Shoulder-surfing resistente Authentisierung an mobilen Endgeräten

Shoulder-surfing resistant authentication on mobile devices

Bachelor-Thesis von Kristoffer Braun und Philipp Rack

Tag der Einreichung:

1. Gutachten: Prof. Dr. Melanie Volkamer
2. Gutachten: Dr. Karen Renaud
Betreuerin: Prof. Dr. Melanie Volkamer

TECHNISCHE UNIVERSITÄT DARMSTADT

Shoulder-surfing resistente Authentisierung an mobilen Endgeräten
Shoulder-surfing resistant authentication on mobile devices

Vorgelegte Bachelor-Thesis von Kristoffer Braun und Philipp Rack

1. Gutachten: Prof. Dr. Melanie Volkamer
2. Gutachten: Dr. Karen Renaud
Betreuerin: Prof. Dr. Melanie Volkamer

Tag der Einreichung:

Erklärung zur Bachelor-Thesis

Hiermit versichere ich, die vorliegende Bachelor-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 15.08.2014

(K. Braun)

Erklärung zur Bachelor-Thesis

Hiermit versichere ich, die vorliegende Bachelor-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 15.08.2014

_____

(P. Rack)

Acknowledgements

Unser Dank gilt Frau Professor Dr. Melanie Volkamer für die Betreuung der Arbeit, insbesondere für ihre hilfreichen Anmerkungen sowie Frau Dr. Karen Renaud für die Implementierung der Online-Studie. Wir bedanken uns ferner bei unseren Familien und Freunden für die Hilfe bei der Rekrutierung der Teilnehmer für unsere Studie sowie das Korrekturlesen der Arbeit. Dank schulden wir auch Viola Dienst für die Unterstützung bei der Analyse der Blickschutzfolie.

Zusammenfassung

Shoulder-Surfing ist bei mobilen Endgeräten ein zunehmendes Problem. Wenn ein Benutzer ein solches Gerät verwendet, könnte ihm nämlich ein (böswilliger) Angreifer dabei über die Schulter schauen und somit an sensible Daten gelangen. Sowohl im privaten alltäglichen Gebrauch als auch insbesondere im geschäftlichen Kontext könnte das zu erheblichen finanziellen Konsequenzen führen. Da die Beobachtung des Authentisierungsprozesses in der Praxis eine Hauptbedrohung darstellt, ist der Schutz davor das zentrale Thema dieser Arbeit. Mit den bei der Beobachtung gewonnenen Erkenntnissen kann sich der Angreifer, wenn er sich in den Besitz des Gerätes gebracht hat, Zugang zu sensiblen Daten und Dienstleistungen verschaffen. Ziel dieser Thesis ist daher die Analyse bereits existierender Authentisierungsverfahren und die Entwicklung eines shoulder-surfing resistenten Verfahrens.

Die hier vorgestellte Lösung, welche resistent gegen Shoulder-Surfing sein soll, basiert auf einer Kombination aus einer Blickschutzfolie und einem Authentisierungsverfahren, bei welchem sich bei jeder Authentisierung die Position der Zahlen beziehungsweise Bilder verändert. Aus der Position des Fingers des Benutzers lassen sich daher keine Rückschlüsse auf eine bestimmte Zahl oder ein bestimmtes Bild ziehen. Um diese Lösung zu evaluieren, wurden zwei verschiedene Studien durchgeführt, und zwar eine zur Wirksamkeit einer Blickschutzfolie sowie eine Online-Studie zum vorgeschlagenen Authentisierungsverfahren.

Zunächst wurde die Blickschutzfolie anhand mehrerer Szenarien getestet. Dabei hat sich gezeigt, dass sie einen ausreichenden Schutz bei bestimmten Szenarien bieten kann. Allerdings muss der Benutzer die Grenzen der Folien kennen und sich entsprechend verhalten. Aus diesem Grund enthält diese Arbeit einige Empfehlungen zur Benutzung der Folie.

Mit der Online-Studie wurde sowohl die Benutzerfreundlichkeit als auch die Akzeptanz des gewählten Authentisierungsverfahrens analysiert. Damit die verschiedenen Verfahren miteinander verglichen werden können, wurden drei Kriterien angelegt: Effizienz, Effektivität und Zufriedenheit. Sie wurde mit vier Gruppen zu je zwanzig Teilnehmern durchgeführt. Jede Gruppe verwendete ein anderes Authentisierungsverfahren. Zwei Gruppen wurden grafische Verfahren und zwei welche mit Zahlen zugeteilt. Allerdings wurden nur Verfahren betrachtet, die mindestens das gleiche Sicherheitslevel wie das Standard PIN-Verfahren aufweisen. Aus diesem Grund wurden jeweils vierstellige Codes verwendet und zwei Varianten mit zufällig angeordnete Eingabefeldern.

