Integrated Citizen Centered Digital Health and Social Care
A. Värri et al. (Eds.)

doi:10.3233/SHTI200711

Do You Know Who Is Talking to Your Wearable Smartband?

Andrei KAZLOUSKI[a,b,1], Thomas MARCHIORO[a,b],
Harry MANIFAVAS[a,b] and Evangelos MARKATOS[a,b]
[a] *Computer Science Department, University of Crete, Greece*
[b] *Institute of Computer Science, Foundation for Research and Technology, Greece*

Abstract. We study seven fitness trackers and their associated smartphone apps from a wide variety of manufacturers, and record who they are talking to. Our results suggest that some of them communicate with unexpected third parties, including social networks, advertisement websites, weather services, and various external APIs. This implies that such unanticipated third-parties may glean personal information of users.

Keywords. fitness trackers, wearable devices, security, privacy

1. Introduction

Having shipped more than 17 million smartbands during the first quarter of 2020, the smart wearable devices market is expected to reach more than 60 million devices per year[2]. The increasing trend towards an active lifestyle, and growing health concerns are likely to boost the sales of wearables, and to reach a much higher penetration in the worldwide population. Although the increasing use of wearables in general, and smartbands in particular, promotes healthier habits, it may have raised public concerns with respect to the privacy they provide. Such concerns are mainly related to the possible leakage of fitness data and other private information.

Health data. Wearable smartbands collect personal and fitness-related data that might include user's heartbeat, sleep patterns, habits, and the exercising routine. Additionally, sensitive data like age, height, gender, weight, and body fat can be inserted manually.

Other sensitive data. At present vendors store personal data of users on proprietary servers. However, since the capability for remote communication is there, apps may use it to contact not only the manufacturer cloud, but other third-party servers as well. During these communications various other sensitive information can be leaked, including location, IP and MAC addresses, an email address, and possibly the phone name/model.

[1] Corresponding Author, Andrei Kazlouski, E-mail: andrei@ics.forth.gr. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skodowska Curie grant agreement No 813162. The content of this paper reflects the views only of their author (s). The European Commission/ Research Executive Agency are not responsible for any use that may be made of the information it contains.

[2] https://www.tizenhelp.com/huawei-xiaomi-dominated-in-chinese-wearable-market-for-q1-2020/

Given the above concerns, we gathered a set of smartbands from various manufacturers, and investigated the following questions:

Who is talking to these smartbands as part of their operation? Or similarly, who are these devices talking to? Are they connecting only to the cloud of their manufacturer in order to permanently and securely store their data, or are they communicating with third parties as well? In the latter case, who are these third parties?

Related work. Previous works focused on privacy of fitness trackers, and on the data that are shared with third parties.

Contacting third parties. Sharing users' data with third parties is regulated by privacy policies. However, the associated terms and conditions tend not to be always clearly expressed [1]. Also, making it optional to read the agreement often induces users put less effort in understanding it [2,3]. Vague policies authorize vendors to legally sell personal data of users to third parties without their explicit consent.

Privacy of smartbands. A number of prior works have studied how the advance of wearables and ubiquitous data collection impacts privacy [4,5,6,7,8,9]. Mass surveillance of users has been studied in [4,6]. Some works [5,9] investigated how concerned people are about disclosure of their data. Lack of control over data by users have been reviewed in [7,8]. It is worth noting that privacy updates for modern wearables often emerge from non-academic research.

Unlike previous academic works discussing potential privacy risks, in this paper we aimed to analyze third-party services that are contacted in practice. We provide the following contributions: we analyze the entities that are contacted by seven variously priced wearable devices; we identify unexpected/undesired (from the standpoint of privacy) third parties that the bands communicate with; we provide guidelines for preserving privacy while retaining essential functionality of the fitness trackers.

2. Methodology

In order to determine what kinds of IP addresses, domains and ISPs communicate with the studied bands, we followed a three-steps pipeline.

Traffic Capture. Smartbands send data to mobile applications using Bluetooth, and apps send/receive data over the Internet. We utilized WireShark[3] to capture the traffic, and learn contacted domains. To analyze what data are sent, we set up a MITM Proxy[4]. Retrieval of domains and IP addresses. After capturing the traffic, we aimed to find the domain names of the servers the smartphone app talks to. We obtained URLs, and IP addresses from our MITM setup. In some cases, we utilized the SNI field of TLS. Identification of the domains' nature. Once we learned both domain names, and transmitted data, we set out to find what kind of business are these domains in. This final step turned out to be the most challenging. While for some domain names (e.g., graph.facebook) it is clear who the owner is, for others (e.g., plbslog.umeng) it is less obvious. To determine physical location of servers we employed Geoip[5]. To study origins of the domain names we utilized the Whois[6] service.

