UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Vínculos
https://revistas.udistrital.edu.co/index.php/vinculos/

Actualidad Tecnológica

Análisis de seguridad en redes LPWAN para dispositivos IoT

Security analysis in LPWAN networks for IoT devices

Cristian Arley González González[1], Fernando Arévalo Tapias[2], Jairo Hernández Gutiérrez[3]

Para citar: C. A. González-González, F. Arévalo-Tapias, J. Hernández-Gutiérrez, "Análisis de seguridad en redes LPWAN para dispositivos IoT". *Revista Vínculos: Ciencia Tecnología y Sociedad,* vol. 16, no. 2, julio-diciembre de 2019, pp. 252-261. DOI: 10.14483/2322939X.15712

Enviado: 12/06/18/ Recibido: 13/06/18/ Aprobado: 12/07/18

Resumen

Este documento muestra el análisis realizado sobre la seguridad en las tecnologías LPWAN, centrando el estudio en las vulnerabilidades presentes en la tecnología Sigfox. La metodología usada se basa en la guía de desarrollo de pruebas presentada por OWASP, que consiste básicamente en la identificación de vulnerabilidades y recomendaciones de pruebas para validarlas. Adicional al uso de la metodología, se realizó una investigación documental sobre vulnerabilidades en las tecnologías LPWAN similares. Se desarrollaron pruebas prácticas basadas en recomendaciones de la industria para el uso seguro del IoT, estas fueron realizadas en un entorno de pruebas básico de comunicación de Sigfox usando la tarjeta Xkit RCZ4; se obtuvo como resultado vulnerabilidades en los dispositivos físicos, en el diseño de estos y en el Backend de Sigfox. Se realizó una comparación con las tecnologías LPWAN en el mercado y se analizó si Sigfox es realmente la red más segura en el campo del IoT como se vende en el mercado.

Palabras Clave: dispositivos, IoT, LoRaWAN, LPWAN, seguridad, Sigfox, vulnerabilidades.

Abstract

This document shows the analysis carried out on the security of LPWAN technologies, focusing the study on the vulnerabilities present in Sigfox technology. The methodology used is based on the test development guide presented by OWASP, which consists basically of identifying vulnerabilities and testing recommendations to validate them. In addition to the use of the methodology, documentary research on vulnerabilities in similar LPWAN technologies was carried out. Practical tests were developed based on industry recommendations for the safe use of IoT, these were performed in a basic Sigfox communication test environment using the Xkit RCZ4 card, resulting in vulnerabilities in physical devices, in their design and in the Sigfox Backend. A comparison was made with LPWAN technologies in the market and it was analyzed if Sigfox is really the safest network in the field of IoT as it is sold in the market.

Keywords: devices, IoT, LoRaWAN, LPWAN, security, Sigfox, vulnerabilities.

1. Tecnólogo en electrónica, Ticbridge. Correo electrónico: proyectos1@ticbridge.com ORCID: https://orcid.org/0000-0002-0577-6946
2. Tecnólogo en electrónica, Ericsson,. Correo electrónico: fernando.arevalo@fsorlam.com ORCID: https://orcid.org/0000-0001-5371-243X
3. Magíster en Administración de Empresas con especialidad en dirección de proyectos, especialista en Servicios Telemáticos e Interconexión de Redes; ingeniero de sistemas. Asesor/consultor de IT para Intelcol SAS. Correo electrónico: jairo.hernandez@intelcolsas.com. ORCID: https://orcid.org/0000-0003-3908-2763

ISSN 1794-211X • e-ISSN 2322-939X • Vol 16, No 2 (julio-diciembre 2019). pp.252-261.Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

1. Introducción

En los últimos años, el internet de las cosas (IoT, por sus siglas en inglés) se ha incorporado a la economía de forma progresiva, generando un diverso mercado de soluciones y comodidades tanto para la industria como para el hogar. Las aplicaciones de IoT se pueden usar para hogares inteligentes, medición inteligente, monitoreo de fábricas, agricultura, edificios inteligentes, etc. Las tecnologías inalámbricas como Bluetooth, WiFi, ZigBee, etc., solían cumplir con los requisitos de comunicación para el IoT; sin embargo, debido a que son tecnologías de conectividad para corto alcance, limitaban la funcionalidad del IoT. Para superar las limitaciones de los protocolos de corto alcance se introducen redes de área amplia y baja potencia (LPWAN), ofreciendo una conectividad de largo alcance en el orden de kilómetros [1]. LPWAN permite que los dispositivos IoT intercambien pequeños mensajes a largas distancias con un nivel de consumo muy bajo de energía, logrando un funcionamiento de los dispositivos de varios años con baterías pequeñas [2], siendo por estas características una solución muy bien aceptada en el ámbito industrial por sus múltiples usos.

