Paul Gerber, Melanie Volkamer

Usability und Privacy im Android Ökosystem

Die Gestaltung des User-Inferfaces kann für die wirksame Ausübung von Datenschutzkontrolle entscheidend sein – das zeigt der Beitrag am Beispiel der Zugriffsberechtigungen von Apps unter Googles Smartphone-Betriebssystem Android, die vom Anwender bei der Installation freigegeben werden. Vor wenigen Monaten hat Google die Darstellung der Berechtigungen im Play Store umfassend überarbeitet. An den vorgenommenen Umstellungen lässt sich zeigen, dass und wie die wirksame Kontrolle von Zugriffsberechtigungen durch den Anwender von der Usability der Darstellung und Aufbereitung dieser abhängt.

Einleitung

Das Smartphone-Betriebssystem Android regelt Zugriffe von Apps auf Daten oder Funktionen mittels Berechtigungen (*Permissions*). Diese Berechtigungen werden in Android in drei Gruppen eingeteilt:

- Normal – Berechtigungen, die Zugriff auf Ressourcen ermöglichen, mit welchen der Anwender gestört, aber nicht ernstlich gefährdet werden kann
- Gefährlich – Berechtigungen, die Zugriff auf Ressourcen ermöglichen, die Kosten verursachen könnten und/oder persönliche Informationen enthalten
- Signature/System – Berechtigungen, die Zugriff auf systemkritische Ressourcen ermöglichen; diese können nicht auf dem normalen Installationsweg angefordert werden

Paul Gerber

ist Wissenschaftlicher Mitarbeiter bei Prof. Volkamer. Er beschäftigt sich mit Produktevaluation und -entwicklung und arbeitet in diesem Kontext im BMBF Projekt ZertApps an der integrierten Darstellung privatsphärenrelevanter Details von Apps.
E-Mail: gerber@psychologie.tu-darmstadt.de

Prof. Dr. Melanie Volkamer

Melanie Volkamer ist Juniorprofessorin an der Technischen Universität Darmstadt. Sie leitet die Arbeitsgruppe Security, Usability, and Society (SecUSo) und forscht schwerpunktmäßig an den Themen elektronische Wahlsysteme und benutzbare Sicherheit.
E-Mail: Melanie.Volkamer@cased.de

Während des Installationsvorgangs über Googles Play Store werden die geforderten Berechtigungen dem Anwender zur Überprüfung vorgelegt. Der Anwender muss nun entscheiden, ob er der Anwendung beziehungsweise dem Hersteller traut und der App Zugriff auf die geforderten (persönlichen) Daten oder Funktionen gewähren möchte. Dabei muss der Anwender den geforderten Berechtigungen als Ganzes zustimmen. Lehnt er ab, kann die App nicht installiert werden.

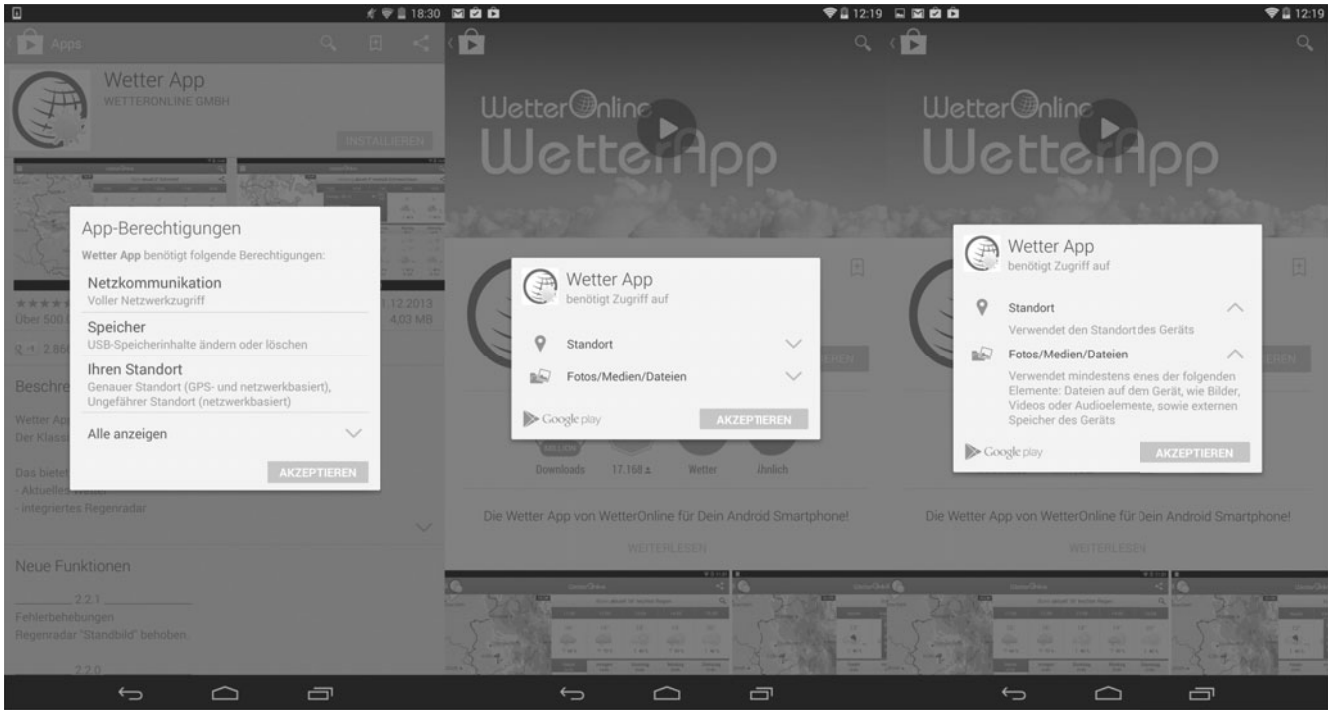
Kritik an diesem Ansatz gab es in den vergangenen Jahren bereits in verschiedenster Form. Beispielweise auf Grund der Tatsache, dass diese Anzeige erst nach dem Betätigen des Installationsknopfes, als Overlay (vgl. Abbildung 1a und b) zur Bestätigung erscheint und damit erst nachdem der Anwender sich entschieden hat, die fragliche App zu installieren [7]. Auch dass Namensgebung sowie Beschreibungen der verschiedenen Berechtigungen sehr technisch und für Anwender wenig verständlich wären [6, 1]. Zusätzlich sind diese so zahlreich (aktuell 146[1] verschiedene), dass die einzelnen Berechtigungen schwer zu lernen und zu erinnern sind [2]. Hinzu kommt, dass Entwickler dazu neigen, eher zu viele Berechtigungen zu fordern, entweder um den Programmierprozess zu vereinfachen oder um sicherzugehen, dass die Anwendung fehlerfrei läuft [4, 10].

