https://doi.org/10.2352/ISSN.2470-1173.2017.6.MOBMU-301

Investigation of security relevant aspects of Android eHealth-Apps: permissions, storage properties and data transmission

Jenny Knackmuss [1]***, Eric Clausing*** [2]***, and Reiner Creutzburg*** [1]

[1] ***Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, P.O.Box 2132, D-14737 Brandenburg, Germany***
[2] ***AV-Test GmbH, Klewitzstr. 7, D-39112 Magdeburg, Germany***

Email: jknackmus@gmail.com, eclausing@av-test.de, creutzburg@th-brandenburg.de

Abstract

The download number of health-promotion apps from App Stores is increasing every year. These so-called eHealth-Apps are for users a great chance to encourage their health status proactively but also to monitor this continuously. However, the resulting positive properties also entail risks. In particular, when users disclose (in addition to their personally identifiable information) some of their health-related data. Nowadays, general apps are more and more criticized in the media, especially the aspects of privacy and data security of user data are in focus [24,25].

The aim of this study is to analyze what risks may arise through the daily use of Android eHealth-Apps to user data. The security investigation focuses on three basic security relevant aspects.

One topic here is the evaluation of required permissions by the providers as well as the transparency towards the users. Furthermore, the data storage of user data will be analyzed, in particular the readability of the stored data in the database and in generated text files. The third critical focus of this study is the monitoring of the data traffic. The background traffic will be checked, i.e. on possible hidden advertising companies, on encrypted or unencrypted communication protocols and on responding provider server.

Introduction

Mobile devices with their wide range of different application possibilities keep an ever stronger entrance into the daily life. While these were initially intended primarily for personal communication, this function field changes significantly. In addition to the large market of entertainment, for example the gaming sector, an area of applications is increasingly developing which has focused on health issues. This area is particularly benefiting from the current time frame of a holistic view on the topic of personal health coupled with the technical possibilities of mobile devices. For example, there are caloric counter, sleep and fitness tracker and health care apps. The evaluation platform HealthOn shows current statistics, analyzes and development trends in German-speaking health and medicine apps [1]. This platform is based on data from the Google Play Store of Google Inc. [2] and from Apple Inc. [3]. The most common applications, however, are based on Android's current market-dominating Android operating system. Compared to Apple Inc., Android shows a steady increase in market share over the last few years [4]. The number of eHealth-Apps on the Google Store has also risen sharply last year. In a period of 12 months from December 2015 to December 2016, the supply of eHealth-Apps has risen by almost 33%, see Figure 1. The increase is almost linear. If this trend continues, the number of available eHealth-Apps in the next year can be estimated to be around 170,000.

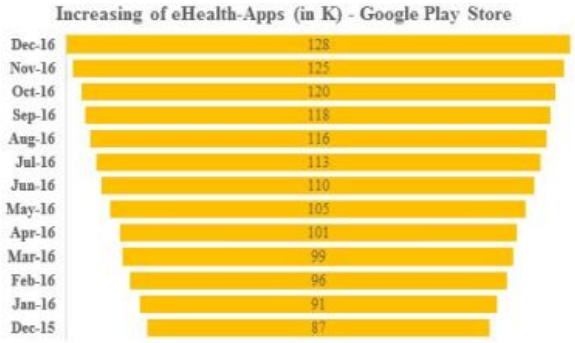

Figure 1. *Number of eHealth-Apps in Google Play Store: Development during Dec 2015 until Dec 2016 (in K), based on [1].*

The mobile applications require a variety of information and data as part of their functionality. To this end, users trust these apps to provide private medical information that is sensitive to data protection. While in the past health data were primarily of interest to health insurance companies, insurance companies and medical doctors, new studies show that these sensitive data are also used by criminals [5]. An indication of this is the increasingly frequent attacks on mobile devices [6], which show how valuable data have become for criminals [7]. Are our intimate private data at risk by the rapid increase in app usage? According to some international studies, the problem with the increased number of eHealth-Apps has arisen [7, 8].

Does this also apply to applications that are subject to German law? Taking these questions into consideration, we are conducting a security investigation of free available German-language health enhancing Android apps. The aim of the work is to analyze to what extent the manufacturers of applications take into account the legal framework in order to ensure data security

and privacy.

Methods and test specification

This study examines security-related issues that demonstrate the threats and risks associated with using free Android eHealth-Apps. The central solution approach is to carry out several security inspections. For an objective and comprehensible assessment of these security tests, generic processes are modeled. These contain several process activities which describe the prerequisite, approach and technical tools for the test execution. The security analysis consists of three different tests. This includes the assessment of access rights, the analysis of data storage and the observation of network-based data traffic. A representative sample of Android eHealth-Apps is set for the test execution by means of structured specifications.

Security feature 1: Access permissions

By examining the access rights, it is shown which access authorization groups are most frequently assigned and which security levels (normal or dangerous [14]) dominate in this context. Furthermore, the required authorizations are checked for necessity from the viewpoint of the user and the classification of the security levels is presented in this context. To check the transparency of the access permissions, the manifest of an app is analyzed for content consistency. Based on these findings, an assessment of possible dangers is carried out.

Security feature 2: Data storage

The study of the data storage focuses on the coexistence and interoperability as well as the possible storage of passwords of an app on the mobile terminal. Security-relevant investigation features are whether data in particular directories are overwritten or whether these are retained on the device in a database. It is also checked whether the storage of these data and passwords is encrypted or in the plain text. These results are used to assess the secure data storage and retention by the app on the mobile terminal.

Security feature 3: Data traffic

In the investigation of data traffic, the IP-based data transmission is considered. The security-relevant aspects to be examined are the extent to which an encrypted data transmission to the app provider's server takes place, to which advertising providers and analysis companies the data is transmitted, and whether data can be spied or manipulated by unauthorized third parties.

App selection

The identification of the relevant Android eHealth-Apps is based on the survey from Statista-research [9]. The subject of this study from 2015 is a survey of 5046 persons aged 16 to 69 years on the user behavior of eHealth-Apps. The study included questions about the current user behavior of eHealth-Apps, whether respondents would spend money on health enhancing apps, and whether they would use the apps when they were available free of charge.

Figure 2 shows the graphical summary of the survey. These results show that apps from all functional areas are used. The main focus is in the areas of "Recipes for healthy nutrition", "Search for medical information" and "Find, match and evaluate doctors, hospitals, other therapists, pharmacies". Furthermore, it is very clear that in contrast to paid apps, the distribution increases, as long as it is in the free offers.

