PhD school: From Eavesdropping to Exploitation: Exposing Vulnerabilities in BLE-Enabled Wearable Medical Devices

Mohammad Alhussan
University College London
mohammad.alhussan.23@ucl.ac.uk

Francesca Boem
University College London
f.boem@ucl.ac.uk

Sara S. Ghoreishizadeh
University College London
s.ghoreishizadeh@ucl.ac.uk

Anna Maria Mandalari
University College London
a.mandalari@ucl.ac.uk

Abstract

This research showcases the potential vulnerabilities in some wearable medical devices that use Bluetooth Low Energy (BLE) for communication, focusing on the risks of Man-in-the-Middle (MITM) attacks, sabotaging and data manipulation attacks. We show how these attacks can compromise not only the confidentiality and integrity of potentially sensitive medical data transmitted by wearable medical devices, but also patients' privacy and safety as well as sensors' reliability.

CCS Concepts

• **Security and privacy** → **Privacy-preserving protocols**; **Penetration testing**; **Vulnerability scanners**; **Denial-of-service attacks**; *Hash functions and message authentication codes*; **Usability in security and privacy**; • **Computer systems organization** → **Real-time operating systems**; • **Applied computing** → **Health care information systems**.

Keywords

BLE, IoMT, MITM, eavesdropping, cybersecurity, ECD, BPM

1 Introduction

In this research, we shed light on some BLE vulnerabilities associated with various present-day wearable medical devices that use both generic and proprietary protocols. We also perform detailed penetration testings (i.e. passive and active MITM attacks) on four wearable medical devices (i.e. SnapECG Electrocardiogram (ECG), OXYLINK and SleepO2 1400 Oximeters, and Wellue BP2A 2031 Blood Pressure Monitor (BPM)) using relatively simple and low-cost pen-testing tools. This research emphasizes the need to avoid relying exclusively on a single wireless communication protocol (i.e. BLE); instead, adopt a multilayered cybersecure communication system to enhance overall security and reliability. In particular, this work answers the following research questions (RQ):

RQ1: *How effective are modern penetration testing techniques in identifying vulnerabilities in BLE-enabled wearable medical devices?* To answer this question we perform explicit penetration testings on various contemporary BLE-enabled wearable medical devices.

RQ2: *What are the advantages of using a multilayered cybersecure communication system over relying solely on a single wireless protocol like BLE for enhancing the security and reliability of wearable medical devices?* We highlight in this research that relying on a single layer of communication represents a significant vulnerability.

2 Background

The majority of wearable medical devices nowadays utilizes BLE for connectivity due to its efficiency, low power consumption and compatibility with a broad range devices. Such utilization not only enables the real-time monitoring and analysis of data through compatible mobile applications, but also, allows to transmit control signals to wearable medical devices wirelessly. Similar to the classic Bluetooth, the fundamental components of the BLE protocol stack comprise the Controller layers, the Host layers, and the Application layer [1]. However, unlike the classic Bluetooth that operates on 79 channels, BLE operates on 40 channels in the 2.4 GHz Industrial, Scientific, and Medical (ISM) band, each with a 2 MHz bandwidth, which helps it maintain low power consumption while enabling efficient and periodic data transfers [2]. In general, BLE packets are categorized into two distinct classifications: Data packet and Advertising packet. Each of these packets starts with a preamble of one byte, succeeded by a 4-byte access address utilized for the identification of radio communication within the physical layer. Subsequently, a Protocol Data Unit (PDU) ranging from 2 to 257 bytes follows. The advertising channel PDU comprises a 2-byte advertising packet type header along with a payload of 0 to 37 bytes. Conversely, a data channel PDU is characterized by a 2-byte data channel header, accompanied by a payload ranging from 0 to 255 bytes. The payload within the data channel packet commences with a 4-byte L2CAP header and concludes with a 4-byte Message Integrity Check (MIC). Lastly, each packet ends with a 3-byte Cyclic Redundancy Check (CRC) [1].

Like all forms of wireless communication technology, BLE is susceptible to several cybersecurity vulnerabilities such as Man in the Middle (MITM), Code Injection, Hijacking, Denial of Service (DoS), Spoofing, and Eavesdropping. In fact, a successful MITM attack could lead to manipulating operational data or falsifying sensors readings to initiate False Positive (FP) or False Negative (FN) attacks. This will eventually lead to gaining full access and control of the wearable medical devices' systems.

