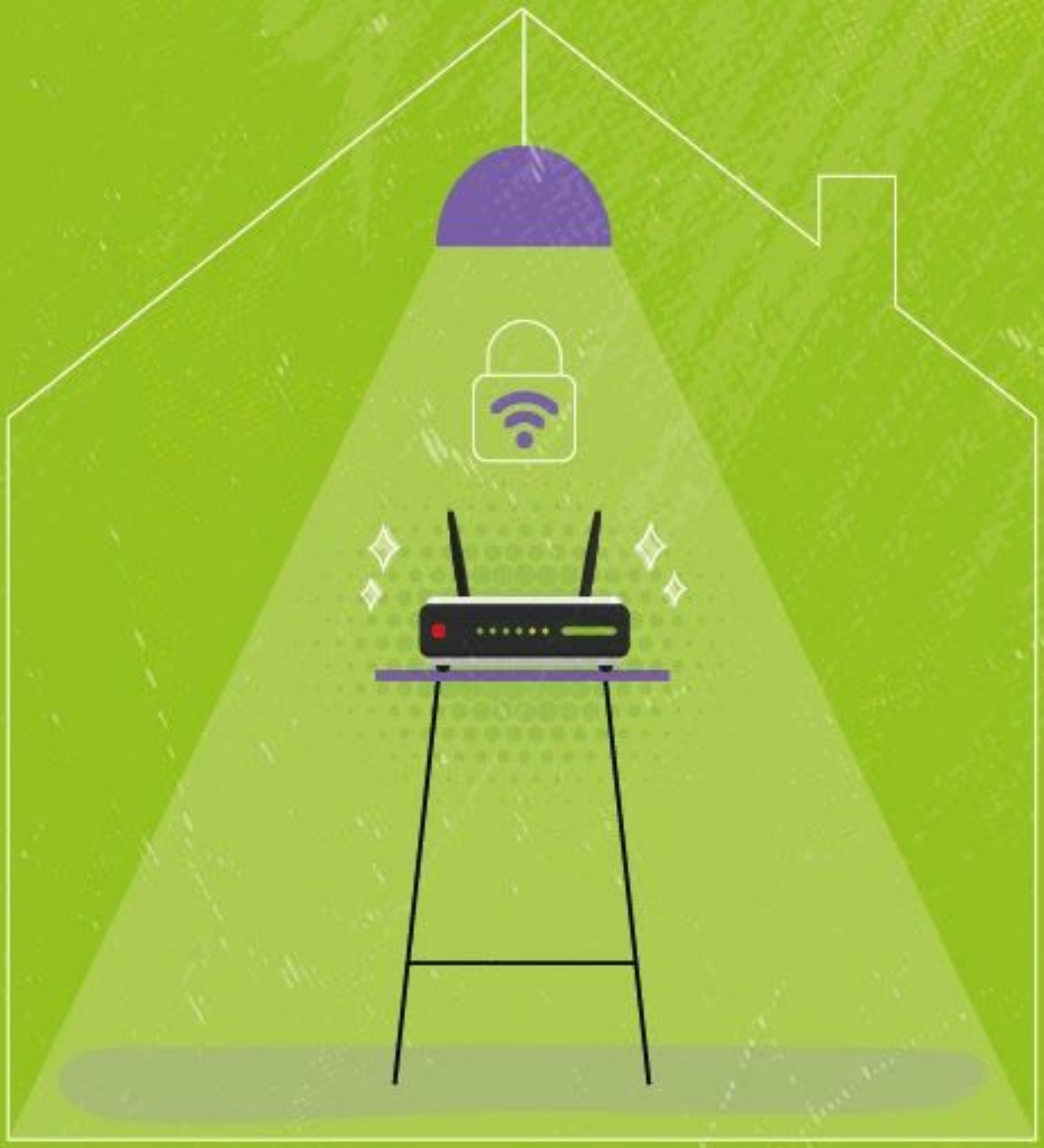
¿Las redes WiFi de casa son seguras?

