3 Existing Software Applications

Existing apps aspiring to improve the privacy of smartphone users, can be divided into several categories:

Advisor: These apps primarily inform the user. The most popular approach is to classify apps according to their risk of violating the users' privacy (e.g. based on access rights they demand). By this means, recommendations can be made as to which apps should better be uninstalled.

Firewall: Furthermore, there are apps operating like a firewall. These apps are intended to protect the smartphone not only from attacks from the outside but also explicitly from unwanted data leakage. For that purpose the internet access for certain apps, or the connection with certain servers can be blocked. Another approach would be to screen critical contents in data traffic, provided that it is not encrypted. Data e.g. of a GPS sensor can still be collected, but the communication channels are controlled.

Manager: Finally, there are apps that block or restrict access to specific data or features for other apps. Operating on this principle data access as well as date leakage can be prevented, since the internet access, for instance, can also be blocked for individual apps.

The functionalities aimed at by PRIVACY-AVARE are: (1) gathering the data privacy profile, (2) transmitting the data privacy profile, (3) Examining violations of the data privacy profile, and (4) reducing the violation. Advisor apps can be roughly allocated to function (3), firewall and manager apps to function (1), (3) and (4). None of the identified apps allows transmitting the preferred profile to several devices (function 2). The actual implementation and the possible preference settings differ from app to app, with manager apps corresponding the most to the desired functionality of PRIVACY-AVARE. In order to evaluate the state-of-the-art, manager apps of the Google Play Store and external sources were identified. 18 apps were found and examined. First of all, it can be stated that these apps differ with respect to their working method, usability and functionality. Therefore, these three aspects are presented below. Subsequently, table 1 gives an overview of all examined apps and finally, exemplary apps are described in detail.

3.1 Working method of the examined privacy apps

Restricting an app can generally be achieved by following two approaches: either by restricting the environment or by modifying the application. Specifically, the following approaches could be identified:

Manifest file (man): An android application that shall have access to the resources of the smartphone, e.g. contacts or internet connection, needs permissions granted by the user. The information on requested permissions is contained in the so-called Manifest File. This file contains meta information, is part of the source code and created during the implementation of the application. The apps examined manipulate this manifest file by modifying the sequence containing the permissions that need to be requested. This procedure requires a new installation of the apps concerned.

Adding a security library (bib): Adding a security library works as follows: The byte code or the source code of the app to be modified is examined with respects to its methods. Then, a separate program code is added to the byte code or source code. This added program code can record and control certain function calls. Consequently, this modifies the source code of an app.

AppOps (ao): Subsequent removal of permissions or selective granting of permissions was implemented in the operating system Android as a feature of the OS version 4.3. However, this

feature has been removed, respectively hidden, with the OS version 4.4.2. Some of the apps examined activate this hidden setting option in order to restore its functionality for the user.

Custom-Rom (cr): Mobile Operating Systems can be divided into two categories: “Custom-ROM” and “Stock-ROM”, the latter being operating systems pre-installed by the manufacturer. “Custom-ROM” refers to operating systems of third-party suppliers that are not pre-installed by the manufacturer. Android operating systems modified by third parties, for instance CyanogenMod, Dirty Unicorns or PAC ROM, also belong to this category. The installation of a Custom-ROM is complex and depends on the manufacturer of the device and the respective Custom-ROM.

XPosed (xp): The XPosed framework allows the installation of different modules that can alter the operating system (Stock-ROM) without de-installing the operating system and replacing it by a so-called custom-ROM. It “replaces” the Android framework. One of these modules is the XPrivacy Module. Using the XPosed Framework one can interfere in every process, i.e. every installed app, respectively alter every method at runtime.

3.2 Usability of the examined data privacy applications

The evaluation of the identified apps is conducted according to the criteria *usability* and *functionality.* Within the scope of the AVARE project aims usability means especially *usability for legal and technical laymen*. Usability can furthermore be distinguished according to the following aspects:

Comprehensibility (How easily comprehensible is the application?)

Learnability (How difficult is it to learn?)

Operability (How much effort needs to be expended to operate the app)

Attractivity (Attractivity of the software)

Conformity (Compliance of the software with standards and agreements –ISO/ IEC, 1991)

It was not an aim of this study to deliver a complete evaluation and analysis of the applications’ usability. While assessing the apps it was stated that –according to their implementation and working method- they impose certain hurdles for the user concerning installation and handling.

These aspects belonging to the concept of usability as described above will be presented in the following. In order to achieve an ease of use for technical laymen, there should be as few obstacles as possible for installing the manager app or for making settings. The following potential obstacles were identified:

Root: Does the app require root access? (Releasing the root access, the so-called “rooting”, of a smartphone can already be regarded as technically demanding)

Store: Is the app available in the Google Play Store? (Is it easy to install and as the user is used to?)

Dependencies: Are there further technically demanding dependencies that have to be fulfilled? For instance, is it necessary to install additional libraries for the app to work at all?

New installation: In order to control an app or to change settings is it necessary to reinstall the app in question?

Update Ability: Do once adjusted settings remain in place after an update of the controlled app? (Respectively, is the update of a controlled app possible at all?)