Se han desarrollado diferentes tecnologías que usan las redes LPWAN para IoT, por ejemplo, Sigfox [3], LoRaWAN [4] y NB-IoT [5], que se presentan como una solución a la conectividad de los dispositivos IoT. Aunque estas tecnologías han sido muy bien aceptadas en la industria, son foco de crítica por la seguridad presentada en los dispositivos [6], probablemente debido a la fama de la inseguridad del IoT basado en WiFi. Sigfox es la red que vende su solución como la más confiable y segura en el mercado, pues la infraestructura sobre la seguridad de sus dispositivos y redes es más robusta que las demás redes bajo el mismo concepto LPWAN. Al ver la poca documentación sobre la seguridad en la red Sigfox, se escoge la red LPWAN como principal para este artículo, analizando la comunicación y seguridad de Sigfox mediante un entorno de pruebas del uso de esta tecnología.

1.1. Antecedentes y trabajos relacionados

La mayoría de los estudios realizados sobre la seguridad en redes LPWAN usadas en IoT se enfocan en LoRaWAN. En el estudio realizado por X. Yang, E. Karampatzakis, C. Doerr, y F. Kuipers [7], se genera un entorno de pruebas controlado de LoRaWAN para definir las características de seguridad presentes en dicha red, analizando las vulnerabilidades y diseñando cinco ataques: (a) un ataque de repetición que conduce a una denegación de servicio selectiva en dispositivos IoT individuales, (b) recuperación de texto sin formato, (c) modificación de mensajes maliciosos, (d) falsificación en la entrega de informes y (e) un ataque de agotamiento de la batería. En el análisis de Mr. Deepu Job sobre LoRaWAN [1], se habla de los mecanismo y vulnerabilidades de seguridad encontrados en las redes LPWAN, mostrando la diferencia entre las tecnologías y una comparación de estas en cuanto seguridad, concluyendo con las vulnerabilidades presentes en LoRaWAN.

En cuanto NB-IoT y Sigfox, se ven estudiadas en el análisis de Laurentiu Coman [8], donde se tratan las vulnerabilidades de las redes LPWAN como capa de enlace. Posteriormente, se presentan tres escenarios prácticos de aprovechamiento de vulnerabilidades como lo son: en LoRaWAN una falsificación de paquetes con fuerza bruta MIC, en Sigfox una denegación de servicio de dispositivo final a partir de un ataque de repetición y en NB-IoT el autor aprovechó la opción de conexión por IP para hacer un reconocimiento de red obteniendo la IP de los dispositivos finales, haciéndolos vulnerables a un ataque desde WiFi. Al no tener una seguridad robusta como una computadora, se hace posible cualquier tipo de control sobre estos dispositivos.

En la comparativa realizada por Franklin Heath Ltd [9], se analizan las redes LTE-M, NB-IoT, EC-GSM-IoT LoRaWAN y Sigfox, comparándolas a partir de las características de comunicación, seguridad y energía, deteniéndose en cada uno de los conceptos tenidos en cuenta.

El principal aporte de este documento es ofrecer un análisis específico sobre la seguridad en Sigfox en contraste con las demás tecnologías LPWAN en el mercado, dando un punto de vista sobre la seguridad presentada en esta.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 16, No 2 (julio-diciembre 2019). pp.252-261.Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

2. Metodología

Para el desarrollo de las pruebas, se utilizó la metodología de seguridad de Open Web Application Security Project (OWASP), una una organización benéfica mundial sin fines de lucro centrada en mejorar la seguridad del *software*, llegando por su trayectoria a una posición única de proporcionar información imparcial y práctica sobre AppSec (seguridad de aplicaciones) a individuos, corporaciones, universidades, agencias gubernamentales entre otras organizaciones en todo el mundo. Al operar como una comunidad de profesionales afines, OWASP emite herramientas de *software* y documentación basada en el conocimiento sobre seguridad de aplicaciones [10]. Dentro de su metodología recomienda un conjunto de pruebas que se dividen en diez subcategorías (recopilación de información, pruebas de gestión de la configuración, pruebas de la lógica de negocio, pruebas de autenticación, pruebas de autorización, pruebas de gestión de sesiones, pruebas de validación de datos, pruebas de denegación de servicio, pruebas de servicios web, pruebas de AJAX) para la detección de vulnerabilidades en los sistemas [11]. Se analizaron los impactos y riesgos de las posibles vulnerabilidades a partir del dispositivo usado, apoyando esta metodología con una investigación de documentos que abordaban el tema de vulnerabilidades presentes en las tecnologías LPWAN. Una vez terminada la investigación de seguridad en otras tecnologías y el seguimiento de la metodología de OWASP, se inició una verificación en las capas de comunicación de la tecnología Sigfox en busca de la presencia de vulnerabilidades en el entorno de pruebas configurado de Sigfox, enfocado en las capas de red que se creían susceptibles a ser vulnerables.

