PRIVACY-AVARE: An Approach to Manage and Distribute Privacy Settings

Sascha Alpers, Andreas Oberweis, Maria Pieper

FZI Forschungszentrum Informatik
Karlsruhe, Germany
e-mail: {alpers, oberweis, pieper}@fzi.de

Stefanie Betz, Andreas Fritsch,
Gunther Schiefer, Manuela Wagner

Karlsruher Institut für Technologie
Karlsruhe, Germany
e-mail: {stefanie.betz, andreas.fritsch, gunther.schiefer,
manuela.wagner}@kit.edu

***Abstract*—Privacy enhancing technologies become increasingly necessary as more and more personal data is collected. Especially, as nowadays everybody is permanently online using different applications and devices, users are often lacking the means to effectively control the access to their private data. Existing approaches provide only isolated solutions for one device and are limited in functionality to control data access. Moreover, existing solutions may not be legally compliant and lack usability, especially for non-experts. Therefore, we present an interdisciplinary approach to manage and distribute privacy settings: PRIVACY-AVARE is intended to enable users to centrally determine their data protection preferences and to apply them globally on different devices (mobiles, tablets, smart homes, cars, ...). In this paper, we present PRIVACY-AVARE by first introducing and discussing main functional and non-functional requirements with a special focus on compliance and usability requirements. Based on this discussion, we then develop a conceptual solution. Finally, we discuss the limitations of our approach and give an outlook.**

Keywords-data protection; mobile apps; privacy enhancing technologies; data sovereignty; usability; legal conformity

I. INTRODUCTION

Everyday life is increasingly characterized by globally connected ubiquitous Information and Communication Technology (ICT). Especially the ubiquitous internet means that citizens and things (like a smart TV) are permanently online, which results in a considerable change of social and business life as well as communication in general. Smartphones, digital social networks, commercial rebate systems, cloud applications and ubiquitous computing lead to an increasing value of personal information. This information is collected, stored, evaluated and exploited, partly without the user being aware of it although European data protection provisions require an adequate level of transparency [1, S. 121]. In contrast to legal obligations like minimizing the data collection, many apps are “overprivileged”, that is, require more privileges than they actually need [2], [3]. In addition, advertising libraries, which are often integrated into free apps to generate revenue, are a potential privacy risk: they receive the same permissions as the apps they are integrated into, but they might use them to provide detailed user profiles [4]. Regardless of advertising libraries, it is not always necessary, that users are clearly identifiable via IDs (for instance, in case of iOS the Unique Device Identifier), but many applications use this information and transfer it only partially encrypted to the respective provider [5]. If users disclose also third persons' personal information (like contact information) without their consent, they can be held liable for data protection infringement [6]. In this complex scenario, users can hardly protect their privacy, especially given the fact that they must solve this problem for different devices. Therefore, it is important to help users protecting their personal data through privacy enhancing technologies. However, researchers face a so called privacy paradox: users often express their concerns on phenomena like Big Data or Internet of Things and the desire for enhancing privacy on the one hand but simultaneously use privacy infringing applications or services without applying privacy protecting solutions on the other hand [7]. There are several approaches to explain this paradox, like the users' missing awareness of privacy risks due to a lack of proper information [8]. Another reason could come from aspects like availability of privacy preserving solutions and effort or expenses involved [9]. Additionally, network effects determine which network a citizen uses. That is why more privacy sensitive alternatives to WhatsApp like e.g. Threema cannot get a big market share if they enter the market after the big player [10]. Therefore, legal conformity, technical functionality and usability could be the key factors for the success of a privacy enhancing solution.

Thus, the question is how to enable a user-friendly restriction of the exposure of personal user data, while allowing users to still benefit from the full range of useful applications – often only offered for free in “exchange” for personal data. In Europe, the upcoming General Data Protection Regulation empowers the citizens' self-determination and obliges app providers to use data minimizing default settings. These obligations also apply to international companies outside the EU, if they offer goods and services to people located within the EU or monitor their behaviour. If app providers violate these obligations, technical control and enforcement mechanisms can support users to claim their right to data protection, but might cause legal infringements with regard to copyright, civil, criminal or public law. If users risk legal consequences they might feel deterred from using privacy solutions. Moreover, in order to limit complexity and involved effort, users should be able to centrally define privacy settings in accordance to their individual preferences once, which then are distributed and enforced on (all) devices of the user.

The outline of the paper is as follows: In the next section (Access Right Management), we discuss existing possibilities for users to control access to their private data with respect to functionality, legal compliance and usability. Our analysis is focused on Android for mobile devices as Android has the biggest market share and is open source [11]. However, the principles apply to any modern operating system. The results of this analysis form the basis for a set of basic requirements for a distributed privacy enhancing system. The requirements are presented in the following section (Requirements Analysis). Then, we describe in section PRIVACY-AVARE our concept for distributed data access control. The main contribution of our concept is the combined consideration of technical, legal and usability concerns. In order to evaluate our approach we discuss our conceptual solution with respect to the initial requirements in the section discussion. Finally, we provide a summary and outlook for future work, including a prototypical implementation of our system for Android devices.

II. ACCESS RIGHT MANAGEMENT

A prerequisite for any approach to enhance privacy is the technical possibility for the users to control access to their private data. For example, to manage privacy settings, both iOS and Android implement an authorization system. In order to be able to access certain personal data such as appointments or contacts, an application must apply for this authorization. Some permissions are then granted automatically by the operating system, others can be given by the user at runtime (iOS and Android version 6 or later) or during installation (Android). Additionally, Android draws a distinction between "normal" and "dangerous" permissions. Setting the time zone would be an example of a normal authorization, while access to contact information is classified as dangerous [12]. However, this predefined classification must be considered critically, since, for example, access to the Internet is one of the "normal" authorizations. This entitlement is questionable for data protection since collected personal data can easily be passed on to third parties over the internet connection.

Different authors have proposed approaches to improve the existing access rights management implementations for iOS and Android in terms of usability and functionality (that is, cognitive and technical empowerment of the user to effectively control data access). These include, for example, the identification and visualization of data outflows [13], the provision of substitute data (shadow data) on access, and the blockade of accesses [14]. Furthermore, in order to allow better data protection decisions by the users, the justification of requests of authorizations is suggested [15]. Another significant point are fine-grained permissions [16] when protecting privacy on any device. It is important to provide the possibility for fine-grained and unambiguous privacy settings.

A. Existing Solutions

As one can see from the discussion above, there is a need to enhance and improve upon the built-in access rights management solutions for mobile devices. And indeed, there are already several applications available to manage the privacy settings. They all have in common, that they try to improve the existing mechanisms to either allow more fine-grained control or better usability. Three kinds of approaches do exist from a technical viewpoint:

1. Remove authorizations via the modification of the manifest file (e.g. Advanced Permission Manager)
2. Add a security library (e.g. SRT AppGuard)
3. Make a modification at the operation system level (e.g. XPrivacy)

Fig. 1 shows these three approaches, visualizing modifications of the (source) code in dark blue. These modifications possibly provoking compliance considerations are discussed below. The latter two solutions use sandboxes. A sandbox is referred to as environment, which restricts actions by an application according to defined rules [17]. By an access restriction the risk of a violation of the defined rules is reduced [18]. This concept, derived from IT security, was adapted to data protection, e.g. by [19].

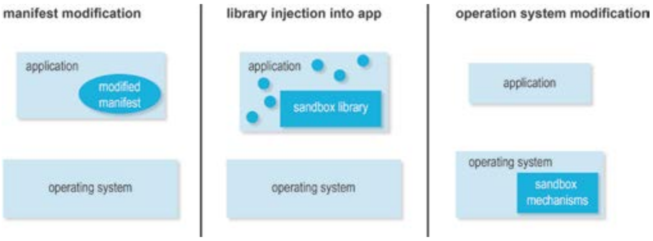


Figure 1. Different mechanisms for right management

We have published an overview of our analysis on existing solutions regarding access management for user support [20], including a comprehensive assessment concerning usability and functionality aspects. In the following, we discuss identified drawbacks concerning relevant aspects of functionality, compliance and usability.

B. Limitations of existing solutions

<u>Functionality</u>

If monitored applications stop working in case of blocking data access, users might feel compelled to unblock and give up privacy protection. Therefore, possibilities to reveal only a selected part of information (e.g., only several contacts or only telephone numbers hiding further information) or provide substitute data are essential functionalities. Currently, only a few solutions grant these options e.g. PDroid or MoboClean (partially) [21].

In case of code modifications the possibility to update monitored apps might be impaired [22]. Furthermore, most solutions require users to adjust privacy settings per app manually, which can be very time-consuming.

