International Journal of Engineering Research
Volume No.6, Issue No.4, pp :209-210

ISSN:2319-6890 (online),2347-5013(print)
1 April. 2017

# A Comparative Security Analysis of Fitness Wearables

**Md. Alam, Mayank Saxena, Rachna Jain**
Department of Computer Science, Bharti Vidyapeeth's College of Engineering
mohammedalam607@gmail.com, mayu99712@hotmail.com, rachna.jain@bhartividyapeeth.edu

***Abstract -Fitness trackers capable of counting steps, measuring heartrates, quality and quantity of sleep and activities are gaining popularity these days. Fitness trackers not only track your activities but also keeps a record of your location very precisely. Data generated by these fitness trackers are used in court rooms and are capable of altering the outcome of a trial. Therefor it is very essential that the information produced by these fitness trackers are protected. In this paper we review eight of the most popular fitness trackers price ranging between 15$ to 150$ and check whether the data generated by them can be corrupted or not. Also we identified the flaws in the few most popular fitness trackers and propose the work that can be done to secure them.***

***Keywords: Wearable, fitness-band, healthcare, fitness-tracker, IoT, Wearable Security.***

## I. Introduction

According to a report by Forrester more than 20% of U.S. adults use a smart watch or fitness tracker on a daily basis. According to the report fitness Is the number one priority for the users. Fitness wearable market is ruled by Apple Watch, Nike Fuel, and Fitbit. It is also stated that market of fitness wearables will increase by 40 percent in next five years. The rise in popularity of the fitness wearables also attracted smart phone and wireless carrier companies. With increasing popularity of fitness wearables comes the concern for the personal data security. Whether the data collected by fitness wearables are secure and legit or not. Also the data collected by fitness wearables are used in court rooms and can decide the outcome of a trial [1,2]. Insurance companies are also providing benefits to their customers who chooses to share their fitness data with them [3]. In most of the fitness wearables, Privacy and Security concerns seem to be an afterthought and are not generally taken in account during the design and manufacturing stages of the fitness wearables. [4]–[7].

This paper contributes in the field as follows: This paper contains comparative systematic review of some of the famous fitness wearables and issues concerning the security of the personal data.

## II. Related work

Paul et al. discuss the privacy policies of Different Fitness Wearable manufactures, finding with whom manufacturers aspire to share the data produced and what privileges a consumer keeps over their own data. They found a number of disturbing statements concerning the ownership and viable treatment of user's data [8]. In 2013, Rahman et al. found some flaws in Fitbit's protocol of communication, e.g. unencrypted and unauthenticated data upload, permitting for easy data manipulation. They created fit Lock a "defence system" for the weaknesses discussed [9]. Zhou et al. monitored up on this effort by recognizing faults in Fit Lock, but did not suggested their own set of modifications to fix the above mentioned issues [10]

## III. Security and Privacy

### A. Data transmission

Mio fuse did not send any data to company server. The IMEI number to Xiaomi, the transfer of the mobile phone serial number to Basis, and the unexpected routine transmissions of fine-grained location data to Jawbone and Withings, were examples of transmissions of sensitive data that did not seem essential, or at least, for which the user is not properly informed.

### B. MAC Address perseverance

MAC address of almost each device remained same over the long period of time. We observed that only the Apple watch changes the Bluetooth MAC address whenever rebooted and after approximately at an interval of 10 minutes.

### C. Transmission Security

We observed that most fitness device's mobile application used HTTP to encrypt their communication with remote servers. These transmissions take place when for signing up, logging in, logging fitness data or any other application events. By choosing HTTP, the fitness tracker companies are helping consumers to get away with third party interference i.e. monitoring or tampering or modifying any data exchanged between user's mobile and company server. This security method does not employ in GARMIN CONNECT and WITHINGS HEALTH MATE which make them vulnerable to third party surveillance or modification.

### D. Data Tampering by "Man in the Middle attack"

A MITM attack is an attack where an attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

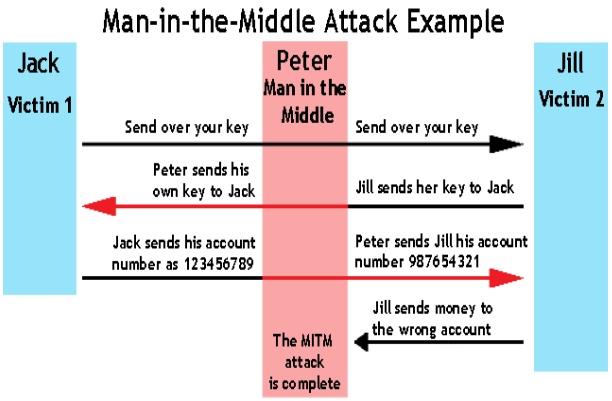
## I. Comparative Analysis w.r.t various security features

Comparative analysis of different security wearables on parameters such as Transmission Security, Data Integrity, Bluetooth Surveillance is shown in table 1.