Each app that has been audited provides its apps in several categories in the Google Play Store. Placing the app is independent of its features and tasks. Often, economic reasons are the decisive criterion. As a rule, the vendor positions his app in the area where he expects the highest number of downloads. For this reason, there is the possibility that apps from a functional area can be found in different categories. According to a study conducted by the Medical University of Hanover [10], eHealth-Apps are mainly offered in the areas of "Medicine", "Health & Fitness" and "Lifestyle". Therefore, the present one will also be focused on these three main areas.

In order to be able to classify the functional areas into a possible category, a random check-up is carried out on the Google Play Store. For this purpose, keywords which are related to the functional areas are entered in the search function in the store. For example, "Fitness", "Healthy Diet", "Pills Monitoring", "Medication Intake", "Stress Reduction", "Caloric Counter" etc. The choice of the apps was then followed by the highest download number and popularity. This examines how frequently the apps from the functional areas are assigned to the categories "Medicine", "Health & Fitness" and "Lifestyle". The 13 functional areas (see Figure 2) are used to define 15 arbitrarily selected apps. The result of this review shows that 60/195 apps in the category "Medicine", 106/195 apps in the category "Health & Fitness" and 13/195 apps are in the category Lifestyle. The overall evaluation has shown that it is not possible to assign a functional area to a category clearly, since it is quite possible that several categories are valid for a functional area. No evaluation could be carried out for the "Memory Training" function area because there is no app in one of the three categories. These apps are generally in the categories "Learning", "Games" or "Thinking".

In summary, the following features, which are important for the choice of apps, can be emphasized:

- App providers offer their apps in various categories in the Google Play Store from an economic perspective. Relevant for these studies are the health enhancing categories "Medicine", "Health & Fitness" and "Lifestyle".
- In the statistical survey in [9] a total of 13 functional areas are assessed regarding their use. It can be seen from the results that every functional area is of fundamental interest to users. Furthermore, there is a clear trend to see that free apps are more downloaded from the Google Play Store than paid apps. For this reason, free apps from 13 functional areas are determined.
- Only apps from the German legal area are considered.

Within the framework of this study, a representative sample of eHealth-Apps will be investigated more closely with regard to their functional areas, taking into account the criteria listed above.

Study 1: Permission

With the implementation of access rights, app vendors bypass the isolation of the Android operating system. When installing an app, the user confirms the required access rights and thus frees access rights to sensitive data. Depending on the authorization group, user data can be collected, processed and stored.

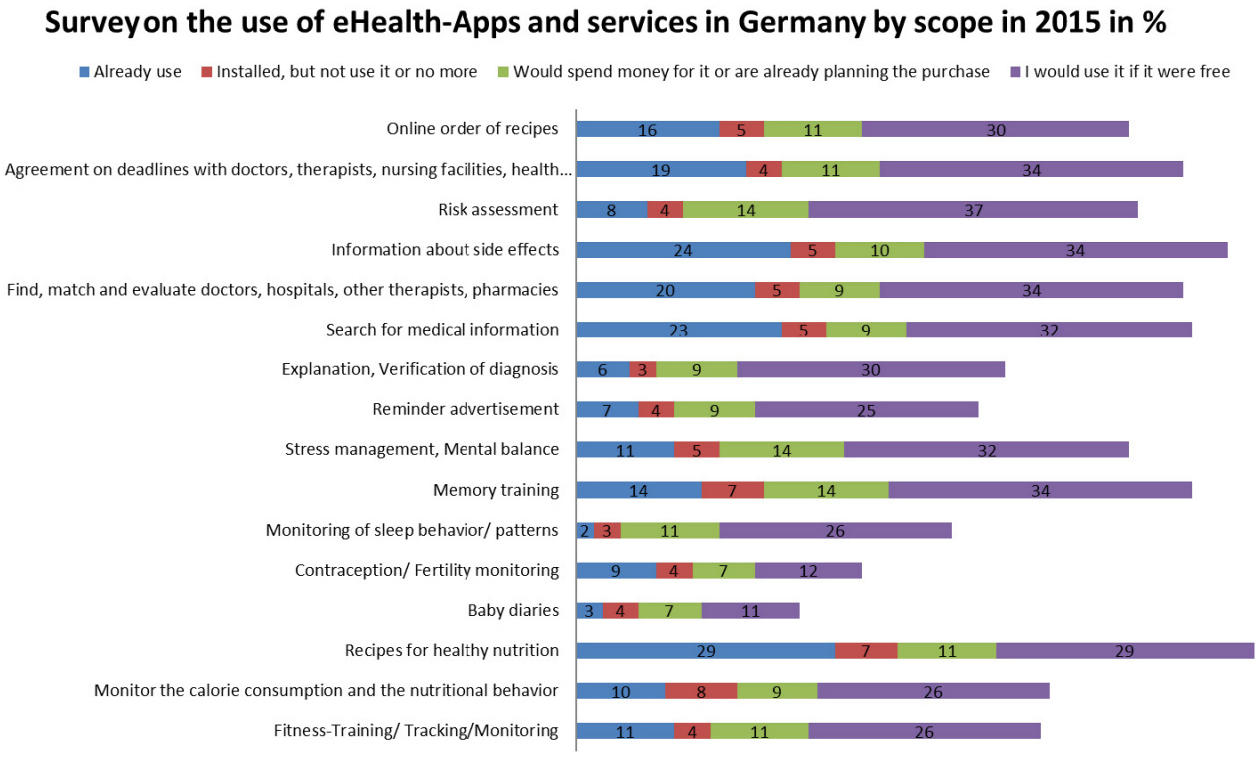

Figure 2. *Survey on the use of selected eHealth-Apps in Germany by functional area, based on [9].*

The user can only keep an overview of these features if he / she is intensively dealing with the requirements of the app in connection with the product description and, if he / she has knowledge about the technical description. Additionally, the user must trust the app provider to disclose the full scope of access rights and not to hide any of these permissions. In order to ensure that the required access rights do not result in a violation of privacy, checks must be carried out on the part of the user. Investigations that a user can implement without great effort are:

- Provide an overview of the required access authorizations,
- Decide whether the requested access rights fulfill the purpose and
- Determine the security level of an access authorization.

In addition to these features, the transparency of the access authorization must be checked against the user. The Google Play Store or mobile device contains all required permissions for an app for the user. However, the permissions implemented in the Android manifest may not be fully visible to the user. This occurs, for example, when an app is updated. If a developer forgets to modify the manifest for changes to an app, it may happen that an app performs an authorization that does not require it to perform its actual function.

Experts are investigating this issue by accessing the apk file of the app. Typically, this is protected by the app provider. If there are vulnerability in the program code of the app or the mobile terminal is rooted, the lock can be released and the apk file becomes visible. The root mode is not activated in the entire analysis. Therefore, the latter approach is excluded.

