Zertifizierte Apps

Dr. Sönke Maseberg[1], Bernhard Berger[2], Paul Gerber[3]

Kurzfassung:
Was bei typischen IT-Produkten seit Jahren gang und gäbe ist, klappt bei Apps nicht wirklich gut – die Evaluierung und Zertifizierung gemäß Common Criteria oder Datenschutz-Gütesiegel innerhalb eines vernünftigen Zeit- und Kostenrahmens. Apps entwickeln sich derart rasant – und sind meist kostenlos oder günstig zu erwerben –, dass ein völlig neuartiges Prüf- und Zertifizierungskonzept entwickelt werden muss. Dieses zu leisten, ist Gegenstand des Verbundprojektes „ZertApps“, das in diesem Beitrag vorgestellt werden soll.

Stichworte: Apps, Mobile Anwendungen, Prüfung, Zertifizierung, IT-Sicherheit, Datenschutz

1. Motivation

Smartphones und Tablets finden eine immer weitere Verbreitung sowohl im privaten als auch im geschäftlichen Umfeld. Wesentlich für ihren Erfolg ist die Tatsache, dass Nutzer mobile Anwendungen – also „Apps“ – einfach und bequem per Klick installieren können. Mit den Chancen dieser Entwicklung gehen jedoch leider auch große Risiken einher. Vor allem durch die wachsende Zahl von mobilen Anwendungen von oft unbekannten Entwicklern. Hierdurch steigt die Gefahr der Verbreitung von Schadsoftware, die sich beispielsweise als nützliche Anwendung tarnt. Zudem können Schwachstellen in Apps von Angreifern als Einstiegspunkte genutzt werden, um unberechtigten Zugriff auf Daten zu erhalten. Je weiter sich Apps verbreiten, desto größer werden insofern die potentiellen Sicherheitsrisiken für den Nutzer

Bei anderen IT-Produkten – etwa Kartenterminals, Firewalls oder Betriebssystemen – haben sich längst Prüf- und Zertifizierungsverfahren etabliert, um mögliche Sicherheitsrisiken aufzuspüren und im Anschluss an eine Prüfung zu bestätigen, dass das IT-Produkt „sicher“ ist. Zu nennen ist hier etwa das Zertifizierungsverfahren anhand der sogenannten Common Criteria (CC) mit Fokus IT-Sicherheit sowie das Datenschutzgütesiegel des Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig-Holstein mit den Schwerpunkten Datenschutzrecht und IT-Sicherheit.

Diese für IT-Produktprüfungen bekannten und nachhaltigen Prüfungs- und Zertifizierungsverfahren sind durchaus übertragbar auf die Prüfung von mobilen Anwendungen bzw. Apps. Allerdings sind die Verfahren zumeist sehr kostspielig für den App-Hersteller und ziehen sich in der Regel über Monate hin. Ferner tragen allgemeine Kriterienkataloge zu Datenschutzrecht und IT-Sicherheit den spezifischen Anforderungen an Apps nicht immer Rechnung. Damit hinken sie der schnellen Dynamik der App-Entwicklung hinterher.

1 datenschutz cert GmbH, Bremen

2 Technologie-Zentrum Informatik und Informationstechnik der Universität Bremen (TZI), Bremen

3 TU Darmstadt, CASED, EC SPRIDE, Darmstadt

2. Zielsetzung

Ziel des Verbundprojekts „ZertApps – Zertifizierte Sicherheit für mobile Anwendungen“ (nachfolgend auch kurz: „ZertApps“), das vom Bundesministerium für Bildung und Forschung (BMBF) gefördert wird, ist daher, das Thema „Sicherheitsanalyse von mobilen Anwendungen“ grundlegend und umfassend zu bearbeiten. Hierfür wird eine spezifische Prüf- und Zertifizierungsplattform für Apps entwickelt. ZertApps umfasst

- das Prüfkonzept,
- eine Unterstützung der Prüfung durch Tools,
- das Prüf- und Zertifizierungsschema,
- eine automatisierte Validierung sowie
- eine Kommunikation der Prüfergebnisse.

Zunächst stehen hierbei Android-Apps im Fokus, da diese derzeit einen größeren Marktanteil an den gängigen Betriebssystemen für Smartphones und Tablets besitzen. Es wird aber auch möglich sein, die Ergebnisse später auf andere Betriebssysteme, wie z.B. iOS, auszuweiten.

