CEA Comité Español de Automática

XLVI JORNADAS AUTOMÁTICA CARTAGENA 2025

UNIVERSIDADE DA CORUÑA

Jornadas de Automática

Auditoría funcional de juguetes IoT con Bluetooth LE

Aveleira-Mata, Jose[a], Narciandi-Rodríguez, Diego[a,*], García-Rodríguez, Isaías[a], Alfonso-Cendón, Javier[b], Rubio-Martín, Sergio[c], Alaiz-Moretón, Héctor[a]

[a]*Grupo SECOMUCI, Departamento de Ingeniería Eléctrica y de Sistemas y Automática, Universidad de León, Campus de Vegazana s/n, 24071, León, España*
[b]*Departamento de Ingeniería Mecánica, Informática y Aeroespacial, Universidad de León, Campus de Vegazana s/n, 24071, León, España*
[c]*Grupo ALBA, Departamento de Ingeniería Eléctrica y de Sistemas y Automática, Universidad de León, Campus de Vegazana s/n, 24071, León, España*

To cite this article: Aveleira-Mata, Jose, Narciandi-Rodríguez, Diego, , García-Rodríguez, Isaías, Alfonso-Cendon, Javier, Rubio-Martín, Sergio, Alaiz-Moretón, Héctor. 2025. Functional Audit of IoT Toys with Bluetooth LE. Jornadas de Automática, 46. https://doi.org/10.17979/ja-cea.2025.46.12272

Resumen

Este trabajo presenta una auditoría funcional de dispositivos comerciales con conectividad Bluetooth Low Energy (BLE), centrada en juguetes conectados en el contexto del Internet de las Cosas (IoT). Se empleó una metodología basada en el uso de dos dongles nRF52840: uno configurado como escáner para identificar direcciones MAC aleatorias, y otro como sniffer BLE integrado en Wireshark para capturar el tráfico entre el dispositivo y su aplicación. Las capturas muestran que varios de los dispositivos analizados transmiten datos sin cifrado ni autenticación, lo que permite ataques como interceptación, inyección de comandos o repetición de mensajes. Como línea de trabajo futuro, se propone el uso de las capturas obtenidas para entrenar modelos de detección de anomalías mediante aprendizaje automático.

Palabras clave: Seguridad en sistemas embebidos; Análisis de tráfico BLE; Juguetes conectados; Detección de intrusiones; IoT doméstico; Auditoría de dispositivos; Comunicaciones inalámbricas seguras

Functional Audit of IoT Toys with Bluetooth LE

Abstract

This work presents a functional audit of commercial devices with Bluetooth Low Energy (BLE) connectivity, focused on connected toys in the context of the Internet of Things (IoT). The methodology is based on the use of two nRF52840 dongles: one configured as a scanner to identify random MAC addresses, and the other as a BLE sniffer integrated with Wireshark to capture traffic between the device and its mobile application. The captures show that several of the analyzed devices transmit data without encryption or authentication, enabling attacks such as interception, command injection, or replay. As future work, we propose using the captured data to train anomaly detection models using machine learning techniques.

Keywords: Embedded system security; BLE traffic analysis; Connected toys; Intrusion detection; Home IoT; Device auditing; Secure wireless communications

1. Introducción

En la última década, la expansión del Internet de las Cosas (IoT) ha impulsado la adopción de tecnologías de comunicación inalámbrica que sean eficientes, versátiles y de bajo consumo energético. Entre ellas, Bluetooth Low Energy (BLE), introducido en 2010 como parte de la especificación Bluetooth 4.0 Want et al. (2013), ha emergido como una solución clave para dispositivos que requieren conectividad continua con un consumo energético mínimo Koulouras et al. (2025). BLE opera en la banda ISM de 2.4 GHz y utiliza técnicas como el salto de frecuencia adaptativo y la modulación GFSK int (2023), permitiendo tasas de transmisión de hasta 2 Mbps en sus versiones más recientes.

*Autor para correspondencia: dnarr@unileon.es

BLE ha evolucionado con mejoras en velocidad, alcance y eficiencia energética. Por ejemplo, la especificación Bluetooth 5.0 introdujo el modo LE 2M PHY, que duplica la tasa de datos, y el modo LE Coded PHY, que extiende el alcance mediante técnicas de codificación avanzadas vinnter (2023). Estas mejoras han consolidado a BLE como una tecnología esencial en aplicaciones que van desde dispositivos médicos y sistemas de automatización del hogar hasta juguetes inteligentes y wearables Koulouras et al. (2025).