Using a special analysis tool, Oxygen Forensic® Suite [11], the analysis can also perform without root privileges. For this purpose, the relevant file must be extracted from the mobile phone. This file is in a packed state after the extraction and has to be unpacked with an additional software.

In the context of this study, the following four properties are tested on a sample of Android eHealth-Apps (see section Tests and Results). The entire investigation process can be represented by generic processes, see Figure 3.

This process sequence represents the top processes step by step. At the beginning of the security analysis for access authorization, the frequency distribution of the access authorization is examined, followed by the examination of the requirements of the access authorization, the classification of the access authorizations into the security levels and finally the examination of the transparency of the access authorizations.

A detailed illustration and description of the sub-processes can be found in [12].

Frequency scale of permissions

This review provides an overview of the required access rights for the apps. This requires that the information is available from the Google Play Store. Installing an app is not necessary for this step. Based on these results, the following investigations are carried out.

Requirement of permissions

The need for access authorization is not assessed by the product description, but by the use of an app. Against this background,

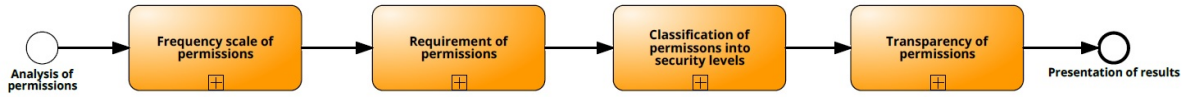

Figure 3. *Process work-flow for analysis of permissions, based on [12].*

the app needs to be installed from the Google Play Store. After the installation, the application is tested for its features, related to the access permissions. An exception to this rule is the "other" authorization group. For this purpose, additional technical methods must be implemented in order to obtain meaningful results. These further studies are therefore not the subject of this study.

Classification of permissions into security levels

The security levels relevant to the user are "normal" and "dangerous". A detailed description of this is given by the German BSI (Federal Office for Security in Information Technology) [13]. The classification of the security level for the individual access authorizations is taken from the information page IzzyOnDroid [14]. This page provides a clear and documented summary of the authorizations with their security levels.

Transparency of permissions

In this test, a target / actual comparison of the access permissions from the Google Play Store and the Android manifest is made. The necessary apk file is extracted with the commercial software Oxygen Forensic® Suite [11]. The non-commercial software apktool [15] is used for unpacking these.

Study 2: Data Storage

Android stores a variety of data. These consist, on the one hand, of data of the user and, on the other hand, of system and user data which are derived from other apps. These data are stored on the internal memory of the mobile phone by default. Users can expand their memory by adding an external storage medium. Typical data for the storage on external media are image, video and music files, since they are expected to require a large storage capacity. In addition to these memory-intensive data, system and user data of an app can also be collected on the external data carriers.

In this study the storage behavior of user data is analyzed. The analysis of the data takes place on the internal memory of the mobile phone. An analysis software Oxygen Forensic® Suite [11], which extracts the entire content of the mobile terminal, is used as an aid. The prerequisite for extracting the data is that no PIN lock is activated. The purpose of the investigation is to examine whether the internal collection of user data on the app increases the risk of data breach and data security breaching. In addition, the user will be able to save the user data during the use of the app and, on the other hand, the presence of residual data after uninstalling the app, see Figure 4. In [12] the detailed illustration and description of the sub-processes is given.

Data analysis during app usage

For the analysis of the app data usage, the following security-relevant test features are the main focus:

- Clearing the user data on the internal memory,
- Export of data (e.g. calendar or contacts),
- Storage of backups, restore of backups and the possibility to encrypt backups,
- Possibility to encrypt the app contents and
- Save the PIN code lock.

Data analysis after uninstalling the app

Data analysis after uninstalling the app focuses on the following security-relevant features:

- presence of residual user data on the internal memory,
- Existence of exported data (such as calendar entries or exported contacts) and
- Presence of PIN code lock.

On the basis of the above-mentioned investigation features, a selection of the Android eHealth-Apps to be examined is made. If an app has the function to create a backup, the possibility of a data export or a PIN code lock, it is at the forefront in the investigation area.

Study 3: Data Traffic

The exchange of data on Android is controlled by the app provider. The user usually consents to the right to install the mobile application. Whether a persistent data communication between a provider server or only once during the commissioning of the app takes place, is often not clear. When software is deployed on a server or data is stored on a server, aspects of data security must be taken into account in addition to the legal requirements. If security features are not implemented at all, the user data are insufficiently protected against access by third parties. To identify vulnerability in the Android eHealth-Apps, the traffic is read in the network. For this, a typical man-in-the-middle attack [16] is simulated. It is assumed that the data is communicated via an encrypted connection (HTTPS). Against this background, the network sniffer "mitmproxy" [17] is used. With this software, both encrypted and unencrypted data traffic can be examined. In addition, the network sniffer includes a function for detecting whether companies can follow unauthorized user activities in the background. If such analysis functions are integrated in the app development, it is imperative to include this in the data protection definition.

In order to identify possible vulnerability in data security and vulnerability in data protection, data transfers in the network are analyzed during this test. The following security-relevant questions are considered:

- What data can be read to what extent?
- Are advertisers visible?
- Are data analyzes carried out by third parties?
- Are the responding servers up-to-date?

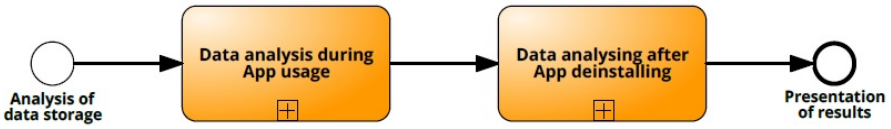

Figure 4. *Process work-flow for analysis of the data storage, based on [12].*

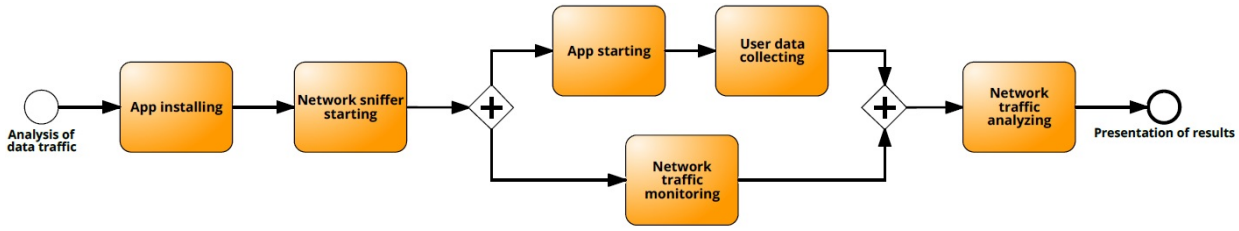

Figure 5. *Process work-flow for analysis of data traffic, based on [12].*

The existing analysis networks are also included in the manifest file. However, the possibility exists that other unregistered companies are involved. With this test also such providers can be recognized. The duration of the app is 60 minutes. The procedure is presented in a fixed process, see Figure 5. A detailed illustration and description of the related sub-processes is explained in [12].