3. Das Prüfkonzept

3.1. Anforderungen an eine App

Jede App ist anders! Die Sicherheitsanforderungen einer Taschenlampen-App sind nicht zu vergleichen mit Anforderungen an eine Messenger-App. Deshalb ist zunächst der Sicherheitsmaßstab für eine konkrete App zu spezifizieren; dieser orientiert sich maßgeblich am Funktionsumfang und den verarbeiteten Daten.

3.1.1. Identifikation und Ist-Aufnahme

Im ersten Schritt wird der Untersuchungsgegenstand – also die zu prüfende und zu zertifizierende App – identifiziert und sodann deren technische Details sowie der Funktionsumfang in einer Ist-Aufnahme dargestellt.

ZertApps sieht das folgende Modell für eine Ist-Aufnahme der Funktionen einer App vor:

- Die zu zertifizierende App steht im Mittelpunkt der Betrachtung.
- Typischerweise findet eine Datenverarbeitung innerhalb des Smartphones oder Tablets statt, wobei die App auch Daten oder Ressourcen anderer Apps oder des Betriebssystems nutzen kann. Ferner kann eine Datenübermittlung an andere, externe Systeme erfolgen. Bezüglich einer Datenverarbeitung oder -übermittlung ist zu beachten, ob personenbezogene Daten im Sinne des Datenschutzrechts relevant sind.
- Die App operiert auf einem Betriebssystem (nachfolgend auch Operating System oder OS genannt) und weist folgende logische Schnittstellen auf:
    - nach außen zu anderen Servern, etwa im Internet (via TCP/IP, WLAN, NFC, Bluetooth etc.);
    - intern zu anderen Apps;

    - intern zu anderen Ressourcen, etwa Kamera, Mikrophone, GPS-Daten, Speicher, Gerätekennung, IMSI, IMEI etc.
- Ferner interagiert die App mit dem Nutzer über eine GUI (Graphical User Interface).

Abbildung 1 illustriert das Modell, das dem ZertApps-Prüfkonzept zugrunde liegt. Das Smartphone wird dabei auch stellvertretend für ein Tablet verwendet.

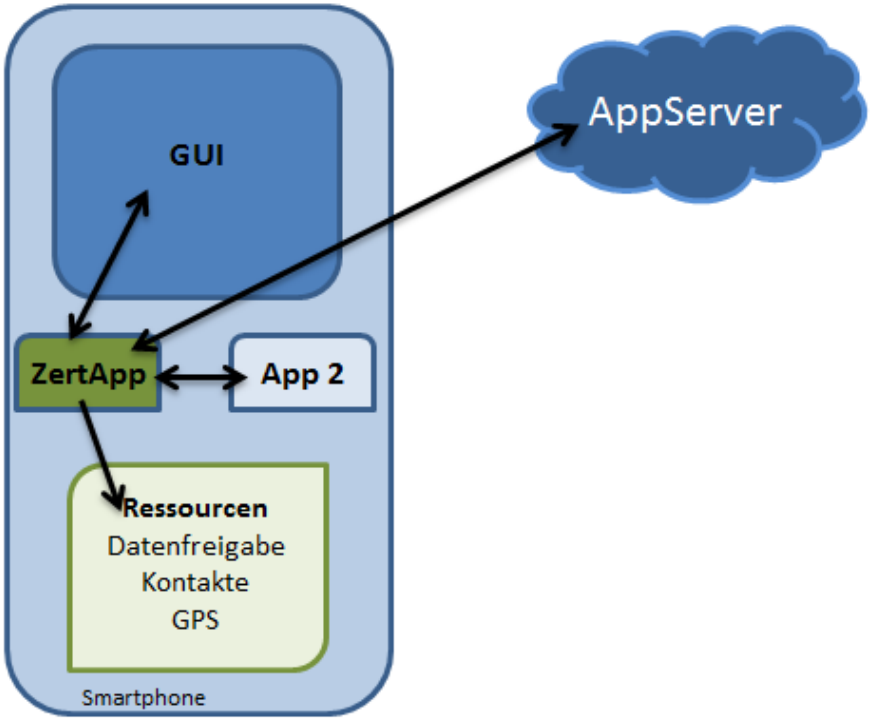

Abbildung 1: ZertApps-Modell

Bei der Ist-Aufnahme werden zur App die folgenden Informationen aufgenommen:

