este proyecto se podría definir como una guía o manual en el que se muestran los ataques y problemas más comunes para cada una de las redes, donde además se darán una serie de soluciones, consejos y recomendaciones, aunque por supuesto habiendo estudiado con anterioridad que son y cómo se comportan cada una de estas redes.

- Lo que se persigue principalmente con la lectura de este proyecto es que todo aquel usuario que lo lea haya adquirido conocimientos sobre:
- Que son, cuales son las ventajas y desventajas, y como trabajan las 5 redes estudiadas, en especial Wifi y Wimax.
- Cuál es la seguridad implementada por cada red y que mecanismos utilizan cada una de estas.
- Que ataques son más comunes en cada una de las redes y que medidas hay que llevar a cabo para evitar estos.
- Que problemas pueden ofrecer generalmente los dispositivos hardware de las diferentes redes y cuáles pueden ser las posibles causas y soluciones.
- Como configurar manualmente dispositivos para lograr una óptima seguridad.
- Cuáles son las diferencias entre Wifi y Wimax.
- Que programas de software son recomendables para garantizar la seguridad de los equipos.

2. Descripción tecnologías existentes y su seguridad

2.1. WEP

WEP o Wired Equivalente Privacy es el algoritmo opcional de seguridad para ofrecer protección a las redes inalámbricas incluido en la primera versión del IEEE 802.11.

El estándar 802.11 ofrece mecanismos de seguridad mediante procesos de autenticación y de cifrado. En el modo Ad Hoc la autenticación puede realizarse mediante un sistema abierto o mediante un sistema de clave compartida. Un punto de acceso que reciba una petición podrá conceder autorización a cualquier estación o solo a aquellas que estén permitidas. Como bien hemos visto en un sistema de clave compartida tan solo aquellas estaciones que posean una llave cifrada serán autenticadas. [2]

WEP emplea el algoritmo RC4 de RSA Data Security, y es utilizado para cifrar las transmisiones realizadas a través del aire. El estándar define el uso de RC4 con claves semillas (seeds) de 64 y/ó 128 bits, de los cuales 24 bits corresponden al vector de inicialización (IV – Inicialization Vector) y el resto, 40 ó 104 bits, a la clave secreta compartida entre emisor y receptor. El IV se genera dinámicamente y debe ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes, para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo ésta. Como es lógico, ambos extremos deben conocer tanto la clave como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en claro dentro de la propia trama al otro extremo, por lo que también será conocido. Lo anterior se puede observar con mayor claridad en la figura 3 adjuntada en el Anexo. [9]

2.2. WPA

WPA es el protocolo posterior a WEP, el cual nació como contramedida a las grandes falencias que poseía WEP con respecto a diversos ataques bastante comunes hoy en día y que son fácilmente realizables dentro de un hogar con un computador común y corriente y con software que se encuentra rondando libremente por internet.

WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como contramedida a la débil seguridad en las redes mientras 802.11i era finalizado. WPA fue creado por la Wi-Fi Alliance, la cual es una asociación comercial mundial que es formada por una gran red de compañías que trae WiFi y estandariza su uso.[7] La IEEE es una organización de consenso de construcción de aparatos electrónicos que diseña, implementa y avanza la tecnología global. Su trabajo encamina la funcionalidad, capacidades e interoperabilidad de una larga variedad de productos y servicios. El protocolo IEEE 802.11i está dirigido a batir la vulnerabilidad de la seguridad que sufrían en ese entonces las redes de computadores con respecto a sus protocolos de autenticación y de codificación. Se utiliza en Wi-Fi Protected Access (WPA2) luego de su implementación en Internet. WPA adopta la autenticación de usuarios utilizando una contraseña pre compartida entre todos los equipos de la red, que de un modo similar al WEP (TKIP), requiere introducir la misma clave en todos los equipos. El proceso de TKIP comienza con una clave temporal de 128 bits que es compartida entre los clientes y los puntos de acceso, luego, se combina la clave temporal con la dirección MAC de cada uno de los hosts y después de esto agrega un vector de inicialización, al igual que con WEP, para producir la contraseña de encriptación, la diferencia radical con el anterior método es la longitud de este (48 bits). Este procedimiento asegura que cada estación utilice diferentes claves para cifrar los datos. Gracias a estos procedimientos la contramedida mientras se implementaba el nuevo protocolo sirvió de respaldo enorme a la seguridad informática ya que logro destruir varios métodos de ataques en el cual WEP era muy vulnerable, como se mencionaba al principio. Otra gran diferencia con WEP es que cambia las claves temporales cada 10.000 paquetes, evitando asi que el atacante tenga mucha información para poder descifrar la clave precompartida. Además, WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas, así pues impide que otros dispositivos envíen tramas ya adoptadas por el dispositivo que recibe. [3]

