Are mHealth apps secure?  
A case study

Chiara Braghin  
Università degli Studi di Milano  
Dipartimento di Informatica  
Email: chiara.braghin@unimi.it

Stelvio Cimato  
Università degli Studi di Milano  
Dipartimento di Informatica  
Email: stelvio.cimato@unimi.it

Alessio Della Libera  
Università degli Studi di Milano  
Dipartimento di Informatica  
Email: alessio.dellalibera@studenti.unimi.it

Abstract—mHealth applications are becoming increasingly widespread since they have the potential to reduce the cost of health care by favoring self-management of chronic diseases or to improve fitness activities. By their very nature, health applications collect and manage health sensitive data, therefore several concerns exist about how privacy, security, and confidentiality are handled. In this paper, we analyze the security issues of mHealth apps from two different perspectives: first, we highlight the security and privacy requirements on health data defined by data protection laws such as the General Data Protection Regulation (GDPR) in the EU, or the Health Insurance Portability and Accountability Act (HIPAA) in US. Then, we consider the security issues from a technological point of view, discussing how the app may protect user data. However, by analyzing a fitness app, we show that, at the moment, none of the well-known practices to protect data is followed, thus often mHealth apps are insecure.

1. Introduction

In recent years, there has been a proliferation of mobile health (mHealth) applications on smartphones and other portable devices. The World Health Organization (WHO) defines mobile health as “Medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants PDAs, and other wireless device”. More specifically, mHealth applications are programs that use smartphones inbuilt tools, such as the Global Positioning System, accelerometer, microphone, speaker, and camera to automatically detect and measure health-related behaviors. In order to measure and upload physiological data, a number of applications may also synchronize wirelessly with other wearable devices, such as wristband sensor, heart rate sensor, belt sensor, shoe sensor, glucometers, blood pressure cuffs or more recently, smart watches or smart clothing with wearable sensing technologies. Moreover, the information transmitted from the wearable device to the smartphone can be archived and analyzed locally in the phone, or remotely in a cloud environment. According to [1], there are currently over 97,000 health and fitness related mobile apps on Google Play and Apple App Store, with 4 million downloads per day, and with a year-over-year growth of 40%.

mHealth apps can be categorized according to their functions into two main groups: the first group includes the general health apps focusing on self-monitoring physiological markers relevant to a person health status, while the second group includes the fitness apps intended to encourage physical activity and healthy diets and to provide physical activity guidelines. Depending on the data collected, mHealth applications may cover a wide range of uses, including patient health and fitness self-management tools, remote and continuous monitoring of patients by caregivers and healthcare experts as well as by the relatives of the patient, reminder systems improving glycemic control in patients with diabetes by prompting the users to take medications and check their blood glucose, symptom monitoring in asthma and heart disease, supporting smoking cessation, an effective source of health information, helping to monitor, improve ad manage fitness activities, weight goals, diet, pregnancy and sleep. Doctors may use the health data transmitted from the patient’s monitoring devices to provide remote consultations or in their research works, or for medical education and training. Nursing staff and pharmacies may use the medical prescriptions issued by doctors for dispensing the required medicine.

A common belief is that mHealth apps have the potential to reduce the cost of health care in a period in which many countries are facing the problem of an aging population with chronic diseases such as obesity, diabetes, high pressure by encouraging healthy behaviors to prevent or reduce health problems, and by supporting chronic disease self-management that may reduce the number of healthcare visits. For now, the efficiency of mHealth applications has been evaluated in a variety of domains, including different clinical areas and countries. The results confirm the effectiveness in improving clinical outcomes. As a consequence, some insurance companies are now using applications data to lower premiums [2]. They are also used for the health care delivery in resource-limited settings [3].

However, several concerns exist about privacy and security in mHealth applications, since they could contain highly personal information, such as social interactions, location, emotional status, blood type, fingerprints and DNA profile,
or other potentially sensitive health conditions [4], [5] that are possibly stored on and transferred to the cloud. The security concerns associated with mHealth sensing are a limiting factor for their widespread adoption.

