e-ISSN: 2528-8091
Vol. 10, N° V CICACI - 2025

Análisis de la vulnerabilidad en la transmisión de datos bluetooth entre dispositivos wearables y móviles

Vulnerability analysis in bluetooth data transmission between wearable and mobile devices

https://doi.org/10.5281/zenodo.20432061

AUTORES:

Fernández Torres Ana del Rocío[1]
Universidad Técnica de Babahoyo
0000-0002-0385-180X
afernandez@utb.edu.ec

Arreaga Elizondo Nallely Herlinda[2]
Universidad Técnica de Babahoyo
arreagaelizondo@fafi.utb.edu.ec

Rojas Gallegos Jeniffer Roció[3]
Universidad Técnica de Babahoyo
jrojas059@fafi.utb.edu.ec

Anabella Flor Cedeño Fernández[4]
Universidad Técnica de Babahoyo
acedenof@fafi.utb.edu.ec

DIRECCIÓN PARA CORRESPONDENCIA: afernandez@utb.edu.ec

Fecha de recepción: 20 / 11 / 2025

Fecha de aceptación: 27 / 11 / 2025

RESUMEN

El estudio se puede resumir como una tendencia muy marcada los dispositivos Wearable, como relojes inteligentes que monitorean los avances en actividad física o por salud para gestionar datos personales. Pero esta transformación por conexiones de Bluetooth y entre varios dispositivos más como la telefonía móvil está representando una amenaza para la

privacidad por los múltiples ataques de vulnerabilidades para los usuarios. Este estudio permite el análisis de las principales vulnerabilidades presente en dicho proceso de comunicación y transmisión, permitiendo asociar tipos de riesgos a los modelos de conexión y sincronización que son más comunes.

El enfoque técnico y contextual, permite evaluar los mecanismos de seguridad para poder ser implementados en la comunicación wearable- móvil y su grado de efectividad frente a las amenazas. Entre los resultados tenemos debilidad en el cifrado de datos, autentificación poco robusta y estar expuestos a ataque. Parte de esta investigación, es proponer buenas prácticas y estrategias de mitigación para mejorar la protección de datos personales en entornos peligrosos que integran tecnología de este tipo. De esta manera el trabajo contribuye a una comprensión más profunda de la seguridad en dispositivos móviles y ofrece normas para su implementación segura en escenarios cotidiano.

Palabras clave: *seguridad, dispositivos wearables, Bluetooth, transmisión de datos, privacidad, ciberseguridad, smartphones.*

ABSTRACT

The study can be summarized as a clear trend toward the use of wearable devices, such as smartwatches, which monitor physical activity or health-related metrics to manage personal data. However, this transformation—driven by Bluetooth connections and interactions with other devices like mobile phones—poses a threat to privacy due to multiple user-targeted vulnerability attacks. This study analyzes the main vulnerabilities present in these communication and data transmission processes, enabling the association of specific risks with the most common connection and synchronization models.

The technical and contextual approach allows for the evaluation of security mechanisms that can be implemented in wearable–mobile communication and their effectiveness against potential threats. The findings highlight weaknesses in data encryption, insufficiently robust authentication, and exposure to various attacks. Part of this research includes proposing best practices and mitigation strategies to enhance the protection of personal data in high-risk

environments involving this type of technology. In this way, the work contributes to a deeper understanding of mobile device security and offers guidelines for their secure implementation in everyday scenarios.

Keywords: *security, wearable devices, Bluetooth, data transmission, privacy, cybersecurity, smartphones.*

INTRODUCCIÓN

El crecimiento en el uso de dispositivos wearables, como relojes inteligentes, bandas deportivas y sensores biométricos, ha transformado la forma en que las personas interactúan con la tecnología y gestionan su información personal. Estos dispositivos, al vincularse con teléfonos móviles mediante conexiones inalámbricas, utilizan en su mayoría el protocolo Bluetooth por su eficiencia energética y facilidad de integración.

No obstante, esta comodidad ha traído consigo nuevas preocupaciones en materia de seguridad. Diversos estudios han documentado que las comunicaciones a través de Bluetooth pueden presentar vulnerabilidades, especialmente cuando no se aplican medidas de protección adecuadas o se utilizan versiones antiguas del protocolo. Ataques como el bluejacking, bluesnarfing y bluebugging, entre otros, permiten interceptar o manipular datos sensibles sin que el usuario lo perciba.