<u>Compliance Considerations</u>

Technical solutions editing the code of computer programs may face copyright infringements [23], [24]. Apps and the operating system are protected under European and international copyright law, as long as the creation required a creative effort and the output is not only dependent on functional considerations. If there is no legitimating license (e.g. open source), customizing requires the permission of the relevant rights' holders or an exemption by law. The European copyright law grants an exemption, if editing of the code is necessary to provide or maintain the designated use of the program. Legal scholars argue this should also involve the legal conformity of a program meaning, that apps or operating systems infringing data protection law could be edited by the users to achieve conformity with data protection obligations [23], [24]. The first problem is that users would have to decide whether a program is infringing data protection regulations or not. The second problem is that "designated use" is not given if editing or blocking data access causes impairments of the functionality of an app. Thus, legal uncertainty remains whether alterations of program code may be justified in order to establish data protection compliance.

Usability Considerations

Basic usability is often overlooked in existing privacy apps (see e.g. [25]). Apart from that, the usability of existing solutions is interlinked with the technical and legal considerations: most of the currently available apps that allow users to manage data access in more detail require a relatively high level of technical proficiency. Especially the more powerful solutions like for example XPrivacy and LBE Security Master require a rooted device and the installation of additional dependencies. These technical hurdles may prevent users, which would otherwise be interested in protecting their privacy better, to actually apply such a solution. Moreover, users face the risk that guarantee or warranty claims are rejected, if the device is rooted. From a legal point of view, distributers or manufacturers are not entitled to exclude warranty rights provided by European / German law, but can restrict a voluntary provided guarantee to conditions as long as these conditions comprise no unreasonable disadvantage to the customers. In judicial proceedings, it might be challenging to proof that the defects are not caused by the user's software adaption. In case of consumer good purchases the seller / producer bears the burden of proof, if the defect is discovered within the first six month. After this period the owner of a rooted device would have to prove that the defect did not occur due to the rooting when claiming warranty.

III. Requirements Analysis

Our goal is to improve upon the existing solutions for access rights management by developing an overarching approach that not only provides the essential functionality, but also accounts for legal compliance and usability. There is a need for an innovative and user-friendly software application that prevents the exposure of personal data, enabling users to centrally define privacy preferences, which then are distributed and enforced on all devices of the user. Also, next to the possibility to enable fine-grained settings of the permissions, we need to provide functions such as pseudonymization or special data record filters to further enable the usage and control of third party applications. Finally, the exercise of effective, technically supported privacy and data protection must take also into account aspects of copyright, civil, criminal and public law. In the following, we describe the central functional (F), compliance (C), usability-related (U), and two additional non-functional (G) requirements that such a solution should fulfil. These requirements have been verbalised based on an extensive analysis of existing solutions and current literature [20], including a comprehensive assessment concerning functional, compliance, and usability aspects:

F-1: Data Blocking and Filtering

A privacy solution must provide the main function to block or filter the data communication between operating system and applications, the user wants to control. Also the data communication between the hardware (e.g. sensors) and applications must be included in the blocking / filtering mechanism to empower the user to control the data communication.

If apps react with failure to a denied data access, even if this blocked data is not necessary to perform the (main) function of the service, mechanisms are required to maintain the functionality. This can be achieved by providing substitute data.

F-2: Ubiquity

Entering privacy-settings once centrally for all devices require a method of secure distribution and actualization. To support the users to protect their data the privacy enhancing technology must be available and enforceable on all relevant platforms and the settings of the user must be shareable over different devices and platforms so that the user needs to configure the solution only once.

C-1: Data security and privacy

Storing personal data protection preferences needs to comply with data protection regulations. The privacy enhancing technology should keep privacy preferences and data (e.g. data that is read during the filtering mechanism) secret and protect these data from attackers and from central service providers. This is important because a privacy enhancing mechanism that acts as data flow control mechanism and with a filtering option discovers a high amount of personal data itself and has to store some of these data, too.

C-2: No infringement of copyrights

In order to ensure legal conformity of the conception, legal questions deriving from copyright, civil, criminal and public law have to be addressed. First, the solution should not infringe copyrights. In Germany there is a dispute whether an infringement is only given, if the code of a protected program is edited [26], or if a change in the program sequence can already comprise an infringement [27]. As the functions of a program are not protected under European copyright law, but the code as a manifestation of the creative conception, the latter opinion could jeopardize the possibilities of program interaction and interoperability [28], which are important objectives of European law. The system should require no source code modification and alterations to the program sequence should be limited to a minimum.

C-3: No breach of contract

As there is no legal obligation to provide personal data even in case of a business model "service in exchange for data" under current law, blocking data access causes no legal infringements. A proposal of the EU commission seeks to legalize contractual agreements about personal data in return for digital content, in case the data is provided actively [29]. However, this proposal conflicts with provisions of the upcoming General Data Protection Regulation (GDPR) in Europe. One key goal of the GDPR is to strengthen the voluntariness of consent in processing personal data. Therefore, a consent for processing data not necessary for the performance of a contract should be considered as invalid, if the consent is requested in exchange for the performance of the contract (Art. 7 para 4 EU 2016/679). As personal data give insights into the personality, human rights obstruct the usage of personal data as a kind of currency, product or property [30] In any case a contractual binding agreement to provide personal data in exchange for a digital service would require much more transparency than provided through privacy declarations or standard terms and conditions.

The utilization of substitute data requires meaningful selection to prevent breach of contractual duties to respect rights and freedoms of contractual partners, tort law infringements or even criminal offences. In the worst case the usage of false data in order to achieve anonymity like a false name, can comprise an illegal identity fraud, if the contractual partner has a legally recognised interest in the true identity of his opponent [31]. Whether there is a "right to lie" strongly depends on the fact, whether the opponent infringes data protection law or personality rights.

Furthermore, a misuse of the privacy application as a cheat software would be possible, if users had the option to choose ID or location data in order to pretend to be someone else or to have reached a certain position relevant e.g. in a game or employment relationship.

Summarizing, the main requirements arising from legal obligations or rather to minimize legal infringements are:

- providing substitute data only as a last resort
- users should not be able to determine substitute data
- substitute data comprises no information or as little information as possible
- transparency towards users about usage and methods of generating substitute data
- guidance for users about typical potential legal requirements

Overall, the usability requirements are focusing on an easy to use Human Computer Interface that allows non-experts to easily manage their privacy settings.

U-1: Simple Installation Process

One basic requirement from the perspective of user experience is to keep the technical hurdles of installation and usage at a minimum. This is important especially with regard to the existing work as these solutions require the user to have deep technical knowledge (see section “existing solutions”).

U-2: Understandability of Privacy Settings

The usability of mobile privacy tools, especially the understandability of privacy settings, is a current research challenge (see e.g. [32], [33]). It has been shown, that users are often overwhelmed by the implications of privacy settings [32]. Therefore, the complexity of privacy-related decisions should be reduced. As a prerequisite, the development of the user interface should follow modern standards and best practices for usability.

The following two additional non-functional requirements are included because we think it is important to have no negative impact on the "user experience" when using our application.

G-1: Performance

The privacy enhancing technology is not allowed to reduce the perceptible performance of the system, especially of the user interface of the foreground app.

G-2: Energy consumption

Energy consumption must not rise substantially on mobile devices, because battery life is limited and the user expects his device to run at minimum for a certain time (e.g. one day) without additional energy supply.

IV. PRIVACY-AVARE

Based on the requirements described above, we have developed a concept for a distributed privacy management solution, named PRIVACY-AVARE. In the following, we first refine the basic functional requirements and then describe a system concept that implements these refined functionalities. We also describe in more detail, how such a system can account for the defined compliance and usability requirements.

A. *Refined Functional Requirements*

In order to enhance privacy our software application PRIVACY-AVARE will have the following three essential functionalities:

(1) Enter the user’s preference profile: PRIVACY-AVARE can be used to record the user’s privacy preferences. The user of PRIVACY-AVARE is supported by suitable explanations for technical and legal laypersons. It creates a personal preference profile. Therefore, we need a user-friendly comprehensive GUI and local data storage capabilities.

(2) Distribute the user’s preference profile: The preference profile can be distributed via a central service to all devices of the user. In order to secure the exchange, a technical requirement is an end-to-end encryption. Therefore, the user uses a locally created key to encrypt the preferences. The key is distributed to other devices either by embedding into a QR code, displaying on the first device and photographing by the second one or entered manually. This means that the users does not have to entrust their preferences to a central service in plain text; the key itself is not known to the central service.