Sin embargo, la creciente integración de BLE en dispositivos cotidianos (IoT) ha traído consigo nuevos desafíos en materia de seguridad. El protocolo permite establecer conexiones sin cifrado ni autenticación, especialmente en dispositivos de bajo coste o muy limitados en batería y capacidad de procesamiento, donde se prioriza el rendimiento y la simplicidad sobre la seguridad Zhang et al. (2020) . Como el caso de los juguetes conectados, que suelen estar diseñados para ser compactos, económicos y energéticamente eficientes, dejando en segundo plano la implementación de medidas de protección adecuadas Classen and Hollick (2021).

Ante este panorama, el análisis de tráfico BLE, conocido como ”sniffing”, sirve para evaluar la seguridad de los dispositivos que utilizan esta tecnología. El ”sniffing”permite capturar y analizar los paquetes de datos transmitidos entre dispositivos BLE, revelando información valiosa sobre su comportamiento, configuración y posibles vulnerabilidades Zachariah et al. (2018).

Este estudio se enmarca dentro de una campaña de concienciación navideña promovida por el Instituto Nacional de Ciberseguridad (INCIBE) INCIBE (2024), cuyo objetivo fue auditar diferentes juguetes conectados al mercado español. Durante la campaña, se analizaron un total de 26 juguetes conectados, centrándose en la detección de vulnerabilidades asociadas a su conectividad, especialmente en aquellos con comunicación inalámbrica. De estos, 8 dispositivos presentaban conexión tanto por internet como mediante Bluetooth Low Energy (BLE). En todos los casos en los que la información transmitida por BLE no estaba cifrada, se ha considerado esta vulnerabilidad como grave.

En este trabajo, nos centramos en los juguetes que utilizan conexiones BLE sin cifrar, mostrando cómo es posible capturar y analizar su tráfico utilizando hardware económico. Exploramos en detalle el proceso de sniffing de tráfico BLE empleando herramientas de bajo coste, como el dongle nRF52840 y el software Wireshark, que permiten visualizar y analizar las comunicaciones entre dispositivos en tiempo real. Como resultado de este análisis, se logró interceptar el tráfico BLE de varios juguetes comerciales y comprobar que una proporción significativa no cifraba las comunicaciones, quedando por tanto expuestos a ataques de tipo Man-in-the-Middle (MITM). Esta aproximación permite visibilizar los riesgos reales presentes en entornos domésticos.

2. Trabajo relacionado

Diversos estudios han demostrado que muchos dispositivos que emplean Bluetooth Low Energy (BLE), incluidos los juguetes inteligentes, presentan deficiencias en la protección de datos tanto en la capa de enlace como en la de aplicación. Incluso en aquellos casos donde se habilita el cifrado, es frecuente el uso del modelo de emparejamiento *Just Works*, que no ofrece protección frente a ataques de intermediario (MITM) Sivakumaran and Blasco (2021) Wen et al. (2020). Cabe destacar que IoT-BLE es vulnerable a ataques de suplantación de identidad en los que un atacante puede hacerse pasar por un dispositivo y proporcionar a sus usuarios información dañina. Por otro lado, la implementacion de este protocolo es simple, por lo que tiene, vulnerabilidades de seguridad y privacidad Nagrare et al. (2023).

En el caso de los juguetes conectados a Internet, estas limitaciones son aún más críticas. En Chu et al. (2018) se demuestra que es posible interceptar comunicaciones entre el juguete y su servidor e incluso inyectar audio malicioso, exponiendo a los menores a riesgos reales. De forma similar en Allana and Chawla (2020) alertan sobre la falta de mecanismos de autenticación adecuados y sobre la presencia de interfaces de usuario poco claras que facilitan accesos no autorizados.