2.3. WPA2/802.11i

WPA2 es el nombre dado por la Wifi Alliance a la segunda fase del estándar IEEE 802.11i. La seguridad es mucho más fuerte y robusta en comparación con el protocolo WPA. WPA2 ya no se basa en un parche temporal sobre el algoritmo RC4 sino que utiliza el algoritmo de encriptación AES. Dicho algoritmo requiere un hardware mucho más robusto que los anteriores protocolos por lo que algunos puntos de acceso antiguos no pueden utilizar dicho protocolo. [12]

La implementación de protección que se aplica en el estándar de seguridad Wifi 802.11a se conoce con el acrónimo CCMP y está basada en el algoritmo AES. El cifrado que se utiliza es una cifrado simétrico de 128 bits y el vector de inicialización tiene una longitud igual que en el WPA, es decir de 48 bits.

3. Vulnerabilidades, ataques y recomendaciones de seguridad

Vamos a ver a continuación los diferentes ataques que pueden afectar a cada una de las tecnologías estudiadas, así como las correspondientes recomendaciones de seguridad.

3.1. WEP

Mostramos a continuación las debilidades del protocolo WEP

3.1.1. Debilidad del vector de inicialización

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. Recordemos que el IV es la parte que varía de la semilla (seed) para impedir que un posible atacante recopile suficiente información cifrada con una misma clave. El estándar 802.11 no especifica cómo manejar el IV. En principio se debería cambiar en cada trama para mejorar la privacidad, pero no es obligatorio, por lo tanto cada fabricante elije como tratar el IV y la mayoría de ellos optan por fijar el IV a 0 cada vez que arrancamos la tarjeta e incrementarlo a 1 para cada trama enviada. Esto provoca que las primeras combinaciones de IVs y clave secreta se repitan muy a menudo.
Además de todo esto, sabemos que el número de IVs diferentes no es demasiado elevado (224=16 millones aprox.), por lo que terminarán también repitiéndose al cabo de horas o días dependiendo del tráfico de la red. Con esto llegamos a la conclusión de que la repetición tarde o temprano se producirá. La cantidad de repeticiones dependerá de la implementación que elija cada fabricante para variar el IV (aleatoria, secuencial, etc.) y de la carga de la red.[9]

3.1.2. Ataques a redes WEP

Como bien se ha dicho a lo largo del proyecto el protocolo de seguridad WEP es totalmente inseguro en cuanto a protocolos de seguridad. Hay principalmente dos métodos de romper la seguridad en este protocolo y por consiguiente obtener su clave, mediante fuerza bruta y mediante crackeo.
El método de fuerza bruta consiste tan solo en ir probando una tras otra posibles combinaciones de claves hasta dar con la correcta. Cabe decir que este método además de poder ser poco efectivo es muy lento.

El otro método, el método de crackeo, averigua la clave aplicando el proceso de cracking a un conjunto de paquetes #data capturados previamente. Para capturar esto paquetes se suele inyectar paquetes ARP con el fin de que se genere movimiento de tráfico en la red y poder así hacer una mayor captura de paquetes.

