Hacking Health: Unveiling Vulnerabilities in BLE-Enabled Wearable Sensor Nodes

Mohammad Alhussan, Francesca Boem, Sara S. Ghoreishizadeh, Anna Maria Mandalari
University College London
{mohammad.alhussan.23, f.boem, s.ghoreishizadeh, a.mandalari}@ucl.ac.uk

***Abstract*—The rise of the Internet of Medical Things (IoMT) in healthcare brings benefits like continuous monitoring, remote patient care, and data-driven treatments. However, it also poses cybersecurity risks. While prior research has investigated this issue, it has not looked at advanced wearable sensor nodes that use combination of Bluetooth Low Energy (BLE) with other wireless protocols. In this paper we conduct a black-box audit of wearable sensor nodes for exploring vulnerabilities associated with them. We use a systematic auditing approach to (1) investigate whether security attacks are effective against wearable sensor nodes, (2) group the vulnerabilities based on susceptibility to certain types of attacks, and (3) provide an in-depth gap analysis of the devices' security behaviour. We develop and release an approach for semi-automated wearable sensor nodes experimentation to reveal their response to common security threats. We perform hundreds of experiments using popular commercial wearable sensor nodes when deployed in an IoMT testbed. Our results indicate not only that these devices are vulnerable to common security attacks, but also their critical security gaps jeopardize patient safety and data integrity.**

***Keywords*—BLE, IoMT, wearable sensor node, security**

I. Introduction

The Internet of Medical Things (IoMT) offers substantial benefits such as continuous monitoring, remote patient management, and data-driven interventions. However, it also presents significant cybersecurity risks as many IoMT devices prioritize functionality and ease of deployment over robust security measures, leaving them more exposed to potential cyberattacks [1]. Among IoMT devices, wearable sensor nodes are becoming increasingly popular due to their ability to provide real-time health data, improve patient engagement, and facilitate personalized healthcare [2]. The global market for wearable sensor nodes was valued at $33.85 billion in 2023, with a forecasted Compound Annual Growth Rate (CAGR) of 25.66% from 2024 to 2030 [3]. By 2045, 1 in 8 adults, totaling around 783 million individuals, will be diagnosed with diabetes, marking a 46% increase [4]. These individuals increasingly rely on Continuous Glucose Monitors (CGMs) that connect with other sensor nodes and applications, forming a cohesive IoMT ecosystem. This integration enables real-time data exchange and remote management of glucose levels, enhancing patient care and promoting proactive health interventions.

Wearable sensor nodes are typically connected with smartphones via Bluetooth Low Energy (BLE) [5], making them susceptible to cybersecurity threats such as data breaches, unauthorized access, and device tampering. Compromised devices especially the wearable sensor nodes within the Operational Technology (OT) environment [6] threaten patient privacy and safety. OT encompasses the hardware and software systems responsible for detecting and managing changes through direct monitoring and control of physical devices, processes, and events in healthcare settings. A recent ransomware attack on Change Healthcare exemplifies these threats, significantly disrupting the U.S. healthcare system by causing operational shutdowns that affected pharmacies and hospitals [7].

There has been public and regulatory scrutiny of cybersecurity in wearable sensor nodes. Kirk *et al.* [8] reveal critical vulnerabilities in insulin pumps, including insecure communication protocols, inadequate authentication measures, and the lack of encryption. These could easily be exploited to remotely manipulate insulin delivery, potentially leading to severe hypoglycemic or hyperglycemic events in patients. Numerous research efforts have studied vulnerabilities and threats in wireless communications, particularly concerning wearable and implantable sensor nodes, as well as general IoMT applications [5], [9]–[27]. However, there is limited research on vulnerabilities of advanced wearable sensor nodes such as those combining BLE with other wireless protocols, that are being increasingly adopted by wearable sensor nodes' manufacturers to enhance security [28].