Otros trabajos han profundizado en las debilidades específicas tanto del protocolo BLE como de los juguetes inteligentes. En Classen and Hollick (2021) demostraron que muchas de las pilas Bluetooth más utilizadas incumplen la especificación del estándar al no notificar al usuario sobre fallos de autenticación, lo que facilita ataques de tipo Man-in-the-Middle (MITM) sin que el usuario tenga constancia de ello. En una revisión amplia Lonzetta et al. (2018) identificaron numerosas amenazas asociadas a BLE en entornos IoT, como BlueBorne o BlueBugging, y destacaron la necesidad de medidas básicas de mitigación, entre ellas el cifrado en la capa de enlace, el uso de emparejamiento seguro y la actualización frecuente del firmware. Por su parte, de Paula Albuquerque et al. (2019) analizaron en profundidad los riesgos técnicos y de dominio presentes en los juguetes conectados, proponiendo una taxonomía que incluye desde la exposición de datos hasta la seguridad física y psicológica del menor, y recomendando el cifrado de extremo a extremo y políticas de control de acceso inspiradas en estándares como ISO/IEC 27001. En una línea similar, de Carvalho and Eler (2017) aplicaron el enfoque de desarrollo seguro de Microsoft (Security Development Lifecycle) al contexto del “toy computing”, identificando múltiples amenazas y definiendo requisitos clave de seguridad como la autenticación robusta, la protección de la privacidad y una adecuada gestión de actualizaciones, aspectos que deberían incorporarse desde el diseño de este tipo de dispositivos. Es fundamental que los fabricantes de juguetes inteligentes prioricen la implementación de medidas de seguridad robustas para proteger la privacidad y seguridad de los niños Radhakrishnan et al. (2024).

Este artículo complementa los trabajos citados mediante un análisis práctico del tráfico BLE generado por juguetes conectados en el contexto del Internet de las Cosas (IoT).

3. Metodología

La metodología seguida en este trabajo se ha dividido en dos grandes fases: la preparación del entorno de captura y la realización de las capturas de tráfico BLE. En la primera fase se configuraron los dispositivos y herramientas necesarias para permitir el análisis del tráfico. En la segunda fase se llevaron a cabo las capturas en escenarios reales con dispositivos

comerciales, permitiendo evaluar su comportamiento y nivel de seguridad.

Tradicionalmente, el análisis de tráfico BLE requería emplear al menos tres capturadores independientes —uno por cada canal de publicidad (37, 38 y 39)— para reconstruir el flujo completo de paquetes mediante la combinación manual de las tres capturas Wang (2024) . Este enfoque resultaba complejo, costoso y propenso a errores, ya que implicaba sincronizar tres dispositivos de captura y procesar múltiples ficheros de captura. Sin embargo, en su libro Koen Vervloesem propuso una técnica de saltos de canal sincronizados implementada en el dongle nRF52840 Vervloesem (2022) , que permite cubrir de forma automática y secuencial los tres canales de publicidad sin necesidad de hardware adicional. De esta manera, un único dispositivo es capaz de realizar la captura integral de todo el tráfico BLE de manera transparente y eficiente.

3.0.1. Material necesario

Para llevar a cabo la preparación del entorno se utilizaron dos dongles nRF52840, dispositivos USB de bajo coste basados en el SoC de Nordic Semiconductor, ampliamente soportados por herramientas como Wireshark y la suite nRF Connect for Desktop. Ambos dongles fueron configurados con funciones distintas y complementarias.

- El primer dongle se utilizó como herramienta de escaneo BLE, mediante el módulo “Bluetooth Low Energy” de nRF Connect. Esta configuración permite detectar dispositivos cercanos e identificar direcciones MAC aleatorias White (2024), una práctica común en dispositivos modernos para mejorar la privacidad, que complica la identificación persistente durante el análisis de tráfico.

- El segundo dongle fue programado con el firmware de sniffer BLE proporcionado por Nordic nrf (2025) , y conectado a Wireshark mediante el plugin extcap. Esta configuración habilita la captura en tiempo real de mensajes publicitarios y paquetes de datos GATT entre el dispositivo BLE y la aplicación móvil, permitiendo un análisis detallado de la comunicación.

3.0.2. Preparación del entorno

El entorno de captura se preparó en un sistema Windows, aunque el procedimiento es extrapolable a Linux. Para ello, se emplearon herramientas oficiales de Nordic Semiconductor, concretamente la suite nRF Connect for Desktop y el paquete de utilidades del nRF Sniffer for Bluetooth LE. Este último incluye tanto el firmware necesario para el dongle como los scripts de integración con Wireshark y los perfiles de análisis específicos para BLE.

