Análisis de seguridad en capa física para el Internet de las Cosas

Dr. Marco Aurelio Cárdenas Juárez
Facultad de Ciencias
Universidad Autónoma de San Luis Potosí
Email: marco.cardenas@uaslp.mx

Dr. Enrique Stevens Navarro
Facultad de Ciencias
Universidad Autónoma de San Luis Potosí
Email: enrique.stevens@uaslp.mx

1. Introducción

El Internet de las cosas (IoT, por sus siglas en inglés) es un concepto que describe la interconexión de diversos dispositivos y objetos a través de Internet, permitiéndoles comunicarse y compartir información de manera inteligente y autónoma. El IoT se basa en la idea de que cualquier objeto, desde electrodomésticos y vehículos, hasta sensores ambientales y equipos médicos, puede convertirse en un dispositivo inteligente capaz de recopilar, transmitir y analizar datos, así como de tomar decisiones con base en ellos. Esta interconexión se logra a través de sensores, actuadores, conectividad de red y plataformas de software especializadas. Los sensores permiten capturar datos del entorno, como temperatura, humedad, movimiento o presión, mientras que los actuadores permiten realizar acciones o modificar el entorno físico en respuesta a la información recibida. La clave del IoT radica en la capacidad de estos dispositivos para compartir y procesar datos de forma automática y en tiempo real. Esto permite crear sistemas más eficientes y optimizados, así como desarrollar aplicaciones y servicios innovadores en diversos campos, como el hogar inteligente, la salud, la industria, el transporte y la agricultura, entre otros. El potencial del IoT es enormemente amplio. Con el aumento de la conectividad y el avance en la miniaturización de los dispositivos, la cantidad de objetos conectados a Internet se espera que crezca exponencialmente en los próximos años. Esto generará un enorme volumen de datos que, analizados juiciosamente, podrán proporcionar información muy valiosa para la toma de decisiones, el monitoreo y el control de procesos, la mejora de la eficiencia de los sistemas y la calidad de vida de las personas.

Sin embargo, el IoT también plantea desafíos en cuanto a la seguridad y privacidad de los datos, así como en la interoperabilidad entre dispositivos y plataformas. La seguridad en la capa física es un aspecto fundamental en el contexto del IoT. A medida que la interconexión de dispositivos y objetos continúa expandiéndose, es crucial garantizar que los datos y la comunicación entre ellos estén protegidos desde el nivel más básico, esto es, en el entorno físico en el que operan. La capa física se refiere a los componentes y elementos físicos que conforman los dispositivos IoT, como sensores, actuadores, redes de comunicación y los propios objetos conectados. En este nivel, las vulnerabilidades y amenazas pueden surgir tanto de ataques directos a los dispositivos como de manipulaciones del entorno físico en el que se encuentran. La seguridad en la capa física implica implementar medidas para prevenir y detectar cualquier intento de manipulación o acceso no autorizado a los dispositivos IoT. Esto incluye proteger los sensores y actuadores contra ataques físicos, como el sabotaje, el robo de información o la interferencia con su funcionamiento. Asimismo, se deben tener en cuenta aspectos como la seguridad de las redes de comunicación utilizadas para conectar los dispositivos, la autenticación de los nodos y la protección de los datos transmitidos. Un

enfoque común para garantizar la seguridad en la capa física del IoT es la implementación de técnicas de criptografía, que permiten cifrar los datos transmitidos y autenticar los dispositivos para asegurar la integridad y confidencialidad de la información. También se utilizan métodos de detección y prevención de intrusiones, como sensores de manipulación, sistemas de monitoreo y alarmas que alertan sobre intentos de acceso no autorizado. La seguridad en la capa física es especialmente relevante en aplicaciones críticas, como la salud, la infraestructura urbana o la industria, donde un acceso no autorizado o una manipulación de los dispositivos IoT puede tener consecuencias graves. Esta investigación se enfoca en la seguridad en la capa física del IoT, explotando la herramienta de *hacking* Flipper Zero para abordar estos desafíos, analizando las vulnerabilidades en la capa física del IoT. Con millones de dispositivos conectados a Internet, desde electrodomésticos hasta sistemas industriales críticos, es fundamental comprender los riesgos de seguridad que pueden comprometer la integridad de los sistemas IoT.

