IMPLEMENTACIÓN DE UN ESCENARIO DE PRUEBAS PARA EL ANÁLISIS DE VULNERABILIDADES EN REDES WIFI

Antonio Caizapanta Tamayo Ing. Carlos Romero

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA
ESCUELA POLITECNICA DEL EJÉRCITO

Resumen

El estándar 802.11 establece los niveles inferiores de las capas del modelo *OSI*, física y enlace de datos, a nivel de subcapa *MAC* se tiene todas las reglas que determinan la forma de acceder al medio (ondas electromagnéticas) y enviar datos. La subcapa *PHY* se involucra con los detalles de transmisión y recepción. Actualmente, los ataques a redes inalámbricas se concentran en estas capas, debido a la falta de encriptación al trasmitir tramas de control y administración.

En los laboratorios del Departamento de Eléctrica y Electrónica, no se tiene un escenario de pruebas para analizar el tráfico en una red *WIFI* [1] y verificar el comportamiento de las tramas antes, durante y después de un ataque, con esto se podrá implementar mecanismos de autenticación de doble vía, que permitan tanto al caliente y el *AP* verificar que se está conectando a la red correcta y de igual forma constatar que el cliente está autorizado para acceder a dicha información.

Abstract

The 802.11 standard establishes the lower levels of the OSI model layers, physical and data link level MAC sublayer has all the rules that determine how to access the medium (electromagnetic waves) and send data. The PHY sublayer is involved with the details of transmission and reception. Currently, wireless network attacks are concentrated in these layers, due to lack of encryption when transmitting management and control frames.

In the laboratories of the Department of Electrical and Electronic, do not have a test scenario to analyze traffic on a WiFi network and verify the behavior of the frames before, during and after an attack, so can implement authentication mechanisms two-way, allowing both the hot and the AP verify that you are connecting to the correct network and similarly found that the client is authorized to access such information.

1. Introducción

Desde un inicio se ha tratado de proveer a los usuarios alternativas que brinden seguridad al tráfico de la información en este tipo de redes, así apareció el protocolo *WEP* el cual cifraba la información que se transmitía, luego de una seria de análisis se determinaron todas las falencias que este protocolo tenia, así que se lo mejoró apareciendo el protocolo *WEP I*, posteriormente el *WEP II, WEP III, WPA*, hasta llegar al estándar 802.11i *(WPA2)*, el cual introdujo la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos, actualmente este es el más difundido y utilizado debido a su alto nivel de cifrado, evitando así los ataques o conexiones no deseadas. Pero con el paso del tiempo nuevos métodos y *software* de desencriptación son creados para vulnerar la protección que brindan los protocolos actuales de seguridades, es necesario identificar posibles ataques antes de que estos afecten la disponibilidad de la red.

2. Características y elementos del escenario de pruebas

El protocolo 802.11i fue aprobado en el año 2004, está dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, *TKIP* (Protocolo de Claves Integra – Seguras – Temporales), y

AES (Estándar de Cifrado Avanzado). Se implementa en *WPA2*.

802.11i fue adoptado y recibió el nombre comercial *WPA2* por parte de la alianza *Wi-Fi*, se introdujeron varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos. [7]

Este protocolo 802.11i implementa el protocolo de encriptación *CCMP* (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) es un mecanismo mejorado de encapsulación criptográfica para la confidencialidad de datos.

Se implementó en el escenario de pruebas el estándar 802.11i a continuación en la figura 2.1 se observa la disposición de la red.

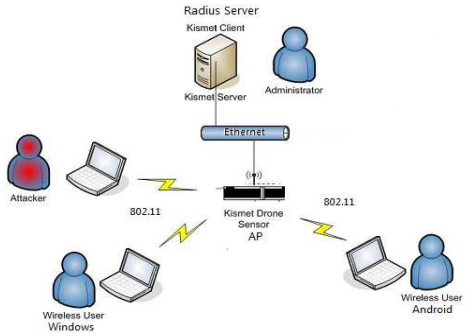

Figura. 2.1. Topología de red

La base principal del diseño del laboratorio de pruebas es la tarjeta *Alix2D2* con el *software OpenWrt* da una libertad de configuración que no se puede lograr con otros tipos de *software* como se lo menciono anteriormente. Al cargar un *software* libre es posible generar nuevas compilaciones para el *hardware* específico de la tarjeta. [3]

Al tener un *hardware* tan robusto con una memoria limitada se puede generar un elemento regulador del tráfico, capaz de realizar las tareas de autenticación más complejas, implementadas a nivel empresarial. En la figura. 2.2 se observa el AP implementado en la tarjeta Alix2D2.

Figura. 2.2 Tarjeta Alix2D2

Una vez que se tiene el AP, se conecta mediante Ethernet a un servidor que tiene las funciones de Kismet server y servidor radius (freeradius). [2]

Para aumentar la seguridad en la red se implementó certificados digitales de autenticación ofreciendo un escenario más robusto y versátil para las pruebas, estos certificados se los instalan tanto en el servidor como en los usuarios que desean acceder a los recursos de la red. [9]

El análisis de los resultados se basa en la modificación de los parámetros a nivel de la capa de enlace de las tramas, bajo ataques a la red, para realizar dichas intrusiones se utiliza el software BackTrack5, como se ve en la figura 2.3 una vez instalado el programa se accede a toda la suite.

