A Study on Vulnerabilities and Threats to Wearable Devices

Felton Blow
f.a.blow@spartans.nsu.edu

Yen-Hung (Frank) Hu
yhu@nsu.edu

Mary Ann Hoppa
mahoppa@nsu.edu

Norfolk State University
Norfolk, Virginia, USA 23504

Abstract - Connected, wearable devices are increasingly being adopted by individuals who want to monitor personal data such as location and vital biometrics, and to receive performance feedbacks and product updates in real time. The quality of life gains these gadgets support for users, and the opportunities they enable for vendors to maintain ongoing relationships with consumers, may backfire if security and privacy are not addressed appropriately. This research explored cybersecurity vulnerabilities, threats, and risks related to wearable devices using the Fitbit smartwatch as a popular example. Analysis focused on the sensors that are integrated into such devices. Understanding how these components work exposed ways they can be exploited, which in turn suggested ways to mitigate potential cyber-attacks on wearable devices. These findings provide a foundation for developing awareness and education, and recommending best practices for wearable devices to balance their functionality and convenience with personal privacy and organizational cybersecurity concerns.

Keywords

Wearable devices, vulnerabilities, threats, risk management

1. INTRODUCTION

Wearable devices are being developed and brought to market so rapidly that security and risk management often appear to be overlooked. As the use of wearable devices continues to grow at an incredible rate, so do device vulnerabilities, and along with them security and privacy risks. In the wrong hands, the data that wearable devices collect can potentially cause more harm than data from smartphones and other devices [1]. Wearable devices have created another attack vector and, if not appropriately controlled or governed, they can facilitate the compromise of data confidentiality, availability and integrity for users and organizations.

Wearable devices are in such high demand because of their ability to deliver useful functionality both conveniently and in real time [2]. These devices also are embedded with sensors that enable the collection of vast amounts of information. Some of the key sensors are accelerometers, gyroscopes, Global Positioning System (GPS), acoustics and voice detection [2]. Since these built-in sensors gather personally identifiable information (PII), users and organizations become subject to vulnerabilities and cyber-threats.

With the increasing popularity of wearable devices, it appears manufacturers and developers are more focused on enhancing features like design aesthetics and power consumption rather than security features and dynamics [2]. Each wearable device is unique to its user, and the data it collects, including the user's location, subjects the user to more risks than in the past [1].

The more personal a device is to individual users, the greater the risk it poses [2]. The problem with wearable devices arises in their security and privacy aspects, due to the lack of authentication, authorization, and insecure approaches to information transfer [1] [4]. Organizations that allow wearable devices in the workplace may not be completely aware of the potential security vulnerabilities their employees' devices create. Most companies – even large organizations with standardized security measures – do not treat these devices as potential threats to network safety and security. Poor assessment management of wearable devices poses a growing security risk [3]. Not knowing where these devices are located in an organization and who is wearing them ultimately poses a threat to the company's infrastructure and assets.

This research focused on collecting, reviewingand analyzing wearable device vulnerabilities to better understand how to secure them. By understanding the components of wearable devices, and the security features they lack, individuals and companies can better protect themselves against threats, and undertake informed steps to enforce policies that will strengthen the management of wearable devices in organizations. The objective of this research was to examine security concerns involving threats and vulnerabilities related to wearable devices that impact individuals and organizations.

Due to its popular demand, groundbreaking technology, and technical details available in the public domain, the Fitbit smartwatch was the major focus of this research. Fitbit is said to inspire wearers to lead more active lives by empowering them with data-driven guidance to reach their goals and features that promote good health [5] [6]. While Fitbit design is geared to engage the consumer, keeping them in motion, there are security features that Fitbits lack, making wearers and their organizations vulnerable to attacks. This lack of security can inspire hackers and criminals to aim their efforts at this device to exploit employee and company information.

To conduct this research, data concerning Fitbit design, features, and vulnerabilities, including how these devices gather, store, and transfer information, was collected from various reputable sources. Understanding how Fitbits operate then was used as a basis to analyze the following major vulnerabilities: authentication, Bluetooth connection, and location / tracking features. Considering these three types of vulnerabilities enables enumerating different types of attacks that can exploit them.