(3) Enable the user to control data access: PRIVACY-AVARE enables the user to allow fine-grained data access. Therefore, PRIVACY-AVARE has different levels of data access control. Data access can be blocked or filtered. Furthermore, PRIVACY-AVARE provides the possibility to use substitute data (no data or specially generated data) in case the app stops working otherwise. This leads to the following technical requirements:

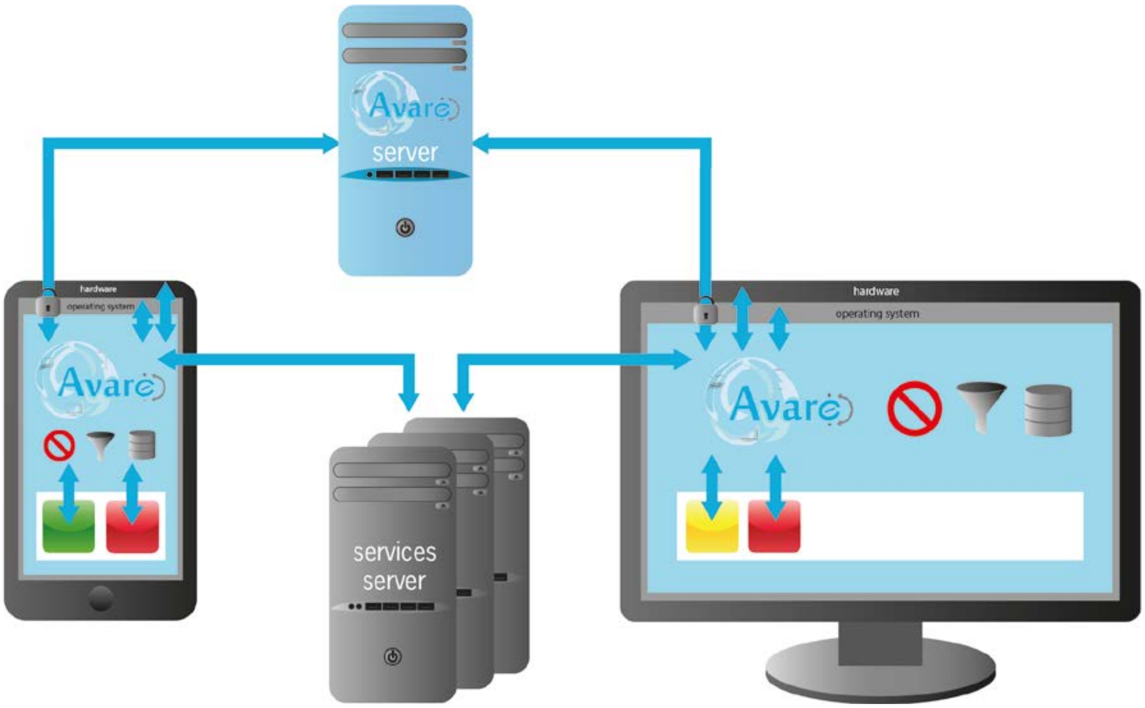


Figure 2. Operating Principle of PRIVACY-AVARE

a) PRIVACY-AVARE has to monitor data access requests at runtime and block data flows corresponding to the blockage rules set by the user.

b) PRIVACY-AVARE has to extract data as defined by filtering rules at runtime.

c) PRIVACY-AVARE has to deliver substitute data to an application that would otherwise react with failure to a denied data access. Thus, PRIVACY-AVARE has to be able to generate plausible substitute data.

d) PRIVACY-AVARE has to incorporate existing permission settings for specific applications.

Those data flow filtering and blockage mechanisms are being executed during runtime.

B. System Concept

From the refined technical requirements, we derive the following architecture: Fig. 2 shows an overview of the operating principle.

PRIVACY-AVARE is based on client server architecture. The server is responsible for storage and delivery of encrypted privacy profiles. The client enables the user to set his privacy preferences in three different levels of granularity. The privacy settings result in rules for data flow control. Furthermore, the client enforces these privacy data flow rules. The client's architecture is designed independently from specific platforms (i.e. Android, iOS, Windows). This facilitates the usage of PRIVACY-AVARE on several terminals (Smartphones, Smart-TV, Tablets) with different operating systems in various versions.

C. Client-Side Concept

As depicted in Fig. 3, the client consists of several components (dark blue boxes): Component 1, the profile capturing-component, enables the users to set their preferences. Those preferences can be set either by application-category-level or on application-specific level. The profile includes preferences for specific data-categories such as “Files”, “Contacts” or “Location”. For each application-category, we propose a set of pre-defined preferences which the user can adopt or overwrite / change on the category or on application-specific level. In order to apply category preferences the user needs to sort his applications into categories. Furthermore, by transmitting the profile via a server to different devices, the user is able to load his profile and sync it.

Component 2, the profile execution component, asserts the users preferences. First of all, we need a sandbox to securely execute third party apps within. Furthermore, we use a reference monitor to capture outgoing and incoming API-calls from or to the third party apps. The reference monitor also executes the rules regarding vertical and horizontal filtering of data or the blockage of data flows. Those rules are extracted from the preference setting component. For example, the user is able to allow a specific application to get only a specified set of his contacts. Another example for our filtering approach is the obfuscation of the user's location. The user is able to choose a location radius, for example 100 km.

D. Server-Side Concept

The server is responsible for synchronizing the privacy preferences of a user between his devices. Therefore, it is

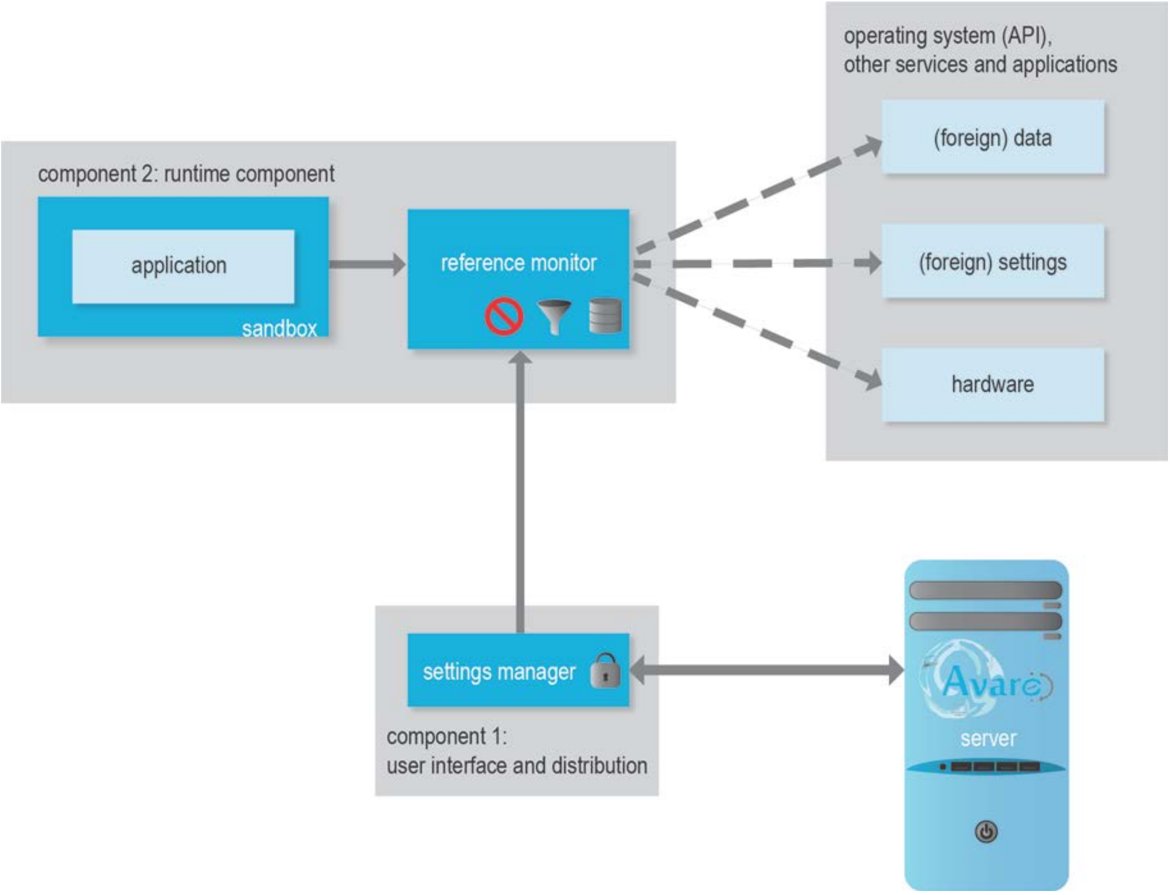


Figure 3. Overview of PRIVACY-AVARE client

necessary to store the encrypted preference profile and the timestamp of the last change under a profile ID. The profile ID is generated by the server when the user logs on for the first time and communicated to the user device. The user device remembers the profile ID and creates a key for symmetric encryption. The device now transmits only the profile ID, the timestamp of the last local modification of the preference profile and an encrypted data block containing the preference profile. The key itself remains on the user's device; the server and its operator are not able to read these preferences and consequently have no knowledge of it. By this means, no further information is stored about the user, so the profile ID is a pseudonym that the server cannot resolve.

The user can now transfer his profile ID and key to other devices. For this purpose, this information is embedded in a QR code and displayed on the display. This QR code can be read with another device. This other device can now log on to the PRIVACY-AVARE server and retrieve the encrypted stored preference profile. With the locally available key, the profile can be decrypted and transferred to PRIVACY-AVARE. Regardless of which device the user takes to make changes to his preferences, they are copied to the server in encrypted form and can be retrieved from the other devices from there. For this purpose, all devices regularly check with the PRIVACY-AVARE server, if there are newer settings and download them if necessary.