Tests and Results

In summary, the research findings show that Android eHealth-Apps have a variety of vulnerabilities. Numerous access rights to sensitive user data are required. In addition, not all of the acquired rights are required to perform the app. There are also differences in content between the rights in the Android manifest and the Google Play Store. The results from the analysis of data storage and data traffic show that the use of eHealth-Apps is insufficiently protected. Reading or reading along the data is easily possible. It is possible to create motion profiles or to detect everyday behavior without technical effort. A violation of the privacy of the user is therefore also not excluded.

Test Study 1: Permissions

The distribution of rights under Android is a much discussed topic in professional circles. Developers require access to the system and its resources by implementing access permissions in the manifest. The user himself decides whether he grants them or not. However, the risks and dangers that may arise as a result are often not understood by every user.

The verification of access permissions will first show which access permissions apply to 60 Android eHealth-Apps and what security levels are hidden behind them. The classification into a high security level (”dangerous”) implies that this right should be considered with care [13].

Based on this, an initial assessment is made as to whether the required access authorizations are required for the function execution. This evaluation takes place from the user’s point of view and on the other hand shows how an app can be assessed with its permissions and which additional properties are to be critically questioned.

With in-depth knowledge about the system structure of Android, it is possible to get more information about the required access rights. For example, by extracting and extracting the apk file, the manifest can be more closely examined. This will quickly reveal whether all permissions are given to the user. As a rule, this is checked by the security authorities of Android. However, it is not impossible for some apps to have this mechanism, although inconsistencies exist. The test to check the transparency of the access rights compares the target and actual status of the rights allocation.

A mobile terminal and an Internet connection are required for carrying out the tests. In addition, additional software is used for transparency testing. The software Oxygen Forensic® Suite [11] is used to extract the apk file and the software apktool [15] is used to extract this file.

Frequency distribution and assignment to the security security levels

As a result, 8/60 (13%) apps do not have access permission groups. This rating does not consider the access permission group ”Other”. This includes several authorizations that are evaluated separately in this test. A total of 14 groups can be assigned. 10/14 (71%) Authorization groups are subject to the ”dangerous” security level. There is a high risk for user data [13]. Taking into account the fact that health data are collected and stored alongside personal data, these rights are considered to be sensitive. Against this background, an examination of the necessity of this allocation of rights is indispensable. 3/14 (21%) of the authorization groups belong to the security level ”normal”. According to the information provided by the BSI, these do not pose a particular risk to equipment or user data [13].

In the test, 21 different access requirements could be identified under the permission group ”Other”. These are often classified as safe for the user. However, taking into account the respective security level, it can clearly be seen that the majority of the security levels are ”dangerous”. Only 7/21 (33%) of the ascertained permission are classified as ”normal” [12].

In the overall view, Android eHealth-Apps require permissions, which pose a great risk and risk to user data and system data. It is therefore particularly important to ensure that there are no unnecessary permissions under these requirements.

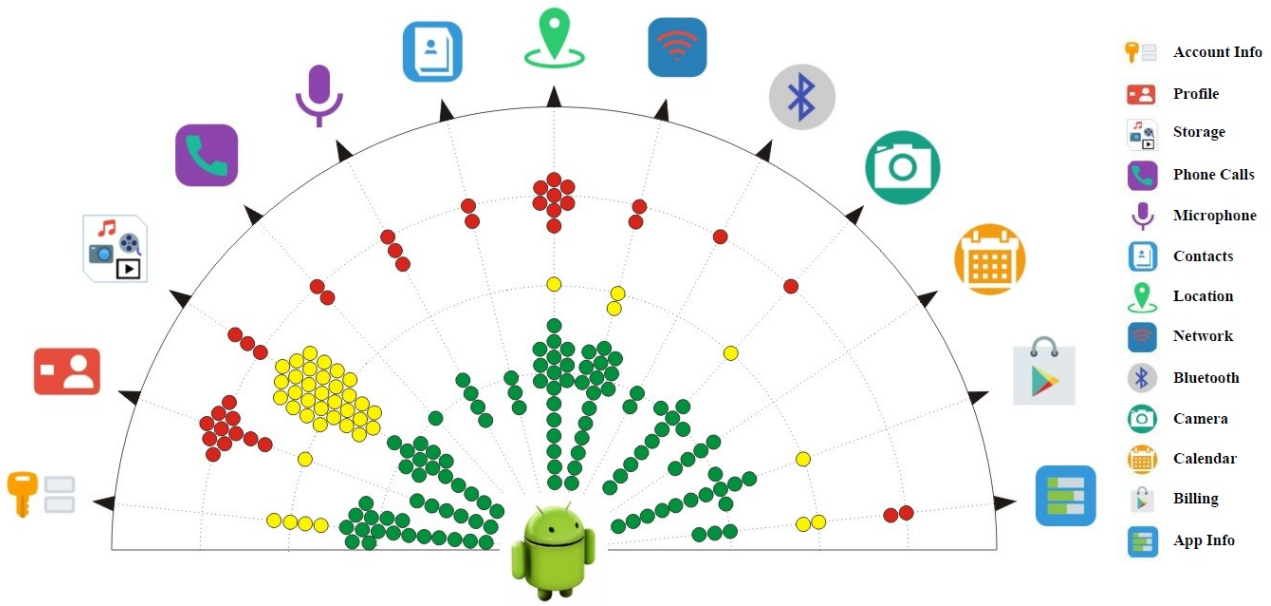

Figure 6. *Graphical presentation of the results from the analysis of the need for permissions from 60 Android eHealth-App.*

Requirement of permissions

The findings of this study provide information about the need for access rights to the main areas. Figure 6 shows the distribution of the 14 access authorization groups with their assessment. The graphics set the access rights in relation to their actual necessity for the respective app main areas [12]. A total of 186 to be confirmed rights could be determined. 109/186 (59%) of the required permissions are necessary to run the app's features. 42/186 (23%) were identified as optional or as not clearly identifiable. This is especially true of the permission "Storage".

