Derived Partial Identities Generated from App Permissions

Lothar Fritsch[1] Nurul Momen[2]

Abstract: This article presents a model of partial identities derived from app permissions that is based on Pfitzmann and Hansen's terminology for privacy [PH10]. The article first shows how app permissions accommodate the accumulation of identity attributes for partial digital identities by building a model for identity attribute retrieval through permissions. Then, it presents an experimental survey of partial identity access for selected app groups. By applying the identity attribute retrieval model on the permission access log from the experiment, we show how apps' permission usage is providing to identity profiling.

Keywords: Identity management, Partial Identity, Access Control, Apps, Permissions, Privacy, Data Protection

1 Introduction

Upon the installation of software applications (apps) on smartphones and other smart devices running with Android OS, the app requests permissions to device services and data. These permissions must get confirmed by the device owner upon installation (Android 5.0 and previous versions) or, during runtime (Android 6.0 and later versions). The burdensome responsibility of understanding complex information flow and making decisions is being shouldered by the user. Several studies showed that users face difficulties and struggle in this regard which result into ineffective measure to preserve privacy; for instance [AT16] [KCS13] [RQM13].

Since the introduction of API 23[3], third party apps can access resource through two major permission groups: a) Dangerous permissions and b) Normal permissions. In case of dangerous ones, user has the opportunity to grant them with much better context[4]. However, dangerous permission granted by a user will be valid for lifetime unless that particular permission is revoked manually. On the other hand, it does not provide any information to support decision making of a user in the later stage. The absence of usage information causes hindrance for reassessing the situation and reconsidering users' initial decision. As a result apps get access to sensitive personal information without any time-constraint. We investigate apps' resource usage trend and build a model to correlate with the possible extraction of partial identity. The automatic assessment of privacy risk has been studied on information-flow level in [PF13]. This work is an effort to complete the gaps identified in privacy management in [FA].

[1] Department of Mathematics and Computer Science, Karlstad University, Sweden, lothar.fritsch@kau.se
[2] Department of Mathematics and Computer Science, Karlstad University, Sweden, nurul.momen@kau.se
[3] https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html; Accessed: 2017-05-12
[4] https://developer.android.com/about/versions/marshmallow/android-6.0.html; Accessed: 2017-05-13

In: L. Fritsch, H. Roßnagel, D. Hühnlein (eds.): Open Identity Summit 2017, Proceedings, Lecture Notes in Informatics (LNI) 277, GI-Edition, 2017, ISBN 978-3-88579-671-8

This paper is organized as follows: section 2 presents relevant background. Section 3 elaborates the attributes derived from permissions. Section 4 describes the model for deriving partial identities from permissoins. A survey focused on apps' resource usage trend and its consequential risks regarding partial identity extraction are described in Section 5. We discuss limitations and future work in Section 6 and finally, conclude in Section 7.

2 Android and Permissions

Android runs on a customized Linux kernel. Basic drivers and other components (audio, display, binder, etc.) provide foundation for the Dalvik virtual machine. Application framework, which is a tertiary layer, is responsible to accommodate the apps. They reside into their isolated sandboxes and can request permissions in order to access resources that are available on the device. Android permissions are categorized into four levels: The *normal* level permissions allow access to low-risk assets granted to any package requesting them. The *dangerous* level permissions are considered high-risk permissions that need user confirmation to grant them. So-called *signature* level permissions grant access only to packages with the same author. Finally, *signatureOrSystem* level permissions grant both packages with the same author and packages installed in the system receive permission to access specific resources.

2.1 App Permission: Privacy Issues

App permissions have caused a number of concerns for information privacy and information security, for instance [Fe11, Au12, Pe12, We12]. The first issue is the persistent access of apps to local resources once permissions are given, even if the user may have chosen to abstain from submitting information if he was asked. Often, users do not perceive the risk from granting broad permissions to apps [Ke12]. Both the studies, reported by Felt et al. [Fe11] and Au et al. [Au12], emphasized on apps having more permissions than needed. Developers' lack of awareness was held responsible for over-privileged apps by Peng et al. [Pe12]. Apps are over-accessing local resources with respect to their purpose or the services they offer to the users. They may have a hidden agenda for data collection which is pointed out by several studies, for instance [Li12, Di10].

