Transforming Healthcare with the Internet of Things
J. Hofdijk et al. (Eds.)

doi:10.3233/978-1-61499-633-0-41

Analyzing Privacy Risks of mHealth Applications

Alexander MENSE [a,1], Sabrina STEGER [a], Matthias SULEK [a], Dragan JUKIC-SUNARIC [a], and András MÉSZÁROS [a]
[a] *University of Applied Sciences Technikum Wien, Vienna, Austria*

Abstract. Mobile health applications are expected to play a major role for the management of personal health in the future. For this purpose, the apps collect a lot of sensitive data from sensors or direct user input, combine it with automatic data such as GPS location data, store it locally and pass it on to web-platforms (often running in a public cloud), where the information can be managed and often shared with others in social networks. However, it is usually not transparent for the user how this sensitive information is handled and where it goes to. This paper shows the result of the analysis of mobile health applications regarding the handling of sensitive data especially with respect to transmission to third-parties.

Keywords. Mobile Health, Security, Privacy

Introduction

Smartphones, tablets, and mobile applications/apps are taking over our daily lives more and more. People are getting more and more addicted to their smartphones. With the help of modern features such as GPS tracking, the smartphone stores a lot of information about us, e.g. where we live, where we sleep, where we work, etc. Almost every app collects a certain amount of personal information about the smartphone user.

Among millions of apps, there are thousands of different mHealth apps, which are supposed to help us lose weight, track our fitness level, or create diet plans. Many of these apps seem to be every useful as personal health assistant, but they actually handle a lot of sensitive and private information that requires appropriate secure handling to protect privacy.

Wu-Chen Su [1] reviewed existing relevant research about smartphone applications in the eHealth domain and identified a set of pertinent challenges. One of these is about security and privacy concerns, which have to be further explored and discussed by researchers. This paper presents the results of the technical analysis of mHealth applications running on Android regarding privacy and security risks.

1. Methods

The evaluation process involved reviewing mHealth applications by primarily analysing data sent over a network communication between the applications and the

[1] Corresponding Author.

Internet. A set of selected ten free applications out of several hundreds available in the "health and fitness" category was systematically selected to represent a broad range of personal health functionalities: personal health record, self-management, calorie counter and diet plan, healthy living and health promotion (activity and fitness tracker, workout, and sports), and medication management.

To provide uniform parameters for every application, a specific test environment made of one specific device was used. Apps were tested on an Android emulator based on a VirtualBox called Genymotion (https://www.genymotion.com). It can emulate specific devices, thus making it a good choice to test mobile applications. The test environment was set up for a Google Nexus 4 device with Android 4.3. To get access and for testing purposes, a Google test account has been created.

Examination and analysis of the data traffic between mobile applications and the internet was done with a proxy which worked like a "man in the middle attack" (operated on a laptop with Windows OS). Furthermore, the proxy was also able to intercept SSL encrypted traffic. The proxy therefore dynamically creates a certificate for the server and signs it with its own root certificate, which is needed to be installed as a trusted certificate on the mobile device. With this configuration, it is possible to debug secure (SSL) communication as well. The test environment is shown in Figure 1.

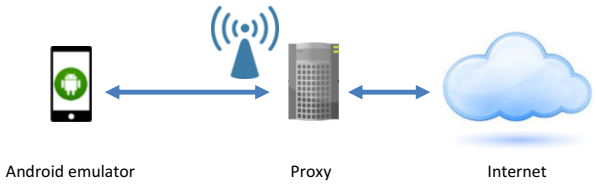

Figure 1. Test environment.

Mobile applications were used according to the intended standard use. They were installed from Google play store, necessary registration and login was done with a test user, and all offered functions were used.

Data collected by the mobile applications were analysed including user input (e.g. name, gender, health data …) and background information (e.g. GPS, device identification, contact data …). Furthermore, it was investigated whether the applications encrypt the traffic and with how many different domains they exchange information.

2. Results

In a first step, the permissions required by the applications were examined. In almost all cases, users have to grant a broad range of permissions including for instance in-app purchases, access to identity information, contacts, location, photos/media/files, camera, microphone, Wi-Fi-connection information, and Bluetooth connection information.