- Art der App: Beschreibung, um welche Art von App es sich handelt;
- Funktionen: Beschreibung des Funktionsumfangs;
- verwendete Schnittstellen: Beschreibung der logischen Schnittstellen, welche die App unterstützt oder benötigt (unter Berücksichtigung des o.g. ZertApps-Modells; Angaben: Name der logischen Schnittstelle, Verwendungszweck, Ziel, relevante Daten, Schutzbedarfskategorie, verwendetes Protokoll);
- verwendete Datenarten: Beschreibung der verwendeten Datenarten samt Schutzbedarfs-Klassifikation (inklusive Angabe des Speicherortes)

Intention ist, dass der App-Hersteller diese Informationen in Form einer Selbstauskunft angibt.

3.1.2. Sicherheitsbedarf

Im nächsten Schritt wird der konkrete Sicherheitsbedarf zusammengestellt. Dies erfolgt in mehreren Schritten. Zunächst werden erfasst:

- Bedrohungen;
- rechtliche Anforderungen;
- Annahmen an Betrieb und Einsatzumgebung.

Ausgehend von den Angaben der Ist-Aufnahme (insbesondere Art der Daten oder Kategorie der App) werden dazu typische Bedrohungen und grundsätzliche rechtliche Anforderungen automatisiert vorgegeben. Diese automatisierten Vorbelegungen lassen sich manuell korrigieren oder ergänzen, wobei entsprechende Begründungen nachzutragen sind. Ferner können – falls relevant – auch Hinweise oder Auflagen an den Benutzer angegeben werden.

Anschließend werden daraus Sicherheitsziele abgeleitet. Dies erfolgt wiederum automatisiert, was sich allerdings manuell korrigieren oder ergänzen lässt, ebenfalls mit entsprechenden Begründungen.

Nachdem die Sicherheitsziele identifiziert worden sind, werden Sicherheitsschwachstellen thematisiert. Zwar reichen grundsätzlich Maßnahmen zu den Sicherheitszielen aus, um den zuvor identifizierten Bedrohungen und rechtlichen Anforderungen hinreichend zu begegnen. Aus Erfahrung lässt sich aber sagen, dass häufig Fehler in der Implementierung oder Schwachstellen in der Realisierung auftreten, etwa bezüglich der Umgebung von Sicherheitsfunktionalitäten. Aus diesem Grund werden hier auch Sicherheitsschwächen thematisiert, um in konsolidierten Sicherheitszielen diese wichtigen Punkte adressieren zu können.

Intention ist, dass der App-Hersteller diese Informationen in Form einer Selbstauskunft validiert und ggf. ergänzt.

3.1.3. Sicherheitserwartung

Die Sicherheitserwartung gibt dem App-Hersteller an, welche Sicherheitsfeatures die zu zertifizierende App aufweisen muss.

Ausgehend vom Sicherheitsbedarf werden aus den angegebenen Bedrohungen, rechtlichen Anforderungen und Annahmen an den Betrieb oder die Einsatzumgebung schließlich die Anforderungen an die App extrahiert. Diese sogenannte Sicherheitserwartung ergibt sich direkt aus dem Sicherheitsbedarf; sie wird automatisiert vorgegeben, kann aber manuell korrigiert oder ergänzt werden, jeweils mit entsprechenden Begründungen.

Intention ist, dass der App-Hersteller diese Informationen in Form einer Selbstauskunft validiert und ggf. ergänzt.

3.1.4. App-Sicherheitsfeatures

Welche Funktionalitäten sind in der zu zertifizierenden App implementiert? Welche Sicherheitsfeatures der App decken die zuvor identifizierte Sicherheitserwartung ab? Welche zusätzlichen Funktionalitäten sind enthalten? Und warum?

Intention ist, dass der App-Hersteller

- seine implementierten Sicherheitsfeatures beschreibt,
- nachweist, dass alle Aspekte zur Sicherheitserwartung abgedeckt sind und
- auch etwaige rechtliche Aspekte begründet sowie
- erläutert, welche zusätzlichen Funktionalitäten aus welchem Grund enthalten sind.