Melamed [29] modifies data transmission from a smartwatch to a device using tools for replay and on-the-fly data modifications. Zhang *et al.* [30] emphasize the necessity for the BLE programming framework in initiators to effectively manage Secure Connections Only (SCO). This approach helps avoid downgrade attacks that exploit pairing protocols, demonstrating that Man in the Middle (MITM) attacks are feasible across various tested BLE products. Li *et al.* [31] demonstrate successful security attacks on older versions of CGMs and insulin pumps, revealing that both passive (eavesdropping) and active attacks (impersonation) can be executed using publicly available information and common hardware. However, their focus is limited to older wireless technologies, not involving BLE, which incorporate more advanced security features [32]. Furthermore, their research focuses on reverse engineering a single system and lacks systematic auditing and security assessments of other wearable sensor nodes. Dadkhah et al. [33] present the CICIoMT2024 dataset, a benchmark for assessing multi-protocol security in IoMT devices, involving a variety of attacks across 40 devices. While their work establishes a comprehensive dataset that contributes significantly to the field, it primarily focuses on dataset creation and the evaluation

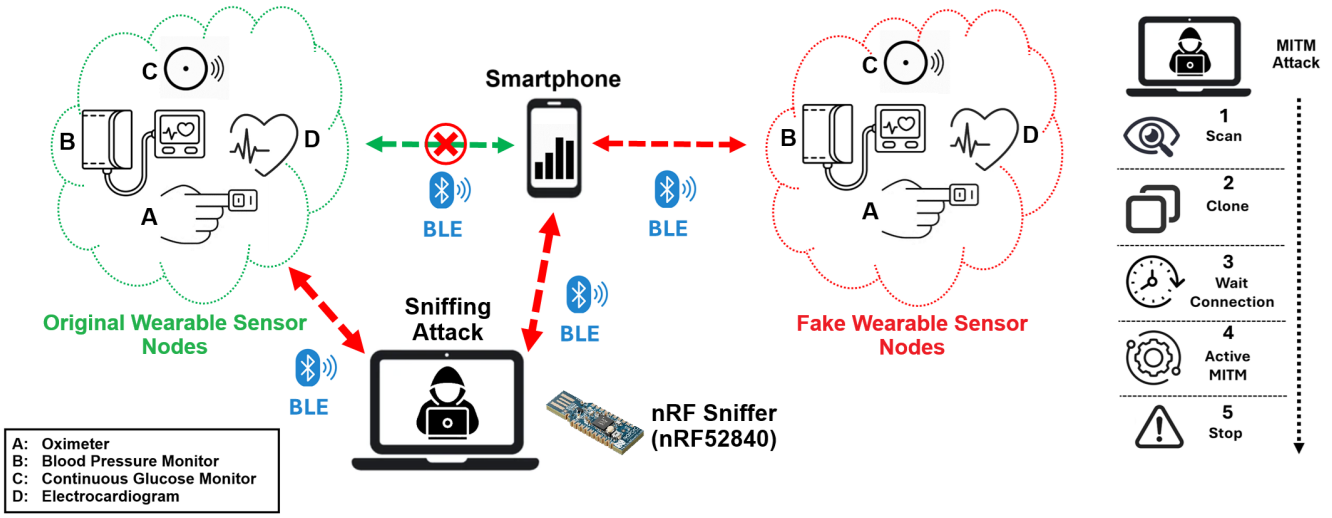


Fig. 1. BLE Sniffing & MITM Execution Processes.

of machine learning (ML) techniques for detecting these attacks. In contrast, our research focuses on more sensitive devices, such as CGMs, and aims to provide a repeatable auditing methodology that can be applied to many devices at scale. By conducting systematic audits on commercially available BLE-enabled wearable sensor nodes, we emulate real-world attacks, including eavesdropping, MITM, and Denial of Service (DoS). This hands-on experimentation not only uncovers critical vulnerabilities that may remain hidden in a dataset-driven context but also highlights the immediate and practical risks these devices face in operational settings, offering a scalable approach to securing wearable sensor nodes ecosystems.

The primary objective of this research is to enhance the security and reliability of BLE-enabled wearable sensor nodes by providing a systematic auditing methodology. We test our auditing methodology on seven commercially available and well-known wearable sensor nodes. We consider devices that utilize the latest BLE specifications, such as BLE 4.0, 5.0 and beyond, which introduce features like increased data transfer rates, extended range, and improved security mechanisms, such as Secure Connections that employ Elliptic Curve Diffie-Hellman (ECDH) and Near Field Communication (NFC) for key exchange. We focus on the implications of potential cyber-attacks, despite the purported security enhancements offered by these newer wireless communication protocols.