In order to store as little information as possible on the PRIVACY-AVARE server (data minimization), no information about the devices used is collected. This way, the profile is only encrypted as a whole. Storing the profile in several individually encrypted parts (e.g. separated by category) could reduce the amount of data to be synchronized, but would reveal more information about a user to the PRIVACY-AVARE server. Even though little critical information is transmitted in plain text, the connection between server and devices is additionally secured with transport encryption.

Users can stop synchronization on one or all of their devices at any time. They can also delete all of their data (profile, timestamp) from the PRIVACY-AVARE server. In addition, there will be a clean-up process that deletes outdated profiles that had no contact with a device for more than 18 months from the PRIVACY-AVARE server. If a user logs back to the server after the end of this period, his profile and ID are restored from his local data.

E. *Compliance*

As it should not be the obligation of the user to decide on complex legal questions, our concept is based on escalation steps minimizing potential infringements. Only if the blocking of data access leads to a loss in functionality of the app, empty data is provided (like an empty address book and calendar, no sound, …), so that the opponent cannot learn anything (wrong) from such data. If the app detects this protective measure, substitute data consisting of publicly available information is provided, in order to reveal no personal information about the user or third users and meanwhile reduce potential damages due to false data. Replacement data could be e.g. public holidays (calendar), public authorities / companies (address book), background noise (microphone), image noise (camera). Special cases are location data and IDs, as providing false location data could also lead to negative consequences for other users, e.g. when data is used by the app provider for traffic jam prediction.

F. *Categorization*

One usability-related goal of PRIVACY-AVARE is to reduce complexity for the user, while still providing the capabilities to effectively enforce privacy preferences. With PRIVACY-AVARE, we aim to support the users in their decisions, by providing recommendations for app categories based on expert judgements. This way, our solution can provide the additional benefit of teaching the user about potential privacy threats and sensible settings. The idea is to categorize apps into groups with similar functionality. A category captures various applications with similar functionalities. For example, one category consists of applications providing navigation functionality. Each category shares a specific set of data usage permissions. The category navigation, for example, needs the location of the user. Suitable permission sets for common categories of applications are provided and set by default but can also be adapted individually by the user. This bears two advantages: First, the user does not have to think about every single app, but can apply her or his privacy preferences once for each category. Second, PRIVACY-AVARE can give recommendations for privacy settings to further support the user. This even opens up the possibility to teach useful settings corresponding to app functionality and possible privacy risks. In the following, we describe our approach to the initial categorization:

As a first step, the relevant kinds of personal data that are stored on a mobile device were identified. Based on the Android permission system, we identified 10 potentially critical ways for apps to access personal data (Camera & Microphone, Location, Sensors, Phone Calls and SMS, Contacts, Calendar, Accounts, Files, Identity and Messages) and additionally three ways for apps to transfer personal data (via Internet Access, Bluetooth or NFC).

In a second step, the identified data access / transfer possibilities were mapped to application-categories. These categories were initially compiled from the existing categories in the Android and iOS app stores. For each application-category and data access / transfer possibility, PRIVACY-AVARE provides a recommendation, whether access should be prohibited, allowed or filtered. To achieve this, results from a user survey (with 14 participants) and judgments from experts (6 participants of the IT security and privacy projects) have been aggregated and served as a basis for discussion and consensus finding between the authors of this paper. On the basis of this consensus, categories with similar profiles have been combined to a total number of 11 app categories.

V. Discussion and Limitations

A. *Technical Limitations (see F-1 to F-2)*

From a conceptual point of view the presented privacy enhancing approach PRIVACY-AVARE fulfils the above presented requirements. Data blocking, filtering and providing substitute data will be achieved by the reference monitor, while the specific implementation will vary according to the operating systems versions. As existing API are used and no manipulation of the code is required, an infringement of copyright is not expected - an advantage over existing access rights management approaches (see page 2). The possibilities to block all categories of data, filter data vertically and horizontally and provide substitute data if necessary comprise essential improvements in comparison to the functionalities provided by Android (from Version 6) and iOS. As this implies the selection of several possible settings, usability is enhanced by categorization, default settings and comprehensible guidance. Rooting of the device is not required so that the installation process is manageable for technical laypersons and guarantee or warranty rights are not at risk. Due to the architecture concept ubiquity and data protection are achieved. The reduction of processed personal data to an essential minimum and the use of encryption for storage and distribution over the internet already complies with the requirements of privacy by design and data security placed by the upcoming GDPR.

One technical challenge for the profile execution component is an implementation-based challenge. Each Operating System offers different technical implementation regarding security and communication aspects. Furthermore, the Android platform can vary its concrete communication implementation on a version-based level. Therefore, we have to consider those variations for the profile execution component in order to be able to catch an applications API call. This leads to different, version-specific implementations of the profile execution component. As there are currently several different Android Versions available, in use and constantly evolving we focus on Android 6 and Android 7. The implementation on each version varies cause of different implementation of the sandbox mechanism, but several codes can be shared (e.g. for filtering data, for generating smart blurred position data).

B. *Compliance Limitations (see C-1 to C-3)*

Although we tried to minimize the risk for data security and privacy threats by technical means such as using transport encryption during server and client communication, a residual risk remains.

By careful selection of substitute data, legal infringements are minimized. But as various constellations are hardly predictable, legal conformity will not be achievable completely without the participation of the user. PRIVACY-AVARE cannot react automatically e.g. to a change of purpose of data processing by an application which might lead to a different consideration concerning the possibilities to provide substitute data. One approach could be the automated analysis of data protection declarations or terms and conditions. Currently, the information provided in these declarations is mostly too vague to draw clear and unambiguous conclusions. Therefore, we support the user by providing explanatory symbols and texts, specific to the category.

Regarding user IDs the challenge is to identify cases where a wrong ID might cause legal consequences and to provide false IDs which are not linked to another person.

C. *Usability Limitations (see U-1 to U-2)*

In order to use PRIVACY-AVARE, the users are not required to root their device or to install additional dependencies in advance.

Regarding our approach to reduce complexity for the user via pre-defined categories, there is a risk that the categories do not capture all relevant kinds of apps and privacy settings. Still, for the categories to support the users in their decisions, it is important to find a balance between specificity of the categories and the total number of categories. A too high number of categories would jeopardize the goal of reduced complexity. We intend to address this risk by allowing the users to create their own categories. It would also be possible to integrate further mechanisms to support the user in properly categorizing the apps. For example, Liu et al. [33] propose a system that recommends predefined setting profiles to the user, based on some initial questions. Oglaza et al. [34] propose a self-learning system that learns from the user's previous decisions to recommend high-level rules. However, this implies that the privacy protecting application likewise needs to process personal data and discover personal preferences.

In order to ensure an easy to use interface we also have iterative usability tests for our prototype. These are intended to identify and address possible usability issues early on during development.

D. *Limitations to general requirements (see G-1 to G-2)*

Enhancing privacy by a sandboxing and data flow control solution with e.g. filtering mechanism can't be done without additional processing and memory effort at runtime. Therefore the implementation reduces performance and enlarges energy consumption. It is only possible to keep the additional effort at a level that does not matter for normal and high-end devices. But for devices with low resources the implementation could have an annoying effect.

VI. Summary and Future Work

In this paper, we describe a privacy enhancing approach respecting functional, legal and usability requirements to enforce the users' privacy preferences centrally on all their devices. The application PRIVACY-AVARE enables the user to define individual privacy settings once and enforce these preferences on all devices by blocking or filtering data access in the first step. If a monitored app reacts with denial of service PRIVACY-AVARE provides empty, blurred or substitute data in the last step. The selection and range of substitute data is limited due to legal considerations and accompanied by explanatory guidance. This interdisciplinary approach ensures the practical applicability of the technical solutions. By using a reference monitor along with sandboxes to restrict data access copyrights should not be affected. The distribution of privacy settings is encrypted to preclude additional privacy risks. The effort to select privacy settings is manageable for laypersons due to prior categorization and default settings. Currently, we are working on a prototypical implementation for Android devices. For the future, we are planning more iterative usability tests to further enhance the usability and the integration of different kind of devices like Smart Home devices.

We will publish the code as open source (under the apache 2.0 licence) until April 2018 on GitHub (https://github.com/fzi-forschungszentrum-informatik/PRIVACY-AVARE) and are working on building a community for the further improvement and development of PRIVACY-AVARE.

Acknowledgment

This work has been financed by the Baden-Württemberg Stiftung gGmbH within the project 'AVARE'.

References

[1] W. Christl and S. Spiekermann, Networks of control: a report on corporate surveillance, digital tracking, big data & privacy. Wien: Facultas, 2016.

[2] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, „Android permissions demystified", in *Proceedings of the 18th ACM conference on Computer and communications security*, 2011, p. 627–638.

