UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE INGENIERÍA DE SISTEMAS

ANÁLISIS DE VULNERABILIDADES EN LA SEGURIDAD DE LA RED WLAN CON IOT EN RESIDENCIAS QUE UTILIZAN DOMÓTICA Y CONTROL REMOTO

Trabajo de titulación previo a la obtención del

Título de Ingeniero de Sistemas

AUTOR: Santiago Nicolas Pineida Parra

TUTOR: Manuel Rafael Jaya Duche

Quito-Ecuador

2022

CERTIFICADO DE RESPONSABILIDAD Y AUDITORIA DEL TRABAJO DE TITULACIÓN

Yo, Santiago Nicolás Pineida Parra con documento de identificación N° 1752154284 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 4 de agosto de 2022

Atentamente,

Santiago Nicolás Pineida Parra

1752154284

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Santiago Nicolás Pineida Parra con documento de identificación N° 1752154284 expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy el autor del Artículo Académico: "Análisis de Vulnerabilidades en la Seguridad de la Red WLAN Con IoT en Residencias que Utilizan Domótica y Control Remoto", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 4 de agosto de 2022

Atentamente,

Santiago Nicolás Pineida Parra

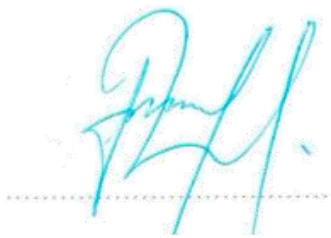
1752154284

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Manuel Rafael Jaya Duche con documento de identificación N.º 1710631035 docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ANÁLISIS DE VULNERABILIDADES EN LA SEGURIDAD DE LA RED WLAN CON IOT EN RESIDENCIAS QUE UTILIZAN DOMÓTICA Y CONTROL REMOTO, realizado por Santiago Nicolás Pineida Parra con documento de identificación N.º 1752154284, obteniendo como resultado final el trabajo de titulación bajo la opción de Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 4 de agosto de 2022

Atentamente,



Ing. Manuel Rafael Jaya Duche, MSc

1710631035

AGRADECIMIENTO

El presente trabajo de investigación como gesto de agradecimiento se lo dedico principalmente a dios y a la virgen, por ser los inspiradores para continuar con los deseos y anhelos más deseados. A mis padres Nicolás y Maurita, por todo su apoyo, sacrificio y amor incondicional que me brindaron durante el transcurso de mi carrera universitaria, por inculcarme valores para ser una mejor persona y nunca rendirme, me siento demasiado orgullo de ser su hijo y llegar a convertirme en lo que soy. A mis hermanas Ade y Pao que siempre estuvieron pendientes de mí y siempre me apoyaron brindándome cariño. Agradecer a mis abuelitos que de igual manera siempre estuvieron conmigo dándome su apoyo y confiaron en mí, por ellos también soy la persona quien soy.

También agradezco a la Universidad Politécnica Salesiana e Ingenieros de la carrera de Ingeniería de Sistemas, por toda su enseñanza y en especial a mi tutor Manuel Rafael Jaya Duche por compartir su valioso conocimiento el cual sirvió para culminar este trabajo de investigación, a mis compañeros por las experiencias y apoyo incondicional que se compartió durante nuestra vida universitaria.

Santiago Nicolás Pineida Parra

ANÁLISIS DE VULNERABILIDADES EN LA SEGURIDAD DE LA RED WLAN CON IOT EN RESIDENCIAS QUE UTILIZAN DOMÓTICA Y CONTROL REMOTO

VULNERABILITY ANALYSIS IN THE SECURITY OF THE WLAN NETWORK WITH IOT IN RESIDENCES THAT USE HOME AUTOMATION AND REMOTE CONTROL

Santiago Nicolás Pineida Parra[1], Manuel Rafael Jaya Duche[2]

Resumen

En el presente artículo tiene como objetivo analizar las vulnerabilidades que existen al conectarse desde dispositivos IoT a la red WLAN, creando un escenario en tiempo real con el módulo ESP32, de esta manera se conecta a las plataformas Firebase, Ubidots y Cayenne. Se obtiene el control remoto de cada una de ellas para controlar de manera amigable en una alerta. Para este análisis de vulnerabilidades se utilizó Kali Linux, dentro de este sistema operativo libre existe la herramienta Ettercap para realizar los respectivos ataques y mediante Wireshark capturar todos los paquetes que se están enviando en la red. Se obtuvo como resultado que la plataforma con mayor seguridad al conectarse es Firebase y Cayenne, estas dos no presentan vulnerabilidades, los paquetes que envían por la red son encriptados. Por otro lado, la plataforma Ubidots presenta vulnerabilidad al enviar paquetes, estos paquetes son de primer plano y sus datos son extraídos muy fácilmente.

Palabras claves: *vulnerabilidad, módulo, sensores, paquetes, plataformas.*

Abstract

The objective of this article is to analyze the vulnerabilities that exist when connecting IoT devices to the WLAN network, creating a real-time scenario with the ESP32 module, thus connecting to the Firebase, Ubidots and Cayenne platforms. Remote control of each of them is obtained to control in a friendly way in an alert. Kali Linux was used for this vulnerability analysis, within this free operating system there is the Ettercap tool to perform the respective attacks and through Wireshark capture all the packets that are being sent on the network. It was obtained as a result that the platform with greater security when connecting is Firebase and Cayenne, these two do not present vulnerabilities, the packets sent over the network are encrypted. On the other hand, the Ubidots platform presents vulnerabilities when sending packets, these packets are foreground and their data are very easily extracted.

Keywords*: vulnerability, module, sensors, packages, platform.*

[1]Estudiante de Ingeniería de Sistemas – Universidad Politécnica Salesiana, Egresado – UPS – sede Quito. Autor para correspondencia: spineida@est.ups.edu.ec

[2]Magister en Redes de Información y Conectividad, Ingeniero en Electrónica y Telecomunicaciones, Profesor de Ingeniería en Sistemas UPS sede Quito, Email: mjaya@ups.edu.ec

1. Introducción

El progreso y la evolución de la tecnología ha traído más formas de comunicación, acortando distancias y habiendo comunicación en todo el mundo. Estos avances ayudan a conectar varios dispositivos a redes, el internet a trasformado la vida de los usuarios, estos al conectarse desde dispositivos inteligentes de casa, ya que por medio de sensores estos se conectan a un mecanismo y de esta forma se comunican a la red [1].

