Security and Privacy Analysis of Low-Cost Fitness Tracking Devices & Apps

Project Research

Wiktor Knapik – C00283826

SETU Carlow Campus
BSc (Hons) IT Security & Cybercrime

Executive Summary

A very small percentage of the population actually know the behind the scenes of how securely their activity data is transmitted. A lot of devices such as fitness trackers rely on Bluetooth Low Energy (BLE) to transmit this data but is it really that secure to keep intruders from uncovering the closed off data.

The goal of my project is to examine the security and privacy risks in the BLE communication used by these devices, specifically focusing on cheap alternatives of Fitness Trackers. The main focus will be on how challenging would it be for someone to listen, track and interfere with data that is transmitted by a user. I will be using a test environment using multiple fitness tracking devices connected with an Android smartphone to capture BLE traffic that occurs when the devices are being used is day to day circumstances.

The tools that I will use to analyse and interfere with the BLE traffic will Wireshark, nRF Connect and a Kali Linux bootable setup. The project will also include realistic attack scenarios which will contain eavesdropping and Man-In-The-Middle attacks which will gather information to learn the possibilities of such an attack. My expected outcome is to identify weaknesses and bad practices uses in these lower cost ended trackers that use BLE. A comparison between a low end and a higher end device will be included to highlight the security cons of such a device and how spending an extra more would be much more beneficial than one would think. With this information gathered, I will provide understandable recommendations for both manufacturers and everyday user on how to reduce the risks.

Table of Contents

Introduction

If you're a gym goer or just have an interest in tracking your health, you would know that wearable fitness trackers can become a part of anyone's everyday life. They are very good in helping people monitor steps, calories burnt, heart rate and sleep with minimum effort. During this tracking process, these devices will collect and transmit sensitive information about the user's health, routines, and location which raises a question on how this data is handled. Most of these devices will be relying on its Bluetooth Low Energy (BLE) to send data to a smartphone device which will be connected via Bluetooth. BLE in general is used because of its low power ability and its good compatibility in constant wireless communication. Due to the design of BLE connections, it can be exposed to threats more often than you would think. These threats consist of passive eavesdropping and Man In The Middle attacks if the security is not configured and implemented right.

There is a gap on the assumption that any device using BLE will offer similar protection as the rest, but that's the not the case as there is a margin between price and security. Although there is a large amount of usage with cheaper fitness tracker, there is still less attention on the work of security on these devices. Related studies on BLE devices and other IoT devices found issues on the strength of pairing methods and encryption that is used to track users even when there is announced protections in place. Up to date research on today's technology has shown that BLE does contain proficient security but it comes with a cost and often ignored for that reason to make the device cheaper.

The main focus is on these lower cost devices with the aim to investigate the security and privacy risks in the BLE communication used by the devices. I will place myself in the shoes of an attacker and examine how challenging it would be for a Man In The Middle to listen in, track or interfere with the data that is being transmitted when the fitness tracker and an Android smartphone is in everyday use. This research will be conducted using multiple devices with different applications linked to the device to make it a fair and even research. BLE traffic will be captured during the fair usage of the device as it was in the use of a consumer using the device for tracking their health. The analysis of the BLE traffic will be done with tools such as Wireshark and the big one will be nRF Connect on a bootable Kali Linux setup. The project is to view practical attack scenarios, including the eavesdropping and all relating Man In The Middle attacks that could be created. I will also be comparing the outcome to the outcome of a higher end tracking device, a more popular brand, Samsung, this will highlight the differences in how BLE security is done with a higher budget in the security aspect. In conclusion this research is to identify security vulnerabilities in cheaper devices. A clear and practical recommendation will be made for the designers and everyday users from the researched outcomes on how to keep personal data, personal.

Methodology

The Approach:

My project will be going over the security of low-cost compared to higher-end fitness trackers which use Bluetooth Low Energy (BLE) which connects to a smartphone, which will be an android device in my case. The main focus will be on the attacker's perspective on what they see or can do by capturing and analysing the BLE traffic. It will also get their perspective on the eavesdropping by doing MITM attacks.