Una investigación sobre módems caseros, por:

Diego Morábito y Paul Aguilar



SOCIALTIC PROTEGE.LA

Índice

Introducción

Existe el mito de que las redes WiFi, sobre todo las del hogar, son vulnerables y de fácil acceso. Hicimos el experimento de acceder de manera no autorizada a una red WiFi para comprobar la teoría. Dentro de los métodos utilizados se encuentra la obtención de hash, ataque por WPS y ataque de fuerza bruta.

**Esto no es una guia para realización de estos ataques, sino un análisis del desarrollo de éstos con el fin de saber si las medidas de seguridad proporcionadas en los módems del hogar son suficientes o no.*

El mito del WiFi

En los últimos años del milenio pasado, debido a la necesidad de conectar dispositivos de cómputo vía inalámbrica, surgió la tecnología que conocemos como WiFi. Unas de las características del WiFi que más han cambiado con los años han sido los mecanismos y protocolos de seguridad que esta tecnología implementa. Estos mecanismos, en sus primeras versiones, eran vulnerados con facilidad, lo cual creó el mito de **"robar la contraseña del WiFi es fácil teniendo los programas adecuados"**.

Este mito, aún vastamente difundido, que, en su momento, era completamente justificado, es necesario cuestionarlo ahora. Además, se cree que la seguridad del Internet al que tiene acceso la mayoría de la población en México y Latinoamérica es de una calidad deficiente. Por ejemplo, en México, Telmex fue el primer gran proveedor de Internet, y logró captar una gran base de clientes pero no ha logrado mantener una buena reputación.

Nos preguntamos: ¿Qué tan sencillo es vulnerar la seguridad de una red WiFi? ¿Por qué? ¿Qué condiciones se requieren para que esto se cumpla? ¿Las medidas de seguridad básicas que brindan los proveedores de Internet son insuficientes? Estas son algunas de las preguntas que intentamos responder.

¿Qué hicimos?

- Realizar un escaneo de redes WiFi en una zona habitacional para trabajar con ellas
- Intentar obtener acceso a las redes detectadas
- Identificar las medidas de seguridad proporcionadas por las redes utilizadas
- Verificar si se cumplen las condiciones necesarias que sustentan el mito del fácil acceso al WiFi

Contexto

Al contratar un servicio de Internet, el Proveedor de Servicios de Internet (Internet Service Provider, ISP) nos brinda un aparato al que comúnmente se le conoce como módem (y que seguiremos llamando así a lo largo de este trabajo). Este aparato en realidad es un router el cual instalan en nuestras casas los técnicos del ISP.

Para hablar con mayor profundidad de estos dispositivos necesitamos definir los siguientes conceptos:

- Un **módem** (acrónimo de modulador-demodulador) es un dispositivo que se encarga de transformar la información en un medio que permita su transmisión a otro medio.
- Un **WAP** (Wireless Access Point - Punto de acceso inalámbrico) es un dispositivo que permite conectarse de manera inalámbrica a una red cableada.
- Un **router** o **enrutador** es un dispositivo que se encarga de redirigir los paquetes de información a los diferentes dispositivos conectados a la red.
- Un **firewall** o **cortafuegos** es un dispositivo (puede ser físico o un programa) que se encarga de establecer las reglas sobre qué tipo de conexiones pueden establecer los dispositivos de la red interna con Internet y viceversa.

Con lo anterior podemos decir que a lo que llamamos **módem** es el dispositivo que nos permite conectar cada uno de nuestros dispositivos (laptops o PC's, celulares, aparatos inteligentes como refrigeradores o televisores, tabletas, etc.) al Internet.

Se establece una red interna o local que, a través del módem, se conecta a la red global o Internet. Una persona con acceso no autorizado a nuestra red WiFi tiene, por lo mismo, acceso a nuestra red local y, si no establecemos una contraseña particular para nuestro módem, también tendrá acceso a las configuraciones del mismo.