3.2. Prüfung einer App

Wie tief soll geprüft werden, ob die Sicherheitsfeatures der App zur Realisierung der Sicherheitserwartung adäquat umgesetzt sind? Reicht eine Selbstauskunft? Muss ein Evaluator den Source-Code untersuchen? Ist die Entwicklungsumgebung relevant, um sicherzustellen, dass die geplanten Sicherheitsfeatures auch tatsächlich in die auszuliefernden Apps implementiert wurden?

Die Antwort, welche Prüftiefe angemessen ist, hängt insbesondere von zeitlichen und finanziellen Ressourcen sowie dem Schutzbedarf der App ab. Deshalb sieht ZertApps verschiedene Prüfstufen vor, in denen unterschiedliche Prüfungsarten kombiniert sind.

3.2.1. Prüfungsarten

Für ZertApps kommen verschiedene Arten der Prüfung in Betracht:

- Selbstauskunft;
- Plausibilitätstests;
- automatisierte Tests;
- Penetrationstests;
- juristische Prüfung;
- Site Visit.

Intention der Selbstauskunft als Prüfungsart ist, dass der App-Hersteller seine App in einer strukturierten Art und Weise darlegt und rechtlich sanktionierbar garantiert, dass seine Angaben zutreffen. Die Selbstauskunft ist damit die erste Stufe, um Vertrauen in eine App zu gewinnen. Die Selbstauskunft selber wird formal geprüft, die Angaben werden inhaltlich allerdings nicht durch Tests nachvollzogen. Um einen Missbrauch durch den App-Hersteller zu verhindern, wird die Selbstauskunft allerdings rechtsverbindlich vom App-Hersteller garantiert. Um der damit ausgesprochenen Garantie des App-Herstellers auch eine verbindliche und rechtlich sanktionierbare Wirkung zu verleihen, wird der App-Hersteller anhand von Allgemeinen Geschäftsbedingungen (AGB) der Zertifizierungsstelle an die Garantiewirkung gebunden. Falsche Angaben führen zu rechtlich durchsetzbaren Sanktionen.

Intention des Plausibilitätstests als nächsthöhere Prüfungsart ist es, durch einfache automatisierte Tests eine grundsätzliche Plausibilität zu den Angaben der Selbstauskunft herzustellen bzw. durch eine automatische Extraktion aus der App eine „vorausgefüllte“ Selbstauskunft zu schaffen, die den Prozess beschleunigt und etwaige Fehler ausschließt. Dazu wird die App über die in der Selbstauskunft angegebene Bezugsquelle

heruntergeladen. Durch den Plausibilitätstest mit automatisiertem Tool werden einige Informationen aus der App in der vorausgefüllten Selbstauskunft bereitgestellt.

Bei den automatisierten Tests erfolgt eine Verifikation der Selbstauskunft und eine Prüfung der Implementierung hinsichtlich handwerklicher Fehler. Dazu werden im Rahmen des ZertApps-Verbundprojektes umfangreiche Tools entwickelt, die u.a. folgende Fragestellungen beantworten helfen:

- Kommunikation: Wohin und mit wem nimmt die App Kontakt auf? Die in der App enthaltenen URLs, IP-Adressen, Telefonnummern etc. werden extrahiert und dahingehend geprüft und bewertet, ob sie dokumentiert und plausibel notwendig sind.
- Implementierung: Die Implementierung von Sicherheitsfunktionalität ist nicht trivial und birgt erfahrungsgemäß viele Schwachstellen. Die Implementierung wird geprüft und bewertet.
- Zugriffe auf Ressourcen: Welche Ressourcen nutzt die App? Die von der App angeforderten Ressourcen (z.B. IMSI, IMEI, Kamera, Mikrophone, GPS, interner Speicher, externer Speicher, SD-Karten) werden extrahiert und dahingehend geprüft und bewertet, ob sie dokumentiert und plausibel notwendig sind.
- Löschen: Es muss eine Möglichkeit geben, Daten zu löschen. Es wird daher geprüft und bewertet, wann und wie welche Daten gelöscht werden.
- Dynamischer Code: Das Nachladen dynamischen Codes, bei dem die zu zertifizierende App lediglich die „Hülle“ aufweist – durch die die eigentliche App dynamisch nachgeladen wird –, enthält nicht die nach außen angegebene Funktionalität der App. D.h. der Endnutzer kann möglicherweise nicht zwischen einer App, die lediglich die Hülle simuliert, und einer App, welche die eigentliche Funktionalität erbringt, unterscheiden. Von daher besteht die Gefahr, dass die zertifizierte App mit einer nicht zertifizierten Funktionalität verwechselt wird. Von daher ist dynamischer Code gegenwärtig nicht zertifizierbar. Es wird geprüft und sichergestellt, dass kein dynamischer Code nachgeladen wird.