Analyzing these threats from the perspective of users and organizations enables recognizing insecure features of these devices, and how they may be targeted during a cyber-attack in a particular user and organizational context will enhance overall security awareness. After analyzing the device, its features, and potential security risks, a list of ways to mitigate these vulnerabilities was developed, along with recommendations to help organizations better manage wearable devices in the workplace. By adopting the recommended preventative measures to help increase the integrity, confidentiality and security of the data they collect, wearable devices can be worn by users in the workplace with less risk to the organization.

The remainder of this paper provides the motivation behind the whys and hows of recommended changes, and is organized as follows: Section 2 presents Fitbit device details. Section 3 explains the current security vulnerabilities associated with Fitbit smartwatches. Section 4 describes several threats aimed at Fitbits. Section 5 includes recommendations for improving Fitbit security and privacy protection. Section 6 concludes this paper.

2. FITBIT SMARTWATCH

Fitbit Inc. was founded in 2007 by Eric Park and Eric N. Friedman. These two men created Fitbit with the idea of bringing amazing experiences to fitness and health by using sensors and wireless technology that can be worn by the user [6]. The number of active users was reported to have grown to more than 25 million by 2017 [7]. The Fitbit app remains the number one health and fitness app in both iOS and Android markets in the U.S. [7].

Fitbits include sensors that collect important data that is eventually transmitted to the Fitbit server. The key sensors found in Fitbit smartwatches are accelerometer, barometer, gyroscope, photoplethysmography, and geolocation [8].

- **Accelerometer**: This sensor is used to determine orientations by measuring the acceleration along three orthogonal axes (X, Y, and Z). This sensor can determine if a Fitbit watch is horizontal or vertical and whether or not it is moving [2] [8].
- **Barometer**: This sensor is used to measure and calculate the steps taken upstairs by the Fitbit wearer. The barometer acts as a basic altimeter to process floor count information [8].

- **Gyroscope**: This sensor is used to measure the device's angular velocity along orthogonal axes (X, Y, and Z). Its main job is to improve the performance of exercise tracking features in the smartwatch. The gyroscope is similar to the accelerometer: both determine orientation, but the gyroscope sensor provides greater precision, measures angular velocity, and also can sense rotation [2] [8].
- **Photoplethysmography**: This sensor provides valuable information related to the wearer's cardiovascular system. It works by using low-intensity infrared light that is more readily absorbed by blood than the surrounding tissues. Changes in blood flow induce changes in the intensity of light that can be detected by the sensor. The measurement of light absorption is used to determine the wearer's heart beats per minute [9].
- **Geolocation**: This sensor enables a Fitbit to determine the physical location of the device (and thus its wearer) using GPS. The device uses an embedded GPS receiver when available. Devices without built-in GPS can use connected GPS from a mobile phone [10].

3. FITBIT SMARTWATCH VULNERABILITIES

In cybersecurity, vulnerabilities are weaknesses that can be exploited. This research explored Fitbit features that can create vulnerabilities for individuals and organizations, to increase awareness of potential security risks, and later to recommend mitigations for avoiding attacks.

Fitbit smartwatches collect a lot of data that can be considered private and potentially dangerous in the wrong hands. According to Fitbit's Legal Policy, Fitbit has labeled three categories of information their services receive/collect from user devices [11]:

- **Data**: Fitbits collect data such as steps, distance traveled, calories burned, weight, heart rate, sleep stage, and active minute. These data are synchronized to devices that transfer information to Fitbit servers.

- **Location**: Fitbits use/receive precise location data including GPS signals, device sensors, Wi-Fi access points, and cell tower identifiers.
- **Usage**: Fitbits collect information about a user's interaction with services, such as when a user views or searches content or installs software.

A compelling reason users must understand the vulnerabilities and attacks possible for their Fitbit smartwatches is because it is a wearable device. Wearable devices are by far the most personal computing devices at this time [1]. Wearable devices are the first category of information technology (IT) devices where there is not only danger due to the exposure of consumer data, but also the real potential to cause physical harm to wearers [1]. For informational purposes and to benefit consumers and companies, this paper lists vulnerabilities in the following sections.

