Mike Kuketz

TÜV Media

Die Schwächen des Android Berechtigungsmodells

TÜVRheinland
Genau. Richtig.

TÜVRheinland®
Genau. Richtig.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie. Detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7406-0121-8

Gesamtherstellung: TÜV Media GmbH, Köln 2016

Den Inhalt dieses E-Books finden Sie auch
in dem Handbuch „Information Security Management“
TÜV Media GmbH, Köln.

Die Schwächen des Android- Berechtigungsmodells

Das Android-Berechtigungsmodell steuert auf Anwendungsebene den Zugriff auf unterschiedliche Ressourcen des Android-Smartphones wie den Kalender, die Standortdaten oder die Kontakte. Aufgrund eklatanter Schwächen eignet sich dieses Konzept allerdings nur unzureichend für den Schutz von Informationen bzw. personenbezogenen Daten. Das vorliegende E-Book beleuchtet die Schwächen des Android-Berechtigungsmodells und erläutert die damit einhergehende Problematik.

Autor: Mike Kuketz
E-Mail: info@kuketz-security.de

1 Motivation

Allround-Talent

Mobile Endgeräte wie Smartphones und Tablets erfüllen heutzutage die unterschiedlichsten Aufgaben und sind kaum noch aus dem Alltag wegzudenken. Kommunikationszentrale, Datenspeicher, Mediaplayer, Spielkonsole und Navigationsgerät sind nur einige Beispiele für die vielfältigen Anwendungszwecke eines mobilen Endgeräts. Man könnte auch sagen: Ein mobiles Endgerät wie ein Smartphone dient als Schnittstelle bzw. „Mittler“ zwischen analoger und digitaler Welt. Dieses wiederum hat zur Konsequenz, dass es zunehmend zu einer Vermischung der beiden „Welten“ kommt, was sich in den unterschiedlichsten Alltagssituationen bemerkbar macht, so z. B.:

- Bargeld wird zunehmend durch kontaktloses Bezahlen mit dem Smartphone (Google Wallet, Apple Pay) abgelöst.
- Die ursprüngliche Navigation mittels Karten wurde längst durch die „smarte“ GPS-Navigation auf der Basis von Smartphone-Apps ersetzt.
- Verabredungen und Terminabsprachen erfolgen zunehmend über sogenannte Messenger-Apps.

- Eintrittskarten, Gutscheine oder Bahntickets werden vermehrt papierlos bzw. digitalisiert online mittels Smartphone bestellt.

Angesichts der fortschreitenden Vermischung dieser zwei Welten enthalten mobile Endgeräte heute die persönlichsten und intimsten Informationen von Personen. Die Informationsvielfalt reicht von Zahlungsinformationen, Kontaktdaten, E-Mail-Korrespondenzen bis hin zu Sucheingaben im Browser, metergenauen Standortinformationen und Vielem mehr. Insbesondere aus kommerziellen Interessen versuchen die unterschiedlichsten Protagonisten, wie zum Beispiel die Werbe- und Medienbranche, Zugang zu diesen Informationen zu erhalten, um daraus vermarktbare Erkenntnisse über eine Person zu gewinnen.

Neues Zeitalter

Insofern ist es im Zeitalter der Digitalisierung essenziell, sich vor Augen zu führen, dass diese Informationen bzw. Daten nicht umsonst als das „Öl des 21. Jahrhunderts“ bezeichnet werden. Mitunter sind die sozialen, ökonomischen, aber auch kulturellen Folgen der systematischen „Förderung“ von Daten durch modernste Technologien heute nicht absehbar. Insbesondere mobile Endgeräte dienen den unterschiedlichsten Protagonisten als eine der zuverlässigsten „Daten-Quellen“ – denn sie enthalten wie vorstehend dargestellt, eine Vielzahl an Informationen über den Nutzer. In diesem Zusammenhang gilt es zu beleuchten, warum es den Protagonisten gerade auf mobilen Endgeräten und insbesondere auf Android vergleichsweise einfach gemacht wird, dieses Informationspotenzial für ihre Zwecke ausnutzen. Von der grafischen Oberfläche eines Smartphones, die durch „Tippen und Wischen“ handhabbar ist, müssen wir uns an dieser Stelle verabschieden und einen Blick hinter die Kulissen werfen. Denn um zu verstehen, welche Mechanismen im Hintergrund wirken, gilt es

das Android-Berechtigungsmodell von seiner technischen Seite zu analysieren.