[3] https://www.wireshark.org/

[4] https://portswigger.net/burp

[5] https://geoip.com

[6] https://www.whois.com/whois/

3. Results

Table 1 illustrates third parties contacted by each smartband/app pair. Arbily Smartwatch (China). Arbily Smartwatch connects to VeryFitPro, a popular fitness app that counts more than 5 million of downloads (July 2020). VeryFitPro connects mainly to its API at the domain veryfitproapi.veryfitplus, which for Europe has servers in Germany.

Third Parties. The VeryFitPro app connects to the aliyuncs domain to upload profile pictures of the users, in case they decide to use one. Information about the user's phone is also sent to ido-ble-lib.cn-hongkong.log.aliyuncs - a server located in Hong Kong. In particular, when the app synchronizes with the band, a Zlib encoded file that contains information about the OS of the phone, the time zone, the phone name, and a timestamp is transmitted. This info might enable third parties to profile app's activity. To enable GPS tracking of user's path during exercise (walking, running, cycling) VeryFitPro contacts the amap domain. Amap API is a mapping service provided by Alibaba Group (China) which owns servers located both in China and the United States.

Table 1. Third parties that are contacted by the bands. Origin refers to the country of origin for ISPs. The Site column implies physical location of the server. Role describes why the domain is contacted (Social = Social Networks). For domain name * replaces .com; IdoBleLogs is the alias for the ido-ble-lib.cn-hongkong.log.aliyuncs.com domain. Ger = Germany; HK = Hong Kong; C = China (i.e. China Unicom).

App	Domain name	IP address	ISP	Origin	Site	Role
VeryFit	*IdoBleLogs*	47.244.67.196	Alibaba	China	HK	Logs
	abroad.apilocate.amap*	205.204.101.28	Alibaba	USA	USA	Location
	cgicol.amap*	198.11.136.99	Alibaba	China	USA	
	control.aps.amap*	140.205.230.4	Alibaba	China	China	
	restapi.amap*	47.246.74.109	Alibaba	China	USA	
MiFit	api.weibo*	114.134.80.166	HGC	HK	HK	Social
	cgi.connect.qq*	203.205.254.62	Tencent	China	HK	
	graph.facebook*	31.13.84.8	Facebook	USA	Austria	
	logs.amap*	203.119.211.252	Alibaba	China	China	Location
	abroad.apilocate.amap*	47.88.68.79	Alibaba	China	USA	
	apilocate.amap*	205.204.101.31	Alibaba	China	USA	
	restapi.amap*	47.246.74.104	Alibaba	China	USA	
	login.sina.com.cn	58.63.236.212	ChinaNet	China	China	Ads
	xtrapath2.izatcloud.net	52.85.156.111	Amazon	USA	Greece	
Samsung	app-measurement*	172.217.21.78	Google	USA	Ger	Analytics
Huawei	api.geetest*	54.77.192.2	Amazon	USA	Ireland	API
TBand	iwhop*	47.56.106.31	Alibaba	China	China	Weather
Wearfit	hmma.baidu*	111.202.114.42	C Unicom	China	China	Ads
	openrcv.baidu*	39.156.66.235	C Mobile	China	China	
	dxp.baidu*	39.156.66.180	C Mobile	China	China	
	plbslog.umeng*	203.119.214.123	Alibaba	China	China	
	iwhop*	47.56.106.31	Alibaba	China	China	Weather

Yoho	plbslog.umeng*	203.119.214.124	Alibaba	China	China	Ads
	ulogs.umeng*	203.119.214.124	Alibaba	China	China	
	log.umsns*	203.119.215.106	Alibaba	China	China	

Xiaomi Mi band 4 (China). MiBand 4 connects to the MiFit app (50 million downloads), developed by Xiaomi. The app mainly connects to api-mifit.huami, an Amazon hosted API domain that collects health data about users. The connected servers are located in Germany, if the app is used from Europe. However, if a user registers from the USA, the app will mostly share health information with American servers.

Third Parties. Similarly to VeryFitPro, MiFit also relies on Amap to track user's position during fitness activities. The correspondent IP addresses can be from Europe, China or Hong Kong. A number of requests are automatically sent to three popular social networks (Tencent QQ, Weibo and Facebook) regardless of whether the user is registered there. Moreover, a user consent for sharing data with these networks is never asked. QQ, for instance, is contacted with a plain text GET request that contains the phone name and the OS version in the query. Although this can be considered minor information, it still enables the social network to gather data about people beyond its userbase. Overall, the app talks to servers from a number of Chinese ISPs: ChinaNet Guangdong, Alibaba, Shenzhen Tencent.