3.1 Lack of Authentication and Physical Security Control

Authentication is the process of identifying an individual using a built-in mechanism in any system or device. Without authentication a hacker can access resources, including services and information, without being an authorized user of the hosting device. Currently, Fitbit smartwatches do not have a built-in security mechanism [2]. Without authentication, Fitbits pose a threat to an individual's personal information and location. The lack of authentication in these devices can lead a hacker directly to an entry point in a company's network for potential exploitation. If such a vulnerability is successfully exploited, it can compromise more information than what is housed on a single device; additional data stores may be penetrated via the network including personal data, passwords, emails, and digital media. This in turn can lead to identity theft and major attacks [2] [12] [13] [14] [15].

3.2 Disadvantages of Bluetooth Connections

Fitbit smartwatches are not capable of directly connecting to the Internet; first they must connect to a device that is Internet capable via Bluetooth Low Energy (BLE) technology [2] [15]. BLE has been adopted as the IEEE 802.15

standard for wireless personal area networks (WPANs) [15]. Thus, when attempting to obtain information from the cloud server, a requirement of most Fitbit devices is to first pair with a device via BLE [2]; that is, synchronization between Fitbits and smartphones/personal computers is performed over Bluetooth [16]. Because Fitbit smartwatches are not standalone devices, vulnerability is increased [2]. Non-standalone devices that have weak connectivity or connect via Bluetooth are prone to Man-in-the-Middle (MitM) attacks [2] [16].

Since Fitbits' main connectivity is Bluetooth, they inherit the same vulnerabilities that most Bluetooth devices have during times of communication. Fitbits are susceptible to various threats such as message modification, denial of service (DoS), and eavesdropping attacks [15]. Below is a detailed list of the different types of threats attributable to BLE communication that jeopardize the security of consumer information collected by Fitbits [15].

- BLE encryption key length requires a minimum key size of just seven bytes for encryption, much smaller and weaker than a full-length 128-bit key.
- BLE provides no user authentication.
- BLE lacks end-to-end security for all links.
- BLE with discoverability and connection ability procedures, makes the device always discoverable and connectable which makes such devices prone to attacks.
- BLE connections are remembered by Fitbit devices. If lost or stolen this makes them vulnerable to compromise.
- BLE authentication parameters are transmitted in clear text, making them susceptible to eavesdropping attacks [15].

3.3 Location/Tracking and Biometric Leakage

Location/tracking in wearable devices refers to the ability to fix the device's (and the wearer's) whereabouts at specific times [17] [18]. As mentioned in previous sections, there are two ways a Fitbit can acquire a user's location:

either by using a built-in GPS, or by pairing with and using a smartphone's GPS. Location/tracking can raise security concerns for individuals and organizations depending on how the information is used.

Fitbits also can track numerous exercises such as running, biking, swimming, or yoga [18]. The wearer can see real-time biometrics and statistics, including heart rate, calories, elapsed time and a post workout summary on their wrist. Not only does Fitbit track workouts, but also it automatically recognizes and records high-movement activities (i.e., those lasting at least 15 minutes) through its smart track feature.

All this information can be transmitted via Bluetooth to smartphone apps, which then send the data through Wi-Fi to cloud servers. In-transit data are at risk for compromise during each leg of the communication. Leakage of information such as heart rates and whereabouts could result in harm to the individual because it is so personal.

At a cost of only $75 USD, Symantec built a portable scanner from components like a Raspberry Pi minicomputer that could acquire location information from wearables [19]. This device was taken to athletic events and busy public spaces and was found to be able to track individuals [17].

4. CYBER-ATTACKS ON FITBITS

To exploit a vulnerability, an attacker must have a technique that can take advantage of a weakness in the system. Given the above itemization of their key capabilities and vulnerabilities, the following sections summarize significant attacks possible against Fitbit smartwatches. Many of these scenarios also can apply to other wearable devices.