Alle Testergebnisse werden mit den Angaben der Selbstauskunft verglichen bzw. im Sinne einer „vorausgefüllten“ Selbstauskunft im Dialog eingeblendet.

Eine weitere Prüfungsart stellen Penetrationstests dar, die noch stärker manuell durchgeführt werden und noch stärker die Angaben der Selbstauskunft verifizieren. Geprüft wird dabei insbesondere das Sendeverhalten der App.

Ob die datenschutzrechtlichen Anforderungen angemessen erfüllt werden, lässt sich nicht automatisiert durch ein Tool, sondern nur durch eine juristische Prüfung klären. Aus diesem Grund ist für die Prüfungsart „Juristische Prüfung“ eine Prüfung mit rechtlichem Hintergrund vorgesehen. Im Rahmen dieser Prüfung wird untersucht, ob die Dokumentation der Selbstauskunft zu den Prüfaspekten „Datenschutz“ und „Spezielle rechtliche Bestimmungen“ vorliegt, plausibel und nachvollziehbar ist. Eine weitergehende juristische Prüfung wird nicht vorgenommen.

Ob die App-Sicherheitsfeatures auch so, wie beschrieben, in die App implementiert und zur Auslieferung kommen, hat letztendlich auch etwas mit der Entwicklungs- und

Produktionsumgebung beim App-Hersteller zu tun. Aus diesem Grund wird beim Site Visit die Entwicklungs- und Produktionsumgebung vor Ort untersucht. Hierbei können anerkannte Standards für einen Site Visit herangezogen und ggf. vorhandene Zertifizierungen anerkannt werden.

3.2.2. Prüfstufen

ZertApps sieht vier Prüfstufen vor – Bronze, Silber, Gold und Platin –, die die obigen Prüfungsarten aufsteigend aufweisen.

3.3. Zertifizierung einer App

Ein ZertApps-Zertifikat gilt für eine exakt definierte Version der App und ist zwei Jahre gültig.

Erfahrungsgemäß unterliegen Software-Produkte – und insbesondere Apps – einem regelmäßigen Update- und Patchprozess. ZertApps sieht entsprechende Verfahren vor, um Updates oder Patches einer zuvor zertifizierten App in einem angemessenen Rahmen erneut zu begutachten und somit das Zertifikat auch auf diese neue Version der App ausweiten zu können. Maintenance- und Re-Zertifizierungsverfahren berücksichtigen die Ergebnisse der vorangegangenen Prüfungen sowie den Umfang etwaiger Änderungen, um eine angemessene Wiederholungsprüfung zu gewährleisten.

4. Toolunterstützte Prüfung

Je nach Prüftiefe sieht das Prüfkonzept unterschiedliche Unterstützungen durch Tools auf Basis von statischen und dynamischen Analysen vor. Hierdurch sollen die sehr aufwendigen und vor allem zeitintensiven Quellcodeaudits so gut wie möglich substituiert werden.

Plausibiltätstests werden mittels schneller Analysen auf Basis der App-Meta-Daten durchgeführt. Die Angaben der Hersteller werden hier vervollständigt oder geprüft. Hierfür wird eine Visualisierung für den Prüfer entwickelt, die die Ergebnisse der Selbstauskunft anzeigt und mittels graphischer Marker auf Abweichungen hinweist.

Automatisierte Tests überprüfen, ob die App Sicherheitsprobleme auf Grund von Konfigurationsfehlern oder Implementierungsschwächen enthält. So wird die Implementierung zum Beispiel auf verwundbare SSL-Verbindungen oder fehlerhafte Verschlüsselung hin untersucht. Die Konfigurationsfehler umfassen unter anderem nicht ausreichend geschützte Datenspeicher oder Softwarekomponenten.