According to EU data protection regulation [Re16], services and apps should provide a sufficiently detailed privacy policy and collect data subject consent before they collect data. However surveys have shown that usage declaration in privacy policies, data collection activities and primary app purpose do not match in many cases [Be14, PG15]. As a general trend, apps have been found to increase their requests for permissions over time [BPW13, We12].

2.2 Access to Identifiable Information Through Permissions

A principal mapping of app permissions to privacy threats has been shown in [Sa12]. The authors focus on directly accessible personal information, not on derived personal information.

In [MTG], nine categories of person-related information accessible through permissions are identified in Android 4.2.2: *(a) Communication data, such as SMS, MMS, Voice, etc., (b) Sensor data, from the Camera or Microphone, (c) Location data, i.e. GPS data (fine location) and location inferred from networks that the user connects (coarse location) or his social media feeds, (d) External storage data that include app data, documents, emails, etc. (e) Contact data, i.e. the smartphone's contact list or contacts derived by the social media that the user participates in, (f) History/Usage data, which indicate the userâs preferences and can be collected by bookmarks, subscriptions to feeds, the call or task logs, social media feeds, the dictionary, (g) Calendar data, which could also be an indicator of contacts and/or the user's location, (h) Identity data, which refers to all the unique identifiers that can be used to identify a user, e.g. his device ID, e-mail addresses, his profile ID, (i) Credentials, the userâs authentication tokens, passwords and PINs* (Quote from [MTG])

The described private information is not classified according to any classification scheme, such as risk, privacy impact, severity or linkability. Since unlinkability is described as one of the foundations of private use of online services in [PH10], we focus our argument on the extraction of private information that can identify a person. We use the concept of **partial identities** as a base for our analysis.

2.3 Identification and Partial Identities

In privacy theory, a digital identity is often defined as an identifier with related identity attributes attached [Cl09]. Pfitzmann and Hansen [PH10] defined: *An identity is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons.*

They point out that there rarely is a single identity for a person, but many combinations and permutations of identity attributes that are used in various sets. Therefore, they introduce the concept of a partial identity by defining: *A partial identity is a subset of attribute values of a complete identity, where a complete identity is the union of all attribute values of all identities of this person.*

A person is then supposed to be linkable if, on any on-line transaction, he or she can get singled out of a dataset based on the combination of partial identity attributes used for the transaction. The concept of the partial identity is further used to define relationships between identity and attribute data as well as relationships between sets of attributes. The authors of [PH10] define anonymity, unlinkability and unobservability properties based on the concept of partial identities. One important observation is that a person is unidentifiable

(anonymous in a data set if that person's attributes cannot get identified within that dataset). On the other hand, a person may become more identifiable, once more attributes get added to a partial identity. So, identifiability is directly proportional to partial identity.

Based on the concept of partial identities, we analyze information gained through app permissions for the partial identity sets that can get retrieved through the permissions. In the next sections, a model is described for building partial identities from information accessible through permissions on Android devices and an empirical study is presented indicating the likelihood of partial identity extraction.

3 Identity-related Attributes Accessible Through Permissions

Partial identities get build by collection of attributes from one or more sources. In this section, we review data accessible through app permissions on Android devices. We classify the accessible data, and discuss how this data directly or indirectly contributes to building partial identities of the device user.

A number of permissions are grouped as dangerous permissions by Android[5]. Analyzing the information accessible through those permissions, we mapped identity attribute building information sources to identity attributes that get collected from the information sources. From the permissions perspective, the partial identity P of an app user is defined as:

P = {Whereabouts, Network ID, GoogleID, BiometricID, PhoneNumber, Address, Area, SocialGraph}

We noticed that there are directly accessible identity attributes, such as phone numbers or fine-grained GPS location, as well as data that can be used to derive identity attributes through various techniques (e.g. profiling, combination with other data, matching with data bases). The following list defines the partial identity attributes, lists the data contributing permissions, and highlights directly accessible attributes in **boldface**.