[3] A. P. Felt, K. Greenwood, and D. Wagner, „The effectiveness of application permissions", in *Proceedings of the 2nd USENIX conference on Web application development*, 2011, p. 7–7.

[4] R. Stevens, C. Gibler, J. Crussel, J. Erickson, and H. Chen, „Investigating User Privacy in Android Ad Libraries", in *Proceedings of the 2011 annual conference on human factors in computing systems*, Vancouver, BC, Canada, 2011.

[5] E. Smith, „iPhone applications & privacy issues: An analysis of application transmission of iPhone unique device identifiers (UDIDs)", *URL www. pskl. us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues. pdf*, 2010.

[6] Local Court Bad Hersfeld, *F 120/17 EASO*. 2017.

[7] L. Vervier, E.-M. Zeissig, C. Lidynia, and M. Ziefle, „Perceptions of Digital Footprints and the Value of Privacy":, 2017, p. 80–91.

[8] D. Leibenger, F. Möllers, A. Petrlic, R. Petrlic, and C. Sorge, „Privacy Challenges in the Quantified Self Movement – An EU Perspective", *Proceedings on Privacy Enhancing Technologies*, Bd. 2016, Nr. 4, Jan. 2016.

[9] Forum Privatheit, „White Paper Selbstdatenschutz". Nov-2014.

[10] M. Schreiner and T. Hess, „Examining the role of privacy in virtual migration: The case of whatsapp and threema", 2015.

[11] Gartner, „Global smartphone sales to end users from 1st quarter 2009 to 1st quarter 2017, by operating system (in million units)". Statista, 2017.

[12] Google, „System Permissions | Android Developers", 2016. [Online]. Verfügbar unter: https://developer.android.com/guide/topics/security/permissions.html. [Accessed: 21. Jun. 2016].

[13] B.-G. Chun *et al.*, „TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones“, 2010.

[14] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, „These aren’t the droids you’re looking for: retrofitting android to protect data from imperious applications“, in *Proceedings of the 18th ACM conference on Computer and communications security*, 2011, p. 639–652.

[15] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang, „Expectation and Purpose: Understanding Users’ Mental Models of Mobile App Privacy Through Crowdsourcing“, in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, New York, NY, USA, 2012, p. 501–510.

[16] M. Nauman, S. Khan, and X. Zhang, „Apex: extending android permission model and enforcement with user-defined runtime constraints“, in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, 2010, p. 328–332.

[17] M. Bishop, *Computer Security: Art and Science*. Addison-Wesley Professional, 2003.

[18] I. Goldberg, D. Wagner, R. Thomas, and E. Brewer, „A secure environment for untrusted helper applications: Confining the wily hacker“, in *Proceedings of the 6th conference on USENIX Security Symposium, Focusing on Applications of Cryptography*, 1996, Bd. 6

[19] M. Backes, S. Bugiel, C. Hammer, O. Schranz, and P. von Styp-Rekowsky, „Boxify: Full-fledged App Sandboxing for Stock Android.“, in *USENIX Security*, 2015, p. 691–706.

[20] „Existing Software“, 2017. [Online]: http://projects.aifb.kit.edu/avare/existing_software/. [Accessed: 18-August-2017].

[21] S. Alpers *et al.*, „AVARE Projektbericht, 1. Meilenstein“, 2016. (https://publikationen.bibliothek.kit.edu/1000063418)

[22] M. Backes, S. Gerling, C. Hammer, M. Maffei, and P. von Styp-Rekowsky, „AppGuard–Fine-grained policy enforcement for untrusted Android applications“, in *Data Privacy Management and Autonomous Spontaneous Security*, Springer, 2014, p. 213–231.

[23] E. Bodden, S. Rasthofer, P. Richter, and A. Roßnagel, „Schutzmaßnahmen gegen datenschutz- unfreundliche Smartphone-Apps: Technische Möglichkeiten and rechtliche Zulässigkeit des Selbstdatenschutzes bei Apps“, *DuD*, Bd. 37, Nr. 11, p. 720–725, 2013.

[24] A. Brummund, „Smartphones and Apps: Datenschutzrechtliche Risiken and deren Begrenzung.“, in *GI-Jahrestagung*, 2014, p. 539–550.

[25] H. Assal, S. Hurtado, A. Imran, and S. Chiasson, „What’s the deal with privacy apps?: a comprehensive exploration of user perception and usability“, in *Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia*, 2015, p. 25–36.

[26] G. Spindler, „Grenzen des Softwareschutzes“, *CR*, Bd. 28, Nr. 7, p. 417–422, 2012.

[27] T. Conraths, „Der urheberrechtliche Schutz gegen Cheat-Software“, *CR*, Bd. 32, Nr. 11, p. 705–708, Jan. 2016.

[28] District Court of Hamburg, Bd. case 308 O 46/16. 2016.

[29] EU Commission, Proposal for a directive of the European parliament and of the Council on certain aspects concerning contracts for the supply of digital content. 2015.

[30] European Data Protection Supervisor, „Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content“. 14th March 2017.

[31] W. Buggisch, „Fälschung beweiserheblicher Daten durch Verwendung einer falschen E-Mail-Adresse?“, *NJW*, p. 3519–3522, 2004.

[32] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, „A conundrum of permissions: installing applications on an android smartphone“, in *International Conference on Financial Cryptography and Data Security*, 2012, p. 68–79.

[33] B. Liu, J. Lin, and N. Sadeh, „Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help?“, in *Proceedings of the 23rd International Conference on World Wide Web*, New York, NY, USA, 2014, p. 201–212.

[34] A. Oglaza, R. Laborde, A. Benzekri, and F. Barrère, „A Recommender-Based System for Assisting Non-technical Users in Managing Android Permissions“, in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 2016, p. 1–9.

2017 3rd IEEE International Conference on Computer and Communications

ICCC 2017

EXCELLENT PRESENTATION

This is certify that

Sascha Alpers

FROM

FZI Forschungszentrum Informatik, Germany

For certifying his/her oral presentation was selected as one of the best in

Session 17: Cryptography Theory and Security Technology

Session Chair
(Signature) Ning Jiang

Conference committee
(Seal)

IEEE International Conference on Computer and Communications ★ ICCC www.privacy-avare.de

PRIVACY-AVARE: An approach to manage and distribute privacy settings

Sascha Alpers, Stefanie Betz, Andreas Fritsch, Andreas Oberweis,
Maria Pieper, Gunther Schiefer, Manuela Wagner

3rd IEEE International Conference on Computer and Communications (ICCC)

13 Dec. – 16. Dec. 2017

Chengdu, China

Outline

- Introduction
- Privacy Paradoxon
- Existing Solutions
- Requirements Analysis
- PRIVACY-AVARE Concept
- Conclusion

Informational Self-Determination

general right of personality is provided by

- the protection of human dignity - Art.1(1) Grundgesetz
- the protection of general personal liberty - Art. 2(1) Grundgesetz

„general right of personality […] guarantees each individual the possibility to develop his/her own personality.“

In 1984 „the Bundesverfassungsgericht ‚invented‘ the new basic **right of informational self-determination**“

- based on the general right of personality

informational self-determination is – in Germany – the constitutional anchor for **data protection**

source / see also: G. Hornung und C. Schnabel, „Data protection in Germany I: The population census decision and the right to informational self-determination“, *Computer Law & Security Review*, 25(1), p. 84–88, Jan. 2009.