Penetrationstests in der Prüfstelle werden durch Tools zur automatisierten architekturellen Risikoanalyse unterstützt. Hierfür wird aus der App-Implementierung (Quelltext) automatisiert eine Sicherheitsarchitektur extrahiert. Diese stellt graphisch die Bestandteile einer Anwendung, die Datenflüsse innerhalb einer App, die Verknüpfung mit anderen Anwendungen und externen Servern sowie die Verwendung von Tracking-Diensten dar. Diese Darstellung erlaubt einer Prüfstelle, schnell einen Überblick über die in einer App umgesetzten Sicherheitsmechanismen zu gewinnen, ohne ein aufwendiges Code-Review durchführen zu müssen. Auf diese Weise kann ohne hohen Aufwand erkannt werden, ob sicherheitskritische Daten, wie zum Beispiel Passwörter,

verschlüsselt auf dem Gerät abgelegt werden oder die Verbindung mit dem Backend kryptographisch gesichert ist. Insgesamt trägt dieser Schritt dazu bei, dass Evaluationen kosteneffizient durchgeführt werden und somit eine Sicherheitszertifizierung für App-Hersteller auch in höherer Prüftiefe finanzierbar wird.

Abbildung 2 zeigt die Darstellung eines kritischen Datenflusses in einer einfachen Testanwendung. Die App liest die eindeutige Gerätekennung aus und versendet diese mittels einer Textnachricht. In der nächsten Ausbaustufe wird die Ansicht um konkrete Ziele von externen Verbindungen erweitert, wie zum Beispiel die Telefonnummern, an die die Nachricht versendet wird.