3.2. WPA

La vulnerabilidad en la tecnología WPA es un caso particular que se ha hecho mas popular ultimamente a medida que avanza la tecnología de ataques, el llamado ¨Dictionary Attack¨ en el cual el atacante intenta descifrar la clave contenida en el Handshake la cual es una combinación encriptada de la clave de acceso. El Ataque Diccionario intenta forzar la clave ¨adivinando¨ la frase que generalmente es una combinación de palabras y números usados comúnmente, asi pues, entre mas grande sea el Diccionario que contenga el programa descifrador mas posibilidades tiene de encontrar la clave. El mayor problema que tiene este tipo de ataque es que la información de la clave solo se puede obtener en el ¨handshake¨ entre el servidor y el usuario, por lo tanto no es un ataque rápido, requerirá de que un usuario se conecte durante el periodo que uno busca obtener la clave, o forzando la desconexión del host Asi pues, Robert Moskowitz declara en ¨Debilidad en la selección de la clave en la interface WPA¨ que ¨La clave utilizada con menos de 20 caracteres es muy poco probable que evada ataques. . . ¨[13]

La ruptura de claves WPA se basa en dos pasos, capturar el handshake y el crackeo mediante diccionario.

Cada vez que un cliente se conecta a una red con cifrado WPA, envía un paquete-saludo, o Handshake al AP al que se va a conectar, donde este paquete-saludo contiene la contraseña encriptada que se desea obtener.
El handshake solo se puede capturar exclusivamente cuando un cliente se conecta al punto de acceso. Por tanto se abren dos posibilidades, esperar pacientemente a que el cliente se desconecte y se vuelva a conectar, o bien, forzar la desconexión del cliente utilizando un ataque de desautenticación (es esto último lo que siempre se suele hacer).

Una vez obtenido el handshake (no se suele obtener a la primera por lo que es muy probable que se tenga que intentar varias veces) tan solo quedara crackear este mediante un diccionario. No obstante no basta con utilizar cualquier diccionario, ya que cuanto más tamaño y combinaciones tenga el diccionario más posibilidades habrá de encontrar la clave buscada.

3.3. WPA2/802.11i

En enero de 2001, el grupo de trabajo i task group fue creado en IEEE para mejorar la seguridad en la autenticación y la encriptación de datos de WPA. [12]

3.3.1. WPS

La idea de WPS no es la de añadir más seguridad a las redes WPA o WPA2, sino facilitar a los usuarios la configuración de la red, sin necesidad de utilizar complicadas claves o tediosos procesos.[1]

WPS contempla cuatro tipos de configuraciones diferentes para el intercambio de credenciales:

- PIN: tiene que existir un PIN asignado a cada elemento que vaya a asociarse a la red. Es necesaria la existencia de una interfaz (pantalla y teclado) para que el usuario pueda introducir el mencionado PIN.
- PBC: la generación y el intercambio de credenciales son desencadenados a partir que el usuario presiona un botón (físico o virtual) en el Router y otro en el dispositivo a conectar. Este método tiene un pequeño problema y es que en el corto lapso de tiempo entre que se presiona el botón en el Router y se presiona en el dispositivo, cualquier otra estación próxima puede ganar acceso a la red.
- NFC: intercambio de credenciales a través de comunicación NFC. La tecnología NFC, permite la comunicación sin hilos entre dispositivos próximos (0 - 20 cm.). Entonces, el dispositivo se tiene que situar al lado del Router para desencadenar la autenticación. De esta manera, cualquier usuario que tenga acceso físico al Router, puede obtener credenciales válidas.

- USB: con este método, las credenciales se transfieren mediante un dispositivo de memoria flash (pendrive) desde el Router al dispositivo a conectar.

El sistema de PIN de esta tecnología WPS puede ser reventado en poco tiempo, debido a un error en el diseño del sistema WPS, por el que el router "avisa" de que estamos fallando, tras solo comprobar los cuatro primeros dígitos de ese número de identificación personal de ocho bits.

