Institut für Visualisierung und Interaktive Systeme
Universität Stuttgart
Universitätsstraße 38
70569 Stuttgart
Germany

Diplomarbeit Nr. 3441

Evaluierung der Effizienz eines auf personenbezogenen Daten basierenden Passwortsystems

Serkan Hoser

Studiengang:	Informatik
Prüfer:	Prof. Dr. Albrecht Schmidt
Betreuer:	Stefan Schneegaß M.Sc. , Dr. Florian Alt
begonnen am:	22.01. 2013
beendet am:	24.07. 2013
CR-Klassifikation:	K.6.5

Kurzfassung

Immer mehr Menschen benutzen Smartphones und Tablets um online Geschäfte zu tätigen. Daher müssen sie sich immer mehr Passwörter merken. Das Problem mit Passwörtern ist, dass sie kompliziert genug sein müssen, um genug Sicherheit zu liefern, da sie sonst leicht geknackt werden können. Wenn sie jedoch zu kompliziert sind, kann man sie sich schlecht merken. Die Sicherheit von Passwörtern wird heutzutage durch Erhöhung der Komplexität erreicht um gegen Wörterbuch Angriffe und Brute-Force Angriffe geschützt zu sein. Die Benutzer konnten sich in Folge dessen nicht mehr an ihre Passwörter erinnern. In dieser Arbeit soll eine Methode der Authentifizierung untersucht werden, die persönliche Daten auf dem Smartphone dazu verwendet Passwortabfragen an den Benutzer zu stellen. Dazu wird eine App für das Android Betriebssystem entwickelt, die über einen Zeitraum Daten der Benutzer sammelt. Anschließend sollen diese Daten zur Authentifizierung der Benutzer verwendet werden. Dazu wurde eine Benutzerstudie durchgeführt welche die Eignung der Daten untersuchte. Die Ergebnisse führen zu dem Schluss, dass sich Bilder und Kontaktfotos am Besten für die kontextbasierte Authentifizierung eignen. Am Ende wird die Arbeit zusammengefasst und ein Ausblick auf Themen gegeben die zukünftig noch untersucht werden sollten.

Abstract

Today, a growing number of people are using smartphones and tablet pc's for online purchasing. For this reason, they have to remember a multitude of passwords. The problem with passwords is, that they have to be complicated enought to guarantee security, but easy enough to remember. Increasing the security of passwords is nowadays done by increasing complexity to be protected against dictionary and brute-force attacks. Thus, users were not able to remember these passwords anymore. This thesis presents a method for authentification that utilizes personal Data that is stored on smartphones. For this purpose, an Android app is developed which is used to record personal Data about its user over a period of time. Afterwards, these data shall be used to authenticate on the phone. Therefore, a user study is conducted, evaluating the feasibility of these data. The results suggest that graphical data are best for context based authentication. The thesis concludes with a summary and a description of future work that can be done in this area.

Inhaltsverzeichnis

1. Einleitung

Durch den technologischen Fortschritt existieren heutzutage immer mehr Systeme deren Verwendung eine Authentifizierung erfordert. Diese Systeme nehmen immer größere Teile im Leben des durchschnittlichen Bürgers ein. Sie sind vielfältig und reichen von sozialen Medien wie Facebook, Twitter über elektronische Auktionshäuser, Online-Banking, Bankautomaten bis hin zu Email-Konten oder der Sperrbildschirm eines Smartphones. Authentifizierung ist also fast allgegenwärtig. Da die Systeme bei denen man sich authentifiziert oft sicherheitskritische Daten, beispielsweise Kontoinformationen, beinhalten, ist die Wahl des Authentifizierungsverfahrens von enormer Bedeutung.
Für die Authentifizierung bieten sich verschiedene Methoden an. „Etwas das man hat“, „Etwas das man ist“ und „Etwas das man weiß“[W77]. Am weitesten verbreitet ist wahrscheinlich „Etwas das man weiß“. Diese Methode verwendet Wissen, das bevorzugt nur der Benutzer hat, um ihn zu authentifizieren. Das klassische Beispiel hierfür sind Passwörter. Um beispielsweise Geld an einem Bankautomaten abzuheben, benötigt man ein Passwort, den sogenannten PIN Code. Wenn man sich bei einem sozialen Netzwerk anmelden möchte wird ebenfalls nach einem Passwort gefragt. Aber auch Einrichtungen wie Schulen, Universitäten oder Bibliotheken verlangen oftmals von ihren Studenten, Benutzern und Mitarbeitern dass sie sich ein Benutzerkonto anlegen und ein Passwort wählen, um sich im von ihnen genutzten System zu authentifizieren. Dabei werden manchmal Anforderungen an das Passwort gestellt, damit nicht befugte Personen keinen Zugang erhalten können. Einem Student der kein sicheres Passwort hat, könnte es beispielsweise passieren dass ein Kommilitone seine Übungsabgaben kopiert.
Als Mindestanforderung an ein Passwort empfiehlt die Benutzerberatung der Universität Stuttgart dass es mindestens 8 Zeichen lang ist. Auch sollte bei der Wahl der Zeichen sichergestellt werden dass aus den Bereichen Kleinbuchstaben, Großbuchstaben und Zahlen jeweils ein Zeichen gewählt wird. Dies soll die Sicherheit des Passworts erhöhen und unbefugten Zugriff verhindern. Das Problem bei Passwörtern ist jedoch, dass es einen Konflikt zwischen Merkfähigkeit und Sicherheit gibt. Das heißt. es ist nicht möglich hohe Sicherheit und gleichzeitig hohe Merkfähigkeit bei einem Passwort zu erreichen. Wählt man das Passwort zu einfach ist es für Betrüger und Diebe ein leichtes, das Passwort zu ermitteln. Wenn aber ein zu schwieriges Passwort gewählt wird, kann man es sich nicht mehr so gut merken. Viele Menschen schreiben daher ihre Passwörter auf und/oder verwenden dasselbe Passwort um sich auf mehreren Systemen zu authentifizieren. Das richtige Gleichgewicht zwischen Sicherheit und Merkfähigkeit zu finden ist nicht immer trivial und kann für manche Menschen ein größeres Problem darstellen. Vor Allem ältere Menschen haben oft Schwierigkeiten sich komplizierte Kombinationen aus Zahlen, Buchstaben und/oder Sonderzeichen zu merken, weshalb Sie oft zu einfachen Passwörtern greifen und da-

mit zum Ziel für kriminelle Energien werden können. Es werden beispielsweise häufig Dinge wie Geburtsdatum, der eigene Name oder Namen von Personen und Dingen im sozialen Umfeld (Familienmitglieder, Haustiere usw...), Tastenkombinationen von nahe beieinander liegenden Tasten wie „qwertz“ und einfach zu merkende Kombinationen wie „abc“, „123“ usw. verwendet. In solchen Fällen ist ein Missbrauch sehr einfach möglich.
Oft reichen aber Passwörter nicht und es werden alternative Authentifizierungsmethoden verwendet oder mehrere Arten der Authentifizierung werden kombiniert, um dem Benutzer mehr Sicherheit zu garantieren. Manche Laptops haben einen Fingerabdruckscanner zu Authentifizierung, und bei einem Bankautomaten kann nur in Kombination mit einer Bankkarte und einem Passwort Geld abgehoben werden.
Auch wenn Passwörter in vielen Fällen einen akkuraten Schutz bieten, sind sie nicht unüberwindbar. Es gibt mehrere Methoden um ein fremdes Passwort herauszufinden. Eine Methode wäre das sogenannte „Shoulder Surfing“. „Shoulder Surfing“ wird von Brennen definiert als :
“...the observation of an individual entering their password without their knowledge. Historically, this involved looking over the individual's shoulder while they were sitting at a terminal” [B2004] .
Eine Lösung für dieses Problem wäre es, bei jedem Anmelden ein anderes Passwort zu verlangen. Ein „Shoulder Surfer“ hätte in so einem Fall keinen Vorteil wenn er ein Passwort gesehen hätte. Damit der rechtmäßige Benutzer sich nicht eine Vielzahl von Passwörtern merken muss, könnten die Passwörter aus Wissen das der Benutzer besitzt, generiert werden. Eine kommerzielle Implementierung dieser Idee stellen die sogenannten SecureID Token dar. Diese wurden von der Firma RSA Security entworfen und stellen ein tokenbasiertes Authentifizierungssystem dar[1]. Das Problem dieses Systems ist es, dass man den SecureID Token stets mit sich tragen muss.
Ein Bereich in dem Authentifizierung eine immer größere Rolle spielt ist der Bereich der mobile Geräte. Fast jeder Mensch in der westlichen Welt besitzt heutzutage ein Smartphone. Auch in Deutschland sind Smartphones weit verbreitet. Die Verbreitung lag laut einer Untersuchung von BITKOM im Oktober 2012 bei 38 %.[2.] Die Rechenleistung von Smartphones nimmt wie auch bei klassischen Computern, immer weiter zu. Dank dieser Rechenleistung erschließen sie sich immer mehr Anwendungsgebiete die traditionell den Desktop Computern vorbehalten waren. Ein Beispiele wäre Möglichkeit Videos in hoher Qualität zu betrachten.
Da Smartphones und Tablets im Vergleich zu Laptops relativ klein und leicht sind, werden sie von immer mehr Menschen nicht nur zum Telefonieren verwendet, sondern auch um im Internet zu surfen, Mails abzurufen oder online einzukaufen. Dienste wie Ebay oder PayPal verknüpfen dabei sensible Daten wie Kontoinformationen mit einem online Account. In solch einem Fall hängt die Sicherheit des Bankkontos von der Sicherheit des Passworts ab, welches man für diese Dienste gewählt hat. Wenn man nun aus Bequemlichkeit seine Passwörter speichert und das Smartphone

1 http://www.rsa.com/press_release.aspx?id=5989

2 http://www.bitkom.org/de/presse/74532_73749.aspx

eine Weile unbeaufsichtigt lässt, kann es passieren das sensible Informationen gestohlen werden und man dadurch im schlimmsten Fall den Zugriff auf wichtige Online-Konten verliert. Ein System zu finden mit dem sichere Passwörter generiert werden können, die aber nicht zu einfach sind, ist eine Herausforderung die es zu bewältigen gilt. Diese Arbeit versucht das Problem der Merkfähigkeit von Passwörtern für mobile Geräte zu lösen. Dazu soll ein alternatives System zur Generierung von Passwörtern geschaffen werden. Die Idee ist es, Daten, die auf dem Smartphone verfügbar sind zu verwenden, um daraus eine Passwortabfrage für den Benutzer zu erstellen. Diese Passwortabfrage könnte bei jedem Login andere Daten verwenden und so dafür sorgen dass keine zwei Passwörter identisch sind, was zur Erhöhung der Sicherheit beitragen würde. Anschließend soll ermittelt werden, wie gut Benutzer sich diese Passwortabfragen merken können. Um diese Idee zu testen, wird eine App entwickelt, die in einer Benutzerstudie auf den Smartphones verschiedener Testpersonen installiert wird und etwa zwei Wochen lang Daten sammelt. Am Ende der Frist soll untersucht werden, wie gut sich Fragen zu Daten auf dem Smartphone für Passwörter eignen. Die Teilnehmer müssen dazu eine Reihe von Fragen beantworten. Diese können sich beispielsweise auf Fotos beziehen (Wo wurde dieses Foto geschossen?), Daten aus der Anrufliste verwenden (Wann haben sie Person X angerufen?) oder versuchen herauszufinden ob der Teilnehmer sich an seinen Aufenthaltsort zu einem vergangenen Zeitpunkt erinnert (Wo waren sie gestern um 12 Uhr?). Diese Studie dient dazu herauszufinden welche Daten und Fragen sich besonders gut eignen. Es gibt eine Vielzahl an Quellen die Daten produzieren, welche für eine Passwortabfrage in Betracht kommen. Jedes halbwegs aktuelle Smartphone besitzt mindestens eine Kamera mit der man Bild– und Videodaten gewinnen kann. Smartphones speichern auch SMS und Anruflisten und diese können ebenfalls für Passwörter verwendet werden. Viele Smartphones haben zudem meist mehrere Sensoren wie einen Beschleunigungsmesser, einen Magnetometer und ein Gyroskop um die Ausrichtung des Smartphones zu erfassen. Auch diese Geräte produzieren wertvolle Daten.
Der Wifi Adapter eines Smartphones kann nach aktuell verfügbaren Wifi Netze suchen, welche dann geloggt werden können. Zu guter Letzt kann man mithilfe von GPS-Tracking aufzeichnen wo das Smartphone sich befindet oder befunden hat.

Der weitere Aufbau dieser Arbeit ist folgender:
In Kapitel *zwei* werden Verwandte Arbeiten beschrieben und Hintergrundinformationen zum Thema und zur Ausarbeitung dieser Arbeit gegeben. Außerdem wird der Begriff der Merkfähigkeit erläutert, da dieser ein Untersuchungspunkt dieser Arbeit ist. Im Unterkapitel Hintergrund werden Informationen erläutert, die für das Verständnis der Arbeit nötig sind.
Im Kapitel *drei* wird das Konzept der Arbeit vorgestellt. Die grundlegenden Probleme sowie deren Lösungen werden erläutert.
Kapitel *vier* erläutert die programmatische Ausarbeitung der in Kapitel drei vorgestellten Idee. Es werden alle Klassen und Methoden beschrieben sowie der Ablauf der Programms vorgestellt.

Kapitel *fünf* handelt von der Durchführung der Studie. Die Auswahl der Teilnehmer, die Installation der Anwendung und die anschließende Befragung werden hier besprochen. In *sechsten* Kapitel werden die Ergebnisse der Studie präsentiert.
Im Kapitel *sieben* wird die Arbeit kurz zusammengefasst. Außerdem werden weitere interessante Fragen erläutert, die während der Arbeit aufgekommen sind.
Kapitel *acht* besteht aus dem Anhang, der den Fragebogen enthält, den die Studienteilnehmer ausfüllen mussten.

2. Hintergrund und verwandte Arbeiten

In diesem Kapitel werden Hintergrundinformationen zum Thema der Diplomarbeit gegeben. Außerdem werden bisher veröffentliche Arbeiten anderer Autoren, die mit dem Thema zusammenhängen, beschrieben.

2.1. Hintergrund

Ein Ziel dieser Arbeit ist es eine zukünftige Studie mit Teilnehmern aus Googles Play Store vorzubereiten. Dazu wurden unterschiedliche Möglichkeiten betrachtet, um die Anwendung, die in den Play Store gestellt werden soll, zu entwickeln. Die Anwendung soll eine Art Authentifizierung auf dem Smartphone ermöglichen. Das Problem ist es, dass man in den Android Betriebssystemen der meisten kommerziell verfügbaren Smartphones keinen Zugriff auf Systemfunktionalitäten hat. Für die Anpassung der Authentifizierungsfunktionalität wäre dies aber nötig. Um das Problem zu lösen stehen drei Möglichkeiten zur Verfügung. Die erste ist es, ein gerootetes Gerät zu nehmen. Auf einem Gerät auf dem man Root Rechte hat, ist es möglich, eine modifizierte Version des Android Betriebssystems zu installieren. Damit ist es möglich die Login Funktionalität des Betriebssystems umzuschreiben. Als zweite Möglichkeit kann die Mindestanforderungen für die Studie als Android Version 4.2 festgesetzt werden. In dieser ist es möglich den Standard Sperrbildschirm von Android mit Widgets auszustatten. Auf diese Art und Weise könnte eventuell das Problem gelöst werden. Die letzte Option wäre es, einen eigenen Homescreen zu schreiben und ihn mit Funktionalität auszustatten um den Bildschirm zu sperren.
Die erste Möglichkeit wurde ausgeschlossen, weil nicht jeder Benutzer eines Android Smartphones sein Gerät gerootet hat oder es rooten möchte. Viele Benutzer haben auch nicht das Wissen oder die Zeit sich mit einer anderen Android Version zu beschäftigen. Daher kann dies nicht als Voraussetzung einer Authentifizierungsanwendung dienen. Die zweite Möglichkeit wurde ebenfalls ausgeschlossen. Das Erweitern des Sperrbildschirm ist dazu gedacht, Anwendungen wie Wettervorhersagen, Nachrichten usw... anzuzeigen ohne das Smartphone zu entsperren. Außerdem ist diese Funktionalität erst ab Android 4.2 verfügbar, womit auf eine Rückwärtskompatibilität zu älteren Android Versionen verzichtet werden müsste. Dies würde die Zahl der Benutzer, die die Anwendung installieren und verwenden würden, einschränken.
Die dritte Option wurde daher als die optimale Lösung angesehen.

2.1.1 Implementierungsgrundlagen

In diesem Unterabschnitt wird die Umgebung beschrieben, in der die Implementierung ausgearbeitet wurde. Dazu zählen Betriebssystem, Entwicklungsumgebung, Programmiersprache und sonstige Tools, die verwendet wurden. Außerdem werden wichtige Elemente des Android Systems erläutert.

2.1.2 Java

Java ist eine objektorientierte Programmiersprache die zu den meist verwendeten Programmiersprachen auf der Welt zählt. Java ist dank der Java Virtual Machine plattformunabhängig und läuft auf jeder Plattform für die es eine Virtual Machine gibt.

Eclipse

Eclipse ist eine sehr beliebte Entwicklungsumgebung speziell für Java Entwickler. Nach der Installation des „Android Development Tool“ Plugins für Eclipse ist es möglich das Android SDK (Software Development Kit) zu verwenden. Außerdem kann man ein Android Gerät per USB an den PC anschließen und seine Anwendung direkt auf dem Gerät testen und ein Debugging durchführen.

Android

Android ist ein Betriebssystem für mobile Plattformen wie Smartphones, Tablets und Netbooks. Android ist Open Source Software und basiert auf einen Linux Kernel. Für Entwickler existiert die Android SDK, die genutzt werden kann um Anwendungen (sogenannte „Apps“) für Android zu programmieren. Die Programmierung geschieht dabei in Java. Dadurch ist es für Java Programmierer relativ einfach, für Android zu entwickeln, es muss nur die Android SDK erlernt werden.

Da Android Open Source Software ist, wird es von vielen Herstellern von mobilen Geräten als Betriebssystem für ihre Geräte verwendet. Zu den Firmen die Android verwenden zählen unter anderem Samsung, HT, Motorola und Huawei. Dadurch hat Android auf mobilen Geräten weltweit eine hohe Verbreitung, in Europa erreichte sie 70 %.[3]

Android SDK Tools

Die Android SDK Tools bestehen aus dem Android SDK Manager und dem Android Virtual Device Manger. Mithilfe des SDK Managers können verschiedene Versionen der Android SDK installiert und verwendet werden. Es ist auch möglich die Google API's zu installieren. Der AVD Manager dient der Emulation von Android Geräten. Es stehen mehrere Geräte der Nexus Klasse von Google sowie Geräte verschiedene Größen, inklusive Tablets, zu Verfügung. Außerdem ist es möglich eigene Geräte zu definieren. Der AVD Manager emuliert viele der Teile eines realen Android Gerätes. Dazu gehört GPS, Beschleunigungssensor, Annäherungssensor und ein Gyroskop. Leider ist die Emulation eventuell aus diesem Grund relativ schwerfällig in der Bedienung.

AnroidManifest.xml

Die AndroidManifest.xml Datei ist ein zentraler Teil in einer Android Anwendung. Jede Anwendung muss eine AndroidManifest.xml Datei besitzen, welche auch nicht anders benannt werden darf. Sie befindet sich im Hauptverzeichnis der Implementie-

3 http://www.zdnet.de/88160639/android-erreicht-70-prozent-marktanteil-in-europa/

rung. Die AndroidMainfest.xml Datei präsentiert dem Android System essentielle Informationen, welche es benötigt um den Anwendungscode auszuführen. Das Manifest hat unter anderem folgende Aufgaben:

- Es benennt das Java Paket für die Anwendung. Der Name dient als eindeutiger Bezeichner.
- Es beschreibt die Komponenten der Anwendung. Die Activities, Services, Broadcast Receivers und Content Provider aus denen die Anwendung besteht werden in die AndroidManifest.xml eingetragen. Es gibt an welche Klassen durch die einzelnen Komponenten implementiert werden und was sie können. Diese Deklaration beschreiben dem System was die einzelnen Komponenten sind und unter welchen Bedingungen sie gestartet werden können.
- Es bestimmt welche Prozesse Anwendungskomponenten beherbergen.
- Es beschreibt welche Rechte die Anwendung haben muss um auf geschützte Teile der API zuzugreifen und mit anderen Anwendungen zu kommunizieren.
- Es deklariert die Rechte die andere Anwendungen haben müssen um mit den Komponenten der eigenen Anwendung zu interagieren.
- Es gibt das Mindestlevel der Android API an das die Anwendung zum Laufen benötigt.
- Es führt die Bibliotheken an gegen die die Anwendung gelinkt wird.[4]

Content Provider

Content Provider verwalten den Zugriff auf eine geordnete Menge von Daten. Sie kapseln die Daten und liefern Mechanismen um Datensicherheit zu gewährleisten. Content Provider sind das Standard Interface, das Daten in einem Prozess und ausgeführten Code in einem anderen Prozess, verbindet. Um auf Daten eines Content Providers zuzugreifen, benutzt man das Content Resolver Objekt aus dem Kontext der implementierten Anwendung. Das Content Resolver Objekt kommuniziert mit dem Provider Objekt, welches eine Instanz einer Klasse die einen Content Provider implementiert ist. Das Provider Objekt erhält Datenanfragen von Clients, führt die gewünschten Aktionen durch und gibt die Ergebnisse zurück an die Clients.[5]
Eine Anfrage an einen Content Provider wird über die „query“ Methode des Content Resolver Objekts durchgeführt, der gewünschte Content Provider sowie die gewünschten Informationen werden als Parameter übergeben. Das Ergebnis dieser Anfrage ist ein Cursor Objekt, das die gewünschten Informationen enthält und wie eine Tabelle durchsucht werden kann.
Smartphones mit dem Android Betriebssystem beinhalten meist eine Reihe von Content Providern, um den Zugriff auf Daten wie Kontaktadressen oder gespeicherte Fotos zu ermöglichen.

4 http://developer.android.com/guide/topics/manifest/manifest-intro.html

5 http://developer.android.com/guide/topics/providers/content-providers.html

2.2. Verwandte Arbeiten

In diesem Unterkapitel werden bisher veröffentliche wissenschaftliche Arbeiten, die in die selbe oder eine ähnliche Kategorie wie diese Diplomarbeit fallen, besprochen.

2.2.1 Authentifizierung

Es gibt generell drei verschiedene Arten der Authentifizierung: „Etwas das man weiß“, „Etwas das man hat“ und „Etwas das man ist“[BJRSY06]. Beispiele für Authentifizierungsmethoden die „Etwas das man weiß“ verwenden, wären alle Arten von Passwörtern wie der Pin Code der Bankkarte, das Login Passwort für den PC oder die Zahlenkombination an einem elektronischen Türschloss. Aber auch grafische Passwörter zählen hierzu. „Etwas das man hat“ bezeichnet sogenannte „Token“, also Dinge die man besitzen muss um sich zu authentifizieren. Ein gutes Beispiel wäre hier wieder die Bankkarte(siehe Abbildung 1). Aber auch andere Arten von Karten wie zum Beispiel der Studentenausweis, mit dem man in spezielle Arbeitsräume kommt, gehören in diese Kategorie. „Etwas das man ist“ bezeichnet biometrische Eigenschaften, wie Fingerabdrücke, Iris und DNA. Diese kommen vor Allem in sehr sicherheitskritischen Systemen zum Einsatz, beispielsweise in Form von Irisscannern(siehe Abbildung 2) oder Stimmanalyzern. Aber mittlerweile sind sie auch in eventuell weniger sicherheitskritischen Bereichen verfügbar wie zum Beispiel Fingerabdruckscanner in Laptops für Privatpersonen. Im Folgenden werden diese drei Ansätze anhand verschiedenen wissenschaftlichen Publikationen erläutert. Bei Passwort basierten Systemen werden grafische Passwörter und Systeme die Fragen zur Authentifikation verwenden näher erläutert.

Abbildung 1: Beispiel für tokenbasierte Authentifizierung: Bankkarte [6]

Abbildung 2: Beispiel für biometrische Authentifizierung: Irisscanner

6 http://upload.wikimedia.org/wikipedia/commons/7/76/Ec-bankkarte.jpg
http://upload.wikimedia.org/wikipedia/commons/1/1b/IriScan_model_2100_iris_scanner_1.jpg

2.2.2 Grafische Passwörter

Es gibt unterschiedliche Arten von Passwörtern. Dazu gehören numerische Passwörter wie der sogenannte PIN Code. Ein Beispiel wäre der Code der zum Benutzen einer SIM Karte in einem Mobiltelefon benötigt wird. Es gibt aber auch alphanumerische Passwörter wie sie beim Anmelden in Computersysteme an Universitäten verwendet werden. Diese beiden Typen sind Passwörter, die vom Benutzer verlangen dass er sich eine Reihe von Zeichen merkt und diese zur Authentifizierung eingibt. Laut Wiedenbeck et al. haben Passwörter zwei sich widersprechende Anforderungen[WWBBM052]:

- Sie sollen einfach zu merken sein und der Authentifizierungsvorgang soll schnell und einfach durchgeführt werden.
- Passwörter sollen sicher sein, d.h. sie sollen zufällig erscheinen und schwer zu raten sein. Sie sollen häufig geändert werden, und nicht für mehrere Systeme verwendet werden. Außerdem sollten sie nicht niedergeschrieben werden.