2.1. Entorno de pruebas de Sigfox

Para el desarrollo de las pruebas, se configuró una conexión de un dispositivo Sigfox, el cual se muestra en el diagrama de red de la Figura 1.

Figura 1. Diagrama del entorno de pruebas Sigfox **Fuente:** elaboración propia.

El entorno de pruebas se compone por:

- Tarjeta programable Xkit Thinxtra: la tarjeta usada para estas pruebas fue el modelo de desarrollo Dev Xkit Thintrax RCZ4, que es la versión disponible para ser usada en Australia, Nueva Zelanda, Asia y Latinoamérica. Esta tarjeta tiene la funcionalidad de conectarse al operador de Sigfox en Colombia que es WND, una de las empresas prestadoras de servicios de redes LPWAN para IoT [12], esta conexión viene por un año en el plan básico de comunicación de Sigfox. La tarjeta viene con una placa de programación Arduino Uno, una antena de 10 cm aproximadamente para la banda de los 900 MHz y un conjunto de sensores integrados en la placa, de los cuales se usó el sensor de temperatura para estas pruebas [13].
- Enlace de radio: es la comunicación realizada entre los dispositivos IoT y las estaciones base (BTS). De fábrica no es un enlace cifrado, ya que se vende como un servicio adicional de Sigfox.
- Estación base (BTS): al manejar Sigfox la frecuencia usada por GSM, aprovecha las BTS de la telefonía móvil para hacer de estas el primer punto de conexión de los dispositivos IoT a la red de Sigfox. Las BTS son los equipos que reciben la señal móvil para ser transmitida en la red del operador [14], en este caso reciben la señal de radio enviada por el dispositivo Sigfox.
- Enlace de internet: por medio de este enlace se envían los datos que llegan a la red de BTS a los

ISSN 1794-211X • e-ISSN 2322-939X • Vol 16, No 2 (julio-diciembre 2019). pp.252-261.Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

servidores de Sigfox, cifrado por HTTPS.
- Backend de Sigfox: es el portal web que permite la configuración de alertas de los sensores, configurando diferentes herramientas de tratamiento de datos y visualización para el usuario.
- Herramientas de visualización: estas herramientas permiten usar los datos que llegan al Backend para ser visualizados de forma más dinámica para el usuario final, con herramientas como AWS IoT, AWS Kinesis, entre otras.
- A partir del entorno de pruebas seleccionado, se procedió a ver los puntos débiles en los cuales se podrían encontrar vulnerabilidades a estudiar; para esto, se tomó como base la guía "IoT Testing Guides" [15] de OWASP, una guía enfocada en evaluar la seguridad de los dispositivos IoT en general, por lo que se revisaron las recomendaciones que se ajustaban a las características de comunicación de Sigfox, al igual se tuvieron en cuenta los mecanismos de protección que presenta Sigfox. Las pruebas que se decidieron realizar fueron:
- Prueba de diseño.
- Actualización de firmware y claves de autenticación.
- Pruebas del dispositivo físico
- Evaluación de alertas del Backend a la reprogramación de la tarjeta de desarrollo.
- Transmisión de paquetes sin antena, evaluación de alerta por equipo desconectado en el Backend.
- Pruebas en la nube (Backend de Sigfox)
- Interceptación de tráfico web validando HTTPS.
- Acceso por fuerza bruta.
- Evaluación de bloqueo de cuenta por múltiples intentos de acceso.
- Antes de iniciar las pruebas fue necesario conocer cómo funciona Sigfox y cuál es la seguridad de la misma.

2.2. ¿Cómo se comunica Sigfox?

Sigfox funciona a partir de dispositivos IoT fabricados con chips específicos admitidos por la red, estos dispositivos envían la información por medio de las estaciones base (BTS) más cercanas que conectan a los servicios de Sigfox, pasando esta información a su punto central, la nube de Sigfox, denominado Sigfox Backend. En esta plataforma, se pueden configurar diferentes servicios de mensajería como AWS IoT, AWS Kinesis, IBM Watson y Microsoft Azure; estas plataformas toman los datos recopilados que llegan a la nube y la muestra de una forma más dinámica para el usuario final [16]. En la Figura 2, se presenta el diagrama de elementos que componen la red de Sigfox.