La situación se agrava si se considera que los dispositivos wearables suelen manejar información de carácter personal o confidencial, como datos de salud, ubicación o contraseñas. A pesar de las mejoras introducidas en las versiones recientes del protocolo, la falta de actualizaciones, las configuraciones por defecto y el desconocimiento de los riesgos siguen siendo factores críticos que exponen a los usuarios.

Este artículo analiza las principales debilidades que afectan la transmisión de datos vía Bluetooth entre dispositivos wearables y móviles. Además, se examinan los impactos potenciales de estas vulnerabilidades y se contrastan distintas estrategias técnicas de mitigación, con el fin de contribuir a una mayor comprensión del problema y fomentar prácticas más seguras en el uso de estas tecnologías.

METODOLOGÍA

La presente investigación utilizo métodos **cualitativo y técnico-descriptivo** para analizar los procesos de identificación y análisis de vulnerabilidades, con énfasis en la tecnología Bluetooth, como podemos ver este enfoque permite comprender las debilidades técnicas del protocolo, las amenazas derivadas y las estrategias de mitigación más efectivas documentadas en la literatura actual**.**

Identificación y análisis de vulnerabilidades

Bluetooth es una tecnología de comunicación inalámbrica que permite el intercambio de datos entre dispositivos a corta distancia. Su bajo consumo de energía y facilidad de conexión han favorecido su adopción en diversos entornos: teléfonos móviles, automóviles, dispositivos médicos, domótica, entre otros. Sin embargo, esta misma popularidad ha expuesto diversas vulnerabilidades de seguridad que pueden ser explotadas por atacantes. Identificar y analizar estas vulnerabilidades es esencial para mitigar riesgos, prevenir intrusiones y garantizar la integridad y confidencialidad de los datos transmitidos (Hasan, R.; Khan, M.; Hassan, M. M., 2020).

La identificación de vulnerabilidades implica reconocer las debilidades del protocolo Bluetooth y los errores de configuración presentes en los dispositivos que lo implementan. Muchas de estas debilidades han sido documentadas por investigadores de seguridad y organizaciones especializadas. Se han demostrado ataques que pueden interceptar comunicaciones, tomar el control del dispositivo o desactivar temporalmente sus funciones (Kumar, S.; Lee, H. J., 2012).

Entre las vulnerabilidades más comunes se encuentra:

- **Bluejacking**, que consiste en enviar mensajes no deseados a dispositivos cercanos. Aunque no representa una amenaza significativa, puede ser una puerta de entrada para ataques más deseables al establecer una conexión no autorizada con el dispositivo objetivo (Faruki, P.; Bharmal, A.; Laxmi, V.; Ganmoor, V.; Gaur, M. S.; Conti, M.; Buyya, R., 2015).

e-ISSN: 2528-8091
Vol. 10, N° V CICACI - 2025

- **Bluesnarfing**, es el más grave mediante el cual un atacante puede acceder sin permiso a información almacenada en el dispositivo, como contactos, mensajes o archivos. Esto ocurre cuando los dispositivos no requieren la autenticación adecuada para compartir datos, algo más común en versiones anteriores del protocolo, o cuando el Bluetooth está permanentemente en modo visible.
- **Bluebugging**, que permite a un atacante tomar el control del dispositivo afectado. Mediante esta técnica, pueden realizar llamadas, enviar mensajes o acceder al micrófono del teléfono, todo ello sin el conocimiento del usuario. Este ataque se basa en la explotación de fallos en la autenticación de comandos y la configuración predeterminada de muchos dispositivos.
- **Ataques Man-in-the-Middle (MitM)**, en los que un atacante intercepta la comunicación entre dos dispositivos Bluetooth sin ser detectado. Si el proceso de emparejamiento no está correctamente cifrado o autenticado, un atacante puede leer o modificar la información transmitida. Esto representa un grave riesgo, especialmente en aplicaciones donde se transmiten datos confidenciales, como contraseñas, historiales médicos o credenciales bancarias.
- **Ataques de repetición también son comunes**. Estos se basan en capturar transmisiones válidas entre dispositivos y retransmitirlas para obtener acceso no autorizado o ejecutar comandos previamente aceptados.
- **Ataques de desautenticación y denegación de servicio (DoS)**, en los que el atacante envía paquetes maliciosos para interrumpir la conexión Bluetooth, provocando que los dispositivos se desconecten o dejen de funcionar temporalmente.