Mediante un ataque por fuerza bruta, nos llevaría entre dos y diez horas descifrar los 8 números del PIN del WPS del router, pues con ese error la seguridad pasa de 100.000.000 de posibilidades a solo 11.000, debido a que solo hay que "acertar" con dos grupos de números por separado: uno de cuatro y otro de tres, pues el último es solo un checksum.

Lo primero decir que la finalidad es conseguir la clave WPA mediante la obtención del PIN del Router. Ese número de 8 dígitos (7 + el checksum) que se encuentra habitualmente en una etiqueta pegada al dispositivo, aunque tambien puede ser cambiado por el usuario del Router.

Al lanzar el ataque, se realizan los siguientes pasos:

- Petición de autenticación
- Petición de asociación
- Petición de EAP

Al finalizar estas peticiones y sus respectivas respuestas, el algoritmo comienza a realizar intentos por descifrar el PIN. Despues de varios ciclos, obtiene los primeros cuatro dígitos y posteriormente el número entero.
Existen dos herramientas para realizar este ataque Wpscrack y Reaver, el sistema utilizado es similar. La diferencia es que Reaver funciona con más adaptadores pero es un poco más lento.
[1]

3.4. Recomendaciones generales de seguridad para redes Wifi

1. Utilizar un cortafuegos debidamente configurado.
2. Apagar el receptor Wifi cuando no se esté utilizando la red. Aunque ya no estemos haciendo uso de internet nuestro dispositivo seguirá vinculado con el punto de acceso.
3. Cifrar todo tipo de archivo confidencial o que contenga información sensible.
4. No escribir información privada o sensible, como por ejemplo información bancaria o personal.
5. En caso de que sea imprescindible enviar información sensible asegurarse de que el sitio web receptor utiliza SSL (en caso afirmativo contara con un icono de candado en la esquina derecha de la barra del navegador o el nombre http terminara en s, es decir https).
6. Desactivar Wi-Fi Ad-hoc, con el fin de evitar que nuestro dispositivo se conecte a otro dispositivo que no conocemos.
7. Utilizar una red privada virtual o VPN.
8. Evitar las conexiones automáticas a redes Wi-fi, ya que si no se correría el riesgo de conectarse a red Wifi abierta que fuese maliciosa.
9. Instalar y configurar debidamente un antivirus.
10. Desconfiar de posibles descargas de aplicaciones Wifi. Estas aplicaciones suelen ser programas maliciosos.
11. No usar la misma contraseña en diferentes sitios, puesto que si una persona obtuviese esta contraseña podría entrar en varios sitios y no solo en uno.
12. Instalar programas opcionales de cifrado. Estos programas aumentan la seguridad de manera que obligan a cifrar todos los datos que se envíen (Force-TLS y HTTPSEverywhere).
13. Desactivar la opción de compartición de archivos.
14. Utilizar autenticación de dos pasos, siendo esta mucha más segura que la autenticación por contraseña única.