4.1 Attacks Due to Lack of Authentication

Advanced persistent threats (APTs) are multi-stage cyber-attacks executed by sophisticated, well-resourced adversaries who target specific information in high-profile companies and governments, usually over a long period of time [20]. Many APTs are aimed at stealing financial information or intellectual property. Because they lack authentication [2], Fitbits can be used as a stepping stone by cyber criminals executing APT attacks.

For example, a tool like FitBite [20] can launch several attacks on Fitbit devices, such as data injection, DoS, and battery drain hacks [2] [20]. Fitbite consists of two modules: the tracker module reads and writes tracker data; and the base module retrieves/injects data from/to the tracker to upload it into the tracker owner's account on the web server [20].

4.2 Bluetooth Connection Compromise via Man-in-the-Middle Attacks

Bluetooth devices such as Fitbit smartwatches are prone to MitM attacks. In a typical MitM exploit, the attacker "sits" between two connecting devices. When the "client" device transmits information intended for the "server" device, the MitM attacker can intercept – and possibly modify – it before passing it along to the recipient [15] [21]. Similarly, when the server sends a response, the attacker can intercept/modify it before passing it to the client.

A challenge to executing a classic MitM attack when BLE communications are involved is Bluetooth can connect to only one device at a time, not two simultaneously. So a MitM attack against a Fitbit smartwatch that is communicating with a mobile app needs to involve two malicious BLE components capable of acting together. One malicious component connects to the mobile app and acts as a smart device; while the other malicious component connects to the Fitbit and poses as the mobile app. Once this connection is established, the two MitM devices use WebSocket protocol to enable two-way communications between them. As in a common MitM attack, the hacker can intercept – and modify if desired – any data sent between the Fitbit and the app over the BLE channel [21].

4.3 Attacks on Location Features via Social Engineering

When a Fitbit watch leaks information such as location data, it can potentially harm individuals and organizations. Other exploits that can occur based on Fitbit vulnerabilities involve social engineering – exploits that rely on the manipulation of humans. An attacker can trick another individual into bypassing normal security procedures, and use that lapse to gain access to a system, a network, or a physical location for financial gain or other nefarious purposes.

Location attacks pose a significant threat to individuals and organizations in terms of confidentiality, integrity, availability, and authenticity [2]. Malicious individuals can track users' locations or places they have visited to initiate phishing attacks, with an ultimate goal of delivering spyware or viruses [2]. As mentioned earlier, most Fitbit watches have a "connected GPS" feature that uses an on-board or connected phone's GPS to determine location [11]. This information may be sent to Fitbit servers and other third-party servers by apps on a Fitbit smartwatch user's phone. Because they are transferred via Bluetooth and Wi-Fi over smartphone networks, Fitbits' location data are vulnerable.

Fitbit location vulnerabilities have even created risk for the U.S. military. An article written by Liz Sly in the Washington Post brought attention to a Global Heat Map that is published to the internet by the GPS tracking company Strava. This interactive map reveals locations and movements of wearable device users who subscribe to the company's fitness services [22] [23]. Unfortunately, malicious actors can use this map to infer sensitive information about the locations and activities of Fitbit-wearing soldiers at U.S. military bases [22].

5. RECOMMENDATIONS FOR HARDENING FITBITS

Since Fitbit smartwatches have multiple vulnerabilities in areas such as authentication, Bluetooth connectivity, and location services, these devices potentially pose more harm to individuals and organizations than smartphones and laptops. Some recommendations are detailed below that can help mitigate key Fitbit vulnerabilities.

5.1 Educate Fitbit Smartwatch Users

Uneducated users can easily fall victim to social engineering, APTs, and other cyber-attacks that exploit the kinds of weaknesses pointed out in this paper. Because humans are consistently called out as the weakest cybersecurity link, an essential element of any wearable vulnerability mitigation strategy is to educate users about their devices.

This research reveals some key device features that Fitbit users should understand better, such as how embedded sensors work, the specific information they gather, and how attackers can exploit vulnerabilities in authentication and connectivity approaches. A significantly stronger security posture can be achieved simply by educating Fitbit users about best-choice settings relevant to security, particularly for location and Bluetooth.