Whereabouts *Precise location.* Gathered from **FINE_LOCATION**, ACCESS_WIFI, BLUETOOTH, NFC, ACCESS_NETWORK, READ_EXT_STOTRAGE, CALENDAR, CAMERA

Network ID *Network access ID*. Gathered from **ACCESS_NETWORK**, **ACCESS_WIFI**

GoogleID *Get Google ID*. Gathered from **GET_ACCOUNTS**

BiometricID *Collects biometric information.* Gathered from CAMERA, BODY_SENSORS, CAMERA, ACCESS_AUDIO, **USE_FINGERPRINT**

PhoneNumber *Retrieves phone number*. Gathered from ACCESS_FINE_LOCATION, CALL_PHONE, SEND_SMS, **GET_ACCOUNTS**

[5] https://developer.android.com/guide/topics/permissions/requesting.html, Accessed: 2017-05-13.

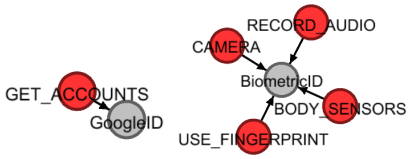

Fig. 1: A permission is being used to gather partial identity information and four permissions are concurrently providing biometric identity information. Red: permission. Gray: partial identity attribute gained through permissions. Arrows: information gathering through permission use.

Address *Retrieves address*. Gathered from **ACCESS_FINE_LOCATION,** CALL_PHONE, SEND_SMS

Area *Retrieves geographic area.* Gathered from ACCESS_COARSE_LOCATION, READ_EXT_STORAGE, READ_CALENDAR, ACCESS_WIFI, ACCESS_NETWORK

SocialGraph *Gathers social graph elements.* Retrieved through **READ_CONTACTS, READ_CALL_LOG, PROCESS_OUTGOING_CALLS**, RECEIVE_MMS

The operations necessary for deriving the indirect attributes include using geographic information systems, reverse-lookup in phone data bases, access to biometric reference databases (such as facebook's face recognition), location profiling over time, and social network analysis on telecommunications data. We restrict the definition to a recursion depth of 1 when combining data with other data. We did not include the case of collusion between apps and servers in trading identifying attributes either, even though this is demonstrated in [Ma12].

4 Model-based Assessment of Permission-accessible Partial Identities

In this section, we propose a graph-based model that will provide information about the potential of apps to access partial identities through permissions. The analysis from the previous section is used to provide a graphical visualization of the construction of potential partial identity information. First, we introduce a model for constructing identity attributes from permissions. Then, we show how the model can be used to assess an app's access to partial identities based on its permissions.

4.1 A Model for Permission-based Partial Identity Retrieval

Figure 1 shows how the GET_ACCOUNTS permission provides to the GoogleID identity attribute. On the other hand, a partial identity attribute can be gathered from various permissions, as shown with the Biometric ID attribute gathered from four different permissions in Figure 1. On the other hand, Fig. 2 shows the overall model based on the analysis in section 3. It shows the conceptualization of all identity attributes. The graph includes all relevant permissions in the red nodes (ellipses). The gray nodes (circles) are the partial