To contribute to the advancement of research in this field and enhance reproducibility, we make all codes and data produced as part of this work available at the following url. [1]

Responsible Disclosure. We responsibly disclosed our results to the manufacturers of the wearable sensor nodes that we studied in this work. At the time of submission, we did not receive responses, we will include details of any subsequent feedback and mitigation in the final version of this paper.

[1]https://github.com/SafeNetIoT/WMD_MITM.git

TABLE I
SUMMARY OF WEARABLE SENSOR NODES USED IN THIS RESEARCH

Device	Description	Manufacturer	Nickname
Wellue BP2A 2031	BPM	Shenzhen Viatom	BPM#1
Dexcom ONE	CGM	DexCom Inc.	CGM#1
FreeStyle Libre 2	CGM	Abbott Laboratories	CGM#2
SnapECG	ECG	Nanjing Xijian	ECG#1
DuoEK Wellue	ECG	Shenzhen Viatom	ECG#2
OXYLINK	Oximeter	Shenzhen Viatom	OXI#1
SleepO2 1400	Oximeter	Shenzhen Viatom	OXI#2

II. EXPERIMENTAL SETUP AND METHOD

In order to have a controlled environment for auditing the devices, we build the testbed shown in Fig.1. In this section we first explain the threat model used in our testbed, we then describe the testbed and the methodology for auditing the devices.

A. Threat Model

We assume that wearable sensor nodes function as components of either open-loop or closed-loop systems. We also assume that our system is composed of four main entities: *(i) The victim*, either a patient with blood pressure lability, a patient with heart arrhythmia, a patient with hypoxemia or a patient with type 1 or 2 diabetes and relies on wearable sensor nodes to function or live a healthy life [34]. *(ii) The operational structure* is composed of an open-loop system that only includes the wearable sensor node (ECG monitors, Oximeters, BPMs, CGMs) or a closed-loop system, such as a hybrid or fully automated artificial pancreas consisting of a CGM sensor, a smart device (containing the control algorithm), and an insulin infusion pump. *(iii) The communication*, standard BLE 4.0 or BLE 5.0. *(iv) The potential adversary*, an individual or organization within the BLE operational range (i.e. 100m) performing malicious active cyberattacks (i.e. MITM and DoS) and/or passive (i.e. Sniffing or Eavesdropping) on the open-loop or closed-loop system.

B. Testbed

Our testbed consists of the following components. *(i) The devices under test*, including ECG monitors, Oximeters, Blood Pressure Monitor (BPM), and Continious Glocuse Monitors (CGM) as detailed in Table I. *(ii) Smartphones:* for controlling the devices through their companion app, iPhone 13 Pro and Google Pixel 3. *(iii) Tools:* we use two ORICO Wireless USB Bluetooth 4.0 Adapter USB Dongles (Transmitter-Receiver) [35], an nRF52840 Nordic Dongle [36], Wireshark software and "Mirage" [37], [38] to conduct the attacks. The Mirage module is based on two main MITM strategies GATTacker and BTLEJuice [38]. *(iv) Data Visualization Tools:* we use a server with Kali Linux [39] and Wireshark installed to perform the eavesdropping, passive and active attacks, show and analyze the intercepted data packets, and demonstrate the impact of the attacks on the integrity and confidentiality of medical data.

