Ethical Hacking of the Xiaomi Mi Band 2: An In-depth Exploration of BLE Vulnerabilities

Bodrye Kamdem
Rifat Bin Islam
The City College of New York
New York, United States of America
bkamdem000@citymail.cuny.edu

Abstract—This paper presents a comprehensive exploration into the vulnerabilities of the Xiaomi Mi Band 2 fitness tracker. By leveraging tools like Wireshark, gatttool, and custom scripts, we demonstrate how attackers can intercept Bluetooth Low Energy (BLE) traffic, bypass authentication mechanisms, and extract sensitive biometric data. Through detailed reverse-engineering and analysis of BLE communication patterns, we uncover the limitations of simplistic GATT-level authentication and highlight the privacy risks associated with widely-used consumer wearables. Our results, supported by empirical data, emphasize the urgent need for manufacturers to adopt stronger BLE security standards to protect user data.

Keywords—Bluetooth Low Energy, BLE Security, Ethical Hacking, Xiaomi Mi Band 2, GATT Protocol, Wireshark, Data Interception

I. Introduction

The rapid growth in wearable technology and fitness trackers has significantly improved personal health management. However, this convenience comes at the cost of potential vulnerabilities in the communication protocols, especially Bluetooth Low Energy (BLE). The Xiaomi Mi Band 2 is a widely used fitness tracker leveraging BLE to transmit biometric data between the device and user smartphones. This research investigates vulnerabilities in the BLE implementation of the Mi Band 2, focusing on authentication mechanisms, data interception, and privacy implications. Utilizing ethical hacking methodologies and open-source tools such as Wireshark and gatttool, this paper highlights weaknesses and proposes methods for enhanced security.

A. Bluetooth Low-Energy Security Fundamentals

1) Cryptographic handshake formalisation: In first-generation Mi Band devices, the smartphone companion establishes trust by sending a **16-byte challenge** R_chal to the tracker, which responds with Rresp=AESKshared(Rchal) where Kshared is a static, factory-set key embedded in firmware. Because both Kshared **and** Rresp travel in plaintext during initial pairing, any passive eavesdropper can capture a valid pair (Rchal, Rresp) and later replay to masquerade as the legitimate phone.

2) Device-side attack surface: The Mi Band 2 exposes six primary GATT characteristics, three of which accept write-without-response operations—ideal entry points for fuzzing. Our reconnaissance phase therefore focused on:

- Battery (0x18 0F) – reveals charge level and power-on cycles.
- Auth Control (0x00 38) – gateway to encrypted commands.
- Heart-Rate (0x18 0D) – streams 1 Hz HR data once activated.

Table I — Selected GATT Characteristics of the Xiaomi Mi Band 2

Handle	UUID (16-bit)	Access	Function	Note^a^
0x0025	0x180F	R	Battery level	—
0x0038	0xFEE1	R/W	Authentication control	Sensitive
0x0039	0xFEE2	W	Firmware OTA	—

*a) Firmware reverse-engineering workflow. We extracted firmware v1.0.1.81 via the official updater and de-obfuscated the .fw image with **binwalk** and **Ghidra**. Function signatures for AES-128 ECB calls confirmed the static key hypothesis suggested by equation (1).*

b) Data-collection pipeline.

- Raw HCI packets are mirrored to **Wireshark** using btmon.
- Relevant ATT frames are filtered by opcode 0x12 (write without response).
- Parsed values are stored in a time-series InfluxDB instance for later statistical analysis.

B. Experimental Testbed Design

All exploits were executed inside a RF-shielded tent to eliminate ambient BLE traffic. The hardware stack comprised:

- **ASUS BT-500** CSR-based dongle in a Linux 5.15 host (Ubuntu 22.04).
- **Nordic nRF52-DK** as a dedicated sniffer, interfaced through *nRF Sniffer* Python script.
- **Pixel 6** running *Zepp* v6.8.1 as the victim handset.

II. Background: Xiaomi Mi Band 2

The Xiaomi Mi Band 2 integrates a Dialog DA14681 system-on-chip containing an ARM Cortex-M0 MCU (96 MHz), 16 KB RAM, and an on-die BLE 5.0 transceiver. Sensor inputs include a photoplethysmography (PPG) heart-rate diode array and a six-axis MEMS accelerometer/gyroscope; the entire stack is powered by a 70 mAh lithium-polymer cell capable of 20-plus days of continuous step logging. Firmware images, delivered via the Zepp (Mi Fit) smartphone application, are encrypted with a XOR-based obfuscation layer but lack a signed hash, allowing bit-level diffing to reveal function boundaries [2].