Die vorgeschlagene Lösung ist für den privaten alltäglichen Gebrauch zu aufwendig. Daher wird für diesen Bereich am Ende der Arbeit ein anderer Ansatz vorgeschlagen. Im geschäftlichen Kontext ist sie dagegen empfehlenswert, weil ein Smartphone hier typischerweise äußerst sensible Daten enthält und der zusätzliche Aufwand durch einen höheren Schutz aufgewogen wird.

Abstract

Shoulder surfing is an increasing problem as mobile devices become ubiquitous. When using such a device a malicious attacker could observe the process by looking over the user's shoulder and could gain sensitive information. Such an event, in terms of both personal and business use, could lead to significant financial loss. Since the observation of the authentication secret is a major threat, preventing it is the main subject of this thesis. With the knowledge obtained from the observation, and the user's device, the thief is able to access all data and services on the device. The goal of this research is therefore the analysis of existing authentication mechanisms and the development of a shoulder-surfing resistant one.

The proposed solution, which should be shoulder surfing resistant, is based on a combination of a privacy screen protector and an obfuscation mechanism. The proposal is to make the positions of the numbers in the input field dynamic rather than static, with the position of the numbers or pictures changing every time the user authenticates him or herself. The secret is thus independent of the user's finger position. To evaluate the solution two different studies were carried out: the first using a privacy screen protector and the second relying on an online study.

The privacy screen protectors were analyzed by developing several scenarios and testing a selection of protectors. The study showed that such privacy screen protectors can indeed provide protection for the given scenarios. However, the user should be aware of the limits of the protectors so that they can behave accordingly. Therefore this thesis includes a list of recommendations to inform such usage.

A user study was conducted to analyze the feasibility of the proposed obfuscation authentication mechanism. In order to compare the different authentication schemes, three criteria were developed: efficiency, effectiveness and satisfaction. The study consisted of four groups in total with twenty participants each. Each group interacted with a different authentication mechanism: two groups received picture codes and two were issued with numerical codes. This thesis only considers mechanisms with the same security level as the traditional PIN method. To achieve this, four digit codes were used and two mechanisms with randomly placed input fields.

The authors conclude that the proposed mechanism would not be suitable for private daily usage, and explain why they came to this conclusion. An approach that might be more appropriate for personal use is presented in the end of the thesis. However, the proposed solution is indeed appropriate in a business context where a smartphone typically contains highly sensitive data and the extra effort will be offset by the extra protection gained.

Inhaltsverzeichnis

1 Einleitung

In den vergangenen Jahren haben Smartphones einen immer größer werdenden Einfluss auf das tägliche Leben gewonnen [GMM13][Cis14]. Während Handys nur zum Versenden von Kurznachrichten oder Anrufen verwendet wurden, bieten Smartphones heutzutage eine Vielzahl von Möglichkeiten, einerseits durch den Fortschritt der Technik, andererseits durch die immer größer werdende Anzahl an Apps. Durch diese ist es mit dem Smartphone inzwischen nicht nur möglich, Fotos zu machen oder im Internet zu surfen, sondern auch Online-Banking zu betreiben oder sogar zu bezahlen[1]. Angetrieben von dieser Entwicklung ersetzen Smartphones im täglichen Leben teilweise schon den Computer. Anders als dieser bietet die aktuelle Smartphonegeneration nicht nur Kameras auf der Vorder- und Rückseite. Auch die Anzahl genutzter Sensoren, wie beispielsweise GPS, die den aktuellen Standort des Benutzers messen, sowie Beschleunigungsmesser und Magnetometer, nimmt zu. Diese Entwicklung hat zur Folge, dass immer mehr private Daten auf dem eigenem Smartphone gespeichert werden. Entsprechend bergen diese neuen technischen Möglichkeiten auch eine Vielzahl von Risiken, insbesondere, da der Benutzer das Smartphone, anders als den Computer, meistens bei sich trägt. Sollten diese Daten in die Hände von Kriminellen geraten, kann großer finanzieller, aber auch persönlicher Schaden entstehen. Aus diesem Grund wird der Schutz dieser Daten immer wichtiger.