El internet de las cosas (IoT) ha sido muy importante durante los últimos años, gracias a esta tecnología muchas personas pueden comunicarse de manera instantánea.

Con el incremento de Internet de las Cosas salen muchas inquietudes por problemas de seguridad con dispositivos conectados. Se pronostica que el aumento de dispositivos conectados a internet de las cosas a superado los 25 000 millones para el año 2022 [2].

Los dispositivos IoT son conectados a la red, de esta manera dan servicios más inteligentes y breves que un dispositivo común. Al utilizar estos dispositivos (IoT) se toma el riesgo de sufrir ataques por hackers. Los dispositivos IoT también se caracterizan por los buenos beneficios que facilitan la comunicación en hogares.

La seguridad debe ser importante ya que, si los dispositivos llegaran a fallar, personas maliciosas se encargarían de destruir y robar información.

IoT es una red de dispositivos conectados a una red. Estos contienen un identificador que es único, este intercambia y recoge información a través de la red. En la actualidad hay empresas que ya utilizan dispositivos IoT para su mejor desarrollo, tales como sensores, rastreadores inteligentes, cámaras de seguridad inteligentes, entre otros.

Las redes inalámbricas se han utilizado ampliamente en sitios libres para el público, las redes WLAN que se van desarrollando van teniendo problemas que es la seguridad, por ello esta investigación intenta evaluar todas las seguridades en redes WLAN [3].

Las tecnologías de redes inalámbricas WLAN para IoT son expuestas a peligrosos ataques de seguridad, esto ocurre por los pocos recursos informáticos que limita el uso de protocolos de seguridad [4]. Para enfrentar este problema los encargados de la seguridad deben elaborar evaluaciones periódicas de las vulnerabilidades en dispositivos IoT.

La domótica es un conjunto de técnicas que facilita la construcción de residencias disminuyendo la energía mecánica y eléctrica, de esta manera reduce el esfuerzo del ser humano al operar sistemas con los puntos de los dedos, aumenta el ahorro en métodos de valores de facturas [5].

Las técnicas de automatización del hogar ayudan a recopilar datos de sensores, estos se procesarán y darán comandos de salida. Esta técnica tiene accesos a redes externas de comunicación o investigación. La domótica permite dar respuestas a las necesidades de los nuevos cambios y estilos de vida. Una de las cosas más importantes de la domótica es dar comodidad al consumidor y facilitar el uso en ello.

El control remoto ayuda hacer tareas en un ordenador sin estar físicamente con un equipo informático. Esto se realiza gracias a programas que existen en el entorno de la informática y permite trabajar en equipos que se encuentren a largas distancias mediante internet.

La solución es reforzar la seguridad de las personas al conectarse a una red WLAN, con esto no existirá información sustraída por personas no deseadas o hackers.

En este artículo se analizará adecuadamente las vulnerabilidades de la seguridad en dispositivos IoT, protegerlos y deshabilitar el reenvío de puertos innecesarios. Así se establecerá una conexión por medio de canales seguros y de

esta manera se salvaguarda información importarte de usuarios y lo más importante no ser afectados por hackers.

2. Materiales y métodos

2.1. Materiales

2.1.1. Hardware

- Módulo EPS32
- Sensores de:
  - Movimiento
  - Gas
  - Magnético
- Actuador
  - Speaker - Buzzer

2.1.2. Software

- Visual Studio Code
- PlatformIO

2.2. Metodología

Para esta investigación se crea un escenario, en este se realiza pruebas de vulnerabilidad que existe en la seguridad de IoT.

2.3. Construcción

En este análisis IoT se realiza una monitorización de lectura de sensores de forma inalámbrica, se utiliza un módulo ESP32 donde irán conectados tres sensores: uno de movimiento, uno de gas y un magnético.

Módulo ESP32: Es utilizado para integrar todo un dispositivo electrónico en un ambiente. Es un lenguaje de programación Arduino. Se utiliza para integrar todo el dispositivo electrónico en un entorno, tiene dos núcleos, un núcleo para ejecutar funciones wifi y un núcleo para ejecutar programas cargados [6].

ESP32 contiene dos módulos wifi y bluetooth. Dispone de una memoria bastante grande que usa baja potencia y también tiene un sensor táctil interno que lo hace adecuado para su uso en proyectos de desarrollo de sistemas de seguridad de puertas. En esta investigación se utilizaron los pines 25, 32, 33 y 34 para sus respectivas conexiones a los sensores, el ESP32 va conectado a la computadora por un cable USB 2.0 Micro B.

Figura 1. Módulo ESP32

Sensor de Gas: El módulo MQ9 es un dispositivo de circuito integrado impresionable para detectar la existencia de Monóxido de Carbono de 10 a 1000 ppm, al momento que este sensor detecta alguna de las señales [7], este emite una señal analógica versátil dependiendo de la cantidad de gas revelada.

Figura 2. Sensor MQ-9

En la mayoría de los casos, el material de detección es un material de dióxido de estaño (SnO2) que tiene electrones libres en su interior. Estos electrones libres son atraídos por el oxígeno a la superficie del material de detección. En la superficie, el oxígeno se absorbe debido a la superficie calentada y, por lo tanto, no hay electrones libres en el dióxido de estaño [8]. El

resultado es: no hay electrones libres, no hay flujo de corriente eléctrica [8].

Tabla 1. Características del Sensor PIR HC-SR501

Voltaje de Operación	4.5V . . . 5V
Alta densidad de gases	Metano, Butano, GLP, Humo
Concentración	300ppm . . . 10000ppm
Consumo de energía	88mA @5V = 440mW
Duración de precalentamiento	2 minutos

Sensor de Movimiento: El sensor PIR HC-SR501 es capaz de detectar movimientos, el voltaje de entrada es de 5V y 20V. La salida del sensor en alta es de 3.3V cuenta este detecta movimiento y baja 0V cuando no hay detección de movimiento. Su corriente de reposo más o menos es de 50µA, es muy bajo el consumo de energía [9].