Diese zwei Punkte beschreiben die zwei wesentlichen Merkmale eines Passwortsystems. Dies sind die Merkfähigkeit und Sicherheit. Eine mögliche Lösung um diese beiden Aspekte von Passwörtern zu stärken wäre die Verwendung von grafischen Passwörtern. Bei grafischen Passwörtern werden Bilder verwendet um sich zu Authentifizieren. Grafische Passwörter haben eine Reihe von Vorteilen gegenüber numerischen und alphanumerischen Passwörtern.

Nielsen beschreibt in seiner Arbeit [Nie93] dass es im Allgemeinen einfacher ist etwas *wiederzuerkennen*, als sich an dieselbe Information aus dem Gedächtnis zu *erinnern*. Dieser Punkt legt nahe, Dinge die man *wiedererkennt,* wie zum Beispiel Bilder als Authentifizierungsmethode zu verwenden.

Dhamija und Perrig führten eine Studie durch, in der sie das von ihnen entwickelte grafisches Authentifizierungssystem „D´ej`a Vu**“** untersuchten[DP00]. In diesem Authentifizierungssystem musste der Benutzer eine Anzahl p von Bildern aussuchen die seine Authentifizierungsbilder darstellten. Bei einer Authentifizierung wurden ihm n Bilder präsentiert, von denen m aus seinen Bildern stammen. Diese mussten erkannt werden. Diese System wurde mit einem PIN und einem alphanumerischen Passwortsystem verglichen. Das Ergebnis war das 90% der Teilnehmer erfolgreich „D´ej`a Vu**“** nutzten, während bei den Passwort und PIN System eine Erfolgschance von 70% gegeben war. Dieses Ergebnis spricht dafür dass sich Benutzer grafische Passwörter eventuell besser merken als klassische Passwörter und PINs.

De Angeli et al. beschreiben in ihrer Arbeit [ACCLG02] ebenfalls ein System das Bilder verwendet um einen Benutzer zu authentifizieren. Es werden detaillierte und farbige Bilder von Objekten verwendet. Um sich zu authentifizieren musst eine Reihe von Bildern erkannt werden. Die Bilder die dazu verwendet werden, und die Reihenfolge in der sie erkannt werden müssen, wird vom System vorgegeben. Das sorgt dafür dass die Benutzer keine einfachen Sequenzen wählen können und erhöht so die Sicherheit. Außerdem sollte damit die Auswahlzeit für das Passwort reduziert wer-

den. Als optimale Eingabemöglichkeit wird der Touch Screen genannt.
Es wurde eine Benutzerstudie durchgeführt die herausfinden sollte ob sich Bilder besser zur Authentifizierung eignen als Zahlen, ob ein Authentifizierungssystem basierend auf Bildern sicherer als numerische Passwörter ist oder als sicherer empfunden wird und welches System von den Benutzern bevorzugt wurde. Weiterhin sollte beantwortet werden ob sich die Position der Bilder auf die Bilderinnerung auswirkt und ob sich Benutzer an eine Sequenz von Bildern erinnern können. Dazu wurden vier verschiedene Systeme entwickelt und verglichen.
Das erste System (PIN) zeigte dem Benutzer ein Ziffernfeld mit den Ziffern Null bis Neun, die so angeordnet wurden wie es bei klassischen Bankautomaten der Fall ist. Hier sollten sich die Benutzer einen vierstelligen PIN merken und korrekt wiedergeben. Das zweite System(VIP1) verwendete anstelle der Ziffern Bilder, wobei die Anordnung dieselbe wie im ersten System war. Die korrekten Bilder wurden immer an der selben Stelle positioniert, jedoch wurden für die andern Positionen jedes mal andere Bilder gewählt. System Nummer drei(VIP2) unterschied sich vom zweiten System dadurch, dass die korrekten Bilder randomisiert platziert wurden. Das letzte System(VIP3) wies dem Benutzer acht Bilder zu gab ihm eine Menge von 16 Bildern, in denen vier der acht Bilder enthalten waren. Der Benutzer musste diese vier Bilder erkennen, die Reihenfolge spielte keine Rolle.
Die Ergebnisse der Studie legten nahe dass PINs basierend auf Bildern weniger fehleranfällig waren. Außerdem wurden sie von den Teilnehmern als angenehmer empfunden. Das vierte System schnitt als schlechtestes ab. Als Ursache wurde genannt dass das visuelle Gedächtnis anfällig für Störungen sei. Außerdem erschwere die zufällige Wahl von vier der acht Bilder, welche jede mal durchgeführt wurde und die zufällige Platzierung der Bilder, das Lernen der korrekten Antworten.
Das erste System schnitt als Bestes ab. Die feste Positionierung der Bilder erhöhten die Eingabegeschwindigkeit und reduzierte die Fehlerrate.
Abschließend wurde festgestellt, dass weitere Entwurfsstudien notwendig sind und das ein falscher Entwurf für grafische Authentifizierungssysteme wie VIP3, den Vorteil eines grafischen Authentifizierungssystems zunichte machen kann.
Takada und Koike implementieren ein System das den Benutzern die Möglichkeit gibt Bilder zu registrieren[TK03]. Mindestens eines der registrierten Bilder muss als Passbild gesetzt werden. Bei einer Authentifizierung muss der Benutzer dann sein registriertes Bild wählen. Der Vorteil dieses Verfahren ist es dass der Benutzer seine persönlichen Lieblingsbilder als Passbilder setzen kann und sich so eventuell besser an sie erinnert. Wiedenbeck et al. untersuchten ein etwas anderes grafisches Authentifizierungssystem. Ihr vorgeschlagenes System namens Passpoints verwendet echte Bilder, auf denen eine Reihe von Stellen gedrückt werden muss. Die verwendeten Bilder werden in ein Grid aus Quadraten unterteilt wodurch die Anzahl der Stellen bestimmt wurde die gewählt werden können. Diese werden bei der Passwortauswahl vom Benutzter ausgewählt. Bei einem Bild mit einer Größe von 1024 x 752 Pixeln und den Auswahlquadraten mit 20 x 20 Pixeln sowie Passwortlänge von fünf ergibt sich ein Passwortraum von $2{,}6 \times 10^{16}$. Ein alphanumerisches Passwort über einem Al-

phabet von 96 Zeichen und einer Passwortlänge von acht Zeichen besitzt einen Passwortraum von 7,2 x 10^{15}. Der Passwortraum des grafischen Systems ist also um eine Größenordnung größer und somit ist die Sicherheit des grafischen Systems vergleichbar mit dem des alphanumerischen Systems. Eine vergleichende Studie ergab dass die Teilnehmer welche das grafische Authentifizierungssystem verwendeten schneller ein Passwort erstellen konnten, aber länger für die Eingabe benötigten und mehr falsche Eingaben machten als Teilnehmer die ein alphanumerisches System verwendeten. Die Merkfähigkeit für beide Systeme war ähnlich. [WWBBM05]
Ein weiteres System das grafische Passwörter verwendet, beschreiben Nazir et al. in ihrer Arbeit [NZI09]. Das vorgeschlagene System verwendet eine Kombination aus alphanumerischem Passwort und grafischen Passwort. Zuerst muss der Benutzer ein alphanumerisches Passwort auswählen. Anschließend werden ihm drei Bildersets aus je neun Bildern präsentiert. Er muss sich aus jedem der drei Mengen drei Bilder aussuchen. Diese werden binär auf zwölf Stellen kodiert. Nach diesem Schritt werden diese Werte zusammen mit dem alphanumerischen Passwort und seinem Benutzernamen kodiert, verschlüsselt und als Passwort gespeichert.
Bei einem Authentifizierungsprozess geschieht folgendes: Der Benutzer meldet sich mit seinem Benutzernamen und dem alphanumerischen Passwort an. Anschließend werden ihm wieder die Bildersets präsentiert. Diesmal sind die Bilder jedoch anders angeordnet. Das heißt der Benutzer muss sich die Bilderinhalte und nicht die Position der einzelnen Bilder merken. Der Benutzer wählt die drei Bilder die er beim Setzen des Passworts gewählt hatte. Es wird wieder das selbe Verfahren auf den Benutzernamen, das Passwort und die Binärwerte der Bilder angewendet. Ist das Ergebnis identisch mit dem gespeicherten Wert, wird der Benutzer authentifiziert. Ist das Ergebnis nicht korrekt, hat der Benutzer zwei weitere Versuche mit den nächsten beiden Bildersets. Falls er bei diesen Bildersets ebenfalls nicht korrekt antwortet, wird das Benutzerkonto gesperrt. Laut Nazir et al. ist dieses System sicher vor vielen Arten von Attacken. Durch die Kombination von alphanumerischen Passwörtern und Bildern sollen Brute Force Attacken erschwert werden. Angriffe die Wörterbücher zur Hilfe nehmen werden erschwert durch ein randomisiertes Passwort und dem Vorhandensein der Bilder als Passwortkomponente. Als weiterer Vorteil dieser Methode wird angegeben dass es den Benutzer nicht überfordert.
Ein grafisches Authentifizierungssystem das kommerziell verwendet wird ist Passfaces™. In Passfaces™ erhält jeder Benutzer eine Folge von Fotos, auf denen Gesichter abgebildet sind, als sogenannte *Passfaces*. Bei einer Authentifizierung muss der Benutzer sein Passface aus einer Menge von neun Bildern erkennen. Als Vorteile dieses Systems werden folgende Dinge genannt:

- Kann nicht aufgeschrieben oder kopiert werden.
- Kann nicht weitergegeben werden.
- Kann nicht geraten werden.
- Es werden kognitive Fähigkeiten benötigt, nicht die Fähigkeit sich Dinge zu merken.

- Kann alleine oder zusammen mit anderen Authentifizierungsverfahren verwendet werden.[7]

Es kann natürlich argumentiert werden ob die aufgezählten Vorteile immer vollständig gegeben sind. Man könnte bei verschiedenen Authentifizierungsversuchen den angezeigten Bildschirm abfotografieren, bis man alle Passfaces aufgenommen hat. Diese könnten nun markiert, kopiert und weitergegeben werden. Dies ist bei einem alphanumerischen Passwort aber immer noch einfacher als bei grafischen Passwörtern.
Grafische Passwörter werden untersucht da sie Verbesserungen in der Authentifizierungsrate versprechen[Nie93]. Es sollte aber auch untersucht werden, wo die eventuellen Risiken und Schwachstellen von grafischen Authentifizierungsverfahren liegen.
Trotz der Verbesserungen die grafische Passwörter versprechen, sind sie nicht vor allen Angriffen gefeilt. Wie erwähnt ist es bei manchen Systemen mit einigen Mitteln möglich sein Passwort „aufzuschreiben“ wodurch wieder dieselben Probleme auftreten können wie bei einem aufgeschriebenen alphanumerischen Passwort. Ein weiteres Problem, dass betrachtet wird, sind „Shoulder Surfing“ Angriffe.
Tari et al. führten eine Untersuchung durch, die das empfundene und tatsächliche Risiko von „Shoulder Surfing“ Angriffen von alphanumerischen Passwörtern und einem grafischen Authentifizierungssystem vergleicht. Es wird das grafische Authentifizierungssystem Passfaces™ mit zwei alphanumerischen Passwörtern verglichen: Eines das Wörterbucheinträge als Passwörter verwendet, und eines das diese nicht verwendet. Passfaces™ wurde in zwei Konfigurationen verwendet. Eine bei der man das Bild mit der Maus auswählt, und eine bei der das Bild über den Nummernblock einer Tastatur ausgewählt wird.
Bei der Passfaces™ Konfiguration mit der Maus, wurde von den Teilnehmern ein höheres „Shoulder Surfing“ Risiko erwartet und auch erfahren. Der Wechsel von der Eingabe mit der Maus zur Eingabe mit der Tastatur reduzierte dieses Risiko erheblich. Dies könnte an der Geschwindigkeit der Eingabe liegen und daran dass der Angreifer auf zwei Stellen gleichzeitig schauen muss. Erstaunlicherweise hatte das Passwortverfahren, welches nicht Wörterbucheinträge verwendete, das höchste Risiko für „Shoulder Surfing“. Das kann daran liegen dass der Angreifer Zeit hat das Passwort Zeichen für Zeichen nachzuverfolgen.
Das Passwortverfahren das Wörterbucheinträge verwendete war resistenter gegen „Shoulder Surfing“ als das Passfaces™ System mit der Maus und dem Passwortverfahren das keine Wörterbucheinträge verwendete. Das könnte daran liegen dass die Geschwindigkeit bei einem richtigen Wort höher ist[TOH06].
Miyachi et al. beschreiben ein System welches grafische Passwörter verwendet. Das System verwendet die DWT(Diskrete Wavelet Transformation) um ein Passwortbild in ein anderes Bild einzubetten[MTHTK10]. Das System wird auf Shoulder-surfing Robustheit und Merkfähigkeit untersucht. Dabei vergleichen sie ihr System mit dem von Harada et al. [HIN04]. Die Untersuchung ergab dass ihr System eine FAR, was in diesem Fall die Erfolgsrate von „Shoulder Surfing“ Angriffen bezeichnet, von 7%

7 http://www.realuser.com/published/The%20Science%20Behind%20Passfaces.pdf

aufwies. Im Gegensatz dazu hatte das System von Harada et al. eine Rate von 69% und bei einem System das keine eingebetteten Passwortbilder verwendete war sie 95%. Die Merkfähigkeit in diesem System nahm auch über einen Zeitraum von vier Wochen kaum ab, wohingegen das System von Harada et al. an Merkfähigkeit verlor. Farmand und Zakaria versuchen in ihrer Arbeit [FZ10] eine Lösung für Shoulder Surfing bei grafischen Authentifizierungssystemen zu finden. Sie verwenden ein System das den Benutzer dazu auffordert zwischen den Bildern bestimmte Zeichen einzugeben.
Ein Faktor der die Sicherheit eines grafischen Authentifizierungssystems beeinflusst, ist die Wahl der Bilder welche zur Authentifizierung verwendet werden. Davis et al. haben in ihrer Arbeit [DMR04] zwei grafische Authentifizierungssysteme auf ihre Sicherheit untersucht unter der Voraussetzung dass die als Passwörter verwendeten Bilder von den Benutzern ausgewählt wurden. Eines der beiden untersuchten Systeme basierte auf Bildern von Gesichtern. In diesem Fall wählten ein großer Teil der Benutzer attraktive Bilder des anderen Geschlechts, oder Bilder von Personen mit der selben Herkunft. 75.9% der Männer wählten Gesichter von Frauen, 63,2 % sogar Bilder von Models. 52,1% der asiatische Frauen wählten asiatische Gesichter. Aus diesen Ergebnissen schließen Davis et al., dass die Wahl der Bilder nicht den Benutzern überlassen sollte, wie es beispielsweise im Passfaces™ System geschieht. Bulling et al. beschreiben in ihrer Arbeit [BAS04] ein grafisches Authentifizierungssystem das keine direkte Interaktion des Benutzers erfordert, sondern über Blicke gesteuert wird. Das Passwort besteht dabei aus Betrachtungspunkten eines Bildes. Dabei werden Teile des Bildes, die Aufmerksamkeit auf sich ziehen, verdeckt um den Benutzer dazu zu bringen ein sichereres Passwort zu wählen. Die Ergebnisse der Untersuchung zeigten, dass diese Methode die Sicherheit des gewählten Passwortes signifikant erhöhte.

2.2.3 kontextbasierte Passwörter

Kontextbasierte Passwörter verwenden persönliche Informationen um einen Benutzer zu authentifizieren. Dazu werden Daten aus verschiedenen Quellen verwendet. Dies können besuchte Webseiten, persönliche Daten auf einem Smartphone oder Bewegungsprofile sein. Die Daten werden aufgezeichnet oder aus vorhandenen Quellen extrahiert und dazu verwendet, dem Benutzer Fragen zu stellen.
Einer der ersten die solch ein System untersuchten waren Zvrian und Haga. Sie verwendeten Fragen wie „Was ist ihr Lieblingsgemüse?“ und „Wenn Sie den Beruf wechseln könnten, welchen neuen Beruf würden sie wählen?“ Die Ergebnisse zeigten dass es einfacher war sich an diese Art von Passwörtern zu erinnern, und diese Passwörter schwer von anderen Personen erraten werden konnten[ZH90].
In der Arbeit von Babic et al. wird ein System untersucht das als Authentifizierungsmethode kurzlebige Fragen bezüglich Aktivitäten des Benutzers verwendet. Damit eine vorherige Eingabe der korrekten Antworten nicht nötig ist, werden Daten verwendet die automatisch abgerufen werden können. Das System soll vier Kriterien erfüllen. Diese sind Geheimhaltung, Erinnerbarkeit, Unaufdringlichkeit und Anpas-

sungsfähigkeit. Geheimhaltung soll garantieren dass richtigen Antworten schwer zu erraten sind. Erinnerbarkeit beschreibt das Kriterium dass der Benutzer sich nur an seine aktuellsten Ereignisse und Netzwerkaktivitäten erinnern muss. Mit Unaufdringlichkeit ist gemeint dass das System im Hintergrund laufen soll. Anpassungsfähigkeit steht für die Eigenschaft des Systems Fragen automatisch generieren und aktualisieren zu können. Um die Fragen zu generieren werden drei verschiedene Kategorien von Informationen verwendet. Diese sind die Netzwerkaktivität, Physikalische Ereignisse und konzeptionelle Meinungen.
Netzwerkaktivität bezeichnet hauptsächlich online Aktivität, wie Emails oder Surfen im Internet. Dazu werden Fragen wie beispielsweise „Welche Webseite haben Sie zuletzt besucht?“ gestellt. Da Benutzer kaum ihrer Surfgewohnheiten mit Anderen teilen, wird hier die Sicherheit des Systems erhöht.
Physikalische Ereignisse sind Ereignisse die aus dem Kalender, empfangenen Emails, sozialen Netzwerken und anderen ähnlichen Diensten extrahiert werden können. Eine passende Frage wäre zum Beispiel „Wo wird das nächste Meeting stattfinden?“. Das Problem dieser Fragen ist, dass deren Sicherheit mit der Anzahl der Teilnehmer eines Ereignisses abnimmt.
Konzeptionelle Meinungen können aus den Emails und den besuchten Seiten im Internet herausgelesen werden. Eine Person mit einem bestimmten Standpunkt wird oft Artikel mit ähnlichen Einstellung zum beschriebenen Thema lesen. Dazu könnten Fragen gestellt werden, wie „Finden Sie den Machtwechsel in Ägypten Positiv?“
Diese Art von Fragen könnten für Angriffe, die das Ergebnis raten, anfällig sein. Um die Sicherheit zu erhöhen, könnten mehrere Antwortmöglichkeiten und mehrere Fragen zu verschiedenen Themen gestellt werden. Es wurde eine Studie mit vier Teilnehmern durchgeführt. Diese kannten sich bis zu einem gewissen Grad untereinander. Jeder Teilnehmer erhielt zwölf Fragen, jeweils vier aus den drei genannten Kategorien. Die Teilnehmer mussten die Fragen beantworten und angeben wie sicher sie sich waren. Dabei stand der Wert drei für „einfach zu erinnern“ und eins für „schwierig zu erinnern“. Außerdem mussten sie die Antworten der anderen Teilnehmer raten.
Die Erinnerbarkeit der Fragen wurden im Durchschnitt mit 2,23 bewertet. Dies zeigt dass diese Art von Fragen von den Benutzern als positiv angesehen werden. Fragen die nach einem Zeitpunkt verlangten, konnten am Schlechtesten geraten werden. Fragen die die Arbeit der Teilnehmer betrafen waren einfacher zu Raten weil die Teilnehmer Kollegen waren[BXYI09].
In [THU10] untersuchen Tang et al. eine Authentifizierungsmethode die Data Mining verwendet. Genauso wie in dieser Arbeit werden auch dort GPS Daten der Benutzer gesammelt. Zusätzlich zu den GPS Daten kommt die Anwendungshistorie dazu welche die Reihenfolge der Starts von Anwendungen festhält. Beim Wechsel der aktuell im Vordergrund laufenden Anwendung wird die neue Anwendung an die Historie angehängt. Das System basiert auf der Sammlung von Benutzerdaten und der Generierung von Regeln aus diesen Daten. Diese Regeln repräsentieren die Gewohnheiten des Benutzers (Wo ist er üblicherweise? Welche Programme benutzt er?). Neue Daten werden nur eingefügt wenn sie diesen Regeln entsprechen oder explizit vom Be-

nutzer autorisiert werden. Das System ist als Client Server Architektur aufgebaut. Der Client ist das Smartphone und der Server ein System, das sich mit der Speicherung der Daten und der Generierung von Regeln befasst. Auf Client Seite gibt es zwei Teile: Die „Data Collection“ Einheit und den „Security Manager“. Die „Data Collection“ Einheit sammelt periodisch Daten und sendet sie an den „Data Preprocessor“ der auf dem Server läuft und die Daten in Form von gerichteten Graphen organisiert. Falls der Anwender Regeln trainiert hat, werden diese in der „Analysis Engine“ mit den ankommenden Daten verglichen. Bei einem positiven Ergebnis werden die Daten gespeichert, bei einem negativen Ergebnis wird erst durch eine Passwortabfrage sichergestellt ob der Benutzer legitim ist. Der „Security Manager“ auf Client Seite empfängt die Authentifizierungsergebnisse von der „Analysis Engine“. Bei einem positiven Ergebnis wird nichts getan, bei einem negativen Ergebnis muss er die erwähnte Passwortabfrage durchführen. Im Falle das die Passwortabfrage nicht erfolgreich beantwortet wird, sperrt der „Security Manager“ das Gerät. Die Regeln werden anhand der gerichteten Graphen generiert, die darstellen in welcher Reihenfolge Anwendungen genutzt werden und welchen Orten in welcher Reihenfolge er sich aufhält(beispielsweise auf dem Weg zur Arbeit). Außerdem werden diese zwei Graphen verknüpft um zu erfassen, wo der Anwender welche Anwendung benutzt. Regeln sind Pfade im Graphen und bestehen aus einem Tripel das aus folgenden Eigenschaften besteht: Ist der Pfad häufig? Wie oft kommt er vor und wie lang ist er. Regeln werden als häufig betrachtet wenn ihr Vorkommen einen bestimmten Schwellenwert erreicht.Mit diesem System wurde eine Studie mit 10 Personen über 20 Tage durchgeführt. Die ersten 15 Tage wurden als Trainingszeitraum genutzt und die letzten fünf als Testzeitraum. Es konnte gezeigt werden das sich die Regeln bei den meisten Teilnehmern nach einer gewissen Zeit stabilisierten. Durch die Wahl von 50 Ergebnissen aus dem Testzeitraum wurde eine Genauigkeit von 0,76 ermittelt, was die Effektivität des Systems beweisen soll.
Nosseir et al. untersuchen in ihrer Arbeit [NCD05] die Machbarkeit eines Authentifizierungssystems das persönlichen elektronische Informationen einer Person verwendet um ihr Fragen zu stellen. Durch eine ausreichende Menge an Daten die nur dem authentischen Benutzer im benötigtem Detailgrad bekannt ist und für einen Angreifer zu umfangreich zum Lernen ist, soll die Sicherheit gewährleistet werden. Die Daten die verwendet wurden waren Kalenderdaten, die verwendeten Fragen waren Multiple Choice Fragen. In einer ersten Studie wurde die Machbarkeit solch eines Systems ermittelt, in einer zweiten Studie wurden die Fragen ausgewählt an die sich die Benutzer gut erinnern konnten. Das Ergebnis war das Fragen zu aktuellen sich wiederholenden und angenehmen Ereignissen besser geeignet waren und weiter untersucht werden sollten.
In einer weiteren Arbeit untersuchen Nosseir und Terzis ein System das Fragen zur persönlichen Historie einer Person stellt und dies als Authentifizierung verwendet[NS10]. Es wurden mehrere Arten von Daten verwendet, unter anderem Daten von akademischen Webseiten, die viele Informationen über die akademische Historie der Teilnehmer lieferten. Es wurde eine Studie durchgeführt. Zu jeder Art

von Daten wurden verschiedene Fragen generiert und geprüft wie gut sich Teilnehmer ihre eigenen Fragen und die der anderen Teilnehmer beantworten konnten.
In der Studie wurden Informationen aus persönlichen akademischen Webseiten verwendet. Es wurde eine Studie mit 25 Teilnehmern aus dem akademischen Bereich durchgeführt. Es wurden Fragen zu den Bereichen Lehre, Forschung, Publikationen, Studium und Freizeit gestellt. Sechs Fragen wurden formuliert, vier textbasierte und zwei auf Bildern basierende Fragen. Die Fragen wurden jeweils den Teilnehmern dessen Daten verwendet wurden sowie anderen Teilnehmern die als „Angreifer“ fungierten, gestellt. Bei den Bildern wurden Bilder von Personen(beispielsweise Koautoren von Publikationen), Orten(Lokationen auf dem Kampus) und Karten (Karte der Universität) gewählt. Von den Antworttypen waren Multiple Choice Antworten sowie ja/nein Antworten vertreten. Zuerst wurden die textbasierten Fragen untersucht. Die Wahrscheinlichkeit richtiger Antworten seitens des Teilnehmers und des Angreifers, bestätigten die Werte einer früheren Studie und wurden als Baseline verwendet. Die Ergebnisse der auf Bildern basierenden Fragen führten zu dem Schluss dass diese Art von Fragen die Wahrscheinlichkeit von korrekten Antworten seitens der authentischen Teilnehmer erhöht und keine Auswirkung auf die Wahrscheinlichkeit von korrekten Antworten seitens der Angreifer hat.
Nosseir et al. untersuchen in ihrer Arbeit [NCRT06] ob Daten, die von „intelligente Umgebungen“ über deren Benutzer generiert werden, zur Unterscheidung von ehrlichen Benutzern und Betrügern verwendet werden können. Es wurde ein Experiment durchgeführt, welches in einem intelligenten Raum, der mit verschiedenen Sensoren ausgestattet war, stattfand. Der Raum war mit Sensoren wie passive Infrarotsensoren, Sensoren die den Zustand der Türen registrierten und Lichtschranken ausgestattet. Da diese Sensoren sehr limitiert sind und keine Auskunft über die Personen die sie auslösen verraten, wurden für die Testpersonen unterschiedliche Routen ermittelt. Ein Beispiel wäre wenn ein Türsensor aktiviert wurde, danach eine Lichtschranke und zuletzt der Infrarotsensor unter einem bestimmten Schreibtisch mehrmals ausgelöst wurde. Wenn die Person den Raum verließ, wurden die Sensoren in der umgekehrten Reihenfolge ausgelöst. Die Studie wurde über einen Zeitraum von 5 Wochen durchgeführt. Anschließend wurden aus den Sensordaten persönliche Situationen abgeleitet und Authentifizierungsfragen generiert. Das Ergebnis der Studie war dass Situationen die von Sensordaten erkannt wurden, dazu verwendet werden können Fragen zu generieren und damit echte Benutzer von falschen Benutzern zu unterscheiden. Dazu sei es aber noch nötig weitere Untersuchungen anzustellen.