Rechtliche Aspekte

Die im Nachfolgenden aufgezeigten technischen Implikationen haben ferner unmittelbare rechtliche Auswirkungen. Denn die Realität der Datenverarbeitung eines (Android-) Smartphones hat direkte Implikationen beispielsweise für die rechtliche Bewertung eines datenschutzrechtskonformen Einsatzes von Android-Smartphones in einem Unternehmen. Mithin ist eine verantwortliche Stelle insbesondere auch von rechtlicher Seite dazu aufgerufen, sich mit der hochkomplexen technischen Datenverarbeitungsrealität eines Smartphones auseinanderzusetzen und zu evaluieren, ob diese mit den gesetzlichen Anforderungen in Einklang gebracht werden kann. Die nachfolgenden, zugegebenermaßen recht technischen Informationen sollen daher den Personen, die in Unternehmen mit dem Schutz von Daten bzw. Informationen beauftragt sind, wie z. B. Datenschutzbeauftragten, Informationssicherheitsbeauftragten, eine Handhabe bieten, den Einsatz von Android-Smartphones im Unternehmen nachzuvollziehen, die damit einhergehenden Risiken adäquat abzuschätzen und entsprechende Maßnahmen zu treffen, den Einsatz von (Android-) Smartphones rechtskonform zu bewerkstelligen.

2 Einführung

Android

Als die Firma Android Inc. 2003 vom Programmierer Andy Rubin gegründet wurde, konnte wohl noch niemand ahnen, welche Rolle „Android“ zehn Jahre später in der IT-Welt einnehmen würde. Google erkannte das Potenzial von Android frühzeitig und kaufte das Unternehmen zwei Jahre später auf. Die erste offizielle Android-Version auf einem Smartphone erschien im Oktober 2008. In den letzten drei Jahren

(2013–2015) lag der Marktanteil von Android im Smartphone-Segment kontinuierlich bei über 80 % – im Jahr 2016 aktuell bei 84 % [1]. Man könnte daher auch sagen: Googles mobiles Betriebssystem Android beherrscht den Markt wie kein anderes. Der Marktanteil der Konkurrenten wie Apples iOS, Blackberry oder Windows Phone schrumpft hingegen immer weiter. Die Marktdominanz von Android ist gewaltig und verhindert faktisch fast jede Neuentwicklung. Es ist daher wenig verwunderlich, dass alternative mobile Betriebssysteme wie Sailfish OS [2] oder Ubuntu Touch [3] vom Markt kaum wahrgenommen werden und so schnell, wie sie eingeführt wurden, auch wieder vom Markt verschwinden werden.

Durchschnittsnutzer entmündigt

Googles Strategie mit Android scheint aufzugehen. Der Erfolg gibt ihnen recht. Doch bei dieser Erfolgsgeschichte gilt es sich auch vor Augen zu führen, welcher Preis dafür von den eigentlichen Nutzern gezahlt wurde. Diese bezahlten und bezahlen nämlich mit den von ihnen „produzierten" Daten. Dieses „Bezahlen mit Daten" nehmen sie jedoch nicht wahr, denn ihnen fehlt die Transparenz, um zu sehen, was eigentlich bei der Smartphonenutzung geschieht. Ferner haben sie auch grundsätzlich keine Möglichkeit, auf die Nutzung Einfluss zu nehmen. Auch wenn es oftmals gerne von den Smartphonenutzern verdrängt wird, aber Androids fragwürdiges, im Nachfolgenden näher dargestelltes Berechtigungsmodell hat in den vergangenen Jahren entschieden dazu beigetragen, dass Durchschnittsnutzer geradezu „entmündigt" wurden und nicht annähernd mehr wissen, was sich im Hintergrund auf ihrem Gerät überhaupt noch abspielt.

Das neue und als evolutionär angepriesene, mit Android 6 (Marshmallow) eingeführte Konzept zur Verwaltung der App-Berechtigungen adressiert die tief sitzenden Probleme auch nur unzureichend.

Um den Leser mit den Risiken, die u. a. durch das Android-Berechtigungsmodell bei der Android-Smartphonenutzung bestehen, vertraut zu machen, sollen im Nachfolgenden die Unzulänglichkeiten des Android-Berechtigungsmodells und die damit verbundenen Konsequenzen aufgezeigt werden. Ferner soll dargestellt werden, weshalb die in Android 6 integrierte Rechteverwaltung auch noch immer nicht ausreicht, um den Nutzer und seine Daten zu schützen.