In a second step the network traffic was analysed. 90% of the evaluated mobile applications communicate with the application developer-controlled website and/or with third-party domains. In fact, only one application did not transmit data at all, but stores it in an unencrypted csv-file located on the SDcard which can be easily accessed and read by any other application or malware.

2.1. Communication with the developer-controlled website

Last year, Symantec [2] published that 20% of a set of analysed tracking applications (not limited to health) transmitted user login credentials in clear text. In 2013, Lie Njie [5] analysed mobile health and fitness applications and discovered that only 15% of them encrypted communication with SSL to the developers' website. Furthermore, Lie Njie [5] found that none of the applications sent the data to third-party advertisers using an encrypted SSL connection. In contrast, in our setup, 100% of the evaluated applications use encrypted (SSL) communication with the developer-controlled website. If applications use the HTTPS protocol it makes it harder to intercept data – but not impossible. By installing a man in the middle certificate it was possible to intercept the traffic of all of the applications, which means none of the applications does appropriate certificate checks and certificate pinning.

2.2. Communication with third party (advertising, analytics) sites

Eighty percent of the analysed free mobile applications contact third-party websites for advertising and analytics. The communication with the advertising sites occurred mainly unencrypted. One of the analysed applications sends also "usage data" in plain text to third-party advertisers after e.g. measuring fitness activities (see figure 2).

```
os=android&model=genymotion google nexus 4 - 4.3 -
api 18 - 768x1280&keywords=Run,run,
jog&oauth_key=5482,5410,&os_ver=4.3&locale=en_US&did
=43bc618c5de25126d5309ec7bda26b2f&postal_code=8783&w
orkout_pace=0.0&age_group=25to34&workout_time=4&gend
er=female&carrier&user_id=64422724&workout_heartrate
=0&workout_calories=0&workout_distance=0.0&workout_s
peed=0.0&make=genymotion&app_ver=3.5.1&app_store=goo
gle.
```

Figure 2. Sending usage data.

Another application transmits the GPS location (latitude and longitude) unencrypted to a third-party advertising site.

On the other hand, it is not transparent to users how much additional data regarding the usage of the app and the mobile device is collected and sent to third-party sites for analytics purposes. This form of data collection is known as behavioural tracking [5]. Ninety percent of the analysed applications provide such information to different sites. While Symantec examined a self-tracking application which contacted 14 domains [2], in our tests the number varied between two and ten different domains. Many different URLs had been identified: admob.com, appsfyler.com, flurry.com, fiksu.com, google-analytics.com, localytics.com, kiip.me, rubiconproject.com, crashlytics.com, newrelic.com. One application sends the data even unencrypted to http://data.flurry.com, while all others use encryption also to transmit analytics data.

Ninety percent of the inspected apps transmit more information than what is necessary for the proper running of the app, e.g. users' location (GPS), android version, phone information etc. (figure 3).

Figure 3. Sending information to analytics sites.

It is obvious that applications contact remote servers for some of their functionalities (to get images and marketing advertisement), nevertheless the number of contacted third-party analytic websites is surprisingly high.

2.3. Device information

The IMEI (International Mobile Equipment Identity) is supposed to be a unique identifier for a device and can never be changed. In 2010, the Wall Street Journal reported that they had analysed 101 popular smartphone applications and had identified 56 applications transmitting the unique device ID. This occurred without users' awareness [4]. The analysis of the encrypted requests shows that 30% of the applications send the device ID to the application developers' websites. For example, to track the user's sport activities, a fitness app delivered the device ID (not IMEI) with each request. While the user enters his/her weight, the device information and the device ID are transmitted. The information sent is shown in figure 4 below:

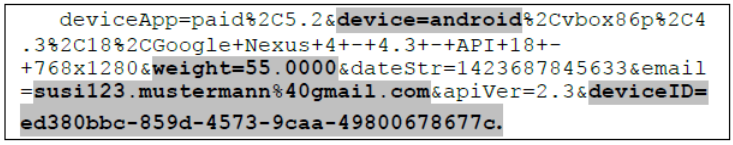

Figure 4. Usage of the unique device identifier.