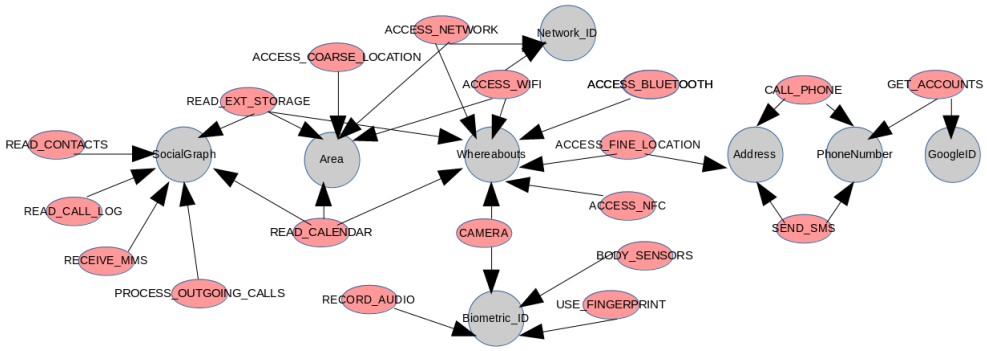

Fig. 2: Graph: permissions providing partial identity attributes. Red ellipse: permission. Gray circle: partial identity attribute gained through permissions. Arrows: information gathering through permissions.

identity attributes that get collected through permission use. Arrows from a permission node to a partial identity node show that a permission is being used to retrieve identity attributes.

4.2 Assessment of an App's Access to Partial Identities

To assess the set of all possible identity attributes, an app's use of permissions is monitored. Using the model above, the actual use of the permissions is used to color the graph from Figure 2 such that all used permissions and all retrieved identity attributes are highlighted. The resulting colored graph shows the overall set of identity attributes that provide to the app's collected partial identity set of the app user. To practically assess permission-based retrieval of identity attributes, we performed a data collection experiment that monitored app permission usage. Section 5 below will present the experiment, and the resulting partial identities retrieved by various app groups are presented in section 5.2 thereafter.

5 Stealing My Identity: A Survey of Actual App Behavior

We developed a monitoring app which is able to log every resource access event by using the *AppOpsCommand*[6]. The app periodically checks for last resource access event by each of the installed apps and writes in a pre-defined format. It stores the log in a JSON file which contains three fields: name of the package/app, name of the accessed resource and time of the resource access event. Following example shows a sample command and log registered from it:

[6] `https://android.googlesource.com/platform/frameworks/base/+/android-6.0.1_r25/cmds/appops/src/com/android/commands/appops/AppOpsCommand.java;Accessed:2017-05-23`

```
#root: adb shell appops get com.google.android.youtube

{‘‘Package":‘‘com.google.android.youtube",‘‘Permission":‘‘READ_EXTERNAL
_STORAGE",‘‘Timestamp":‘‘Fri Mar 03 09:56:35 GMT+01:00 2017"}
{‘‘Package":‘‘com.google.android.youtube",‘‘Permission":‘‘WRITE_EXTERNAL
_STORAGE",‘‘Timestamp":‘‘Fri Mar 03 09:56:35 GMT+01:00 2017"}
```

Tab. 1: Apps for resource usage monitoring.

App Category	Apps
Google	Youtube, Chrome, google music, google maps,, weather, google+, photos, hangout, news, drive, docs, slides, sheets, fit, playgames, play books, play movies, android tv remote, gmail, calendar, earth, google news
Communication	Messenger, Kiko, Viber, Skype, Imo, Telegram, WeChat, Line, Tango, Slack
Social	Facebook, Instagram, Twitter, Musically, LinkedIn, Snapchat, Tumblr, Pinterest, Foursquare, Yelp
Fitness	Lifesum, Endomodo, 30dayFit, LifeLong, RunKeeper, Pedometer, CalorieCounter, Runtastic, 7minWorkout, Fitbit
Music	Spotify, SoundCloud, Shazam, Tidal, FreeMusic, Sonos, Deezer, JangoRadio, SoundHound, iHeartRadio
Weather	weather.com, WeatherApp, AccuWeather, YahooWeather, WeatherBug, PalmaryWeather, WeatherAndClock, GoWeather, WeatherAndRadar, WeatherXL-pro
Games	TempleRun 2, 8ballPool, FruitNinza, TalkingTom, Pou, AsphaltAirborn, ClashOfClans, Farmville, CandyCrush, SubwaySurfers
Shopping	eBay, Amazon, Wish, Zalando, AliExpress, Zara, Lidl, Asos, shpock, H&M
Travel	booking.com, trivago, TripAdvisor, Uber, hotels.com, airBnB, TomTom, Kayak, Expedia, Here
Misc.	Tinder, Badoo, OkCupid, Duolingo, Babel, Netflix, Dropbox, AVG, Firefox, NewsRepublic