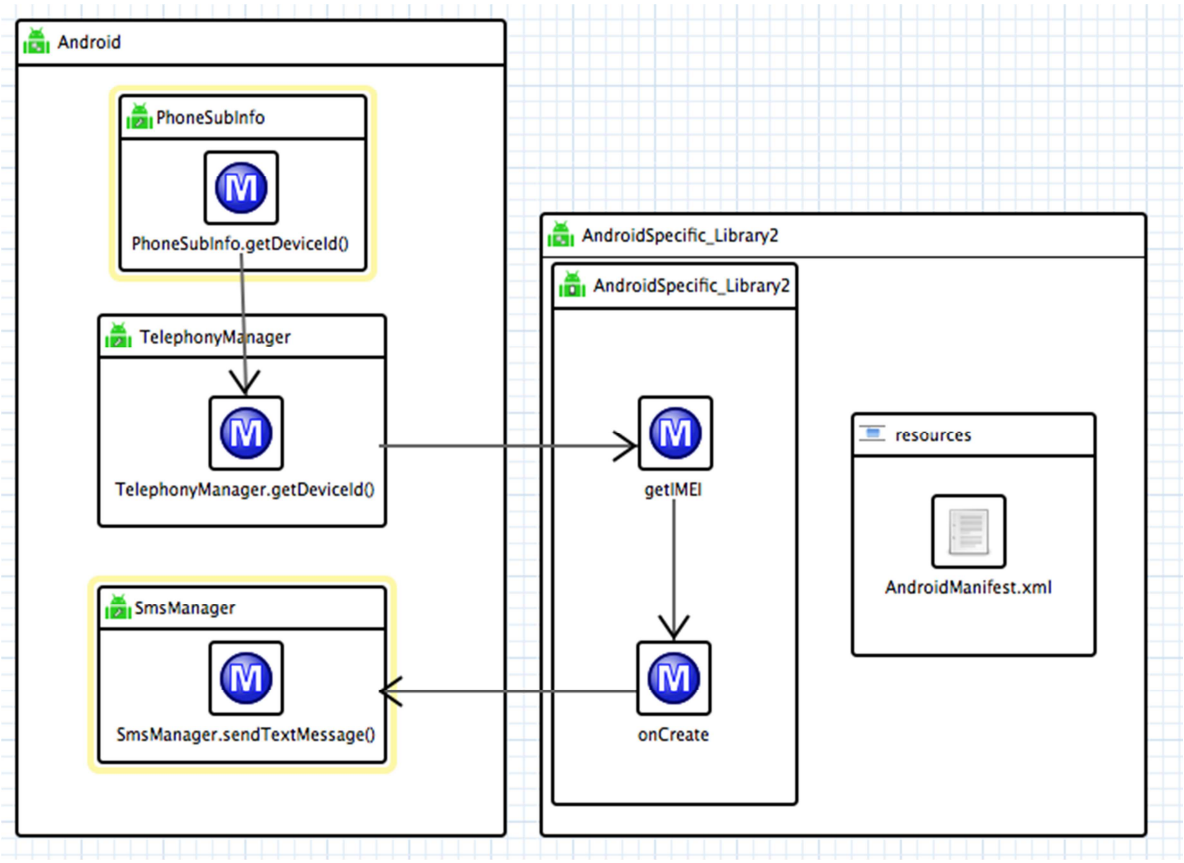

Abbildung 2: Darstellung eines kritischen Datenflusses

5. Das Prüf- und Zertifizierungsschema

ZertApps sieht ein klassisches zweistufiges Zertifizierungsverfahren zur Prüfung und anschließenden Zertifizierung vor. Dieses zweistufige Verfahren sieht eine klare Rollen- und Aufgabenverteilung zwischen Prüf- und Zertifizierungsstelle vor:

- Zunächst überprüft eine Prüfstelle, ob der Untersuchungsgegenstand die Anforderungen des Kriterienwerkes erfüllt. Sie dokumentiert ihr Prüfungsergebnis und empfiehlt anschließend – sofern die Prüfung ergab, dass der Untersu-

chungsgegenstand die Anforderungen erfüllt – die Erteilung eines entsprechenden Zertifikates.
- Der Zertifizierungsstelle obliegt die Zertifizierung eines Untersuchungsgegenstands, in der anschließend in Form eines Zertifikates dargestellt werden kann, dass die Anforderungen des Kriterienwerkes erfüllt werden.

Dieses zweistufige Verfahren mit klarer Rolle- und Aufgabenverteilung hat sich international in diversen Prüfungs- und Zertifizierungsverfahren etabliert – etwa den ISO 9001- oder den Common Criteria (CC)-Verfahren – und gewährleistet die Vergleichbarkeit der Prüfungen und Zertifizierungen. Aus diesem Grund liegen internationale und nationale Anforderungen vor, die vorgeben, wie Prüf- und Zertifizierungsstellen aufgebaut sein müssen, um sichere und verlässliche Prüfungen und Zertifizieren durchführen zu können. Diese Vorgaben wurden auf die spezifischen Anforderungen zur Prüfung und Zertifizierung von Apps konkretisiert – etwa ISO 17025 bzw. ISO 17065.

Ferner liegen vor: Schemadokumente, die die Vorgehensweise zur Prüfung sowie zur Zertifizierung von Apps beschreiben.

6. Automatisierte Validierung

Herkömmliche IT-Produkte, die ein Zertifikat aufweisen, zeigen dieses „Logo“ häufig als beigefügte Graphik oder als Link auf eine Zertifikatsliste. Diese vom Prozess losgelösten Artefakte sind für Apps nicht praktikabel. Denn hier muss direkt angezeigt werden, ob eine App eine gültige „ZertApp“ ist. Deshalb soll ein Validierungssystem entstehen, das die Prüfung, ob eine App ein gültiges Zertifikat aufweist oder nicht, automatisch durchführt.

Eine mögliche Lösung, die im Forschungsprojekt gegenwärtig durchdacht wird: Das Validierungssystem greift beim ersten Start und nach jedem Update der App auf einen Zertifizierungsserver zurück. Dieser validiert die anfragende App gegen seinen Datenbestand und bewilligt bzw. verweigert die Darstellung des Zertifikates auf dem Smartphone. Eine wichtige Komponente hierbei ist natürlich der App-Store, damit zertifizierte Apps bereits hier dargestellt werden. Deshalb wird ergänzend die Lösung verfolgt, dass der App-Store die Gültigkeit regelmäßig prüft. Nicht nur die Darstellung, ob eine App eine gültige „ZertApp“ ist, ist wichtig, sondern auch eine angepasste Darstellung der Prüfergebnisse.