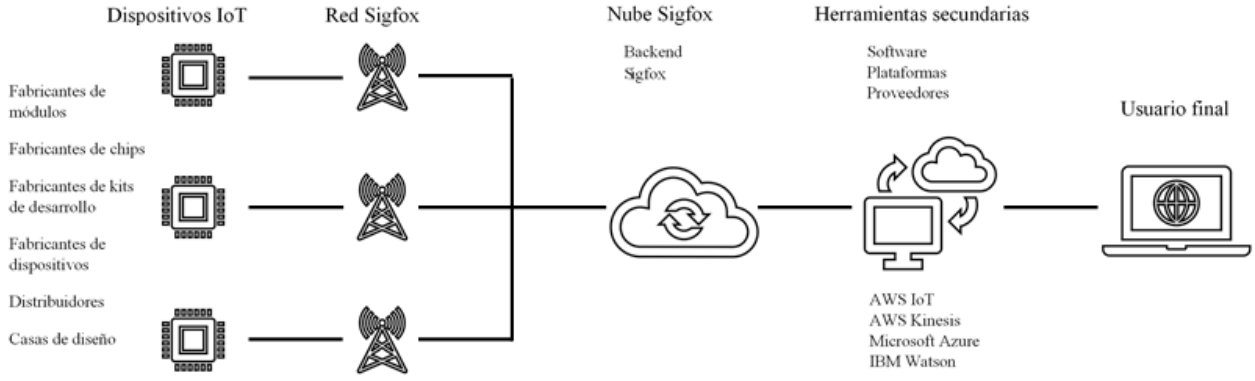

Figura 2. Diagrama de elementos de la red Sigfox **Fuente:** elaboración propia.

Sigfox utiliza Ultra-Narrow, modulación de ancho de banda (UNB) para enviar mensajes pequeños a través de la banda ISM sub-GHz sin licencia (868 MHz en Europa, 915 MHz en los Estados Unidos). Dependiendo del carácter ambiental, las estaciones base pueden recibir estos mensajes a largas distancias de 10 km a 50 km. En Europa, las regulaciones del ciclo de trabajo de la banda ISM de 868 MHz limitan los dispositivos Sigfox a 36 transmisiones por hora y seis segundos de tiempo en el aire por paquete. Como la modulación UNB impone una velocidad de datos limitada de 100 bps,

ISSN 1794-211X • e-ISSN 2322-939X • Vol 16, No 2 (julio-diciembre 2019). pp.252-261.Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

un dispositivo Sigfox puede enviar seis mensajes por hora con una carga útil máxima de 12 bytes por mensaje [17]. A pesar de estas limitaciones, Sigfox es un estándar LPWAN adecuado para muchas aplicaciones de IoT que no son críticas para el tiempo, por ejemplo, monitoreo para medidores de agua, detección de la calidad del aire, entre otras [2].

2.3. Seguridad en Sigfox

Aunque los dispositivos Sigfox Ready TM son objetos IoT, no están conectados directamente a internet y no se comunican utilizando el protocolo de internet. En realidad, los dispositivos Sigfox Ready TM no están conectados a ninguna red ni a ninguna estación base. Cuando se requiere que los datos se transmitan o reciban desde internet, el dispositivo transmite un mensaje de radio, este mensaje es recogido por varias estaciones de acceso y es transmitido a Sigfox Core Network, que a su vez lo entrega a un destino predefinido, generalmente una aplicación IoT [18].
Siendo esta la primera barrera de seguridad presentada por Sigfox, se le suma a esto la seguridad de datos en movimiento por medio de tres procesos:

- Autenticación. Se aprovisiona cada dispositivo Sigfox Ready TM durante la fabricación con una clave simétrica única de autenticación, cada mensaje enviado o recibido por el dispositivo contiene un token criptográfico que se calcula basado en esta clave de autenticación.
- Antirrepetición. Cada mensaje de Sigfox contiene una secuencia contadora que es verificado por Sigfox Core Network para detectar y descartar los intentos de reproducción.
- Antiespionaje. Por defecto, los datos se transmiten a través de la interfaz aérea sin ningún cifrado. Sin embargo, dependiendo de la aplicación, estos datos pueden ser muy sensibles y su privacidad debe estar garantizada, Sigfox ofrece a los clientes la opción de implementar sus propias soluciones de cifrado de extremo a extremo o confiar en una solución de cifrado proporcionada por el protocolo Sigfox [18].

Una solución dedicada protege los centros de datos de Sigfox contra una amplia gama de ciberataques como la denegación de servicio (DoS), denegación de servicio distribuido (DDoS), reflexiva denegación de servicio (RDoS) y denegación reflexiva distribuida deservicio (DRDoS). Esta solución, suministrada y mantenida por el proveedor de servicios de internet de Sigfox, ofrece una protección basada en la nube, servicio con varios centros de lavado para detectar y mitigar los ciberataques contra redes y sitios web. Esta solución utiliza algoritmos de detección y mitigación de coincidencia de patrones de tráfico específicos de Sigfox para evitar falsos positivos [18].

