Anwenderforum für Fernmeldetechnik, AFCEA Computer, Elektronik und Automatisierung

AFCEA Bonn e.V. Studienpreis 2017

Kernthesen der Arbeit

Titel der Arbeit:	IMPROVING RISK COMMUNICATION TO SUPPORT USERS IN SECURITY AND PRIVACY DECISIONS THROUGH PERSONALIZED RUNTIME PERMISSION DIALOGS
Tag der Einreichung:	20.01.2017
Hochschule:	Rheinische Friedrich-Wilhelms Universität Bonn
Name des Verfassers:	Maria Muszynska
Betreuender Professor:	Jun.-Prof. Dr.-Ing. Delphine Reinhardt

Was ist die Quintessenz der Arbeit?

Die Benutzung von mobilen Applikationen (Apps) benötigt vielfach Zugriff auf private Daten. Oftmals werden hierbei mehr Daten angefordert als für die Kernfunktionalität einer App nötig wären, da das Erstellen eines Kundenprofils aus gesammelten Informationen das Geschäftsmodell vieler Apps ist. Neben Daten, wie z.B. Bildern und Nachrichten, kann hierbei auch auf Metadaten und diverse Sensoren zurückgegriffen werden um weiteres Wissen abzuleiten. Bei dem führenden mobilen Betriebssystem Android muss der Benutzer entscheiden ob eine App Privilegien (z.B. den Zugriff auf sensible Daten/Datenquellen, sicherheitsgefährdende Funktionalitäten) erhalten soll oder nicht. Diverse Studien kamen zu dem Ergebnis, dass diese Entscheidungsdialoge häufig ignoriert werden und auch bei genauerem Studium, aufgrund zu knapper oder technischer Erläuterungen, nicht verstanden werden. Es ist von zentraler Wichtigkeit, dass Nutzer sich der Konsequenzen von Berechtigungen bewusst sind, um solche Entscheidungen mündig treffen zu können. Daher müssen Berechtigungen auf eine Weise erklärt werden, sodass Nutzer stets bewusst und informiert das potentielle Risiko gegen den Nutzen einer App abwägen können.

Der in dieser Arbeit vorgestellte Ansatz ist ein menschengerechteres System, das Benutzer unterstützt eine bewusste Entscheidung über die Zurverfügungstellung persönlicher Daten zu treffen. Das vorliegende Risiko wird anhand persönlicher Daten konkret veranschaulicht. Hierfür wurden die gegenwärtigen Entscheidungsdialoge erweitert, sodass verständliche Erläuterungen, sowie persönliche, relevante Beispiele Teil des Entscheidungsprozesses werden können. Zum einen werden durch diese Personalisierung Berechtigungsbeschreibungen konkreter und zum anderen beugt eine zufällige Auswahl an Beispielen Gewöhnungseffekten vor.

Im Rahmen dieser Arbeit wurden 5 Fokusgruppen mit insgesamt 36 Teilnehmern durchgeführt um eine nutzerfreundliche Darstellung der Risiken durch Berechtigungen zu erreichen. Zusätzlich wurde die Relevanz von Informationsflüssen, d.h. Datenversand durch Apps an externe Empfänger, für Nutzer untersucht und erarbeitet wie dies verständlich modelliert werden könnte. Insgesamt war es von besonderer Wichtigkeit zu erörtern wie auch unser System den Privatsphärewünschen von Nutzern entsprechen kann. Auf Basis dieser Ergebnisse wurde ein Prototyp implementiert der für zwei weitere Nutzerstudien, mit insgesamt 40 Teilnehmern, verwendet wurde. In den Studien konnte gezeigt werden, dass die neuen Entscheidungsdialoge das Wissen über die Fähigkeiten einer App nach Berechtigungsvergabe erheblich verbesserte. Als Konsequenz wurde mithilfe der Dialogerweiterungen, im Vergleich zu den Standard-Dialogen, häufiger die privatsphärefreundlichere Entscheidung im Sinne der Datensparsamkeit getroffen. Es zeigte sich zudem, dass auch die Präsentation der Informationsflüsse für Nutzer von hoher Wichtigkeit ist und ein Abschätzen tatsächlicher Gefahren aufgrund der Vergabe von Berechtigungen an spezifische Apps erleichtert. Die Erkenntnisse aus dieser Arbeit sind für viele Anwendungsfälle, in denen privatsphäre- und sicherheitsrelevante Entscheidungen durch Menschen getroffen werden, wichtig und unsere Lösungsansätze übertragbar.