Im Juni 2014 führte Google ein umfangreiches Update des Play Stores durch und veränderte hierbei auch die Darstellung der Berechtigungen. Abbildung 1a zeigt die bis dahin (Play Store Version 4.6.17) aktuelle Darstellung für die „Wetter App". Abbildung 1b und c die jeweils entsprechende Darstellung seit Play Store Version 4.8.19, wobei die mittlere Darstellung unmittelbar dann erscheint, wenn der Anwender auf „Installieren" drückt. Die rechte Darstellung zeigt die gleiche Darstellung mit aufgeklappten Details.

In der alten Darstellung wurden im oberen Teil, zusammengefasst in verschiedene Gruppen, die potenziell gefährlichen Berechtigungen aufgeführt. Das sind jene, die von Google als „gefährlich" klassifiziert wurden. Durch einen Klick auf „Alle anzeigen" konnten auch die von Google als „Normal" eingestuften Berechtigungen eingeblendet werden.

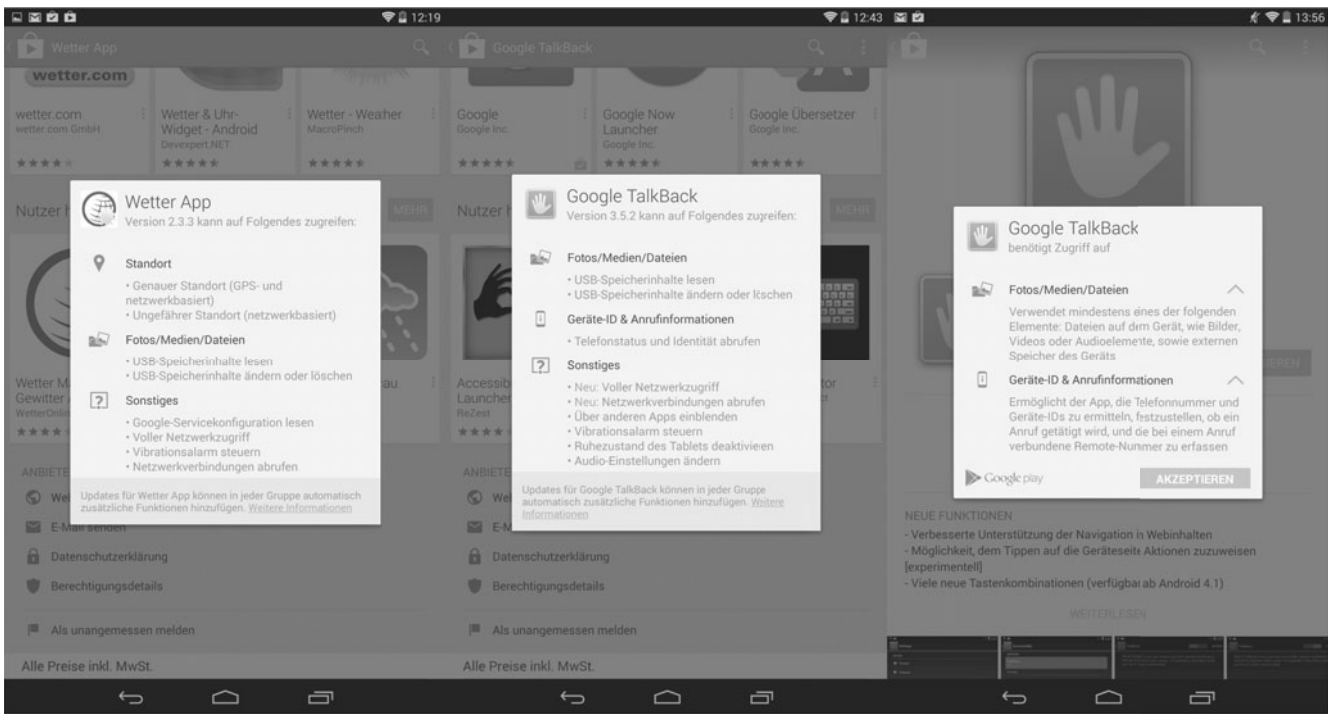
1 http://developer.android.com/reference/android/Manifest.permission.html