Read and write access to the SD card is not always necessary because most of the apps require data storage on a Web server or no large amounts of data have to be stored. However, it may happen that a user does not have enough memory for the system's pure system data, then the app has to be stored on the external medium. A clear assignment is not possible in this context. The same applies to the permission "App Info". The logging of the app activities is usually used to evaluate the error behavior. However, apps that have very few features or do not require additional activities do not necessarily have to retrieve active or running apps or log device activity.

35/186 (19%) of access requests were not considered necessary. Taking into account the security levels, the groups other than the groups "Network" and "Profile" are to be regarded as critical.

For example, with a magazine app, a user can download health magazines and then read them. This app does not have any additional features. The app provider prompts the permission "Storage", "Network", "Profile" and "Location". In this case, a valuation was made as follows:

Profile: The application does not require registration, nor can content be shared. "Find Known Accounts" is not necessary.

Location: The app does not allow any more functions than downloading magazines. The determination of the exact and approximate location is also not necessary here.

Storage: This function does not have to be required. The magazines are available to the user in PDF format and must be downloaded from a provider server. A PDF has an average size of 4-5 MB. Against this background, the result here is optional.

Network: No journals can be downloaded without connecting to the WLAN. For this reason, this right is relevant to the execution of the app. The access permission group "other" was not considered for time reasons. On the basis of the results from the assignment of the security levels, further checks are to be carried out here in order to exclude possible weak points.

In the case of the function test, further abnormalities have been determined in addition to these results. For example, an app for medical search allows an export of contact details to the personal contacts of the mobile phone, although the necessary right is not explicitly required. Another example is the one app for healthy eating. This is used to perform a voice memory. However, confirmation of access to the microphone is not required [12]. The reason for this is that the implemented permissions in the Android manifest are not fully visible to the user. An initial assessment is possible with the results from the variance analysis of the access authorizations.

Transparency of permissions

The results from the comparison of the access permissions of the manifest file and the Google Play Store are shown in Figure 7.

Of the 60 Android eHealth-Apps, only 59 applications were tested. The app "DDG Pocket Guidelines" crashed regularly during the test execution.

As a result, 49/59 (83%) of apps were unable to detect any deviations from the requirements. 10/59 (17%) Apps showed differences between the target and the actual state. These inconsistencies were found in both the manifest and the Google Play Store. Furthermore, the manifest file can identify permissions that are not defined in the current Android version [14]. Possi-

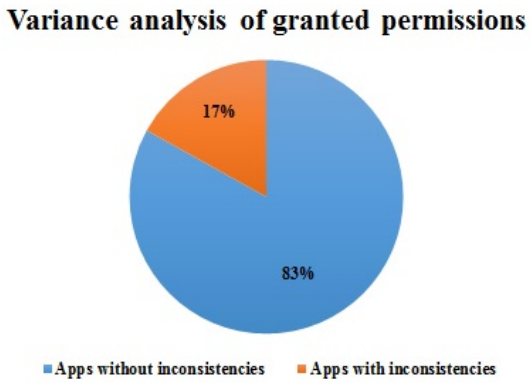

Figure 7. *Result of the variance analysis of permissions, based on [12].*

ble causes for such differences and inconsistencies can be found by further investigations.

Test Study 2: Data Storage

The internal data storage of system and user data of an Android eHealth app does not in itself represent a great risk. However, if security gaps exist within an app, there is the possibility of a violation of privacy. Furthermore, there is a risk that third parties will gain unauthorized access to this data.

The aim of the data analysis is to find out whether system and user data can be read out by the mobile terminal or read through by other applications. The main focus of this study is on the type of data retention, data export behavior, the storage of app PIN codes, and the storage type of backups.

A mobile terminal, an Internet connection and the analysis software Oxygen Forensic® Suite are required for the test execution. The analysis of the internal memory is performed on 16 Android eHealth-Apps. In the following, the results obtained are explained in the individual criteria.

Data retention

The category of data storage includes relevant criteria, with which an initial assessment is made on the visibility of the stored user data. This concerns, on the one hand, the data retention when using the Android eHealth app and, on the other hand, the remaining data retention after uninstallation. Another test criterion is the type of storage. Security-relevant features here are whether data is stored in encrypted or encrypted form. In addition to the type of encryption of the data, the location is relevant for storage, such as on the terminal or a web server. In the case of a clear-text storage, the data are always visible to unauthorized third parties. Regardless of whether it is stored on the device or on a Web server. In these cases, there is a great risk with regard to the required data security. If personal or health-related data are stored, there is also a risk of personal privacy. If the data is encrypted, there is a lesser risk of infringement. In summary, the results for data retention can be assessed as follows:

1. For 8/16 (50%) apps, the user data is stored on a web server and encrypted. 2. For 4/16 (25%) apps, the user data is stored in the plain text on the mobile device, see Figure 8. 3. For 3/16 (19%) apps the user data are stored on a web server and additionally in the plain-text on the mobile phone. 4. For 1/16 (6%) apps, the user data is stored in plain text as well as encrypted. A pattern of storage is not visible at first sight.

Example of a plain text storage in an app database

Data export

With the function of data export, for example, an app can be used to export calendar entries, contacts, alarm settings or data via email. These data are usually stored in other applications, such as calendars. As a result, in most cases the original protection of the user data no longer exists. Data shared via the email account can often be found in the mailbox or even in the email client's archive.

Furthermore, reminders in the personal calendar are visible to everyone. These and other security features allow you to analyze user activities and behaviors. The user then only has the option of manually deleting these exported data. If he does not delete this data, sensitive data is permanently present on the mobile device.

For the above reasons, the export function when using a mobile application as well as the reliable deletion of this data is checked after uninstallation. 10/16 apps (63%) have an export function and 10/16 apps (63%) do not delete the data when removing the app. This makes it possible to conclude uniformly that in 10/10 (100%) of the apps the exported data after the uninstallation continue to be recognized on the mobile device in the plain-text. For example, the wake-up setting for an app to monitor sleep behaviors remain fully active even after uninstalling the app. The alarm function was maintained and the notes on sleeping behavior contained in it were still displayed. In addition, the majority of the apps can be used to export "reminders" and "contact data". These data are in part presented in such detail that confidential information, such as medical appointments or medication revenues, can be viewed by unauthorized third parties and used for statistical analyzes, for example.

PIN code

The PIN code lock of an app is an additional feature that is supposed to protect the sensitive content of the app. As soon as an application protected by PIN code is opened, the application prompts the user to enter his password. Apps, which are activated by a registration by user data are excluded from this. Such registrations are, for the most part, permanently active and need not be confirmed again in the case of repeated use. An app is protected by a PIN code only if the selected password is kept under lock and key by both the user and the app. If the password is stored in the plain-text, the app is thus not adequately protected.