3 Zugriffskontrollmodelle

Wer Was Wie

Das Android-Berechtigungsmodell basiert auf Rechten, die den Zugriff auf bestimmte Ressourcen des Smartphones überwachen und steuern. Dieses anerkannte Prinzip ist in der Informatik unter dem Begriff Zugriffskontrollmodell [4] bekannt. Dabei wird auf der Basis von Regeln und Strukturen durch ein Zugriffskontrollmodell entschieden, ob beispielsweise der Zugriff auf einen Prozess, eine Datei oder ein Netzwerkdienst ermöglicht wird oder der Komponente der Zugriff verwehrt bleibt. Vereinfacht ausgedrückt, regelt daher ein solches Modell:

„Wer darf in einem IT-System auf welche Ressourcen wie zugreifen".

Subjekt, Objekt und Berechtigung/ Zugriffsrecht

Abstrakt werden Zugriffskontrollmodelle anhand dreier grundlegender Elemente beschrieben, nämlich des Subjekts, des Objekts und der jeweiligen Berechtigung bzw. des entsprechenden Zugriffsrechts. Diese Elemente werden nachfolgend kurz beschrieben, u. a. um ein einheitliches, notwendiges Begriffsverständnis zu schaffen:

Subjekt: Initiator der Handlung bzw. agierende Einheit

1. einzelne Nutzer wie beispielsweise Alice, Bob oder Nutzergruppen
2. (System-)Prozesse, Rechner

Objekt: Gegenstand der Handlung bzw. zu schützende Einheit

1. (System-)Prozesse, Dateien
2. (Nutzer-)Konten

Berechtigung bzw. Zugriffsrecht: Zugriffsmethode, die einem Subjekt auf ein Objekt gewährt wird

1. z. B. lesen, schreiben, löschen, ausführen

Verbreitung

Klassische Zugriffskontrollmodelle wie beispielsweise die Zugriffskontrollmatrix (Access Control Matrix) oder Zugriffskontrolllisten (Access Control List) sind in alle gängigen Betriebssysteme wie etwa Windows, Unix/Linux, Mac OS integriert. Sie legen fest, in welchem Umfang einzelne Subjekte Zugriff auf bestimmte Objekte haben.

Zugriffskontrollliste

In Abbildung 1 wird eine Zugriffskontrollliste dargestellt. Der markierte Bereich veranschaulicht exemplarisch, welche Zugriffsrechte (Lesen, Schreiben, Ausführen) die Subjekte (Alice, Bob, Carol, Dave) auf das Objekt (Datei1) besitzen. Bei jedem Zugriff auf das Objekt werden die Zugriffsrechte des jeweils angemeldeten Subjekts vom System geprüft und entsprechender Zugriff verweigert bzw. gewährt.

Das Android-Berechtigungsmodell basiert ebenfalls auf einem Zugriffskontrollmodell. Im folgenden Abschnitt wird dieses Modell vorgestellt und die damit einhergehende Problematik näher beleuchtet.

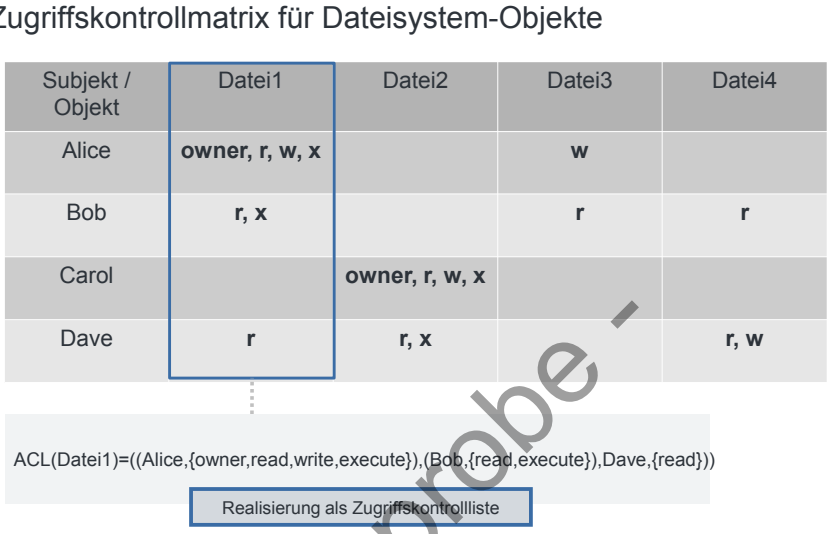

Abb. 1: Zugriffskontrollliste

4 Das Android-Berechtigungsmodell

Sicherheitsarchitektur

Eine zentrale Komponente der Android-Sicherheitsarchitektur ist das Berechtigungsmodell. Es überwacht und steuert den Zugriff auf diverse Ressourcen, wie beispielsweise die der Smartphonekamera eines Android-Systems. Das Berechtigungsmodell ist ein zentraler Bestandteil der Android-Sicherheitsarchitektur [5], die auf unterschiedlichen Mechanismen basiert. Jeder dieser Mechanismen spielt eine entscheidende Rolle, wenn es um die Kontrolle und Einhaltung der Systemsicherheit des Android-Systems geht.