Tabla 2. Características del Sensor PIR HC-SR501

Voltaje de entrada	5V 20V o 3.3V
Voltaje de funcionamiento	3.3V
Corriente de reposo	50 µA
Salida de nivel	HIGH 3.3V/LOW 0V
Tiempo de estabilización inicial	60s
Disparo	Simple (L) Repetido (H)
Tiempo de retardo	2.5s a 5min
Distancia de mediación	3m a 7m
Ángulo de medición	Ángulo de cono 110 grados

El HC-SR501 se compone por tres opciones de instalación:

La primera es un único disparador (débil) donde muchos disparadores consecutivos se reconocen como un solo disparador, o un disparador repetitivo (alto) donde se calcula cada disparador encontrado.

La segunda es en tiempo de retardo, este establece cuánto tiempo la salida del HC-SR501 permanece ALTA después de detectar movimiento, de 2,5 segundos a 5 minutos.

La tercera instalación mide la distancia de 3 a 7 metros. El ángulo de medición del HC-SR501 es de 110°, lo que le permite capturar movimientos en un ángulo amplio frente al sensor.

Figura 3. Sensor Movimiento PIR HC-SR501

Los dispositivos termoeléctricos, como los PIR, contienen elementos de material cristalino que generan una carga eléctrica cuando se exponen a la radiación infrarroja. El cambio en la cantidad de radiación que provoca el cambio de voltaje es medido por el amplificador [10].

Sensor Magnético: El sensor MC38 es usado para propósitos de seguridad en el hogar, es compatible con Arduino, Raspberry Pi, Visual Studio Code, ESP32, entre otros, de esta manera es potencial para construir muchos sistemas de seguridad.

Figura 4. Sensor Magnético MC38

El módulo del sensor MC30 regularmente es cerrado, por lo cual envía un dato lógico (1) cuando las dos partes del sensor están conectadas y (0) cuando una de las partes es separada.

Tabla 3. Características del Sensor MC30

Voltaje de alimentación máxima	100V

Corriente máxima	0.5A
Potencia nominal:	3 W
Mecanismo	Normalmente Cerrado (NC)
Distancia de activación mínima	15mm
Distancia de activación máxima	25mm
Largo del cable	20cm
Dimensiones	27 mm x 14 mm x 8 mm
Peso	16 gramos

Speaker - Buzzer: Es un dispositivo que convierte una señal eléctrica a una señal de audición, está compuesta por una bobina y un electroimán.

Figura 5. Speaker 5V

Este dispositivo se utiliza para la construcción de alarmas sonoras, estas pueden ir ensambladas en tarjetas electromagnéticas, multímetros, laptops, alarmas de autos, entre otros.

Funciona de la siguiente manera: Se conecta la corriente, pasa por la bobina del electroimán, ahí produce el campo magnético que hace temblar una lámina de acero cubierta de la armadura.

Tabla 4. Características del Sensor MC30

Voltaje de operación	**5V DC**
Corriente máxima	30 mA
Dimensiones	12 mm x 9.5 mm
Peso	2 gramos
Frecuencia de resonancia	23K Hz
Salida de sonido mínimo a 10 cm	85 dB
Temperatura de trabajo	-20°C a 70°C
Temperatura de almacenamiento	-30°C a 105°C
Pines	VCC (+) GND

2.4. Implementación

Para la obtención de datos del sensor de movimiento, gas y magnético se puede obtener mediante el Módulo ESP32, este dispositivo enviará de forma inalámbrica a la nul

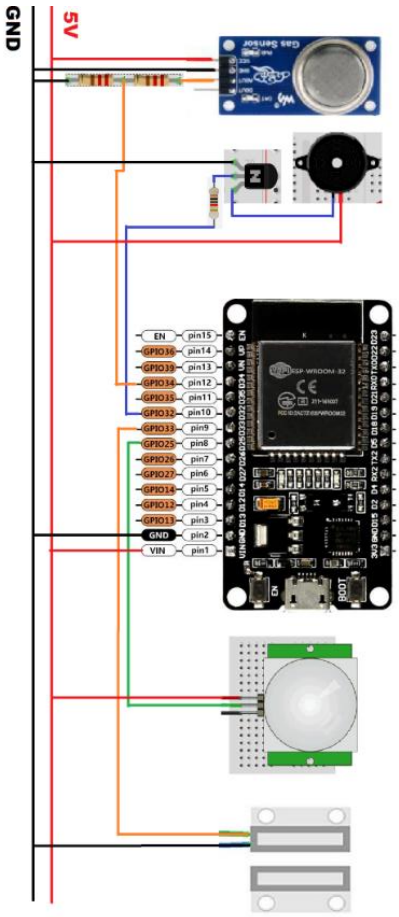


Figura 6. Bosquejo de Conexión ESP32 con sensores y un Speaker

Estos sensores enviarán datos mediante módulo ESP32 y serán almacenados en la nube a diferentes plataformas, dichas plataformas son: Firebase, Cayenne y Ubidots.

En la figura 7, se observa el escenario elaborado con el módulo ESP32.

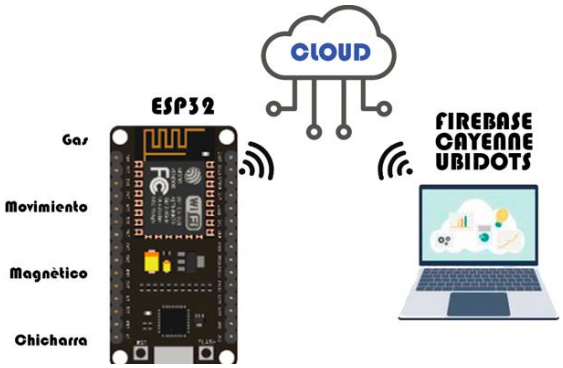


Figura 7. Escenario ESP32 conectado a la nube

2.5. Conexión a las plataformas

En los últimos años se han creado plataformas IoT con software que permite la conexión con dispositivos, sensores y equipos industriales de manera digital, de esta forma se genera una red para la comunicación y creación de información importante [11].