Abbildung 1 | (a) Links Berechtigungsanzeige des Google Play Store bis einschließlich Version 4.6.17 (b) Mitte entsprechende Darstellung seit Version 4.8.19 (c) Rechts entsprechende Darstellung mit angezeigten Details



Mit dem Update nahm Google einige Veränderungen an der Struktur der Darstellung, den Formulierungen sowie dem Detaillierungsgrad der Anzeige vor. Darüber hinaus führte Google mit dem Update eine weitere Berechtigungsanzeige innerhalb des Play Stores ein, die sich insbesondere im Hinblick auf den Detaillierungsgrad von jener unterscheidet, welche beim Betätigen des Installieren-Buttons erscheint. Sie ist ebenfalls über die App-Detail-Seite erreichbar. Hierfür muss der Anwender zunächst an das Ende der Seite scrollen und dann über den vorletzten Eintrag „Be-

Abbildung 2. (a) Links Darstellung der Berechtigungen der App „Wetter App", wie sie über den Eintrag „Berechtigungsdetails" im Play Store seit Version 4.8.19 einsehbar ist (b) Mitte Darstellung bei neu geforderten Berechtigungen durch ein App-Update unter „Berechtigungsdetails" (c) Rechts Analog zu b, jedoch nach betätigen von „Aktualisieren"



rechtigungsdetails“ die entsprechende Darstellung aufrufen. Abbildung 2 zeigt die Darstellung für die gleiche App.

Dieser Beitrag wirft einen kritischen Blick auf die Änderungen, welche Google an der Berechtigungsdarstellung innerhalb seines Stores vorgenommen hat. Hierbei stehen vor allem Fragen hinsichtlich der Möglichkeiten und Schwierigkeiten des Anwenders im Fokus, seine Privatsphäre eigenständig und effizient zu schützen. Zu diesem Zweck wird zunächst der neue Berechtigungsbildschirm einer detaillierten Analyse unterzogen und in seinen Eigenschaften beschrieben. Danach werden die resultierenden Konsequenzen, im Hinblick auf die Möglichkeiten des Anwenders, eine fundierte Entscheidung über die geforderten Berechtigungen und damit den Schutz seiner Privatsphären zu treffen, untersucht. Im dritten Abschnitt werden diese schließlich im Kontext aktueller Forschung diskutiert sowie ein Ausblick auf Handlungsmöglichkeiten gegeben.

Beschreibung des neuen Berechtigungsbildschirms

Im Gegensatz zur alten Darstellung hat Google die Berechtigungen nun in insgesamt dreizehn neue Berechtigungsgruppen unterteilt. Diese sind in der Onlinedokumentation von Google[2] aufgelistet und näher beschrieben. Sie unterscheiden sich deutlich von den Kategorien, welche aus der alten Darstellung (vgl. Abbildung 1a) bekannt waren. Wie in Abbildung 1b dargestellt, werden dem Anwender bei Drücken des Installieren-Buttons nur noch diese Gruppen, zu denen die von der App angeforderten Berechtigungen gehören, inklusive des zugehörigen Symbols angezeigt. Rechts neben jeder Gruppe befindet sich ein Pfeilsymbol. Hiermit kann der Anwender eine etwas detailliertere Beschreibung zur jeweiligen Berechtigungsgruppe erhalten. Diese beinhaltet aber nicht die vollständige Liste der geforderten Berechtigungen der jeweiligen Gruppe. Einen „Alle anzeigen“-Button, analog zur alten Darstellung, gibt es nicht mehr. Somit kann der Anwender auf diesem Wege keine vollständige Liste aller geforderten Berechtigungen, seien sie von Google als „gefährlich“ oder „normal“ eingestuft, erhalten.