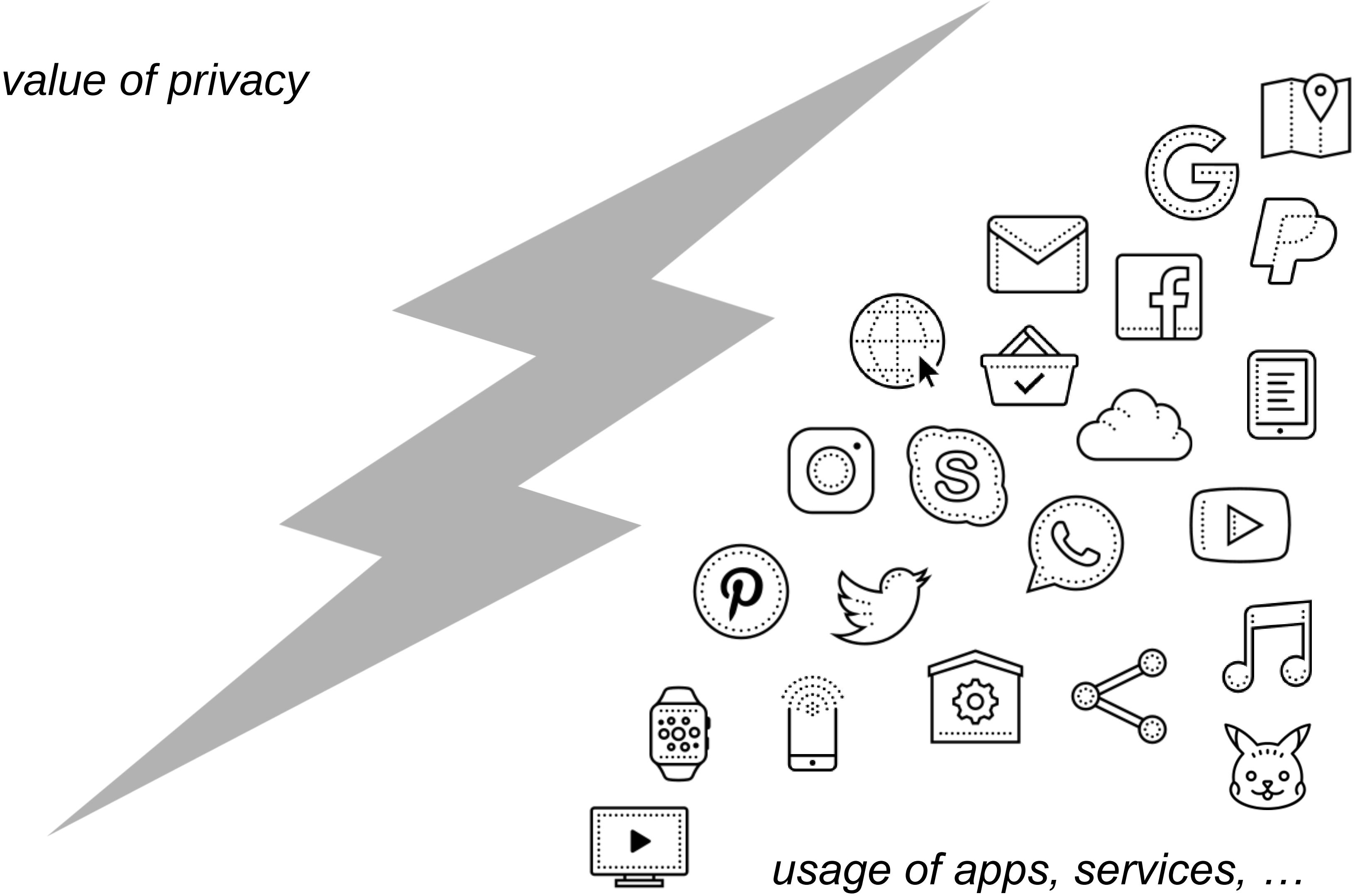
Chief Aim of Data Protection

- *not* about protecting data

- but about protecting each natural person
  - ➔ natural persons right to the protection of their personal data

Privacy Paradoxon

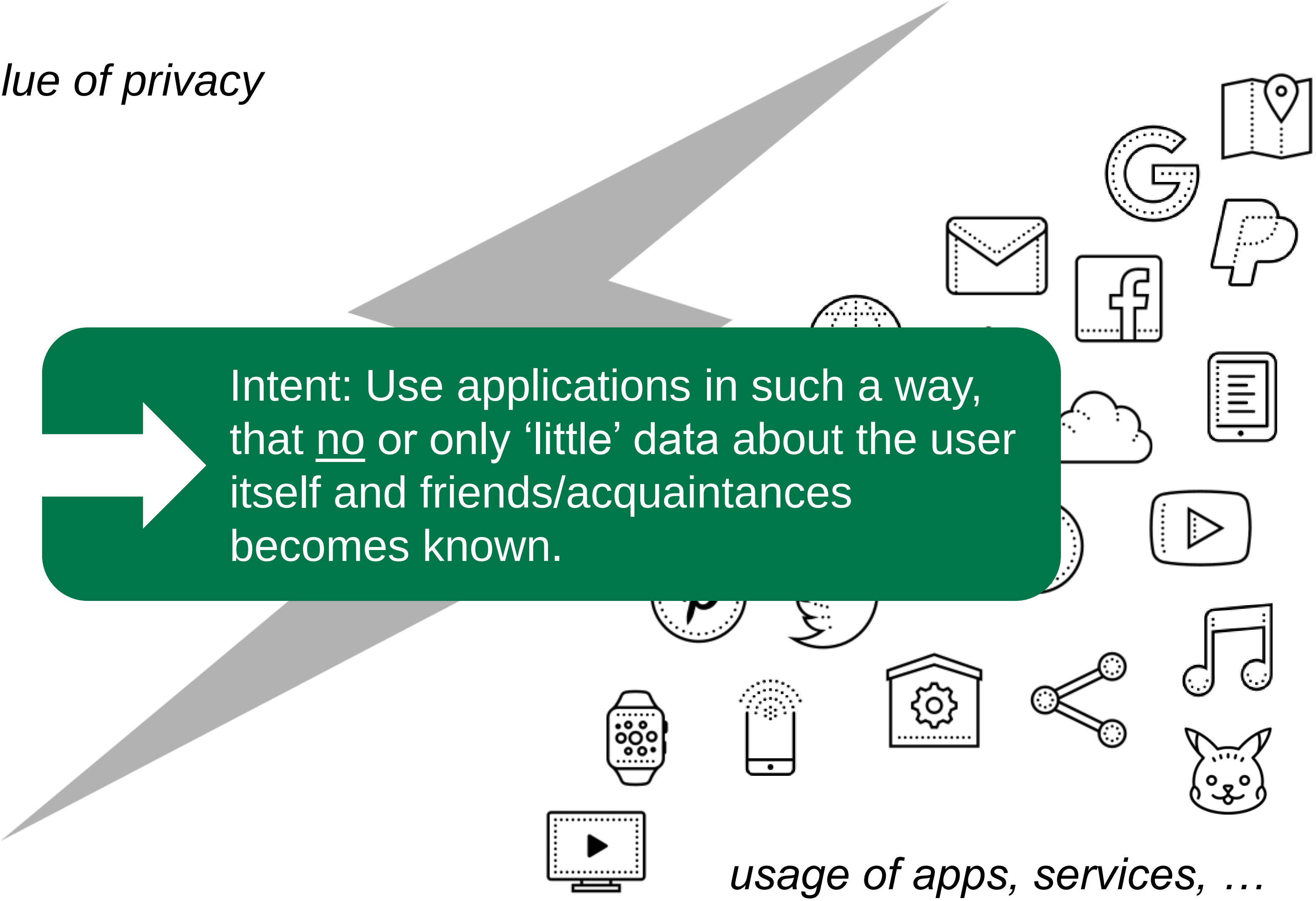
high value of privacy



usage of apps, services, …

Privacy Paradoxon

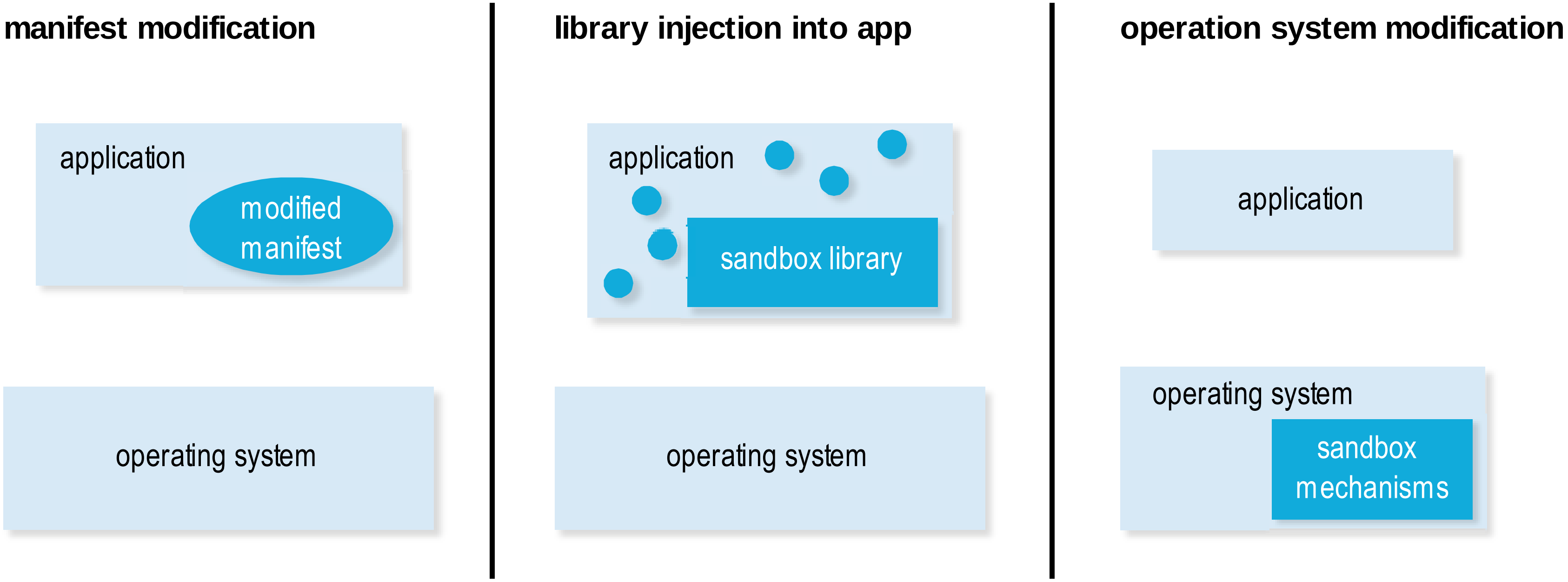
high value of privacy



Intent: Use applications in such a way, that no or only ‘little’ data about the user itself and friends/acquaintances becomes known.

