Wearable Devices-FitBit

Sami ALosaimi

Abstract— the paper explains the wearable devices and how it works and how it connects. Also, the paper focuses on the security issues.

1 INTRODUCTION

Fitbit Inc. Is an American company based in Atlanta that produces products under the same name? The company is owned by Eric Friedman and James Park who founded it in 2007. Fitbit has many popular products to its credit. Some of the products include wearable gadgets including wireless devices, activity and fitness trackers among others. The Fitbit tracker was the first such product launched by the company. It tracks pulse rate, climbed steps, heart rate, sleep duration, and other fitness metrics.

The Need for tracking Fitness

Fitness tracking has become a very popular concept in the last decade. Though people had been keeping a check on their fitness and health for a long time, the trend has been rampant since the launch of Fitbit and other fitness trackers. A telephonic survey revealed that approximately 69% Americans maintain a record of at least one of the health indicators. Common indicators include diet, exercise, weight and various symptoms that could lead to a disease. First and then try to pronounce them together and compare.

The study also shows that people who have been suffering from chronic diseases are very conscious about their health and fitness indicators. Surprisingly, these individuals are as found to be more interested in knowing about health than other citizens. The study shows that approximately 68% individuals suffering from two chronic conditions closely monitor their health. Approximately 40% are those who suffer from at least one chronic condition. Only 19% are those who have repeatedly shown experience in tracking their chronic conditions, despite not suffering from any chronic conditions or diseases. These stats show just how serious they are about their health and safety.

An Insight into Fitbit Fitness Tracker

All Fitbit products feature a three-dimensional accelerometer that senses user's movement. This tracker keeps a track of steps the user takes. The data is then combined with other metrics to calculate the total distance walked. The wireless station receives data from the tracker and charge battery. Upon connected to a computer, the wireless base station will upload all the data to Fitbit website.

On the website, you'll find many features that'll help present an overview of your fitness. For instance, you can set your tracking goals for a specific duration or keep your diet activity in check. Moreover, you can also track your physical activity such as exercise and walk etc. Similarly, the device also tracks other movements such as floors climbed and the overall intensity and duration of the activity during the process. The data also shows how many calories a user burned during an activity which makes it a handy tool for fitness conscious people. Though there are many types of wearable fitness trackers available, increasing popularity and user-friendliness makes Fitbit perhaps the most sought after of all wearable devices in the world today. It is more affordable and sends your data to the website through an app in no time. There is an onboard wireless support that helps the device upload your data to your website account immediately as you take it. This way, you can keep a track of your fitness data and compare it with earlier statistics over time.

Fitbit users state that using the device has helped them monitor their fitness to a good degree. Fitbit is particularly good for people suffering from obesity, heart problems and diabetes. With its ability to compare different results simultaneously, the device has encouraged users to pay more attention to their daily diet and physical activities. Taking data once in a while and then continuing the same routine is not enough. Fitness experts urge the need of taking data and improving

over their existing performance. Users of Fitbit must calculate their daily routine such as diet, exercise, sleep patterns and make necessary changes wherever possible. Patients using Fitbit have been observed to gradually increase their physical exercises and manage diet routines within weeks. This helps them reduce blood pressure and sugar levels. Using Fitbit is all about taking the jumble of information and put it into actionable information.

Security Issues and Vulnerabilities Associated with Fitbit and other Wearable

Fitbit uses multiple sensors to collect the generated data of the wearer. Since Fitbit is small in size and lightweight, it lacks the capacity to store user data. Instead, it transmits the collected data through wireless transmission method. These are short range transmissions that carry the data to either the smartphone or a computer. Afterward, the data is transmitted to the app that analyzes the data and shows the results. Some apps also send a copy of the data to a cloud-based server that is hosted by device vendors. In some cases, these vendors offer more services such as detailed analysis to the users. It is obvious that this method of forwarding data can give way to security vulnerabilities. For instance, a vulnerability can surface when:

- The data is sent to the smartphone
- The data is sent to the vendor
- When data is stored in the cloud server

When Data is sent to the Smartphone

Like most fitness trackers, Fitbit sends the data to user's smartphone via Bluetooth. It is known that sending data over Bluetooth can cause security vulnerabilities such as data leakage and theft. The data remains vulnerable if appropriate security measures are not taken. A study noted that out of different fitness trackers tested, only two devices managed to adequately secure the data. All the rest fell short in providing desirable security to the data sent. Several problems surfaced during the process including:

- Lack of authentication processes between smartphone and fitness tracker
- Constant activity and visibility of Bluetooth connection
- Some devices lack encryption that gave way to open connectivity with any random Bluetooth device and shared the data

The study found that it is possible to connect with some fitness trackers and execute commands. This is possible with devices that have little or no data encryption methods at all. The study also explored the possibility to hack into a fitness tracking device and deliver a malware via an unencrypted Bluetooth port. Fortunately, only 17 bytes of malware code could be delivered. This proved that not fitness tracking devices could be hacked through a malware. However, Symantec researchers concluded that fitness trackers using low-energy Bluetooth connections can be hacked for tracking location. This is so because Bluetooth LE devices broadcast as signal make the device visible to nearby Bluetooth connections. These signals can be located by using Bluetooth scanners. They scanned LE Bluetooth devices and identified several signals.