Devices:

The devices will consist of 5 different fitness trackers each with different applications. These 5 devices are sourced from Temu, AliExpress and Shein, common online stores which cheap products are bought by consumers. An android smartphone is used rather than IOS due to the nature of Android OS. Another fitness tracker sourced from Samsung will be used in order to compare the cheap to higher end security to compare the features of each device's security.

Data capture and tools:

The main goal is to capture BLE communication between the fitness trackers and their connected android smartphone while in day to day usage. BLE traffic will be collected during pairing, synchronisation, and normal activity. Tools like Wireshark and nRF Connect will be used to sniff and log packets and connection events. nRF connect will be my main tool used with a nRF52840 Dongle which will help identify services and characteristics exposed by each device.

Additional tools will be used from a bootable Kali Linux setup. This should offer a wide variety of tools, scripts and attack frameworks which are useful to create a MITM attack on the connections that are beyond simple passive capture.

Analysis and Planned Attacks:

Packets will be investigated to source any unencrypted values or patterns which would allow for the attacker to follow the user's device or interfere in the activity. This is done after the analysis of the captured traffic which will identify if the traffic is sent with encryption.

The aim is to see what a MITM attacker could obtain using available hardware and software. It will be done with a realistic attack scenario.

Evaluation and expected outputs:

Findings will be recorded with comparisons in encryption, strength of pairing, and the success and failure percentages of the MITM attacks on each device. The findings will also be used in order to compare the low cost to the higher end tracking devices to find out how device price and brand relate to BLE security in practice. After the completion of the MITM attacks, the recordings will be written into set of tables, short case studies for each device and the recommendations for improving BLE security.

1. IoT Device Security and BLE Communication

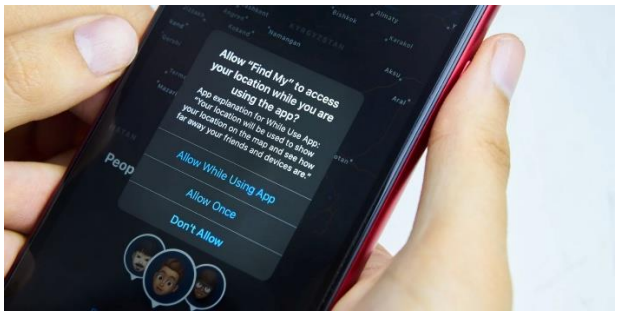
1.1 Definition and Types of IoT Devices

IoT stands for "**Internet of Things**" which are everyday devices that connect to the internet or other devices in order to send and receive data. These everyday devices include Fitness Trackers, camera, speakers and headphones. They are controlled with an application or web interface but they require a small processor and a stable network connection.

1.2 Fitness Trackers as IoT Devices

Fitness trackers are a great type of IoT devices because they are designed to be able to be used all day, contain sensitive health information and require a **wireless connection**. This make them a specific type of IoT devices as it monitors various of activity in which the data is synchronized to a phone and often to cloud services.

1.3 Device Permissions and Smartphone Apps



(Figure 1. Device Permissions)

When using a tracking device paired with its intended companion app, the **app will ask for permissions** such as Bluetooth, location, storage and notifications. These permissions are required to be accepted in order for the application to access specific device features or data that is needed in order to function properly or to provide a service. Due to the impact a permission can have on privacy and security, the system requires the user to manually approve access. If the permission is misused, it could potentially send data to attackers or third parties. Users often accept permissions without reading them because they want to use the application quickly or the application applies pressure to the user alerting them the application will not work as intended if the permission is denied.