5.1 Survey Procedure

We used ten Nexus 7 (2012) tablets running on Android 6.0 - Marshmallow. As there is no stock ROM available for this device, we had to rely on a custom one named AOSP Grouper[7]. Each of the devices was flashed with the mentioned ROM and basic apps (downloaded from Open Gaaps project[8]) were installed. Additionally, it required root access for all the devices. Finally, our prototype app was installed to listen and to accumulate logs of system events related to permission usage. Throughout the survey period, each of the devices was assigned to monitor a particular category of apps. The summary of devices and apps is provided in Table 1. An exception was made for the first category by choosing vendor specific apps. Due to the fact that Google is the largest vendor to offer many apps

[7] https://androidcommunity.com/android-marshmallow-ported-to-nexus-7-2012-everything-working-20151019/; Accessed: 2016-12-27

[8] http://opengapps.org/; Accessed: 2017-05-23

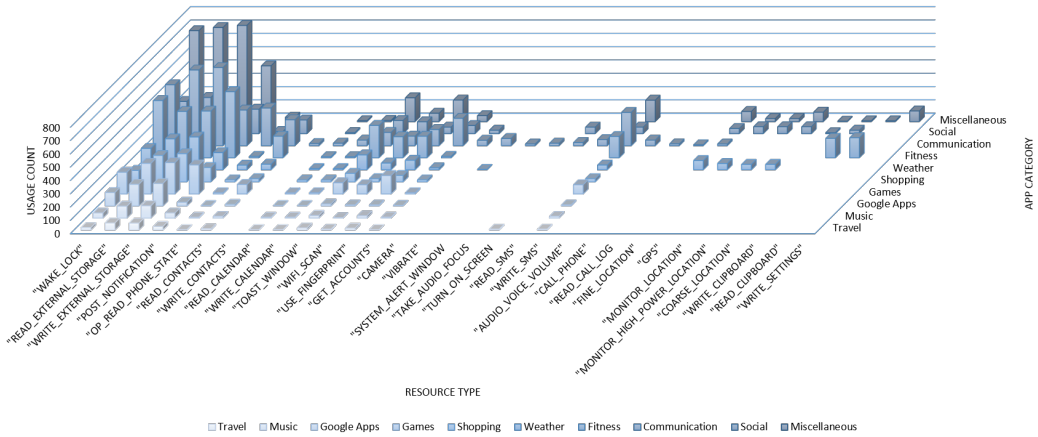

Fig. 3: Summary of resource usage by different app groups installed on test devices.

of different categories, we intended to compare their behavior with the rest. Throughout this phase, the devices remained idle (kept on a shelf). Only notable interaction was to use the prototype app for collecting log or, to plug in the recharging cable once a day. This phase was carried out between 4–10 March, 2017. Pseudo user accounts were created in order to be able to download and install apps from Google Play Store. They were new, had no history, and did not reflect a real person's everyday behavior. We named them as 'pseudonymous test accounts'. However, a few default apps from Google had to be installed in each device which caused common resource utilization by those apps and services. This is another reason behind isolating Google apps in a separate category.

5.2 Results

Here, our findings are presented briefly. It is indeed difficult to examine the vast pool of apps and determine their behavior. Thus we chose to monitor a subset of popular apps and bundled them into several categories with a view to formulate a plausible assumption. First, an overview of resource usage trend is discussed. Then we try to correlate apps' resource usage behavior with the partial identity extraction model described earlier. Because of having limited space, only two partial identity attributes are described with likelihood for extraction.