Des Weiteren werden an dieser Stelle nur die ersten zwölf Berechtigungsgruppen angezeigt. Die dreizehnte („Sonstiges“) findet sich nur in der gesonderten Darstellung (vgl. Abbildung 2), in welcher sich auch die vollständige Liste der geforderten Berechtigungen findet. Wie in der alten Darstellung hat der Anwender weiterhin nur die Wahl, entweder allen geforderten Berechtigungen zuzustimmen oder auf die betreffende App zu verzichten. Im neuen System kommt hinzu, dass eine Zustimmung zu den geforderten Berechtigungen ebenfalls eine Zustimmung zur entsprechenden Berechtigungsgruppe beinhaltet. Dies bedeutet, dass eine App, welcher bei Installation beispielweise der lesende Zugriff auf den USB-Speicher gewährt wurde (also die Gruppe „Fotos/Medien/Dateien“), in einem zukünftigen Update ohne Benachrichtigung des Anwenders alle weiteren Berechtigungen dieser Gruppe anfordern kann und bewilligt bekommt. Sie könnte also, ohne Wissen des Anwenders, in Zukunft auch mit der „Ändern und Löschen“-Berechtigung auf den USB-Speicher zugreifen.

2 Onlinedokumentation „App-Berechtigungen prüfen“ von Google https://support.google.com/googleplay/answer/6014972?hl=dehttps://support.google.com/googleplay/answer/6014972?hl=de; letzter Abruf 29.09.2014

Auswirkungen auf den Schutz der Privatsphäre

Im Folgenden sollen Konsequenzen, welche aus den von Google durchgeführten und im vorherigen Abschnitt beschriebenen Änderungen folgen, aufgezeigt und auf ihre Bedeutung für die Privatsphäre des Anwenders untersucht werden.

Erschwerter Zugriff auf tatsächliche Berechtigungen

Der Play Store von Google enthält keine nähere inhaltliche Beschreibung der Kategorien. In der detaillierteren Darstellung (vgl. Abbildung 2) ist jedoch am unteren Rand ein Link in die Onlinedokumentation zur Berechtigungsanzeige eingebaut. In dieser Dokumentation kann der Anwender nachlesen, wie die Berechtigungsgruppen heißen und welche Berechtigungen sie enthalten, um auf diesem Wege Einblick in die geforderten Berechtigungen zu erhalten. Eine vollständige Liste der geforderten Berechtigungen findet er aber an der gewohnten Stelle nicht mehr. Diese gibt es nur noch über die oben angesprochene und in Abbildung 2a gezeigte Detaildarstellung.

Der solcherart erschwerte Zugriff führt wahrscheinlich dazu, dass selbst dem interessierten und motivierten Anwender schnell die Lust vergehen wird, für jede App bei jedem Update jede Änderung detailliert zu prüfen, sodass der Schutz der eigenen Privatsphäre im schnelllebigen Android-Ökosystem zur Sisyphusarbeit wird.

Zustimmung zu Berechtigungsgruppen und nicht mehr zu einzelnen Berechtigungen

Ebenfalls ausschließlich in der detaillierteren und umständlich zu erreichenden Darstellung im Store findet sich ein Hinweis darauf, dass eine App aus einer bestätigten Berechtigungsgruppe jederzeit, ohne den Anwender zu informieren, jede weitere Berechtigung der gleichen Berechtigungsgruppe anfordern kann. Ausschließlich dort wird auch erklärt, dass dies einzig auf die Gruppe „Sonstiges“ nicht zutrifft.

Nur wenn eine App in einer neuen Version eine Berechtigung einer bisher nicht bestätigten Gruppe oder eine Berechtigung der Gruppe „Sonstiges“ anfordert, ist ein manuelles Eingreifen des Anwenders für das Update notwendig. Das heißt, dass eine App sich ohne Wissen des Anwenders selbst deutlich größere Zugriffsrechte einräumen kann, solange sie sich innerhalb der bereits bestätigten Berechtigungsgruppen bewegt.

Unklare Darstellung von Berechtigungsänderungen

Fordert Android doch ein manuelles Eingreifen seitens des Anwenders, muss dieser in der Play Store App die entsprechende App-Detail-Seite aufrufen und manuell auf „Aktualisieren“ drücken, um das Update und damit die neuen Berechtigungen zu bestätigen. Daraufhin wird erneut der Berechtigungsbildschirm angezeigt und der Anwender kann zustimmen oder auf das Update verzichten. Wie die Abbildung 2c zeigt, hat der Anwender auf diesem direkten Weg jedoch gar keine Chance, die neuen Berechtigungen zu prüfen, da die Kategorie „Sonstiges“ überhaupt nicht im Berechtigungsbildschirm angezeigt wird. Er merkt somit überhaupt nicht, welchen Berechtigungen er hierbei zustimmt. Einzig die am Ende der App-Detail-Seite verfügbaren „Berech-

tigungsdetails“ listen diese mit einem grünen „Neu:“ (vgl. Abbildung 2b) davor auf.

Verlässt der Anwender sich auf die Aussage in der Dokumentation von Google, dass er stets aufgefordert wird, Änderungen an der Gruppe „Sonstiges“ zu überprüfen und zu bestätigen und sieht keine entsprechenden Änderungen in der Anzeige, kommt er wahrscheinlich auch nicht auf die Idee, in der detaillierten Ansicht nachzuschauen. Das Gleiche gilt für einen Anwender, der die Dokumentation nicht gelesen hat und somit aller Wahrscheinlichkeit nach noch nicht einmal von der Existenz der Gruppe „Sonstiges“ Kenntnis hat, da diese niemals im Berechtigungsbildschirm auftaucht.