Uno de los dongles nRF52840 fue programado con el firmware de sniffing (sniffernrf52840donglenrf528404.1.0.hex) utilizando la aplicación nRF Programmer. Para ello, se activó el modo DFU del dispositivo y se cargó el archivo .hex desde el entorno gráfico de la herramienta. La escritura del firmware habilita al dongle para actuar como una fuente de capturas BLE controlada externamente.

La integración con Wireshark se realizó mediante el plugin extcap proporcionado por Nordic. Este fue instalado copiando la carpeta completa extcap, junto con la subcarpeta SnifferAPI, al directorio personal de *extcap* de Wireshark, accesible desde las rutas internas del propio programa. Adicionalmente, se configuró un perfil de análisis BLE específico Figura 1, ProfilenRFSnifferBluetoothLE, que permite visualizar y decodificar correctamente estructuras de paquetes como ATT, GATT o L2CAP.

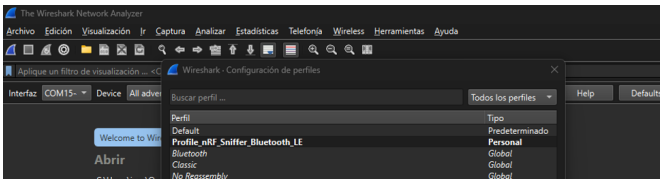

Figura 1: Configuración de Wireshark con la interfaz “NRF Sniffer for Bluetooth LE”

Para garantizar la compatibilidad con los scripts auxiliares del sniffer, se utilizó Python 3.11.5 o anterior, ya que versiones posteriores presentan problemas con la ejecución del archivo nrfsnifferble.bat.

Una vez completada esta configuración, Wireshark es capaz de detectar automáticamente la interfaz ”NRF Sniffer for Bluetooth LE”, permitiendo la captura directa de tráfico BLE, incluidos los paquetes de publicidad y los mensajes de aplicación intercambiados tras el emparejamiento.

En paralelo, se configuró un segundo dongle nRF52840 para operar como escáner BLE mediante la funcionalidad *Bluetooth Low Energy* de la suite nRF Connect. Al conectar el dispositivo, la aplicación gestiona de forma automática la instalación del firmware necesario y permite realizar exploraciones periódicas del entorno radioeléctrico. Esta herramienta resulta especialmente útil para identificar dispositivos que emplean direcciones MAC aleatorias como se puede ver en la Figura 2.

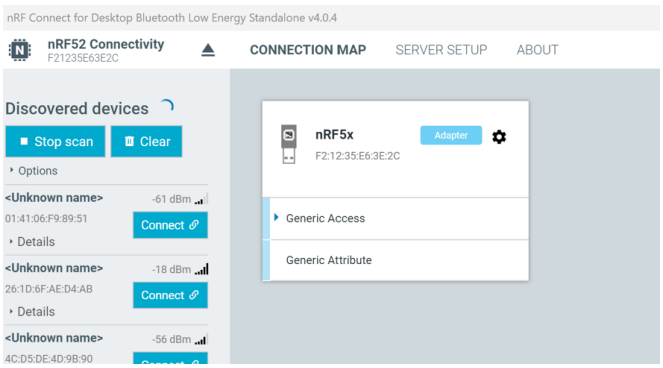

Figura 2: Escaneo de dispositivos y la identificación de MAC aleatorias

En resumen, el entorno de análisis se basa en el uso de dos dongles nRF52840 con funciones diferenciadas pero complementarias. El primero actúa como escáner BLE, permitiendo detectar dispositivos cercanos y registrar sus direcciones MAC aleatorias, que pueden cambiar dinámicamente por motivos de privacidad. Una vez identificada la MAC correspondiente al dispositivo de interés, esta información se utiliza como referencia para iniciar la captura detallada del tráfico mediante el

segundo dongle, configurado como sniffer BLE e integrado en Wireshark. Este flujo de trabajo permite correlacionar eventos de emparejamiento y comunicación con dispositivos específicos, como se muestra en la Figura 3 .