Teniendo acceso a uno o ambos componentes, un atacante puede modificar diferentes aspectos técnicos de la red local para poder obtener acceso a los diferentes dispositivos y a la **información guardada en ellos**. Por lo anterior, es de vital importancia que las configuraciones básicas de seguridad establecidas por los proveedores de Internet en nuestros módems sean suficientes para evitar los accesos de personas no autorizadas tanto a la red local como al dispositivo en sí.

Detrás de las contraseñas

Las contraseñas son una de las configuraciones básicas de seguridad para nuestras redes de WiFi del hogar, es decir, es la tecnología encargada de administrar la manera en la que los dispositivos se conectan al módem. Cuando introducimos nuestra contraseña, hay toda una serie de acciones que no vemos que permiten establecer una **conexión segura entre nuestro dispositivo y el módem**. Sin entrar a detalles, existen cuatro protocolos actualmente en uso que permiten cifrar las contraseñas para establecer conexiones seguras.

1. **WEP** (Wired Equivalent Privacy o Privacidad equivalente a cableado) que ahora ha caído en desuso (de hecho en nuestras pruebas no encontramos ninguna red que utilizara este protocolo).
2. **WPA** (WIFi Protected Access o Acceso Protegido a WiFi).
3. **WPA2** (el más usado y más seguro) Es la mejora del protocolo WPA.
4. **WPS** (WiFi Protected Setup). Este no es un mecanismo de seguridad en sí mismo, sino que se sirve del protocolo WPA2 para establecer conexiones seguras entre el módem y los dispositivos de la red interna con la intervención mínima del usuario. Es un mecanismo rápido de conexión.

Algunos de los protocolos mencionados con anterioridad tienen vulnerabilidades que permiten a un atacante tener acceso de manera no autorizada a una red WiFi.
El primer protocolo, WEP, ha caído en desuso debido a que los atacantes podían acceder a la red en cuestión de minutos.
El protocolo WPS al estar basado en el protocolo WPA también es vulnerable, pero requiere ciertas condiciones contextuales para que el ataque sea exitoso.

WPA y WPA2 son actualmente los protocolos de seguridad más utilizados ya que son los que actualmente cuentan con los mecanismos más efectivos, y se han vuelto el estándar en los dispositivos más recientes.

Desarrollo

¿Qué material utilizamos?

- **Equipo de computo:** Asus VivoBook x510u
- **Sistema Operativo:** Linux Mint 19.3
- **Tarjeta de red WiFi:** Ralink RT5372. Driver: rt2800usb.
- **Tarjeta gráfica:** Nvidia GeForce 930mx
- **Software:**
    - Airmon-ng
    - Hashcat
    - Reaver

Escaneo de redes WiFi

El análisis de redes WiFi se realizó de 9am - 10am en un día de trabajo normal entre semana. Este dato es importante porque para realizar los ataques a los módems es necesario que exista al menos un dispositivo conectado a ellos. Probablemente, debido a la hora y el día, pocas de las redes escaneadas tuvieron algún dispositivo conectado.

El resultado del análisis fueron **18** redes dentro del alcance:

- 8 de ellas fueron Infinitum (Telmex)
- 3 de ellas fueron iZZi
- 7 de ellas tenían el SSID (nombre de la red) modificado (no de fábrica) y, por lo mismo, no se pudo conocer el proveedor de Internet.

Para el escaneo se utilizó el programa **airmon-ng** y todas estas redes fueron encontradas en la banda de transmisión de 2.4Ghz[1].

Los canales de transmisión usados variaban sin que se pudiera establecer una correlación entre canal de transmisión y proveedor de Internet.

Los canales de transmisión encontrados fueron:

- 3 redes en canal 11
- 7 en canal 1
- 4 en canal 6
- 1 en canal 9
- 1 en canal 3
- 1 en canal 8
- 1 en canal 10

Ataque por obtención de hash

Una vez detectada la red, se analiza la misma para averiguar cuántos dispositivos están conectados al **WAP**. Las redes que no cuentan con dispositivos conectados quedan descartadas. En las que sí cuentan con dispositivos conectados se hace un **ataque de desautentificación**.