Fordert eine App nicht nur Berechtigungen der Kategorie „Sonstiges“ neu ein, sondern beispielsweise die Berechtigung für den Zugriff auf den aktuellen Standort, wird diese Berechtigungsgruppe nun im Berechtigungsbildschirm angezeigt. Hierbei findet sich aber keinerlei Markierung der neuen Gruppe(n), sodass der Anwender auch in diesem Fall nur durch manuellen Vergleich mit den alten Berechtigungen oder die schwer aufzufindenden Berechtigungsdetails herausfinden kann, was sich geändert hat.

Das heißt, dass nicht nur der Anwender nun ganzen Gruppen von Berechtigungen seine Zustimmung quasi vorab als Blankoscheck erteilen muss, sondern noch hinzukommt, dass zukünftige Änderungen entweder ungefragt vorgenommen oder nicht beziehungsweise schwer erkennbar angezeigt werden. Dies öffnet möglichem Missbrauch Tür und Tor. Darüber hinaus ist der entsprechende Hinweis so klein gedruckt und im direkt erreichbaren Berechtigungsbildschirm gar nicht eingeblendet, dass davon auszugehen ist, dass der Großteil der Anwender überhaupt keine Kenntnis von den geänderten Rahmenbedingungen hat.

Nicht immer intuitive Zuordnung von Berechtigungen zu Berechtigungsgruppen

Betrachtet man sich etwas genauer die Zuordnung der einzelnen Berechtigungen zu den Berechtigungsgruppen, so fällt auf, dass in einigen Fällen scheinbar thematisch zusammengehörende Berechtigungen dennoch in unterschiedlichen Gruppen eingeordnet sind. So enthält die Berechtigungsgruppe „Identität“ z. B. die Berechtigungen „Konten auf dem Gerät suchen“[3] und „Konten hinzufügen oder entfernen“[4]. Die Berechtigungen „Konten erstellen und Passwörter festlegen“[5] und „Konten auf dem Gerät verwenden“[6] sind jedoch unter „Sonstiges“ zu finden und somit für den Anwender bei der Installation nicht sichtbar.

Dieser Umstand ist für Anwender zumindest verwirrend, wenn nicht gar gefährlich, da er keine vollständige Kenntnis über die geforderten Berechtigungen erlangt, sondern davon ausgehen muss, dass die fragliche App nur einen Teil der möglichen Berechtigungen anfordert und gewährt bekommt.

Ein weiteres Beispiel für diese Vorgehensweise findet sich in der Berechtigungsgruppe „Geräte- und App-Verlauf“. Diese enthält die Berechtigung „Lesezeichen für Webseiten und das Webprotokoll lesen“, wohingegen die Berechtigung „Lesezeichen für Webseiten setzen und das Webprotokoll aufzeichnen“ in der Gruppe „Sonstiges“ einsortiert ist. Analog findet sich in der Gruppe „WLAN-Verbindungsinformationen“ die Berechtigung „WLAN-Verbindungen abrufen“, aber nicht die Berechtigung „WLAN-Verbindungen herstellen und trennen“, die in der Gruppe „Sonstiges“ enthalten und somit erneut nur umständlich für Anwender zu prüfen ist.

Das bedeutet, dass sich der Anwender schlicht nicht auf die Darstellung im Berechtigungsbildschirm bei der Installation einer App verlassen kann. Auf Grund der zumindest verwirrenden Zuordnung zu den einzelnen Gruppen läuft der Anwender ständig Gefahr, für ihn und seine Interessen relevante Änderungen am Zugriffsverhalten seiner installierten Apps zu übersehen und somit ungewollt persönliche Daten preiszugeben.

Erklärungen für Berechtigungen sind nicht intuitiv zu finden

Die Risikobewertung wird für den Anwender weiter erschwert durch den Umstand, dass Erklärungen der Berechtigungen nicht im Play Store verfügbar sind. Der Anwender kann nur externe Quellen, wie z. B. Webseiten oder Apps von Dritten, zur Information nutzen oder die App installieren und danach in den Systemeinstellungen die einzelnen Berechtigungen prüfen. Hier kann durch Berühren der jeweiligen Berechtigung eine kurze Erläuterung aufgerufen werden. Die Sortierung und Gruppierung an dieser Stelle folgt im Augenblick (Android v. 4.4.4) jedoch einem gänzlich anderen Schema als im Play Store. So findet sich in der Darstellung der Systemeinstellungen im Fall der „Wetter App“ aus Abbildung 1 der Begriff „Fotos“ oder „Medien“ überhaupt nicht. Stattdessen findet sich bei den entsprechenden Berechtigungen ein USB-Logo. Die Berechtigungen der Gruppe „Sonstiges“ sind in drei andere Kategorien aufgeteilt, welche mit einem Schlüssel-Symbol („Google-Service Konfiguration lesen“), einem Wi-Fi-Symbol („Voller Netzwerkzugriff“) beziehungsweise einem Akku-Symbol („Vibrationsalarm steuern“) gekennzeichnet werden. Die App zu installieren und danach die Berechtigungen zu prüfen ist aber in Hinblick auf den Schutz der Privatsphäre auf keinen Fall ein gangbarer Weg, da die App bei der Installation bereits alle geforderten Zugriffsmöglichkeiten erhält und eine nachträgliche Prüfung und eventuelle Deinstallation eine mögliche Verletzung der Privatsphäre nicht ungeschehen machen kann.