When Data is sent to the vendor's website

Another common vulnerability occurs when the Fitbit sends the data to the vendor. However, this will only take place if the tracker is not properly secured. Fitbit properly secured the data before sending it over to the vendor's website. However, this was not the case with some fitness trackers. Some smartphone apps were found to have transmitted user login credentials as plain text. Suffice to say that they failed to properly encrypt the sent data. Sending unencrypted data is an open invitation to hackers. They can easily intercept the data and hack into the user's account. It allows them to steal or manipulate all the information as a result. Moreover, sending unencrypted data also can also result in Denial of Service, a common vulnerability that hackers often utilize to get hold to vulnerable accounts and data. In a DoS, the hacker attempts to prevent the user from accessing his account. This is done so by overwhelming the account with service requests.

When the Data is sent to the cloud server

Realistically, this type of vulnerability should not occur. However, not only is the data still vulnerable, it can be problematic in two ways:

- An unsecured cloud server could result in data breaches

- Cybercriminals often end up stealing and selling private data

Unfortunately, there are no known regulations that could prevent a hacker from selling private data. They find buyers for this information with ease. For instance, companies such as health insurance, marketers, third parties and employers are interested in buying this information. The irony is that the user remains unaware of all this.

Considering the increasing popularity of Fitbit among users in the last few years, several Fitbit accounts were found to have been compromised. The devices have been found to contain security issues in the software and tracking mechanism lately. Though these threats vary in nature, they all provide an opportunity for hackers to hack into your Fitbit.

Fortunately, none of these hacks were serious in nature and the company claims to be working on a fix. Isolated Fitbit accounts, e-mails, and passwords have been hacked and their personal information has been compromised.

Moreover, attackers have attacked accounts and have released information on the black market. Moreover, in some cases, hackers have managed to infect computers through specific vulnerabilities such as key logging malware. A key logging malware is a type of spying software that can record all entered information on your computer's log file. Though the file is generally encrypted, the malware can read through it and can read every detail you enter using your keyboard.

Tips for protecting your data

By now, it is apparent that fitness trackers can have vulnerabilities that cybercriminals can exploit. However, users can take the following steps to ensure their data remains secure. These are:

- Changing your device's name to an unrecognizable name, perhaps a code word if possible. The purpose is to make it difficult for trackers to track your device. For instance, change your device's identifiable name to an unidentifiable one.

- Before creating an online account for storing your personal data on the cloud server, use a very strong password. Your password should contain a mix of characters and numbers. The purpose is to make difficult for hackers to break it. Also, use different passwords and write them down for reference. This is important for users who use multiple accounts simultaneously.

- Take caution while accepting friends online and never share your personal information with people you don't know personally. Socializing is an important part of fitness tracker users. They often share their experienced with one another and exchange valuable tips among each other. Fitness trackers such as Fitbit provide facility to accept or reject friends, much like any social media forum. However, you should be careful in accepting friend requests from unknown people. You never know who you may be dealing with so take caution.

- Always read through the privacy policy and terms and conditions of your fitness tracker. This will clear things on how the manufacturer of your fitness tracker will use or limit your provided information.

- Keep yourself updated on any developing news about fitness trackers. Since they are relatively new to the market, you may find useful information on how to keep your account protected against any vulnerability.

There is little doubt that Fitbit is among the safest fitness tracking devices in the market. The company has done everything it could to protect client's information. They've released regular updates to keep vulnerabilities out of the loop. In doing so, the company published updated information on how to keep your account secure from hackers and spammers recently. You will find valuable information such as recovering and resetting the password, updating the software settings among others. There is updated customer support, updated security center, and security interpreting page is included.

4 REFRENCE

Friedman, J. (2016, March 1). Attack Your Attack Surface. Retrieved from https://www.skyboxsecurity.com/sites/default/files/Attack Surface Visualization.pdf

Checkoway, S. (n.d.). Comprehensive Experimental Analyses of Automotive Attack Surfaces. Retrieved from • http://www.autosec.org/pubs/cars-usenixsec2011.pdf

University of Washington

Heumann, T. (n.d.). Quantifying the Attack Surface of a Web Application. Retrieved from • http://testlab.sit.fraunhofer.de/downloads/Publications/heumann-quantifying_the_attack_surface_of_a_web_application-GI_Sicherheit_2010.pdf

University of Hagen

Manadhata, P., & Maxion, R. (2007, August 1). An Approach to Measuring A System's Attack Surface. Retrieved from • http://www.cs.cmu.edu/~wing/publications/CMU-CS-07-146.pdf

M. (n.d.). What is the Security Development Lifecycle ? Retrieved from https://www.microsoft.com/en-us/sdl/default.aspx