2.2.4 Token

Token basierte Authentifizierungsverfahren verlangen vom Benutzer ein sogenanntes *Token* um ihn zu authentifizieren. Hallsteinsen et al. haben ein Verfahren untersucht bei dem das Smartphone als Authentifizierungstoken verwendet wird. Die Authentifizierungsstelle sendet ein sogenanntes „Challenge“ an das Smartphone, aus dem ein „One Time Password“ generiert wird. Ist dies identisch mit dem Passwort das auf der Authentifizierungsseite generiert wird, wird der Benutzer authentifiziert[HJT07]. In

einer anderen Arbeit beschreiben Thanh et al. ein Verfahren, Smartphones und deren SIM Karte als Authentifizierungsmethode für alle Internetanwendungen zu verwenden[TJFTJ08]. Kunyu et al. präsentieren in ihrer Arbeit [KJJ09] ein Token basiertes Authentifizierungsverfahren welches ein Smartphone als Token nutzt und Bluetooth zu Datenübertragung verwendet. Tanvi et al. stellen in ihrer Arbeit [TSK11] ebenfalls ein tokenbasiertes Authentifizierungssystem vor, welches Smartphones als Token nutzt. Aloul et al. implementieren ein System das das Smartphone als Token in einem Zwei Faktoren Authentifizierungssystem verwendet. Die Idee ist es, anstelle mehrerer Authentifizierungstoken bei sich zu haben, mehrere Softwaretoken auf dem Smartphone zu installieren und zur Authentifizierung in verschiedenen Systemen zu verwenden[AZE09].
Die bisher genannten Systeme nutzen ein Smartphone meist *als Token* um sich bei einem System zu authentifizieren. Es geht also um die Authentifizierung auf einem System mithilfe eines Smartphones, nicht aber auf dem Smartphone selbst. Bojinov und Boneh versuchen im Gengensatz dazu in ihrer Arbeit „Mobile Token-Based Authentication on a Budget“ ein Gerät zu entwickeln das genutzt werden kann um sich *auf* einem mobilen Gerät zu authentifizieren und das Gerät somit zu Entsperren. Es werden zwei Optionen untersucht: Ein Gerät das den Magnetsensor eines Smartphones anspricht und es auf diese Art und Weise entsperrt, und ein Gerät das eine bestimmte Tonfolge erzeugt die vom Mikrofon des Smartphones aufgenommen und als Entsperrsignal gewertet wird. Das erste Token, das sogenannte „MagKey“ bestand zunächst aus einer festen Anordnung von Magneten, deren Orientierung eine Art Passwort kodierten. Dies erwies sich aber als nicht zuverlässig da der Magnetsensor eines Smartphones nicht empfindlich genug sei. Als nächster Schritt wurde ein Gerät mit einem aktiven Schaltkreis gebaut das ein digitales Signal als Folge von Veränderungen im magnetischen Feld eines Induktors erzeugen kann. Dieses Gerät lieferte viel zuverlässigere Ergebnisse. Als Token das einen Ton erzeugt um das Smartphone zu entsperren wurde ein piezoelektrischen Summer verwendet. Die Auswertung ergab das das Verfahren das den Magnetsensor eines Smartphones anspricht, aufgrund des Nachlassens des magnetischen Feldes mit der Entfernung, schwieriger benutzbar war, aber hohen Schutz vor Abhörattacken lieferte, da ein Angreifer sehr nahe an das Smartphone herankommen muss um das Signal zu erfassen. Das Verfahren das auf Sound basiert um das Smartphone zu entsperren lieferte gute Ergebnisse. Der piezoelektrische Summer der verwendet wurde hatte den Vorteil das es einen geringen Energieverbrauch hatte[BB11].

2.2.5 Biometrie

Biometrische Authentifizierungsverfahren sind Verfahren, die Dinge wie Fingerabdrücke und DNA als Authentifizierungsmethode verwenden. Der Vorteil bei der Verwendung biometrischer Verfahren ist, dass man sich keine Passwörter merken muss und keine Authentifizierungstoken bei sich haben muss um sich zu authentifizieren. Die Authentifizierung ist abhängig von den biologischen Eigenschaften der sich authentifizierenden Person. In einer Studie die von Clarke und Furnell mit 297 Teilneh-

mern durchgeführt wurde, gaben 83% an dass sie eine Art von biometrischer Authentifizierung auf dem Smartphone gut finden würden[CF05].
Bei den biometrischen Authentifizierungsverfahren spielt im Gegensatz zu den Passwortverfahren die Merkfähigkeit keine Rolle, da es nichts gibt das man sich merken muss. Der wichtigste Punkt ist hier die Sicherheit. Auch kann bei biometrischen Verfahren im Allgemeinen nichts gestohlen werden da kein Passwort aufgeschrieben wird und kein Token existiert. Es gibt zwar Methoden um biometrische Authentifizierungssysteme zu täuschen, diese sind aber generell mit technischem Aufwand verbunden. Galbally-Herrero et al. untersuchen in ihrer Arbeit [GFRAOT06] beispielsweise die Möglichkeit, Sensoren mit falschen Fingerabdrücken aus Silikon zu täuschen. Es gibt verschiedene biometrische Methoden die man für die Authentifizierung verwenden kann. Beispiele hierfür sind Gesichtserkennung, Handerkennung, Fingerabdrücke, Irisscan, Stimmerkennung und Tastendruckerkennung.
Tao und Veldhuis beschrieben in ihrer Arbeit ein biometrisches Authentifizierungssystem für Mobile Geräte welches Gesichtserkennung nutzt. Dabei werden drei Aspekte betrachtet die eine Herausforderung für ein Authentifizierungssystem auf mobilen Systemen darstellen. Dies sind der Sicherheitsaspekt, der Bequemlichkeitsaspekt und der Komplexitätsaspekt. Für die Bewertung des Sicherheitsaspekts wurde die FAR (False Accept Rate) und die FRR(False Reject Rate) verwendet. Die FAR beschreibt die Wahrscheinlichkeit mit der ein Angreifer auf das Gerät zugreifen kann. Um Sicherheit zu gewährleisten sollte dieser Wert ausreichend niedrig sein. Bei einem „False Reject“ hat das System die biometrischen Eigenschaften des rechtmäßigen Benutzers nicht erkannt, und dieser muss die Authentifizierung wiederholen. Das kann zu Unannehmlichkeiten seitens des Benutzers führen. Aus diesem Grund sollte auch die FRR ausreichend niedrig sein. Um noch benutzerfreundlicher zu sein sollte die Authentifizierung ohne explizite Benutzerinteraktion möglich sein. Die Durchführung der Authentifizierung soll aus Sicherheitsgründen auf dem Gerät durchgeführt werden. Daher muss der Algorithmus eine geringe Komplexität aufweisen um nicht zu viele Ressourcen des mobilen Gerätes zu verwenden.
Hadid et al. untersuchen eine Methode der Authentifizierung die Gesichts- und Augenerkennung nutzt. In ihrer Arbeit [HHSP07] werden zwei Implementierungen erläutert und verglichen. Es wird ein System implementiert, welches Haar-like features mit AdaBoost für die Gesichts- und Augenerkennung und die „Local Binary Pattern“ Methode für eine Augenerkennung verwendet. Zum Vergleich wurde ein anderes Gesichtserkennungssystem implementiert, welches die Hautfarbe für eine schnelle Erkennung verwendet.
Trotz der beschränkten Prozessor- und Speicherkapazitäten zeigte dass System gute Werte. Es wurden durchschnittliche Authentifizierungsraten von 82% für kleine Bilder(40x40 Pixel) und eine Rate von 96% für Bilder die aus 80 mal 80 Pixeln bestehen erreicht.
Trewin et al. führten eine Studie durch in der sechs verschiedene Authentifizierungsschemata für mobile Geräte auf Anwenderfreundlichkeit untersucht wurden. Es wurde ein Passwortverfahren und drei verschiedene biometrische Verfahren basierend

auf, Stimm- Gesichts- und Gestenerkennung verwendet. Die zwei letzten Untersuchungspunkte waren Verfahren die eine Kombination aus Gesten- und Stimmerkennung sowie Gesichts- und Stimmerkennung verwendeten. Die Eingaben der Benutzer wurden nicht auf Korrektheit geprüft. Stattdessen wurde ein Server im lokalen Netzwerk dazu verwendet die Eingaben auf ihre Qualität zu prüfen.Die Ergebnisse der Versuche wurden mit den FTE(Failure to Enroll), FTA(Failure to Aquire) und der „User Action Time“ Metriken bewertet. FTE beschreibt die Teilnehmer die nicht in der Lage waren das System zu nutzen, FTA ist der Teil der Teilnehmer die kein Input in der benötigten Qualität liefern konnten und „User Action Time“ die Zeit die Benutzer benötigten, um qualitative Eingaben zu machen. 90% der Benutzer konnten mit wenigen Anweisungen und einer kleinen Einlernzeit qualitative Eingaben machen. Die Systeme die auf Gestenerkennung und Passwörtern beruhten hatten eine längere Eingabezeit als die Systeme mit Gesichts- und Stimmerkennung[TSKMSB12].
Eine Methode, die keine „harten“ biometrischen Eigenschaften wie Fingerabdrücke oder Stimmmuster verwendet, wären die sogenannten Verhaltensbiometrien.
McLoughlin und Naidu untersuchen wie das Tastendruckverhalten eines Menschen als Validierungsmethode auf mobilen Verbrauchergeräten eingesetzt werden kann. Sie kommen zum Schluss dass das Tastendruckverhalten nicht als Hauptauthentifizierung genutzt werden sollte, aber beispielsweise gemeinsam mit einem PIN Code verwendet werden könnte, um für mehr Sicherheit zu sorgen[MN09].
Derawi et al. untersuchen in ihrer Arbeit [DGLBB10] ein System das Fingerabdrücke sowie die Gangart eines Menschen als biometrische Authentifizierungsmethode betrachtet. Die Untersuchung kam zum Schluss, dass eine alleinige Verwendung der Gangart nicht ausreichend ist aber verwendet werden könnte um eine andere Authentifizierung, wie den Fingerabdruckscan, zu stärken.
Sui et al. beschreiben ein biometrisches System bei dem nicht die biometrischen Eigenschaften *direkt* verwendet werden, sondern die Unterschiede zwischen den Biometrieinformationen der zu authentifizierenden Person und den Biometrieinformationen einer sogenannten Referenzperson berechnet werden und zur Authentifizierung dienen. Dies sorgt dafür, dass die Biometrieinformationen einer Person nicht direkt gespeichert werden, was die Privatsphäre schützt[SZD11].
Einen sehr interessanten Ansatz verfolgen auch Klonovs et al. Sie testen ein System das ein Token, Gesichtserkennung und Gehirnwellen nutzt um einen Benutzer zu authentifizieren. Dabei wird zuerst ein Token verwendet, um den Vorgang zu starten und dem System mitzuteilen welcher Benutzer anwesend ist. Da der EEG Scan nur durchgeführt werden kann wenn ein Benutzer das ist und dieser relativ stillsteht, wird dies durch eine Gesichtserkennung geprüft. Der Bewegungssensor stellt sicher dass der Benutzer stillsteht. Anschließend wird dem Benutzer ein Bild angezeigt, und über ein EEG Headset das Muster des Benutzers gelesen. Stimmt dies mit dem gespeicherten Muster überein, wird er authentifiziert. Das gespeicherte Muster wurde zuvor, als der Benutzer in einer entspannten Lage war, aufgenommen und gespeichert. Als Probleme merkten Klonovs et al. an, dass das Befestigen des Headsets, beson-

ders für Personen mit vielen Haaren, relativ umständlich war und in diesem Bereich weiter geforscht werden müsse. Da das Referenzmuster des Benutzers in einer entspannten Lage aufgenommen wurde, ist es für einen Angreifer schwieriger, das System zu täuschen, weil dieser normalerweise gestresst sein wird.

2.2.6 Merkfähigkeit

Merkfähigkeit wird in unterschiedlichen Bereichen erforscht. Alt et al. untersuchen in ihrer Arbeit [ASGS13], ob interaktive Public Displays einen Effekt auf die Merkfähigkeit haben. Ihre Ergebnisse deuten an, dass Interaktion die allgemeine Merkfähigkeit verbessert. Yan et al, führten eine Studie durch in der sie den Teilnehmern verschiedene Ratschläge zur Passwortwahl gaben[YBAG04]. Es wurden drei Gruppen gebildet. Die erste Gruppe erhielt traditionelle Ratschläge wie „mindestens sieben Zeichen und ein Zeichen das kein Buchstabe ist. Gruppe zwei bekam ein Papier auf dem die Buchstaben A bis Z und die Ziffern 1 bis 9 wiederholt aufgedruckt waren. Die Teilnehmer sollten die Augen schließen und zufällig acht Zeichen wählen. Diese sollten sie sich aufschreiben und versuchen zu merken. Die dritte Gruppe sollte sich sogenannte *Passphrases* als Passwort merken. Diese bestehen aus den ersten oder letzten Buchstaben der Wörter eines Satzes, den man sich merken muss. Die Ergebnisse bestätigten, dass es für Benutzer schwierig ist sich an zufällige Passwörter zu erinnern und dass Passwörter die aus Sätzen gebildet werden, schwieriger zu erraten sind. Es wurde auch herausgefunden dass zufällige Passwörter nicht besser sind als Passwörter die aus Sätzen gebildet worden sind. Außerdem wurde gezeigt dass es nicht schwieriger ist sich an Passwörter aus Sätzen zu erinnern als an Passwörter die naiv gewählt wurden.
Forget und Biddle entwickelten ein System, dass die Passwörter von Benutzern um zwei zufällige Zeichen erweitert. Es wurde festgestellt, dass die Merkfähigkeit des Passworts abnahm, falls das ursprüngliche Passwort schon sicher war. Dies konnte folgendermaßen erklärt werden. Miller hat in seiner Arbeit beschrieben dass ein Mensch sich ungefähr sieben sogenannte „Chunks“ merken kann[M56]. Chunks sind Informationsstücke die ein Mensch semantisch zusammenfasst und sich so als eine Einheit merken kann. Beispiele wären Postleitzahlen wie 70569, oder Vorwahlen wie 0711. Sichere Passwörter enthalten schon eine größere Anzahl an Informationsstücken als unsichere Passwörter. Durch das Einfügen von zwei extra Zeichen wird die Anzahl der Informationsstücke erhöht und erschwert bei sicheren Passwörtern die Merkfähigkeit. Passwörter die aus wenigen solchen Stücken bestehen wie beispielsweise einfache Wörter aus dem Wörterbuch, werden durch Hinzufügen von Chunks sicherer und sind trotzdem noch merkbar.

3. Konzept

Wie in der Einleitung kurz beschrieben wurde, handelt diese Diplomarbeit von Authentifizierung auf mobilen Geräten. Viele Authentifizierungsverfahren verwenden eine Art Passwort das aus alphanumerischen Zeichen besteht. Bei diesen Passwörtern besteht ein Konflikt zwischen Sicherheit und Merkfähigkeit. Umso komplizierter und sicherer ein Passwort ist, umso schlechter kann man es sich merken. Um diese Probleme von Authentifizierungssystemen zu lösen, sollte in dieser Arbeit ein etwas anderer Ansatz untersucht werden. Es sollte eine Methode der Authentifizierung verwendet werden die aus dem persönlichen Kontext eines Benutzers Fragen generiert und diese Fragen an die Person stellt, die sich versucht zu authentifizieren. Anhand der richtigen oder falschen Antworten soll der Benutzer erkannt werden.
Als Erstes wird das Authentifizierungsverfahren betrachtet. Es gib drei Klassen von Authentifizierungsverfahren, „Etwas das man weiß“, „Etwas das man hat“ und „Etwas das man ist“. Das Paradigma „Etwas das man weiß“ beschreibt alle Verfahren die eine Art Passwort zur Authentifizierung verwenden. Als Beispiel wurden in Kapitel zwei das Login Passwort bei den meisten Betriebssystemen für den PC genannt. Bei „Etwas das man hat“ wird ein sogenanntes „Token“, also ein Gegenstand den man besitzt, zur Authentifizierung verwendet. Ein gutes Beispiel war hier die Bankkarte, welche man benötigt um am Bankautomaten Geld abzuheben. „Etwas das man ist“ beschreibt Verfahren die biometrische Eigenschaften einer Person verwenden, wie beispielsweise Fingerabdrücke. Diese Arbeit untersucht Fragen um den Benutzer zu authentifizieren. Dabei wird kontrolliert ob er die richtigen Antworten kennt. Das heißt das System basiert auf Dingen die man weiß und gehört damit zur ersten Kategorie. Die Wahl des Authentifizierungsklasse ergab sich direkt aus der Aufgabenbeschreibung der Diplomarbeit.
Es gibt verschiedene Arten sich auf einem Smartphone zu authentifizieren. Die üblichen verwenden eine Art Passwort zu Authentifizierung des Benutzers. Eine Ausnahme bildet das von Bojinov und Boneh beschriebene System welches ein Hardwaretoken zum Entsperren des Smartphones verwendet [BB11].
Auf einem Android Smartphone (Samung Galaxy Nexus S) gibt es fünf Möglichkeiten das Gerät zu Entsperren. Die Option „Keine“ deaktiviert die Bildschirmsperre. Die Option „Finger bewegen“ lässt den Bildschirm durch eine Wischbewegung entsperren. Es gibt die Möglichkeit einen PIN Code zu verwenden. Auch ist es möglich ein alphanumerisches Passwort zu setzen. Die letzte Authentifizierungsmethode beruht nicht darauf, dass der Benutzer sich eine Folge von Zeichen merken muss. Hier muss der Benutzer mit dem Finger ein Muster auf dem Bildschirm zeichnen, das bis zu neun vorgegebene Punkte miteinander verbindet.
Um Fragen über den Kontext zu stellen, müssen Daten gesammelt werden. Dazu sollten Sensoren (Kamera oder GPS Adapter) die auf mobilen Geräten verfügbar sind verwendet werden. Die Daten sollen über einen längeren Zeitraum gesammelt wer-

den um sicherzustellen dass genügend Daten vorhanden sind, um verschiedene Fragen zu stellen. Wenn zu wenig Daten vorhanden sind, erhöht sich die Wahrscheinlichkeit dass sich die selben Fragen wiederholen. Dies könnte dazu führen, dass eine Unbefugte Person durch „Shoulder Surfing“ an das Passwort kommt.

Anschließend werden die gesammelten Daten analysiert um Fragen zu den gesammelten Daten zu generieren. Diese werden dann dem Benutzer gestellt. Es soll herausgefunden werden, wie gut ein solches Authentifizierungssystem funktioniert. Dazu sollten eine Reihe von Kennzahlen ermittelt werden, anhand derer das System bewertet wird.

Der persönlicher Kontext sind Dinge die vom Benutzer abhängig sind und die über die Daten, die mithilfe des Smartphones gesammelt werden, ermittelt werden können. Dazu zählen beispielsweise Standortdaten, die aus GPS Daten des Smartphones ermittelt werden können, und Konversationsgewohnheiten, die aus den Anruflisten und den SMS Daten ermittelt werden können. Dinge wie Lieblingsbiersorte oder Lieblingsfarbe gehören hier nicht zum Kontext, da es keine Sensoren gibt aus deren Daten diese Informationen ermittelt werden können.

Ein wichtiger Punkt ist die Wahl der Daten, die gesammelt werden sollen, und die Sensoren, die diese Daten produzieren. Auf einem mobilen Gerät häufen sich im Laufe der Zeit viele verschiedene Arten von Daten an. Durch führen von Telefonaten füllt sich die Anrufliste mit Gesprächsdaten wie Gesprächspartner, Gesprächszeit, Gesprächsdauer und ob das Gespräch ein einkommender Anruf oder eine selbst initiiertes Gespräch war. Es werden Informationen über SMS gespeichert, dazu gehören Sender, Datum und Länge der Nachricht. Da die meisten mobilen Geräte wie Smartphones und Tablets eine Kamera besitzen, sammeln sich auch Bilder und Videos auf dem Gerät an. Sensoren wie Beschleunigungsmesser, Gyroskop und Magnetometer produzieren ständig Daten die gespeichert werden können. Über den GPS Empfänger kann eine Standortlokalisierung durchgeführt werden welche wiederum Daten wie Breitengrad und Längengrad liefert.

Verschiedene Arten von Daten sind unterschiedlich direkt für Fragen zu verwenden. Daten wie Bilder oder Anruflisten benötigen fast keine Bearbeitung um daraus Fragen abzuleiten. Man kann den Benutzer direkt fragen mit wem er telefoniert hat oder was auf einem Bild zu sehen ist. Daten wie Breitengrad und Längengrad müssen erst in ein Form gebracht werden, die für den Benutzer verständlich ist. Dies könnte eine Adresse oder der Name eines bekannten Bauwerks (beispielsweise der Eiffel Turm) sein. Erst jetzt kann man eine Frage wie „Was ist an dieser Adresse“ stellen. Außerdem können diese Daten mit anderen Informationen, wie zum Beispiel einem Datum, kombiniert werden um Fragen wie „Wann waren sie zuletzt am Eiffelturm“ zu stellen.

Daten die von Sensoren wie Gyroskop oder Beschleunigungsmesser kommen sind am indirektesten für Fragen zu gebrauchen. Es benötigt etwas mehr Aufwand um aus Beschleunigungsdaten eine Frage wie beispielsweise „Wann haben sie sich zuletzt mit mehr als 50 km/h bewegt“ zu erstellen.

