Live Demonstration: Hacking Health: Unveiling Vulnerabilities in Wireless Wearable Sensors

Mohammad Alhussan, Francesca Boem, Sara Ghoreishizadeh, Anna Maria Mandalari (UCL)
{mohammad.alhussan.23, f.boem, s.ghoreishizadeh, a.mandalari}@ucl.ac.uk

***Abstract*—This live demonstration showcases the potential vulnerabilities in some wireless wearable sensors 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.**

***Keywords*—BLE; MITM; IoMT; cybersecurity; IoT**

I. Demonstration Setup

The recent technological emergence of Internet of Medical Things (IoMT) has not only offered immense benefits by enabling continuous monitoring, remote patient management, and data-driven interventions, but has also imposed significant threats. Wearable medical devices are widely spread and are often interconnected with smartphones through BLE, which makes them vulnerable to various attacks such as data breaches, unauthorized access, and device tampering [1].

We conduct a live demo of some hacking techniques on several commercially available wearable sensors as shown in Figure 1, where a MITM attack is represented. The experimental setup consists of:

Wearable Sensors: We use a variety of wearable sensors, such as electrocardiograms (ECG), oximeters and blood pressure monitors, sold by well-known manufacturers (SnapECG, Wellue Oxylink, OMRON RS1 BPM).

Hacking Tools: We use Two BLE enabled dongles. A sophisticated hacking tool "Mirage" is utilized for conducting the MITM attacks [2]. We also demonstrate the capabilities of Mirage in intercepting and modifying data transmitted between the devices and their associated apps.

Data Visualization Tools: We use a laptop with Kali Linux [1] installed to show the intercepted data packets and demonstrate the impact of MITM attacks on the integrity and confidentiality of medical data (Figure 2). During this demo we highlight the potential consequences of unauthorized access to sensitive medical information.

II. 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 intervention of data or by performing multiple attacks themselves.

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

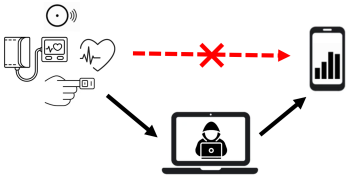

Fig. 1. Wireless Wearable Sensors MITM Attack.

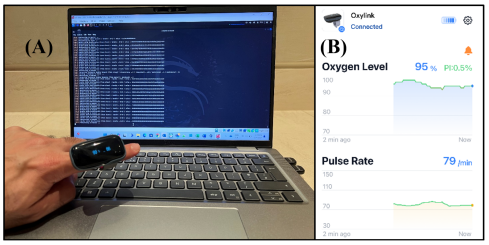

Fig. 2. (A) MITM Attack on Oximeter (B) App Interpreted Results.

III. Conclusions

This practical exhibition of security vulnerabilities in wearable sensors offers valuable insights into the challenges raised in safeguarding confidential medical information. By illustrating the dangers connected with BLE attacks, 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.

This demonstration acts as a catalyst for the healthcare sector to prioritize cybersecurity in the development and deployment of wearable sensors, protecting patient confidentiality and well-being in an increasingly interconnected healthcare environment. In our experiments we do not cause any real threat. All experiments are contained within our own testbed.

References

[1] A. Barua, M. A. Al Alamin, M. S. Hossain, and E. 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] R. Cayre. Mirage documentation. Available: https://homepages.laas.fr/rcayre/mirage-documentation/. [Accessed: Apr. 8, 2024].