Flipper Zero es una herramienta versátil disponible comercialmente, que puede ser utilizada para evaluar y mejorar la seguridad en el IoT (ver Figura 1). Para lo anterior, es necesario explorar las capacidades y características de Flipper Zero, que incluyen la capacidad de realizar pruebas de penetración, el análisis de señales inalámbricas, la emulación de dispositivos y la decodificación de protocolos, por lo que se utilizará como herramienta de investigación en el contexto de seguridad para identificar y solucionar vulnerabilidades en la capa física del IoT. Es importante señalar, su capacidad para evaluar la resistencia de los dispositivos IoT antes de su implementación, detectar y mitigar ataques físicos en tiempo real, y educar a los profesionales sobre las técnicas de *hacking* utilizadas por los adversarios. Al comprender las vulnerabilidades en la capa física y utilizar herramientas como Flipper Zero, podremos fortalecer la seguridad en el IoT y fomentar un entorno digital confiable y seguro.

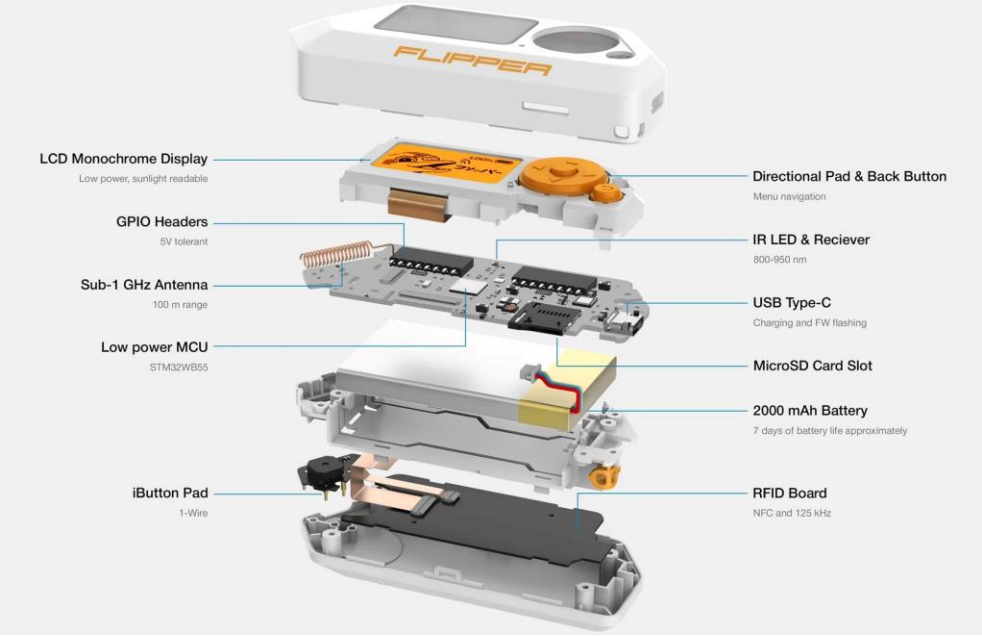

Figura 1. Componentes de Flipper Zero
Fuente: https://flipperzero.one/

2. Objetivos

La tesis de maestría proporcionará una contribución al campo de la seguridad en el IoT, permitiendo un mejor entendimiento y protección de los sistemas IoT en su capa física. A continuación, se presentan el objetivo general y los objetivos específicos de este tema de tesis para la Maestría en Ingeniería Electrónica opción Telecomunicaciones.

2.1 Objetivo general

Investigar y analizar los riesgos de seguridad en la capa física de los sistemas IoT, identificando vulnerabilidades y posibles ataques que puedan comprometer la integridad y confidencialidad de los dispositivos y datos, utilizando Flipper Zero como herramienta de análisis y evaluación.

2.2 Objetivos específicos

- Investigar el estado del arte en seguridad en la capa física para el IoT, revisando las principales amenazas y vulnerabilidades existentes, así como los enfoques y técnicas utilizados para mitigar los riesgos.
- Familiarizarse con el funcionamiento y las capacidades del dispositivo Flipper Zero, comprendiendo sus características y herramientas específicas relacionadas con la seguridad en la capa física.
- Realizar un análisis detallado de los dispositivos IoT seleccionados, examinando su arquitectura, componentes y protocolos de comunicación utilizados, con el objetivo de identificar posibles puntos débiles en la capa física.
- Diseñar y llevar a cabo experimentos utilizando el Flipper Zero para evaluar la seguridad en la capa física de los dispositivos IoT analizados. Esto puede incluir pruebas de penetración, evaluación de vulnerabilidades y manipulación de dispositivos para identificar posibles riesgos.
- Recopilar y analizar los datos obtenidos durante los experimentos, documentando las vulnerabilidades identificadas, los posibles ataques realizados y las medidas de seguridad efectivas aplicadas.
- Proponer recomendaciones y pautas para fortalecer la seguridad en la capa física de los sistemas IoT analizados, considerando las vulnerabilidades identificadas y las mejores prácticas de seguridad existentes.
- Validar las recomendaciones propuestas mediante la implementación y prueba de soluciones de seguridad en la capa física, utilizando el Flipper Zero para evaluar la efectividad de estas medidas.
- Evaluar y comparar los resultados obtenidos en términos de la mejora de la seguridad en la capa física de los dispositivos IoT analizados, destacando las fortalezas y limitaciones de las soluciones implementadas.