User requirements: To what extent the user must be technically experienced to use the app reasonably?

For the factor *user requirements*, grades were assigned, which are explained in the following list:

1: The app allows general or abstract settings (for instance, rules like “Provide all apps with fake contacts instead of my real contacts”)

2: The app gives recommendations for settings (for instance, from which apps permissions should be removed)

3: The app explains possible settings

4: The app only allows to make settings

5: The user cannot make settings without technical know-how

+ or – were assigned, if the app fulfills the usability level corresponding to the grade particularly well or comparatively bad.

3.3 Functionality of the examined data privacy apps

All examined data privacy apps allow creating a data privacy profile. Regarding their functionality, the data privacy apps vary in terms of what personal data they deny or restrict access for. Furthermore, the data privacy apps differ in whether and how they prevent data leakage. This results in the following criteria:

The app denies access to…

Calender: e.g. doctor’s appointment

Camera: e.g. unnoticed pictures

Contacts: e.g. Telephone numbers of friends

Location Data: e.g. movement profile

Microphone: unnoticed audio recording

Sensors: e.g. Health data

SMS: e.g. personal messages

Storage: e.g. personal documents

Telephone: e.g. Calls list

Identity: e.g. clear ID of the device

Apps: e.g. installed applications

The apps prevents data leakage via…

Bluetooth: Communication with other Bluetooth devices

Internet: Internet access with W-LAN oder data network

NFC: Near Field Communication with other devices

System Apps: Can system apps also be controlled?

Advertising: Is advertising blocked specifically?

Table 1 lists the evaluation of all apps according to access, leakage and other criteria (system, advertising). Besides merely blocking the access (block), some apps allow the setting, that the user is asked for his permission (ask). In some cases the user can define that fake data shall be provided (fake).

				Usability						Functionality																
										Access											Leakage			Other	
Name	Creator	Arbeitsweise	Quellcode	Root	Store	Depen.	New inst.	Update.	User req.	Calendar	Camera	Contacts	Location	Microfone	Sensors	SMS	Storage	Telephone	Identity	Apps	Bluetooth	Internet	NFC	System	Advert.
AppOps	*nativ*	ao	no	yes	no	no	no	?	4	b	b	b	b	b	b	b	b	b	b	b	b	b	b	yes	no
APK Permission Remover	Steel-Works	man	yes	nein	yes	no	yes	no	3	b	b	b	b	b	b	b	b	b	b	b	b	b	b	no	no
Advanced Permission Manager	Steel-Works	man	yes	no	yes	no	yes	no	3	b	b	b	b	b	b	b	b	b	b	b	b	b	b	no	no
SRT AppGuard	Backes SRT GmbH	bib	yes	no	no	no	yes	yes	2	b	b	b	b	b	-	b	b	b	b	b	-	b	-	no	no
MoboClean	Mobo-Clean	bib	yes	no	no	no	yes	yes	2+	-	-	a b	f b	-	-	a b	-	a b	a b	-	-	b	-	no	no
Privacy Protector	Houzuo Guo	?	no	no	yes	no	no	?	4	-	-	-	b	-	-	-	-	-	-	-	b	b	-	no	no
LBE Security Master	Lamian	xp	no	yes	no	no	no	?	2+	-	a, b	a, b	a, b	a, b	-	a, b	-	a, b	a, b	-	b	b	-	yes	yes
Parasol	Parasol .cool	?	?	yes	no	no	no	?	2+	b	b	b	b	b	b	b	-	b	-	-	-	-	-	no	no
Gemini App Manager	SEASMIND	?	?	yes	yes	no	no	?	4	b	b	b	b	b	b	b	b	b	b	b	b	b	b	yes	no
Permissions Denied	Stephen (Stericson)	?	?	yes	yes	no	?	?	3	?	?	b	?	?	?	?	?	?	?	?	?	b	?	?	no

App Guard	Ganesh Pokale	?	?	yes	yes	no	?	?	3	?	?	?	?	?	?	?	?	?	?	?	b	b	?	?	no
Pdroid	mateorod	cr	no	yes	no	yes	?	?	4	?	?	?	a, b, f	?	?	?	?	?	a, b, f	?	?	?	?	?	no
XPrivacy	Marcel Bokhorst	xp	no	yes	yes	yes	no	?	3-	a, b	a, b	a, b	a, b	a, b	a, b	a, b	a, b	a, b	a, b	a, b	?	a, b	a, b	no	no
Kapauer	Azalgo	xp	no	yes		yes	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
Permission Master	Droid Mate	xp	no	yes	yes	yes	no	?	3	b	b	b	b	b	b	b	b	b	b	b	b	b	b	no	no
3c Toolbox	3c	xp	no	yes	yes	yes	no	?	3-	b	b	b	b	b	b	b	b	b	b	b	b	b	b	yes	no
MinMinGuard	FatMinMin	xp	no	yes	no	yes	no	?	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	?	yes
AdBlocker	Kubinkie	xp	no	yes	no	yes	no	?	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	?	yes

Tabelle 1: Manager Apps