Auf Grund der fehlenden Erläuterungen der Berechtigungen wird es selbst dem interessierten Anwender unnötig erschwert, eine wirklich fundierte Entscheidung über die geforderten Berechtigungen seiner Apps zu treffen, da hierfür deren Bedeutung für ihn verständlich sein muss.

Unpersönlichere und damit harmloser klingende Bezeichnungen von Berechtigungen

Vergleicht man die Bezeichnungen der Namen der aktuellen Berechtigungsgruppen mit dem jeweiligen Äquivalent aus der alten Darstellung fällt auf, dass diese technischer und unpersönlicher geworden sind. So hieß es in der alten Darstellung noch (Zugriff auf) „Ihren Standort“, „Persönliche Informationen“ oder „Ihre personenbezogenen Daten“. In der aktuellen Darstellung wurden diese ersetzt durch die Bezeichnungen „Standort“ sowie „Kontakte/Kalender“. Ein semantischer Bezug zur eigenen Per-

3 Ermöglicht der App, eine Liste der dem Telefon bekannten Konten abzurufen. Dabei kann es sich um Konten handeln, die von installierten Apps erstellt wurden.

4 Ermöglicht der App, Konten hinzuzufügen und zu entfernen oder deren Passwörter zu löschen.

5 Ermöglicht der App, die Kontoauthentifizierungsfunktionen de s Konto-Managers zu verwenden, einschließlich der Funktionen zum Erstellen von Konten sowie zum Abrufen und Festlegen der entsprechenden Passwörter.

6 Ermöglicht der App, Authentifizierungs-Token anzufordern.

son wird hier eindeutig vermieden, sodass ein Anwender assoziativ eher in Richtung „Funktion“ als in Richtung „Privatsphäre“ neigen könnte.

Durch die Umbenennung der Berechtigungsgruppen wird eine Depersonalisierung erreicht, sodass gerade unerfahrenere Anwender, die mit der Technik weniger vertraut sind (also der Großteil aller Anwender), eher dazu neigen werden, die Berechtigungsanzeige als weniger relevant für die eigene Person und die eigenen Ziele zu bewerten. Dies könnte verstärkend auf die ohnehin bestehende Tendenz wirken, die Berechtigungsanzeige komplett zu ignorieren und somit unbeabsichtigt persönliche Informationen an Dritte weiterzugeben.

Fazit und Handlungsmöglichkeit

Mit der neuen Berechtigungsdarstellung, welche seit Juni 2014 im Play Store implementiert ist, hat Google vieles geändert, um es dem Anwender nach eigener Aussage[7] leichter zu machen eine *fundierte* Entscheidung zu treffen, ob eine App installiert werden soll oder nicht. Die Abstraktion der vollständigen Liste aller geforderten Berechtigungen in dreizehn Berechtigungsgruppen, welche zusätzlich ein möglichst intuitiv erkennbares Symbol bekamen, soll es dem Anwender ermöglichen, einfacher erkennen zu können, worauf eine App auf Grund der Berechtigungen Zugriff haben wird.

Will der Anwender alle Informationen zu den geforderten Berechtigungen haben, kann er diese nun nur noch über die am Ende der Detail-Seite platzierten „Berechtigungsdetails“ erreichen. Der normale Anwender, der schlicht auf „Installieren“ drückt, bekommt somit einen großen Teil der geforderten Berechtigungen überhaupt nicht zu Gesicht und ist sich dessen vermutlich nicht einmal bewusst.

Die Resonanz in den allgemeinen Medien war recht überschaubar[8] und ausschließlich eher einschlägige Medien, wie z.B. www.heise.de[9], www.golem.de[10] oder www.areamobil.de[11] sowie www.androidnext.de[12] befassten sich mit der Thematik. In diesen Quellen wurde vor allem auf die Tatsache eingegangen, dass der Anwender nun ganzen Gruppen von Berechtigungen seine Zustimmung erteilt, nicht mehr nur einzelnen Berechtigungen, was bei aktivierten automatischen Updates, wie oben ausgeführt, zu gravierenden Erweiterungen der Zugriffsrechte einer App führen kann, ohne dass der Anwender dies mitbekommt. Reichweitenstarke allgemeine Onlinepublikationen wie z. B. www.faz.net, www.spiegel.de oder www.bild.de berichteten gar nicht darüber.