The objective of this paper is tree-fold: first, we investigate if and how mHealth application are affected by the current regulations on data protection. Then, we discuss how to achieve the necessary minimal security and privacy requirements by highlighting the security and privacy issues that must be faced when dealing with mHealth apps, both as a user or as a developer. Finally, we end showing how, despite there are possible secure solutions, in practice many apps face security problems mostly due to bad implementations and/or poor privacy-awareness of users.

2. EU and US Data Protection Regulations for Health Data

The EU General Data Protection Regulation (GDPR) [6], replacing the old directive on the 25th May 2018, and the US Health Insurance Portability and Accountability Act (HIPAA) [7], published in 1996 and updated frequently afterwards, define the legal framework for health data processing in Europe and in the United States, respectively. In particular, they specify the requirements on the collection, processing and storage of sensitive data. The key issue is whether health data is to be considered sensitive since one of the pre-requisites for data protection regulations applicability is the need to understand if an application manages (collects, stores, shares) health sensitive data.

2.1. GDPR

The most important law in the EU Data Protection regulatory framework is the General Data Protection Regulation - GDPR, which calls for the harmonization of the rules on the protection of EU citizens’ data (contrary to what the old directive 95/46/EC did).

2.1.1. Definition of Health Sensitive Data. According to art. 4, par. 15 of the GDPR, “data concerning health” are defined as “personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status” and they may be considered as a sub-category of Personal Data. Despite the formal definition, still grey-areas apply, like in the case with well-being data (e.g., physical activity) and leave room for subjective interpretations. For this reason, the definition provided by the GDPR is further explained by the Art. 29 Working party, the EU body with advisory status on data protection matters, which allows to identify situations in which personal data can be considered as Health Data [8]:

- **raw data**, i.e., data collected by apps or devices, that can be used, independently or in combination with other data, to draw conclusions about an individual’s actual health status or health risks;
- **data that allow to deduce health status**, i.e., data collected via an app or a device regardless of the accuracy, legitimacy or adequacy of the deduction.

Therefore, when dealing with an eHealth app, it is essential to define the type of data it collects, since different data bring about different legal (and technical) challenges. Examples of health data that can be easily labelled as sensitive are heart rate (ECG), weight tracking, blood pressure, healthcare payments, step counts, heartbeat tracking, diseases and many others.

On the contrary, the case of a fitness app counting persons’ steps must be analysed in depth: if the app is not used in a medical context and data cannot be combined with other data, then the collected data is not considered neither health nor sensitive data. However, if data is combined with other data-sets, such as heart rate measurements done by the app, or it is used to assess persons’ ability to perform stressful activities, than it can reveal sensitive (and discriminating) activities, and thus it has to be considered as health sensitive data. A consequence is that lifestyle and well-being apps most of the time need to be GDPR-compliant.

2.1.2. Key aspects of the regulation. The main security and privacy requirements within the GDPR with respect to the implementation of an mHealth app are:

- **Explicit consent**: “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”, i.e., the app must request consent to collect, use and move data on an informed basis. The app must also state clearly which are the permissions it requests.
- **Right to be forgotten**: users may request to have all their data deleted.
- **Mandatory data breach notifications**: the authorities and users must be notified of data leaks within 72 hours.
- **Privacy by Design**: Privacy and data protection must be a key consideration from the start and throughout the full project lifecycle. The techniques to be used should include: “encryption and pseudonymisation of personal data; the ability to restore personal data availability in the event of a security incident or technical issue in a timely manner; ensuring ongoing confidentiality, integrity, and availability of data processing systems and services; establishing a process for regular security testing and assessment of the effectiveness of security practices and solutions in place”. Moreover, under the new regulations, any company or individual that processes or handles the data will be responsible for its protection. This
A broader scope: any company either based in the EU or which deals with any data involving EU citizens or organizations is required to comply with GDPR, no matter where the company is based or where data processing takes place.