[1] Se encontraron muy pocas módems transmitiendo a 5Ghz y por eso no se les tomó en cuenta.

Un ataque de desautenticación consiste en mandar un **frame de desautentificación** al WAP, lo que hace que el dispositivo (o dispositivos) conectado se desconecte de la red y tenga que volver a conectarse (esto sucede de manera automática). Para poder realizar este ataque sólo es necesario saber la dirección MAC del WAP (la dirección MAC es un identificador único para cada dispositivo físico).

El monitoreo de redes y el ataque de desautenticación se realizaron con el software airmon-ng.

Durante el ataque de desautenticación es necesario obtener un dato conocido como lo es el **hash de la contraseña** de conexión a la red del módem, el cual se obtiene al aprovechar el proceso llamado **4-way handshake**. Cuando obtenemos un hash derivado del aprovechamiento del 4-way handshake, lo denominaremos “handshake obtenido”.

En este proceso (el 4-way handshake) hay un intercambio de diferentes claves entre el dispositivo que desea conectarse y el módem para poder establecer una conexión segura. La contraseña de la red se intercambia entre los dispositivos a través de una función hash.

Esta es una función que permite otorgarle a una cadena de datos (en este caso la contraseña) una cadena de valores únicos. En otras palabras, cuando uno aplica una función hash a un conjunto de datos, lo que resulta es una cadena de valores únicos para ese conjunto de datos. Si el conjunto de datos cambia, aunque sea mínimamente, el resultado de la función hash también cambiará. Este proceso se utiliza para comprobar la integridad de un cierto conjunto de datos.

Una vez que se obtuvo el hash correspondiente, este se somete a un proceso para tratar de obtener los datos originales que generaron ese hash, básicamente si tenemos el hash, a partir de él intentaremos obtener la contraseña que lo generó en un inicio.

Es importante mencionar que la función hash es de una sola vía, es decir que no se puede reconvertir la cadena de valores de un hash a los datos originales. Lo que sí se puede hacer es intentar, a partir de un conjunto de datos, obtener el mismo hash. En esto consiste el proceso de previamente mencionado.

Estas fueron las redes a las cuales se les hicieron los ataques de desautentificación y los resultados:

Intensidad de señal (PWR)	Canal de transmisión	# de dispositivos conectados al AP	Rango de ataque[2]	Resultado
53-56	6	4	0-10	Handshake capturado
59-60	11	4	0-10	Handshake capturado
Fuera de rango o no hay dispositivos conectados[3]*	-	-	-	-
63-67	1	2	0-10 (2x) 0-20 (2x)	Handshake no obtenido
72-73	11	1	0-10 (2x) 0-20 (2x)	Handshake no capturado
68-72	10	1	0-10 (2x) 0-20 (2x)	Handshake no capturado
74-76	1	3	0-10 (2x) 0-20 (2x)	Handshake no capturado

*Este resultado se repitió en 12 redes de wifi.
De los ataques de desautenticación realizados, solamente se pudieron capturas dos hashes, por lo cual solamente intentamos atacar estas dos redes.

Obtención de la contraseña a través del hash

Una vez capturados los hash se procedió a intentar obtener la contraseña que los generó. Para este proceso, se utiliza una una tarjeta de video dedicada, la cual permite procesar información con mayor velocidad que un microprocesador convencional.

El proceso para obtener el dato original del hash consiste en lo que se llama comúnmente un ataque de diccionario. Es decir que a un número enorme de datos probables (en este caso contraseñas que posiblemente generaron el hash obtenido) se les aplica la función hash y el resultado se compara con el hash obtenido previamente para ver si coinciden.

[2] Este es el número de *frames* de desautorización que se mandaron antes de obtener el *hash.*
[3] Fuera de rango o no hay dispositivos conectados: aunque el AP pueda estar dentro del rango de alcance, no necesariamente lo están los dispositivos, lo que implica que no se puede llevar a cabo el ataque.