3. Resultados

A continuación, se muestran los resultados obtenidos a partir de la investigación y desarrollo de pruebas en el entorno usado de Sigfox.

3.1. Vulnerabilidades encontradas en Sigfox
3.1.1. Diseño de dispositivos

Al evaluar el manejo de Sigfox sobre las actualizaciones para los dispositivos posterior a la venta, se vio que la mayoría de los dispositivos Sigfox, incluyendo el Xkit Thinxtra, no son actualizables de forma remota ni de forma física, esto debido a que Sigfox no genera actualizaciones periódicas para sus dispositivos. Sigfox genera solo actualizaciones enfocadas al Backend, usualmente destinadas a corrección de errores o el diseño del aplicativo web, haciendo que el firmware y las claves almacenadas a largo plazo de autenticación en los dispositivos, sean el mismo durante toda su vida útil.
La vida útil de los equipos de Sigfox es de aproximadamente de diez años, lo cual excede considerablemente las recomendaciones de los "cripto periodos" del NIST publicados en el documento "Recommendation for Key Management" [19], que indica un cambio de claves criptográficas inferior a cada cinco años; por lo tanto, las claves almacenadas en el dispositivo y la red son vulnerables en el tiempo. Al seguir incrementando el mercado de estos dispositivos, siendo altamente deseables las claves, incrementará el interés de aprovechar estas vulnerabilidades en el futuro, logrando, por ejemplo, suplantaciones de

ISSN 1794-211X • e-ISSN 2322-939X • Vol 16, No 2 (julio-diciembre 2019). pp.252-261.Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

dispositivos o alojamientos de virus distribuibles en la red en el futuro a partir de enlaces falsos de BTS.

3.1.2. Dispositivos físicos

Los dispositivos de Sigfox generalmente funcionan en plataformas de tipo Arduino, tarjetas programables a partir del compilador de Arduino; de igual forma, algunos kits usan directamente el Arduino Uno, como lo es el Xkit Thinxtra; hay modelos de Lora como el ST Murata Lora WAN que es compatible con la red Sigfox, al igual que hay módulos programables con Raspberry Pi. Todos estos dispositivos tienen el mismo concepto en común: tarjetas reprogramables, sin carcasa ni bloqueo de puertos, haciendo que sean fácilmente reprogramables de forma física. Al realizar la verificación de alertas del Backend de Sigfox, se vio que muestra las últimas conexiones del equipo; sin embargo, no muestra una alerta de una desconexión prolongada.

El tener comunicación con una distancia de tiempo mínima de diez minutos, debido a que se limitan a seis mensajes por hora la comunicación de Sigfox por la modulación UNB, hace posible que se puedan desconectar el equipo, reprogramarlo —lo que no toma más de veinte segundos— y ponerlo en funcionamiento sin una alteración en la funcionalidad para el Backend.

También son susceptibles a la pérdida de comunicación de forma sencilla, ya que al trabajar con frecuencias bajas es necesario el uso de una antena considerablemente grande (aproximadamente 10 cm), la cual es fácilmente desmontable, dejando a este dispositivo sin comunicación con Sigfox, lo cual fue comprobado quitando la antena durante el envió de paquetes, los cuales dejaron de ser recibidos por el Backend al no tener una antena el dispositivo.

3.1.3. Backend de Sigfox

El Backend de Sigfox es el portal web que permite registrar y administrar los dispositivos adquiridos para la red Sigfox, desde este portal se puede cambiar el tipo de mensajes del sensor, la plataforma que tomará los datos para procesarlos de forma más dinámica, entre otras funcionalidades. Esta aplicación web está protegida por HTTPS (Hypertext Transfer Protocol Secure), lo que la hace segura a ataques de fuerza bruta o análisis de datos.

Las pruebas se iniciaron comprobando el funcionamiento del HTTPS al interceptar el tráfico web por medio de Brupsuit (herramienta de Kali Linux, que permite un marco de prueba de penetración web basado en Java [20]), ello con el fin de verificar si se podían variar las credenciales de acceso al momento de ser enviados por la página web. El resultado que entregó esta prueba fue que la página no permitía el acceso al variar los datos desde la interceptación de tráfico, mostrando que el HTTPS funcionaba. Posteriormente, al ver que no funcionaba el acceso por Brupsuit por interceptación de tráfico, se realizaron pruebas de fuerza bruta con Hydra [21] y Medusa [22] (crackers de inicio de sesión paralelos que admiten numerosos protocolos para atacar que vienen incorporados en Kali Linux) sin lograr el acceso, ya que generaban falsos positivos de acceso o un acceso denegado de la página a las herramientas.