Para generar la conexión y enviar datos entre el ESP32 a la plataforma Firebase, se genera un código de programación, donde se crean las credenciales de la plataforma, este permite la conexión del módulo a internet y de esta manera se establece una buena comunicación. Para ese caso solicita el Host y la Autenticación, estas son únicas y son generadas en la plataforma.

```
#define FIREBASE_HOST "control-esp32-43cc0-default-rtdb.firebaseio.com"
#define FIREBASE_AUTH "k6gpDxj1PpZ9bgs2p6ZuCLvcRpx10eItcFXJiww3"

#define WIFI_SSID "SPineida1706"
#define WIFI_PASSWORD "1752154284001"

// Potentiometer is connected to GPIO 34 (Analog ADC1_CH6)
const int PinADC = 34;
const int InSensorMov = 25;
const int InSensorMag = 33;
const int Chicharra = 32;

int EstSenMov = 0;
int EstSenMag = 0;
```

Figura 8. Código de conexión a la plataforma Firebase

La conexión entre el ESP32 y la plataforma Cayenne myDevices solicita Nombre del Usuario, contraseña e ID del cliente, estas credenciales son únicas y generales en la plataforma.

En la figura 9, se muestra el código de conexión a la plataforma Cayenne myDevices.

```
// WiFi network info.
char ssid[] = "SPineida1706"; //NOMBRE DE LA RED
char wifiPassword[] = "1752154284001"; // CLAVE DE LA RED

// Cayenne authentication info. This should be obtained from t
char username[] = "8bc84800-e67a-11ec-a681-73c9540e1265";
char password[] = "9f67e3402d494e0f6205ad4bb0b163924710672d";
char clientID[] = "77922650-e67d-11ec-9f5b-45181495093e";

// Potentiometer is connected to GPIO 34 (Analog ADC1_CH6)
const int PinADC = 34;
const int InSensorMov = 25;
const int InSensorMag = 33;
const int Chicharra = 32;

int EstSenMov = 0;
int EstSenMag = 0;
```

Figura 9. Código de conexión a la plataforma Cayenne myDevices

Para generar la conexión entre el ESP32 y la plataforma Ubidots solicita su TOKEN que es único para cada proyecto creado. Como muestra la figura 10.

```
const char *UBIDOTS_TOKEN = "BBFF-ZY77BnoyDyo4zeBZNe5D3YLYOF6G78";
const char *WIFI_SSID = "SPineida1706";
const char *WIFI_PASS = "1752154284001";

const char *DEVICE_LABEL_1 = "SensoresEsp";
const char *VARIABLE_LABEL_1 = "VarMag";
const char *VARIABLE_LABEL_2 = "VarMov";
const char *VARIABLE_LABEL_3 = "VarGas";

int periodo = 5000;  // tiempo que esta el LED en alto y bajo
unsigned long tiempoAnterior = 0;  //guarda tiempo de referencia pa

// Potentiometer is connected to GPIO 34 (Analog ADC1_CH6)
const int PinADC = 34;
const int InSensorMov = 25;
const int InSensorMag = 33;
const int Chicharra = 32;

int EstSenMov = 0;
int EstSenMag = 0;
```

Figura 10. Código de conexión a la plataforma Ubidots

2.6. Datos mostrados en las plataformas

A continuación, se muestra las capturas de pantallas de las plataformas, donde muestra información de los tres sensores y el controlador.

Al momento de conectarse el módulo ESP32 con la plataforma Firebase. Se observa en la figura 11.

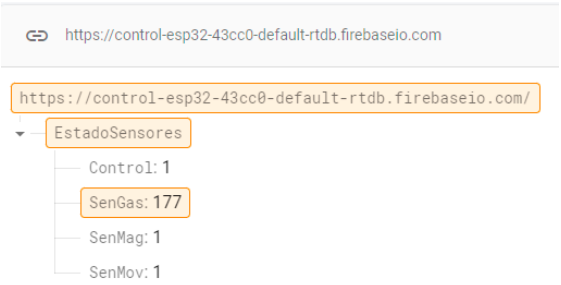


Figura 11. Información obtenida en Firebase

Conexión el módulo ESP32 con la plataforma Ubidots. Se observa en la figura 12.

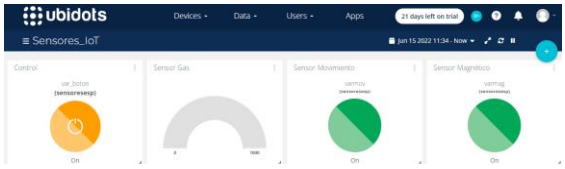


Figura 12. Información obtenida en Ubidots

Conexión el módulo ESP32 con la plataforma Cayenne. Se observa en la figura 13.

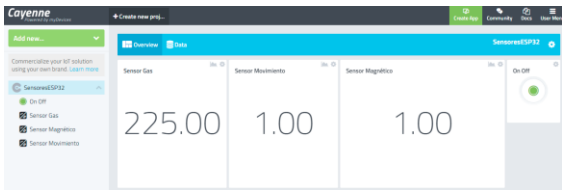


Figura 13. Información obtenida en Cayenne myDevices

2.7. Control remoto

Es la posibilidad de hacer tareas en un ordenador sin estar físicamente con un equipo informático. Cumplen con una labor importante en los entornos para fácil acceso y más cuando se presenta un riesgo [12].

Mediante el control remoto se controla la activación de los sensores en cada una de las plataformas. Se crea un interruptor donde se logra apagar el Speaker.

En este sentido las condiciones de los sistemas de comunicación se convierten en un objetivo importante para la construcción de sistemas de monitoreo y control, debido a su buen rendimiento y seguridad que brinda [12].

2.8. Herramientas para analizar y capturar datos

Wireshark: La metodología de monitorizar datos en Wireshark se trata de analizar protocolos open – source y obtener paquetes que se transmiten en la red durante él envió de datos desde los sensores hacia el módulo ESP32 y luego a las plataformas.