En nuestro caso utilizamos una lista que contiene 40 millones de palabras con diez caracteres cada palabra en una mezcla de minúsculas, mayúsculas y números. Elegimos que la longitud de las palabras fuera 10 porque normalmente esa es la longitud de las contraseñas en los módems analizados. Claro está que **si la persona cambió la contraseña, esto no serviría**. De tal manera que este método sólo funciona si el usuario no ha cambiado su contraseña.

El tiempo que duró el ataque a los dos hash obtenidos fue de 1 hora y 30 minutos por hash. El resultado fue negativo, ya que **no pudimos obtener la contraseña**.

Ataque por WPS

Otro método utilizado para intentar acceder a la red fue utilizar las vulnerabilidades del protocolo WPS.

Como explicamos más arriba, este no es un protocolo de seguridad sino un protocolo que permite configurar una red local y el acceso de los dispositivos al módem de una manera que le implique menos trabajo al usuario, una sincronización rápida.

La vulnerabilidad de este protocolo es que si está activado, una persona sin acceso físico al módem puede utilizar un programa (en este caso **Reaver**) que emula el acceso físico al módem, de tal manera que se puede intentar establecer una conexión.

El programa intenta conectarse intentando diferentes contraseñas (todas numéricas). En los módems que pudimos identificar como de Telmex, nunca se pudo establecer una conexión con el módem que permitiera intentar este ataque. Esto sólo fue posible en los módems del proveedor de Internet iZZi. Sólo pudimos establecer una conexión en los módems del provedoor iZZi.

Se intentó dicho ataque en los tres módems iZZi, pero el resultado fue negativo debido a que tienen una configuración de seguridad que hace que el número de intentos de conexión por WPS esté limitado (como funciona en códigos de acceso en smartphones). En términos prácticos esto implica que si uno intenta cierto número de contraseñas y ninguna es la correcta, se tiene que esperar cierto tiempo para poder volver a intentar. La espera es de un minuto y este número va en aumento a medida que se intentan más accesos. Después de un cierto número intentos, este protocolo inhabilita el acceso para la dirección MAC del dispositivo que está intentando conectarse.

Ataque de fuerza bruta

Por último se intentó acceder a un módem del proveedor Telmex del cual sabíamos que la contraseña era solamente numérica. Este módem, aunque aún en uso, no es de los más nuevos que instala este proveedor. Con el hardware ya mencionado y el uso del programa **hashcat** intentamos hacer un ataque de **fuerza bruta**.

Este método consiste en **probar todas las combinaciones posibles de caracteres** que puedan generar la contraseña, en este caso de una cadena de 10 números.

Después de dos horas, el porcentaje completado fue del 1.38%. Esto implica que si el tiempo de trabajo de la GPU es lineal, tardaríamos un máximo 145 horas en dar con la contraseña. Sin embargo, es importante remarcar que de entrada sabíamos la longitud de la contraseña y sus características (i.e. que sólo eran números).

Conclusiones

En la cultura de la seguridad **se asume que cualquier sistema es vulnerable** y, con los suficientes recursos (conocimientos y hardware), es sólo cuestión de tiempo que uno pueda tener acceso a éste.

A la hora de pensar en las medidas de seguridad implementadas para un módem de uso hogareño no se busca crear un sistema 100% seguro, sino un sistema que, para vulnerar, exija bastantes recursos para hacerlo o, en otras palabras, **un sistema que no sea rentable atacar.**

En nuestro caso resulta que los métodos más comunes para atacar módems no son rentables. Se requiere de mucho tiempo y de un poder de procesamiento que no está al alcance de todos.

Las configuraciones básicas de seguridad de fábrica con las que vienen los módems, es decir, las contraseñas y el uso de WPA2 y WPS, son adecuadas para el uso en el hogar.

En este sentido, ataques como un **evil twin** (suplantación de una red) o **ingeniería social** podrían resultar más efectivos con una inversión menor de dinero y tiempo.