5.2 Apply Multi-Factor Authentication

The more security layers/factors there are in place, the more hardened systems and data are against unauthorized access. Users have become accustomed to multi-factor authentication through their smartphones and laptops. But Fitbit smartwatches lack authentication mechanisms, presumably because there was more focus on functional design than security during their development [2].

Fitbits should integrate biometric security similar to smartphones. A biometric security solution can prevent unauthorized access by using unique user characteristics such as fingerprints, retina patterns, and facial recognition. The potential downside to this solution is increased cost. But considering the potential for Fitbits to leak PII, the expense of adding authentication functions seems to be a good long-term investment [24].

Besides security awareness and training, another tactic for safeguarding Fitbit users against APT attacks is to enhance authentication methods [14]. As discussed earlier, Fitbit watches do not have built-in authentications. Some mitigating measures that can be undertaken include disabling certain settings, turning off functions when not in use, and knowing which third-party apps have and enforce privacy policies, and which do not.

A multi-factor approach to verify the user's identity – for example, combining biometric security with additional methods such as a pin or a password – would correct for the current lack of authentication and render Fitbits less susceptible to some attacks [12] [13]. By using multiple factors to authenticate these devices, Fitbit users can avoid key vulnerabilities even if their device is lost or stolen. Collected information would be better secured for individual safety, as well as for organizations that allow Fitbit smartwatches on their premises [12] [13].

5.3 Use Near-Field Communication

There are some compelling reasons that should encourage migrating Fitbits from BLE to Near-Field Communication (NFC). The range of NFC is only about 4 centimeters; whereas Bluetooth can support connections of 30 feet or more. Because most Fitbits connect via Bluetooth, their pairing features expose them to a greater variety of potential cyber threats that exploit communication distance, including MitM and port scanners.

Bluetooth may have trouble dealing with interference when trying to send signals between devices, especially in crowded locations when there are several other devices nearby trying to communicate with the same systems. The proximity requirement for NFC device communication may help mitigate such interference while also limiting Fitbit vulnerability to the attacks mentioned above. Thus NFC-supported connectivity not only could help harden Fitbits against key cyber-attacks, but also make their information synchronization functions more robust [25] [26].

5.4 Create Use Policies and User Agreements

The pervasiveness of Fitbits in nearly every aspect of daily life introduces vulnerabilities in businesses, as employees increasingly wear these devices in the workplace. Organizations can deter some cyber threats by creating appropriate Fitbit use policies and user agreements. But first, organizations must understand the capabilities and vulnerabilities of Fitbit smartwatches. As mentioned in previous sections, military bases and governments exemplify organizations that need strong policies so that information will not be leaked or tracked via Fitbit wearers.

Use policies and user agreements related to wearable devices like Fitbits should minimally address consent to tracking and monitoring on-premises devices. To further prevent potential data leakage due to a lack of Fitbit authentication and other known vulnerabilities, employees might be forbidden from using certain Fitbit capabilities altogether – such as never connecting to the organization's network. Companies also should incorporate the other mitigation recommendations mentioned in this paper to help reduce the potential for wearable-enabled attacks.

6. CONCLUSIONS

The rapid adoption of Internet of Things (IoT) connected devices including Fitbit smartwatches in almost every aspect of life – from work, to school, the gym, and even during sleep – creates a climate where cyber-attacks can flourish. Individuals and organizations must balance their desire to be constantly sharing data and tracking activities through connected devices, against the security risks these devices can pose. The findings of this research should serve as a security awareness wake-up call to encourage individuals and organizations to understand, prepare for and prevent future attacks that leverage vulnerabilities in authentication, Bluetooth, and location features of Fitbit smartwatches and, in doing so, help to protect the confidentiality, integrity and availability of valuable information assets.

REFERENCES

[1] A. J. Mills, R. T. Watson, L. Pitt and J. Kietzmann, "Wearing Safe: Physical and Informational Security in the Age of the Wearable Device," Business Horizons, vol. 59, no. 6, pp. 615-622, 2016.

[2] K. W. Ching and M. M. Singh, "Wearable Technology Devices Security and Privacy Vulnerability Analysis," International Journal of Network Security & Its Applications (IJNSA), vol. 8, no. 3, pp. 19-30, 2016.