Figura.2.3 Software para intrusiones

Utilizando BackTrack5 se realizaran los ataques DoS y MiTM.

3. Análisis de las tramas capturadas

Se tienen tramas de datos, las que transportan la información de capas superiores, tramas de gestión que permiten mantener las comunicaciones y tramas de control, como su nombre lo indica, controlan el medio.

Las tramas beacon ocupan la mayor cantidad de tramas, durante el trafico de la red antes de establecerse la asociación de los elementos de la red, son tramas de gestión enviadas por el punto de acceso (tarjeta Alix2D2) para difundir su presencia y la información de la red, en la figura 3.1 se indica la estructura de la trama

Figura. 3.1 Trama beacon

A continuación se describe cada uno de los campos:

ESS/IBSS: Indica si el transmisor es un AP.

IBSS: Indica si la arquitectura esta en modo ad-hoc

CFP: Establece si se requiere una confidencialidad de los datos.

Privacy: Menciona si el AP soporta autenticación wep.

Short Preamble: Este campo se añadió a 802.11b para soportar las altas tasas de DSSS PHY. [10]

El valor 1 indica que se está usando SP, al usar el estándar 802.11g se requiere que este valor este en 1.

PBCC: El valor 1 indica que se está utilizando codificación convolucional binario paquete esquema de modulación.

Channel Agility: el valor de 0 indica que no se lo esta usando, apoya la alta tasa DSSS PHY.

Spectrum Management: indica si el dispositivo implementa DFC y TPC para los canales de 5GHz.

Short Slot Time: toma el valor de 1 cuando la ranura de tiempo es más corto para usar el estándar 802.11g.

Automatic Power Save Delivery: Indica con que frecuencia la estación en modo de ahorro de energía se activa para escuchar tramas beacon de administración.

DSSS-OFDM: se tiene el valor de 1 cuando se está usando DSSS-OFDM.

Delayed Block Ack/ Immediate Block Ack: permiten establecer una sesión para el intercambio de un ADDBA request y response, the block ack sessions son usados para establecer un tráfico particular entre dos estaciones. [25]

El análisis está enfocado a las falencias de seguridad, en el protocolo de seguridad más robusto actualmente implementado, en la figura 3.2 se tienen los campos de esta trama.

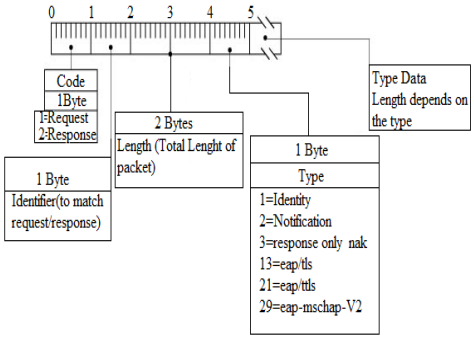

Figura. 3.2. Trama EAP

Code: aquí se especifica si es una solicitud o una respuesta 1/0.

Identifier: el identificador asigna un número para relacionarlo con la respuesta o solicitud dependiendo el tipo de código.

Length: establecer la longitud del paquete

Type: dependiendo del valor tomado se tiene una función específica en la figura 4.6 se ven los tipos más utilizados.

Type Data: es un campo que depende del campo anterior type. [7]

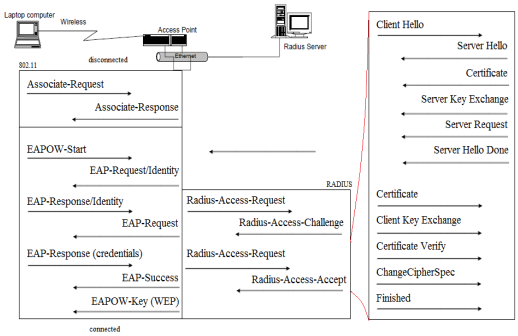

Figura. 3.3 Proceso de asociación

La figura 3.3 presenta un completo diagrama de las tramas obtenidas en el proceso de asociación, autenticación y conexión del terminal a la red. [8]

4. Variación de tramas bajo ataques

El primer ataque es el detallado en la figura 4.1 DoS,

Figura. 4.1 Ataque DoS

El proceso en el cual se basa este ataque es el siguiente, primero se ubica a un conjunto de host los cuales serán las víctimas entonces, el atacante va a generar tanto tráfico dirigido a los puertos del servidor (objetivo), para saturar el flujo de la información, debido al sin número de solicitudes realizadas por el atacante, el servidor va a llegar a un punto en el cual limite de un servicio a la red. [6]

En la figura 4.2 se puede observar en que trama específicamente el AP envía una trama de des asociación para bloquear al usuario de la red.

