Demo: 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 live demonstration 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 live demonstration, 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 Threat Model

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 [3]. *(ii) The operational structure* is composed of an open-loop system consisting of ECGs, Oximeters and BPMs *(iii)*

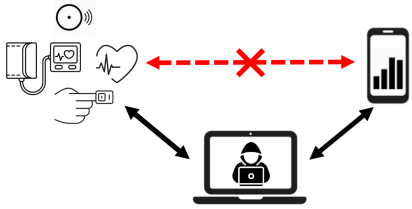

Figure 1: MITM Attack Structure

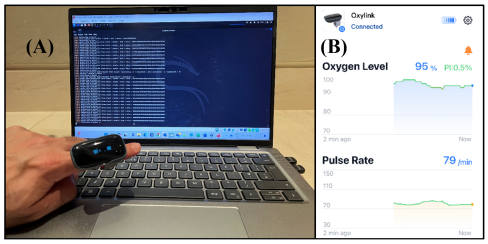

Figure 2: (A) MITM Attack on Oximeter (B) App Interpreted Results.

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.

4 Demonstration Setup

We conduct a live demo of some hacking techniques on several commercially available wearable sensors. The 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" [4, 5] for conducting the passive and active MITM attacks as seen in Figure 1.

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).

5 Visitor Experience

With our live demonstration of security attacks on multiple wearable sensors, visitors gain a deeper understanding of the vulnerabilities inherent in these devices. People also witness the potential consequences of unauthorized access to such devices. Additionally, attendees can actively engage in the experiments by wearing the sensors and observing the real-time interception of data or by performing multiple attacks themselves.

6 Conclusion

The integration of wearable medical devices into the IoMT revolutionizes healthcare by enhancing continuous monitoring and patient management. However, our practical exhibition of security vulnerabilities in wearable medical devices reveals significant cybersecurity vulnerabilities and threats associated with the BLE utilization in these devices. By illustrating the dangers connected with BLE attacks on various devices, including ECGs, Oximeters and BPMs, participants acquire a more profound comprehension of the significance of strong security measures in ensuring patients' safety and data reliability. Looking ahead, it is crucial for researchers, manufacturers, healthcare providers, and policymakers to cooperate in establishing efficient security procedures to lessen these vulnerabilities and guarantee the secure and safe integration of IoMT devices. Moreover, our findings underscore the urgent need for robust cybersecurity measures beyond single protocol reliance. A multilayered approach, incorporating strong encryption, secure authentication, and continuous monitoring, is essential to protect against potential cyberattacks.

This demonstration 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] Dictionary - health tools. https://familydoctor.org/your-health-resources/health-tools/dictionary/. Accessed: Aug. 1, 2024.
[4] R. Cayre. Mirage documentation. Available: https://homepages.laas.fr/rcayre/mirage-documentation/. Accessed: Apr. 8, 2024.
[5] 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.

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