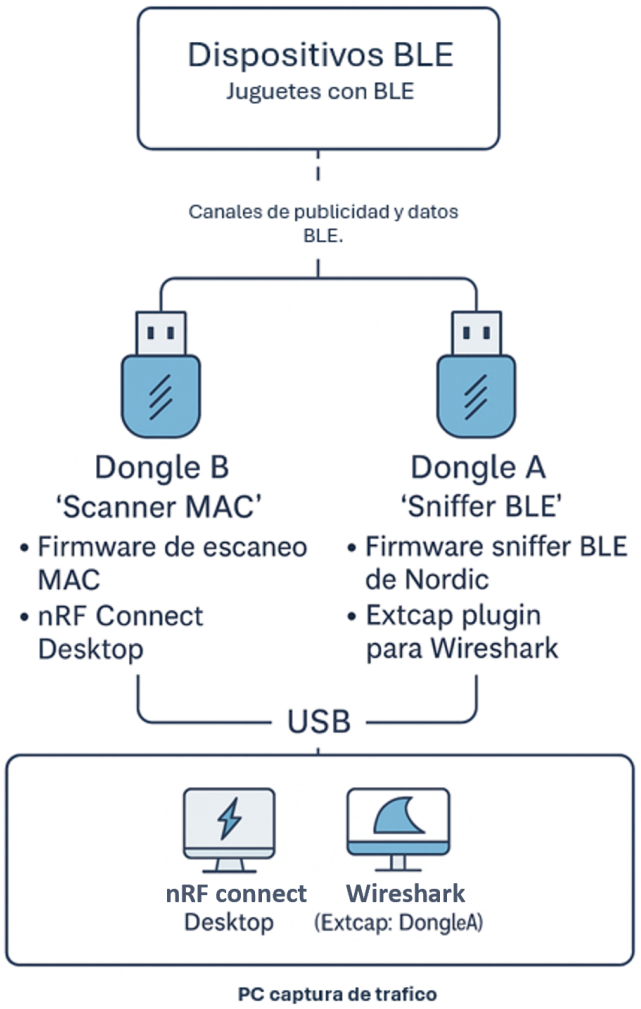

Figura 3: Entorno de caputra de trárfico BLE

4. Resultados

Se llevaron a cabo pruebas con varios dispositivos comerciales con conectividad BLE, utilizados habitualmente en contextos educativos o lúdicos. Por motivos de confidencialidad, no se mencionan sus nombres comerciales. El procedimiento seguido en todos los casos consistió en la identificación previa mediante escaneo de direcciones MAC, el emparejamiento con su aplicación oficial y la posterior captura del tráfico con Wireshark utilizando el dongle configurado como sniffer.

En algunos casos, se observaron direcciones MAC aleatorias, lo cual dificulta el seguimiento persistente de los dispositivos, pero no impide su detección puntual para iniciar la captura. Una vez establecida la comunicación entre la aplicación móvil y el dispositivo, se analizaron los paquetes intercambiados, aplicando filtros como btatt para centrarse en el protocolo ATT (Attribute Protocol)

El análisis de los campos presentes en los paquetes reveló que el atributo Authentication Signature se encontraba desactivado (False) en todas las capturas observadas Figura 4. Esto indica que los datos se transmiten sin cifrado ni autenticación. Un atacante situado en las proximidades podría interceptar las tramas, deducir el formato de los datos intercambiados o incluso inyectar comandos falsos en la comunicación.

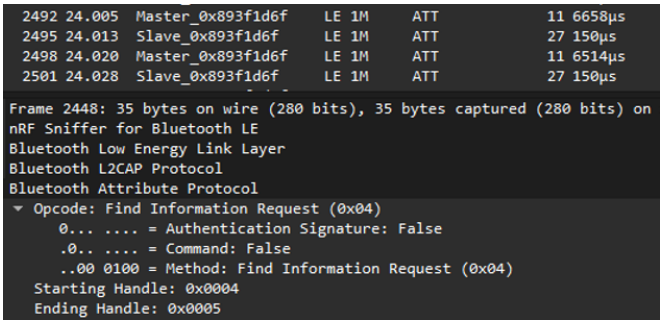

Figura 4: Captura de paquete BLE con Authentication Signature desactivado

Durante las pruebas se capturaron secuencias que aparentemente correspondían a comandos funcionales, tales como activación de luces, sonidos o movimientos. Estos datos, transmitidos en texto claro, eran interpretables directamente en formato hexadecimal, lo que facilita su análisis o explotación. Como se muestra en la Figura 5, la ausencia de protección criptográfica básica deja expuestos los dispositivos a ataques tanto pasivos como activos.