Table 1 Comparative Analysis w.r.t various security features.

| Device | App | Transmission security | Data integrity | Bluetooth surveillance |
|---|---|---|---|---|
| Apple watch | Watch | Uses https, Certificate pinning | No test performed | LE policy |

| | | | | |
|---|---|---|---|---|
| Basis peak | Basis peak 1.14.0 | Uses https, Certificate pinning | No test performed | No LE policy |
| Fitbit charge HR | Fitbit 2.10 | Uses https | MITM test yet to be performed. | No LE policy |
| Garmin vivosmart | Garmin connect 2.13.2.1 | No https Besides signup/login | MITM test yet to be performed. | No LE policy |
| Jawbone UP 2 | Jawbone UP 4.7.0 | Uses https | MITM test yet to be performed. | No LE policy |
| Mio fuse | Mio go 2.4.4 | No user data sent | No test performed | No LE policy |
| Withings pulse O2 | Withings health mate 2.09.00 | Uses https, Security hole(android) | MITM test yet to be performed. | No LE policy |
| Xiomi mi band | Mi fit 1.6.122 | Uses https | MITM test yet to be performed. | No LE policy |


Man-in-the-Middle Attack Example
Jack
Victim 1
Peter
Man in the Middle
Jill
Victim 2
Send over your key
Send over your key
Peter sends his own key to Jack
Jill sends her key to Jack
Jack sends his account number as 123456789
Peter sends Jill his account number 987654321
Jill sends money to the wrong account
The MITM attack is complete

We observed that Garmin Connect did not use HTTPS for most application functions. In addition to not usingtransport security the application used OAuth 1.0 for user authentication.In practice, Garmin's decision to use OAuth 1.0 without HTTPS for its mobile applications enabledthird parties to collect user requests and subsequently modify them. Such modificationslet third parties inject false fitness data or even delete fitness events from a user's profile. It wasalso possible for this third party to alter a user's privacy settings, stated gender, or other profileinformation.

## Conclusion

In the course of our technical investigations into transmission security, data integrity, and Bluetooth privacy, we discovered several issues that confirm concerns about the potential uses of fitness tracking data beyond the typical case of a user monitoring their own personal wellness. The unique identifiers broadcast by all studied devices except for the Apple watch were fixed. These static identifiers enable third parties, such as shopping malls, to persistently monitor where fitness wearables are located at a given point in time. These findings confirm concerns relating to the privacy of Bluetooth emissions and geo locating fitness trackers more generally. Garmin Connect lack of HTTPS encryption exposed its customers to the risk their sensitive fitness data was being collected or tampered by unauthorized third parties, as did a security vulnerability in the Withings Health Mate application. Our findings confirm concerns about the potential for unknown parties to access fitness data. Finally, the fitness data generated by several wearable devices can be falsified by motivated parties, calling into question the degree to which this data should be relied upon for insurance or legal purposes. This confirms the concerns that people could fraudulently input device data are grounded in reality. Basic security claims hid the truth that two applications exhibited serious troubles in keeping the privacy of personal information in transfer over the internet network. Some diverse categories of sensitive information, usually in the form of unique identifiers that could connect fitness and biographical data to a single mobile phone hardware or single specific fitness wearable, were apparently collected by some fitness tracking companies. However, such identifiers were not necessarily made accessible to consumers. As a consequence of these inaccurate, or in some cases contradictory findings, consumers may be misled or confused about the real degree of security measures in place or extent of personal data collected by fitness tracking companies.

## References

i. *Hill, K.: Fitbit data just undermined a woman's rape claim. http://fusion.net/story/ 158292/fit bit-data-just-undermined-a-woman's-rape-claim/ (Accessed on November 21, 2015), 2015.*

ii. *Olson, P.: Fitbit Data Now Being Used in The Courtroom. http://www.forbes.com/ sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/ (Accessed on November 21, 2015), 2014.*

iii. *Bernard, T. S.: Giving Out Private Data for Discount in Insurance. http://www.nytimes. com/2015/04/08/your-money/giving-out-private-data-for-discount-in-insurance.html (Accessed on November 21, 2015), 2015.*

iv. *Orlando Arias, Grant Hernandez, and YierJin, "Privacy and security in internet of things: A case study on google nest thermostat," in Design Automation Conference, 2015, (Poster).*

v. *Grant Hernandez, Orlando Arias, Daniel Buentello, and YierJin, "Smart Nest Thermostat: A smart spy in your home," in Black Hat USA, 2014.*

vi. *O.Arias,J.Wurm,KhoaHoang,andY.Jin,Privacyandsecurity in internet of things and wearable devices," IEEE Transactions on Multi-Scale Computing Systems, vol. 1, no. 2, pp. 99–109, 2015.*

vii. *Jacob Wurm, Orlando Arias, Khoa Hoang, Ahmad-Reza Sadeght, and YierJin, "Security analysis on consumer and industrial iot devices," in 21st Asia and South Pacific Design Automation Conference (ASP-DAC 2016), 2016, pp. 519–524.*

viii. *Paul, G.; Irvine, J.: Privacy Implications of Wearable Health Devices. In: Proceedings of the 7th International Conference on Security of Information and Networks. SIN '14, ACM, NewYork, NY, USA, pp. 117–121, 2014.*

ix. *Rahman, M.; Carbunar B.; Banik, M.: Fit and Vulnerable: Attacks and Defences for a Health Monitoring Device. ArXive-prints, 2013.*

x. *Zhou, W.;Piramuthu, S.: Security/privacy of wearable fitness tracking IoT devices. In: Information Systems and Technologies (C*ISTI), 2014 9th Iberian Conference on. IEEE, pp. 1–5, 2014