Usar el ataque y ver la vulnerabilidad que existe entre el enlace del módulo ESP32 y aplicación.

Sistema Operativo Kali Linux

Es distribuido por Linux de código abierto especialista de herramientas para el análisis y diseño de la seguridad, este ayuda a realizar embestidas a los enlaces inalámbricos que existen entre el módulo ESP32 y las aplicaciones.

2.9. Ataque

ARP Spoofing **s**e basa en el envenenamiento de las tablas ARP. Es un ataque que utilizan los hackers para entrar a una red local y robar paquetes de datos que están transportándose, de esta manera pueden controlar el tráfico que existe y también pueden detenerlo. ARP es necesario para la transmisión de datos en la red Ethernet.

Se encarga de la suplantación para enviar mensajes falsos a la Ethernet. Con este ataque acomete la dirección MAC con la dirección IP y podrá controlar todo el tráfico completo.

Este ataque puede llegar a substraer datos sensibles de empresas o usuarios. Es uno de los más comunes utilizados por ciberdelincuentes ya que se filtra de una manera muy fácil los paquetes que son enviados por la red, a diferencia de otros ataques no es tan sencillo visualizar paquetes que circulan en la red.

3. Resultados y discusión

De acuerdo con el análisis aplicado se procede a realizar el ataque que se propuso al Módulo ESP32 conectado mediante Kali Linux, de esta manera se obtiene los siguientes resultados.

3.1. Ataques Plataformas

3.1.1. Ataque Spoofing con la herramienta Ettercap de Kali Linux a la plataforma Firebase

Mediante Kali Linux y la herramienta de Ettercap se escanea todos los hosts que están conectados a la red, de esta manera identificamos la IP de nuestro módulo IoT, la IP en este caso es 192.168.100.221 y nuestra puerta de enlace 192.168.100.1. Como muestra la figura 14.

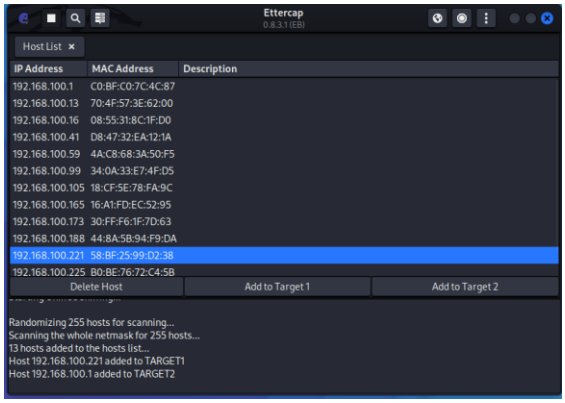


Figura 14. Captura de los hosts conectados a la red en Ettercap

Seleccionamos en Target1 a nuestra víctima de suplantación de MAC 192.168.100.221 y como Target2 la puerta de enlace que por esta se suplantará su MAC 192.168.100.1 y así se consigue toda la información enviada por la IP atacada.

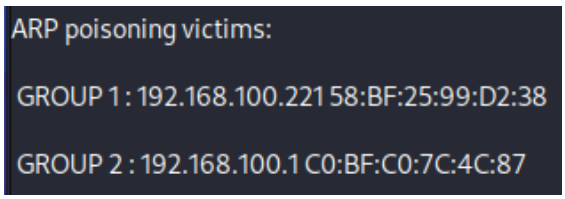


Figura 15. Remplazo MAC

Desde Visual Studio Code se muestran la información que están siendo enviada a la plataforma de Firebase. Como muestra la figura 16.

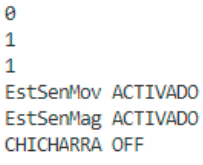


Figura 16. Datos enviados a Firebase

Aplicando el ataque pierde la conexión entre el módulo ESP32 y la plataforma. Como muestra la figura 17.

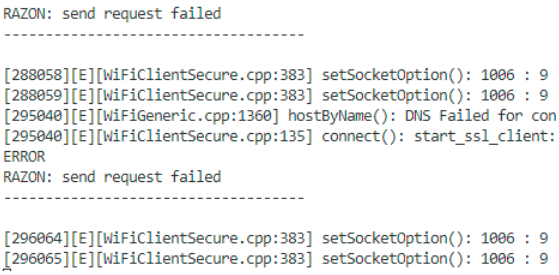


Figura 17. Pérdida de datos Firebase

Wireshark indica la actividad que está realizando el módulo inalámbrico ESP32 hasta la plataforma Firebase. Como indica la figura 18.

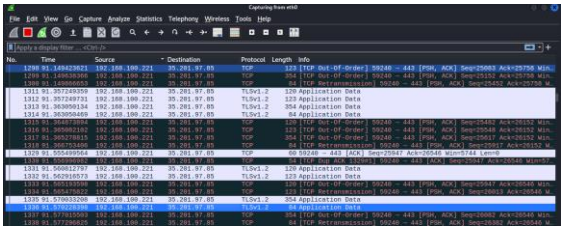


Figura 18. Captura de paquetes enviados en Wireshark enviados de la Plataforma Firebase

Los datos mostrados en Wireshark son encriptados ya que no se muestran en primer plano, es decir son seguros. Como indica la figura 19.

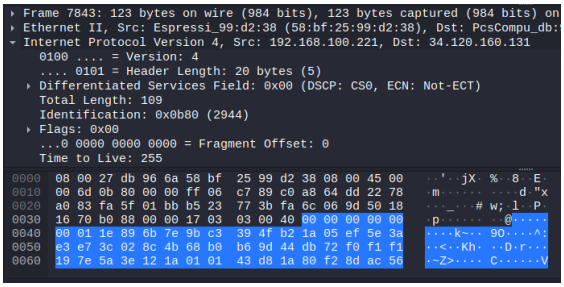


Figura 19. Captura de paquetes encriptados

3.1.2. Ataque Spoofing con la herramienta Ettercap de Kali Linux a la plataforma Ubidots

Mediante Kali Linux y la herramienta de Ettercap se escanea todos los hosts que están conectados a la red, de esta manera identificamos la IP de nuestro módulo IoT que en este caso la IP es 192.168.100.14 y nuestra puerta de enlace 192.168.100.1 como se muestra en la figura 20.