[3] J. P. L. Goh, "Privacy, Security, and Wearable Technology," Landslide, vol. 8, no. 2, pp. 1-8, 2015.

[4] "8 Security Threats Wearables Pose to Companies and Individuals," VIPRE Security News, https://www.vipre.com/blog/8-security-threats-wearables-pose-companies-individuals/

[5] "Health Solutions," Fitbit, https://healthsolutions.fitbit.com/wellness/

[6] "Who We Are," Fitbit, https://www.fitbit.com/about

[7] "Fitbit Community Grows to More Than 25 Million Active Users in 2017," Fitbit, https://investor.fitbit.com/press/press-releases/press-release-details/2018/Fitbit-Community-Grows-to-More-Than-25-Million-Active-Users-in-2017/default.aspx

[8] "Fitbit Privacy Policy," Fitbit, https://www.fitbit.com/legal/privacy-policy

[9] "Developer - Sensor Guides," Fitbit, https://dev.fitbit.com/build/guides/sensors/

[10] S. Cheriyedath, "Photoplethysmography (PPG)," News - Medical Life Sciences, https://www.news-medical.net/health/Photoplethysmography-(PPG).aspx

[11] "Geolocation (GPS) Guide," Fitbit, https://dev.fitbit.com/build/guides/geolocation/#monitoring-the-current-location

[12] A. Bianchi and I. Oakley, "Wearable Authentication: Trends and Opportunities," it - Information Technology, vol. 58, no. 5, pp. 255-262, 2016.

[13] J. Leonard, "Wearable Product Security: What you need to know," https://blog.nordicsemi.com/getconnected/wearable-product-security-what-you-need-to-know

[14] P. Chen, L. Desmet and C. Huygens, "A Study on Advanced Persistent Threats," B. De Decker and A. Z´uquete (Eds.): CMS 2014, LNCS, vol. 8735, pp. 63-72, 2014.

[15] S. Kaur, "How to Secure Our Bluetooth Insecure World!" IETE Technical Review, vol. 30, no. 2, pp. 95-101, 2013.

[16] M. Rahman, B. Carbunar and M. Banik, "Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device," https://arxiv.org/abs/1304.5672

[17] B. C. d. S. Cyr, W. Horn, D. Miao and M. Specter, "Security Analysis of Wearable Fitness Devices (Fitbit)," https://www.semanticscholar.org/paper/Security-Analysis-of-Wearable-Fitness-Devices-(-)-Cyr-Horn/f4abebef4e39791f358618294cd8d040d7024399

[18] T. Melamed, "An Active Man-in-the-Middle Attack on Bluetooth Smart Devices," International Journal of Safety and Security Engineering, vol. 8, no. 2, pp. 200-211, 2018.

[19] L. Eadicicco, "A New Wave of Gadgets Can Collect Your Personal Information Like Never Before," Business Insider - Australia, https://www.businessinsider.com.au/privacy-fitness-trackers-smartwatches-2014-10

[20] M. B. Barcena, C. Wueest and H. Lau, "How Safe Is Your Quantified Self?" Symantec, 2014.

[21] S. Curtis, "Wearable tech: how hackers could turn your most private data against you," https://www.telegraph.co.uk/technology/internet-security/10925223/Wearable-tech-how-hackers-could-turn-your-most-private-data-against-you.html

[22] L. Sly, "U.S. soldiers are revealing sensitive and dangerous information by jogging," Washington Post, https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?utm_term=.a226487de1fd

[23] S. Carter, "The Challenges and Benefits of Multi factor Authentication - MFA 101, Part 2," http://blog.identityautomation.com/the-challenges-and-benefits-of-multi-factor-authentication-mfa-101-part-2

[24] S. Vispute, "NFC Vs. Bluetooth: A Detailed Comparison," https://techspirited.com/nfc-vs-bluetooth

[25] Strava, "Strava Global Heatmap," https://www.strava.com/heatmap#7.00/-120.90000/38.36000/hot/all

[26] "Near Field Communication versus Bluetooth," http://nearfieldcommunication.org/bluetooth.html