Cyber Security Risks in Wearable Devices

Stacey Vargas and Durig Lewis
Department of Physics and Astronomy, Virginia Military Institute, Lexington, USA

vargas@vmi.edu
lewisde@vmi.edu

Abstract: The growing popularity of wearable devices, particularly for medical and fitness applications, has increased reliance on these technologies for tracking biometric data. These devices typically transmit data in multiple stages, beginning with Bluetooth Low Energy (BLE) connectivity, followed by transmission to internet-enabled devices, and ultimately to cloud storage. Each communication step introduces potential cybersecurity vulnerabilities. Understanding the functionality of wearable devices, the data transmission process, and the associated cyber risks, is crucial to safeguarding users against cyberattacks. This paper explores the types of sensors used in wearables, the data transmission workflow, and the cybersecurity challenges involved. It also discusses potential preventative measures to mitigate these risks.

Keywords: Wearable devices, Cybersecurity, Biometric data, Bluetooth low energy, Internet of Things (IoT), Cloud storage

1. Introduction

The number of Americans using wearable devices (WD), such as smartwatches or fitness trackers, continues to grow at rapid rates. According to a survey sponsored by the National Institute of Health almost one in three Americans uses a wearable device to track their health data (National Heart, Lung, and Blood Institute 2023). A wearable device is unique to an individual user and is defined as any electronic device that can be attached to the body or clothing to monitor and collect data (TechTarget). These devices can collect data ranging from health statistics such as body temperature, blood oxygen, and heartrate to information on the individual's location. The information is synchronized with the WD and can be shared with a company or service provider through an app. Most wearable devices connect to smartphones or internet-ready devices using Bluetooth Low Energy (BLE). As its name suggests, BLE is designed to transfer small amounts of data with minimal power consumption, which is beneficial when trying to preserve battery lifetime (Balasubramanian et al, 2020). However, as with any type of connectivity, a device using BLE is susceptible to cybersecurity threats. In most wearables, once data is transferred from the WD to an internet-capable device, the data is shared with a cloud server using cellular or Wi-Fi networks, adding additional layers of vulnerability. These risks are substantial, and thus additional research is needed to identify vulnerabilities and mitigate potential threats. This paper aims to provide an overview of wearable devices, the data transmission process, the cybersecurity risks involved, and potential preventative measures. In addition, it offers insights for individuals and researchers seeking to minimize cyber threats in wearable technology.

2. Research Methodology

This research is part of a funded project investigating cyber risks in wearable devices (WDs). The initial phase involved thoroughly reviewing the latest information on cyber risks associated with WDs. The sources reviewed included journal articles, whitepapers, websites, and reports. While the literature review, which forms the basis of this paper, was comprehensive, the work remains ongoing. In addition to the literature review, the grant also supports an experimental component to detect hidden wearable devices, though it is outside the scope of this paper.

3. Wearable Devices and Their Market

Microelectronics and small sensors have revolutionized the world of wearable devices. These sensors allow WDs to collect vital data from users in real-time (Blow et al, 2020). Common sensors found in WDs include accelerometers, which detect movement patterns and intensity, and geolocation sensors, which track the user's location and orientation (Aroganam et al, 2019). Wearables also use photoplethysmography, which employs light sensors to monitor blood volume and circulation, particularly through the wrist, providing insights into the user's cardiovascular health (Nelson et al, 2023). These sensors, often used in combination, allow WDs to track activities, measure heart rates, count steps, and monitor various other health metrics. The data obtained by the sensors is stored in WDs and later shared with third parties. During the transfer process, the data is susceptible to cyber vulnerabilities. Unfortunately, many users are oblivious to the associated risks.

The market for wearables continues to grow. Currently, it is estimated that one in three Americans use a wearable device. Wearable devices have expanded into many domains from headsets to rings such as the Oura

and the Samsung Galaxy Ring. Currently, the global wearable device market is evaluated at $178 billion and is expected to grow at a compound growth rate of 14.6% reaching over $500 billion by 2033 (Horizon Databook, 2023). Given this rapid expansion, it is crucial to assess the cybersecurity risks of wearables, raise awareness among users, and develop strategies to minimize these risks.