1.4 Common Vulnerabilities in IoT Devices

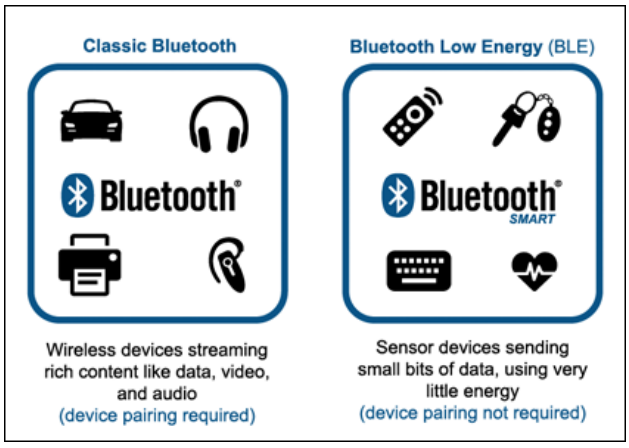
(Figure 2. Top 10 IoT Security Vulnerabilities)

Wearables rely on **three major layers**:

1. **The device** (Bluetooth)
2. **The mobile application** (Bluetooth pairing + Data display)
3. **The cloud** (Data storage + User accounts)

If a vulnerability is created in any layer, it can exposed sensitive user information such personal identity data or recorded logs.
Tracking devices are vulnerable as they combine the cloud, application and the device which all rely on each other to provide a working service. Lack of encryption can leak data during transmission and an attacker could exploit the device if weak passwords or outdated firmware exists. A flaw could lead to sensitive personal data exposure.

1.5 Introduction to Bluetooth Low Energy (BLE)



(Figure 3. Classic Bluetooth vs. BLE)

Bluetooth Low Energy (BLE) is a **low power wireless communication protocol** which is designed to allow the connection of small devices and is used in fitness trackers and smartwatches to smartphones and other central devices. The "little energy" is designed by operating in the 2.4 GHz ISM band which only uses a total of 40 RF channels, allowing this efficient and reliable communication. BLE is designed with three main goals:

- Low Energy Consumption
- Short Range communication
- Support for many small, low cost devices

These goals have made BLE the standard communication method for most modern fitness trackers.

1.6 BLE Security Features (pairing modes, encryption, privacy addresses)

BLE is designed with many security features which is aimed to protect wearable devices during its communication, including different **pairing methods**, **encryption** and privacy protections such as randomized **MAC addresses**. The pairing method determines how the devices connect to each other.

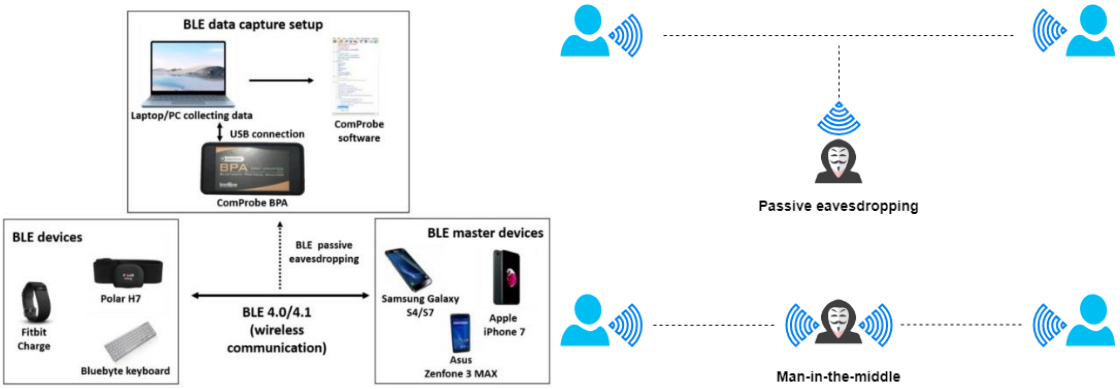
1.7 Comparison Example: BLE in Wireless Headphones vs Fitness Trackers

To understand BLE security importance I will compare it to a different device which also uses BLE as its form of communication to another device. It can be determined that although headphones protect audio that trackers are at a higher risk on the security aspect. Trackers will handle personal health for a long period of time and it's background sync which makes weaker BLE more serious than other devices like headphones.