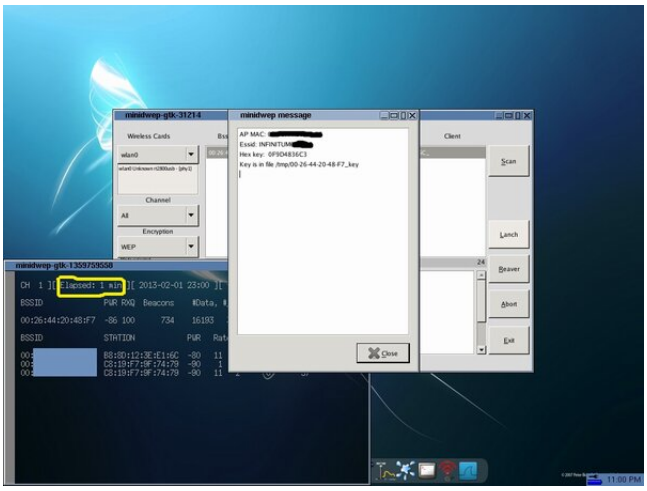
4. Resultado de los ataques

4.1. WEP

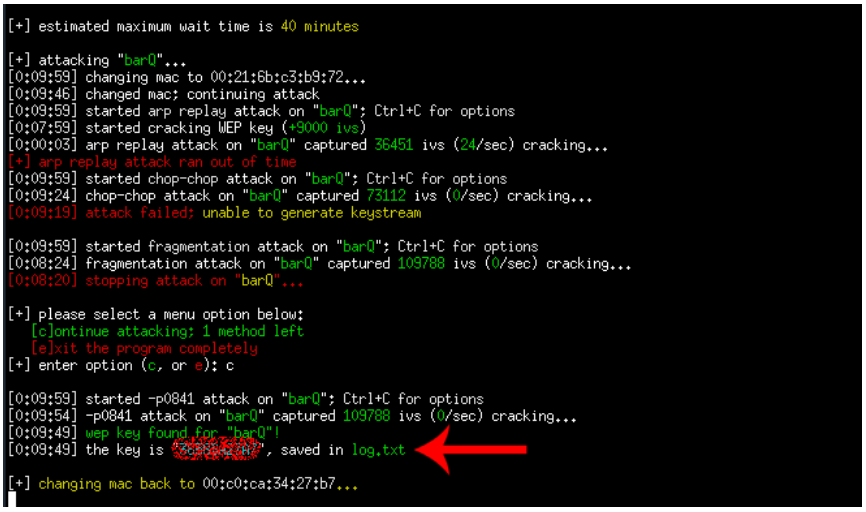
Como ya se mencionó anteriormente, la seguridad WEP es la más facil de descifrar. Para probar éste metodo se uso el programa minidwep de XiaoPan, que lo que hace es:

1. Capturar paquetes 802.11 que circulan por la red de una manera pasiva.
2. Si lo anterior no funciona, hay que actuar de manera activa, esto quiere decir inyectar paquetes.
3. Contiene una erramienta de criptoanálisis que nos permite recuperar la clave a partir de la captura mediante airodump-ng de paquetes cifrados

Primero buscamos todas las redes al alcance de nuestra antena. Un breve resumen se muestra en la figura 4