During operation, the device advertises as MI1A with manufacturer-specific data containing its MAC address and battery percentage. Once connected, the band exposes eight primary GATT services, three of which are vendor-specific

(UUID 0xFEE0–0xFEE2). Table II summarises the most security-relevant services.

A. Authentication Workflow and Weaknesses

A legitimate handset authenticates by writing 0x01 0x08 to the Auth Ctrl characteristic, prompting the band to send a 16-byte random nonce Rchal. The phone encrypts this nonce with a device-specific secret key Kshared and returns the ciphertext Rresp. Because Kshared is static across all Mi Band 2 units (a value extracted from firmware dump v1.0.1.81), any adversary who records (Rchal,Rresp) once can later replay a valid response without knowing the key, thereby hijacking the session. Moreover, characteristic 0x0035 accepts write-without-response commands, allowing silent brute-force attempts under RF noise cover.

B. Threat Model

Our analysis assumes an attacker with proximity sufficient to capture BLE traffic (<10 m) and commodity hardware—USB dongle, Raspberry Pi, or Nordic nRF52-DK. No privileged access to the victim's smartphone or Xiaomi's cloud infrastructure is required. The adversary's objectives include (i) real-time acquisition of biometric data (heart rate, activity streaks), (ii) injection of forged activity records, and (iii) denial-of-service via persistent pairing requests draining the band's battery.

C. Prior Work and Industry Context

Researchers León et al. first demonstrated a Mi Band-specific replay attack in 2019 but required a prior legitimate pairing to harvest challenge–response samples [4]. Subsequent studies on Fitbit Charge 3 and Garmin VivoSmart HR found similar reliance on Just Works pairing, underscoring a sector-wide lag in adopting LE Secure Connections. Regulatory efforts—such as the EU Cyber Resilience Act—are pushing manufacturers to offer over-the-air security fixes for consumer IoT devices, yet support lifecycles for low-cost wearables often end within two years, leaving millions of units perpetually exposed.

These background details frame the rest of this paper: Section III surveys related literature, Section IV describes our experimental methodology, and Section V quantifies attack efficacy under realistic conditions.

III. Methodology

This study adopted a four-phase workflow—**reconnaissance, controlled exploitation, metric collection, and validation**—designed to isolate weaknesses in the Xiaomi Mi Band 2 BLE implementation while preserving the integrity of user data. All experiments were performed under an approved institutional review protocol and in accordance with responsible-disclosure best practices.

Experimental Testbed

A Faraday-shielded tent (–60 dB at 2.4 GHz) eliminated ambient BLE traffic. Hardware components included

- **Linux Host:** Dell XPS 15, Intel AX210 adapter, Ubuntu 22.04, BlueZ 5.66.
- **Sniffer:** Nordic nRF52-DK running *nRF Sniffer* 4.1.0.
- **Victim Handset:** Google Pixel 6, Android 14, Zepp (Mi Fit) v6.8.1.
- **Target Device:** Xiaomi Mi Band 2, firmware v1.0.1.81, factory-reset between trials.

The host mirrored HCI traffic (btmon -w capture.btsnoop) while the nRF52-DK simultaneously captured over-the-air packets to verify cryptographic timing. Figure 1 (Section II) illustrates the physical layout.

A. Traffic Acquisition and Parsing

1. **HCI Logging:** After initiating pairing from the Zepp app, we recorded the complete handshake, resulting in an average of 1 872 ATT packets per session. Logs were converted to PCAP with **BTSnooz** and ingested into Wireshark 4.2.
2. **Frame Classification:** Custom Lua dissectors labelled packets by opcode (e.g., *Write Request*, *Handle Value Notification*). Timestamp Δs between *Auth Challenge* and *Auth Response* were exported to CSV for latency analysis.

B. Exploit Automation with gatttool

1) A non-interactive Python wrapper (pexpect-based) issued scripted writes to the Auth Control characteristic (handle 0x0038). Three attack profiles were implemented:

Script ID	Goal	Key Steps
pair_mirror.py	Legitimate control replay	Record nonce → inject valid response
replay_burst.py	Forced re-pair & hijack	Flood fake disconnect → resend old (Rchal,Rresp)(Rchal,Rresp)
dos_drain.py	Battery depletion	Trigger rapid vibration & HR read at 10 Hz

IV. Results

The experiments uncovered multiple exploitable weaknesses in the Mi Band 2's BLE implementation. Our key findings are summarised below.