usage of apps, services, …

Existing Solutions



manifest modification

application

modified manifest

operating system

library injection into app

application

sandbox library

operating system

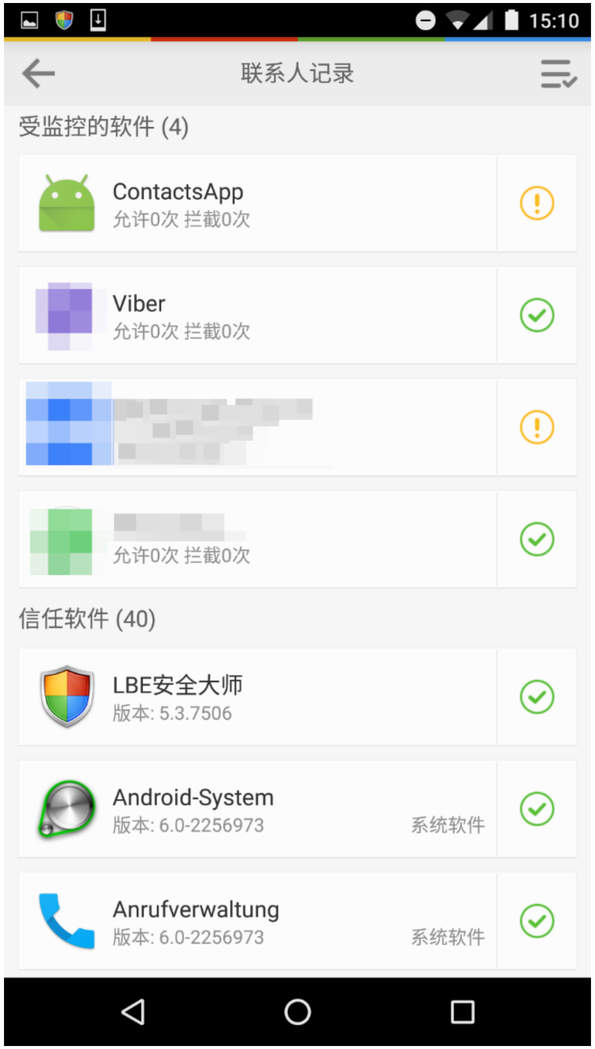
operation system modification

application

operating system

sandbox mechanisms

Existing Solutions



15:10

联系人记录

受监控的软件 (4)

ContactsApp
允许0次 拦截0次

Viber
允许0次 拦截0次

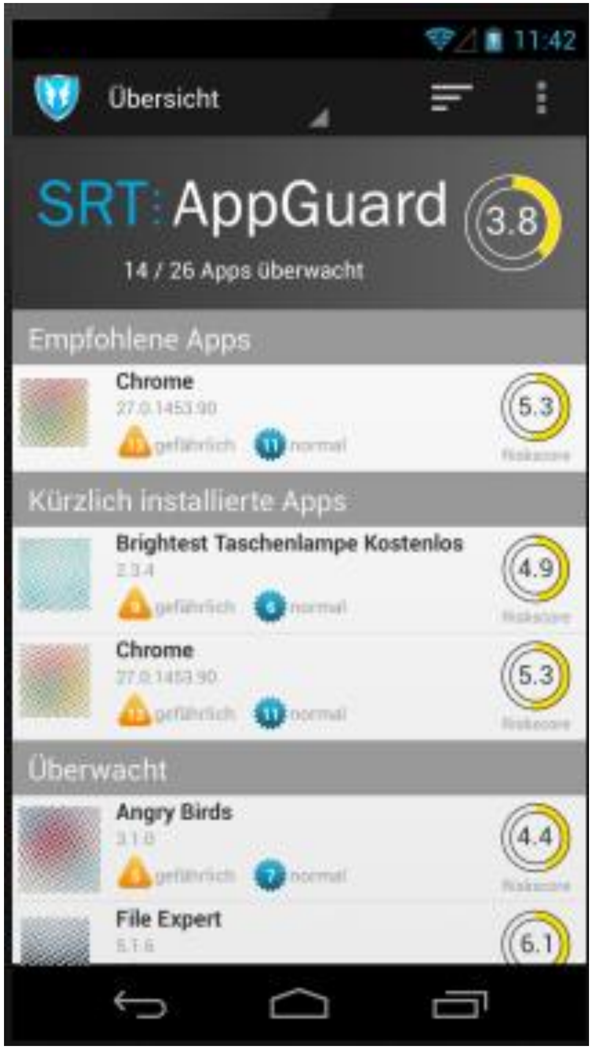
允许0次 拦截0次

信任软件 (40)

LBE安全大师
版本: 5.3.7506

Android-System
版本: 6.0-2256973 系统软件

Anrufverwaltung
版本: 6.0-2256973 系统软件



11:42

Übersicht

SRT:AppGuard 3.8

14 / 26 Apps überwacht

Empfohlene Apps

Chrome
27.0.1453.90
13 gefährlich 11 normal
5.3 Risikoscore

Kürzlich installierte Apps

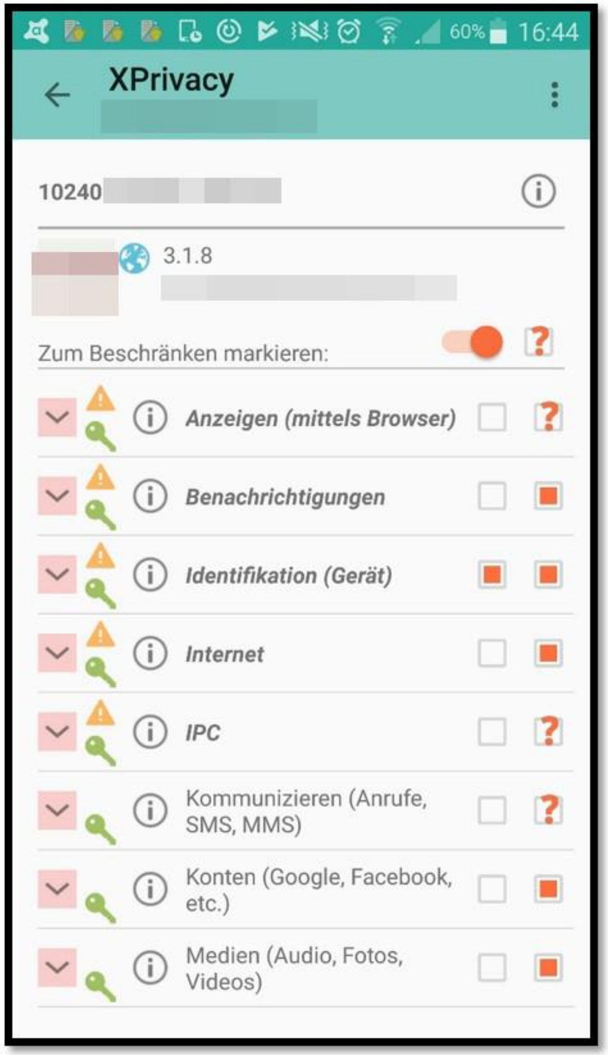
Brightest Taschenlampe Kostenlos
2.3.4
9 gefährlich 6 normal
4.9 Risikoscore

Chrome
27.0.1453.90
13 gefährlich 11 normal
5.3 Risikoscore

Überwacht

Angry Birds
3.1.0
6 gefährlich 7 normal
4.4 Risikoscore

File Expert
5.1.6
6.1



60% 16:44

XPrivacy

10240

3.1.8

Zum Beschränken markieren:

Anzeigen (mittels Browser)	□	?
Benachrichtigungen	□	🟥
Identifikation (Gerät)	🟥	🟥
Internet	□	🟥
IPC	□	?
Kommunizieren (Anrufe, SMS, MMS)	□	?
Konten (Google, Facebook, etc.)	□	🟥
Medien (Audio, Fotos, Videos)	□	🟥

Functional Requirements

- Data Blocking and Filtering
  - block data that the user not wants to share with a app / service
  - filter data if the user wants to share specific data
    - E.g. only share name and telephone number with a communication app.
  - fall back: substitute data

- Ubiquity
  - Unique formalisation of preferences
  - Synchronization of preferences across all platforms and devices of a user

Compliance Requirements

- Data security and privacy
  - Preference profile is stored and synchronized in such a way that no third party is aware of it
  - Also data the PRIVACY-AVARE reads e. g. in the context of filtering are protected