3. Perfil del estudiante

Interés por ampliar su conocimiento de comunicaciones inalámbricas y aspectos de seguridad para el Internet de las Cosas. Experiencia de programación en Matlab o Python, en el manejo de tarjetas de prototipado rápido para diseñar dispositivos del Internert de las Cosas y en la operación de analizadores de espectro. Gusto por la instrumentación electrónica. Disposición para trabajar en equipo en ambientes multidisciplinarios en el contexto internacional.

Disponibilidad para viajar. Estudios de licenciatura en ingeniería en telecomunicaciones, telemática, electrónica, eléctrica, biomédica, tecnologías de la información, computación, sistemas inteligentes o grados afines.

4. Cursos optativos sugeridos

Para el desarrollo de esta investigación, el o la estudiante deberá poseer un conocimiento sólido en redes y comunicaciones inalámbricas, por lo que se sugieren los siguientes cursos optativos:

- Redes de comunicación
- Comunicaciones inalámbricas
- Telemetría
- Sistemas electrónicos embebidos

5. Vinculación y productos esperados

Esta investigación está vinculada a otras instancias nacionales e internacionales a través de un proyecto relacionado con plataformas del internet de las cosas, por lo que durante su realización es posible llevar a cabo estancias cortas de investigación. Además, se espera obtener un artículo publicado en conferencia internacional o revista indexada.

6. Bibliografía complementaria

[1] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Computer Networks*, vol. 76, pp. 146 – 164, 2015.

[2] E. Santos-Luna, et al., “A Software Development Based on Software-Defined Radio Devices for Transmitting Digital Signals,” *ICMEAE*, 2019. doi: 10.1109/ICMEAE.2019.00032

[3] F. Al-Turjman, M. Alarabeyyat and S. H. Bouk, "IoT-Based Intelligent Transportation Systems: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2617-2644, Thirdquarter 2019. doi: 10.1109/COMST.2019.2904153.

[4] M. U. Gorgani, M. Fotouhi and S. Talebi, "A Survey on IoT Cloud Platforms," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1835-1845, April 2019. doi: 10.1109/JIOT.2018.2886992.

[5] M. M. Hassan, F. Al-Turjman and M. A. Al-Rodhaan, "A Comprehensive Survey of Security and Privacy in Internet of Things (IoT) Systems: Existing Solutions and Recent Advances," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 473-483, Firstquarter 2020. doi: 10.1109/COMST.2019.2934719.

[6] S. L. Hu, F. Wu and L. Jin, "A Survey on Industrial Internet of Things: A Technical Perspective," *IEEE Access*, vol. 6, pp. 78238-78258, 2018. doi: 10.1109/ACCESS.2018.2887730.

[7] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, Sept. 2013. doi: 10.1016/j.future.2013.01.010.

[8] J. Wan, S. Tang, D. Li, S. Wang and C. Imran, "A Survey on Application of Deep Learning in Internet of Things," *IEEE Access*, vol. 6, pp. 32979-32993, 2018. doi: 10.1109/ACCESS.2018.2842681.

[9] D. Kaur and P. K. Sharma, "*Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,*" Journal of King Saud University - Computer and Information Sciences, vol. 30, no. 4, pp. 431-448, Oct. 2018. doi: 10.1016/j.jksuci.2017.12.001.

[11] M. Gia, M. M. Uddin and S. G. Jeon, "A Survey of Authentication Schemes in Machine-to-Machine Communications for the Internet of Things," I*EEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2096-2123, Thirdquarter 2018. doi: 10.1109/COMST.2018.2820161.

[12] F. N. Siby and S. Dey, "Privacy in Internet of Things (IoT): A Survey," *Computers & Electrical Engineering*, vol. 66, pp. 1-21, July 2018. doi: 10.1016/j.compeleceng.2018.01.005.

[13] S. Khan, S. A. Madani, W. A. Khan, A. Ghani, S. U. Khan and W. A. Jan, "Security and privacy in Internet of Things (IoTs): Models, algorithms, and implementations," IEEE Communications Magazine, vol. 55, no. 1, pp. 119-125, Jan. 2017. doi: 10.1109/MCOM.2017.1600598.