2. Man-in-the-Middle (MITM) Attacks: Principles and Applications

2.1 Definition and General Concept of MITM Attacks

A Man In The Middle attack is an attack method to read, change or inject data into communication processes by avoiding detection. The attack comes from the name of being in the **middle of the two connections** that are communicating directly to each other.



(Figure 4. Passive Eavesdropping vs. MITM)

2.2 Typical MITM Attack Methods (ARP spoofing, TLS interception, rogue AP, BLE MITM etc.)

A common MITM attack would consist of setting up a rogue Wi-Fi access point so the victim can connect through the attacker's router. The main difference between a MITM attack method on web traffic and wireless such as BLE is that in encrypted web traffic the attacker may try TLS interception using a malicious certificate on the compromised device, while on BLE the attacker relays traffic between the two ends. In BLE the attack will prioritise the pairing stage because of the fast there is no user verification of keys. The attacker use two different connection, **device<->attacker<->phone**, possibly altering data values as they pass.

2.3 Conditions Required for Successful MITM (proximity, pairing mode, user behaviour)

- Within the range of the BLE connection
- Suitable hardware to listen and relay traffic
- If forced re-pairs are possible

User behavior that makes a MITM more successful:

- User accepts pairing prompts without hesitation
- User's device uses insecure pairing modes

2.4 Potential Impact on Fitness Tracker Data (eavesdropping, modification, tracking)

Fitness trackers can be impacted from eavesdropping attacks on the activity or health data if the there is unencryption or weak security. The attacker can modify the readings and track

when and where a device is active.

2.5 Example MITM Scenarios on Other BLE Devices (e.g. headphones, smart locks)

A different example on another device would be a MITM attack on wireless headphones. The attack could capture or alter media control messages or could downgrade security to listen to audio streams.

3. Practical Setup: Kali Linux Bootable USB and Security Tools

3.1 Overview of Kali Linux

Kali Linux is a **Linux distribution** which is downloaded containing a large amount of security and penetration testing tools which would not be an ideal desktop to be used for everyday use.. Kali Linux is very useful when it comes to network analysis, vulnerability assessment, and wireless testing.

3.2 Reasons for Choosing Kali Linux for This Project

I am choosing to use Kali Linux for this project as contains Bluetooth and traffic analysis tools which are installed and already configured.

3.3 Key Security Tools Used

Minimal tools from Kali Linux will be used for my research, focusing on the tools that can capture and inspect the BLE traffic or can simulate attacks.

3.3.1 Wireshark for BLE Packet Capture

Wireshark is a **protocol analyser** that can **capture and decode network packets** which also includes frames when used alongside a sniffer tool. I will be using Wireshark in my research to record the pairing and data transfer sessions between fitness trackers and the Android phone. I will also use it to identify if payloads are encrypted or are readable.

3.3.2 nRF Connect / nRF Sniffer for BLE Scanning and Analysis

I will also use **nRF Connect** to scan for nearby BLE devices to interact with them. It will also provide me with an analysis of how the tracker talks to the phone.

(Figure 5. nRF52840 Dongle)

3.3.3 Any Additional Tools (e.g. mitmproxy, hcitool, btlejack)

I will also be using other tools to better my outcome of getting a successful MITM attack on the BLE connection. These tools will be used for tasks such as command line Bluetooth utilities to manage adapters, or specialized BLE attack frameworks to attempt relaying.

3.4 Bootable USB and Persistent Storage

For my project I will run Kali Linux from a bootable USB so the testing environment will remain separate from my everyday operating system. I will configure it to remain persistent so it allows the saving of the drivers, captured logs and the configuration files.