4. Cyber Risks in Wearable Technology

Since wearables are devices on the Internet of Things (IoT), WDs are vulnerable to cyberattacks. The fact that most wearables collect personal, and health data complicates the risk factor for the user. If a device is compromised, users may unknowingly expose sensitive information to malicious actors, leading to dangerous consequences. In addition, cybersecurity threats cross a variety of boundaries including confidentiality, integrity, availability, and more. Figure 1 provides insight into how attacks have evolved from 2008 to 2020 (Sectigo 2020). The attacks continue to grow and evolve with the development of new devices including wearables.

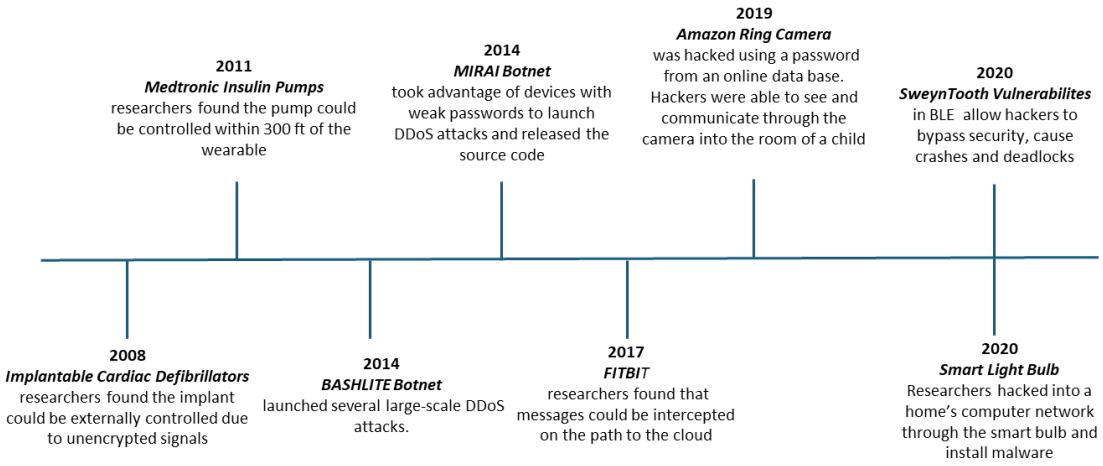

Figure 1: The figure highlights how attacks on IoT devices have evolved from 2008 to 2020

Most wearable devices do not connect directly to the Internet. Instead, the data is transferred via Bluetooth Low Energy to an Internet-capable device (Seneviratne, 2027). Standard Bluetooth is used for short-distance radio frequency communication. Cybercriminals have hosted multiple attacks on Bluetooth (Silva-Trujillo et al, 2023). With modifications to Bluetooth, BLE was developed for devices requiring battery longevity for optimal operation. BLE conserves battery life by remaining in a low-power sleep mode until the device initiates pairing with an IoT device. To simplify the pairing process, there is limited, or no user interaction needed which leaves the device exceptionally vulnerable to cyberattacks. It has been shown, that in devices using low-security BLE, passive sniffing can successfully intercept data during the pairing process (Wu et al, 2020). In passive sniffing, a hacker can capture information in a network without interfering with it. Once a data packet is captured, attackers can use free download tools such as Wireshark to analyze the packet (Cusak et al, 2017). To minimize the risk of such a passive attack, users should pair with LE Secure available in BLE 4.2 or higher. With BLE 4.2, the pairing is performed using the Diffie-Helman Key Exchange algorithm which allows for encryption over a public communication channel (ScienceDirect). Using this method, the WD and the IoT device each have private and public keys. This is different from the previous version of BLE where both devices shared one key. The dual key pairing makes it more difficult for hackers to crack the code. One device can share data using the public key and the other device can decrypt the data with its private key (TechTarget). Even with the implementation of Diffie-Helman Key Exchange, WD users may remain vulnerable through a lack of authentication. If the device is not verified before pairing, the system is susceptible to Man in the Middle Attacks (MITM) also known as an On-Path Attack. As it sounds, the attacker places itself between the two devices and intercepts the data being transmitted, which could be personal information or identification. The attacker can then impersonate a device and continue to collect user information (Malik et al, 2019). WD users should implement some type of authentication to prevent MITM attacks.

When a wearable device transfers data to an IoT device, it often relies on the IoT device as a gateway to the cloud, since wearables typically lack direct internet connectivity. Unfortunately, IoT devices may have weak points where an attacker may enter, such as poor authentication, lack of encryption, shared network access, and missing firmware updates. If an attacker gains access to the IoT it can compromise the WD data. Thus, wearable device users should implement basic security measures to minimize risks when connecting with IoT

devices. Some basic steps include using a two-step authentication process, encrypting data, updating firmware, having a firewall on the IoT device, and using Virtual Private Networks (VPN) instead of Wi-Fi to help protect the user.