Sin embargo, al verificar el bloqueo de la página web a múltiples intentos de ingreso, se evidenció que no existe dicho bloqueo, y al no tener verificación tipo captcha o similar, se hace vulnerable a un acceso de fuerza bruta por medio de un bot que llene el formulario de ingreso, un código fácilmente realizable en Python, por medio de la herramienta Selenium usando el explorador Mozilla. En la Figura 3, se observa el diagrama de bloques del código usado.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 16, No 2 (julio-diciembre 2019). pp.252-261.Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

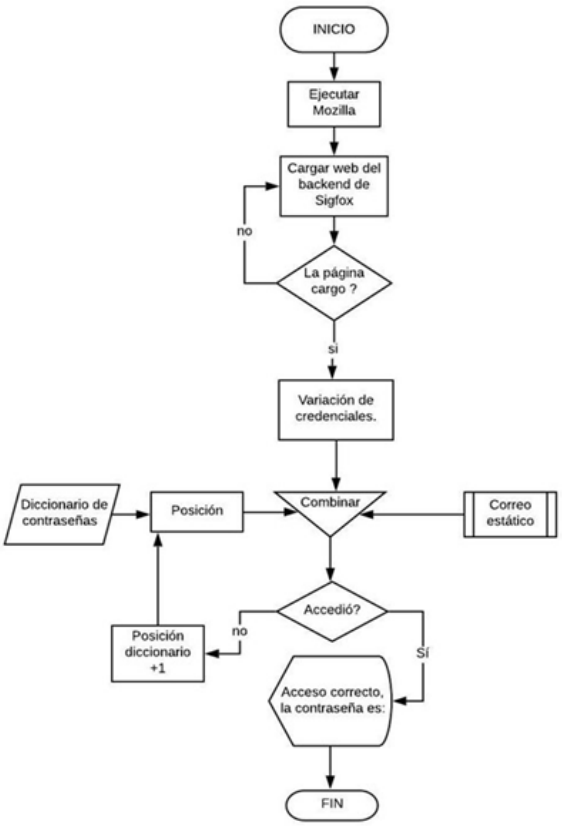

Figura 3. Diagrama de bloques código implementado. Fuente: elaboración propia

Inicialmente, el resultado de este *bot* fue un bloqueo al navegador por intentos repetitivos en poco tiempo, ya que se realizaba un intento cada un segundo, para lo cual se acomodó un tiempo entre intentos de tres segundos y una pausa cada ocho intentos consecutivos, saltando así el bloqueo de la página al navegador de forma sencilla. Se lograron hacer 100 intentos de ingreso de forma automática en aproximadamente once minutos, estimando hacer mil intentos en aproximadamente una hora y cincuenta minutos.

Esto abre la puerta a un ataque dirigido, que al recopilar suficiente información puede acceder al Backend y tomar un control parcial de la actividad de los dispositivos, pues se pueden deshabilitar las alertas sin ningún aviso por parte del aplicativo web; podrían eliminar los dispositivos creados en la cuenta, al tener los datos de acceso pueden deshabilitar la cuenta o cambiar el correo logrando hacer inservibles los dispositivos. Esta vulnerabilidad puede llegar a una denegación de servicio parcial o total de la red específica del cliente de la red Sigfox.

En la Tabla 1, se presenta el resumen de los resultados obtenidos.

Prueba	Resultado
Actualización de ***firmware*** y claves de autenticación.	Sigfox no presenta actualizaciones a nivel de *firmware*; por lo tanto, las claves de autenticación son las mismas durante la vida útil del dispositivo.
Evaluación de alertas del Backend a la reprogramación de la tarjeta de desarrollo o por equipo desconectado en el Backend.	No se tiene alerta alguna en el control de dispositivos del Backend sobre desconexión y reprogramación del dispositivo final.
Interceptación de tráfico web y acceso por fuerza bruta validando HTTPS.	El HTTPS funciona, bloqueando los intentos de acceso por fuerza bruta ya sea por métodos de interceptación de tráfico o al realizar intentos con herramientas como Hydra y Medusa.
Evaluación de bloqueo de cuenta por múltiples intentos de acceso.	No existe un bloqueo de la página para múltiples intentos fallidos de acceso, se vio vulnerable a métodos de acceso por fuerza bruta a partir de diligenciar el formulario de ingreso (usuario y contraseña) de forma automática.