Gear Fit 2 Pro (South Korea). Gear Fit 2 Pro is a smartwatch produced by Samsung which must be linked to Samsung Health. The app has been installed more than 1 billion times through Google Play Market, and it mostly connects to servers owned by Google and Amazon. Most of the domains that are contacted by the app belong to Samsung and can be considered "safe". Nevertheless, the amount of traffic that is generated for advertisement purposes, mainly towards dls.di.atlas.samsung, is quite consistent. Creating a large quantity of undesired traffic causes bandwidth and power consumption. Samsung Health utilizes an analytics service by Google.

Huawei Band 3 Pro (China). We used Huawei band 3 Pro with the Huawei Health application. The app has been downloaded more than 100 million times as of July 2020. The domains hicloud and dbankcdn (and others with similar names) are owned by Huawei. To execute its functions Huawei Health contacts servers in China, Germany, United States, and Ireland. In Germany it uses servers of T-Systems, in Ireland it communicates with Amazon servers, in China and USA it talks to Huawei and Alibaba IPs. Since Huawei Band 3 pro is endowed with an inbuilt GPS, there is no need for the app to contact third-party APIs for tracking user's location during training. To our surprise it also appears that Huawei Health does not contact any third-party ads services. Third Parties. Huawei Health employs a CAPTCHA service Geetest to prevent botting. Low-cost Bands. These smartbands (price <e15) include RoHs, M4, and Naxius. Due to the absence of dedicated vendor servers, the corresponding apps (Wearfit, Tband, and Yoho Sport) do not send away any health data of the users.

Third Parties. Since the mentioned manufacturers do not produce their own applications, they rent them from other companies. Thus, every entity contacted by these apps can be considered a "third party". Tband and Wearfit obtain current temperature in Celsius from iwhop. Wearfit and Yoho sport communicate with various servers of Alibaba for advertisement.

4. Discussion and Conclusion

It appears that the saying "if you are not paying for the product, you are the product" applies to fitness trackers: although the apps can be used free of charge, users are giving their data in return. Manufacturers aim to maximize their profit by collecting as much information as possible and eventually sharing it with third parties. Although no illicit activity emerged from our studies, once users accept the privacy agreement (which is mandatory in order to use the fitness tracker) they are likely to lose control over their own data. Moreover, it is often the case that the agreement does not even specify who are these third parties. However, privacy-conscious consumers are still able to protect their data from being uncontrollably shared. It is possible to restrict access of applications to particular domains by using mobile firewalls. Such services allow customers to block any connection to any domain, including advertisement and tracking services. Although this might cause the app to stop working properly. Alternatively, it is possible to utilize an open-source "jail break" application Gadgetbridge (https://github.com/Freeyourgadget/Gadgetbridge). This app allows users to use their smartbands without transmitting any data to vendors' servers. Currently it supports more than 30 popular models of wearables. With an immense number of various smartbands readily available, we expect the majority of them to contact "unexpected" services. We analyze traffic of seven commercial wearable devices. We show that their official mobile applications contact many unexpected or even "unwanted" third-party servers such as location services, advertisement and analytics providers, and various APIs. Every person who wears a fitness tracker on her wrist is likely "donating" private information to the device manufacturer. We recommend every privacy-conscious individual to study the privacy policy before purchasing a desired wearable to learn which sensitive data can be shared. In case of unacceptable policies, we suggest consumers to consider more transparent vendors. It is still feasible, however, to use the majority of smartbands without leaking sensitive data. Mobile firewalls, and/or dedicated "no-traffic" apps are able to restrict third parties from gathering private information. Note that in these cases some of the device functionality might fail.

References

[1] Balebako R, Shay R, Cranor LF. Is your inseam a biometric? evaluating the understandability of mobile privacy notice categories. CMU, Tech. Rep. CMU-CyLab-13-011.

[2] Acquisti A, Grossklags J. Privacy and rationality in individual decision making. IEEE security & privacy 2005; 3(1): 26–33.

[3] Steinfeld N. I agree to the terms and conditions:(how) do users read privacy policies online? an eyetracking experiment. Computers in Human Behavior 2016; 55: 992–1000.

[4] Hilts A, et al. Every step you fake: A comparative analysis of fitness tracker privacy and security, Open Effect Report. Available at: https://openeffect.ca/reports/Every_Step_You_Fake.pdf.

[5] Vitak J, Liao Y, Kumar P, Zimmer M, Kritikos K. Privacy attitudes and data valuation among fitness tracker users, in: International Conference on Information, Springer. 2018; 229–239.

[6] Ball K, et al. Big data surveillance and the body-subject. Body & Society 2016; 22 (2): 58–81.

[7] Crawford K, Lingel J, Karppi T. Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. European Journal of Cultural Studies 2015; 18 (4-5): 479–496.

[8] Peppet SR. Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. Tex. L. Rev. 2014; 93:85.

[9] Raij A, et al. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. SIGCHI Conference on Human Factors in Computing Systems, 2011: 11–20.