The lack of adequate protection in IoT devices poses a risk not only to the wearable user but also to other devices connected to the same network. A 2023 Nokia Threat Intelligence Report revealed a dramatic increase in IoT devices engaged in botnet-driven Distributed Denial of Service (DDoS) attacks, rising from 200,000 to 1 million in one year (Nokia, 2023). Combining the words, robot and network, a botnet, is a network of IoT devices infected by malware that allows a bad actor to control the devices and launch cyberattacks including DDoS (Bhattacharya et al, 2024). In a DDoS attack, an excessive amount of malicious traffic is sent to a website or service to overwhelm it which can cause the network or server to crash. Identifying the devices contributing to the attack is difficult, and such attacks can harm wearable users and others connected to the network.

Once WD data is transmitted to an IoT device, it is typically sent to the cloud for storage. Fitness wearables like WHOOP monitor a variety of health metrics including, heart rate, respiratory rate, temperature, blood oxygen, sleep, stress, recovery, and more (Whoop). These devices collect sensitive health data that, if managed by a medical professional, would be protected under HIPAA regulations. However, wearable users are sharing this data via BLE to an IoT device and eventually to the cloud. Wearable devices can also be hacked through cloud connectivity. The cloud, while convenient, is an attractive target for hackers due to the potential to access data from multiple users in a single breach (World Economic Forum, 2021). Data breaches, where unauthorized access occurs, pose a significant risk to wearable users, especially given that much of their health data is stored in the cloud. Some researchers are investigating blockchain as a more secure option for cloud storage (Baalamurugan et al, 2021). Unlike the cloud which stores all data in a central location, blockchain shares it in multiple locations or blocks making it more difficult for all data to be accessed during a cyberattack. There are additional features such as cryptographic techniques and immutability, meaning once the data enters the blockchain it cannot be altered, which may make blockchain a more secure option than the cloud for wearable devices.

Some wearable companies like WHOOP are allowing third-party involvement by offering WHOOP Developer Platform where users can develop and integrate apps with WHOOP. The marketing by Whoop states “enables third-party applications to create meaningful integrations” (WHOOP). WHOOP users can create apps to monitor something new and share it with other users. In addition, WHOOP users can also share their data with other WHOOP users. Although there are measures in place by the company indicating the integration by third-party developers is secure, this may increase the attack surface, potentially introducing new vulnerabilities.

5. Conclusion

Wearable devices, such as smartwatches, fitness trackers, and medical implants continue to grow in popularity, as do the cyber risks associated with their use. Data collected by WDs including personal, financial, and medical information, is transmitted through multiple steps, involving Bluetooth, IoT devices, and cloud storage. Each of these steps presents an opportunity for cyberattacks. If a cyberattack takes place during any step of the data transmission process, attackers may gain access to sensitive information. To protect users, wearable manufacturers should implement robust security measures, such as multi-factor authentication, data encryption, firmware updates, and other preventative strategies. At the same time, users must be aware of the risks and remain vigilant in their efforts to minimize cyber vulnerability. As the wearable market expands, ongoing research into cybersecurity threats and effective prevention methods is crucial to safeguarding users' data and privacy. In this ongoing project, the authors will further explore the literature, reviewing additional sources to analyze wearable device attacks and optimize processes to mitigate these threats. Funding for this research also supports experimental work to detect hidden wearables, which is ongoing, although outside the scope of this call for papers.

Acknowledgements

Project sponsored by the National Security Agency under Grant/Cooperative Agreement Number H98230-21-l-0167. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation herein. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Security Agency This manuscript is submitted for publication with the understanding that the United States Government is authorized to reproduce and distribute reprints.

References

Aroganam, G., Manivannan, N., & Harrison, D. (2019). Review on wearable technology sensors used in consumer sport applications. *Sensors (Basel), 19*(9), 1983. https://doi.org/10.3390/s19091983.

Baalamurugan, K. M., Kumar, S. R., Kumar, A., Kumar, V., & Padmanaban, S. (Eds.). (2021). *Blockchain Security in Cloud Computing*. Springer Cham. https://doi.org/10.1007/978-3-030-70501-5.