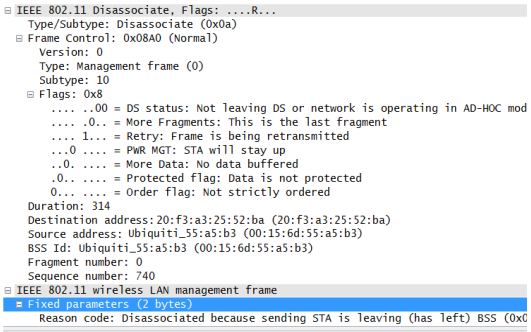

Figura. 4.2 Desasociación de AP y Usuario

El segundo ataque es llamado Man in the Middle, en la figura 4.3 se detalla el proceso de ataque.

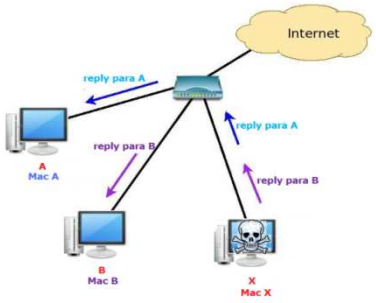

Figura. 4.3. MiTM

Una computadora invasora X envía un paquete de *ARP reply* para A indicando que la dirección *IP* de la computadora B apunta hacia la dirección *MAC* de la computadora X, y de la misma forma envía un paquete de *ARP reply* para la computadora B mostrando que la dirección *IP* de la computadora A, apunta hacia la dirección *MAC* de X. Como el protocolo *ARP* no guarda los estados, las computadoras A, B asumen que enviaron un paquete de *ARP request* solicitando esta información, y asumen los paquetes como verdaderos. A partir de este punto, todos los paquetes enviados y recibidos entre las computadoras A, B pasan por X (atacante.)

En la figura. 4.4 se observa la tabla arp que se encuentra registrada en el AP.

```
root@OpenWrt:~# arp
IP address       HW type     Flags       HW address            Mask     Device
192.168.1.50     0x1         0x2         00:19:66:18:78:ae     *        br-lan
192.168.1.47     0x1         0x2         84:c9:b2:7c:57:6f     *        br-lan
192.168.1.3      0x1         0x2         00:21:00:36:52:39     *        br-lan
192.168.1.4      0x1         0x2         20:f3:a3:25:52:ba     *        br-lan
root@OpenWrt:~#
```

Figura. 4.4 Tabla ARP del AP

El atacante clona su mac para receptar toda la información que va al atacado, de esta manera se crea la intrusión y se obtiene información sensible para la red. [4]

5. Conclusiones

Mediante el tratamiento de la información, se ubicó el ataque a la red además se evidenciaron vulnerabilidades en las tramas (información sin cifrar) que circulaban por el canal. [5]

Previamente a la asociación del terminal con el punto de acceso, tanto el usuario como la clave se envían sin encriptación, esto puede ser fácilmente interceptado por un tercero para realizar una validación fraudulenta de esta manera accediendo a los recursos de la red.

Los certificados digitales incrementaron el nivel de seguridad en la red, ya que proporcionan una llave (*key*) aleatoria y fuertemente encriptada, limitando de esta forma el acceso a la información una vez que se haya establecido el handshake entre el solicitante y el servidor.

El modelo de pruebas implementado, será la base para futuros análisis del flujo de datos a niveles de enlace, con esto se podrá desarrollar un modelo para detectar ataques como denegación de servicios, arp spoofing, suplantación de identidad, etc, en redes WLAN 802.11, utilizando parámetros de paquetes de control y gestión de la capa MAC, basada en el tipo de tráfico de la red.
Realizar prácticas en el laboratorio, permitirá una mejor comprensión de los modelos de seguridad implementados actualmente en grandes entornos corporativos, el principio de instalación y funcionamiento es el mismo, la única diferente en el dimensionamiento de la red y aplicaciones propias de cada institución.

Referencias Bibliográficas

[1] WECA, http://www.wi-fi.org/

[2] IEEE 802.11TM WIRELESS LOCAL AREA NETWORKS, http://www.ieee802.org/11

[3] Redes Wifi
http://recursostic.educacion.es/observatorio/web/es/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi

[4] IEEE 802®: OVERVIEW & ARCHITECTURE,
http://standards.ieee.org/about/get/802/802.html

[5] Protocolo Wep,
http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/de_l_j/capitulo_3.html#

[6] IEEE 802.11i,
http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[7] EAP Protocol,
http://tools.ietf.org/html/rfc3748

[8] PEAP y EAP-TTLS,
http://www.oreillynet.com/wireless/2002/10/17/peap.html

[9] AES,
http://www.evolsystem.net/algoritmo/AES/

[10] Tarjetas Alix,
http://www.pcengines.ch/alix2d2.htm

Biografía
Antonio Caizapanta Tamayo

Nació en Quito en 1988.
Realizo sus estudios secundarios en el Colegio Particular Paulo VI. Obtuvo el título de bachiller con especialidad Físico-Matemáticas en 2006. Entre 2006 y 2011 estudió en la Escuela Politécnica del Ejército, en este momento está realizando la tesis profesional sobre “implementación de un escenario de pruebas para el análisis de vulnerabilidades en redes wifi”