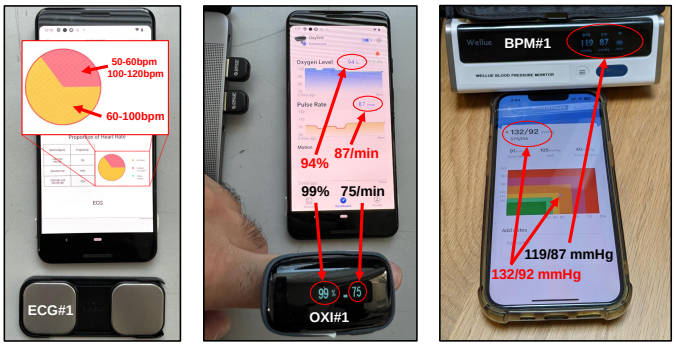
C. Auditing Methodology

We provide a methodology for auditing the devices against 4 main attacks, passive and active MITM attack, DoS attack and sniffing. We write auditing script for performing these attacks and reading the response. Each auditing experiment iterates for at least 30 times per device per type of attack. Our MITM attack execution process is divided into five main steps (Fig. 1): **Scan.** Performs an active scan in order to discover the target device. This process involves identifying available BLE devices in the vicinity and collecting relevant data about their advertising packets. **Clone.** Clones the target device and applies the selected advertising strategy. This means creating a virtual version of the target device that can mimic its behaviour and signals. This allows us to attract connections from legitimate devices, as they may mistake the clone for the original. **Wait Connection.** Waits for an incoming connection from the smartphone. **Active MITM.** Performs either passive attacks by intercepting and forwarding legitimate packets between the smartphone and the connected device, or active attacks through a set of auditing scripts that execute specific commands and inject payloads into the communication to manipulate data flow. **Stop.** Stops execution.

For sniffing, we employ the *nRF Sniffer (nRF52840)* [36] as shown in Fig. 1, upon initiation, the sniffer discovers all proximate BLE devices actively advertising, broadcasting Bluetooth address and address type, full or abbreviated name, along with the Received Signal Strength Indication (RSSI). The sniffer's software comprises firmware that is programmed onto a development kit (DK) and a capture plugin for Wireshark used to analyze the captured logs.

Our DoS auditing methodology utilizes auditing scripts that ensure the server maintains a continuous connection with the wearable sensor nodes, thereby preventing the smartphone from establishing contact with the device, leading to a "loss of view".

Note: We do not cause any real threats in our experiments. All experiments are contained within our own testbed.



(A) (B) (C)

Fig. 2. (A) Active MITM on ECG#1 (B) Active MITM on OXI#1 (C) Active MITM on BPM#1

III. Results

In this section we present our auditing results along with a detailed analysis of intercepted BLE data logs of the wearable sensor nodes, according to the specific attack types and vulnerabilities encountered.

A. Man-in-the-Middle (MITM)

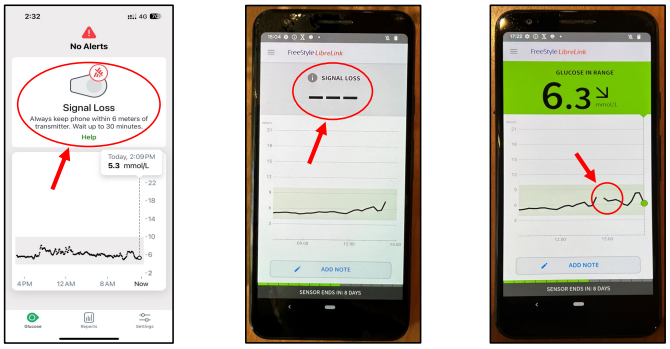
MITM attack is successfully performed on ECG monitors, oximeters, BPM and CGMs and multiple vulnerabilities are found as follows.

(i) Active MITM. Upon successfully performing this attack on the ECG#1, we find that its packet structure includes only the *Header Information* and *Payload Content*. The absence of robust encryption is evident; as during the attack, we are able to modify several payloads of the packets, demonstrating successful data manipulation, where the heart rate readings show fake unhealthy conditions as shown in Fig. 2 (A).

Similarly, we assess OXI#1 and OXI#2. Since both share identical BLE structures and security mechanisms, we focus on OXI#1, whose packet structure includes typical BLE header fields with notification handles containing encoded data related to oxygen level and heart rate. This data can be decoded using the typical BLE packet format, where oxygen-level data can easily be found in the fourth six bytes of the packet. The only authentication observed is a two-character hexadecimal key sent from the oximeter to the smartphone after each packet. However, we observed that once this key is captured, a replay attack can easily and successfully be carried out. For example, during an MITM attack on OXI#1, the original payload associated with the key "39" (oxygen level = 97%, heart rate = 94/min) is replaced with a previously captured payload tied to the key "db" resulting in an oxygen level = 96% and heart rate = 65/min, indicating a successful replay attack as shown in Fig. 2 (B).