Análisis de seguridad diferentes dispositivos que utilizan tecnología Bluetooth Low Energy (BLE).

La siguiente tabla resume los resultados obtenidos en una práctica de análisis de seguridad sobre diez dispositivos que utilizan tecnología Bluetooth Low Energy (BLE). Se evaluaron

tres mecanismos clave: cifrado AES en la capa de enlace, generación de claves de sesión temporales, y autenticación por clave compartida.

Nº	Dispositivo	Tipo / Categoría	Cifrado AES en enlace	Renovación de claves	Autenticación por clave compartida	Conclusión general	Observaciones técnicas
1	Dispositivo A	Teléfono inteligente (alta gama)	Confirmación de código numérico mostrada	Requiere autenticación tras desvincular	Códigos coincidentes en pantalla	Cumple con los 3 mecanismos	Comportamiento ideal y seguro
2	Dispositivo B	Reloj inteligente (serie premium)	Requiere PIN de emparejamiento	Nueva autenticación solicitada	Confirmación numérica clara	Cumple con los 3 mecanismos	Seguridad robusta en todas las fases
3	Dispositivo C	Auriculares inalámbricos (nueva generación)	Solicita código visible	Se genera nueva sesión al reconectar	Coincidencia de código numérico	Cumple con los 3 mecanismos	Compatible con prácticas modernas de seguridad
4	Dispositivo D	Pulsera inteligente / wearable deportivo	Autenticación inicial activa	Solicita PIN nuevamente	Visualización numérica en ambos extremos	Cumple con los 3 mecanismos	Se ajusta al estándar BLE
5	Dispositivo E	Auriculares inalámbricos (gama baja)	Emparejamiento sin autenticación	Reconexión automática sin validación	No muestra confirmación alguna	No cumple con ningún mecanismo	Potencialmente vulnerable
6	Dispositivo F	Reloj inteligente (modelo económico)	Solicita código al emparejar	No renueva clave de sesión	No muestra código compartido	Parcial: solo cifrado AES activo	Deficiente gestión de sesiones y autenticación
7	Dispositivo G	Smartphone básico	Emparejamiento directo	Solicita autenticación tras reconexión	Sin confirmación numérica	Parcial: solo renovación de claves	Cifrado ausente compromete privacidad
8	Dispositivo H	Wearable genérico	Sin solicitud de PIN o código	Reconexión automática	Coincidencia de código numérico	Parcial: solo autenticación por clave	Carencia de cifrado y rotación de claves
9	Dispositivo I	Auriculares económicos	Código solicitado al conectar	Mismo vínculo aceptado sin verificación	No hay código visual compartido	Parcial: solo cifrado activo	Sesión persistente sin autenticación
10	Dispositivo J	Smartband básica	Sin verificación al emparejar	Reutiliza sesión anterior	No hay prueba de clave compartida	No cumple con ningún mecanismo	Alta exposición a ataques de intermediario

Tabla1. -*Autores análisis de dispositivos con parámetros de seguridad*

Estrategias de Mitigación

El análisis de estas vulnerabilidades ha llevado al desarrollo de **estrategias de mitigación**, entre las que se destacan el uso de protocolos de seguridad avanzados, actualizaciones periódicas de firmware y educación al usuario final. La siguiente tabla resume una evaluación comparativa de algunas de las principales estrategias de mitigación adoptadas en entornos Bluetooth:

Criterio	Cifrado AES	Claves de sesión temporales	Autenticación por clave compartida
Descripción técnica	Algoritmo de cifrado simétrico de 128 bits en modo CCM (BLE) que garantiza confidencialidad e integridad	Claves dinámicas generadas durante el emparejamiento que son válidas solo por sesión	Validación mediante PIN o código de confirmación entre dispositivos
Nivel de seguridad proporcionado	Alto	Alto	Medio - alto
Tipo de amenaza de mitigación	Intercepción de datos mediante lectura de tráfico	Ataques de repetición debido a la reutilización de claves	Acceso no autorizado suplantando el dispositivo
Visibilidad para el usuario	Baja dado a que opera en segundo plano	Nula porque es completamente transparente	Alta porque requiere acción del usuario
Compatibilidad con versiones Bluetooth	BLE 4.0 en adelante	Bluetooth 2.1+ con Segure Simple Pairing (SSP)	Universal
Ventajas	Tiene una alta protección sin afectar la usabilidad	Tiene una mayor protección sin intervención del usuario	Mejora el control del usuario sobre a qué dispositivos se conectan
Limitaciones	Proviene de un soporte nativo, por lo que no siempre es configurable por el usuario	Es difícil de verificar sin alguna herramienta especializada	Muchos usuarios prefieren la comodidad de un emparejamiento rápido sacrificando la seguridad

Tabla2.- *Recolección de información de diferentes fuentes de protocolos*

RESULTADOS

Resultados de la tabla de incidencias en 10 dispositivos de diferente gama y prácticas de protocolos de seguridad cifrado AES, entre otros.

Según el análisis de una muestra de dispositivos que se procedió a evaluar, estos dispositivos pertenecientes a diferentes categorías de uso y marca, evidencian un cumplimento variado de mecanismos de seguridad en la transmisión por un medio que está bien utilizado como es vía Bluetooth. Se identificó que solo cuatro dispositivos (A, B, C y D) cumplen con los tres mecanismos fundamentales evaluados: cifrado AES en el enlace, renovación de claves de sesión y autenticación por clave compartida.

Los dispositivos todos de gama media-alta o premium exhiben un comportamiento alineado con las buenas prácticas actuales en ciberseguridad, presentando confirmación numérica clara, renovación de sesión tras desvinculación y protección contra emparejamientos no autorizados.

En contraste, dos dispositivos (E y J) no cumplen con ninguno de los mecanismos analizados. Ambos corresponden a dispositivos de gama baja, cuyas implementaciones permiten emparejamientos sin validación y reconexión automática sin renovación de claves ni autenticación. Esto los convierte en objetivos vulnerables ante ataques de intermediario (MitM) o suplantación de identidad, debido a la ausencia total de controles de seguridad básicos.

Por otro lado, se identificaron cuatro dispositivos (F, G, H e I) que presentan cumplimiento parcial. Cada uno implementa solo uno de los tres mecanismos evaluados, lo que genera un nivel de protección limitado.

Ejemplo, el Dispositivo F activa cifrado al momento del emparejamiento, pero carece de renovación de clave y validación posterior, exponiendo la sesión a accesos persistentes. Similarmente, el Dispositivo G renueva claves tras la reconexión, pero no muestra confirmación visual ni usa cifrado, lo que puede comprometer la privacidad de los datos. Estos casos reflejan una implementación incompleta de las medidas de seguridad, especialmente en modelos económicos.

En términos generales, se observó una correlación directa entre la gama del dispositivo y el cumplimiento de mecanismos de seguridad. Los modelos de gama alta o premium muestran integración adecuada de medidas de protección, mientras que los dispositivos de menor costo o genéricos presentan deficiencias críticas en la gestión de sesiones, autenticación y cifrado.

Resultados del análisis bibliográfico

El estudio permitió reconocer de forma estructurada un conjunto de vulnerabilidades recurrentes en dispositivos con conectividad Bluetooth, entre las que destacan:

- Bluejacking, Bluesnarfing y Bluebugging, como vectores de ataque activos aún en versiones modernas cuando no se implementan adecuadamente protocolos de seguridad.
- Existencia de ataques Man-in-the-Middle (MitM) y repetición, asociados con procesos de emparejamiento inseguros o cifrado débil.
- Alta presencia de dispositivos vulnerables debido a la falta de actualizaciones, configuraciones predeterminadas inseguras y desconocimiento del usuario.

Resultados del análisis técnico.

A través del análisis técnico, se logró clasificar las amenazas según su nivel de impacto y probabilidad de explotación, estableciendo una priorización clara para su mitigación:

- Ataques como el Bluesnarfing y Bluebugging presentan riesgo alto, al comprometer directamente la confidencialidad y el control del dispositivo.
- El Bluejacking y los ataques de desautenticación/DoS fueron clasificados como riesgo moderado, pero representan una puerta de entrada o una forma de interrupción operacional.
- Las debilidades en la autenticación y el cifrado del proceso de emparejamiento representan un vector común para múltiples amenazas.