2.4. Contact information

In addition to the device information, applications were suspected to collect information from the local contact list. We could prove that e-mail addresses but not phone numbers were collected and delivered encrypted to the application developers' website. For example, a fitness application tracking running activities delivers the contact e-mail addresses to help the user find his or her friends faster (figure 5).

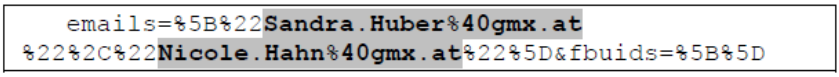

Figure 5. Usage of contact information.

3. Discussion

An issue to be discussed is the location of the servers where data is transmitted to. While the analysis shows that 90% of analytics and advertising servers are located

outside Europe, the location of the developer-controlled servers highly depends on the country the developing company resides. Sending sensitive data to outside of the EU is bound to privacy law restrictions, which are usually handled by letting the user explicitly agreeing to the terms & conditions, resp. the privacy policy.

A recently published study from Huckvale et al [10] about the analysis of apps included in NHS England's Health Apps Library, that actually shows results similar to those described in our analysis (expressing the lack of security and privacy of many mHealth apps) evaluated privacy policies. They show that most apps do not handle data according to their privacy policy, and that some apps do not even have any privacy policy. Besides, it's well known that such policies are often quite large and complex documents that users mostly care as low as they care for the rights an app asks for.

Mitigation of security and privacy concerns of mHealth apps has come in the focus of the European Commission and is addressed in the "Green Paper on mobile Health (mHealth)" [11] from technical up to legal levels.

Technical measures (independent of the OS and apps) to offer users a minimum of control over the transmission of sensitive data are still quite limited. A first technical approach would be the use of a privacy proxy that blocks unwanted traffic. It may analyse data streams to determine unwanted traffic to ad-sites as well as analytics-sites and can block these connections. A second approach could be the active filtering of sensitive information or the provision of fake information. Sensitive information is removed from the unwanted communication streams by using for instance taint analysis techniques to analyse data flows and mark (taint) sensitive values. Also fake information could be delivered to tracking and advertising networks. Users can define to send random or an explicit amount of fake answers (e.g. PDroid-Tools).

References

[1] Wu-Chen Su, A Preliminary Survey of Knowledge Discovery on Smartphone Applications (apps): Principles, Techniques and Research Directions for E-health, International Conference on Complex Medical Engineering, pp.369-374, IEEE Computer Society Press, June 2014.

[2] M. B. Barcena, C. Wuesst, H. Lau, "How safe is your quantified self?" Symantec, August 2014.

[3] N. Elenkov, "Android Security Internals: An In-Depth Guide to Android's Security Architecture," No Starch Press, October 2014.

[4] S. Thurm, Y. I. KANE, "Your Apps Are Watching You," The Wall Street Journal, December 2010.

[5] L. Njie, "Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications," Research Performed For: Privacy Rights Clearinghouse, July 2013.

[6] Google Android Dev, "http://developer.android.com/guide/topics/admin/device-admin.html," Device Admin, Last Access: 18th February 2015.

[7] Google Android Dev, "http://developer.android.com/reference/android/app/admin/DevicePolicyManager.html," Device Policy Manager, Last Access: 18th February 2015.

[8] A. B. Jeng, L. Hahn-Mingm, C. Chen, C. Tien, „Android Privacy," IEEE, Dept. Of Comput. Sci. & Inf. Eng., July 2012.

[9] Forbes, "f you're not paying for it, you become the product", http://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/", Last Access: 18th February 2015.

[10] Kit Huckvale, José Tomás Prieto, Myra Tilney, Pierre-Jean Benghozi, and Josip Car, Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. BMC Medicine 2015, 13:214. doi:10.1186/s12916-015-0444-y

[11] European Commission, Green Paper on mobile Health ("mHealth"). http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5147, Last Access: 6th January 2016