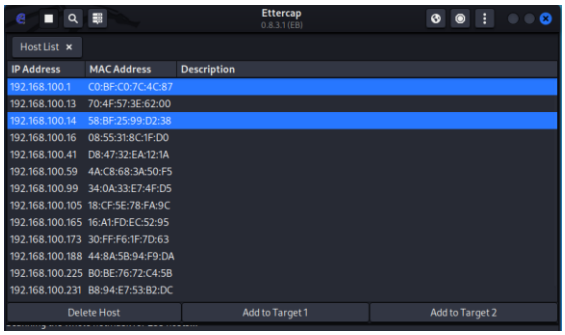


Figura 20. Captura de los hosts conectados a la red en Ettercap

Se selecciona en Target1 a nuestra víctima de suplantación de MAC 192.168.100.14 y como Target2 la puerta de enlace que por esta se suplantará su MAC 192.168.100.1 y así obtenemos toda la información enviada por la IP atacada.

Se logra tomar el control de los paquetes que están recibidos y enviados. En la figura 21 se muestra.

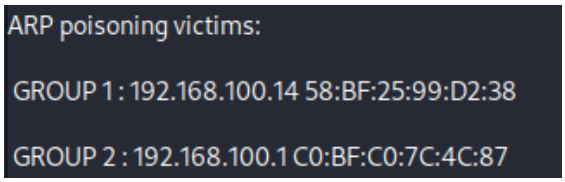


Figura 21. Reemplazo de MAC

Se utiliza el analizador de protocolos Wireshark, ya que esta muestra todos los paquetes que se están enviando por la red.

Wireshark indica la actividad que está realizando el módulo inalámbrico ESP32 hasta la plataforma Firebase. Como muestra la figura 22.

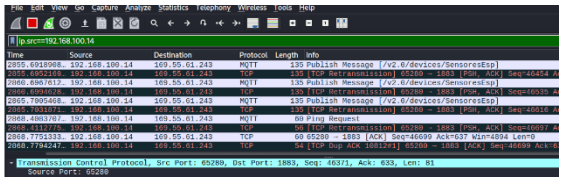


Figura 22. Datos capturados en Wireshark

En la plataforma Ubidots mediante el control remoto que se obtuvo, se apaga todos los sensores. Como se muestra en la figura 23.

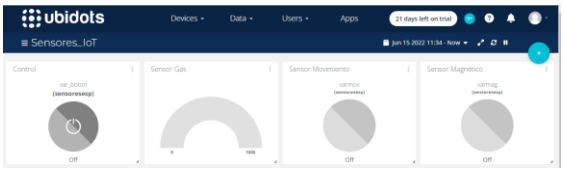


Figura 23. Sensores apagaos en Ubidots

De esta manera en Wireshark se observa que no hay transmisión de datos, todos los sensores están 0, eso quiere decir que no hay transmisión de señales. Como indica la figura 24.

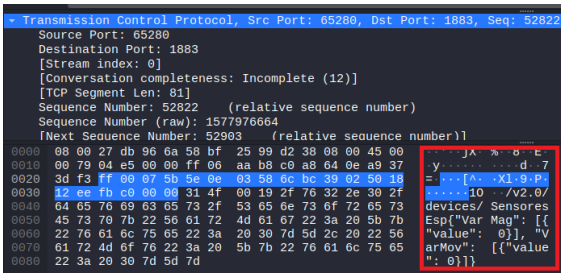


Figura 24. Datos en 0 ya que no se envía información por los sensores apagados

De la misma manera se activan los sensores a través de plataforma. Como muestra la figura 25.

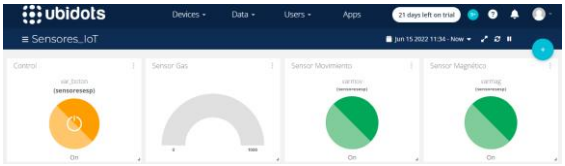


Figura 25. Sensores encendidos desde la Plataforma Ubidots

Una vez encendidos los sensores el speaker comienza a dar señal.

Los datos que se están enviando y recibiendo aparecen en Wireshark son los mismos datos que se ve en la consola de Visual Studio Code. Como indica la figura 26.

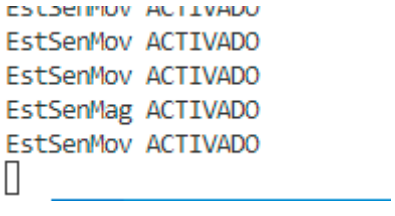


Figura 26. Datos capturados en Visual Studio Code de la Plataforma Ubidots

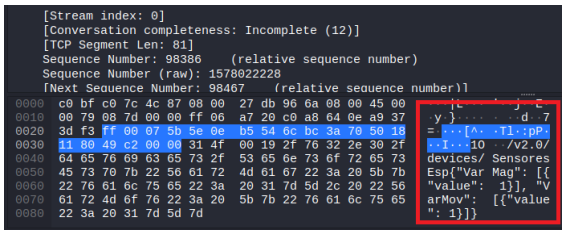


Figura 27. Datos capturados en Wireshark no encriptados de la Plataforma Ubidots

3.1.3. Ataque Spoofing con la herramienta Ettercap de Kali Linux a la plataforma Cayenne

En Kali Linux utilizamos la herramienta Ettercap donde mostrará todos los hosts que están conectados a nuestra red, se identifica la IP de nuestro módulo que en este caso la IP es 192.168.100.231 y nuestra puerta de enlace 192.168.100.1 como se muestra en la figura 28.