Correspondingly, during the MITM attacks on BPM#1, handle value notifications are successfully altered to push the blood pressure point into the unhealthy region (the orange region in Fig. 2 (C)), indicating a successful data manipulation attack.

(ii) Passive MITM. In the process of executing this attack on the CGM#1 and CGM#2 devices, we successfully connect



(A) (B) (C)

Fig. 3. (A) CGM#1 App Loss of View Attack (B) CGM#2 App Loss of View Attack (C) CGM#2 App Loss of View Effect

to the devices and perform a "services discovery" operation (extracting device attributes) via the *ble_connect* and the *ble_discover* modules within the *Mirage* tool. The extracted data provides detailed information about the services, characteristics, and attributes of these devices, which are crucial for understanding their BLE protocol implementation. We are also able to extract device information such as *Bluetooth Device Address*, *Name*, *Company*, *Flags* and *Advertising Data*.

By conducting BLE security analysis on the CGM#1, we conclude that it uses *Just Works Pairing* method, which is the simplest form of Secure Simple Pairing (SSP) in BLE technology and does not require any human interaction to complete the pairing [40]. Conversely, by executing BLE security analysis on the CGM#2, we conclude that it uses *Out-of-Band (OOB)* method, which is the most advanced form of Secure Simple Pairing (SSP) in BLE technology as it requires the use of Near Field Communication (NFC) to complete the pairing [40]. Although no data manipulation is successfully performed, due to the robustness of the OOB method against such attacks [40], the multiple partially successful passive MITM attacks could potentially cause battery depletion and loss of view.

B. Sniffing

The analysis of the BLE packet data sniffed from the CMG#1 reveals key security components: the *Random Number (rand)* is all zeros. This imposes a serious security risk because the predictability of the random numbers can allow attackers to compromise security protocols more easily. Additionally, the *Encrypted Diversifier (EDIV)* also appears to be a non-random or default value. The captured *Session Key Diversifier Master (SKDm)* and the *Session Key Diversifier Slave (SKDs)*, both suggest secure, randomized session key generation. The captured *Master Session Initialization Vector (IVm)* and the *Slave Session Initialization Vector (IVs)*, both appear sufficiently randomized, indicating a positive security status.

As for the CGM#2, the analysis of the captured BLE packet data shows key components linked to BLE security. The captured logs contain several *ATT Packets* labelled "Rcvd Handle Value Notification", indicating that the CGM#2 actively sends updates, likely glucose readings, to the paired device. The analysis also reveals proprietary data transactions,

TABLE II
WEARABLE SENSOR NODES AUDITING RESULTS.
✓ : SUCCESSFUL ATTACK, ✓̸ : PARTIALLY SUCCESSFUL ATTACK,
✗ : UNSUCCESSFUL ATTACK

Devices	**Types of Attacks**			
	Sniffing (nRF52840 Nordic Dongle)	Passive MITM (Mirage)	Active MITM (Mirage)	DoS (Mirage)
ECG#1	✓	✓	✓	✓
ECG#2	✓	✓̸	✗	✓
OXI#1	✓	✓	✓	✓
OXI#2	✓	✓	✓	✓
BPM#1	✓	✓	✓	✓
CGM#1	✓	✓̸	✗	✓
CGM#2	✓	✓̸	✗	✓

which are crucial as they may contain sensitive algorithms and information that, if compromised, could undermine the device's functionality and the accuracy of health data.

C. Denial of Service (DoS)

DoS attacks are successfully executed on all seven devices to cause loss of availability, with a particular focus on ECG#2, CGM#1 and CGM#2. Despite the extensive data interactions from ECG#2, no active MITM attacks are conducted due to the consecutive disconnection commands initiated by the device (ECG). However, the seamless connection and redirection of packets between the device (ECG) and the smartphone's App (ViHealth App) could be considered as potential hijack or DoS attack due to the loss of availability it causes.