- No infringement of copyrights
  - PRIVACY-AVARE must respect the rights of other developers
  - Foreign code as a manifestation of a creative conception is not manipulated
  - Alternations to the program sequence should be limited to a minimum

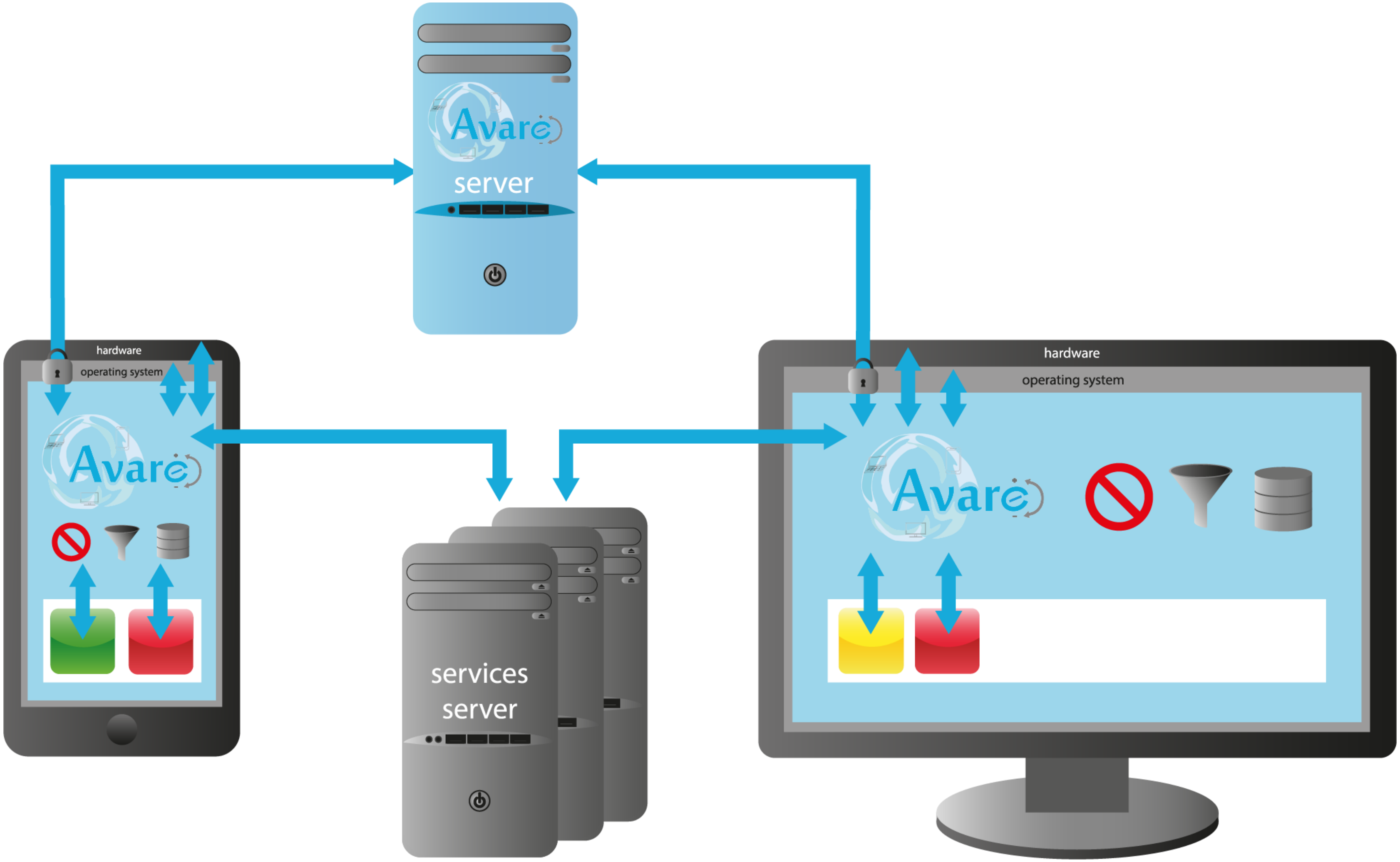
- No breach of contract

Usability & User Experience (UUX)

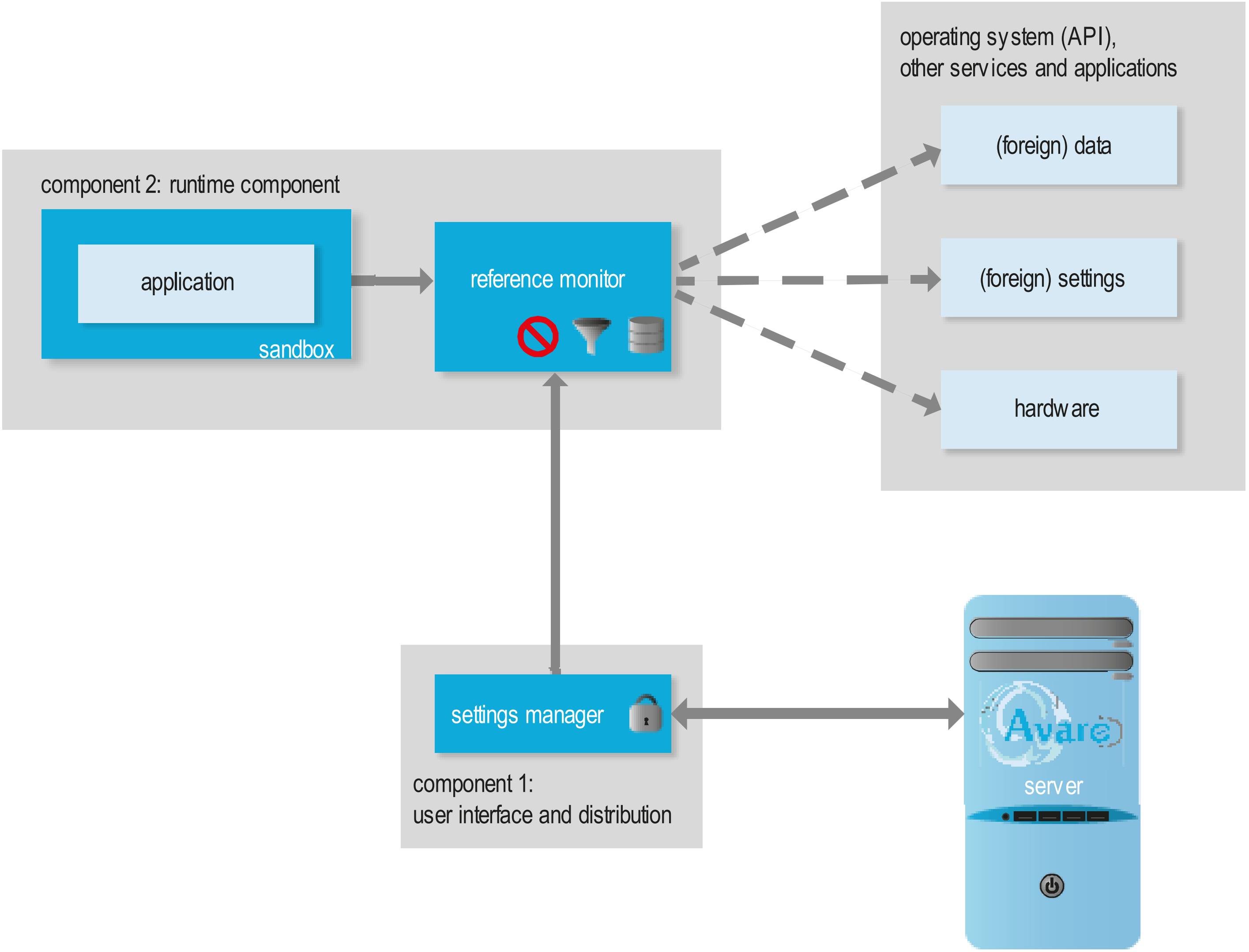
- Simple Installation Process
  - PRIVACY-AVARE is also for end users without deep technical knowledge
  - Installation by end user without root privileges

- Understandability of Privacy Settings
  - User must be able to formalise his own preferences
  - User interface should follow common and modern standards
  - User interface should reduce the complexity of privacy settings

PRIVACY - AVARE



PRIVACY - AVARE


operating system (API), other services and applications
(foreign) data
(foreign) settings
hardware
component 2: runtime component
application
sandbox
reference monitor
settings manager
component 1: user interface and distribution
Avare
server

Conclusion

- Development of PRIVACY-AVARE Solution is platform specific.
  - Even minor version updates changes the possibilities
  - Problem: Developer uses techniques that hackers use for exploits

- PRIVACY-AVARE as …
  - … as a standardized description of preferences
  - … as UI with a good end user experience
  - … as tool for synchronization between devices

- platform-specific enhancement tools
  OR
- *operation system APIs to enhance fine granular preferences*

THANK YOU

Some icons originate from https://icons8.com or are based on these.