Bei der Wahl der Daten muss man sich immer fragen, ob und was für Fragen zu den

gesammelten Daten gestellt werden können. Daten die vom Sensor „Kamera“ gesammelt werden sind Bilder und Videos. Dazu könnte man zum Beispiel fragen, wo ein Bild aufgenommen wurde oder wer darauf zu sehen ist.
Interessant ist auch die Rate mit der die Sensoren Daten erzeugen. Sensoren die sehr viele Daten erzeugen, könnten eventuell massiv den Speicher des Gerätes belasten, und bei sehr häufigem Zugriff auf den Speicher das Gerät verlangsamen.
Bei der Wahl der Daten die gesammelt werden sollen, muss auch beachtet werden, wie persönlich diese sind. Viele Menschen möchten persönliche Daten nicht oder nur sehr ungern preisgeben. Daten wie Standortinformationen, oder Anruflisten sind sehr persönlich, da man daraus ableiten kann, wo die Person war und mit wem sie wie häufig Kontakt hatte. Um Menschen dazu zu bewegen, eine Anwendung die ihre Daten aufzeichnet trotzdem zu verwenden, muss man sie überzeugen, dass die Vorteile der Anwendung die Nachteile, die durch das Preisgeben von persönlichen Daten entstehen, überwiegen. Ein Argument, das man anbringen kann, ist die Tatsache, dass keine persönlichen Daten das Smartphone verlassen. Die Fragen werden mithilfe einer Anwendung gestellt, welche auf dem Smartphone ausgeführt wird. Die Ergebnisse der Befragung, sagen nur aus, welche Fragen korrekt beantwortet worden sind. Wer die Fragen beantwortet hat ist nicht ersichtlich.
Die Fragen die den Benutzern gestellt werden, verwenden Daten die auf dem Smartphone gesammelt wurden. Dabei besteht eine Frage aus einem statischen Teil und einem dynamischen Teil. Der statische Teil bestimmt die Art der Frage. Wird eine Frage bezüglich einem Bild gefragt? Oder nach einem getätigten Anruf? Der dynamische Teil wählt beispielsweise ein bestimmtes Bild oder einen bestimmten getätigten Anruf und integriert ihn in die Frage (Wer ist auf dem Bild zu sehen? Wann haben sie Person X zuletzt angerufen?).
Der Unterschied zu alphanumerischen Passwörtern ist, dass man sich bei dieser Methode nichts „merken“ muss im herkömmlichen Sinne. Fragen die zum persönlichen Kontext gebildet werden beschreiben Dinge aus dem alltäglichen Leben, an die man sich „erinnern“ muss, die man sich aber nicht explizit „merkt“. Ein Passwort für ein Email-Konto wird man solange still aufsagen, bis man es sich einigermaßen gemerkt hat. Durch wiederholtes Anwenden wird die Information fester im Gedächtnis verankert. Eine Information wie „Mit wem habe ich zuletzt telefoniert?“ wird man üblicherweise nicht solange im Stillen wiederholen bis man es sich gemerkt hat.
Ein Benutzer der ein Kontext basiertes Authentifizierungssystem verwendet, wird aber voraussichtlich nach einer Weile wissen welche Art von Fragen existieren. Das könnte dazu führen dass er sich Dinge „merkt“ die als Teil einer Frage verwendet werden können. Er könnte sich beispielsweise die Orte die er an einem Tag besucht hat, mit Uhrzeiten verknüpfen und versuchen sich diese wie ein Passwort zu merken. Der Unterschied zu üblichen Passwörtern der aber immer noch bestehen bleibt, ist die Tatsache, dass sich das Passwort ständig ändert.
Wenn möglich soll die Überprüfung der Antworten auf Korrektheit automatisiert erfolgen. Bei einer Frage die nach einem Zeitpunkt verlangt,soll, mithilfe der Informationen, die auf dem Smartphone geloggt wurden, ermittelt werden, ob die Antwort

des Benutzers korrekt ist. Dabei kann eine Toleranz gewährt werden, damit der Benutzer nicht auf die Minute genau antworten muss. Bei Fragen die nach dem Multiple Choice Prinzip eine Antwort verlangen, ist eine Toleranz natürlich nicht so einfach realisierbar. Die Auswertung der Fragen ist aber nicht immer automatisiert möglich. Einige Fragen erlauben als Antwort Freitext, welcher jedoch schwierig automatisch überprüfbar ist. Eine Frage wie beispielsweise „Wo wurde dieses Foto aufgenommen?“ kann mit „Daheim“ „Zuhause“, „auf der Arbeit“ etc. beantwortet werden. Das System kann nicht die GPS Koordinaten , die in die Bilder eingebettet sind automatisch eine Eingabe wie „zuhause“ zuordnen. In diesen Fällen müssten die Informationen von Hand mit den Eingaben des Benutzers verglichen werden.
Um dieses Konzept auf Tauglichkeit bezüglich Merkfähigkeit und Sicherheit zu überprüfen, soll eine Studie durchgeführt werden. Hierfür soll eine Anwendung für das Betriebssystem Android entwickelt werden, die auf den Smartphones von einer gewissen Anzahl von Teilnehmern installiert wird. Nach der Installation zeichnet die Anwendung eine Reihe von Daten auf. Nach zehn bis vierzehn Tagen wird der Teilnehmer zu eine Befragung eingeladen. Eine weitere Anwendung wird auf dem Smartphone der Teilnehmer installiert. Diese soll die auf dem Smartphone aufgezeichneten Daten verwenden um dem Teilnehmer dazu Fragen zu stellen.
Einige Ideen die während der Entwicklung des Konzeptes aufkamen, wurden im weiteren Verlauf der Arbeit verworfen. Dazu zählt auch das Mitzeichnen der Inhalte von SMS. Die Inhalte von SMS Nachrichten würden eine interessante Informationsquelle für Kontextfragen liefern. Man könnte den Benutzer Teile einer SMS Nachricht präsentieren und ihn nach dem Absender fragen. Ein Problem das hier auftauchen könnte, wäre die Tatsache, dass viele Menschen ihren Namen in die gesendete Nachricht schreiben. Das heißt man dürfte nicht die ganze Nachricht anzeigen, sondern müsste längere Nachrichten wählen und hiervon Teile anzeigen. Leider haben viele Smartphone Benutzer eine SMS Flat in ihrem Mobilfunkvertrag, und senden daher auch öfters sehr kurze Nachrichten. Die Tatsache, dass SMS Gespräche in Android wie ein Chatgespräch angezeigt wird, unterstützt diese Entwicklung nur noch.
Auch wurde überlegt geführte Gespräche in Teilen aufzuzeichnen. Anschließend könnte nach dem Gesprächspartner und/oder dem Thema des Gesprächs gefragt werden. Das Aufzeichnen von SMS Inhalten und Gesprächen wurde aber aufgrund Datenschutzbedenken verworfen.

4. Implementierung

4.1. Architektur

Die Implementierung besteht aus zwei Teilen. Der erste Teil ist eine Anwendung die Daten auf dem Smartphone aufzeichnet. Der zweite Teil ist eine Anwendung die dem Benutzer Fragen zu den aufgezeichneten Daten stellt, und deren Antworten speichert.

4.1.1 Logging

Dies ist der erste Teil der Implementierung. Er besteht lediglich aus drei Klassen.
Eine Klasse die eine *Activity* implementiert, einer Klasse die einen Service implementiert und eine Klasse die einen *BroadcastReceiver* implementiert (siehe Abbildung 3). Die *Activity* soll lediglich dazu dienen den Service zu starten. Dieser übernimmt dann das eigentliche Aufzeichnen der Daten. Ein Implementierung der *BroadcastReceiver* Klasse sorgt dafür dass die Anwendung sich bei einem Neustart des Betriebssystems automatisch neu startet. Im Folgenden werden diese drei Klassen näher erläutert.

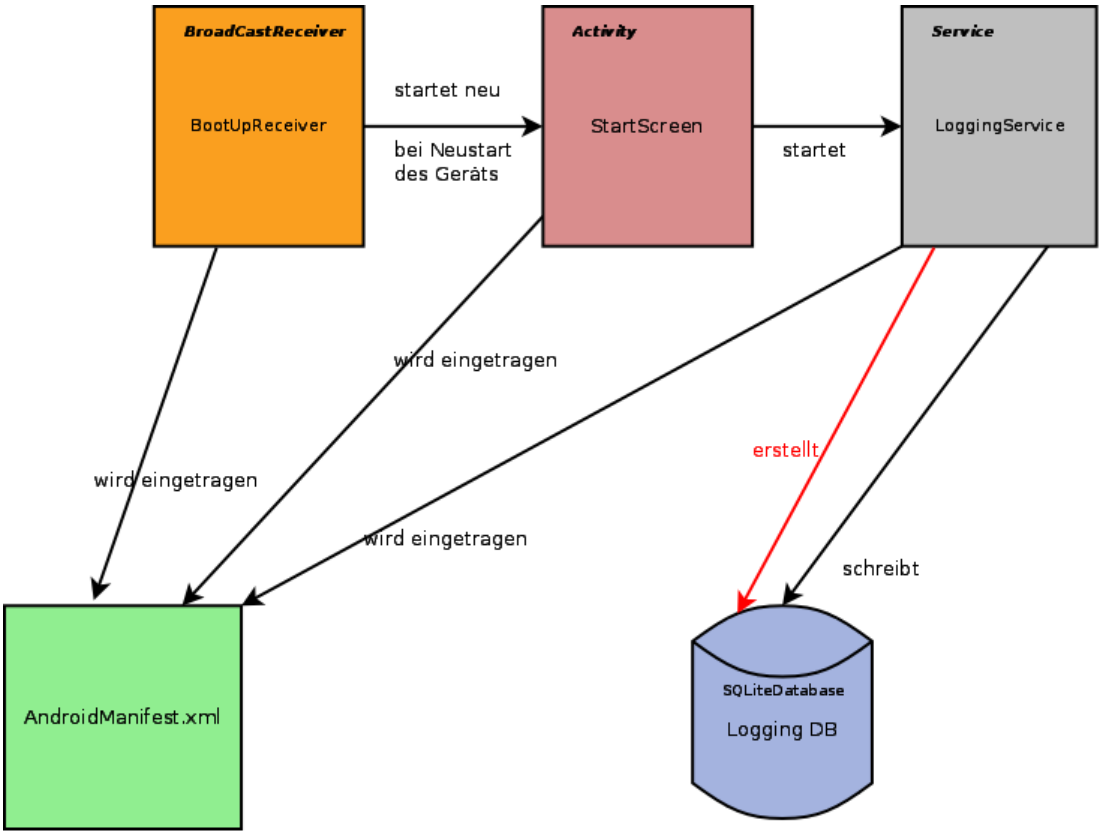

Abbildung 3: Architektur der Logging Anwendung

4.1.1.1 StartScreen Klasse

Die *Start Screen* Klasse ist eine Implementierung der *Activity* Klasse von Android. Sie besitzt als UI lediglich einen Knopf. Um den Knopf eine Funktion zu geben, wurde ein *onClickListener* implementiert. Dieser hat die Aufgabe die *LoggingService* Klasse zu instanziieren und zu starten. Beim Start der Anwendung wird geprüft ob GPS aktiviert ist. Im Falle dass GPS nicht aktiviert ist, wird der Benutzer mithilfe einer Nachricht darauf hingewiesen und es werden automatisch die Systemeinstellungen von Android geöffnet. Durch Verlassen der Systemeinstellungen kommt der Benutzer zurück zum *StartScreen*. Nach dem Drücken des einzigen Knopfes verschwindet die *Activity* und der Service läuft im Hintergrund.

BootUpReceiver Klasse

Die *BootUpReceiver* Klasse implementiert die *BroadCastReceiver* Klasse von Android. Diese Klasse soll dafür zu sorgen, dass die Logging Anwendung bei einem Neustart des Gerätes sofort gestartet wird. Nachdem der Benutzer sein Gerät eingeschaltet und seinen PIN Code eingegeben hat, startet die Anwendung wie üblich mit der *StartScreen Activity*. Der Benutzer muss nur noch den Start Knopf betätigen und der LoggingService wird wieder ausgeführt.

LoggingService Klasse

In der Klasse *LoggingService* geschieht der größte Teil der von der Logging Anwendung durchgeführten Aktionen. Sie implementiert den von der *StartScreen Activity* gestarteten Service und dient dazu, einmal pro Tag die Anruflisten und Informationen über erhaltene SMS zu loggen. Außerdem soll jede Minute ein Scan nach kabellosen Netzen durchgeführt und die Ergebnisse gespeichert werden. Die vom Wifi Adapter konfigurierten kabellosen Netze sollen ebenfalls geloggt werden. Und schließlich soll der aktuelle Standort in Form von geographischem Breitengrad und geographischem Längengrad gespeichert werden.
Die erste Version der Implementierung der Logging Anwendung verwendete mehrere separate Implementierungen der Service Klasse um die verschiedenen Daten, die geloggt werden sollten, aufzuzeichnen. Daten die einmal pro Tag geloggt werden sollten, also Anruflisten und SMS Informationen, wurden in einem Service behandelt, und Daten die einmal pro Minute aufgezeichnet werden sollten, in einem anderen Service. Dies führte jedoch zu dem Problem dass zwei Services gleichzeitig auf dieselbe SQLite Datenbank zugriffen und es zu einem Absturz des Programms kam. Um dieses Problem zu lösen, wurden beide Service Implementierungen später in einer Klasse zusammengefasst. Die *LoggingService* Klasse kann in drei Bereiche gegliedert werden. Dies sind die Initialisierung, das Aufzeichnen der Daten und die Hilfsfunktionen.

Zunächst wird der Initialisierungsteil abgearbeitet. Damit Daten geloggt werden können muss eine Datenbank erstellt werden. Dazu müssen die Tabellen, die angelegt

werden sollen, definiert werden, Dies geschieht in Form von einigen String Konstanten. Diese Konstanten bestimmen die Tabellennamen und die Spaltennamen der einzelnen Spalten der Tabellen.
Der LifeCyle eines Services beginnt mit der Methode *onCreate*. Diese wird bei der Generierung des Services vom System aufgerufen. Diese Methode wird nur einmal zu Beginn aufgerufen, deshalb eignet sie sich für Programmierschritte, die nur einmal ausgeführt werden sollen. In diesem Fall soll die Klasse *NotificationManager* instanziiert werden. Dieses wird dazu verwendet um Benachrichtigungen an das System zu senden. Anschließend wird die erste Benachrichtigung erstellt. Diese ist eine Instanz der *Notification* Klasse. Die Benachrichtigungen erinnern den Benutzer des Smartphones daran, das der Logging Service läuft.
Als nächstes wird die Methode *onStartCommand* betrachtet. Zu Beginn wird eine Datei angelegt die einige von der Logging Anwendung benötigten Daten speichert. Dazu wir über den Context der *LoggingService* Klasse kann mit der Methode *getSharedPreferences* durch die Übergabe eines Dateinamens ein *SharedPreference* Objekt generiert. Diese wird im weiteren Verlauf der *doLogging* Methode verwendet. Anschließend wird die Methode *startForeground* der *Service* Klasse aufgerufen. Diese soll dem Betriebssystem sagen, dass der Service im Vordergrund läuft und nicht beendet werden soll. Die Methode *startForeground* erhält zwei Parameter. Der Erste ist eine eindeutige id, welche später dazu benutzt wird um weitere Benachrichtigungen zu senden. Der zweite Parameter ist ein *Notification* Objekt. In diesem Fall wird die Notification, die zuvor generiert wurde, an *startForeground* übergeben und diese wird dann zusammen mit den anderen Benachrichtigungen von Android (GPS Zustand etc...) in der oberen Leiste angezeigt solange der Service läuft. (siehe Abbildung 4)

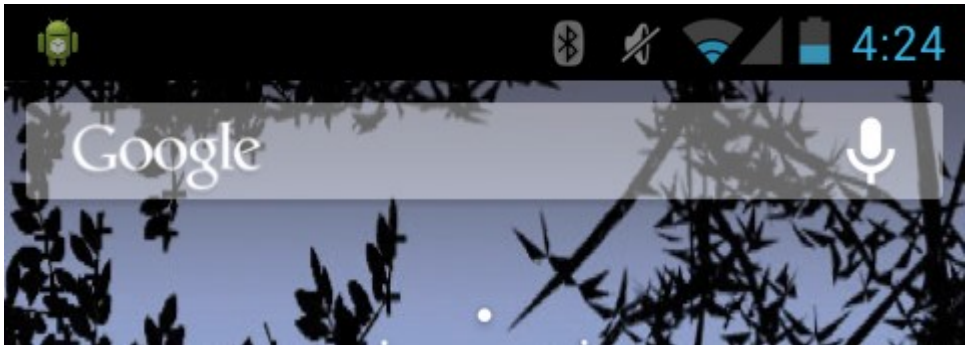

Abbildung 4: Das Android Symbol repräsentiert den laufenden LoggingService.

Im nächsten Schritt wird eine Datei mit dem Namen „Logging.db“ auf dem externen Speicher erstellt. Der externen Speicher kann entweder eine SD Karte im Smartphone oder ein Teil des im Gerät verbauten Speichers sein. Der externe Speicher wurde gewählt, weil sich dadurch der Zugriff auf die Datenbank auch von anderen Anwendungen als einfach erwiesen hat.

Die Datenbank wird durch ein *SQLiteDatabase* Objekt repräsentiert. Mithilfe einer Instanz dieser Klasse wird über die Funktion *openOrCreateDatabase* eine neue SQLite Datenbank angelegt, oder eine bestehende geöffnet. Die Datenbank wird in die zuvor erstellte Datei geschrieben.
Um die Tabellen für alle zu loggenden Daten zu erstellen, wurden drei Strings verwendet, die klassische SQL „Create table“ Befehle darstellen, und über die Methode *execSQL* des *SQLiteDatabase* Objektes an die Datenbank gesendet wurden. Bevor die Tabellen erstellt werden, wird aber zuerst mit der Methode *tableExists* geprüft ob die Tabelle schon existiert. Anschließend werden, wenn nötig, die Tabellen erstellt.
Da im weiteren Verlauf Informationen über Wifi Netzwerke gespeichert werden sollen, wird nun ein ein *WifiManager* Objekt vom System angefordert. Dieses Objekt wird später verwendet um nach verfügbaren Wifi Netzen zu suchen.
Als nächstes wird ein *Timer* Objekt erstellt. Ein *Timer* führt seinen Code in einem eigenen Thread aus. Um Code auszuführen muss ein *TimerTask* Objekt erstellt werden. Dessen *run* Methode beinhaltet den eigentlichen Code. Dieser *Timer* soll regelmäßig die Methode *doLogging* aufrufen, welche für das eigentliche Aufzeichnen der Daten zuständig ist. Ebenso in der *run* Methode wird eine *Notification* erstellt, und über die Methode *notify* des *NotificationManagers* gesendet. Die Methode *notify* enthält genauso wie *startForeground* eine id und eine *Notification* als Parameter. Durch das Verwenden derselben id wie zuvor in *startForeground* ist es möglich die angezeigte Benachrichtigung zu aktualisieren.
Der nächste Schritt ist die Erstellung eines *LocationListener* Objekts. Dieses ist nötig um regelmäßig aktuelle Standpunktinformation zu erhalten. Der *LocationListener* enthält vier Methoden, von denen die *onLocationChanged* Methode am interessantesten ist. Diese wird aufgerufen wenn sich der Standpunkt um einen bestimmten Wert ändert. Dies wird später mithilfe eines *LocationManager* Objekts erreicht. Der Grund dafür dass zuerst der *LocationListener* definiert wird ist, dass der *LocationManager* einen *LocationListener* als Parameter benötigt um Standortaktualisierungen anzufordern. Nachdem der *LocationListener* erstellt worden ist, wird ein *LocationManage*r Objekt angelegt und ein Verweis auf den „Location Service“ vom System angefordert. Die Methode *requestLocationUpdates* des *LocationManagers* bestimmt nun, wie oft und in welchem räumlichen Abstand Standortaktualisierungen angefordert werden sollen. In diesem Fall wird alle 60 Sekunden und bei einer Entfernung von 3 Metern, eine Aktualisierung der Standortinformationen angefordert. Die Methode *schedule* des zuvor definierten *Timer* Objekts wird aufgerufen um den *Timer* zu starten. Als Parameter wird der *TimerTask* der ausgeführt werden soll, die Zeit nach dem der *Timer* zum ersten Mal ausgeführt werden soll, und die zeitlichen Abstände der Ausführungen übergeben. Der Service gibt als letzte Aktion die Konstante „START_STICKY“ zurück an das System. Das soll dem System mitteilen, dass dieser Service wieder gestartet werden soll falls er vom System beendet wurde.

Der Logging Teil der Implementierung wird in der Methode *doLogging* durchgeführt. Zunächst wird eine Instanz der Klasse *SimpleDateFormat* erstellt. Dieses Ob-

jekt dient der späteren Formatierung des Datums. Das Format entspricht der Form (hh:mm dd:MM:YYY).
In den nächsten zwei Abschnitten der *doLogging* Methode werden Anruflisten und SMS aufgezeichnet. Damit dies nur ein mal am Tag geschieht, wird zuerst die *SharedPreferences* Datei ausgelesen. Es wird nach dem Eintrag „LastDailyLogInMillis“ gesucht. Dieser Wert repräsentiert eine Datumsangabe in Millisekunden. Dieser Wert wird vom aktuellen Datum abgezogen und es wird geprüft ob der Differenzwert mehr als einen Tag ergibt. Ist dies der Fall, sollen die Anruflisten und die SMS Informationen aufgezeichnet werden. Beim ersten ausführen der *doLogging* Methode ist noch kein Eintrag in den *SharedPreferences* vorhanden. Deshalb wird der Wert 0 zurückgegeben. Nachdem der Wert 0 vom aktuellen Datum abgezogen wird, wird geprüft ob der Wert mehr als ein Tag in Millisekunden ergibt. Beim ersten Mal ist dies immer der Fall, also wird der Teil, der die Anruflisten und die SMS aufzeichnet, ausgeführt.
Im nächsten Abschnitt werden die Anruflisten des Benutzers geloggt. Dazu wird zunächst wird ein *ContentResolver* Objekt erstellt. Dieses dient dazu einen ContentProvider anzusprechen. Content Provider ermöglichen den Zugriff auf Daten, die wie in Tabellen einer relationalen Datenbank angeordnet sind. In diesem Fall sind es Daten über die getätigten Anrufe des Benutzers. Ein String Array enthält die Spalten der konkreten Tabelle aus der Informationen gewonnen werden sollen. Nachdem die gewünschten Zeilen im Array gespeichert wurden, wird mithilfe des der Methode *query* des *ContentResolvers* eine Anfrage an den Provider geschickt. Die Anfrage enthält als Parameter unter anderem die Uri des Content Providers und das String Array das die gewünschten Spalten definiert. Das Ergebnis der Anfrage ist ein C*ursor* Objekt, welches eine Art Tabelle mit den gewünschten Spalten darstellt. Der *Cursor* kann jetzt mit einer for Schleife durchsucht werden. Die Informationen aus jeder Zeile werden in verschiedenen Variablen abgelegt.
Auf ähnliche Art und Weise werden Informationen über SMS extrahiert. Dazu wird wieder eine Anfrage an einen Content Provider gesendet, welches als Antwort ein *Cursor* Objekt zurückgibt. Auch hier werden die gewünschten Daten in Variablen gespeichert. Nachdem die Informationen extrahiert worden sind, wird für jeden Informationsset (Daten einer SMS, Daten eines Anrufs) jeweils eine Methode aufgerufen. Die Methode *addCallLogData* fügt Informationen über einen Eintrag der Anrufliste in die Datenbank. Die Methode *addSmsData* fügt analog dazu Informationen über gespeicherte SMS in die Datenbank. Zum Schluss wird das aktuelle Datum in Millisekunden umgewandelt und in die *SharedPreferences* geschrieben. Dadurch wird sichergestellt dass das nächste Aufzeichnen der Anruflisten und SMS Daten nicht mehr innerhalb der nächsten 24 Stunden geschieht.
Bevor nun als nächstes GPS und Wifi Informationen geloggt werden können, wird der Zustand des Wifi Adapters ermittelt und gespeichert. Die möglichen Zustände für Wifi sind „enabled“, „enabling“, „disabled“, „disabling“ und „unknown“. Der Zustand wird später benötigt um nach einem Wifi Scan den ursprünglichen Zustand herzustellen. Als nächstes wird der Zustand des Wifi Adapters geprüft. Falls er einen der Zustände „disabling“ „disabled“ oder „unknown“ entspricht, wird der Wifi-Adapter

nun aktiviert, um einen Scan durchführen zu können. Eine boolsche Variable merkt sich ob der Wifi Adapter aktiviert oder deaktiviert war.
Die folgenden Zeilen enthalten zwei while Schleifen. Die erste Schleife läuft, solange der Zustand des Wifi-Adapters nicht auf „enabled“ gesetzt wurde. Ohne diese Schleife könnte versucht werden, einen Scan durchzuführen, bevor Wifi aktiviert worden ist. Der Nachteil ist natürlich das wenn der Zustand des Wifi Adapters niemals auf „enabled“ gesetzt wird weil der Adapter vielleicht defekt ist, die Ausführung in eine Endlosschleife gerät. Als nächstes wird ein Wifi Scan durchgeführt. Dazu wird die Methode *scan* des zuvor generierten *WifiManager* Objekts verwendet. Die zweite der vorhin erwähnten while Schleifen wartet auf die Ergebnisse der Scans. Anschließend werden die Ergebnisse in einer Liste gespeichert. Es wird ermittelt ,ob und mit welchem Wifi Netz das Gerät verbunden ist. Nun wird die letzte bekannte Position angefordert. Davor wird geprüft ob schon eine Position bekannt ist.
In den nächsten zwei Abschnitte werden die gescannten Wifi Netzwerke und die vom Wifi Adapter konfigurierten Wifi Netzwerke in die Datenbank eingefügt. Dazu wird die Methode *addData* verwendet.
Der letzte Teil der *LoggingService* Klasse besteht aus den Hilfsfunktionen. Diese sind die Methoden *addCallLogData, addSmsData* und *addData*. Die Methode *addCallLogData* wird verwendet um Daten über Anrufe in der Datenbank abzulegen. Dazu wird ein Objekt der *ContentValue* Klasse erstellt. In dieses Objekt werden Paare von Spalten und Werten geschrieben. Die Werte werden der Methode beim Aufruf als Parameter übergeben. Die Spalten sind die Spaltennamen der Tabelle, in die Werte eingefügt werden sollen. In diesem Fall ist es die Tabelle „TABLE_CALL_LOGS“ Über die *insert* Methode der *SQLiteDatabase* Instanz wird das *ContentValue* Objekt in die Datenbank eingefügt. Dadurch wird in der Tabelle ein neuer Eintrag erzeugt, welcher in den einzelnen Spalten die gewünschten Werte enthält. Die Methoden *addSmsData* und *addData* funktionieren auf die selbe Art und Weise, der einzige Unterschied ist die Tabelle, in die geschrieben wird.