5.2.1 Idle-time Usage: Phones Never Sleep

Figure 3 summarizes the resource utilization scenario by installed apps during the Stationary Phase of this study. Though the devices were left idle, apps kept accessing resources containing sensitive user information. The most accessed resource is the READ-/WRITE_EXTERNAL_STORAGE. Understandably, communication and social apps have

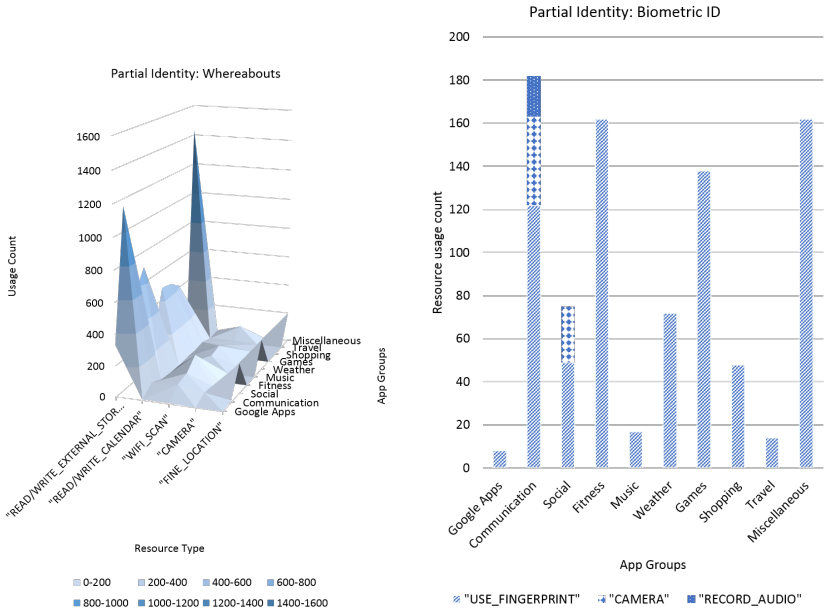

Fig. 4: Likelihood of partial identity extraction for attributes (statistics showing the cumulative sum for corresponding permission access count by app groups): a) Whereabouts could be extracted from five permissions and b) Biometric ID could be extracted from three permissions.

the access to the highest number of resources. On the other hand, dating apps from miscellaneous category were found responsible for being the biggest consumers of idle-time resource consumption.

5.2.2 Partial Identity Extraction

How likely is it to extract partial identities from the collected data? We try to visualize the relationship with respect to the partial identity model presented earlier. We present couple of examples which depict likelihood of partial identity attribute extraction. It should be noted that frequency of resource usage represents the risk or, likelihood of partial identity extraction in real-time. Though some cases are subject to one-time extraction (for example - biometric IDs), others pose threat to disclose partial identities in a dynamic manner and with better accuracy (for example - whereabouts). Figure 4 depicts the possibility of extracting partial identity attributes (Whereabouts and Biometric ID) from our model. Similar pattern could also be depicted for other attributes (Social graph, Area, etc.) as well. In case of 'Whereabouts' attribute, the highest access frequency to file storage shows that an indirect location attribute is accessed more frequently, while WiFi hotspots and fine location are occasionally used. On the other hand, "USE_FINGERPRINT" is the most used resource for profiling 'biometric ID'. Figure $4_{\text{Biometric\_ID}}$ also shows an interesting observation from another angle: significant portion of the resource usage was caused by

"USE_FINGERPRINT", though there was no such hardware available on the test devices. Since Miluzzo et al. [Mi12] showed that finger taps are subject to reveal sensitive data, such intriguing observation compels further investigation in future.

6 Limitations and Future Work

To limit the scope of this work, we excluded a number of issues from our investigation. Retrieving additional identity attributes through permission escalation through colluding apps or services, as described in [Ma12] was not in scope of our research. Several other opportunities to extract identity attributes have not been considered in our model yet. Heart rate monitors and other sensors for biometric vital signals from fitness watches and other wearable devices have not been considered. The use of covert channels such as audio beacons [Su13] has been omitted. Our data gathering experiment also had a very limited scope. However, we did see a number of trends. We conclude, however, that we need to gather a larger, and more detailed, data sample. In particular, the use of the fingerprint-related permission, even on devices with no fingerprint scanner is a detail that calls for further investigation. We need, in addition, consideration of an app's permission use compared to advertising libraries' usage of permissions [Gr12]. Those accesses should get separated in future analysis. A major distortion from real-life use was provided by the experimental setup. In experiment, blank tablet devices were used in association with pseudonymous and unused accounts. The usage of apps and the profiling was therefore not connected to a real person's history of app and device use, but occurred on a new pseudonym that had no history.