(a) Xiaopan buscando redes WEP

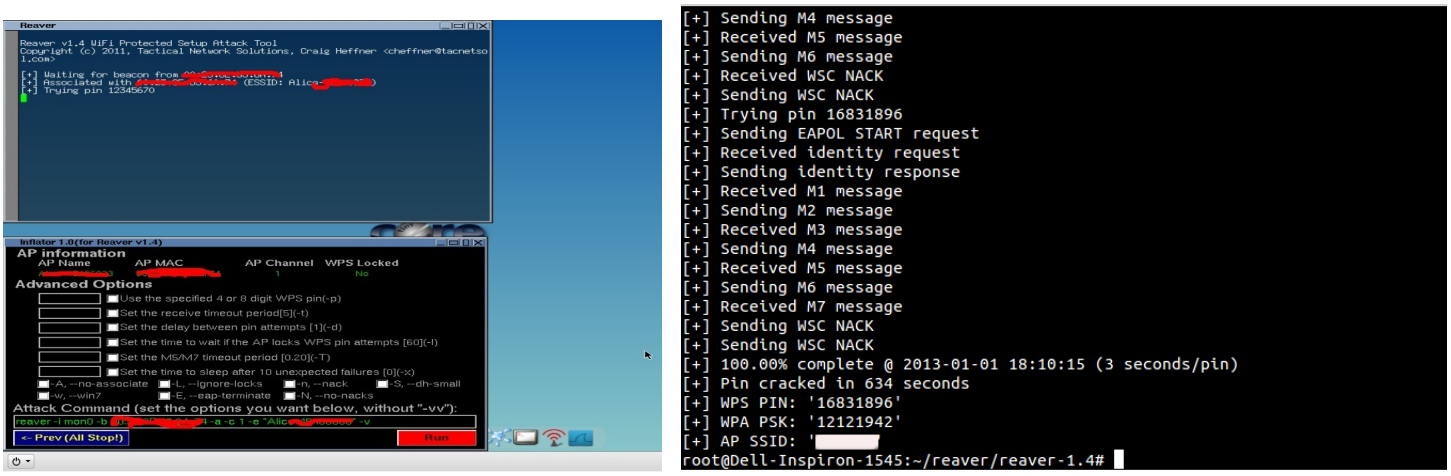


(b) Llave encontrada por pin

Figura 1: Pantalla con clave WEP desencriptada

4.2. WPA2 con WPS

Para poder obtener la clave de una red WPA2 lo más común (y usualmente más útil) es mediante sucesivos intentos por obtener una conexión mediante pin con el router. Se van probando una serie de combinaciones hasta que se encuentra la correcta, el router acepta la conexión y se obtiene la clave. Para esta demostración, igual se usa XioPan, ahora con la herramienta Reaver.



(a) Xiaopan asociando pin

(b) Pin crackeado

Figura 2: Pantalla con clave WPA desencriptada

5. Conclusiones

Como bien se ha visto a lo largo del proyecto, ninguna tecnología o red inalámbrica se puede considerar cien por cien segura, ya sea por las vulnerabilidades que pueda presentar cada una de estas o por el continuo intento por parte de hackers de intentar vulnerar y encontrar cada punto débil de estas.

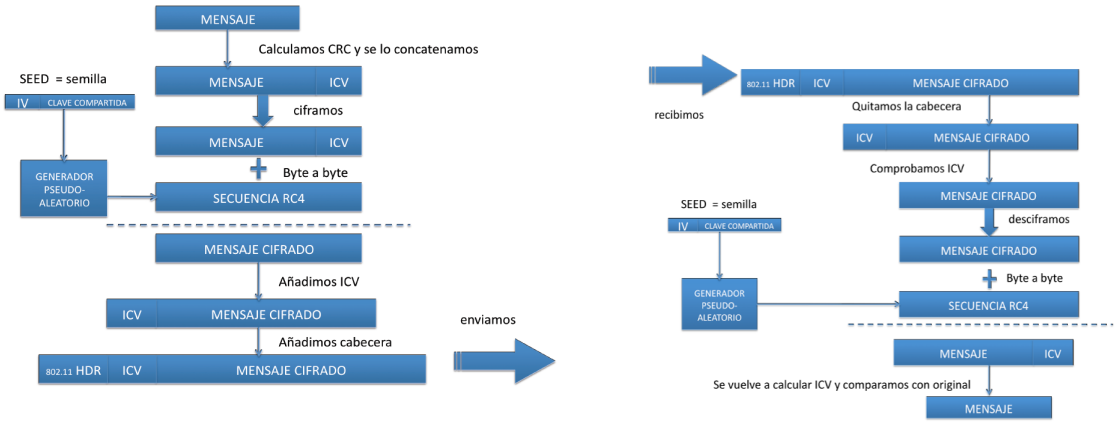
De todas las redes estudiadas tenemos que resaltar una sobre las demás, en cuanto a seguridad se refiere, es decir la red Wimax. Esta red pese a tener ciertas vulnerabilidades y varios ataques reconocidos contra ella como bien se ha expuesto en el proyecto es prácticamente invulnerable debido principalmente a los certificados X.509 y al potente cifrado que implementa, así como gracias a la propia arquitectura de esta.

La red Wifi por su parte es con diferencia la red más versátil y que permite más opciones en cuanto a configuración de seguridad, pudiendo configurar desde el nombre de nuestra red hasta el tipo de protocolo de red. No obstante y pese a todas las posibles configuraciones que ofrece se podría considerar la red más insegura puesto que es la más vulnerada de todas. El motivo de esto no es que implemente una mala seguridad, ya que incluso puede implementar el protocolo WPA2 y el cifrado AES, cuya combinación es actualmente la más fuerte.