2.2. HIPAA

HIPAA is the acronym for Health Insurance Portability and Accountability Act, an American legislation of 1996 aimed at improving the efficiency and effectiveness of the health care system in the U.S. It provides a baseline protection for personal health record and every business processing electronic Protected Health Information (ePHI) within the US need to comply with it.

2.2.1. Definition of Health Sensitive Data. HIPAA is composed of four main parts, called rules (some added in the years thereafter to 1996 by the HHS, the U.S. department of Health & Human Services). Among them, the Privacy Rule defines what has to be considered protected health information (PHI) in the US, i.e., “information that relates to the past, present, or future physical or mental health or condition of an individual, which identifies the individual and that is transmitted or maintained by electronic media or in any other form or medium”.

That is, protected health information is any information in a medical record that can be used to identify an individual including: medical records, billing information, health insurance information, and any individually identifiable health information. Health information that is not considered PHI includes data such as: calories burned, steps taken, or distance covered.

So how do you know if you are dealing with protected health information (PHI) or consumer health information? If your device or application currently shares or will share the user’s personal health data held in the app or device with a covered entity such as a doctor, then you are dealing with protected health information. On the contrary, if you are building a wearable device or application that collects the user’s personal health information, but do not plan on sharing it with a covered entity such as a doctor at any point in time, then you do not need to be HIPAA compliant and do not violate the HIPAA Privacy Rule.

2.2.2. Key aspects of the regulation. The four main parts composing the HIPAA are the Privacy Rule, the Breach Notification Rule, the Enforcement Rule and the Security Rule. The necessary disposition aimed at achieving security are contained in the Security Rule, which “establish[es] a national set of security standards for protecting certain health information that is held or transferred in electronic form”.

Also in the case of HIPAA there are some grey areas: for example, they are generally considered not applicable or transferable to cloud computing environments. Recently, the security requirements defined by HIPAA in the Privacy Rules when dealing with mobile devices have been extended to: (i) the transmission of collected data has to ensure integrity and confidentiality. (ii) Data is then maintained on a remote server where secure storage mechanisms are essential. (iii) Finally, data access should be guaranteed only to authorized people such as doctors, who use it to monitor the patient’s condition.

3. How to build secure mHealth Apps

In order to achieve the necessary minimal security and privacy requirements and, as a consequence, to be compliant with the current regulations discussed in the previous section, mHealth applications have to:

1) secure the data during the communication between the (possible) external sensor and the phone, and during the (possible) transfer to a cloud environment;
2) secure the data (and processing) inside the phone and in the cloud environment;
3) be transparent on how data is managed (collected, stored and transferred) and by whom.

In this section, we analyse and further investigate these security issues in the context of mHealth apps, then we suggest possible solutions based on the current techniques available, finally, we show how in practice, from a number of recent studies, the actual mobile app ecosystems is far from being secure.

3.1. Confidentiality and Integrity of mHealth data during the transmission

Security issue: In a wireless network, an adversary can observe the transmissions of a specific device and he can infer some information about the data being transmitted, or on the device transmitting the data, based on the address in the transmitted packet, or on other identifying information in the packet, such as the size of the packet, or the timing of the packet sequence. Moreover, if the protocol does not support any form of cryptography, the adversary may also be able to modify the data being transmitted.

Possible solutions: Security issues affecting data communications span over three layers: network, transport, and application. There exists a number of protocols for the WiFi environment [9] providing security properties ranging from data confidentiality, where an adversary should not be able to learn the contents of the underlying data in the packet, to data authenticity, where an adversary should not be able to forge a packet without being detected, data integrity, where an adversary should not be able to modify a packet without being detected, and finally to unlinkability, where the adversary should not be able to link different packets sent from/to the same node.

Moreover, there have been also some attempts to make the protocols energy efficient without compromising their
security or privacy properties [10], [11], since they are often used by low-power sensors. Bluetooth Low Energy (BLE) [12], which is rapidly becoming one of the most common wireless standards in use today, implements various security features, such as a pairing method to securely exchange cryptographic keys and a protocol to transfer data encrypted using AES-CCM cryptography.