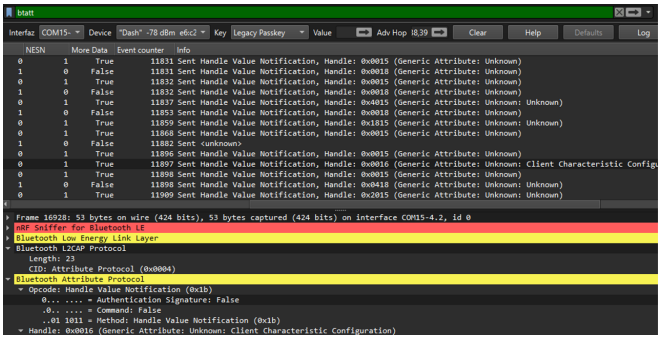

Figura 5: Captura de tráfico BLE con comandos transmitidos en texto claro

Este comportamiento muestra que las medidas de seguridad en ciertos productos comerciales basados en BLE son escasas o inexistentes. Se observa un interés en la facilidad de uso o el bajo coste frente a consideraciones básicas de confidencialidad e integridad de las comunicaciones las cuales no se han tenido en cuenta.

5. Conclusiones y trabajos futuros

Los resultados obtenidos muestran que algunos dispositivos comerciales con conectividad Bluetooth Low Energy (BLE) transmiten datos sin aplicar cifrado ni autenticación. Esta falta de protección permite no solo la captura pasiva de información, sino también la posibilidad de realizar ataques

como inyección de comandos, modificación de mensajes o repetición de paquetes previamente observados.

Este tipo de vulnerabilidades puede tener impacto en entornos donde se emplean dispositivos BLE sin medidas básicas de seguridad, especialmente cuando se utilizan en contextos domésticos o educativos.

Como línea de trabajo futura, se plantea utilizar este tipo de capturas para entrenar modelos de detección de anomalías. Para ello, sería necesario generar un conjunto de datos etiquetado con tráfico legítimo y con ejemplos de distintos ataques realizables sobre dispositivos BLE. Una vez diseccionado y procesado, este conjunto de datos permitiría entrenar modelos de aprendizaje automático capaces de detectar comportamientos anómalos en tiempo real.

El objetivo final sería reutilizar el sniffer como un sistema de detección de intrusiones (IDS) en tiempo real, Esto haría posible ejecutar el IDS sobre un sniffer BLE sin modificar el firmware de los juguetes, que suelen tener hardware muy limitado. Toda la detección se realizaría en un dispositivo externo (con un dongle nRF52840), sin afectar al rendimiento, la configuración ni el coste de los juguetes. Esto permite aplicar medidas como la detección temprana de patrones anómalos en el tráfico o accesos inusuales a servicios, sin necesidad de instalar agentes ni actualizar los dispositivos, a diferencia de los sistemas clásicos basados en firmas o protección activa, que requieren mayor intervención sobre el sistema..

Agradecimientos

Este trabajo ha sido financiado por el Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea (Next Generation), gracias al proyecto “Seguridad en entornos domésticos y empresariales de Internet de las Cosas en el contexto de tecnologías 5G-IoT”.

Referencias

, 02 2023. Introduction to bluetooth low energy (ble).
URL: https://www.argenox.com/library/bluetooth-low-energy/introduction-to-bluetooth-low-energy-v4-0/

, 01 2025. nrf sniffer for bluetooth le.
URL: https://www.nordicsemi.com/Products/Development-tools/nrf-sniffer-for-bluetooth-le/download

Allana, S., Chawla, S., 08 2020. Childshield: A rating system for assessing privacy and security of internet of toys. Telematics and Informatics 56, 101477–101477.
URL: https://doi.org/10.1016/j.tele.2020.101477
DOI: doi:10.1016/j.tele.2020.101477

Chu, G., Apthorpe, N., Feamster, N., 01 2018. Security and privacy analyses of internet of things children’s toys. arXiv.
URL: https://arxiv.org/abs/1805.02751
DOI: doi:10.48550/ARXIV.1805.02751