SQLite Datenbank

Um die gewünschten Informationen aufzuzeichnen, wurde eine SQLite Datenbank erstellt. Diese enthält die drei Tabellen, deren Namen zu Beginn der *LoggingService* Klasse definiert wurden. Die Tabellen sind „call_logs“, „sms_data“ und „every_minute_logging_table“ Im folgenden werden diese Tabellen näher erläutert. Die Tabelle „call_logs“ speichert Informationen über geführte Gespräche.
Sie enthält folgende Spalten:

- id (INTEGER), dies ist der Primärschlüssel der Tabelle
- cached_name (TEXT), der Name des Gesprächskontakts falls vorhanden
- call_log_date (INTEGER), Gesprächsdatum als Zahl der Millisekunden seit dem 1. Januar 1970
- call_duration (INTEGER), Dauer des Gesprächs
- entry_acknowledged (TEXT), ob ein Anruf gesehen wurde
- phone_number (TEXT), Nummer des Gesprächspartners

- call_type (TEXT), Art des Anrufs entweder incoming, outcoming oder missed

Daten über gespeicherte SMS werden in der Tabelle „sms_data“ abgelegt.

Diese Tabelle beinhaltet die folgenden Spalte:

- id (INTEGER), dies ist der Primärschlüssel der Tabelle
- sender(TEXT), Name oder Nummer des Absenders (hängt davon ab ob der Sender als Kontakt gespeichert wurde)
- received_date(INTEGER), Empfangsdatum der SMS in Millisekunden (siehe oben)
- send_date(INTEGER), Sendedatum einer SMS in Millisekunden
- sms_length(INTEGER), Länge einer SMS

Die Tabelle „every_minute_logging_table“ soll die Wifi und GPS Informationen speichern.

Sie besteht aus folgenden Spalten:

- id (INTEGER), dies ist der Primärschlüssel der Tabelle
- date(INTEGER), das Datum in Millisekunden
- date_String(TEXT), das Datum als lesbaren String
- ssid(TEXT), der Name eines Wifi Netzes das in die Datenbank eingetragen wurde.
- avail_or_config(INTEGER), ob das Netzwerk ein konfiguriertes Netzwerk oder ein Netzwerk aus einem Scanergebnis ist
- latitude(REAL), der geographische Breitengrad
- longitude(REAL), der geographische Längengrad
- wifi_state(INTEGER), Der Zustand des Wifi Adapters. Es gibt 4 Zustände, welche mit den Werten 0-3 beschrieben werden.
- connected_wifi(TEXT), SSID des Wifi Netzes mit dem man verbunden ist.

4.1.2 Fragebogen Anwendung

Der zweite Teil der Ausarbeitung ist eine Anwendung, die den Benutzer Fragen zu den im ersten Teil aufgezeichneten Daten stellt. Außerdem werden Fragen zu Bildern, die sich auf dem Smartphone des Benutzers befinden, gestellt.
Abbildung 5 zeigt die Architektur der Fragebogen Anwendung. Sie beginnt mit einer *Activity*. Startend von dieser Klasse kann man alle Teile der Fragebogen Anwendung erreichen. Jeder Teil des Fragebogens(SMS, WIFI, usw...) besteht aus einer oder

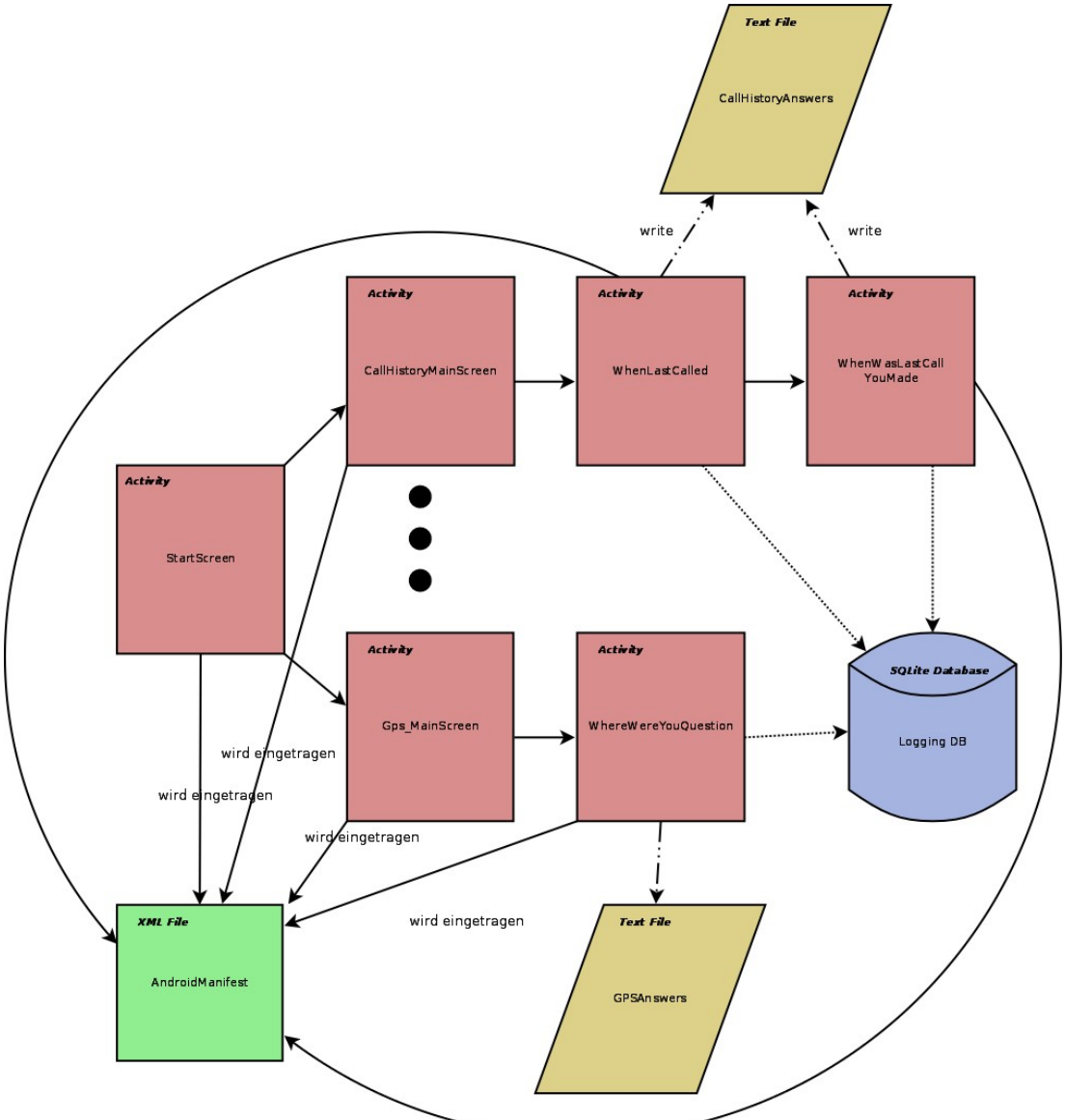

Abbildung 5: Architektur der Fragebogen Anwendung. Es wurden nicht alle Teile des Fragebogens dargestellt, da die Fragen meistens nach dem selben Schema ablaufen.

mehreren *Activities* welche jeweils eine Frage repräsentieren. Diese Fragen können nacheinander erreicht werden, indem der Knopf der aktuellen Frage betätigt wird. Die Ergebnisse der Fragen werden von jeder *Activity* in einer Textdatei abgelegt. Dabei teilen sich *Activites*, die Fragen zu dem selben Gebiet fragen (beispielsweise SMS) eine Textdatei.

Fragen zu CallHistory

Der Teils des Fragebogens, der Fragen zu der Anrufliste des Benutzers stellt, beginnt mit einer *Activity*, welche als eine Art Begrüßungsseite für den Benutzer dient und ihn zu den Fragen weiterleiten soll. Über einen Button mit der Aufschrift „Beginnen“ gelangt man zur ersten Frage. Es existieren acht Fragen zu den Anruflisten. Diese

Fragen können in drei Kategorien angeordnet werden. Die erste Kategorie benutzt im GUI ein oder mehrere Picker Elemente um den Benutzer eine Eingabe zu ermöglichen(siehe Abbildung 6). Die Klassen *WhenLastCalled*, *WhenWasLastCallYouMade*, *WhenDidXLastCall* und *LastTimeYouCalledX* gehören in diese Kategorie. Diese vier Klassen sind alle nach dem selben Schema implementiert. Mithilfe der genannten Picker Elemente wird nach einem bestimmten Zeitpunkt gefragt. Nachdem der Benutzer seine Eingabe getätigt hat wird die korrekte Antwort auf die Frage aus der Datenbank geholt und mit der Eingabe des Benutzers verglichen. Das Ergebnis, also ob die Antwort des Benutzers korrekt war, wird in einer Textdatei abgelegt.
Die konkrete Implementierung geschah folgendermaßen: Zunächst wird eine Instanz der *SQLiteDatabase* Klasse erstellt. Damit erhält man Zugriff auf die Datenbank die von der Logging Anwendung erstellt wurde. Anschließend wird eine SQL Anfrage an die Datenbank geschickt. Es gibt 2 Möglichkeiten eine Anfrage an die Datenbank zu senden. Über die Methode *query* sowie über die Methode *rawQuery.* Die *query* Methode verwendet eine Reihe von Parametern, um den gewünschten Tabellennamen die gewünschten Spaltennamen usw... zu übermitteln. Die *rawQuery* Methode hingegen nimmt als Parameter eine klassische SQL Anfrage der Form SELECT * FROM * WHERE. Programmierer die der SQL Sprache mächtig sind, können so direkt Anfragen an die Datenbank senden. Die Fragen der Picker Kategorie verwenden die *rawQuery* Methode um benötigte Informationen aus der Datenbank zu holen. Bevor die SQL Anfrage erfolgt , muss in den Klassen *WhenDidXLastCall* und *LastTimeYouCalledX* noch ein weiterer Schritt durchgeführt werden. Diese zwei Fragen unterscheiden sich von den anderen beiden insofern als dass sie aus zwei Komponenten bestehen. Genauso wie in den andern beiden Klassen wird nach einem Zeitpunkt in der Vergangenheit gefragt, an dem ein Anruf getätigt wurde. Zusätzlich wird aber auch nach einer Person gefragt mit der dieses Gespräch geführt wurde. Die Person wird zufällig aus der Liste der Kontakte gewählt. Anschließend wird der Name des Kontakts in die Frage integriert. Danach geht es weiter mit der Datenbankanfrage. Nachdem die Abfrage erfolgt ist, werden die Ergebnisse in einem *Cursor* Objekt gespeichert. Im nächsten Schritt wird die Textdatei angelegt, in der die Ergebnisse gespeichert werden sollen. Dabei verwendet jede Fragemenge eine eigene Datei. Die Ergebnisse der Fragen zur Anrufliste stehen in einer anderen Datei wie die Ergebnisse der Fragen zu den GPS. Das dient der Übersicht und besseren Auswertbarkeit der Ergebnisse.
Die Auswertung der Eingabe des Benutzers geschieht in einem *onClickListener* der für den Button, der zu nächsten Frage führt, implementiert wurde. Das heißt erst nachdem der Benutzer seine Eingabe getätigt und den Button für die nächste Frage gedrückt hat, wird die Auswertung durchgeführt. Dabei wird der Zeitpunkt, der über den *DatePicker* und eventuell den *TimePicker* bestimmt wurde, in Millisekunden seit dem 1.Januar 1970, der sogenannten Unixzeit, umgerechnet. Nach dem Umwandeln der eingegebenen Zeit, wird der Wert mit dem Eintrag aus dem Datenbank verglichen. Bei *WhenLastCalled* und *WhenWasLastCallYouMade* ist dies der Zeitpunkt an dem zuletzt jemand angerufen hat oder ein Anruf angenommen wurde. Bei der

Durchführung des Vergleichs ist eine Abweichung von maximal 30 Minuten erlaubt. Das heißt der Benutzer muss sich nicht auf die Minute genau an den Zeitpunkt des letzten Anrufs erinnern, sondern hat ein wenig Spielraum. Das Ergebnis des Vergleichs wird anschließend in eine Textdatei in Form „Korrekte Antwort„ oder „Falsche Antwort“ geschrieben. Die letzte Aktion die im *onClickListener* geschieht, ist das Aufrufen der nächsten Frage.

Die zweite Kategorie von Fragen zur Anrufliste verwenden ein Spinner Element um eine Art von DropDown Menü zu realisieren(siehe Abbildung 7). Aus dieser kann dann ein Element als Antwort auf die Frage gewählt werden. In Abbildung 2 ist ein Beispiel hierfür zu sehen. Die Klassen *WhoCalledMeLast*, *WhoLastCalled*, und *WhoLastCalledCouldntReach* gehören in diese Kategorie. Auch hier wird zunächst Zugriff auf die Datenbank erlangt und die Textdatei für die Ergebnisse der Frage vorbereitet. Der Unterschied zur vorherigen Kategorie ist die Art der Eingabe der Antwort. In der vorherigen Kategorie wurde ein Zeitpunkt angegeben. Hier muss ein Element aus einer Menge von Elementen gewählt werden. Dies ist vergleichbar mit einer Multiple Choice Frage in klassischen Fragebögen. Die Antwortmenge besteht in diesem Fall aus den Namen der Kontakte, die der Benutzer auf seinem Smartphone gespeichert hat. Ein *onClickListener* prüft, ob die ausgewählte Antwort mit der korrekten Antwort, die aus der Datenbank extrahiert wurde, übereinstimmt. Das Ergebnis wird auf die selbe Art und Weise wie in der ersten Kategorie gespeichert. Damit der Benutzer Auswahlmöglichkeiten hat, muss das Spinner Element noch gefüllt werden. Dies geschieht durch Elemente aus der Anrufliste. Es werden je nach Frage nur eingehende, oder ausgehende Anrufe berücksichtigt. Die Namen der Gesprächspartner werden verwendet, um den Spinner zu füllen. Da in der Anrufliste mehrmals derselbe Name auftauchen kann, werden anschließend doppelt auftauchende Namen eliminiert. Zusätzlich wird eine „Ich weiß es nicht“ Option hinzugefügt.

Die dritte Kategorie besteht lediglich aus der *LastCallDuration* Klasse. In dieser Klasse wird nach einer Zeitdauer in Sekunden gefragt. Die Eingabe geschieht über eine Instanz der Klasse *EditText*, die Eingabemöglichkeiten wurden auf Zahlen begrenzt. Da es wahrscheinlich relativ schwierig ist sich auf die Sekunde genau an die Länge eines Gesprächs zu erinnern, wurde auch hier eine Toleranz implementiert, welche 30 Sekunden beträgt. Nach der Überprüfung der Eingabe werden auch hier die Ergebnisse in die selbe Textdatei geschrieben.

Abbildung 6: Frage aus der Picker Kategorie. Der Benutzer muss einen Zeitpunkt auswählen.

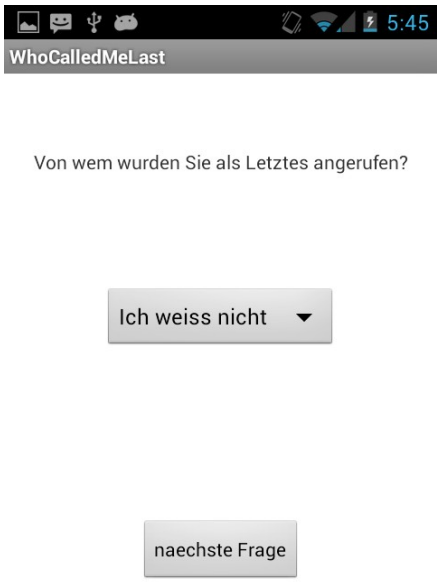

Abbildung 7: Frage aus der Spinner Kategorie. Der Benutzer wählt hier einen Namen aus.

Frage zu GPS

Im Gegensatz zu den anderen Bereichen zu denen Fragen gestellt wurden, existiert in diesem Bereich nur eine Frage. Diese wird von der *WhereWereYouQuestion* Klasse implementiert. Die Frage lautet : „Wo waren sie am folgenden Datum:". Die Eingabe der Antwort geschieht über ein Textfenster, welches durch eine Instanz der *EditText* Klasse implementiert wird. Über ein *SQLiteDatabase* Objekt wird Zugriff auf die Datenbank erlangt, und die benötigten Informationen werden extrahiert. In diesem Fall wird auf die Tabelle „every_minute_logging_table“ zugegriffen, aus der die Spalten „latitude“, „longitude“, „date“, und „date_String“ verwendet werden. Es wird zufällig ein Eintrag aus der Datenbank gewählt und dessen Datum wird in die Frage integriert. Dabei wird darauf geachtet dass der Längengrad und Breitengrad des gewählten Datenbankeintrags nicht null ist. Das ist wichtig, weil in solch einem Fall keine Adressinformationen extrahiert werden können. Tritt solch ein Fall auf, wird solange zufällig ein neuer Eintrag gewählt, bis die Kriterien erfüllt sind. Da die Spalte „date_String“ ebenfalls verwendet wird, muss das Datum, das in der Unixzeit angegeben ist, nicht umgerechnet werden, sondern kann direkt in die Fragestellung integriert werden. Die Zeit wurde zuvor schon in der Logging Anwendung umgerechnet und für den Gebrauch in dieser Klasse gespeichert.
Ein Instanz der *Geocoder* Klasse wird erstellt und wird verwendet um aus dem Längengrad und Breitengrad eine tatsächliche Adresse zu ermitteln. Dazu ist eine Inter-

netverbindung nötig. Nach betätigten des „Ok“ Buttons, wir der dafür implementierte *onClickListener* ausgeführt. Da die Eingabe der Antwort aus Text besteht, ist es in diesem Fall schwierig das Ergebnis automatisch zu überprüfen. Deshalb werden der Längengrad, der Breitengrad ,die daraus erhaltene Adresse und die Antwort des Benutzers in einer Textdatei gespeichert. Die Kontrolle der Adresse geschieht dann später manuell. Gegebenenfalls kann der Benutzer zu Rate gezogen werden.
Da es in diesem Teil des Fragebogens nur diese eine Frage gibt, sollte die Frage mehrmals beantwortet werden. Der „Ok“ beendet deshalb die Anwendung nicht, sondern gibt dem Benutzer per Vibration Feedback. So weiß er dass die Eingabe akzeptiert wurde. Durch den Zurück Knopf von Android kann er wieder zum Startbildschirm der GPS Frage und kann diese dann erneut beantworten.

Frage zu den Fotos von Kontakten

Genauso wie im vorhergehenden Abschnitt, existiert in diesem Teil nur eine Frage. Sie lautet „Wer ist auf dem Bild zu sehen?“ und wird von der Klasse *WhoQuestion* implementiert. Es wird zufällig ein Kontakt aus der Kontaktliste des Benutzer ausgewählt und dessen Kontaktfoto wird dem Benutzer präsentiert. Der Benutzer muss nun bestimmen wer der auf dem Bild abgebildete Kontakt ist. Die Eingabe geschieht über ein *EditText* Textfeld. Die Eingabe des Benutzers, sowie der Name des Kontaktes dessen Foto verwendet wurde, wird bei Betätigen des „Ok“ Buttons in einer Textdatei abgespeichert. Weil es in diesem Bereich nur eine Frage gibt, sollte diese, genauso wie die GPS Frage, mehrmals beantwortet werden. Der „Ok“ Button führt nicht zu einer anderen Frage, und verlässt die Anwendung nicht, sondern liefert dem Benutzer eine Rückmeldung, indem das Smartphone kurz vibriert wird. Durch Betätigen des Zurück Buttons des Smartphones, kommt der Benutzer zurück zum Startbildschirm der Frage und kann diese anschließend wieder beantworten.

Fragen zu WIFI

Es wurden insgesamt drei Fragen zu Wifi Netzen gestellt. Genauso wie die Fragen zur Anrufliste, können die Fragen zu den geloggten Wifi Informationen in dieselben drei Kategorien gegliedert werden. Die erste Frage lautet „Wo haben sie das Netzwerk zuletzt gesehen?“. Hier wird, genauso wie in der Klasse *WhenDidXLastCall* die Frage dynamisch generiert. Es wird zufällig der Name eines Wifi Netzes aus der Datenbank gewählt und in die Frage integriert. Die Eingabe des Benutzers erfolgt über ein *EditText* Objekt. Die Eingabe des Benutzers wird zusammen mit der echten Adresse des Wifi Netzes, welche genauso wie im GPS Teil des Fragebogens mit Hilfe eines *Geocoders* herausgefunden wurde, abgespeichert. Die Frage „Wann haben Sie folgendes Netzwerk zuletzt gesehen“ verwendet einen *Date Picker* zur Beantwortung und wird von der Klasse *WhenQuestion* implementiert. Auch hier wird ein zufälliges Wifi Netz aus der Datenbank gewählt und in die Frage integriert.
Die Frage „Mit welchem Netzwerk waren sie als letztes verbunden?“ nutzt einen Spinner zur Eingabe der Antwort und wird von der Klasse *WhichQuestion* implementiert.

Fragen zu SMS

Zu den SMS wurden drei Fragen gestellt. Diese werden in den Klassen *LastSMSReceivedQuestion*, *SmsLengthQuestion* und *WhoSentMeLastSMS implementiert.* Es wird nach dem Zeitpunkt des letzten SMS Erhalts, der Länge der letzten erhaltenen SMS und dem Absender der letzten erhaltenen SMS gefragt. Die erste der drei Fragen wird über einen Picker beantwortet, die zweite über ein *EditText* Textfeld in dem die Länge der letzten SMS angegeben werden kann und bei der dritten Frage wird ein Spinner Element verwendet um dem Benutzer die Optionen, aus denen er wählen kann, zu präsentieren. Die Antworten werden in der Datei „SMSAnswers.txt“ abgespeichert.

Fragen zu Bildern

Es wurden 3 Klassen implementiert die Fragen zu Bildern stellen. Diese sind *WhereQuestions*, *WhenQuestions* und *EventQuestion*, in denen nach dem Ort, der Zeit und dem Anlass der Aufnahme eines Fotos gefragt wird. Der Ort kann über ein *EditText* eingeben werden, der Zeitpunkt über einen *DatePicker* und das Event ebenfalls über ein *EditText* Textfenster. Die Eingabe wird in einer Textdatei gespeichert.

4. Implementierung

5. Studie

Im Rahmen diese Arbeit wurde eine Studie durchgeführt. In diesem Kapitel wird die Durchführung der Studie beschrieben. An der Studie nahmen insgesamt 10 Personen teil. Es sollte herausgefunden werden, wie gut die Leistung von auf Kontext basierenden Passwörter in Hinblick auf Merkfähigkeit und Sicherheit ist.
Die Teilnehmer waren zwischen 20 und 57 Jahre alt (Mittelwert: 31,9 Standardabweichung: 9,3). Es nahmen 8 männliche und 2 weibliche Personen teil. Die Mehrheit der Teilnehmer waren Studenten oder hatten studiert. Die Verteilung der Faktoren Alter, Geschlecht und Beruf der Teilnehmer kam aufgrund des sozialen Umfeldes des Verfassers zustande. Einer der Teilnehmer war über den größten Teil der Aufzeichnungszeit im Urlaub und ein Teilnehmer stammt nicht aus dem akademischen Umfeld. Das sollte zur Diversifizierung der Ergebnisse beitragen.