The results for the category of the PIN code lock are to be evaluated in the total with insufficient. The user has only in 3/16 apps (19%) the possibility to secure his sensitive data additionally. By critically viewing this result, only two apps offer the user a secure app lock. In these cases, the stored password can not be read out. The test does not include testing the passport hardness and the possibility of repeated input, which can not exclude a brute-force attack [18].

Backup

Data that has been lost can be recovered by a backup. The test examined the backups, which can be triggered manually by the user and are available offline. An automatic synchronization of the data on a web server is excluded from the test. In this case,

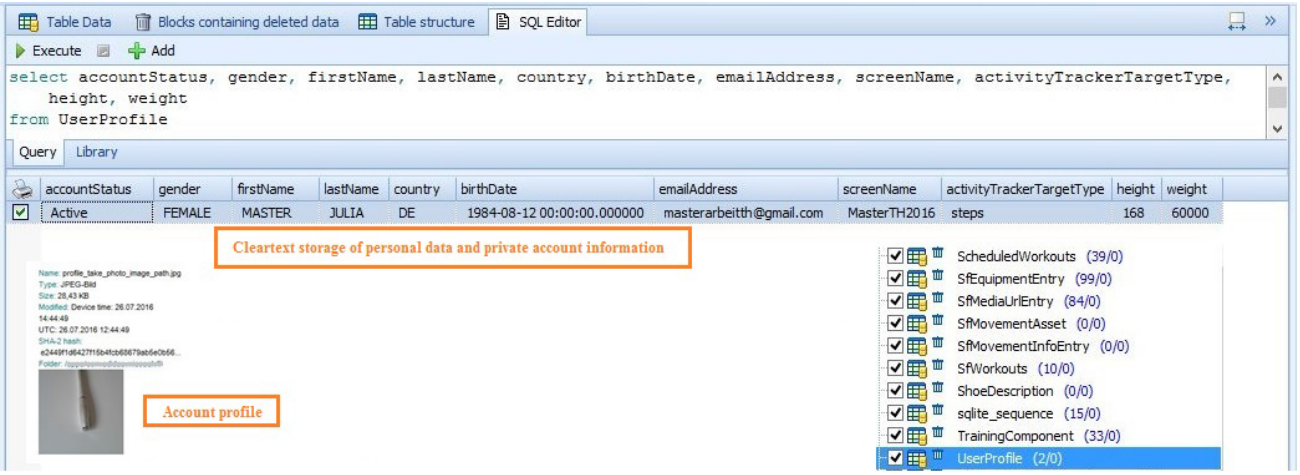

Figure 8. *Example of a plain-text storage in an app-database.*

the user must be online to access his data. In this backup process, the web provider is directly responsible for the hosted data.

In summary, three apps provide the function to create a backup offline. An additional password protection of the backup was not possible. There were two scenarios when restoring the backup:

- Restore the data, despite protection of the data by a password and
- View the data without the app installed on the mobile device.

Both scenarios could be easily executed. Although a menstrual calendar app is locked by a PIN, it was possible to restore the data without further input. An additional PIN is not requested. The backup files of the Apps Drugs and Sleep Monitor can be opened with a common text editor. The contents of these files are readable in the plain-text.

Test Study 3: Data Traffic

Data exchanged in a network is subject to a greater risk than internally stored data. However, internally stored data is not protected against spying. If unauthorized persons obtain the necessary rights, there is not only the risk of privacy and data protection but also the data security is no longer available. The former is also true if third-party data are recorded in the background or hidden advertising providers are active.

The purpose of this analysis is to determine the extent to which data can be read by the mobile device during the transfer. In this context, not only user data can be assessed, but also hidden advertising placement can be recognized. The same applies to apps that pass protective data to third parties. When a mobile application sends data to a vendor server, service characteristics must be used for data security and data protection, such as server versions and active certificates used.

A man-in-the-middle attack [16] is simulated for the test execution with the software mitmproxy [17]. This allows the network activities of the applications to be analyzed and the properties of the target servers to be determined. The test is applied to 25 Android eHealth-Apps. The following scenarios were identified in the test:

1. Active advertising,
2. Active data collection by third party,
3. Visible data transfer,
4. Visible data on web databases,
5. Servers which do not correspond to the state of the art and
6. Only a small proportion of providers use secure data communication.

Active data transfer

With the use of a mobile application, a large number of active third-party providers have become visible. This data transmission to analysis networks is shown in Figure 9.

In the middle of this graph, the determined networks are listed. The size of the network cubes illustrates which company was most frequently identified. In this test, Google Analytics is the most popular among app providers. There, 16/25 (64%) apps send periodically information. Second is Flurry Analytics from Yahoo [23]. There, 14/25 (56%) apps pass on their data. Googlesyndication use 8/25 (32%) app providers and Baidu 5/25 (20%). The companies etracker and Facebook are less used. Each 1/25 (4%) providers use this offer to evaluate user data or activities.

The analysis networks are especially active with the apps ”Fitness Point”, ”BMI Rechner & Gewichtstagebuch”, ”Ernährungstagebuch & Gewicht”, ”Rezepte zum abnehmen” and ”Chefkoch - Rezepte zum Abnehmen”. During the tests up to 50 events could be observed. It is noticeable that these five apps monitor the healthy nutrition of a user and its progress. Whether all mobile applications with these characteristics exhibit these strong activities is to be found by further investigations. Of the 25 analyzed apps, no interactions with third parties could be found only with the apps ”Apotheke unterwegs”, ”Diabetes Rechner”, ”AOK genießen”and” mudra-art”. Considering that these apps also require access to sensitive data, the distribution of the permissions in the image is also critical. At this point, it is not excluded that other user data is collected in addition to the app-related data [19]. In addition to the analysis networks, advertising activities were also identified. 5/25 (20%) apps contain hidden ads.