Abstrakt dargestellt, tauschen diese Mechanismen untereinander Informationen über Subjekte (Apps, Nutzer), Objekte (Dateien, Geräte) und Zugriffsrechte (Lesen, Schreiben, Lö-

schen etc.) aus. Neben dem Berechtigungsmodell existieren weitere Komponenten der Android-Sicherheitsarchitektur, wie die Geräteverschlüsselung und Verified Boot [6], die jedoch aufgrund ihrer Komplexität nicht Bestandteil des vorliegenden E-Books sind.

Ressourcen

Eine Ressource in Android ist ein Objekt, auf das ein Subjekt (App, Nutzer) zugreift – die jeweils vergebenen Berechtigungen kontrollieren/limitieren diesen Zugriff. Auf einem Android-Gerät existieren unterschiedliche Ressourcen, die sich grob in die drei folgenden Kategorien einteilen lassen:

- **API-Ressourcen:**
  Über die Android-API [7] (Programmierschnittstelle) kann ein Entwickler Zugriff auf unterschiedliche Ressourcen erhalten, falls die dafür notwendige Berechtigung vom Smartphonenutzer (zuvor) erteilt wurde. Als Beispiel sei hier die Berechtigung „Telefonstatus und Identität abrufen [8]“ genannt, die den Zugriff auf unterschiedliche Informationen der Ressource „Telefon“ ermöglicht. Die Erteilung des Zugriffs führt deshalb u. a. dazu, dass eine App die International Mobile Equipment Identity (IMEI) oder die Seriennummer der SIM-Karte auslesen kann. Die IMEI ist eine eindeutige 15-stellige Seriennummer, anhand deren ein Smartphone weltweit eindeutig identifiziert werden kann. Es handelt sich daher bei der IMEI aufgrund des damit einhergehenden „Missbrauchspotenzials“ um ein sehr sensibles, unbedingt schützenswertes Datum. Weitere Berechtigungen und die darüber abrufbaren Ressourcen bzw. Informationen werden in Abschnitt 4.1.1 vorgestellt.
- **Dateisystem-Ressourcen:**
  Dateien stellen unter Android ebenso Ressourcen/Objekte dar, deren Zugriff grundsätzlich reglementiert und kontrolliert wird. Nach dem Vorbild des Unix-Dateisystems

existieren die Berechtigungen Lesen, Schreiben und Ausführen. Gestattet sind die Zugriffe jedoch immer nur dann, wenn auch der entsprechende Nutzer bzw. die Gruppe dazu berechtigt ist. Standardmäßig hat nach dem Android-Berechtigungsmodell eine App lediglich Zugriff auf die eigenen Dateien im Dateisystem. Realisiert wird dies über einen eindeutigen Identifikator (ID bzw. UID) [9], der einer App während der Installation vom System zugewiesen wird. Jede Datei einer App wird anschließend mit der zugewiesenen UID markiert, die stellvertretend für die Nutzer und Gruppen bei Unix-Systemen steht.

- **IPC-Ressourcen:**
  Das Android-System isoliert Apps in getrennten (Speicher-) Bereichen, reglementiert den Zugriff auf Dateien und verhindert auf Kernel-Ebene [10] die direkte Interaktion zwischen zwei Prozessen. Aufgrund dieser strikten Trennung wird eine Inter-Process Communication (IPC) benötigt, die den Austausch von Daten bzw. Informationen zwischen System- und App-Prozessen steuert. Unter Android werden für die Kommunikation zwischen Prozessen das eigens dafür entwickelte Binder-Framework [11] und weitere Hilfsmittel wie Intents [12] oder Broadcast Receiver [13] verwendet. Daten, die über die IPC ausgetauscht werden, gelten ebenfalls als Ressourcen.

Zwei getrennte Mechanismen

In Android sind (streng genommen) zwei getrennte Berechtigungsmodelle implementiert, die jedoch eng zusammenwirken und somit auch als eines „großes Ganzes“ angesehen werden können. Gemeinsam überwachen und steuern diese beiden Modelle den Zugriff auf unterschiedliche Ressourcen des Smartphones.

1. **Linux Kernel (Sandbox):**
   Während ihrer Laufzeit befindet sich eine App innerhalb eines isolierten Bereichs im Arbeitsspeicher (RAM) des