Classen, J., Hollick, M., 06 2021. Happy mitm.
URL: https://doi.org/10.1145/3448300.3467822
DOI: doi:10.1145/3448300.3467822

de Carvalho, L. G., Eler, M. M., 01 2017. Security requirements for smart toys, 144–154.
URL: https://doi.org/10.5220/0006337001440154
DOI: doi:10.5220/0006337001440154

de Paula Albuquerque, O., Fantinato, M., Kelner, J., de Albuquerque, A. P., 12 2019. Privacy in smart toys: Risks and proposed solutions. Electronic Commerce Research and Applications 39, 100922–100922.
URL: https://doi.org/10.1016/j.elerap.2019.100922
DOI: doi:10.1016/j.elerap.2019.100922

INCIBE, 01 2024. Estudio de la ciberseguridad juguetes conectados. Tech. rep.
URL: https://www.incibe.es/sites/default/files/espacios/ed2026/laboratorio/EstudioINCIBE_ciberseguridad_juguetes_conectados.pdf

Koulouras, G., Katsoulis, S., Zantalis, F., 02 2025. Evolution of bluetooth technology: Ble in the iot ecosystem.
URL: https://doi.org/10.3390/s25040996
DOI: doi:10.3390/s25040996

Lonzetta, A. M., Cope, P., Campbell, J. P., Mohd, B. J., Hayajneh, T., 07 2018. Security vulnerabilities in bluetooth technology as used in iot. Journal of Sensor and Actuator Networks 7, 28–28.
URL: https://doi.org/10.3390/jsan7030028
DOI: doi:10.3390/jsan7030028

Nagrare, T., Sindhewad, P., Kazi, F., 01 2023. Ble protocol in iot devices and smart wearable devices: Security and privacy threats. arXiv (Cornell University).
URL: https://arxiv.org/abs/2301.03852
DOI: doi:10.48550/arxiv.2301.03852

Radhakrishnan, I., Jadon, S., Honnavalli, P. B., 06 2024. Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained iot devices. Sensors 24, 4008–4008.
URL: https://doi.org/10.3390/s24124008
DOI: doi:10.3390/s24124008

Sivakumaran, P., Blasco, J., 01 2021. argxtract: Deriving iot security configurations via automated static analysis of stripped arm binaries. arXiv (Cornell University).
URL: https://arxiv.org/abs/2105.03135
DOI: doi:10.48550/arxiv.2105.03135

Vervloesem, K., 06 2022. Develop your own bluetooth low energy applications for raspberry pi.
URL: https://koen.vervloesem.eu/books/

vinnter, 02 2023. What’s new with ble5? and how does it compare to ble4?
URL: vinnter.se/whats-new-with-ble5-and-how-does-it-compare-to-bl

Wang, Z., 02 2024. Securing bluetooth low energy: A literature review.
URL: https://arxiv.org/abs/2404.16846
DOI: doi:10.48550/arXiv.2404.16846

Want, R., Schilit, B. N., Laskowski, D., 10 2013. Bluetooth le finds its niche. IEEE Pervasive Computing 12, 12–16.
URL: https://doi.org/10.1109/mprv.2013.60
DOI: doi:10.1109/mprv.2013.60

Wen, H., Lin, Z., Zhang, Y., 10 2020. Firmxray: Detecting bluetooth link layer vulnerabilities from bare-metal firmware.
URL: https://doi.org/10.1145/3372297.3423344
DOI: doi:10.1145/3372297.3423344

White, N., 06 2024. Using the nordic nrf sniffer for ble.
URL: https://dojofive.com/blog/using-the-nordic-nrf-sniffer-for-ble/

Zachariah, T., Clark, M., Dutta, P., 10 2018. Bluetooth low energy in the wild dataset, 27–28.
URL: https://doi.org/10.1145/3277868.3277882
DOI: doi:10.1145/3277868.3277882

Zhang, Y., Weng, J., Dey, R., Fu, X., 01 2020. Bluetooth low energy (ble) security and privacy. Springer eBooks, 123–134.
URL: https://doi.org/10.1007/978-3-319-78262-1_298
DOI: doi:10.1007/978-3-319-78262-1_298