Tabla 1. Resumen de resultados obtenidos. **Fuente**: elaboración propia.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 16, No 2 (julio-diciembre 2019). pp.252-261.Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

4. Conclusiones

Sigfox cuenta con estándares de seguridad a destacar respecto a las otras tecnologías, cuenta con sistema de autentificación, cambio de frecuencia de enlace, protección de repetición, un bajo rendimiento diario de enlace descendente, entre otras múltiples características que logran un ambiente seguro para la red de Sigfox al día de hoy. Sin embargo, en el desarrollo de este documento se analizó el funcionamiento de algunos sistemas de seguridad de la red Sigfox en busca de brechas de seguridad por medio de un entorno de pruebas. Dichas pruebas dieron como resultado que Sigfox cuenta con algunas vulnerabilidades de diseño en los dispositivos físicos y en la nube de Sigfox; aunque estas vulnerabilidades no representan un peligro para la red global, sí afectan al usuario como individuo, por lo que son importantes de corregir para el desarrollo futuro de esta red, ya que se proyecta como la red LPWAN para IoT más usada en el futuro.

Cada tecnología tiene limitaciones a partir de su diseño, ya sea por su cobertura, el costo de los dispositivos que se pueden conectar o las vulnerabilidades de seguridad que puedan tener, este último punto se encuentra presente en todas las tecnologías LPWAN. Al hacer una comparativa de Sigfox con las tecnologías paralelas de LPWAN, se evidencia que es de las redes más robustas respeto a seguridad, una de las más confiables en el mercado, ya que sus sistemas generan complicaciones a los individuos que deseen atacarla y aprovechar sus dispositivos. Si se ven estas soluciones en comparación con el uso de WiFi en IoT, a excepción de NB-IoT, todas las demás tecnologías son independientes del uso de conexión por IP, logrando por esta característica una restricción al acceso por medio de una computadora, por lo que se deben usar diferentes dispositivos que permitan el enlace a estas frecuencia; sin embargo, al no usar IP (específicamente Sigfox, ya que LoRa puede tener esta opción) no se puede tomar control del dispositivo para el uso en una red externa como se hace en los ataques de DoS con equipos WiFi de IoT.

4.1. Discusión

A partir de la investigación realizada y las propias experiencias adquiridas al realizar algunas pruebas de la funcionalidad y seguridad de la red Sigfox por medio del entorno de pruebas, se observa que el querer atacarla y encontrar sus vulnerabilidades resulta frustrante y poco accesible para el que quiera atacarlo, pues a diferencia de las otras redes, Sigfox no lo pone nada fácil. Si bien se critica que de fábrica no viene con encriptación y se toma como un servicio aparte, el sistema de enlace con las BTS, la autenticación y la variación de frecuencias de enlace genera una barrera de seguridad para evitar que se produzca una interceptación de hombre en medio, sin contar que en la capa de radio cada mensaje Sigfox se identifica en la red con una identificación única y se autentica gracias a una firma realizada con una clave segura única almacenada en el dispositivo. Además, esta firma permite detectar el ataque de hombre en medio [23].

Si se compara Sigfox con otras tecnologías es la que menos protagonismo tiene en los documentos que tratan la seguridad en este tipo de redes, pues generalmente se menciona como una red segura con pocas brechas de seguridad y confiable. Si se observa el caso de LoRaWAN, es una de las redes con el mayor índice de vulnerabilidades encontradas, explotadas y documentadas, como se ve en el estudio de [7], donde se recopilan pruebas de penetración, vulnerando desde los paquetes hasta el desempeño de la batería. De igual forma, se tiene la investigación sobre los mecanismos de seguridad de las redes LPWAN [1] en el cual se nombra a Sigfox como una de las tecnologías más seguras y de diseño único, documento que toma como ejemplo de red vulnerable a LoRaWAN. En [24], discute la posible susceptibilidad de LoRa a diferentes ataques utilizando hardware comercial, viendo los aspectos de dispositivos comprometidos, claves de red, técnicas de jamming y agujeros de gusanos.

En conclusión, se encuentran múltiples investigaciones mostrando resultados referentes a la seguridad en LoRa, y es de hacer énfasis pues es una de las tecnologías predilectas en el mercado, ya que fue una de las primeras que se acopló a las necesidades de la industria. De las demás tecnologías se ve poco, pues NB-IoT presenta poca información de seguridad, y se documenta su funcionamiento en algunas comparaciones respecto

ISSN 1794-211X • e-ISSN 2322-939X • Vol 16, No 2 (julio-diciembre 2019). pp.252-261.Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

a las otras redes como en el documento de Franklin Heath Ltd [9] o el ejemplo de vulnerabilidad encontrado en el análisis de [7].