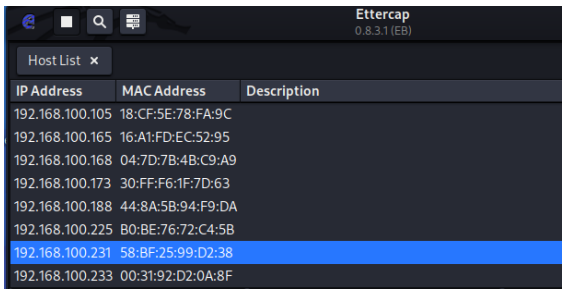


Figura 28. Hosts detectados a la red

Seleccionamos en Target1 a nuestra víctima de suplantación de MAC 192.168.100.231 y como Target2 la puerta de enlace que por esta se suplantará su MAC 192.168.100.1 y así extraemos toda la información enviada por la IP atacada.

Se obtiene el control de los paquetes que están recibidos y enviados. En la figura 29 se muestra.

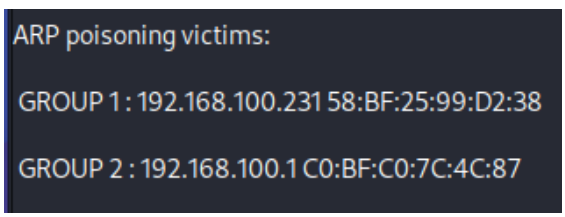


Figura 29. Reemplazo de MAC

Se utiliza Wireshark para mostrar él envío y recibido de paquetes que están en la red. Como indica la figura 30.

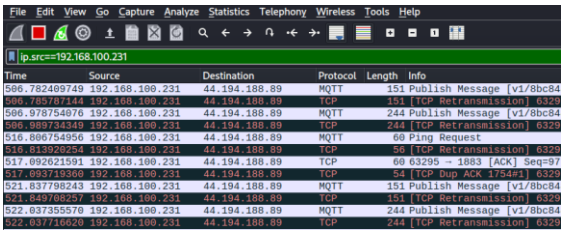


Figura 30. Datos capturados en Wireshark

En la plataforma Cayenne se indica los datos que envían los sensores del módulo ESP32. Como se muestra en la figura 31.

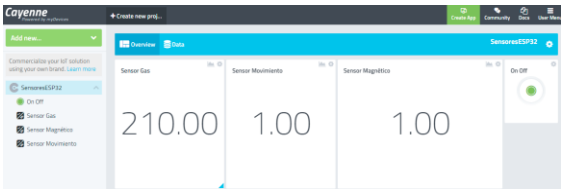


Figura 31. Sensores activados desde la Plataforma Cayenne

Desde Visual Studio Code se muestran la información que están siendo enviada a la plataforma de Cayenne. Como muestra la figura 32.

```
[2676] Connecting to mqtt.mydevices.com:1883
[3279] Connected
Enviando Datos a Cayenne
Enviando Datos a Cayenne
Enviando Datos a Cayenne
Enviando Datos a Cayenne
EstSenMag ACTIVADO
CHICHARRA OFF
EstSenMov ACTIVADO
CHICHARRA OFF
```

Figura 32. Información mostrada en Visual Studio Code

Aplicando el ataque se pierde la conexión entre el módulo IoT y la plataforma de Cayenne.

```
[404039] Network connect failed
[412039][E][WiFiGeneric.cpp:1360] hostByName(): DNS Failed for mqtt.mydevices.com
[412039] Network connect failed
[420043][E][WiFiGeneric.cpp:1360] hostByName(): DNS Failed for mqtt.mydevices.com
[420043] Network connect failed
[428039][E][WiFiGeneric.cpp:1360] hostByName(): DNS Failed for mqtt.mydevices.com
[428039] Network connect failed
[436039][E][WiFiGeneric.cpp:1360] hostByName(): DNS Failed for mqtt.mydevices.com
[436039] Network connect failed
[444039][E][WiFiGeneric.cpp:1360] hostByName(): DNS Failed for mqtt.mydevices.com
[444039] Network connect failed
```

Figura 33. Desconexión entre el módulo ESP32 y Cayenne

Los datos mostrados en Wireshark son encriptados y no se muestran en primer plano, es decir, son seguros. Como indica la figura 34.

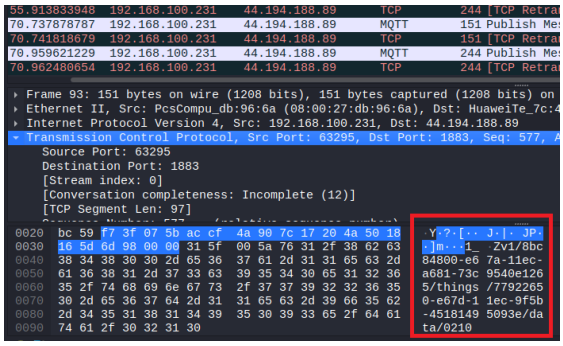


Figura 34. Captura de paquetes encriptados de la Plataforma Cayenne

3.2. Soluciones para el ataque

Protocolo ARP y Spoofing

Una de las soluciones para este ataque sería el cifrado de tráfico DNS, este protege los datos. Otra solución es usando una VPN, esto garantizará la confiabilidad de las conexiones de la red.

Es recomendable ingresar a páginas que tengan el protocolo HTTPS para garantizar seguridad ya que este brinda información cifrada.

3.3. Discusión

En base a las pruebas realizadas creando un escenario en tiempo real con el módulo ESP32 y tres sensores conectados para enviar datos a las tres plataformas, se obtiene los siguientes resultados.

Con respecto a la plataforma Firebase, una de las plataformas IoT creada por Google, se obtiene el control remoto de manera de cuadro de texto, es decir, si en el control está el número “1” los sensores están activos y se recibirá los datos que envía inalámbricamente del módulo ESP32, caso contrario si en el cuadro de texto está el número “0” los sensores son desactivados, tal como indica la figura 11, de esta manera se observa el estado de los sensores en cualquier parte que se tenga acceso a internet. Sobre el investimento ARP Spoofing se logra atacar a la ip del módulo IoT, como indica la figura 14.

En Wireshark se observa el envío de paquetes a la plataforma, claramente se observa que los paquetes son encriptados, esto quiere decir que la conexión entre al módulo ESP32 a la plataforma Firebase es segura puesto que se observa protocolos TLSv1.2, de esta manera no se obtiene datos visibles a primer plano. De esta manera las vulnerabilidades para Firebase no existen y es muy recomendable el uso de esta plataforma.