3.4.1 What Is a Bootable USB Drive

The Bootable USB Drive is a USB stick installed with the Kali Linux OS. By doing this, I can start the OS directly with the USB attached to my desktop device. This will be useful for temporary environments and reduces the risks of accidently modifying my host system.

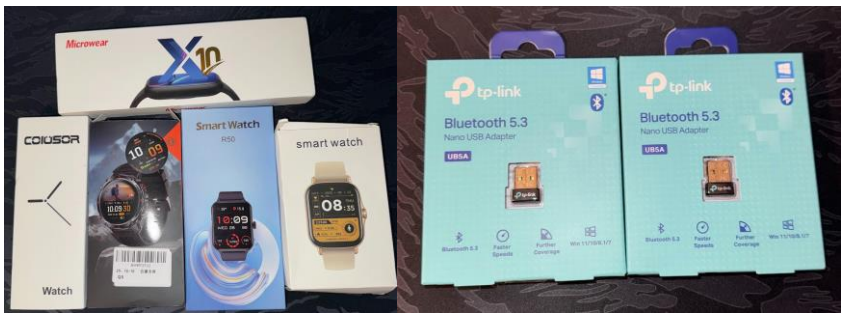
(Figure 6. USB used for bootable Kali Linux)

3.4.2 What Is Persistent Storage and Why It Is Useful

Persistent Storage will allow me to retain my Wireshark profiles, tool settings and the captured BLE traces across the many testing session that will take place. The persistent storage will keep the data after any shutdown of the Kali Linux Operating System.

3.5 Hardware Used (laptop, adapters, dongles)

The hardware I will be using will be an Android smartphone which will be for pairing and syncing. I have 5 trackers that have a different mobile application to them to get an accurate research done on the trackers, plus the trackers come from 3 different online shops including AliExpress, Shein and Temu. I will also include a higher end tracker to do a security comparison based on the product's price. I will be using a HP Laptop which will be running Kali Linux from the USB. I will be using an external BLE dongle that supports sniffing which will be used for traffic capture.



(Figure 7. Wearable Tracker Devices used & USB Adapters)

3.6 Network and Bluetooth Configuration for Sniffing

The external adapter will need to be configured as the interface for BLE scanning. Each test will consist of a repeated pairing and data sync processes. The tools will be running in the background which will save the captured logs with matching filenames which will show the device, data and the connectivity methods.

3.7 Ethical and Safety Considerations

An ethical measure will be in place while investigating BLE security that will not place any device or systems at risk. This research will be done on only the devices that I own, I will not attempt to intercept traffic that does not come from my own devices. The scanning will only be for the purpose of my research to test the trackers and capture relevant traffic.
The project will follow all legal and ethical guidelines which will be conducted in my home environment to avoid any unauthorized access to external systems. The data that I will source for this project will remain confidential and only used for the analysis for my research.

4. Reverse Engineering and Traffic Analysis in IoT Research

4.1 Role of Reverse Engineering in IoT Security

Reverse Engineering is used in IoT Security for understanding on the how closed source devices and their applications work without the full technical details available. Reverse Engineering gives us a great inside look into the firmware or mobile apps. By looking inside, researchers can see how the data is handled and if the security features such as encryption and authentication are implemented in the right way or if producers make claims for marketing purposes only.

4.2 Android App / APK Reverse Engineering

Reverse engineering plays a big role in my project by focusing on the android companion apps that connect to the fitness trackers. Reverse engineering allows for to inspect the configuration files and code paths which control BLE connections and the permissions. This is all done by unpacking the app files without modifying it for normal users.

4.2.1 Looking for BLE-Related Code, Permissions and Endpoints

The aim for my reverse engineering into the app's manifest and configuration files will be to check for Bluetooth and location permissions and find any hard coded endpoints or keys which would hopefully reveal how user data is sent to back end servers. This is on the focus on the code that sets up the Bluetooth connections.