**In practice:** A study of the Privacy Rights Clearinghouse [13] on 43 paid fitness applications found that only 13 percent of them encrypted all data between the app and the developer’s website. In [14], the author reviewed the security and privacy policies for the 110 apps included in a study of sensitive data sharing by mobile apps. He focused on what, if anything, those policies said about the use of encryption for data in transit. Among the reviewed apps, many of the accessible privacy policies contained general language saying that security measures would be used but did not specifically promise that encryption would be used, a limited number included language implying that the apps encrypted some types of data in transit, five said nothing about security, and one policy affirmatively stated that encryption was not used.

### 3.2. Securing data in the cloud or in the phone

**Security issue:** mHealth data should be **securely stored** in the cloud or in the mobile device, and only be accessed by **authorized users**.

**Possible solutions:** Secure data storage consists in the use of cryptographic algorithms to ensure both the confidentiality and the integrity of data.

In general, mechanisms to avoid unauthorized accesses are based on authentication of the user with the device or the cloud service, based on credentials such as username and password, however various attacks such as offline/online password guessing can threaten the authentication mechanisms in place. Techniques such as two-factor authentication can be used to overcome this problem.

**In practice:** In [15], a number of existing mHealth apps have been analyzed against the most common mobile apps vulnerabilities defined by OWASP in 2014. The analysis detected safety flaws in the Apk code, which can trigger threats over user’s data and over the information recorded into the server, mainly because of “Insecure Data Storage”.

### 3.3. Transparency on the usage of data

**Security issue:** Many companies have significant commercial interests in collecting clients’ private health data and sharing them third parties such as with insurance companies, research institutions or even the government agencies. From the user’s point of view, third party use of personal health information could lead to possible employment discrimination, loss of insurance coverage, higher insurance premiums or other privacy intrusions.

**Possible solutions:** Mobile applications should improve transparency for end users about their commercial data practices of mobile applications that collect, store and transfer personal information by presenting in formation in effective privacy policies.

End-users should also become aware of the importance of reading privacy policies in order to have control over their data.

Developers should also minimize the number of permissions that their applications request in order to make the applications less vulnerable to external attacks and to reduce the risk of over-privileged applications.

**In practice:** According to some empirical analysis of a large amount of the most frequently rated and commonly used applications for iOS and Android, most applications did not have a privacy policy [16], [17]. When present, the policy either did not focus on the app but on the services offered by the developer, or required college-level literacy, or did not adequately address the purpose of collection, transfer, storage and destruction of user’s data, and who exactly the information was shared with, or which specific permissions were given to the application.

In 2014 the US Federal Trade Commission (FTC) published an analysis of 12 popular mHealth applications [18]; they found that the applications were sending the device’s screen size, device model, and language setting to 76 different third parties, whereas only a subset received exact information like the phone’s Unique Device Identifier (UDID), the phone’s media access control address (MAC address) and its International Mobile Station Equipment Identity (IMEI), or users’ personal information (i.e., not only users’ running routes, eating habits, sleeping patterns, and the cadence of how they walk, but also gender, geo-location and zip codes).

The paper [16] analyzed the 600 most commonly used apps and found that only 183 (30.5 percent) had privacy policies. In addition, the privacy policies that were available did not make information privacy practices transparent to users, require college-level literacy, and were often not focused on the app itself.

On the other hand, a survey of 584 university students indicated that the majority of mobile device end-users do not completely read privacy policies, although they would be concerned if their location is shares with a third party [19].

### 4. Case Study: a Fitness Tracker

Although, as shown in the previous section, the growth of the mHealth market fostered an emerging interest in studying their security and privacy issues, none of the cited studies analyses the potential of the Bluetooth Low Energy protocol. For this reason, we decided to analyze a fitness tracker using the BLE protocol to communicate and synchronize with the mobile app.

The fitness tracker we analyzed is a valid alternative to the best-known brands such as Fitbit, Garmin, Polar, etc. since, at a lower price, it gives a large set of functionalities: it collects distance traveled, calories consumed, heart rate, hours of sleep, and, by using an app installed on the
phone, it allows to receive different notifications (e.g., from Whatsapp, Facebook, Skype, etc.) and to see incoming calls.