Con respecto a la plataforma Cayenne, es una plataforma para dispositivos IoT de la misma manera se logra obtener el remoto agregando un Button que controle los datos recibidos del dispositivo IoT, si el Button está en color verde los datos están transmitiendo tal como muestra la figura 13. De igual manera se logra obtener esa interface en cualquier computadora que tenga acceso a internet. Sobre el ataque ARP Spoofing se obtener la IP del módulo IoT, como indica la figura 28. En Visual Studio Code se ve la pérdida de comunicación que existe entre el dispositivo IoT y al AP, como se muestra en la figura 33.

En Kali Linux a través de Wireshark se observa todos los paquetes que se están enviando a la plataforma Cayenne, se muestra que los paquetes enviados están encriptados, esto quiere decir que la conexión entre al módulo ESP32 a la plataforma Cayenne es segura puesto que se observa protocolos MQTT, este transmite datos crudos en forma de binarios, de esta manera no se obtiene datos visibles a primer plano y los datos no caerán en personas maliciosas. Los usuarios que utilizarán esta plataforma tendrán su información muy protegida.

Con respecto a la plataforma Ubidots es una plataforma IoT que permite enviar datos de sensores a la nube, así mismo se obtiene el control remoto mediante un Button como muestra la figura 12. Los datos son enviados cuando el control esté encendido y se logra controlar a través de un Smartphone ya que para PlayStore existe una aplicación.

Mediante Kali Linux en Wireshark se visualiza los paquetes que se están trasmitiendo del dispositivo IoT a Ubidots en tiempo real, se observa que los datos están siendo obtenidos sin ningún tipo de encriptación ni seguridad. Se afirma que este análisis es peligroso, es decir, existe vulnerabilidad al enviar paquetes desde el módulo ESP32 a la plataforma, en la figura 26 y figura 27, se observan los mismos datos enviados en primer plano. Al momento que una persona maliciosa esté en la red, esta podrá extraer esos datos y exponer al usuario.

Firebase y Cayenne resultaron ser plataformas seguras, ya que los paquetes se están enviando encriptados y con respecto a la plataforma Ubidots los datos son accesibles y no es recomendable utilizarla.

4. Conclusiones

Los resultados obtenidos con el escenario que se armó en tiempo real para enviar datos a diferentes plataformas mediante el módulo ESP32 de forma inalámbrica se obtiene el control remoto, de esta manera se vigilará desde cualquier lugar que exista acceso a internet. Realizando los respectivos ataques se encuentra vulnerabilidad en una de ellas, se trata de la Plataforma Ubidots, donde se pudo observar datos en primer plano del sensor de movimiento, gas y magnético, esto ocasiona inseguridad al usar esta plataforma. Las conexiones seguras que existieron en este análisis fue en la plataforma Firebase y Cayenne, dichas plataformas mandan sus paquetes encriptados, ya que utilizan protocolos como MQTT, este protocolo transmite datos crudos y formato de binarios y TLS v1.2 que en la actualidad este protocolo se encarga de encriptar datos que produce la web.

Referencias

[1] N. A. ARIAS SILVA, «ANÁLISIS DE SEGURIDAD DE VULNERABILIDADES Y ATAQUES,» Bogota , 2019.

[2] C. Lee y A. Fumagalli, «Internet of Things Security - Multilayered Method For End to End Data Communications Over Cellular Networks,» *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 24-28, 2020.

[3] F. Lidanta, A. Almaarif y A. Budiyono, «Vulnerability Analysis of Wireless LAN Networks Using Penetration Testing Execution Standard: A Case Study of Cafes in Palembang,» pp. 1-5, agosto 2021.

[4] S. Verma, Y. Kawamoto y N. Kato, «A Network-Aware Internet-Wide Scan for Security Maximization of IPv6-Enabled WLAN IoT Devices,» vol. 8, nº 10, pp. 8411-8422, 2021.

[5] K. Agarwal, A. Agarwal y G. Misra, «Review and Performance Analysis on Wireless Smart Home and Home Automation using IoT,» pp. 629-633, 2019.

[6] Andreas, C. R. Aldawira, H. W. Putra, N. Hanafiah, S. Surjarwo y A. Wibisurya, «Door Security System for Home Monitoring Based on ESP32,» *Procedia Computer Science*, pp. 10-11, 2019.

[7] A. Fadlilah, «Repository Universitas Riau,» enero 2020. [En línea]. Available: https://repository.unri.ac.id/handle/123456789/10204. [Último acceso: 08 junio 2022].

[8] DIYI0T, «Tutorial del sensor de gas MQ2 para Arduino, ESP8266 y ESP32,» 15 septiembre 2020. [En línea]. Available: https://diyi0t.com/mq2-gas-sensor-arduino-esp8266-esp32/. [Último acceso: 17 mayo 2020].

[9] cdaviddav, «ElOsciloscopio,» 16 Marzo 2021. [En línea]. Available: https://elosciloscopio.com/hc-sr501-sensor-de-movimiento-pir-para-arduino-esp8266-y-esp32/. [Último acceso: 11 mayo 2022].

[10] C. Volt, «RogerBit,» 29 Enero 2021. [En línea]. Available: https://rogerbit.com/wprb/2021/01/detector-de-movimiento-con-luz-esp32-y-notificaciones-por-telegram/. [Último acceso: 11 Mayo 2022].

[11] B. IoT, «barbara,» 16 Abril 2021. [En línea]. Available: https://barbaraiot.com/blog/plataformas-iot-que-son-y-como-pueden-beneficiar-a-tu-empresa/. [Último acceso: 2022].

[12] L. Serna Guarín, L. J. Morantes Guzmán y E. Delgado Trejos, Transferencia óptima de datos para el monitoreo y control, I. T. Metropolitano, Ed., iTM, 2015, pp. 2-3.

[13] S. Verma, Y. Kawamoto y N. Kato, «A Network-Aware Internet-Wide Scan for Security Maximization of IPv6-Enabled WLAN IoT Devices,» vol. 8, nº 10, pp. 8411-8422, 2021.