We are able to hijack the new or established sessions when the smartphone and the wearable sensor nodes get disconnected and try to reconnect every 5 mins for the CGM#1 and every 1 min for the CGM#2, which eventually causes loss of view (Signal Loss) as shown in Fig. 3 (A), (B), and (C).

Table II summarizes the results of all our experiments. In particular, we find all 7 tested devices susceptible to DoS and sniffing attacks, 4 out of 7 devices are vulnerable to passive and active MITM attacks, while 3 out of 7 devices are partially receptive to passive MITM attacks but secure against active MITM attacks.

IV. CONCLUSION

Our study reveals significant cybersecurity vulnerabilities and threats associated with wearable sensor nodes. We perform and release a systematic auditing methodology for attacks (i.e. sniffing, MITM, and DoS attacks) and gap analysis on various commercial devices, including ECG monitors, Oximeters, BPMs and CGMs. Our results highlight critical security gaps that could jeopardize patient safety and data integrity. Our findings underscore the urgent need for robust cybersecurity measures beyond single protocol reliance. Based on our findings, we argue there is need for a multi-layered approach, incorporating strong encryption, secure authentication, and real-time monitoring of device performance and security status.

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] Karen Taylor, Amen Sanghera, William Lin, Mark Steedman, and Matthew Thaxter. Medtech and the internet of medical things: How connected medical devices are transforming health care. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf, July 2018. Accessed: Oct. 2024.

[3] Inc. Grand View Research. Wearable medical devices market size, share & trends analysis report by product type (smart watches, fitness trackers), by application (cardiovascular diseases, diabetes), by region, and segment forecasts, 2024 - 2030, 2024. Available online: https://www.grandviewresearch.com/industry-analysis/wearable-medical-devices-market. Accessed: Oct. 2024.

[4] About diabetes, international diabetes federation. https://idf.org/about-diabetes/what-is-diabetes/, 2024. Accessed: Oct. 2024.

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

[6] LogRhythm. Securing operational technology in healthcare. https://logrhythm.com/blog/securing-operational-technology-in-healthcare, January 2024. Accessed: Oct. 2024.

[7] CRN. 10 major cyberattacks and data breaches in 2024 (so far). *CRN*, 2024. Accessed: Oct. 2024.

[8] K. Kirk, A. Belkin, P. Dhanrajani, and S. Raghavan. Cybersecurity of medical devices: The importance of secure design. *Nature Medicine*, 25(7):1038–1044, 2019.

[9] 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.

[10] 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.

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

[12] 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.

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

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

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] All About Circuits. Vulnerabilities and attacks on bluetooth le devices—reviewing recent info. 2024. Accessed: Oct. 2024.

[29] 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.

[30] 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.

[31] 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.

[32] Yue Zhang, Jian Weng, Rajib Dey, and Xinwen Fu. *B Bluetooth Low Energy (BLE) Security and Privacy*, pages 1–. 10 2019.

[33] Sajjad Dadkhah, Euclides Neto, Raphael Ferreira, Reginald Molokwu, Somayeh Sadeghi, and Ali Ghorbani. Ciciomt2024: A benchmark dataset for multi-protocol security assessment in iomt. *Internet of Things*, 28:101351, 08 2024.

[34] Dictionary - health tools. https://familydoctor.org/your-health-resources/health-tools/dictionary/. Accessed: Oct. 2024.

[35] Orico usb mobile product. https://www.orico.cc/usmobile/product/detail/id/3425. Accessed: Oct. 2024.

[36] Nordic Semiconductor. nrf sniffer for bluetooth le. = https://www.nordicsemi.com/Products/Development-tools/nRF-Sniffer-for-Bluetooth-LE, August 2024. Accessed: Oct. 2024.

[37] R. Cayre. Mirage documentation. Available: https://homepages.laas.fr/rcayre/mirage-documentation/. Accessed: Oct. 2024.

[38] 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.

[39] Kali linux. https://www.kali.org/. Accessed: Oct. 2024.

[40] Bluetooth Special Interest Group. Bluetooth core specification 5.1. = https://www.bluetooth.com/specifications/specs/core-specification-5-1/, July 2024. Accessed: Oct. 2024.