5.1. Beginn der Datenaufzeichnung

Die Studie wurde in 2 Schritten durchgeführt. Im ersten Schritt wurde mit jedem Teilnehmer ein Termin zum Beginn der Studie vereinbart. Nach der Begrüßung wurde der Teilnehmer darum gebeten eine Einverständniserklärung zu unterschreiben. In dieser Erklärung wurde er auf das Thema der Studie hingewiesen und dass er jederzeit zurücktreten kann. Auch musste er entscheiden ob er damit einverstanden ist dass ein Foto von ihm in der Diplomarbeit verwendet wird. Anschließend musste er einen Fragebogen zu seiner Person ausfüllen. Im Fragebogen wurde nach dem Geschlecht, Alter und Studiengang bzw. Beruf gefragt. Wie lange der Teilnehmer schon ein Smartphone besitzt, was die Marke und das Modell des aktuellen Smartphones war, wie oft der Teilnehmer auf das Smartphone schaut und mit welchem System das Smartphone gesperrt wird waren ebenfalls Fragen, die gestellt wurden. Die letzte Frage musste in manchen Fällen näher erläutert werden, da nicht jedem Teilnehmer klar war, was damit gemeint ist. Nachdem der Teilnehmer diese Daten angegebenen hatte, wurde ihm die Studie erklärt. Um die Ergebnisse der Studie nicht zu beeinflussen, wurde nicht der wahre Grund für die Durchführung der Studie genannt. Dem Teilnehmer wurde erklärt, es ginge um die Art und Menge von Daten die sich auf einem Smartphone ansammeln. Dies wurde auch in der Einverständniserklärung als „Accumulation of different types of Data on Smartphones“ aufgeführt. Die Tatsache dass der wahre Grund der Studie nicht genannt wurde, hat Vor- und Nachteile. Falls die gesammelten Daten für die Authentifizierung auf dem Smartphone genutzt werden sollen, ist es realistischer, dass der Benutzer darüber informiert wird. In diesem Fall würde der Benutzer versuchen, die Daten besser im Gedächtnis zu behalten, was zu einer gesteigerten Effizienz des Systems führen könnte. Im Fall dieser Studie hat man darauf verzichtet weil herausgefunden werden sollte, an welche Art von Daten die Teilnehmer sich am Besten erinnern können. Falls dem Teilnehmern der wahre Grund der Studie genannt worden wäre, hätten sie sich die Daten eventuell aufge-

schrieben und so versucht, sich die Daten besser einzuprägen, um damit dem Verfasser damit zu helfen. Bei der Erklärung der Studie wurde besonders auf den Datenschutzaspekt wert gelegt. Es wurde ausdrücklich darauf hingewiesen, dass die Daten nur lokal auf dem Smartphone gespeichert werden und nicht etwa per Internetverbindung an einen Server versendet werden. Zusätzlich wurde er darauf hingewiesen dass die Daten nur zu Auswertezwecken gesammelt und nach der Auswertung gelöscht werden. Ebenso wurde ihm erklärt, dass zwei Wochen lang Niemand Zugriff auf die Daten haben wird und nach Ablauf dieser Zeit nur der Diplomand die Daten einsehen kann. Dem Teilnehmer wurde mitgeteilt, dass nach Ablauf von 10 bis 14 Tagen eine Befragung durchgeführt wird. Als nächstes folgte die Installation der Anwendung die zum Loggen der Daten diente (siehe Kapitel 4), die direkt auf das Smartphone installiert wurde ohne den Google Play Store zu benutzen. In den meisten Fällen geschah dies über ein USB zu micro-USB Kabel über das das Smartphone an einen Rechner angeschlossen wurde. Damit wurde die Anwendung als installierbare Datei in Form einer .apk Datei auf das Smartphone des Teilnehmers kopiert und von dort aus installiert. In einigen Fällen wurde die Datei per Email an den Teilnehmer versandt, welcher sie dann auf sein Smartphone herunterlud und installierte. Nach dem Installieren der Anwendung wurde ein Testlauf durchgeführt. Die Anwendung wurde gestartet und das Smartphone wurde für einige Minuten im Freien herumgetragen um eine Standortbestimmung per GPS zu ermöglichen. Anschließend wurde kontrolliert ob das Aufzeichnen der Daten funktioniert hat. Dazu wurde das Smartphone wieder an einen Rechner angeschlossen und die Datenbank Dateien wurden auf den Rechner kopiert. Mithilfe eines SQLite Browsers (siehe Abbildung 8), wurde die Datenbank geöffnet und der Inhalt überprüft.

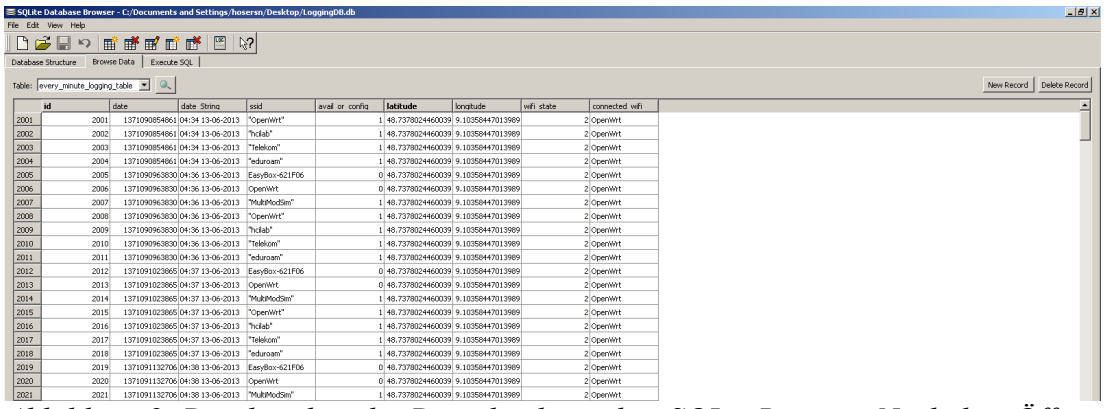

Abbildung 8: Durchsuchen der Datenbank mit dem SQLiteBrowser. Nach dem Öffnen einer Datenbank können alle Tabellen durchsucht werden. Außerdem ist es möglich Anfragen an die Datenbank zu stellen. Es wurde der SQLite Database Browser verwendet.

Es wurde überprüft ob eine GPS Lokalisation stattgefunden hatte und auch die sonstigen Daten wie Anruflisten usw. korrekt aufgezeichnet wurden. Im Rahmen des Tests wurde der Teilnehmer darum gebeten, sein Smartphone aus und wieder einzu-

8 http://sqlitebrowser.sourceforge.net/

schalten. Dies sollte dem Teilnehmer klarmachen, wie sich das Programm bei einem Neustart des Geräts verhält und wie er in diesem Fall reagieren muss. Anschließend wurden das Programm neu gestartet. Ab diesem Zeitpunkt begann die 2-Wochen-Frist, nach der die Befragung zu den gesammelten Daten durchgeführt werden sollte.

5.2. Durchführung der Befragung

Nachdem eine Frist von 10 bis 14 Tagen vergangen war, wurde der Teilnehmer zu einer Befragung eingeladen. Als Befragungsort wurde dem Diplomanden ein Büro zu Verfügung gestellt, in dem die Befragung ungestört durchgeführt werden könnte. Die eigentliche Befragung wurde in 2 Schritten durchgeführt. Der erste Teil der Befragung bestand aus der Fragebogen Anwendung die für Android programmiert wurde. (siehe Kapitel 4) Dazu wurde die Fragebogen Anwendung in Form einer .apk Datei auf das Smartphone des Teilnehmers installiert. Anschließend wurde der Teilnehmer dazu aufgefordert die einzelne Bereiche des Fragebogens zu verwenden (siehe Abbildung 9). Durch die Verwendung eines elektronischen Fragebogens wurde sichergestellt dass die Daten des Benutzers auf dem Smartphone verbleiben konnten. Dies trug zur Aufrechterhaltung der Privatsphäre bei. Jeder Teilnehmer musste die Fragen in einer anderen Reihenfolge beantworten. Es wurden Permutationen mithilfe des Latin „Square“ Verfahrens ermittelt und verwendet. Als zweiter Teil wurde ein klassischer Fragebogen verwendet. Dieser Fragebogen bestand aus vier Teilen. Der allgemeine Teil beinhaltete Fragen zur Person, wie Geschlecht und Alter, Fragen zu den Nutzungsgewohnheiten des Teilnehmers und mit welchen Personengruppe er welche Informationen teilen würde. Dazu sollte er vier Gruppen definieren: Die Gruppe mit der er keine Informationen teilt, die Gruppe mit der er wichtige Informationen teilt, die Gruppe mit der er manche Informationen teilt und die Gruppe mit der er keine Informationen teilt.
Der zweite Teil des Fragebogens befasste sich mit der Akzeptanz die die Teilnehmer dem System entgegenbringen. Es wurde gefragt ob und in welchen Situationen (privat, semi-privat, öffentlich) der Teilnehmer das System verwenden würde. Diese Fragen wurden in Form einer Likert-Skala gestellt. Ebenfalls wurde nach dem Sicherheitsbedürfnis des Teilnehmers gefragt. Der Fragebogen wurde durch zwei UEQs(User Expericence Questionnare) vervollständigt. Diese Fragebögen dienen der Evaluierung der Erfahrung die die Teilnehmer mit der Anwendung gemacht haben[LHS08].
Der dritte Teil des Fragebogens beschäftigte sich mit der Sicherheit. Es sollte zunächst das vom Teilnehmer zur Zeit benutzte System und anschließend die übrigen Kontextinformationen bezüglich ihrer Sicherheit bewertet werden. Der Teilnehmer sollte anschließend angeben, inwieweit die Personengruppen, die er im ersten Teil des Fragebogens definiert hatte, seiner Meinung nach seine Kontextinformationen und sein aktuelle Passwort kennen. Alle Fragen in diesem Teil des Fragebogens verwendeten eine Likert Skala.
Der vierte Teil des Fragebogens behandelte die Anwenderfreundlichkeit. Es wurde gefragt, ob der Teilnehmer Schwierigkeiten hatte sich an manche Informationen zu

erinnern und wie er seine Erinnerung an die Kontextinformationen über verschiedene Zeiträume(1 Stunde, 1 Tag, 1 Woche, 1 Monat) einschätzte. Auch diese Fragen werden in Form einer Likert-Skala gestellt. Der Fragebogen wird mit einigen Freitext Fragen abgeschlossen die dazu dienen in Erfahrung zu bringen, ob der Teilnehmer generell Probleme mit den Fragen hatte. Die letzte Frage sollte herausfinden ob der Teilnehmer noch zusätzliche Anmerkungen zu den Fragen hatte.

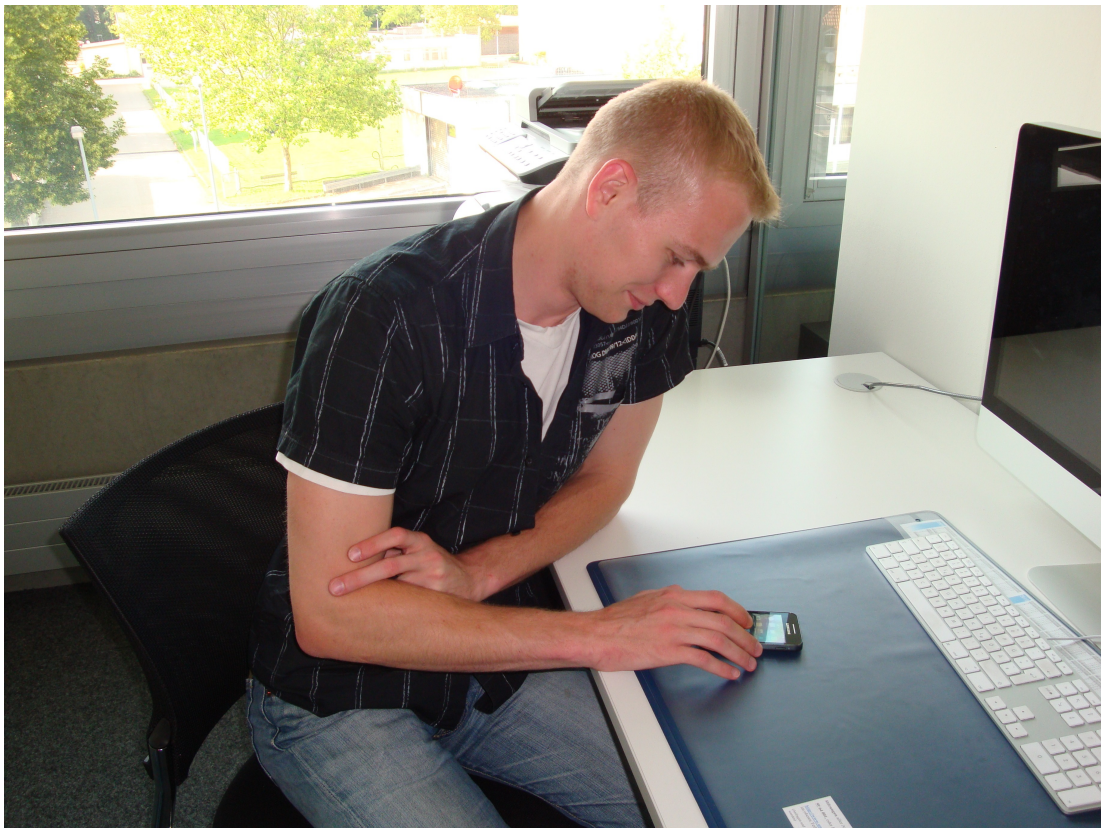

Abbildung 9: Teilnehmer beim Ausfüllen des elektronischen Fragebogens

Nachdem der Teilnehmer den elektronischen Fragebogen beendet hatte (siehe Abbildung 9), wurde ihm der klassische Fragebogen zur Beantwortung vorgelegt. Während dieser den Fragebogen ausfüllte, wurden die Textdateien, die vom elektronischen Fragebogen angelegt wurden und die Ergebnisse des Teilnehmers beinhalteten, vom Diplomanden zu weiteren Auswertung kopiert. Anschließend wurden alle Anwendungen und Daten vom Smartphone des Teilnehmers entfernt. Nachdem der Teilnehmer den klassischen Fragebogen komplett ausgefüllt hatte, wurden dem Teilnehmer nach einer Unterschrift 15 Euro ausgehändigt.
Während der Durchführung der elektronischen Befragung traten einige Unregelmäßigkeiten auf. Es konnten nicht jede Informationen von jedem Teilnehmer gesammelt werden. Das lag teils an Problemen mit der Internetverbindung des Smartphones , und teils daran dass einige Teilnehmer keine Bilder oder Kontaktfotos gespeichert hatten.
Eine weitere Komplikation trat bei Fragen nach den Fotos von Kontakten auf. Die

Tatsache, dass einige Teilnehmer ihre Smartphones mit einem Google Konto verbunden hatten führten dazu, dass nicht nur nach Fotos von Kontakten aus dem Telefonbuch gefragt wurden, sondern auch nach Kontakten aus dem Google Konto. In diesen Fällen kam es vor, dass der Teilnehmer das Kontaktfoto des Kontakts zuvor noch nie gesehen hatte.
Es kam vor, dass Bilder auf dem Smartphone des Teilnehmers nicht von ihm aufgenommen wurden. Ein Teilnehmer hatte Album Covers als Bilder auf seinem Smartphone gespeichert. Ein anderer Fall war es, dass der Teilnehmer ein Bild zugeschickt bekommen hatte und es so nicht selber aufgenommen hatte. In diesen Fällen machten Fragen wie „Wo wurde dieses Bild aufgenommen?“ oder „Wann wurde dieses Bild aufgenommen?“ wenig Sinn.
Einige Fragen die nach einer Zeitangabe verlangten, hatten keine Option für den Fall dass der Teilnehmer die Antwort „ich weiß es nicht“ geben wollte. In solchen Fällen wurden die Frage und die Entscheidung des Teilnehmers vom Diplomanden zur späteren Auswertung vermerkt.

6. Ergebnisse der Studie

Die Ergebnisse der Studie lassen sich in zwei Teile gliedern. Die Ergebnisse des elektronischen Fragebogens, und die Ergebnisse des klassischen Fragebogens.

6.1. Elektronischer Fragebogen

Für die Auswertung des elektronischen Fragebogens wurden die Textdateien, die der Fragebogen automatisch bei Beantwortung einer Frage anlegte, verwendet. Dabei gab es sechs verschiedene Fragebereiche.

6.1.1 Anruflisten

Hier wurden acht Fragen gestellt. Diese betrafen, die letzten getätigten Anrufe, die Personen mit denen diese Anrufe geführt wurden und die Länge der Anrufe. Das Beste Ergebnis wurde bei der Frage nach der Länge des letzten Anrufs erzielt. Hier wussten sechs der zehn Teilnehmer die richtige Antwort. Die Hälfte der Teilnehmer konnte sich an den letzten Anruf, den sie getätigt hatten, erinnern. Bei den übrigen Fragen wurden nur maximal drei richtige Antworten gegeben. Die Tatsache dass auch sehr lange zurückliegende Anrufe (>1Jahr) für die Fragen verwendet wurden, erschwerte einige der Fragen. Die Ergebnisse lassen schließen, das sich Anruflisten nicht sehr gut als Kontextinformationen eignen, doch könnte ein weiterer Test der einen eingeschränkten Zeitraum für die Anrufe verwendet, dieses Ergebnisse positiv beeinflussen.

6.1.2 Kontaktfotos

In diesem Teil des Fragebogens wurde das Bild eines Kontakts präsentiert und nach dem Namen gefragt. Es hatten acht der zehn Teilnehmer Kontaktfotos auf ihrem Smartphone gespeichert. Davon beantworteten sechs Teilnehmer die Frage drei mal, ein Teilnehmer zwei mal und ein Teilnehmer ein mal. Da der elektronische Fragebogen die Antworten der Teilnehmer, sowie den Namen des angezeigten Kontaktes, in einer Textdatei abspeicherte, konnte die Korrektheit der Antworten überprüft werden. Von den 21 Antworten waren 16 korrekte Antworten, eine falsche Antwort und viermal wurde mit „Ich weiß nicht“ geantwortet. Fünf Teilnehmer hatten ihr Smartphone mit einem Google Konto verbunden und bekamen so auch Bilder von Kontakten, die nicht im Smartphone gespeichert waren. Einige der „Ich weiß nicht“ Antworten sind auf diesen Umstand zurückzuführen. Der Anteil der korrekten Antworten liegen bei 76.2 %, womit Kontaktfotos ein guter Kandidat für zukünftige Forschung in diesem Bereich sind.

6.1.3 Bilder

Es konnten von vier Personen Informationen zu Bildern gesammelt werden. Das lag zum Einen daran, das manche Teilnehmer keine Bilder auf dem Smartphone gespeichert hatten. Bei einem anderen Teilnehmer waren nur Bilder gespeichert die er nicht aufgenommen hatte und die somit für die gestellten Fragen keine Relevanz hatten.

Außerdem traten bei einigen Teilnehmern Komplikationen aufgrund der Android Version auf. Ein Teilnehmer hatte beispielsweise eine angepasste Androidversion auf seinem Smartphone installiert. Aus diesen Gründen konnte auch in den anderen Fragebereichen nicht immer von Allen Teilnehmern Antworten gesammelt werden. Von den Teilnehmern die die Fragen beantworten konnten, wussten alle wo die angezeigten Bilder aufgenommen wurden oder zu welchen Ereignissen diese aufgenommen wurden. Um ein aussagekräftigeres Ergebnis zu erhalten sollten aber weitere Untersuchungen durchgeführt werden. Viele der verwandten Arbeiten die sich mit grafischen Passwörtern beschäftigen(siehe Kapitel 2) sprechen aber dafür dass sich Bilder zur Authentifizierung eignen könnten.

6.1.4 GPS Daten

In diesem Teil wurde der Teilnehmer gefragt, wo er sich zu einem bestimmten Zeitpunkt aufhielt. Es konnten von acht Personen Daten gesammelt werden. Jeder Person beantwortete diese Frage drei mal. Von den insgesamt 24 Versuchen waren 16 richtig und 8 falsche Antworten.Die Erfolgsrate lag also bei 66,67 %. Jedoch wurden auch solche Angaben als richtig gewertet, bei denen der Teilnehmer nicht die komplette Adresse kannte oder eine mäßig genaue Angabe (Uni Stuttgart Stadtmitte) machte. GPS Daten eignen sich also nur bedingt für die Authentifizierung, vor Allem wenn genaue Angaben verlangt werden. Wenn der Teilnehmer aber über den Grund der Datenaufzeichnung aufgeklärt worden wäre, könnten eventuell bessere Ergebnisse erzielt werden.

6.1.5 SMS Daten

Es wurden von allen zehn Personen Antworten zur Uhrzeit, Länge und Absender der zuletzt erhaltenen SMS gesammelt. Von den zehn Teilnehmern konnten neun die Fragen zum Datum oder Länge der SMS nicht ausreichend beantworten. Dabei durfte die Antwort für das Datum eine halbe Stunde vom korrekten Datum und die Antwort für die Länge um zehn Zeichen von der korrekten Länge abweichen. Eine Antwort außerhalb dieses Toleranzbereiches wurde als falsche Antwort gewertet. Den Absender der letzten SMS konnten drei Personen richtig nennen, zwei gaben falsche Antworten und fünf waren der Meinung dass der Absender nicht in den Antwortmöglichkeiten aufgeführt wurde. Diese Ergebnisse führen zu dem Schluss dass sich SMS als Kontextinformationen weniger gut eignen.

6.1.6 Wifi Daten

In diesem Teil des Fragebogens wurden drei Fragen gestellt. Es wurde nach dem Standort eines Wifi Netzwerks,den Zeitpunkt wann ein bestimmtes Netzwerk gesehen wurde und mit welchem Wifi Netz der Teilnehmer zuletzt verbunden war, gefragt. Daten von acht der Teilnehmer konnten gesammelt werden. Es wurden zwei Fragen von zwei Teilnehmern und drei Fragen von sechs Teilnehmern beantwortet. Zu der Frage nach dem Standort kamen zwei richtige, zwei falsche und zwei „Ich weiß nicht“ Antworten. Die Frage, wann ein bestimmtes Netzwerk zuletzt gesehen wurde, wurde nur ein mal richtig, fünf mal falsch und zwei mal mit „Ich weiß nicht“

beantwortet. Bei der Frage nach dem Netz mit dem man zuletzt verbunden war, kamen drei richtige, drei falsche und zwei „Ich weiß nicht“ Antworten. Insgesamt waren sechs der Antworten korrekt, zehn waren falsch und bei sechs Fragen gaben die Teilnehmer an die Antwort nicht zu kennen.

6.2. Klassischer Fragebogen

Der klassische Fragebogen bestand hauptsächlich aus Fragen die mit einer Likert Skala von eins bis fünf beantwortet wurden. Es gab drei Multiple Choice Fragen und mehrere Fragen, bei der nach einem Kommentar des Benutzers gefragt wurde. Der Fragebogen wurde in vier Teile unterteilt. Diese Teile waren die allgemeine Fragen sowie Fragen zur Akzeptanz, Sicherheit und Anwenderfreundlichkeit.

6.2.1 Allgemeine Fragen

Zu Beginn des allgemeinen Teils des Fragebogens wurden demografische Daten der Teilnehmer erfasst. Die nächste Frage betraf die Benutzung eines Smartphones und fragte nach der aktuellen Display Sperre. Nur drei Teilnehmer hatten eine Art Passwortschutz für ihr Smartphone aktiviert, von denen zwei das Mustersystem verwendeten und einer ein alphanumerisches Passwort. Die restlichen Teilnehmer entsperrten ihr Smartphone mit der Option „Finger bewegen“ (sechs Teilnehmer) oder hatten gar kein Sperrsystem. Nur drei Teilnehmer gaben an schon mal ein grafisches Authentifizierungssystem benutzt zu haben. Die meisten Teilnehmer sagten dass sie ihr Smartphone sehr häufig bis häufig benutzen. Die Bewertung fand bei dieser Frage auf einer Likert Skala von eins bis sieben statt, wobei sieben für sehr häufig stand und eins für nie. Der Mittelwert war 6,3, die Standardabweichung betrug 0,79. Die letzte Frage des allgemeinen Teiles betraf die Funktionen des Smartphones, die genutzt wurden. Dabei war die häufigste Nutzung die Telefonfunktion (neun Teilnehmer) gefolgt von der SMS Funktion (sieben Teilnehmer). Der Dienst „What's App“, Spiele und Social Media Funktionen wurden von sechs Teilnehmern genutzt. Vier gaben an im Internet zu surfen und einer benutzte die Navigation des Gerätes.