1.1 Motivation

Eine geeignete Methode, um die Daten zu schützen, ist ein Authentisierungsverfahren in Kombination mit der Bildschirmsperre. Bei einem solchen Verfahren muss sich der Benutzer erst authentisieren, um auf die eigentlichen Funktionen des Smartphones zugreifen zu können, beispielsweise Apps, die mit privaten Daten interagieren. Unkritische Funktionen, wie Uhrzeit und seit einiger Zeit auch Apps wie zum Beispiel die Foto-App, sind dagegen ohne Authentisierung vom Sperrbildschirm aus nutzbar. Dieses Authentisierungsverfahren soll verhindern, dass ein Angreifer in einem unbeobachteten Moment oder bei Diebstahl des Smartphones an die privaten Daten gelangt. Dabei authentisiert sich der Benutzer an einem System, welches diesen wiederum authentifiziert. Dieser kann sich dabei entweder durch Wissen, bloßen Besitz, durch ein biometrisches Merkmal oder einer Kombination dieser Ansätze authentisieren.

Authentisierung durch **Wissen** existiert schon sehr lange, beispielsweise als PIN bei einem Geldautomaten und wurde dann auch für Smartphones übernommen. Durch die vielfältige Nutzung von Accounts an Computern und im Internet hat sich auch die Nutzung von Passwörtern durchgesetzt. Während eine PIN (*Personal Identification Number*) nur aus Zahlen besteht (siehe näher unter Kapitel 2.1), gibt es bei Passwörtern durch die zusätzliche Auswahl von Buchstaben und Sonderzeichen viel mehr Möglichkeiten, was die Sicherheit erhöht. Bei Android-Smartphones ist es außerdem möglich, sich mit Hilfe eines Musters (*unlock pattern*) zu authentisieren.

Im letzten Jahr (2013) wurde mit der Vorstellung des IPhone 5s insbesondere die Authentisierung durch **biometrische Merkmale** populär. Während es bereits seit einigen Jahren möglich ist, sich durch ein so genanntes „Face Unlock“-Verfahren bei Android-Geräten zu authentisieren, bietet das neue IPhone die Möglichkeit, den eigenen Fingerabdruck zu benutzen. Seit der Einführung verwenden auch andere Hersteller diesen Sensor bei ihren Smartphones. Alle Geräte haben jedoch die Gemeinsamkeit, dass

[1] Google Wallet: https://www.google.com/wallet/ (abgerufen am 12.06.2014)

sie nur im hohen Preissegment verfügbar sind. Verfahren, die auf körperlichen Merkmalen basieren, sind jedoch nicht nur sicherheitstechnisch bedenklich. Beide Verfahren, Authentisierung durch Gesichtserkennung beziehungsweise Fingerabdruck, haben einerseits Probleme mit false-positive- und false-negative-Erkennung. Andererseits stellen sie ein Sicherheitsrisiko aufgrund von Überlistung durch Fotos bei der Gesichtserkennung [Mus12], beziehungsweise wegen unbemerkt genommenen Fingerabdrücken bei der Fingerabdruckerkennung [Clu13] dar. Insbesondere seit dem letzten Jahr rückt auch der Datenschutz in den Vordergrund und die Angst, auf diese Weise die eigenen biometrischen Daten an große Firmen weiterzugeben, da sie ein eindeutiges Identifizierungsmerkmal darstellen. Wegen der genannten Probleme und da die Fingerabdruckerkennung nur bei teuren Smartphones verfügbar ist, sind diese Authentisierungsverfahren wenig verbreitet.

Verfahren mit Authentisierung durch **Besitz** existieren bei aktuellen Smartphonebetriebssystemen nicht. Jedoch wurde auf der Google I/O 2014[2] ein Verfahren vorgestellt, bei dem sich ein Benutzer, sofern er in diesem Moment eine Smartwatch trägt, die mit dem Smartphone verbunden ist, durch Tragen der Uhr authentisiert. Dabei genügt es, dass sich die Uhr in nächster Nähe des Benutzers befindet und per Bluetooth mit dem Gerät verbunden ist.

Da zur Zeit eine Authentisierung durch Biometrie mit hohen Kosten verbunden ist und es für Authentisierung durch Besitz noch kein verfügbares Verfahren gibt, ist das am weitesten verbreitete Verfahren Authentisierung durch Wissen. Allerdings ist festzustellen, dass viele Menschen überhaupt keine Authentisierung verwenden.