3 Literature Review

Numerous studies in the literature [3–22] address BLE and other wireless communication vulnerabilities and threats, examining their impact on wearable and implantable medical devices, as well as general IoMT applications. However, relatively few have specifically explored the broader implications for patient safety and data protection, along with the unique security challenges faced by wearable medical devices utilizing BLE technology. Tal Melamed [23] hooks

into Smart-watch sports counter and modifies the data sent from the smart watch into the device using GATTacker tool. He also uses BtleJuice tool to execute replay and on-the-fly data modifications. On the other hand, Zhang *et al.* [24] show that the BLE programming framework of an initiator (e.g. an Android mobile) must properly handle Secure Connections Only (SCO) initiation, status management, error handling, and bond management; otherwise severe flaws can be exploited to perform downgrade attacks, forcing the BLE pairing protocols to run in an insecure mode without user's awareness. Yet, no pen-testings have been performed in the literature on CGMs, Oximeters or ECGs. In addition, Chunxiao Li *et al.* [25] demonstrate security attacks conducted in the laboratory on glucose monitoring and insulin delivery systems available on the market and proposes defenses against such attacks. However, that research is confined to older versions of CGMs and insulin pumps that communicate using the 915 MHz frequency rather than BLE and does not include penetration testings of other wearable medical devices. Furthermore, Guo *et al.* [26] propose a method for handling Battery Exhaustion Attacks that involves making suspicious nodes periodically switch their connections to the neighbors of their connected nodes. When a node is identified as malicious, it is blacklisted to prevent future attacks. However, no penetration testings are carried out on real commercial wearable medical devices. Additionally, no MITM attacks are performed.

4 Threat Model and Definitions

In our threat model we assume that our system is composed of four main entities: *(i) The victim*, which is a patient with blood pressure lability (hypertension or hypotension), a patient with heart arrhythmia (tachycardia or bradycardia), a patient with hypoxemia (low oxygen levels) and relies on wearable medical devices to function or live a healthy life [27]. *(ii) The operational structure* is composed of an open-loop system consisting of ECGs, Oximeters and BPMs *(iii) The communication*, which is standard BLE 4.0 or BLE 5.0. *(iv) The potential adversary*, which is an individual or organization within the BLE operational range (i.e. 100m) performing malicious passive (i.e. Eavesdropping) and/or active cyberattacks (i.e. MITM) on wearable medical devices.

In BLE, **MITM** attacks can occur during the pairing process or during established sessions between devices. An attacker can place himself between the peripheral device and the central, and accordingly intercept the communication to steal encryption keys or manipulate data being exchanged (Figure 1 (A)). BLE uses encryption during the pairing process, but vulnerabilities can be exploited if it is not properly implemented or if weaker pairing mechanisms are used [28]. On the other hand, **Eavesdropping** on BLE is the process by which unauthorized individuals intercept and decode BLE communications, exploiting the unencrypted or poorly encrypted transmission of data between devices (Figure 1 (B)). This security breach can compromise personal data or control signals [29].

5 Experimental Setup

We demonstrate the capabilities of the "Mirage" tool in intercepting and modifying data transmitted between the devices and their associated apps. A virtual Machine with Kali Linux in a controlled

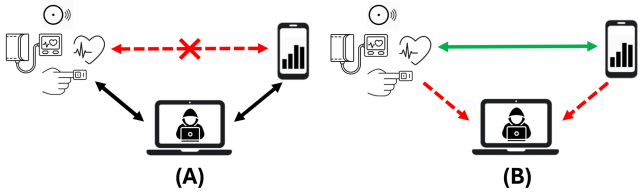

Figure 1: (A) MITM Attack Structure (B) Sniffing Attack Structure

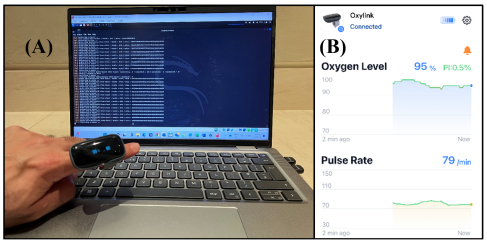

Figure 2: (A) MITM Attack on Oximeter (B) App Interpreted Results.

environment is used to perform our experiments. Our experimental setup consists of:

Wearable Medical Devices: we use a variety of wearable medical devices offered by well-known manufacturers, such as Electrocardiograms (ECG) (e.g. SnapECG), Oximeters (e.g. Oxylink and SleepO2 1400), and Blood Pressure Monitors (BPM) (e.g. Wellue BPM).