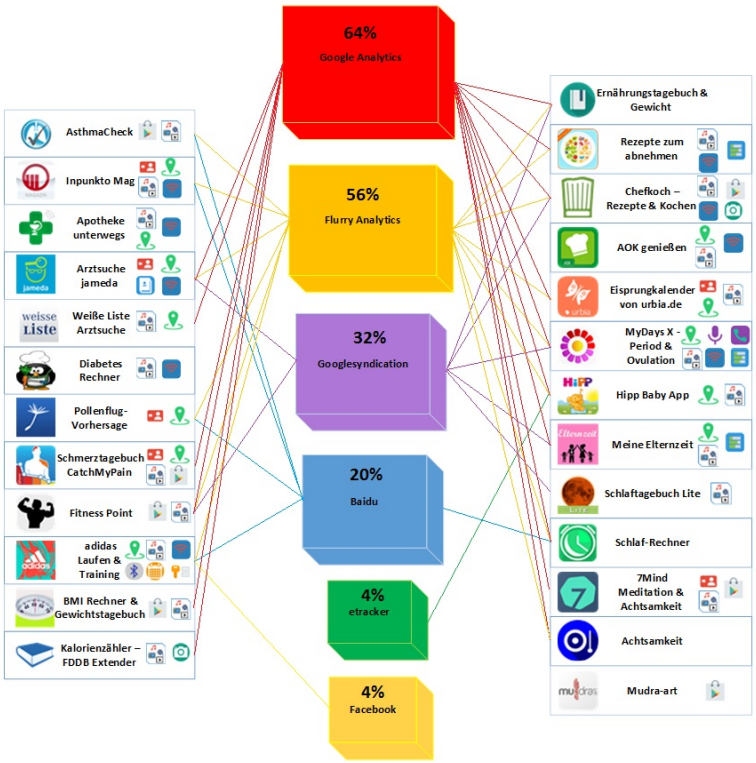

Figure 9. *Summary of the test results from the analysis of the data exchange between the apps and analysis networks, based on [19].*

Visibility of the data

The investigation shows that data of any kind is communicated in the plain-text in the network. The data includes sensitive user data, logging of authentications, database queries. Except for this are the apps that do not send data via the network or which are not connected to a web server. 4/25 (16%) of the apps examined communicate with an encrypted registration of the user ID.

Figure 10 is an app example, where a plain-text transmission of registration data takes place at a company server. In this example, the user's personal data and, on the other hand, sensitive data about the child are to be recognized. In addition, the communication request contains the email address and the login data including the password. Assuming that the user uses the same user data in other apps, unauthorized persons can access other sensitive data without additional information.

Server communication

When analyzing traffic, some vendor servers could be identified by their name and its implemented programming language. As a result, 5/8 (63%) of the ascertained operating systems are up to date. In contrast, 7/8 (88%) of the implemented programming languages are outdated. PHP is preferred by providers. However, 5/6 (83%) of the discovered versions are so legacy that they are no longer supported by the PHP Group [20]. The vulnerability database "CVE Details" shows how this language is nurturing. Ignored vulnerabilities, at the same time also legacy versions, cause a variety of vulnerability [21].

App users can access provider data only in five cases via an encrypted Internet connection. The key length as well as the encryption method used correspond to the minimum requirements based on BlueKrypt [22].

Summary and Conclusion

The assessment of access authorization has shown that the health enhancing apps demand a large number of permissions to use personal data. Most of these permissions have access to sensitive data and are subject to a level of security that is considered to be a matter of concern. Furthermore, it was found that only 59% of the ascertained permissions were required for the functional execution. The variance analysis to the content from the Google Play Store and the Android manifest shows only a small deviation, which is positive.

The analysis of data storage and network-based data traffic shows that the security of the data is at risk. Data is kept in the plain-text on the mobile device or when stored on a provider server, the data transmission is not sufficiently protected. The possibility of a backup or an additional PIN code lock is only possible with very few providers. As shown, the backup can be read out without additional technical effort. After uninstalling, exported data is still visible. In addition, the user does not receive sufficient information about the services running in the background. Analysis and hiding advertising companies and adware programs are activated by installing an application. When analyzing the server structure used by the vendors, it was found that partially legacy systems are used here. These systems therefore have further vulnerabilities and the data hosted thereon are thus no longer adequately protected.

Various security-relevant factors were discovered during the

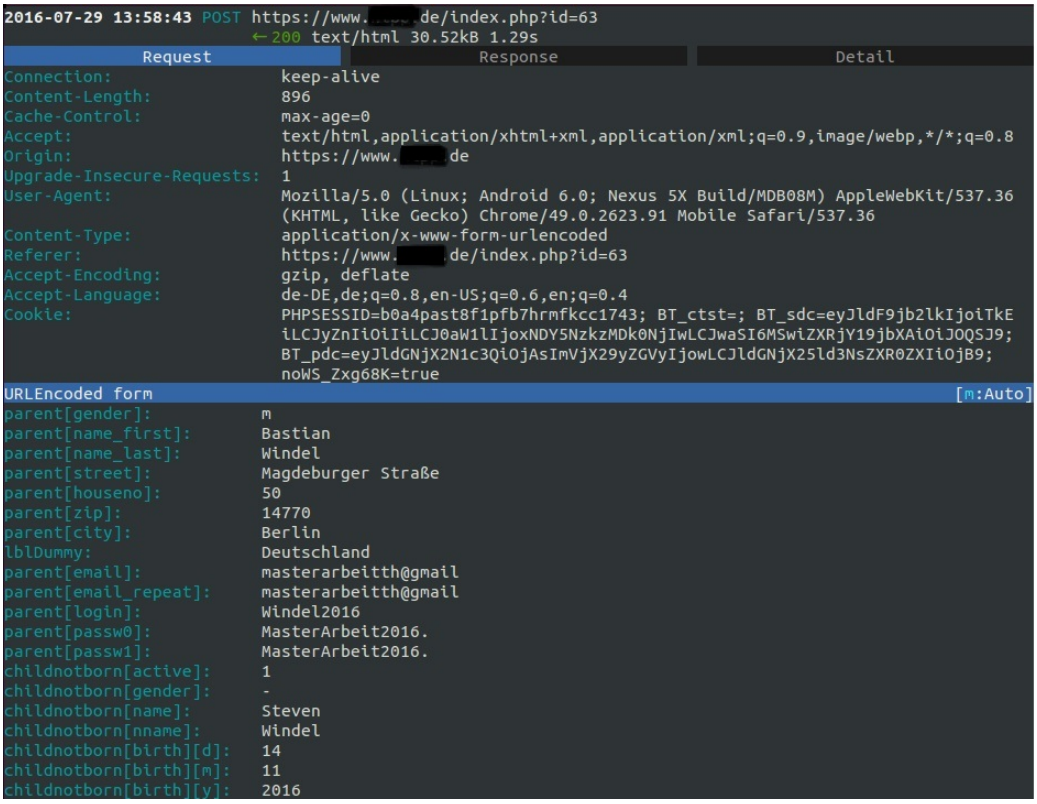

Figure 10. *Visible user activity in a network using the example of a baby app, based on [12].*

test procedure, which are to be examined in more detail. These results may help identify further weaknesses. Additionally, additional security audits for paid apps can be made to determine whether paid health-promoting applications have a better security level than the investigated free eHealth-Apps.