Resultados de la tabla comparativa de estrategias de mitigación

- El uso de cifrado AES y claves de sesión temporales representa un nivel alto de protección, especialmente si se implementan correctamente desde el firmware del dispositivo.
- La autenticación por clave compartida, aunque accesible, tiene limitaciones importantes cuando no se complementa con otras medidas.
- Las estrategias más eficaces operan de forma transparente para el usuario, lo que mejora la seguridad sin afectar la experiencia de uso, pero su implementación depende de la compatibilidad con versiones modernas de Bluetooth.

DISCUSIÓN

Los resultados obtenidos son la reflexión sobre el estado actual de la seguridad en dispositivos con tecnología Bluetooth, revelando no solo la persistencia de vulnerabilidades ampliamente documentadas en las citas bibliográficas, sino también la limitada adopción de mecanismos efectivos de mitigación.

Los resultados obtenidos permiten observar una relación clara entre el nivel de seguridad implementado y la gama del dispositivo. En la muestra analizada, los dispositivos de gama media-alta o premium (A, B, C y D) demostraron cumplir adecuadamente con los tres mecanismos evaluados: cifrado AES, renovación de claves de sesión y autenticación por clave compartida. Esta coincidencia sugiere que los fabricantes de estas líneas priorizan la integración de prácticas actualizadas de ciberseguridad, probablemente en respuesta a exigencias del mercado y a la necesidad de proteger datos sensibles.

En cambio, los dispositivos de gama baja (E y J), que no cumplen con ningún mecanismo, evidencian un enfoque centrado más en la funcionalidad que en la seguridad. La ausencia de cifrado, autenticación y validación en las sesiones de emparejamiento los convierte en un punto débil evidente en cualquier ecosistema inalámbrico. Esta situación no es aislada: varios

estudios revisados destacan cómo el *bluejacking*, *bluesnarfing*, *bluebugging* y otros ataques continúan siendo posibles precisamente por configuraciones predeterminadas poco seguras o por la falta de actualizaciones periódicas.

Los casos intermedios (F, G, H e I) revelan una implementación parcial de medidas de protección. Es decir, a pesar de incorporar alguna capa de seguridad, como el cifrado o la autenticación visual, no se garantiza la renovación de sesiones o el emparejamiento seguro, lo cual deja abiertas varias rutas de ataque. Esta fragmentación en la protección sugiere una falta de estandarización entre fabricantes y, posiblemente, una subestimación del riesgo por parte de los usuarios.

Las vulnerabilidades como el Bluesnarfing o el Bluebugging han sido reportadas desde hace más de una década, su presencia continúa siendo significativa en dispositivos de uso cotidiano, lo cual evidencia una brecha preocupante entre el conocimiento técnico disponible y su implementación práctica.

En este sentido, uno de los hallazgos más relevantes es la tendencia a priorizar la usabilidad sobre la seguridad.

La mayoría de los ataques documentados se basan en errores de configuración o la permanencia de modos de visibilidad activados por defecto, lo que sugiere que los fabricantes aún no integran una cultura de "seguridad por diseño".

Esta situación se agrava al considerar que muchos usuarios desconocen los riesgos asociados al uso cotidiano del Bluetooth, especialmente en espacios públicos o redes abiertas.

Por otro lado, la evaluación comparativa de estrategias de mitigación permitió establecer que existen soluciones técnicas robustas como el cifrado AES y las claves de sesión dinámicas cuya eficacia es ampliamente reconocida.

Los resultados refuerzan la necesidad de que la identificación de vulnerabilidades no sea un proceso puntual, sino una tarea continua y articulada dentro de la gestión integral del riesgo. Tal como indican autores como Fernández y López (2019), el monitoreo constante y la adaptación a las amenazas emergentes son elementos clave para mantener un entorno tecnológico resiliente.

Finalmente, se constata que la investigación en este campo no debe limitarse al aspecto técnico. La interacción entre tecnología, usuario y políticas de seguridad demanda un enfoque multidisciplinario que incorpore también la dimensión humana y organizacional.