Our observation of partial identity retrieval through apps will be extended by several aspects in the near future. We plan to add relative weights to edges in the graph to express how much a particular permission contributes to an identity attribute. The weight could get retrieved, for example, from a privacy impact analysis' result. Another weight attribute for the edges under investigation is the correspondence of an attribute source to identity assurance levels, computational efforts or other parameters that quantify identification risk. We consider to use coloring in the graph notation as a counter on the number of permissions contributing to establish an identity attribute. A better differentiation between direct and indirect identity attribute channels in the graphical representation as well as a conceptualization will extend the model. Finally, we consider the use of visualization as a tool to communicate identification risks through apps to users.

7 Conclusion

Even if the devices remained idle throughout the survey period, a great deal of identity data was being accessed by apps. To some extent, we show that such data is subject to extraction of partial identity. Though Android offers an option to revoke granted consent for certain types of permissions, no information is provided to the user for reassessing the situation and reconsidering initial decisions. We intend to keep working in this direction and design a warning mechanism in order to support informed decision making process.

We believe, appropriate representation of risks related to partial identity would motivate privacy preserving user behavior.

References

[AT16] Alohaly, Manar; Takabi, Hassan: Better Privacy Indicators: A New Approach to Quantification of Privacy Policies. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). 2016.

[Au12] Au, Kathy Wain Yee; Zhou, Yi Fan; Huang, Zhen; Lie, David: Pscout: analyzing the android permission specification. In: Proceedings of the 2012 ACM conference on Computer and communications security. ACM, pp. 217–228, 2012.

[Be14] Bechmann, Anja: Non-informed consent cultures: Privacy policies and app contracts on Facebook. Journal of Media Business Studies, 11(1):21–38, 2014.

[BPW13] Book, Theodore; Pridgen, Adam; Wallach, Dan S: Longitudinal analysis of android ad library permissions. Report arXiv preprint arXiv:1303.0857, Rice University, 18-Apr-2013 2013.

[Cl09] Clarke, Roger: A sufficiently rich model of (id) entity, authentication and authorisation. In: The 2nd Multidisciplinary Workshop on Identity in the Information Society, LSE. volume 5, 2009.

[Di10] Di Cerbo, Francesco; Girardello, Andrea; Michahelles, Florian; Voronkova, Svetlana: Detection of malicious applications on android os. In: International Workshop on Computational Forensics. Springer, pp. 138–149, 2010.

[FA] Fritsch, Lothar; Abie, Habtamu: A Road Map to the Management of Privacy Risks in Information Systems. In (Informatik, Gesellschaft fr, ed.): Sicherheit 2008: Sicherheit, Schutz und Zuverlssigkeit. Konferenzband der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft fr Informatik e.V. (GI), Lecture Notes in Informatics LNI 128. volume 128, Gesellschaft fr Informatik, Bonn, pp. 1–15.

[Fe11] Felt, Adrienne Porter; Chin, Erika; Hanna, Steve; Song, Dawn; Wagner, David: Android permissions demystified. In: Proceedings of the 18th ACM conference on Computer and communications security. ACM, pp. 627–638, 2011.

[Gr12] Grace, Michael C.; Zhou, Wu; Jiang, Xuxian; Sadeghi, Ahmad-Reza: Unsafe exposure analysis of mobile in-app advertisements. In: Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks. ACM, pp. 101–112, 2012.

[KCS13] Kelley, Patrick Gage; Cranor, Lorrie Faith; Sadeh, Norman: Privacy as part of the app decision-making process. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, pp. 3393–3402, 2013.