Con esto, se da una idea de la confianza que genera Sigfox en el mercado. Si bien tiene vulnerabilidades potenciales a futuro, estas son mejorables en el tiempo como, por ejemplo, una mejora en el diseño que permita la actualización de los dispositivos, realizar el desarrollo de equipos menos expuestos agregando una funcionalidad que permitan la detección de reconfiguración de estos; en cuanto al Backend, probablemente la mejora más importante de todas sería implementar un bloqueo al número máximo de intentos para el ingreso. De igual forma, al día de hoy es poco el daño masivo que pueden generar estas vulnerabilidades, debido a que cuenta con la infraestructura de comunicación más robusta entre las otras tecnologías.

Referencias

[1] S. Chacko, M. Job, "Login Bases de datos" https://iopscience-iop-org.bdigital.udistrital.edu.co/article/10.1088/1757-899X/396/1/012027/pdf

[2] T. Janssen, M. Aernouts, R. Berkvens y M. Weyn, "Outdoor Fingerprinting Localization Using Sigfox". https://www.researchgate.net/publication/328982852_Outdoor_Fingerprinting_Localization_Using_Sigfox

[3] Sigfox, "Sigfox - El proveedor de servicios de comunicaciones globales para Internet de las cosas (IoT)". https://www.sigfox.com/

[4] LoRa Alliance, "LoRaWAN: redes de área amplia para IoT". https://www.lora-alliance.org

[5] GSMA, "Tecnología Nb-iot", https://www.gsma.com/iot/ estrecho-banda-internet-de-cosas-nb-iot

[6] M. Morelos, "Dispositivos de internet de las cosas generan desconfianza entre los usuarios", https://elceo.com/tecnologia/dispositivos-de-internet-de-las-cosas-generan-desconfianza-entre-los-usuarios/

[7] X. Yang, E. Karampatzakis, C. Doerr, F. Kuipers, "Security vulnerabilities in lorawan", En Proceedings - Acm/IEEE International Conference on Internet of Things Design and Implementation, 2018.

[8] Laurentiu, K. Mateusz y M. Nordal, "Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT". https://www.researchgate.net/publication/334629575_Security_Issues_in_Internet_of_Things_Vulnerability_Analysis_of_LoRaWAN_Sigfox_and_NB-IoT

[9] Franklin Heath Ltd, "LPWA Technology Security Comparison". https://fhcouk.files.wordpress.com/2017/05/lpwa-technology-security-comparison.pdf

[10] Owasp.org, "OWASP Foundation". https://www.owasp.org/index.php/Main_Page

[11] Owasp.org, "Pruebas de Seguridad en aplicaciones web según OWASP". https://www.owasp.org/images/2/2f/OWASP_SUSCERTE.pdf

[12] WND Group, "WND Colombia". https://www.wndgroup.io/colombia

[13] Thinxtra.com, "Xkit – Thinxtra". https://www.thinxtra.com/solutions/thinxtraproducts/xkit

[14] Silex System and Telecom, "Estación Base de telefonía Móvil. Una estación base o BTS". https://silexst.com/estacion-base-de-telefonia-movil

[15] Owasp.org, "IoT Testing Guides – OWASP". https://www.owasp.org/index.php/IoT_Testing_Guides

[16] Blockchain Administration, "Como funciona la red LPWAN Sigfox". https://blockchainadministration.blogspot.com/2018/12/como-funciona-la-red-lpwan-sigfox.html

[17] B. Vejlgaard et al., "Coverage Comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km² Area", En IEEE 85th Vehicular Technology

[18] Conference (VTC Spring), Sydney, Australia, 2017, https://doi.org/10.1109/vtcspring.2017.8108182Sigfox, "Make things come alive in a secure way", https://www.sigfox.com/en/technology/security

[19] E. Barker, "NIST Special Publication 800-57 Part 1 Revision 4. Recommendation for key management", https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

ISSN 1794-211X • e-ISSN 2322-939X • Vol 16, No 2 (julio-diciembre 2019). pp.252-261.Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

[20] R. Davis, "What is burp suite. Pentest tool description". https://www.pentestgeek.com/what-is-burpsuite
[21] Tools.kali.org, "Hydra Package Description". https://tools.kali.org/password-attacks/hydra
[22] Systemadmin.es, "Medusa - Herramienta genérica para hacer ataques de fuerza bruta". http://systemadmin.es/2010/09/medusa-herramienta-generica-para-hacer-ataques-de-fuerza-bruta
[23] Sigfox, "Data Security - ask Sigfox". https://ask.sigfox.com/questions/155/data-security.html
[24] E. Aras, G. S. Ramachandran, P. Lawrence y D. Hughes, "Exploring the Security Vulnerabilities of LoRa", En 3rd IEEE International Conference on Cybernetics (CYBCONF), 2017, pp. 1-6. https://doi.org/10.1109/cybconf.2017.7985777

ISSN 1794-211X • e-ISSN 2322-939X • Vol 16, No 2 (julio-diciembre 2019). pp.252-261.Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.