4.3 Methods Used in Existing Wearable / BLE Studies

In previous studies they experiment with attack tools or modified apps to test if encryption or authentication can be bypassed. The study would end with a report on which devices or models were more or less resistant. Static analysis is done of the apps or the firmware with controlled traffic captures while the device is in every day usage.

4.4 How This Project's Method Fits into the Existing Research

I will be using previous research for a general pattern but will narrow my work to a small set of low cost and a higher end tracker. A comparison will be conducted under the same conditions to identify the difference between the security of the two different cost trackers. By combining reverse engineering of the tracker's app with BLE traffic captures and MITM attacks, my aim is to show the strength of the security users receive with the device for their everyday use and if cheaper devices actually don't spend resources on the security aspect.

Comparative Approaches and Research Gaps

The existing studies on wearable and BLE security tests a small set of most common brand of devices in depth. Many papers combine the static analysis of apps or firmware with traffic captures and one common type of attack such as basic sniffing to get the research on user data protection of these fitness trackers. The studies often just focus on the brands everyone knows that are used by hundreds of million users but often don't compare the low cost device under the same conditions.

I find this to have many gaps, that is why I will be using the cheap alternatives which just have a few hundred purchases with no major branding or name. To this I will also be doing a side by side comparison of multiple devices using repeatable BLE scenarios. The studies also just look at either app behaviors or the wireless traffic but they don't combine their analysis with reverse engineering, detailed BLE captures and a MITM attack in one study. My project stands out within the research gap because I will evaluate how realistic certain attacks are for an attacker with beginner knowledge.

How to stay secure and protected from these attacks (Mitigation)

When it comes to personal information it is very important that it remains personal. The most important step for security is to choose and configure fitness trackers that actually use the stronger Bluetooth security options. MITM attacks and eavesdropping are a lot harder on newer devices which support securing pairing modes, encrypted connections and randomised Bluetooth addresses. Another step to being more secure is to update the device firmware regularly and apps up to date. Users should also consider pairing or syncing their devices in a populated public area. Users should also disable Bluetooth when not in use and remove old pairings or devices they no longer have in use.

Mitigation from manufacturer side is to enable LE Secure Connections by default and ensure all sensitive GATT characteristics are just accessible over encrypted and authenticated connections. Regular security testing should be done to fix weaknesses and give users more control over the permissions and what data they want to collected and shared.

Conclusion

The findings for my project will show the inconsistency across multiple devices in the Bluetooth Low Energy (BLE) security in fitness trackers. It will prove that cheaper trackers have a strict budget which affects the security aspect in the device. Comparing the results to the higher end tracker will show that the higher end device provides better use of secure pairing, encryption and address randomisation while the cheaper devices are more likely going to have a low security flow that is easy to observe and interfere with. Although I will be following a pattern, I have found a gap in the research on the topic of wearables that will extend the results by doing multiple different analysis methods and doing a comparison between low cost to high end devices in the same tests. This research will show how design choices and the price of the device changes the security and protection the user will get in everyday usage.

Several recommendations can be made to manufacturers such as enable strong BLE security features by default, make sure there is a strong secure connection during pairing and require mandatory encryption. Privacy settings in the apps should be provided clearly and the apps should have regular firmware updates to allow patches for vulnerabilities.

Users should also follow recommendations to remain secure. Users should choose a tracker from a known brand that is has documented their security practices and keeping apps and firmware updated.

In conclusion, my project sets out to examine the strength of the security fitness trackers have while using BLE, with a higher focus on the cheaper alternatives. I want to give out and understanding on what an attacker with realistic tools could do or eavesdrop on. My results from comparing low cost to higher end should show that BLE standard has strong security options and a high level of protection on users, but it's on the manufacturing side to implement and configure good security. Also from the comparison, it will show there is still a lot of improving to be done in budget devices and that better configurations and the use of security features are all important steps to move towards more secure and higher privacy wearables.