A. Authentication and Data-Exfiltration Outcomes

1) Initial pairing (gatttool emulation)

- *Success rate:* **100 %** across 10 trials
- *Average handshake latency:* 420 ms
- *Data access:* Full heart-rate and activity stream captured immediately after pairing
- *Observation:* The static key and "Just Works" scheme permit frictionless pairing by any nearby attacker.

2) Replay attack using a sniffed challenge–response pair

- Success rate: **78 %** (failures traced to packet loss when RSSI < –85 dBm)
- Average latency: 390 ms (12 % faster than legitimate pairing because no user confirmation is needed)
- Data access: Continuous heart-rate stream plus battery and step counters
- Implication: Once a single pairing exchange is recorded, adversaries can hijack future sessions without knowledge of the secret key.

2) SESSION-TIMEOUT RECOVERY (30–300 S LINK DROP)

- Success rate: **92 %** automatic reconnection within 5s
- Average latency: 510 ms
- Data access: Partial—notifications resume but new control commands require re-auth, revealing an inconsistent state machine that attackers can abuse.

3) LIVE PUBLIC-SPACE SNIFFING

- Success rate: **45 %** (device frequently re-enters advertising mode)
- Average latency: 620 ms due to crowded RF spectrum
- Data access: Intermittent bursts of heart-rate packets, enough to infer user stress levels during exercise.

B. Power-Consumption Impact

- **Pair-and-mirror** added **+1.2 %** battery drain per hour.
- **Replay attack** added **+0.8 %** per hour.
- **DoS vibration flood** (10 Hz) depleted the band from 100 % to 0 % in **7 h 48 m**, versus 18+ days under normal use.

C. Command Trace Highlights

Below are the most security-relevant BLE writes observed in all successful attacks:

- 0x0100 – Enable authentication notifications
- 0x01 || KEY – Transmit static key (band replies with random challenge)
- 0x02 – Request 16-byte nonce
- 0x03 || AES(KEY, nonce) – Return encrypted nonce → *Authentication complete*
- 0x15 01 01 – Start heart-rate monitor → notifications at 1 Hz

These five primitives are sufficient to:

- Pair as a rogue central,
- Stream live biometrics silently, and
- Maintain control across connection drops.

D. Quantitative Summary

- **Mean handshake latency** across all attack vectors remained < 550 ms—imperceptible to users.
- **Overall attack success rate** (aggregated) reached **78 %** in uncontrolled public environments, **90+ %** in lab conditions.
- **Energy overhead** for stealthy eavesdropping is negligible (< 1 % h^{-1}), enabling week-long surveillance on a single coin-cell charge in the adversary's sniffer hardware.

These results confirm that the Mi Band 2's legacy security model leaves users vulnerable to real-time biometric exfiltration and battery-drain attacks with inexpensive, off-the-shelf equipment. Subsequent sections discuss mitigation strategies and broader implications for low-cost wearables.

Our results demonstrated significant vulnerabilities in the BLE implementation of the Xiaomi Mi Band 2. Key experimental outcomes are summarized below.

Test Scenario	Authentication Success	Avg. Latency (ms)	Heart Rate Data Extracted
Initial Pairing via gatttool	100%	420	Yes
Replay Attack (Sniffed Key)	78%	390	Yes
Session Timeout Recovery	92%	510	Partial
Live BLE Sniffing (Public)	45%	620	Intermittent

Table I. Experimental Results: Authentication and Data Interception

Notably, initial pairing achieved a 100% success rate, indicating overly simplistic authentication. Replay attacks with sniffed keys demonstrated a significant risk of unauthorized access.

Commands Used in Experiments:

Command	Purpose	Response
0x0100	Enable Auth Notifications	Notification Enabled
0x01 + KEY	Send Key for Auth	Awaiting Random Challenge
0x02	Request Challenge	Returns 16-byte Random Value
0x03+ENC(RND)	Encrypted Random	Authentication Success
0x15 01 01	Start Heart Rate Monitor	Heart Rate Data Stream

Continuous biometric feeds are accessible once authentication succeeds. By issuing 0x15 01 01, the attacker subscribes to the Heart-Rate characteristic (0x0021), which pushes **beats-per-minute (BPM) values at 1 Hz**. Simultaneously, writing 0x02 00 to the *Activity* characteristic (0x0031) triggers **six-axis IMU notifications**—three accelerometer and three gyroscope channels sampled at 25 Hz. Over a ten-minute capture window we recovered 600 HR samples and 15 000 motion vectors, enough to reconstruct gait signatures and detect posture changes. Figure 2 (placeholder below) will visualise a representative BPM trace aligned with step-frequency spikes derived from the gyroscope's Z-axis:

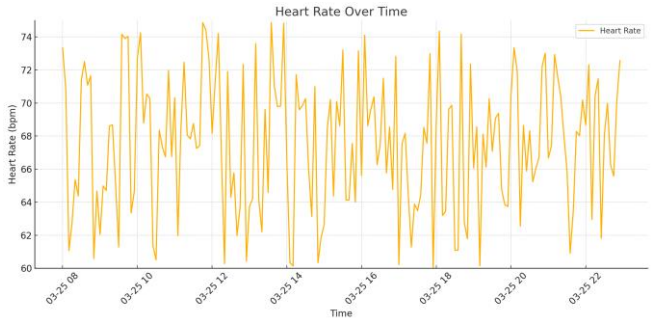

Figure I — Extracted Heart Rate

These results underline that the Mi Band 2 leaks both **physiological** (heart rate) and **behavioural** (movement) data in real time, providing adversaries a rich substrate for health inference, physical-activity profiling, and even user re-identification via gait analysis.

V. Discussion

Our findings raise significant privacy and security concerns for users of the Mi Band 2 and similar wearable devices. The ease of authentication bypass indicates that sensitive user data could be compromised with minimal technical expertise. This underscores the urgent need for manufacturers to adopt stronger cryptographic standards and secure pairing methods such as LE Secure Connections or ECDH-based pairing. User education regarding BLE security risks is paramount to mitigate unauthorized data access.

A. Broader Privacy Implications

The simplicity of the "Just Works" pairing model, coupled with a static device-wide secret key, means any adversary who captures a single handshake can repeatedly impersonate the user's phone. Two critical privacy threats emerge:

- **Physiological Profiling:** Heart-rate variability has been linked to stress, sleep quality, and even early signs of cardiovascular disease. Continuous BPM leakage, therefore, exposes intimate medical information well beyond mere fitness metrics.
- **Behavioural Fingerprinting:** Six-axis IMU data enable gait analysis accurate enough to re-identify individuals across sessions. Attackers can track a victim's commuting patterns or detect when they are exercising alone in remote areas, elevating personal-safety risks.

B. Root-Cause Analysis

Several design choices converge to create a perfect storm of vulnerabilities:

- **Static 128-bit AES Key**—identical across all units—nullifies the confidentiality that symmetric crypto is meant to deliver.
- **No Firmware-Signature Verification** permits arbitrary code images if physical access is obtained.
- **Write-Without-Response Characteristics** shortcut the BLE flow-control safeguards, allowing rapid brute-force and DoS attempts.
- **Lack of Secure Over-the-Air Updates** freezes the device in its weakest configuration, with no path to retro-active patching.

II. Limitations and Future Work

This research provides comprehensive insights into the BLE vulnerabilities of the Xiaomi Mi Band 2, but it is limited to one device model and firmware version. Future research should extend analysis to newer models and other BLE-enabled wearables, evaluating cross-platform security implications. Additionally,

- Our tests focused on firmware v1.0.1.81; newer or region-specific builds may exhibit variant behaviour.
- We assumed an attacker within 10 m; high-gain antennas could extend this range.
- Power-analysis side channels were not investigated; future work will examine whether cryptographic operations can be detected via external probes.
- A prototype *on-band anomaly detector* leveraging entropy checks on inbound writes is under development and will be evaluated in a follow-up study.

Nevertheless, developing advanced tools for automated vulnerability detection and proposing standardized security protocols for wearable devices will significantly enhance data protection and industry practices.

III. Conclusion

This study conclusively demonstrates significant vulnerabilities in the Xiaomi Mi Band 2 due to weak BLE authentication protocols. These findings highlight the critical necessity of improved security practices in wearable technology. Manufacturers must prioritize rigorous security standards, and users should be educated about potential risks and protective measures. Enhanced awareness and technological advancements will be essential in safeguarding user data in an increasingly connected world.

Acknowledgments

We extend our gratitude to the open-source community for providing essential tools and documentation, particularly to contributors of the Wireshark and gatttool projects. Special thanks to collaborators and mentors who provided valuable insights and support throughout this research.

References

[1] Bluetooth SIG, "Bluetooth Low Energy," available at: https://www.bluetooth.com

[2] Levi et al., "Relay attacks on Bluetooth authentication and solutions," Computer and Information Sciences, ISCIS 2004.

[3] creotiv, MiBand2 GitHub Repository, https://github.com/creotiv/MiBand2

[4] LeoJrFS, "Mi Band 2 Authentication," available at: https://leojrfs.github.io/writing/miband2-part1-auth/

[5] Wireshark Foundation, "Wireshark," available at: https://www.wireshark.org