Smart Phones: two smart phones are utilized in our experiments (i.e. iPhone 13 Pro and Google Pixel 3).

Pen-testing Tools: we use two ORICO Wireless USB Bluetooth 4.0 Adapter USB Dongles (Transmitter-Receiver) and a sophisticated pen-testing tool "Mirage" [30, 31] for conducting the passive and active MITM attacks.

Data Visualization Tools: we use a server with Kali Linux [1] installed to perform the passive and active MITM attacks, show and analyze the intercepted data packets, and demonstrate the impact of the attacks on the integrity and confidentiality of medical data (Figure 2).

6 Conclusion

The integration of wearable medical devices into the IoMT revolutionizes healthcare by enhancing continuous monitoring and patient management. However, our research reveals significant cybersecurity vulnerabilities and threats associated with the BLE utilization in these devices. Penetration testings executed on various devices, including ECGs, Oximeters and BPMs highlight critical security gaps that could jeopardize patient safety and data integrity. Moreover, the findings underscore the urgent need for robust cybersecurity measures beyond single protocol reliance. A multilayered approach, incorporating strong encryption, secure authentication,

[1] https://www.kali.org

and continuous monitoring, is essential to protect against potential cyberattacks.

This research acts as a catalyst for the healthcare sector to prioritize cybersecurity in the development and deployment of wearable medical devices, protecting patient confidentiality and well-being in an increasingly interconnected healthcare environment.

Future work includes the development and implementation of multilayered cybersecurity systems for wearable medical devices, incorporating advanced multi-authentication techniques and redundancy measures. By integrating multiple layers of security, we aim to enhance the resilience of these devices against cyber threats. **Note:** We do not cause any real threats in our experiments. All experiments are contained within our own testbed.

References

[1] Arup Barua, Md Abdullah Al Alamin, Md. Shohrab Hossain, and Ekram Hossain. Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey. *IEEE Open Journal of the Communications Society*, 3:251–281, 2022.

[2] Bluetooth SIG. Bluetooth technology overview, 2024. Accessed: Aug. 5, 2024.

[3] G. Kwon, J. Kim, J. Noh, and S. Cho. Bluetooth low energy security vulnerability and improvement method. In *Proceedings of the International Conference on Consumer Electronics Asia (ICCE-Asia)*, pages 1–4, Seoul, South Korea, October 2016.

[4] J. Uher, R. G. Mennecke, and B. S. Farroha. Denial of sleep attacks in bluetooth low energy wireless sensor networks. In *Proceedings of the IEEE Military Communications Conference (MILCOM)*, pages 1231–1236, Baltimore, MD, USA, November 2016.

[5] S. Jasek. Gattacking bluetooth smart devices. In *Proceedings of the Black Hat USA Conference*, pages 1–15, July/August 2016.

[6] M. Yaseen et al. Marc: A novel framework for detecting mitm attacks in ehealthcare ble systems. *Journal of Medical Systems*, 43(11):324, 2019.

[7] H. Wen, Z. Lin, and Y. Zhang. Firmxray: Detecting bluetooth link layer vulnerabilities from bare-metal firmware. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 167–180, New York, NY, USA, November 2020.

[8] A. H. Omre and S. Keeping. Bluetooth low energy: Wireless connectivity for medical monitoring. *Diabetes Science and Technology*, 4(2):457–463, 2010.

[9] L. Guo-Cheng and Y. Hong-Yang. Design and implementation of a bluetooth 4.0-based heart rate monitor system on ios platform. In *Proceedings of the International Conference on Communications, Circuits and Systems (ICCCAS)*, volume 2, pages 112–115, Chengdu, China, November 2013.

[10] Q. Zhang and Z. Liang. Security analysis of bluetooth low energy based smart wristbands. In *Proceedings of the 2nd International Conference on Frontiers in Sensor Technology (ICFST)*, pages 421–425, Shenzhen, China, April 2017.

[11] D. Antonioli, N. O. Tippenhauer, K. B. Rasmussen, and M. Payer. Blurtooth: Exploiting cross-transport key derivation in bluetooth classic and bluetooth low energy, 2020. arXiv preprint.