Balasubramanian, Karthikeyan Kalyanasundaram, et al. "Neural network-based Bluetooth synchronization of multiple wearable devices." Nature Communications, vol. 14, no. 1, 2023, Article number: 40114, 1-10, doi: 10.1038/s41467-023-40114-2.

Bhattacharya, S., Khanna, A., & Dubey, R. (2024). Botnet Detection and Mitigation: A Comprehensive Literature Review. *International Journal of Computer Trends and Technology, 72*(1), 77-82. https://doi.org/10.14445/22312803/IJCTT-V72I1P113 .

Blow, F., Hu, Y.-H., & Hoppa, M. A. (2020). A study on vulnerabilities and threats to wearable devices. Journal of The Colloquium for Information Systems Security Education, 7(1), 1-20.

Cusack, B., Antony, B., Ward, G., & Mody, S. (2017). Assessment of Security Vulnerabilities in Wearable Devices. In Proceedings of the 15th Australian Information Security Management Conference. Cyber Forensic Research Centre, Auckland University of Technology, Auckland, New Zealand.

Horizon Databook. (2023). Wearable technology market size, share & trends analysis report: By product (head & eyewear, wristwear), by application (consumer electronics, healthcare), by region (Asia Pacific, Europe), and segment forecasts, 2023 - 2030 (Report No. 978-1-68038-165-8). Horizon Databook. https://www.grandviewresearch.com/industry-analysis/wearable-technology-market .

Mallik, A., Ahsan, A., Shahadat, M. M. Z., & Tsou, J.-C. (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science, 3*(2019), 77–92. https://doi.org/10.5267/j.ijdns.2019.1.001.

National Heart, Lung, and Blood Institute. "Study Reveals Wearable Device Trends Among U.S. Adults." NIH News, National Institutes of Health, 2023, https://www.nhlbi.nih.gov/news/2023/study-reveals-wearable-device-trends-among-us-adults.

Nelson, B. W., Harvie, H. M. K., Jain, B., Knight, E. L., Roos, L. E., & Giuliano, R. J. (2023). Smartphone photoplethysmography pulse rate covaries with stress and anxiety during a digital acute social stressor. *Psychosomatic Medicine, 85*(7), 577-58. https://doi.org/10.1097/PSY.0000000000001178.

Nokia. (2023, June 7). Nokia Threat Intelligence Report finds malicious IoT botnet activity has sharply increased. https://www.nokia.com/about-us/news/releases/2023/06/07/nokia-threat-intelligence-report-finds-malicious-iot-botnet-activity-has-sharply-increased/ .

ScienceDirect. (n.d.). Hellman Algorithm. In *ScienceDirect Topics*. Retrieved August 6, 2024, from https://www.sciencedirect.com/topics/computer-science/hellman-algorithm.

Sectigo (2020) Evolution of IoT Attacks, Evolution-of-IoT-Attacks-Interactive-IG_May2020.pdf.

Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., Hassan, M., & Seneviratne, A. (2017). A survey of wearable devices and challenges. *IEEE Communications Surveys & Tutorials, 19*(4), 2573-2620.

Silva-Trujillo, A. G., González González, M. J., Rocha Pérez, L. P., & García Villalba, L. J. (2023). Cybersecurity analysis of wearable devices: Smartwatches passive attack. *Sensors, 23*(12), 5438. https://doi.org/10.3390/s23125438.

TechTarget. (n.d.). Diffie-Hellman key exchange. https://www.techtarget.com/searchsecurity/definition/Diffie-Hellman-key-exchange.

TechTarget. (n.d.). Wearable technology, https://www.techtarget.com/searchmobilecomputing/definition/wearable-technology .

WHOOP. (n.d.). Retrieved from https://www.whoop.com/us/en/the-data/#insights.

WHOOP. (n.d.). Introduction. In *WHOOP Developer Documentation*. Retrieved from https://developer.whoop.com/docs/introduction/

World Economic Forum. (2021, August 3). Threats to IoT devices are constantly evolving, but is security keeping up? *World Economic Forum*. Retrieved from https://www.weforum.org/agenda/2021/08/threats-to-iot-devices-are-constantly-evolving-but-is-security-keeping-up/.

Wu, J., Nan, Y., Kumar, V., Tian, D. (J.), Bianchi, A., Payer, M., & Xu, D. (2020). BLESA: Spoofing attacks against reconnections in Bluetooth Low Energy. In Proceedings of the 14th USENIX Workshop on Offensive Technologies (WOOT 2020) USENIX Association. https://www.usenix.org/conference/woot20/presentation/wu.