7. Kommunikation der Prüfergebnisse

Nach erfolgreicher Zertifizierung müssen die Testergebnisse an den Anwender kommuniziert werden. Dies betrifft zum einen die durchlaufene Prüftiefe, welche aus den unterschiedlichen Sicherheitserwartungen an die jeweilige App resultiert, als auch eine Beschreibung des jeweiligen Prüfprozesses sowie die Ergebnisse des selbigen. Hierbei gilt es sowohl die begrenzten Ressourcen mobiler Geräte in Hinblick auf Platzangebot und Interaktionsformen zu beachten als auch eine verständliche, übersichtliche und dennoch möglichst vollständige Darstellung zu implementieren. Dies fördert die Transparenz des Gesamtprozesses und unterstützt somit Akzeptanz der Zertifizierung

durch den Anwender. Darüber hinaus ist für den Entscheidungsprozess des Anwenders unabdingbar zu wissen, welche Sicherheitserwartungen er an die jeweilige App stellen kann.

Neben den im Juni 2014 eingeführten Änderungen des Berechtigungsbildschirms (vgl. Abbildung 3) des Android Play Stores gibt es bereits diverse Vorschläge für eine optimierte Darstellung der von einer App angeforderten Berechtigungen innerhalb des Stores. Alle vorgeschlagenen Darstellungen beschränken sich auf die (teilweise stark abstrahierte) Aufbereitung der angeforderten Berechtigungen und/oder nutzen nicht standardisierte Codeanalysen (z.B. um die Nutzung einer spezifischen Berechtigung durch die App zu prüfen), welche für den Anwender nicht transparent gemacht werden.

Abbildung 3: Vergleich Berechtigungsbildschirm im Android Play Store vor Juni 2014 (links) und danach (rechts)

Im Rahmen des Forschungsprojektes werden deshalb verschiedene Darstellungsformen in einem nutzerzentrierten Prozess getestet und iterativ weiterentwickelt. Hierbei steht neben Vollständigkeit und Verständlichkeit der Zusammenfassungen, vor allem auch die Einfachheit der Generierung dieser im Vordergrund. So soll eine Implementierung in bereits bestehende App Store Lösungen möglichst nahtlos umsetzbar sein. Insbesondere der notwendige und gleichzeitig hinreichende Abstraktionsgrad der technisch anspruchsvollen Prüfergebnisse ist hierbei eine Kernherausforderung, welche interdisziplinär im Projekt bearbeitet wird. Im Rahmen der Kommunikation der ermittelten Prüfergebnisse wird auch der allgemeine Zertifizierungsprozess transparent gemacht, so dass sowohl Endanwender als auch Sicherheitsexperten individuell einschätzen können, ob das von der App zu erwartende Sicherheitsniveau den eigenen Ansprüchen genügt.

8. Zusammenfassung und Ausblick

Apps gewinnen zunehmend an Bedeutung – nicht nur im privaten Umfeld, sondern auch im Business-Bereich. Deshalb sind Apps auch für Angriffe interessant. Wie sind diese zu schützen? Wie kann man sichere von unsicheren Apps unterscheiden? Wie kann ein Unternehmen sicherstellen, dass nur geprüfte, sichere Apps installiert werden können? Das Projekt forscht dazu an Lösungen, durch welche Apps in verschiedenen Prüftiefen schnell, effektiv und kostengünstig geprüft werden können. Die Prüfung und Zertifizierung erfüllt alle internationalen Anforderungen an entsprechende Prozesse, ist aber beschleunigt. Und passt sich damit der Dynamik von Apps an.

Literaturhinweise

Bundesamt für Sicherheit in der Informationstechnik, „BSI – Technische Richtlinie, Kryptographische Verfahren: Empfehlungen und Schlüssel-längen“, BSI TR-02102.

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn, „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“.

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model.

Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components.

Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components.

Common Methodology for Information Technology Security Evaluation, Evaluation methodology.

Düsseldorfer Kreis, „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter“, 16.06.2014

Gerber, P. & Volkamer, V. (2015). Usability und Privacy im Android Ökosystem. Datenschutz und Datensicherheit, Vol. 2, 2015 (in press)

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.

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.

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.

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.

Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein, „ULD-Kriterienkatalog“