[Ke12] Kelley, Patrick Gage; Consolvo, Sunny; Cranor, Lorrie Faith; Jung, Jaeyeon; Sadeh, Norman; Wetherall, David: A conundrum of permissions: installing applications on an android smartphone. In: International Conference on Financial Cryptography and Data Security - FC2012 Workshops, LNCS 7398. Springer Berlin Heidelberg, pp. 68–79, 2012.

[Li12] Lin, Jialiu; Amini, Shahriyar; Hong, Jason I; Sadeh, Norman; Lindqvist, Janne; Zhang, Joy: Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing. ACM, pp. 501–510, 2012.

[Ma12] Marforio, Claudio; Ritzdorf, Hubert; Francillon, Aurlien; Capkun, Srdjan: Analysis of the communication between colluding applications on modern smartphones. In: Proceedings of the 28th Annual Computer Security Applications Conference. ACM, pp. 51–60, 2012.

[Mi12] Miluzzo, Emiliano; Varshavsky, Alexander; Balakrishnan, Suhrid; Choudhury, Romit Roy: Tapprints: your finger taps have fingerprints. In: Proceedings of the 10th international conference on Mobile systems, applications, and services. ACM, pp. 323–336, 2012.

[MTG] Mylonas, Alexios; Theoharidou, Marianthi; Gritzalis, Dimitris: Assessing privacy risks in android: A user-centric approach. In: International Workshop on Risk Assessment and Risk-driven Testing. Springer International Publishing, pp. 21–37.

[Pe12] Peng, Hao; Gates, Chris; Sarma, Bhaskar; Li, Ninghui; Qi, Yuan; Potharaju, Rahul; Nita-Rotaru, Cristina; Molloy, Ian: Using probabilistic generative models for ranking risks of android apps. In: Proceedings of the 2012 ACM conference on Computer and communications security. ACM, pp. 241–252, 2012.

[PF13] Paintsil, Ebenezer; Fritsch, Lothar: Executable Model-Based Risk Analysis Method for Identity Management Systems: Using Hierarchical Colored Petri Nets. In: Trust, Privacy, and Security in Digital Business - Proceedings of the TrustBus 2013 conference (LNCS 8058). Lecture Notes in Computer Science LNCS, Springer, Berlin, pp. 48–61, 2013.

[PG15] Pu, Yu; Grossklags, Jens: Using conjoint analysis to investigate the value of interdependent privacy in social app adoption scenarios. 2015.

[PH10] Pfitzmann, Andreas; Hansen, Marit: Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology. In: Designing privacy enhancing technologies. Technische Universitt Dresden, pp. 1–9, 10-Aug-2010.

[Re16] Regulation, General Data Protection: 679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Off J Eur Union, p. L119, 2016.

[RQM13] Rosen, Sanae; Qian, Zhiyun; Mao, Z Morely: Appprofiler: a flexible method of exposing privacy-related behavior in android applications to end users. In: Proceedings of the third ACM conference on Data and application security and privacy. ACM, pp. 221–232, 2013.

[Sa12] Sarma, Bhaskar Pratim; Li, Ninghui; Gates, Chris; Potharaju, Rahul; Nita-Rotaru, Cristina; Molloy, Ian: Android permissions: a perspective combining risks and benefits. In: Proceedings of the 17th ACM symposium on Access Control Models and Technologies (SACMAT 2012). ACM, pp. 13–22, 2012.

[Su13] Sun, Zheng; Purohit, Aveek; Bose, Raja; Zhang, Pei: Spartacus: spatially-aware interaction for mobile devices through energy-efficient audio sensing. In: Proceeding of the 11th annual international conference on Mobile systems, applications, and services. ACM, pp. 263–276, 2013.

[We12] Wei, Xuetao; Gomez, Lorenzo; Neamtiu, Iulian; Faloutsos, Michalis: Permission evolution in the android ecosystem. In: Proceedings of the 28th Annual Computer Security Applications Conference. ACM, pp. 31–40, 2012.