[12] A. K. Das, P. H. Pathak, C.-N. Chuah, and P. Mohapatra. Uncovering privacy leakage in ble network traffic of wearable fitness trackers. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*, pages 99–104, February 2016.

[13] H. O'Sullivan. Security vulnerabilities of bluetooth low energy technology (ble). Technical report, Tufts University, Medford, MA, USA, 2015.

[14] T. Melamed. An active man-in-the-middle attack on bluetooth smart devices. *Safety and Security Studies*, 8(2):200–211, 2018.

[15] A. C. Santos, J. L. Soares Filho, Á. Í. Silva, V. Nigam, and I. E. Fonseca. Ble injection-free attack: A novel attack on bluetooth low energy devices. *Journal of Ambient Intelligence and Humanized Computing*, 20:1–11, September 2019.

[16] Q. Zhang, Z. Liang, and Z. Cai. Developing a new security framework for bluetooth low energy devices. *Computational Materials and Continua*, 59(2):457–471, 2019.

[17] R. Cayre, D. Cauquil, and A. Francillon. Espwn32: Hacking with esp32 system-on-chips. In *2023 IEEE Security and Privacy Workshops (SPW)*, pages 311–325, San Francisco, CA, USA, 2023.

[18] G. Stergiopoulos, P. Kotzanikolaou, C. Konstantinou, and A. Tsoukalis. Process-aware attacks on medication control of type-i diabetics using infusion pumps. *IEEE Systems Journal*, 17(2):1831–1842, June 2023.

[19] C. Contasel, D.-C. Tranca, A.-V. Palacean, and D. Rosner. Increasing communication security for bluetooth medical devices in ehealth systems. In *2022 21st RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pages 1–4, Sovata, Romania, 2022.

[20] M. Casagrande, E. Losiouk, M. Conti, M. Payer, and D. Antonioli. Breakmi: Reversing, exploiting and fixing xiaomi fitness tracking ecosystem. *Transactions on Cyber-Physical Systems (TCHES)*, 2022(3):330–366, June 2022.

[21] G. Zheng et al. A critical analysis of ecg-based key distribution for securing wearable and implantable medical devices. *IEEE Sensors Journal*, 19(3):1186–1198, February 2019.

[22] C. Pu, H. Zerkle, A. Wall, S. Lim, K.-K. R. Choo, and I. Ahmed. A lightweight and anonymous authentication and key agreement protocol for wireless body area networks. *IEEE Internet of Things Journal*, 9(21):21136–21146, November 2022.

[23] T. Melamed. Hacking bluetooth low energy based applications. In *Proceedings of the International Conference on Internet Monitoring and Protection (ICIMP)*, pages 1–23, Venice, Italy, June 2017.

[24] Yue Zhang, Jian Weng, Rajib Dey, Yier Jin, Zhiqiang Lin, and Xinwen Fu. Breaking secure pairing of bluetooth low energy using downgrade attacks. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 37–54. USENIX Association, August 2020.

[25] Chunxiao Li, Anand Raghunathan, and Niraj K. Jha. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*, pages 150–156, 2011.

[26] Z. Guo, I. G. Harris, Y. Jiang, and L.-F. Tsaur. An efficient approach to prevent battery exhaustion attack on ble-based mesh networks. In *Proceedings of the IEEE International Conference on Computer Network and Communications (ICNC)*, pages 1–5. IEEE, January 2017.

[27] Dictionary - health tools. https://familydoctor.org/your-health-resources/health-tools/dictionary/. Accessed: Aug. 1, 2024.

[28] Mike Ryan. Bluetooth: With low energy comes low security. In *Proceedings of the 7th USENIX Conference on Offensive Technologies*, 2013.

[29] John Padgette, Karen Scarfone, and Lily Chen. Guide to bluetooth security. NIST Special Publication 800-121 Rev. 2, National Institute of Standards and Technology, 2012. Accessed: Aug. 3, 2024.

[30] R. Cayre. Mirage documentation. Available: https://homepages.laas.fr/rcayre/mirage-documentation/. Accessed: Apr. 8, 2024.

[31] R. Cayre, V. Nicomette, G. Auriol, E. Alata, M. Kaaniche, and G. Marconato. Mirage: Towards a metasploit-like framework for iot. In *2019 IEEE 30th International Symposium on Software Reliability Engineering (ISSRE)*, pages 261–270, Berlin, Germany, 2019.