The various security analyzes in the use of health apps have shown that the developing companies have not recognized the problem, or have little motivation to close these gaps. In order to eliminate this deficit, different strands of action are conceivable. First of all, the user should raise awareness. If, for example, an avoidance behavior occurs in the application of certain eHealth-Apps due to security concerns, the companies will eliminate the cause of maladministration as quickly as possible. For this, it is necessary to give the user information which allows a simple and fast assessment. An even more stringent unification in the representation of the usage rights, such as a traffic light system, is conceivable here. The introduction of independent control authorities is another supporting mechanism that certifies, for example, apps that meet tightly defined security criteria. The resulting additional security checks mean that the provider must plan more time to publish their products. On the other hand, it increases the security and thus also the quality with regard to data protection, which in turn increases the user's confidence and leads to a wider spread of the many applications which are helpful in many respects.

References

[1] A. Striegel, Health-App Dashboard - Apps weltweit: Google & Play & iPhone, `https://www.healthon.de/health-app_dashboard`, HealthOn, 2016, Status 27.12.2016 12:20.

[2] Google Inc., Google Play: `https://play.google.com`, 2016.

[3] Apple Inc., iTunes – Alles für gute Unterhaltung – Apple (DE), `http://www.apple.com/de/itunes/`, 2016.

[4] V. Briegleb, Android und iOS hängen alle ab, `http://www.heise.de/newsticker/meldung/Smartphones-Android-und-iOS-haengen-alle-ab-3300959.html`, Heise Online, 2016, Status 22.08.2016 20:15.

[5] C. Kerwel, S. Augsten, Ärzte im Visier von Cyber-Kriminellen, `http://www.security-insider.de/aerzte-im-visier-von-cyber-kriminellen-a-539291/?cmp=nl-15&uuid=3E4F5810-15D6-4145-BB521C40E820A4FA`, Security Insider, 2016, Status 21.08.2016 11:40.

[6] Security Magazine, Attacks on Mobile Devices and Apps on the Rise, `http://www.securitymagazine.com/articles/87322-attacks-on-mobile-devices-and-apps-on-the-rise`, 2016, Status 21.08.2016 11:20.

[7] Intersog, Mobile Health Apps and Security, `http://ehealth.intersog.com/blog/mobile-health-apps-and-security`, 2016, Status 21.08.2016 11:30.

[8] D. He; M. Naveed, C. A. Gunter, K. Nahrstedt; "AMIA Annual Symposium" Security Concerns in Android mHealth Apps, `http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4419898/`, 2014, Status 21.08.2016 12.00.

[9] Statista; Nutzung ausgewählter Applikationen und -Services in Deutschland nach Funktionsbereich 2015, http://de.statista.com.statistik/daten/studie/454390/umfrage/nutzung-von-digital-health-applikationen-und-services-nach-funktionsbereich/, Statista, 2015, Status 12.04.2016 17:18.

[10] U.-V. Albrecht, Chancen und Risiken von Gesundheits-Apps (CHARISMHA), http://charismha.weebly.com/uploads/7/4/0/7/7407163/charismha_gesamt_v.01.3-20160424.pdf, 2016, Status 06.05.2016 13:50.

[11] Oxygen Forensics, Oxygen Forensic Extractor, http://www.oxygen-forensic.com/de/products/oxygen-forensic-extractor, 2016, Status 29.12.2016 17:40.

[12] J. Knackmuss, Sicherheitsrelevante Aspekte bei der Nutzung von Android eHealth-Apps, Master Thesis, Technische Hochschule Brandenburg, Dept. Computing and Media, August 2016. https://www.researchgate.net/publication/307571399_Sicherheitsrelevante_Aspekte_bei_der_Nutzung_von_gesundheitsfordernden_Android_eHealth-Apps, Status 27.12.2016 12:20.

[13] Bundesamt für Sicherheit in der Informationstechnik, BSI für Bürger (Hrsg.): BSIFB - App-Berechtigungen bei Android, https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungMobileApps/Android/Android_node.html, 2016, Status 26.05.2016 16:02.

[14] A. Itzchak Rehberg, Android App Permissions, https://android.izzysoft.de/applists/perms, Android izzisoft, 2014, Status 28.05.2016 10:20.

[15] GitHub, Apktool - A tool for reverse engineering Android apk files, http://ibotpeaches.github.io/Apktool/, 2016, Status 15.07.2016 20:30.

[16] K. Lipinski; H. Lackner; O. P. Laué, Oliver; G. Kafka; A. Niemann; E. Raasch; B. Schoon; A. Radonic, Man-in-the-Middle-Angriff, http://www.itwissen.info/definition/lexikon/Man-in-the-Middle-Angriff-man-in-the-middle-attack.html, IT-Wissen, 2016, Status 01.08.2016 10:00.

[17] A. Cortesi, M. Hils, T. Kriechbaumer, mitmproxy Project, https://mitmproxy.org/, 2015, Status 01.08.2016 10:10.

[18] K. Lipinski; H. Lackner; O. P. Laué, Oliver; G. Kafka; A. Niemann; E. Raasch; B. Schoon; A. Radonic, Brute-Force-Angriff, http://www.itwissen.info/definition/lexikon/Brute-Force-Angriff-brute-force-attack.html, IT-Wissen, 2016, Status 22.08.2016 10:50.

[19] A. Barczok, Achim, Smartphone-Schnüfflern auf der Spur, c't Android, 2016.

[20] PHP Group, PHP - Supported Versions. http://php.net/supported-versions.php, 2016, Status 14.08.2016 18:20.

[21] CVE Details, PHP - CVE security vulnerabilities, versions and detailed reports, https://www.cvedetails.com/product/128/PHP-PHP.html?vendor_id=74, 2016, Status 15.08.2016 17:30.

[22] D. Giry, Cryptographic Key Length Recommendation. https://www.keylength.com/en/compare/, BlueKrypt, 2016, Status 01.08.2016 09:30.

[23] Yahoo!, Flurry Analytics - Yahoo Developer Network, https://developer.yahoo.com/analytics/, 2016, Status 01.08.2016 18:10.

[24] A. Hoppe, J. Knackmuss, M. Morgenstern, R. Creutzburg: Privacy Issues in Mobile Health Applications - Assessment of current Android Health Apps. in Proceesings of Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications, IS&T Electronic Imaging Symposium 2017. San Francisco, CA (USA)

[25] ONC launches new challenge focused on privacy in health apps. http://www.imedicalapps.com/2017/01/onc-health-app-privacy-challenge/ Status 24.01.2017 19:30.