6.2.2 Akzeptanz

Die Frage ob die Teilnehmer ein System verwenden würden welches Kontextinformationen nutzt um den Benutzer zu authentifizieren, wurde auf einer Likert Skala von eins bis fünf, wobei eins für „Lehne vollständig ab“ und fünf für „Stimme vollständig zu“ steht, in Mittel mit einer 2,6 bewertet. Die Standardabweichung betrug 1,34. Dabei bewegten sich die meisten Antworten im Bereich von zwei bis vier, mit nur drei Ausreißern davon zwei die das System vollständig ablehnten und einer der das System vollständig akzeptierte. Bei der Akzeptanz der Verwendung von Kontextinformationen(siehe Abbildung 10) ist zu erkennen dass die Teilnehmer im Durchschnitt am wenigsten Problem hatten wenn sie das System in einer privaten Umgebung verwenden würden. Dabei waren die Kontaktfotos am beliebtesten, gefolgt von den Bildern. SMS und Anruflisten wurden von den Teilnehmern ähnlich akzeptiert. An fünfter Stelle lagen die Wifi Informationen und zuletzt kamen die Informationen über den Standort. Die Tatsache dass die Akzeptanzwerte der Wifi Informationen an

vorletzter Stelle lagen und die Werte für drei Bereiche relativ ähnlich waren, lässt darauf schließen dass sich diese Informationen allgemein nicht gut für Fragen eignen und es daher egal ist in welcher Situation sie verwendet werden. Die Tatsache dass die GPS Daten an letzter Stelle liegen, führt zu dem Schluss, dass die Teilnehmer nicht wollen, dass Daten über ihren Aufenthalt gespeichert werden da sie sich so eventuell beobachtet fühlen. Diese These wurde auch von mindestens einer Person bestätigt(„Wollen Sie mich verfolgen?“).

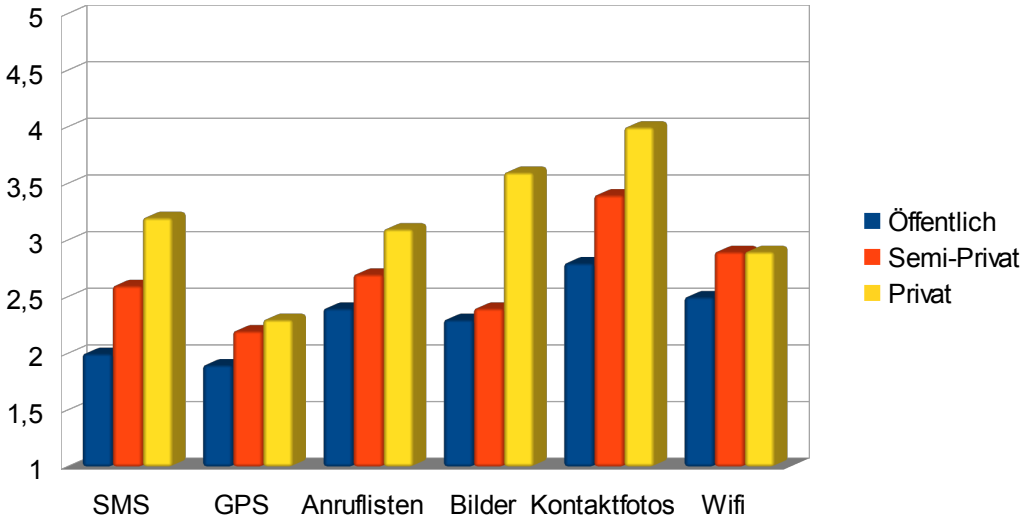

Abbildung 10: Akzeptanz der Kontextinformationen durch die Teilnehmer

Anschließend wurde eine Frage bezüglich der Wichtigkeit der Privatsphäre gestellt. Das Mittel der Antworten betrug 4,1, die Standardabweichung 0,94. Als nächstes wurden die Teilnehmer nach Sicherheitsbedenken bezüglich der verwendeten Daten gefragt. Drei der Teilnehmer hatten nur Bedenken falls die Daten weitergegeben würden. Ein Teilnehmer fand das System in der Öffentlichkeit unangebracht, hatte aber ansonsten keine Bedenken.
Vier Teilnehmer hatten unterschiedliche Bedenken. Ein Teilnehmer merkte an dass bei normalen Gesprächen in Facebook eventuell GPS Informationen weitergegeben werden und somit Passwortinformationen anderen Personen zugänglich sind. Ein anderer Teilnehmer würde das System nicht benutzen da seine Freunde manche der benötigen Informationen ebenfalls besäßen. Der dritte Teilnehmer der Bedenken hatte, argumentierte, dass andere Personen über das Entsperrsystem Informationen über ihn erhalten könnten. Die letzten zwei Fragen des Akzeptanzteiles waren User

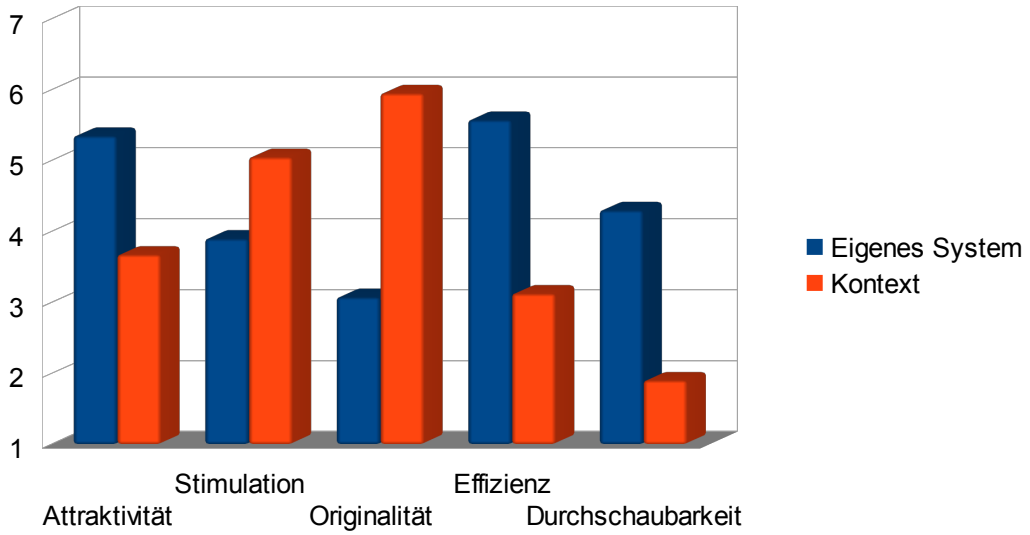

Abbildung 11: Ergebnisse der „User Experience“ Fragebögen

Experience Questionnaires, mit denen das zur Zeit benutzte Sperrsystem und ein System, das Kontextinformationen verwendet, bewertet werden sollte. Die Punkte Attraktivität, Effizienz und Durchschaubarkeit wurden beim eigenen System am Höchsten bewertet (siehe Abbildung 11). Das könnte mit der Tatsache zusammenhängen dass fast keiner der Teilnehmer einen nennenswerten Schutz aktiviert hatten (7 Teilnehmer), sondern meistens die Option „Finger bewegen“ verwendeten, um das Smartphone zu entsperren. Ein Authentifizierungssystem das auf Kontextinformationen basiert wurde als stimulierend bewertet. Das liegt wahrscheinlich an der Tatsache, dass man bei solch einem System zur Beantwortung der Fragen nachdenken muss, und nicht durch ein leichtes Fingerwischen oder Eingabe eines gelernten Passwortes das Smartphone entsperrt. Ein Kontextsystem wurde auch als origineller als das eigene System bewertet. Der Grund hierfür ist vermutlich, dass es sich von den bekannten Sperrsystemen auf dem Smartphone erheblich unterscheidet und deshalb als etwas Neues angesehen wird. Die Durchschaubarkeit des Kontextsystems wurde sehr schlecht bewertet (Mittelwert : 1,9). Die Fragen zu den Kontextinformationen wurden von den Teilnehmern als zu kompliziert betrachtet. Dies könnte an der Eingabe der Antworten liegen und müsste in zukünftigen Versionen modifiziert werden.

6.2.3 Sicherheit

Dieser Teil des Fragebogens begann mit einer Frage bezüglich der subjektiven Einschätzung der Sicherheit der einzelnen Kontextinformationen. Das eigene System wurde als relativ unsicher bewertet(Mittelwert:2,1, Standardabweichung: 1,37) was wohl an der Tatsache lag, dass die meisten Teilnehmer ihr Smartphone nicht gesichert hatten. Als sicherstes wurden Bilder und GPS mit einem Mittelwert von 3,3 bewertet(Standardabweichung Bilder: 1,14 GPS: 1,00). Die Teilnehmer hatten teilweise selber Schwierigkeiten sich an die GPS Daten zu erinnern, und waren der Meinung

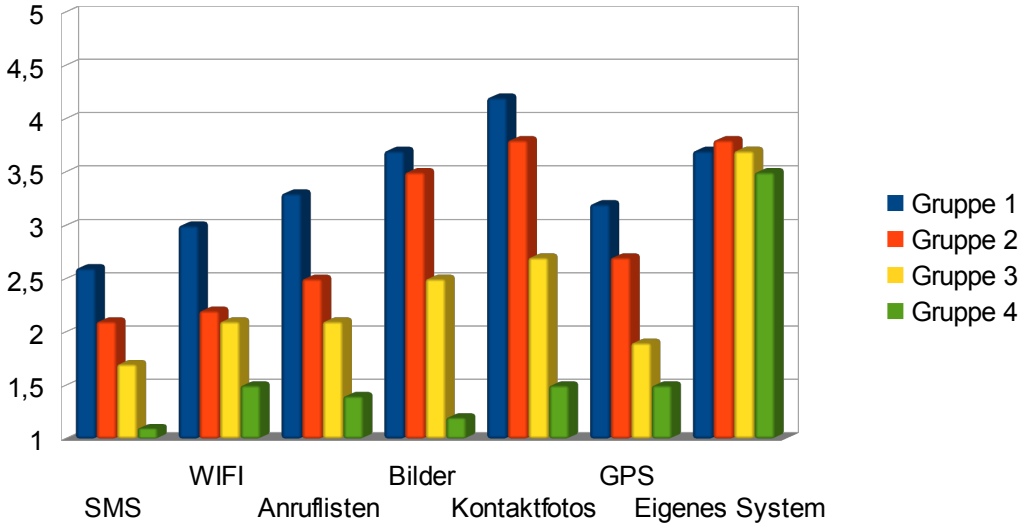

Abbildung 12: Ratbarkeit der Kontextinformationen durch andere Personen.

dass es andere wohl auch nicht könnten. Die nächsten sechs Fragen ließen den Teilnehmer einschätzen, wie gut andere Personen die nötigen Informationen zum Entsperren des Smartphones kannten oder erraten konnten. Dabei wurden vier Gruppen gebildet: Personen mit denen man alle Informationen teil, Personen mit denen man manche Informationen teilt, Personen mit denen man wichtige Informationen teilt und Personen mit denen man keine Informationen teilt. Gruppe eins bestand aus Partnern, bester Freund/beste Freundin und Familie. Ein Teilnehmer ordnete ausschließlich sich selbst in diese Gruppe ein. Gruppe zwei beinhaltete meistens Freunde und Familie. Zur Gruppe drei gehörten Bekannte und Arbeitskollegen. In die letzte Gruppe wurde von allen Teilnehmern Fremden oder Unbekannte eingeordnet. Personen der Gruppe eins können laut Teilnehmer am Besten die nötigen Informationen erraten, Gruppe vier hat laut Teilnehmer geringe Chancen an die Informationen heranzukommen. Die Bewertung der einzelnen Informationen nahm von Gruppe eins bis Gruppe vier erheblich ab (siehe Abbildung 12). Die einzige Ausnahme hier, war das Passwort des eigene Systems. Da viele Teilnehmer gar keinen keinen Schutz hatten, wurden die Möglichkeit, das andere Personen das Passwort erraten können, für alle Gruppen fast gleich bewertet.

6.2.4 Anwenderfreundlichkeit

Die erste Frage in diesem Teil des Fragebogens betraf das allgemeine Erinnerungsvermögen an die Kontextdaten. Die einzelnen Kontextdaten wurden auf einer Likert Skala von eins bis fünf bewertet. Die Wifi Daten wurden am schlechtesten, im Durchschnitt mit 2,6 (Standardabweichung: 1,50) bewertet. Am Besten konnten die Teilnehmer sich an die Kontaktfotos erinnern (Mittel: 4,1 Standardabweichung: 1,04). Die zweite bis siebte Frage wurde gestellt um herauszufinden ob die

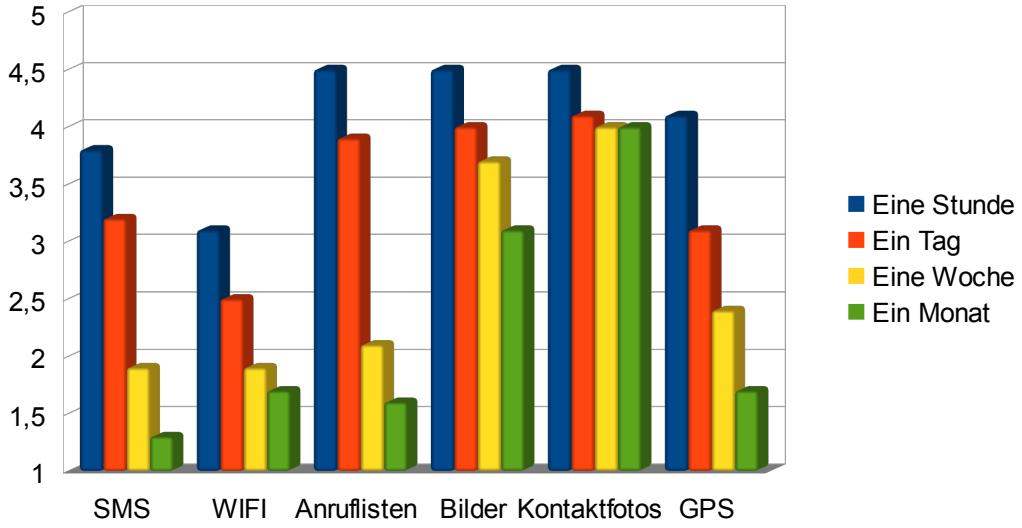

Abbildung 13: Errinerungsvermögen an die Kontextinformationen

Teilnehmer glauben, dass sie sich an bestimmte Daten nach unterschiedlichen Zeitspannen erinnern können (siehe Abbildung 13). Die Zeitpunkte nach denen gefragt wurde waren „nach einer Stunde“, „nach einem Tag“, „nach einer Woche“ und „nach einem Monat“. Wie zu erwarten war, dachten die Teilnehmer bei den meisten Daten, dass sie sich nach längeren Zeiträumen immer schlechter an die Daten erinnern können. Die einzige Ausnahme waren die Kontaktfotos. Bei diesen waren die Werte relativ nahe beieinander(Stunde: 4,5; Tag: 4,1; Woche: 4; Monat:4;). Kontaktfotos sind keine Bilder die von einem bestimmten Ereignis oder Ort abhängig sind. Entweder man kennt die Person oder man kennt sie nicht. Natürlich kann es sein dass man Kontaktfotos von Personen gespeichert hat, mit denen man kaum oder keinen Kontakt hat oder bei denen der letzte Kontakt sehr lange zurückliegt. Die meisten Teilnehmer dieser Studie aber hatten Bilder von Kontakten an die sie sich noch ausreichend erinnern konnten. Ein weiteres Problem das hierbei auftreten kann ist die Verknüpfung des Smartphones mit einem Google Account. In solchen Fällen hatte der Teilnehmer keine Kontrolle über die verwendeten Bilder. Es könnten Fälle auftreten, in denen die Gegenseite ein Bild von einem Gegenstand als Kontaktfoto verwendet. In diesen Fällen wäre eine Erkennung der richtigen Person schwieriger, außer man hat Kontakt mit ihr. Der letzte Teil des Fragebogens wurde mit einigen Freitextfragen abgeschlossen. Es wurde gefragt ob die Teilnehmer Probleme hatten sich an bestimmte Daten zu erinnern oder ob sie bestimmte Fragen unlösbar fanden. Die Teilnehmer hatten Probleme sich an Daten zu Anrufen, SMS, GPS Koordinaten und Wifi Netzen zu erinnern. Ein Teilnehmer kommentierte dass er Schwierigkeiten hatte sich an alle Daten zu erinnern, da er nicht darauf vorbereitet gewesen sei. Nur ein Teilnehmer hatte Probleme mit Bildern, und keiner mit Kontaktfotos. Dies ist ein weiteres Indiz das für die Untersuchung von grafischen Kontextinformationen in zukünfti-

gen Arbeiten spricht. Als unlösbar wurden Fragen zu Daten bewertet, die zulange in der Vergangenheit lagen, oder bei denen zu detaillierte Antworten erwartet wurden.

7. Zusammenfassung und Ausblick

In dieser Arbeit wurde untersucht, ob persönliche Kontextinformationen genutzt werden können, um einen Benutzer auf einem Smartphone zu authentifizieren und welche Ergebnisse ein Authentifizierungssystem, das auf persönlichen Kontextinformationen basiert, liefert. Die Idee war es, dem Benutzer Fragen zu stellen welche aus persönlichen Daten, die auf dem Smartphone gespeichert sind, generiert wurden. Der Vorteil solch eines Systems ist es, dass jede Frage anders ist und die Fragen individuell an den Benutzer angepasst werden. Dies kann „Shoulder Surfing“ Angriffe erschweren. Um die Idee zu testen, wurde eine Anwendung für das Android Betriebssystem entwickelt, welche verschiedene Daten auf den Smartphones mehrerer Teilnehmer über einen Zeitraum von 10 bis 14 Tagen aufgezeichnet hat. Diese wurden verwendet um dem Benutzer Fragen in Form eines elektronischen Fragebogens zu stellen. Ein klassischer Fragebogen bewertete daraufhin die Einstellung des Benutzers zum System. Die Ergebnisse wurden anschließend ausgewertet. Die Auswertung ergab, dass sich vor Allem Kontaktfotos und Bilder besonders gut für kontextbasierte Authentifizierung eigneten.
In einer Folgestudie soll eine reale Anwendung des vorgestellten Konzepts untersucht werden. Dazu soll eine Applikation entwickelt werden die in den Play Store von Google gestellt wird. Interessierte sollen sich diese Applikation herunterladen und installieren können und nehmen somit an der Studie teil. Die Aufgabe der Applikation ist es eine Art Authentifizierungssystem zu implementieren, welches der Teilnehmer der Studie anstelle seines üblichen Authentifizierungssystems verwenden kann, um sein Smartphone zu Entsperren. Die Anwendung soll ebenfalls einen Teil beinhalten der Dateien des Benutzers aufzeichnet. Anschließend leitet sie aus den aufgezeichneten Daten Fragen ab und stellt diese dem Benutzer. Die erfolgreichen und nicht erfolgreichen Login Versuche sollen aufgezeichnet werden und diese Ergebnisse sollen mit Einverständnis der Teilnehmer, zur Auswertung an einen Server gesendet werden.
Studien die mithilfe eines App Stores durchgeführt werden, haben einige Vorteile gegenüber Studien die im Labor durchgeführt werden. Studien die im Labor durchgeführt werden, finden in einer kontrollierten Umgebung mit einer kleinen Gruppe statt. Diese können eine hohe interne Gültigkeit, aber eine geringe externe Aussagekraft. Dies bedeutet, dass die Ergebnisse nicht unbedingt verallgemeinert werden können. Deshalb haben Forscher angefangen Feldstudien in App Stores durchzuführen[HP13].
Henze et al. haben fünf App Store Studien untersucht, um herauszufinden welche Faktoren eine App Store Studie erfolgreich machen[HPPSB11]. Die Punkte die diskutiert wurden sind die Verteilung der Benutzer, die gesammelten Daten sowie die Gültigkeit der Ergebnisse. Es stellte sich heraus dass die Verteilung der Benutzer nicht repräsentativ für die Weltbevölkerung ist. Die meisten Daten wurden in der Stu-

die gesammelt, in der die Benutzer nicht darüber informiert wurden, dass Daten gesammelt wurden. Um qualitatives Feedback zu erhalten reichten Benutzerbewertungen aus dem App Store nicht aus und es mussten andere Quellen hinzugezogen werden. Um gültige Aussagen treffen zu können war es wichtig unvorhergesehene Benutzung der App in Betracht zu ziehen. Die Befragung in dieser Arbeit wurde unter kontrollierten Bedingungen durchgeführt. Wusste ein Teilnehmer nicht genau was mit einer Frage gemeint ist, konnte er den Diplomanden jederzeit um Hilfe bitten. Die Studie besitzt also eine hohe interne Validität. Damit die Ergebnisse der Studie verallgemeinert werden können, sollte eine App Store Studie durchgeführt werden. Damit diese Studie erfolgreich ist und genug Benutzer erhält, sollten die von Henze et al. beschriebenen Kriterien beachtet werden. Außerdem sollte die Anwendung aus dieser Studie so erweitert werden, dass sie zugänglicher für den durchschnittlichen Benutzer eines Smartphones ist. Um dieses Ziel zu erreichen, müssen einige Aspekte des Systems modifiziert werden.
Die Anwendung die in der Studie verwendet wurde, besteht aus zwei Teilen: Das Aufzeichnen der Daten und die Befragung. Diese Teile wurden getrennt implementiert und verwendet. Während die Befragung durchgeführt wurde, fand keine Datenaufzeichnung mehr statt. Der einzige Schnittpunkt der zwei Teile war die Datenbank.
Bei einer zukünftigen Play Store Anwendung, müssen diese Teile miteinander zusammenarbeiten. Der Anwender muss darauf hingewiesen werden, dass die Anwendung zuerst eine gewisse Menge von Daten benötigt und das die Nutzung vorher noch nicht sinnvoll ist. Nach dem die gewünschte Menge an Daten vorhanden sind, soll der Anwender darüber informiert werden, dass er die Anwendung nun nutzten kann. Ab diesem Zeitpunkt müssen beide Teile der Anwendung parallel laufen. Das heißt es muss sichergestellt werden, dass der Zugriff auf die Datenbank koordiniert stattfindet. In der vorangegangenen Studie musste dies nicht beachtet werden.
Ein weiterer Punkt der für eine Play Store App ausgebaut werden muss, ist die Eingabe der Antworten. Diese ist in der bisherigen App relativ aufwändig. Um eine Person auszuwählen, betätigt der Benutzer ein Drop Down Menü und wählt dann eine von mehreren Optionen aus. Diese Liste kann teilweise sehr umfangreich sein und den Benutzer dazu zwingen die Liste zu scrollen, wenn er die richtige Antwort finden will. Bei einer Zeitangabe wird über einen Date Picker und/oder einen Time Picker der gewünschte Zeitraum gewählt. Auch dies ist relativ zeitaufwendig im Vergleich zu anderen Authentifizierungsmethoden auf dem Smartphone.
In der Arbeit von De Angeli et al. wird ein System beschrieben bei dem Bilder wie bei dem klassische PIN Code Eingabefeld eines Bankautomaten angeordnet sind und auf einem Touch Screen präsentiert werden. In einer zukünftigen Play Store App könnten die Einträge auf ähnliche Art und Weise präsentiert werden um die Interaktion des Benutzers mit dem Smartphone zu vereinfachen. Der Benutzer müsste dann nur noch durch Berührung eine der Optionen auswählen.
Einige Teilnehmer der Studie kritisierten, dass nach Dingen gefragt wurde die zulange in der Vergangenheit lagen. Es kam vor das seit einem Anruf nach dem gefragt wurde, mehr als ein Jahr Zeit vergangen war. Der Grund hierfür war, dass alle Anruf-

informationen verwendet wurden die auf dem Smartphone gespeichert waren. Um das Problem zu lösen, sollte das System so modifiziert werden, dass nur Informationen verwendet werden die in einem bestimmen Zeitraum liegen. Wie groß dieser Zeitraum sein muss, um ein Gleichgewicht zwischen Menge der Informationen und Erinnerungsfähigkeit an die richtige Antwort zu finden, sollte untersucht werden.
Die verwendeten Informationen eigneten sich nicht alle gleich gut für eine Authentifizierungssystem.
Durch die Verknüpfung des Smartphones mit online Konten wie dem Google[9] oder Facebook[10] Konto stehen eine große Menge an neuen Daten zur Verfügung. Vor Allem Facebook liefert viele verschiedene Arten von Daten. Nachrichten an andere Benutzer, benutzte Anwendungen(Spiele usw...) Pinnwandeinträge und vieles mehr. Es könnte untersucht werden, ob und welche dieser Informationen extrahiert und für ein Authentifizierungssystem verwendet werden können. Analog zur Logging Anwendung in dieser Arbeit könnte eine Facebook Anwendung implementiert werden, welche verschiedene Daten zusammenfasst und an das Smartphone sendet. Solch eine Anwendung hätte auch den Vorteil, dass sie dem Benutzern eine gewisse Kontrolle über die verwendeten Daten geben könnte
Der nächste Aspekt der für eine Play Store Anwendung zu beachten ist, ist die Konfigurierbarkeit. Eine Anwendung sollte konfigurierbar sein, um ein positives Benutzungserlebnis zu liefern. Das GUI ist für eine einfache Benutzung enorm wichtig. Die Art und Weise, wie die Authentifizierungsfragen präsentiert und wie die Antworten eingegeben werden, sollte vom Benutzer angepasst werden können. Auch sollte die Anzahl der Antwortmöglichkeiten eingeschränkt werden können. Ein Benutzer der 200 Kontakte in seinem Smartphone gespeichert hat, möchte nicht bei jeder Frage die Antwort aus 200 Kontakten wählen müssen. Der Benutzer sollte jedoch darauf hingewiesen werden dass eine zu geringe Zahl von Antwortmöglichkeiten die Sicherheit des Systems reduziert.
Der Benutzter sollte auch die Wahl haben, welche Daten für die Authentifizierung verwendet werden sollen. Ein Benutzer der öfters mit verschiedenen Wifi Netzen verbunden ist, könnte sich vielleicht besser an diese Informationen erinnern, als an die letzte SMS die er verschickt hat. Manche Benutzer möchten vielleicht nicht das private Fotos als Authentifizierungsfotos auf ihrem Smartphone auftauchen, vor Allem wenn eine Authentifizierung in der Öffentlichkeit stattfindet.
Der Zeitraum über den die Daten aufgezeichnet werden sollen, muss konfigurierbar sein. Benutzer die in der Lage sind, sich gut an länger zurückliegende Ereignisse erinnern können, hätten dadurch die Möglichkeit die Sicherheit des Systems zu erhöhen, indem mehr Daten verwendet werden. Anderseits könnten Menschen mit schlechtem Erinnerungsvermögen die Rate der erfolgreichen Authentifizierungsversuche erhöhen. Das dies auf Kosten der Sicherheit geht, muss dem Benutzer klar gemacht werden. Ohne diese Einstellmöglichkeit könnte der Benutzer,bei zu häufigem Fehlschlagen der Authentifizierung frustriert werden und die Anwendung deinstallie-