Los motivos de esto son principalmente 3: es muy sencillo captar una señal Wifi; nadie o casi nadie desactiva la señal de emisión Wifi cuando no se está utilizando (esto implica en que un hacker pueda estar todo que desee intentando hackearla); se puede obtener información muy valiosa, pudiendo provocar además mucho daño en caso de que se quiera; y sobre todo hay una masiva cantidad de programas, tutoriales e información a lo largo de internet de como hackear esta red.

Por tanto sea cual sea la red que se esté utilizando siempre se deberá seguir el mismo procedimiento de seguridad con el fin de evitar los máximos ataques posibles, es decir configurar plenamente está conforme a todo lo visto en el proyecto y sobre todo utilizarla de una manera debidamente correcta.

6. Anexos



(a) Encriptación WEP

(b) Desencriptación WEP

Figura 3: Diagrama de encriptación y desencriptación en seguridad WEP

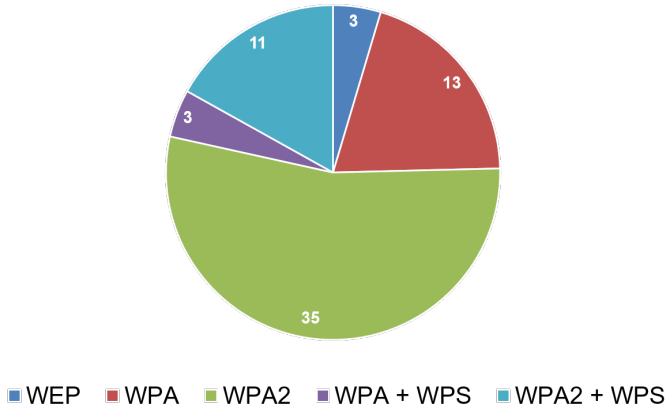


Figura 4: Gráfica resumen de redes analizadas

Referencias

[1] http://cayro.webcindario.com/wifi/reaver.htm.

[2] http://samhain.softgot.com/criptografia/lecturasnotas/algoritmos/rc4.pdf.

[3] https://es.wikipedia.org/wiki/tkip.

[4] https://es.wikipedia.org/wiki/wpa2.

[5] https://www.osi.es/es/actualidad/blog/2014/11/07/que-es-wps-pin-y-por-que-debes-desactivarlo.

[6] http://www.seguridadwireless.net/hwagm/traduccion-aircrack-ng.html.

[7] http://www.wi-fi.org/who-we-are.

[8] A. ALZAABI. *Security Algorithms for WIMAX*. PhD thesis, University of Hertfordshire, Hatfield, UK, 2013.

[9] M. JUWAINI. *A review on WEP wireless security protocol*. PhD thesis, University Kebangsaan Malaysia, Malaysia, 2012.

[10] A. H. LASHKARI. *A Survey on Wireless Security protocols (WEP,WPA and WPA2/802.11i)*. PhD thesis, University of Malaya (UM), Malaysia, 2009.

[11] A. H. LASHKARI. *Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)*. PhD thesis, University of Malaya (UM), Malaysia, 2009.

[12] G. LEHEMBRE. *Seguridad Wi-Fi: WEP, WPA y WPA2*. PhD thesis, www.hakin9.org, 2006.

[13] R. PRODANOVIC. *A Survey of Wireless Security*. PhD thesis, Air Forces and Aircraft Defense, Serbian Army, Serbia, 2007.

[14] Christian Ridderström. *Legged locomotion: Balance, control and tools — from equation to action*. PhD thesis, The Royal Inst. of Technology, SE-100 44 Stockholm, Sweden, May 2003.

[15] C. Scarfone, K. Tibbs and M. Sexton. *Guide to Securing WiMAX Wireless Communications*. PhD thesis, National Institute of Standards and Technology Gaithersburg, 2010.

[16] Albentia Systems. *Seguridad en redes WiMAX 802.16-2009*. PhD thesis, None, 2011.