In our analysis, we analyzed the app with respect of some of the aspects highlighted above. In particular, we followed three main steps:

1) Analysis of the permission of the app and of its privacy policy;
2) Static analysis and inspection of the code;
3) Analysis of the BLE traffic between the fitness tracker and the smartphone.

The smartphone we used for the test is a LG-G3 (LG-D855) running Android 5.0.

4.1. Analysis of the Privacy Policy

The privacy policy is of dubious validity since the security and privacy issues are not explicitly stated. For example, it is not specified which data is shared with a third-party, or if and when it is encrypted.

4.2. Static analysis of the App

The objective of this phase was to understand the behavior of the app and to highlight possible vulnerabilities by examining the code. In particular, we focused on: (i) discovering possible sensitive information within the code; (ii) locating the code fragments building the BLE packets; (iii) detecting accesses to log files and eventually activating them.

The app code was not obfuscated, thus we used jadx-gui [20] and Bytecode Viewer [21] to decompile and view the code, class by class. We discovered that the BLE protocol was not used properly, leading to a number of security flaws, as described in the next section.

4.3. Analysis of the BLE traffic

During this phase, we used an Ubertooth One antenna to capture the traffic and Wireshark to analyze it. The code analysis previously performed helped us in understanding the traffic. We found a number of vulnerabilities that are not due to the BLE protocol itself, but by the fact that none of the security mechanisms provided by the protocol have been used. The vulnerabilities are discussed in the following subsections.

4.3.1. Non-encrypted communication. The traffic analysis confirmed what we noticed by looking at the code: the communication is not encrypted, thus data confidentiality is not guaranteed. In fact, by passive eavesdropping, it is possible to read all the packets transmitted. For example, after enabling the notification option, we verified that, in the case of a Skype message, both the name of the sender and the content of the message were transmitted in clear. In Figure 1, we show part of the content of a Skype massage notification intercepted with Wireshark, where we highlighted the name of the sender of the message that is transmitted not encrypted.

In case of a phone call, either the number or the name of the caller -if the incoming number was recorded in the Contact list of the smartphone-, are transmitted in clear and shown in the display of the fitness tracker.

It is also possible to execute an active Man-in-the-Middle attack and modify the data, thus also data integrity is not guaranteed. In order to execute a MiTM attack on a Skype notification, we configured a Burp proxy intercepting the packets. In Figure 2, we show the original content of the message (i.e., the string Test, encoded as 0x54657374) and the content after the attack (i.e., the string Ciao, encoded as 0x4369616F).

4.3.2. Missing authentication. We also found that, during the communication between the tracker and the smartphone, no user authentication is required. As a consequence, any smartphone nearby can connect to the fitness tracker. Once connected, the malicious device may send arbitrary messages in place of the legitimate user.

4.3.3. Tracking. Since all BLE packets include a device address, it is possible to track the BLE device as it is moving and communicating, unless it changes its address periodically. BLE adds the ability to periodically change the address, but such a feature is not used by the fitness tracker we analyzed: during all the tests the address of the device has never changed, thus the device can potentially be tracked.
5. Conclusion

Mobile health (mHealth) applications are currently widely spread among smartphone users. Despite the warm welcome from users, mHealth apps have raised a number of concerns on the way they manage possible sensitive and private information such as health data.

In this paper, we investigate from two different points of view the security issues of mHealth apps:

- On one side, we analyze how current regulation (the General Data Protection Regulation in the EU, or the Health Insurance Portability and Accountability Act in US) protect the user and his data, thus giving a set of requirements that app developers must satisfy in order to comply.
- On the other side, we point out which are the critical parts of the applications and how the protocols and cryptographic techniques currently available can be used to guarantee their security.

We also analyzed a fitness app and came to the alarming conclusion that still many apps do not meet the expected standards for security and privacy, thus endangering their users’ sensitive personal data.

References