CONCLUSIONES

Muchos dispositivos con tecnología Bluetooth aún presentan fallas en la implementación de protocolos esenciales de seguridad. Estas carencias los hacen vulnerables a ataques como emparejamientos no autorizados y suplantación de identidad. El uso sin protección compromete la integridad y confidencialidad de los datos transmitidos, representado un riesgo mayor en dispositivos wearables utilizados para información personal o médica.

Se detectó un bajo nivel de conocimiento por parte de los usuarios sobre los riesgos asociados al Bluetooth. Una gran mayoría desconoce qué es el cifrado AES o qué tipo de información puede ser interceptada, esta falta de información limita la capacidad del usuario para protegerse. Además, muchas personas aceptan conexiones inseguras por desconocimiento, el educar al usuario es esencial para una verdadera estrategia de seguridad.

Aunque muchos usuarios prefieren emparejamientos rápidos, existe una clara disposición a adoptar métodos más seguros si estos son explicados adecuadamente. Esto demuestra que la seguridad y la usabilidad no son excluyentes. Un diseño funcional puede facilitar la adopción de buenas prácticas sin generar molestias. La experiencia del usuario debe estar alineada con medidas de protección efectivas. Esto garantizará un entorno más seguro para la transmisión de datos.

REFERENCIAS BIBLIOGRÁFICAS

Faruki, P.; Bharmal, A.; Laxmi, V.; Ganmoor, V.; Gaur, M. S.; Conti, M.; Buyya, R. (2015). Android Security: A Survey of Issues, Malware Penetration, and Defenses. IEEE Communications Surveys & Tutorials, 998–1022.

Godínez-Rodríguez, E., Ortíz, M. P., Balankin, A., Flores, R., Ortíz, J. P., García, V. M. S., & Cruz, M. A. M. (2021). Encriptado de Imágenes Basado en Advanced Encryption

Standard y Caos Image Encryption Based on Advanced Encryption Standard and Chaos.

Hasan, R.; Khan, M.; Hassan, M. M. (2020). A Survey on Bluetooth Security Threats and Defense Mechanisms. IEEE Access, 255–273.

Kumar, S.; Lee, H. J. (2012). Security Issues in Bluetooth Communication and Solutions. International Journal of Computer Applications, 26-31.

Godínez-Rodríguez, E., Ortíz, M. P., Balankin, A., Flores, R., Ortíz, J. P., García, V. M. S., & Cruz, M. A. M. (2021). Encriptado de Imágenes Basado en Advanced Encryption Standard y Caos Image Encryption Based on Advanced Encryption Standard and Chaos.

Montenegro Torres, D. (2020). Comparación de algoritmos de encriptación para la transferencia de archivos en mensajería instantánea. Repositorio Institucional - USS. https://repositorio.uss.edu.pe/handle/20.500.12802/7478

Pereto Soler, C. (2024). Diseño de un sistema de monitorización y control de datos del entorno a través de nodos LoRa accesibles desde una app del teléfono móvil. https://riunet.upv.es/handle/10251/201804

Rodríguez Sanz, J. J. (2020, junio). Exfiltración de datos a través de enlaces Bluetooth [Info:eu-repo/semantics/bachelorThesis]. E.T.S. de Ingenieros Informáticos (UPM). https://oa.upm.es/62903/

Ruano-Daza, D. M., Valiente-Simbaqueba, B. D., Guevara-Triana, L. F., & Poblador, M. S. P. (2021). Centro de Investigación de la Universidad Distrital Francisco José de Caldas. Revista Vínculos, 18(2), Article 2. https://revistas.udistrital.edu.co/index.php/vinculos/article/view/17632

Sesé Vega, E. (2020). Estudio de las vulnerabilidades de la tecnología Bluetooth. https://hdl.handle.net/10609/106368

Fernández, J., & López, R. (2019). Continuous Vulnerability Monitoring and Adaptive Security Strategies. *Revista Iberoamericana de Seguridad Informática*, 95-110.

Khan, M. A., Ahmed, S., & Tariq, M. (2021). Vulnerability Identification and Risk Assessment in Cybersecurity: A Comprehensive Review. *Journal of Information Security*, 210-225.