Der Anwender wird bei dieser Problematik von Google allein gelassen und ihm bleibt nur die Möglichkeit, die Autoupdate-Funktion für jede App individuell zu deaktivieren und jedes Update manuell mit der umständlich zu erreichenden Darstellung aus den „Berechtigungsdetails“ am Ende der App-Detailseite zu überprüfen.

Die neue Darstellung beschränkt sich standardmäßig darauf, nur noch die Namen der Kategorien anzuzeigen. Das kann zur Folge haben, dass eine App, die vier Berechtigungen aus einer Gruppe fordert, weniger Berechtigungen zu haben scheint als eine, die jeweils eine Berechtigung aus zwei verschiedenen Gruppen anfordert. Vor dem Hintergrund, dass Anwender die komplexe Berechtigungsarchitektur von Android eher selten verstehen [6] und der Tatsache, dass Menschen dazu tendieren, komplexe Entscheidungen mittels Heuristiken zu vereinfachen, erscheint die Informations-Abstraktion Besorgnis erregend. Vor allem, da es plausibel erscheint, dass Anwender zu heuristischen Entscheidungen wie zum Beispiel „weniger Berechtigungen sind besser“ neigen, dies aber in der aktuellen Darstellung nicht ersichtlich ist.

Auf dieser Grundlage kann der Anwender kaum eine fundierte Entscheidung darüber treffen, ob er beispielsweise eine QR-Code-Scanner App installieren möchte, die einzig (nachvollziehbarerweise) Zugriff auf die Kamera[13] fordert, da diese Forderung dank der abstrahierten Darstellung so missverständlich formuliert wird („Verwendet mindestens eines der folgenden Elemente: Kamera(s), Mikrofon(e)“), dass der Anwender daraus nicht schlau werden kann. Auch hier bleibt dem interessierten Anwender keine Wahl, als den umständlichen Weg über die „Berechtigungsdetails“ für jede für ihn potentiell interessante App zu gehen.

Selbst wenn man vom idealen Fall eines Anwenders ausgeht, der sich aufmerksam die von Google bereitgestellten Onlineressourcen zur neuen Anzeige durchliest, birgt die neue Anzeige auf Grund der nicht sichtbaren „Sonstiges“-Gruppe ein für ihn kaum kalkulierbares Risiko. Google formuliert zwar explizit, dass der Anwender *stets dazu aufgefordert* wird, die Änderungen zu überprüfen, jedoch erscheinen die Änderungen nur in den deutlich schwerer zu findenden „Berechtigungsdetails“.

Auf dem offensichtlichen, vermutlich von den allermeisten Anwendern beschrittenen Weg werden diese Änderungen still schweigend ausgeblendet. Selbst Änderungen in den angezeigten zwölf Gruppen werden in der Darstellung nicht markiert, sodass eine Prüfung schwer fallen muss. Entgegen diesem idealisierten Szenario glauben viele Anwender, dass die Store-Betreiber alle Apps testen und gefährliche löschen [5]. Insofern erscheint es plausibel, dass der Anwender in der Realität meist die Dokumentation nicht gelesen hat und somit nur die Anzeige kennt, die auf den „Installieren“- beziehungsweise „Aktualisieren“-Button folgt.

Er ist sich also keines Problems bewusst, da er die Berechtigungsgruppe „Sonstiges“ überhaupt nicht kennt. Er kann somit schwerlich überhaupt auf die Idee kommen, eine weitere Anzeige zu suchen bzw. zu vermuten, dass er nicht alle geforderten Berechtigungen gesehen hat. Hier ist es Googles Aufgabe sowie die der Forschungsgemeinschaft, aufzuklären und bessere Lösungen zu entwickeln. In der Forschungsgemeinschaft gibt es bereits verschiedene Vorschläge, die Darstellung der geforderten Berechtigungen in Android zu verbessern [u. a. 5, 7, 8, 9] und so den Anwender besser in die Lage zu versetzen, seine individuellen Wünsche hinsichtlich der eigenen Privatsphäre in Einklang mit der Auswahl der zu installierenden Apps zu bringen.

7 Basierend auf der Onlinedokumentation „App-Berechtigungen prüfen“ von Google; letzter Abruf 29.09.2014

8 Eine Google Suche mit den Begriffen „Berechtigungsanzeige Play Store“ für den Zeitraum vom 01.05.2014 bis 31.07.2014 liefert insgesamt nur fünf deutschsprachige Treffer (letzte Durchführung 01.10.2014)

9 http://heise.de/-2211827 (letzter Abruf 01.10.2014)

10 http://www.golem.de/news/google-play-store-android-apps-erhalten-leichter-mehr-berechtigungen-1406-106856.html (letzter Abruf 01.10.2014)

11 http://www.areamobile.de/news/27347-android-google-erschwert-pruefen-von-app-berechtigungen (letzter Abruf 01.10.2014)

12 http://www.androidnext.de/news/google-play-store-juengstes-update-sorgt-fuer-laxere-handhabung-von-app-berechtigungen/ (letzter Abruf 01.10.2014)

13 https://www.secuso.informatik.tu-darmstadt.de/de/research/results/privacy-friendly-qr-scanner-app/