Sources

Nordic Semiconductor (n/a) Setting up nRF Sniffer for Bluetooth LE. Nordic Developer Academy. Available at: https://academy.nordicsemi.com/courses/bluetooth-low-energy-fundamentals/lessons/lesson-6-bluetooth-le-sniffer/topic/nrf-sniffer-for-bluetooth-le/ (Accessed: December 2025).

NovelBits (n/a) Master BLE Advertising Packet Analysis: nRF Sniffer & Wireshark. Available at: https://novelbits.io/nordic-ble-sniffer-guide-using-nrf52840-wireshark/ (Accessed: December 2025).

NebraskaCERT (2016) Security of Bluetooth Network Data Traffic. CSF-Jun2016.pdf. NebraskaCERT. Available at: https://www.nebraskacert.org/CSF/CSF-Jun2016.pdf (Accessed: December 2025).

Liu, X. et al. (2025) 'The newer, the more secure? Standards-compliant Bluetooth Low Energy man-in-the-middle attacks on fitness trackers', Cybersecurity, 8(1), Article 15. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC11945526/ (Accessed: December 2025).

Wu, X., Liu, Y. and Zhang, Z. (2024) Intercepting Bluetooth Traffic from Wearable Health Devices. In: Proceedings of the SafeThings 2024 Workshop. Available at: https://safe-things-2024.github.io/accepted_papers/safethings24-final11.pdf (Accessed: December 2025).

O'Neill, P. (2018) Smartwatch Vulnerability Analysis: Focusing on Bluetooth Low Energy. MSc dissertation. Trinity College Dublin. Available at: https://publications.scss.tcd.ie/theses/diss/2018/TCD-SCSS-DISSERTATION-2018-015.pdf (Accessed: December 2025).

Haataja, K. and Toivanen, P. (2021) 'A survey on Bluetooth Low Energy security and privacy', Computer Networks, 194, 108119. Available at: https://www.sciencedirect.com/science/article/pii/S1389128621005697 (Accessed: December 2025).

Gabriele, D. et al. (2024) 'Wearable activity trackers: A survey on utility, privacy, and security', ACM Computing Surveys, 56(4), pp. 1–42. Available at: https://dl.acm.org/doi/10.1145/3645091 (Accessed: December 2025).

eInfochips (2025) Bluetooth Low Energy (BLE) Security and Privacy for IoT. eInfochips Blog. Available at: https://www.einfochips.com/blog/bluetooth-low-energy-ble-security-and-privacy-for-iot/ (Accessed: December 2025).

Images Used:

Cardinal Peak (n.d.) Top 10 IoT security vulnerabilities. Cardinal Peak Blog. Available at: https://www.cardinalpeak.com/blog/top-10-iot-security-vulnerabilities (Accessed: December 2025).

Onset Computer Corporation (n.d.) Bluetooth Low Energy: A closer look. Available at: https://www.onsetcomp.com/resources/informational-pages/bluetooth-low-energy-closer-look (Accessed: December 2025).

MakeUseOf (2022) How do iPhone and iPad app permissions work? MakeUseOf. Available at: https://www.makeuseof.com/iphone-ipad-permissions-how-do-they-work/ (Accessed: December 2025).

Pérez, A. et al. (2022) 'On the security of Bluetooth Low Energy in two consumer wearable heart rate monitors/sensing devices', Sensors, 22(3), Article 1072. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC8839540/ (Accessed: December 2025).

Nordic Semiconductor (n.d.) Setting up nRF Sniffer for Bluetooth LE. Nordic Developer Academy. Available at: https://academy.nordicsemi.com/courses/bluetooth-low-energy-fundamentals/lessons/lesson-6-bluetooth-le-sniffer/topic/nrf-sniffer-for-bluetooth-le/ (Accessed: December 2025).

eInfochips (2025) Bluetooth Low Energy (BLE) Security and Privacy for IoT. eInfochips Blog. Available at: https://www.einfochips.com/blog/bluetooth-low-energy-ble-security-and-privacy-for-iot/ (Accessed: December 2025).

Figure Table