9 https://accounts.google.com/Login?hl=de

10 https://de-de.facebook.com/

ren. Eine Möglichkeit die Sicherheit des Systems zu erhöhen wäre es mehrere Fragen hintereinander zu stellen. Diese könnten aus den verschiedenen Kategorien (SMS, Kontaktfotos...) gewählt werden. Auch wäre es denkbar einen weiteren Authentifizierungsfaktor wie Biometrie in Verbindung mit dieser Arbeit zu untersuchen. Bei den Fotos von Kontakten könnte Spracherkennung anstelle einer Texteingabe angewendet werden. Durch eine Methode der Stimmerkennung könnte der Benutzer auf Echtheit geprüft und somit die Sicherheit erhöht werden.
Ein weitere Idee für zukünftige Arbeiten wäre es, persönliche Kontextinformationen mit einigen der in Kapitel zwei vorgestellten Arbeiten zu kombinieren und die Ergebnisse zu untersuchen. Die Arbeit von De Angeli et al. untersucht unter anderem ein Verfahren das Bildsequenzen nutzt um einen Benutzer zu authentifizieren. Die Bilder sind hierbei bestimmten Kategorien zugeordnet.[ACCLG02] Eine Modifikation dieses Systems die in einer zukünftige Arbeit untersucht werden könnte, wäre es, die verwendeten Daten so zu verändern, dass anstelle der vorgegebenen Kategorien, Bilder aus dem persönlichen Kontext des Benutzers gewählt werden. Mögliche Kategorien wären Kontaktfotos der Telefonkontakte, Fotos, die mit der Kamera aufgenommen wurden, Bilder aus sozialen Netzwerken, usw. Damit könnte untersucht werden, ob die Wahl von Bilderkategorien aus dem persönlichen Kontext Einfluss auf das Ergebnis hat. Nazir et al. verwenden in ihrem System ebenfalls Bilder zur Authentifizierung. Dazu muss aus drei Bildersets je ein Bild gewählt werden, welches zusätzlich zu einem alphanumerischen Passwort dazu verwendet wird um sich zu authentifizieren.[NZI09] Auch hier könnten wieder Bilder aus dem persönlichen Kontext des Benutzers gewählt werden um anschließend die Bildersets zu generieren. Dadurch dass der Benutzer mit den Bildern mehr oder weniger vertraut ist, könnte es die Erinnerung des Benutzers an sein Passwort verbessern.

8. Anhang

I.Allgemeine Fragen

Alter: _____

Geschlecht: männlich [ ] weiblich [ ]

Studiengang/Beruf: _____

Welche Display-Sperre benutzen Sie?
[ ] Keine
[ ] Finger bewegen
[ ] Muster
[ ] PIN
[ ] Passwort

Man teilt unterschiedliche Informationen des alltäglichen Lebens (z.B. Urlaubspläne, Telefongespräche, etc.) mit unterschiedlichen Menschen. Nennen Sie Beispiele mit denen Sie die jeweiligen Informationen teilen würden:

Alle Informationen _____

Wichtige Informationen _____

Teil der Informationen _____

Keine Informationen _____

Hatten Sie schon Erfahrung mit grafischen Passwörtern? Ja [ ] Nein [ ]

Wie Häufig benutzen sie ihr Smartphone?

Sehr häufig Nie

Welche Dienste benutzen Sie auf Ihrem Smartphone?
Telefonieren [ ]
SMS [ ]
VideoChat/Skype [ ]
WhatsApp [ ]
Spielen [ ]
Social Media [ ]

II.Akzeptanz

1)Ich würde dieses System verwenden?

Stimme vollständig zu				Lehne vollständig ab

2)Ich würde Fragen zu SMS in folgenden Situationen verwenden?

Öffentlich:

Stimme vollständig zu				Lehne vollständig ab

Semi-Privat:

Stimme vollständig zu				Lehne vollständig ab

Privat:

Stimme vollständig zu				Lehne vollständig ab

3)Ich würde Fragen zu WIFI in folgenden Situationen verwenden?

Öffentlich:

Stimme vollständig zu				Lehne vollständig ab

Semi-Privat:

Stimme vollständig zu				Lehne vollständig ab

Privat:

Stimme vollständig zu				Lehne vollständig ab

4)Ich würde Fragen zu Anrufen in folgenden Situationen verwenden?

Öffentlich:

Stimme vollständig zu				Lehne vollständig ab

Semi-Privat:

Stimme vollständig zu				Lehne vollständig ab

Privat:

Stimme vollständig zu				Lehne vollständig ab

5)Ich würde Fragen zu Bildern in folgenden Situationen verwenden?

Öffentlich:

Stimme vollständig zu				Lehne vollständig ab

Semi-Privat:

Stimme vollständig zu				Lehne vollständig ab

Privat:

Stimme vollständig zu				Lehne vollständig ab

6)Ich würde Fragen zu Kontaktfotos in folgenden Situationen verwenden?

Öffentlich:

Stimme vollständig zu				Lehne vollständig ab

Semi-Privat:

Stimme vollständig zu				Lehne vollständig ab

Privat:

Stimme vollständig zu				Lehne vollständig ab

7)Ich würde Fragen zu GPS in folgenden Situationen verwenden?

Öffentlich:

Stimme vollständig zu				Lehne vollständig ab

Semi-Privat:

Stimme vollständig zu				Lehne vollständig ab

Privat:

Stimme vollständig zu				Lehne vollständig ab

8)Wie wichtig ist Ihnen ihre Privatsphäre?

Sehr wichtig				Gar nicht wichtig

9)Haben Sie Sicherheitsbedenken bezüglich der verwendeten Kontextinformationen (SMS, Bilder, etc)?

Bitte bewerten Sie ihre aktuelle Bildschirm-Sperre.

	1	2	3	4	5	6	7		
unverständlich	○	○	○	○	○	○	○	verständlich	1
kreativ	○	○	○	○	○	○	○	phantasielos	2
leicht zu lernen	○	○	○	○	○	○	○	schwer zu lernen	3
wertvoll	○	○	○	○	○	○	○	minderwertig	4
langweilig	○	○	○	○	○	○	○	spannend	5
uninteressant	○	○	○	○	○	○	○	interessant	6
schnell	○	○	○	○	○	○	○	langsam	7
originell	○	○	○	○	○	○	○	konventionell	8
gut	○	○	○	○	○	○	○	schlecht	9
kompliziert	○	○	○	○	○	○	○	einfach	10
herkömmlich	○	○	○	○	○	○	○	neuartig	11
unangenehm	○	○	○	○	○	○	○	angenehm	12
aktivierend	○	○	○	○	○	○	○	einschläfernd	13
ineffizient	○	○	○	○	○	○	○	effizient	14
übersichtlich	○	○	○	○	○	○	○	verwirrend	15
unpragmatisch	○	○	○	○	○	○	○	pragmatisch	16
aufgeräumt	○	○	○	○	○	○	○	überladen	17
attraktiv	○	○	○	○	○	○	○	unattraktiv	18
unsympathisch	○	○	○	○	○	○	○	sympathisch	19
konservativ	○	○	○	○	○	○	○	innovativ	20

Bitte bewerten Sie eine Bildschirm-Sperre die Kontext Informationen benutzt.

	1	2	3	4	5	6	7		
unverständlich	○	○	○	○	○	○	○	verständlich	1
kreativ	○	○	○	○	○	○	○	phantasielos	2
leicht zu lernen	○	○	○	○	○	○	○	schwer zu lernen	3
wertvoll	○	○	○	○	○	○	○	minderwertig	4
langweilig	○	○	○	○	○	○	○	spannend	5
uninteressant	○	○	○	○	○	○	○	interessant	6
schnell	○	○	○	○	○	○	○	langsam	7
originell	○	○	○	○	○	○	○	konventionell	8
gut	○	○	○	○	○	○	○	schlecht	9
kompliziert	○	○	○	○	○	○	○	einfach	10
herkömmlich	○	○	○	○	○	○	○	neuartig	11
unangenehm	○	○	○	○	○	○	○	angenehm	12
aktivierend	○	○	○	○	○	○	○	einschläfernd	13
ineffizient	○	○	○	○	○	○	○	effizient	14
übersichtlich	○	○	○	○	○	○	○	verwirrend	15
unpragmatisch	○	○	○	○	○	○	○	pragmatisch	16
aufgeräumt	○	○	○	○	○	○	○	überladen	17
attraktiv	○	○	○	○	○	○	○	unattraktiv	18
unsympathisch	○	○	○	○	○	○	○	sympathisch	19
konservativ	○	○	○	○	○	○	○	innovativ	20

III.Sicherheit

1)Bewerten Sie bitte die Sicherheit der einzelnen Kontext Informationen und die ihres jetzigen Systems.

SMS:

Sehr sicher				Sehr Unsicher

WIFI:

Sehr sicher				Sehr Unsicher

Anrufe:

Sehr sicher				Sehr Unsicher

Bilder:

Sehr sicher				Sehr Unsicher

Kontaktfotos:

Sehr sicher				Sehr Unsicher

GPS:

Sehr sicher				Sehr Unsicher

Eigenes System:

Sehr sicher				Sehr Unsicher

2)Denken Sie Gruppe 1 kennt die Antworten zu Fragen bezüglich folgender Daten?

SMS:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

WIFI:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Anrufe:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Bilder:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Kontaktfotos:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

GPS:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

3)Denken Sie Gruppe 2 kennt die Antworten zu Fragen bezüglich folgender Daten?

SMS:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

WIFI:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Anrufe:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Bilder:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Kontaktfotos:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

GPS:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

4)Denken Sie Gruppe 3 kennt die Antworten zu Fragen bezüglich folgender Daten?

SMS:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

WIFI:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Anrufe:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Bilder:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Kontaktfotos:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

GPS:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

5)Denken Sie Gruppe 4 kennt die Antworten zu Fragen bezüglich folgender Daten?

SMS:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

WIFI:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Anrufe:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Bilder:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Kontaktfotos:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

GPS:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

6)Kennt folgende Gruppe ihr aktuelles Passwort für Ihre Display Sperre?

Gruppe 1:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Gruppe 2:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Gruppe 3:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

Gruppe 4:

Ja	Wahrscheinlich	Vielleicht	Eher nicht	Nein

IV.Anwenderfreundlichkeit

1)Wie schwer ist es ihnen gefallen sich an die folgenden Dinge zu erinnern?

SMS:

Sehr einfach				Sehr schwer

WIFI:

Sehr einfach				Sehr schwer

Anrufe:

Sehr einfach				Sehr schwer

Bilder:

Sehr einfach				Sehr schwer

Kontaktfotos:

Sehr einfach				Sehr schwer

GPS:

Sehr einfach				Sehr schwer

2)Denken Sie, dass sie sich an die folgenden Daten nach einer Stunde erinnern können?

SMS:

Ja		Vielleicht		Nein

WIFI:

Ja		Vielleicht		Nein

Anrufe:

Ja		Vielleicht		Nein

Bilder:

Ja		Vielleicht		Nein

Kontaktfotos:

Ja		Vielleicht		Nein

GPS:

Ja		Vielleicht		Nein

3)Denken Sie, dass sie sich an die folgenden Daten nach einem Tag erinnern können?

SMS:

Ja		Vielleicht		Nein

WIFI:

Ja		Vielleicht		Nein

Anrufe:

Ja		Vielleicht		Nein

Bilder:

Ja		Vielleicht		Nein

Kontaktfotos:

Ja		Vielleicht		Nein

GPS:

Ja		Vielleicht		Nein

4)Denken Sie, dass sie sich an die folgenden Daten nach einer Woche erinnern können?

SMS:

Ja		Vielleicht		Nein

WIFI:

Ja		Vielleicht		Nein

Anrufe:

Ja		Vielleicht		Nein

Bilder:

Ja		Vielleicht		Nein

Kontaktfotos:

Ja		Vielleicht		Nein

GPS:

Ja		Vielleicht		Nein

5)Denken Sie, dass sie sich an die folgenden Daten nach einem Monat erinnern können?

SMS:

Ja		Vielleicht		Nein

WIFI:

Ja		Vielleicht		Nein

Anrufe:

Ja		Vielleicht		Nein

Bilder:

Ja		Vielleicht		Nein

Kontaktfotos:

Ja		Vielleicht		Nein

GPS:

Ja		Vielleicht		Nein

6)Hatten Sie Schwierigkeiten sich an die Daten zu erinnern? Wenn ja, an welche?

7)Kamen ihnen Fragen seltsam oder unlösbar vor? Wenn ja, welche?

8)Haben Sie sonstige Anmerkungen?

Literaturverzeichnis

[ACCLG02]
De Angeli, Antonella; Coutts, Mike; Coventry, Lynne; Johnson,Graham I. : VIP: a visual approach to user authentication, AVI '02 Proceedings of the Working Conference on Advanced Visual Interfaces,2002

[ASGS13]
Alt, Florian; Schneegass, Stefan; Girgis, Michael; Schmidt, Albrecht : Cognitive Effects of Interactive Public Display Applications, PerDis '13 Proceedings of the 2nd ACM International Symposium on Pervasive Displays, 2013

[AZE09] Aloul, Fadi; Zahidi, Syed; El-Hajj, Wassim : Two Factor Authentication Using Mobile Phones, AICCSA 2009. IEEE/ACS International Conference on Computer Systems and Applications, 2009

[B2004] V. A. Brennen, "Cryptography Dictionary," vol. 2005, 1.0.0 ed, 2004.

[BAS04] Bulling, Andreas; Alt, Florian; Schmidt, Albrecht : Increasing the Security of Gaze-Based Cued-Recall Graphical Passwords Using Saliency Masks, . Proceedings of 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing, 2004

[BB11] Bojinov,Hristo; Boneh, Dan : Mobile Token-Based Authentication on a Budget, HotMobile '11 Proceedings of the 12th Workshop on Mobile Computing Systems and Applications, 2011

[BJRSY06]
Brainard, John; Juels, Ari; Rivest, Ronald L.; Szydlo, Michael; Yung, Moti: Fourth-Factor Authentication: Somebody You Know, CCS '06 Proceedings of the 13th ACM conference on Computer and communications security, 2006

[BXYI09] Babic, Anitra; Xiong, Huijun; Yao, Danfeng;Iftode, Liviu :Building Robust Authentication Systems With Activity-Based Personal Questions, SafeConfig '09 Proceedings of the 2nd ACM workshop on Assurable and usable security, 2009

[CF05] Clarke, N.L.; Furnell, S.M.: Authentication of users on mobile telephones

e A survey of attitudes and practices,*Computers & Security*, Vol. 24, No. 7., 2005

[DGLBB10] Derawi, Mohammad O.; Gafurov, Davrondzhon; Larsen, Rasmus, Busch, Christoph; Bours, Patrick: Fusion of Gait and Fingerprint for User Authentication on Mobile Devices, 2010 2nd International Workshop on Security and Communication Networks (IWSCN), 2010

[DMR04] Davis, Darren; Monrose, Fabian; Reiter, Michael K. : On User Choice in Graphical Password Schemes, SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium,2004

[DP00] Dhamija, Rachna; Perrig, Adrian: D´ej`a Vu: A User Study Using Image for Authentication, SSYM'00 Proceedings of the 9th conference on USENIX Security Symposium ,2000

[FB08] Forget, Alain; Biddle, Robert : Memorability of Persuasive Passwords, CHI EA '08 CHI '08 Extended Abstracts on Human Factors in Computing Systems, 2008

[FZ10] Farmand, Samaneh; Bin Zakaria, Dr.Omar: Improving Graphical Password Resistant to Shoulder-Surfing Using 4-way Recognition-Based Sequence Reproduction (RBSR4), 2010 The 2nd IEEE International Conference on Information Management and Engineering (ICIME), 2010

[GFRAOT06] Galbally-Herrero, J.; Fierrez-Aguilar, J.; Rodriguez-Gonzalez, J. D.; Alonso-Femandez , F.; Ortega-Garcia, Javier; Tapiador, M. : Onthe Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks, Proceedings 2006 40th Annual IEEE International Carnahan Conferences Security Technology, 2006

[HHSP07] Hadid ,A.; Heikkild, J. Y.; Silven, .; Pietikdinen, M.: Face and Eye Detection for Person Authentication in mobile Phones, ICDSC '07. First ACM/IEEE International Conference on Distributed Smart Cameras, 2007.

[HIN04] Harada, Atsushi; Isarida, Takeo; Nishigaki , Masakatsu: A Proposal of User Authentication Using Mosaic Images, Joho Shori Gakkai Shinpojiumu Ronbunshu, 2004

[HJT07] Hallsteinsen, Steffen; Jørstad, Ivar; Thanh, Do Van: Using the mobile

phone as a security token for unified authentication, ICSNC 2007 Second International Conference on Systems and Networks Communications, 2007

[HP13] Henze, Niels; Pielot, Martin : App Stores: External Validity for Mobile HCI, interactions Volume 20 Issue 2, 2013

[HPPSB11] Henze, Niels; Pielot, Martin; Poppinga, Benjamin; Schinke, Torben; Boll, Susanne : My App is an Experiment: Experience from User Studies in Mobile App Stores, International Journal of Mobile Human Computer Interaction (IJMHCI)Volume 3, Issue 4, 2011

[KJJ09] Kunyu, Peng; Jiande, Zheng;Jing, Yang : An Identity Authentication System based on Mobile Phone Token, IC-NIDC 2009. IEEE International Conference on Network Infrastructure and Digital Content, 2009

[KPOH13] Klonovs , Juris; Petersen, Christoffer Kjeldgaard; Olesen, Henning;Hammershøj, Allan : ID Proof on the Go: Development of a Mobile EEG-Based Biometric Authentication System, Vehicular Technology Magazine, IEEE (Volume:8 , Issue: 1), 2013

[LHS08] Laugwitz,Bettina; Held, Theo; Schrepp, Martin : Construction and Evaluation of a User Experience Questionnaire, USAB '08 Proceedings of the 4th Symposium of the Workgroup Human-Computer Interaction and Usability Engineering of the Austrian Computer Society on HCI and Usability for Education and Work, 2008

[M56] Miller, G.A. : The magical number seven, plus or minus two: Some limits on our capacity for processing information. , Psychological Review 56, 1956

[MN09] Mcloughlin, I.V.; Naidu, N. : Keypress biometrics for user validation in mobile consumer devices, ISCE '09. IEEE 13th International Symposium on Consumer Electronics, 2009

[MTHTK10] Miyachi, Takao; Takahashi, Keita; Hasegawa, Madoka; Tanaka, Yuichi; Kato, Shigeo : A Study om Memorability and Shoulder-Surfing Robustness of graphical Password using DWT-based Inage Blending, Picture Coding Symposium (PCS), 2010

[NZI09] Nazir, Iffat; Zubair, Izzar; Islan, M Hasan: User Authentication for Mobile Device through Image Selection, 2009

Literaturverzeichnis

[NCRT06] Nosseir, Ann; Connor, Richard; Revie, Crawford; Terzis, Sotirios: Question-Based Authentication Using Context Data, NordiCHI '06 Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles, 2006

[NCD05] Nosseir, Ann; Connor, Richard; Dunlop, Mark D. :(2005) Internet authentication based on personal history - a feasibility test., Proceedings of Customer Focused Mobile Services Workshop at WWW2005, 2005

[Nie93] Nielsen, Jakob: Usability Engineering, Academic Press, 1993

[NS10] Nosseir, Ann; Terzis, Sotirios: A Study in Authentication via electronic personal History Questions, ICEIS 2010 - Proceedings of the 12th International Conference on Enterprise Information Systems, 2010

[SZD11] Sui, Yan; Zou, Xukai; Du, Eliza Yingzi : Biometrics-based authentication: a new approach, 2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), 2011

[THU10] Tang, Yujin; Hidenori, Nakazato; Urano, Yoshiyori :User Authentication on Smart Phones Using a Data Mining Method, 2010 International Conference on Information Society(i-Society), 2010

[TJFTJ08] Thanh, Do van; Jønvik, Tore; Feng, Boning; Thuan, Do van; Jørstad, Ivar : Simple Strong Authentication for Internet Applications using Mobile Phones, IEEE GLOBECOM 2008 IEEE Global Telecommunications Conference, 2008

[TK03] Takada, Tetsuji; Koike, Hideki : Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images, Human-Computer Interaction with Mobile Devices and Services Lecture Notes in Computer Science Volume 2795, 2003

[TOH06] Tari, Furkan; Ozok, A. Ant; Holden, Stephen H.: A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords, SOUPS '06 Proceedings of the second symposium on Usable privacy and security, 2006

[TSKMSB12] Trewin, Shari; Swart, Cal; Koved , Larry; Martino, Jacquelyn; Singh, Kapil; Ben-David, Shay : Biometric Authentication on a Mobile Device: A

Study of User Effort, Error and Task Disruption,ACSAC '12 Proceedings of the 28th Annual Computer Security Applications Conference, 2012

[TSK11] Tanvi, Parekh; Sonal, Gawshinde; Kumar, Sharma Mayank : Token Based Authentication using Mobile Phone, 2011 International Conference on Communication Systems and Network Technologies, 2011

[W77] Wood, HM: The use of passwords for controlled access to computer resources., National Bureau of Standards Special Publication 500e9. U.S Department of Commerce/NBS; 1977

[WWBBM05] Wiedenbeck, Susan; Waters, Jim; Birget, Jean-Camille; Brodskiy, Alex; Memon, Nasir : PassPoints: Design and longitudinal evaluation of a graphical password system, International Journal of Human-Computer Studies - Special isssue: HCI research in privacy and security is critical now, 2005

[WWBBM052] Wiedenbeck, Susan; Waters, Jim; Birget, Jean-Camille; Brodskiy, Alex; Memon, Nasir : Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice, SOUPS '05 Proceedings of the 2005 symposium on Usable privacy and security, 2005

[YBAG04] Yan, J.; Blackwell, A.; Anderson, R.; Grant, A. : Password memorability and security: empirical results, Security & Privacy, IEEE (Volume:2 , Issue: 5), 2004

[ZH90] Zviran, Moshe;Haga, William J. : Cognitive passwords: The key to easy access control, Computers & Security Volume 9, Issue 8, 1990

Abbildungsverzeichnis

Erklärung

Ich versichere, diese Arbeit selbstständig verfasst zu haben.
Ich habe keine anderen als die angegebenen Quellen benutzt und alle wörtlich oder sinngemäß aus anderen Werken übernommene Aussagen als solche gekennzeichnet.
Weder diese Arbeit noch wesentliche Teile daraus waren bisher Gegenstand eines anderen Prüfungsverfahrens.
Ich habe diese Arbeit bisher weder teilweise noch vollständig veröffentlicht.
Das elektronische Exemplar stimmt mit allen eingereichten Exemplaren überein.

Stuttgart, den 24. Juli 2013 _____