Eine umfassende Betrachtung und ein Vergleich der Wirksamkeit der verschiedenen Ansätze fehlten jedoch bisher. Unter anderem hier setzt das vom BMBF geförderte Forschungsprojekt ZertApps[14] an. Im Rahmen des Projektes arbeiten Forscher aus Bremen und Darmstadt gemeinsam an integrierten Lösungen, die dem Anwender Werkzeuge an die Hand geben, um die Kontrolle über seine Privatsphäre zu behalten. Hierbei gilt es, neben dem Vergleich bereits vorgeschlagener Lösungen zur Darstellung der Berechtigungen auch die Bedeutung von Informationen, welche sich nicht direkt aus den geforderten Berechtigungen ableiten lassen, aber den Kontext der App-Nutzung näher beschreiben, genauer zu untersuchen. So könnte es beispielsweise von großer Relevanz für den Anwender sein, mit welchen Partnern eine spezifische App Daten austauscht, um zu bewerten, ob er ihr und den Interaktionspartnern soweit vertraut, dass er den Zugriff auf persönliche Daten freigibt. Ebenfalls sehr bedeutsam für die Bewertung des Anwendungskontextes könnte es sein, aus welchem Grund beziehungsweise für welche spezifische Funktionalität eine App eine bestimmte Berechtigung anfordert. Die Nützlichkeit dieser Informationen gilt es zu bewerten, ebenso wie Möglichkeiten der verständlichen und benutzbaren Integration in das grafische Interface zu entwickeln, sodass Usability und Privacy keine getrennten Konzepte mehr sind, sondern von Usable Privacy gesprochen werden kann.

Danksagung

Dieser Beitrag wurde vom Bundesministerium für Bildung und Forschung im Rahmen des Projektes „ZertApps“[14] gefördert und unterstützt.

Literatur

[1] Egelman, S., Tsai, J., Cranor, L. F., & Acquisti, A. (2009). *Timing is everything?* In: Proceedings of the 27th international conference on Human factors in computing systems – CHI 09 (p. 319). New York, USA: ACM Press.

[2] Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). *Android Permissions: User Attention, Comprehension, and Behavior.*

[3] Felt, A. P., Egelman, S., & Wagner, D. (2012). *I've got 99 problems, but vibration ain't one.* In: Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices – SPSM '12 (p. 33). New York, USA: ACM Press.

[4] Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. (2011). *Android permissions demystified.* In: Proceedings of the 18th ACM Conference on Computer and Communications Security – CCS '11, 627.

[5] Harbach, M., Hettig, M., Weber, S., & Smith, M. (2014). *Using personal examples to improve risk communication for security & privacy decisions*. In: Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems – CHI '14, 2647–2656.

[6] Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., & Wetherall, D. (2012). *A Conundrum of Permissions: Installing Applications on an Android Smartphone.* In: J. Blyth, S. Dietrich, & L. J. Camp (Eds.), Financial Cryptography and Data Security (Vol. 7398, pp. 68–79). Berlin, Heidelberg: Springer.

[7] Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013). *Privacy as part of the app decision-making process*. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems – CHI '13, 3393.

[8] Kraus, L., Wechsung, I., & Möller, S. (2014). *Using Statistical Information to Communicate Android Permission Risks to Users*. In: G. Lenzini & G. Bella (Eds.), Proc. of 4th Int. Workshop on Socio-Technical Aspects in Security and Trust (STAST), IEEE.

[9] Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012). *Expectation and Purpose : Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing*. In UbiComp'12 (pp. 501–510). Pittsburgh, USA.

[10] Vidas, T., Christin, N., & Cranor, L. F. (2011). *Curbing Android Permission Creep*. In: W2SP.

Links

[a] *Android-Apps erhalten leichter mehr Berechtigungen*, Golem.de, 02.06.2014, http://www.golem.de/news/google-play-store-android-apps-erhalten-leichter-mehr-berechtigungen-1406-106856.html

[b] *Google erschwert Prüfen von App-Berechtigungen*, areamobile, 03.06.2014, http://www.areamobile.de/news/27347-android-google-erschwert-pruefen-von-app-berechtigungen

[c] *Google Play Store: Jüngstes Update sorgt für laxere Handhabung von App-Berechtigungen*. http://www.androidnext.de/news/google-play-store-juengstes-update-sorgt-fuer-laxere-handhabung-von-app-berechtigungen/

[d] Onlinedokumentation *„App-Berechtigungen prüfen“* von Google, https://support.google.com/googleplay/answer/6014972?hl=dehttps://support.google.com/googleplay/answer/6014972?hl=de

[e] *Play Store ermöglicht Apps mehr Rechte ohne Nachfragen*, heise online, 30.05.2014, http://heise.de/-2211827

[f] *Privacy friendly QR Scanner App*, Forschungsgruppe Security, Usability and Society, Fachbereich Informatik, Technische Universität Darmstadt, https://www.secuso.informatik.tu-darmstadt.de/de/research/results/privacy-friendly-qr-scanner-app/

14 http://www.zertapps.de/