Ein großes Problem, was die oben genannten Authentisierungsverfahren betrifft, die auf Wissen basieren, ist das so genannte Shoulder-Surfing [TOH06]. Dabei versucht ein Angreifer dadurch Informationen zu erhalten, dass er dem Benutzer über die „Schulter schaut“, siehe Abbildung 1. Dieses Verfahren wird insbesondere oft verwendet, um an PINs oder Passwörter zu kommen. Sollte es ein Angreifer also schaffen, die PIN des Benutzers mitzulesen, kann das ernsthafte Konsequenzen für diesen haben. Es stellt eine besonders große Gefahr dar, da vielen Benutzern dieses Risiko unbekannt ist und sie sehr leichtsinnig mit ihrer Authentisierung umgehen [Sec12]. Des Weiteren gibt es Situationen bei denen der Benutzer seine Authentisierung auch gegenüber vertrauten Personen nicht offenlegen möchte. Dies ist ein eher sozialer Aspekt, da der Benutzer durch Abwenden des Smartphones nicht unhöflich wirken möchte. Obwohl sie ein ähnliches Sicherheitsmerkmal wie die PIN für den Geldautomaten darstellt, achten viele bei der Authentisierung am Smartphone nämlich nicht darauf, den Vorgang zu verdecken, wie sie es bei einem solchen tun würden.

Das Ziel des genannten Angriffs ist, nach erfolgreichem Shoulder-Surfing des Authentisierungsverfahrens, sich Zugang zu den Daten des Benutzers zu verschaffen entweder durch die kurzzeitige und unbemerkte Verwendung des Smartphones durch den Angreifer oder den Diebstahl des Gerätes. Bis der Benutzer den Angriff bemerkt und den Zugang über das Internet sperren lässt, kann der Angreifer versuchen, an die gewünschten Informationen zu gelangen und im ungünstigsten Fall sogar den Sperrmechanismus deaktivieren. In diesem Fall ist ein nachträgliches Sperren wirkungslos. Ein erfolgreicher Angreifer kann sich als Benutzer ausgeben und so Informationen bekommen und sozialen Schaden (zum Beispiel Bloßstellung) oder durch den Zugriff auf gespeicherte Konten auch finanziellen Schaden anrich-

[2] Google IO 2014: https://www.google.com/events/io

ten, da bei vielen Benutzern die Anmeldeinformationen für Onlinedienste auf dem Gerät automatisch gespeichert werden.

Dieser Angriff ist insbesondere bei Firmensmartphones beziehungsweise privaten Geräten, die für geschäftliche Zwecke verwendet werden, sehr gefährlich. Ein Angreifer, der Zugriff auf Firmeninterna hat, kann großen finanziellen Schaden verursachen, beispielsweise durch die Veröffentlichung von Interna oder den Verkauf von Firmengeheimnissen an die Konkurrenz. Bei diesen sehr wertvollen Daten ist es deshalb besonders wichtig, dass das verwendete Authentisierungsverfahren vor Shoulder-Surfing schützt.

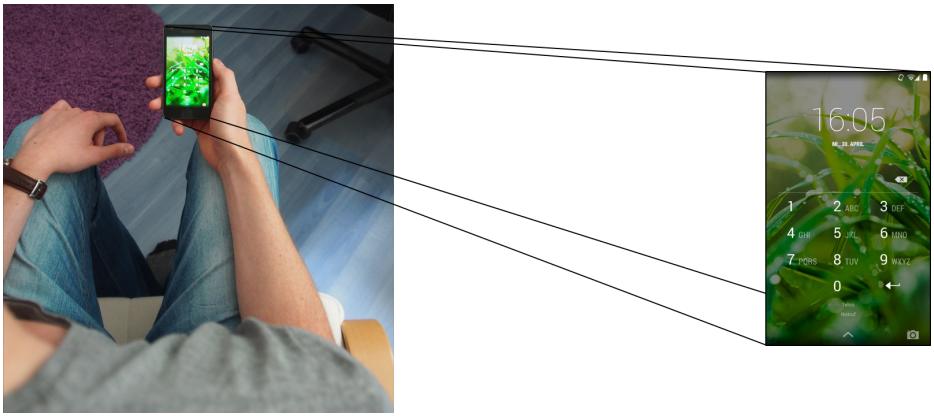


Abbildung 1: Beispiel Shoulder-Surfing

Abgesehen von den oben genannten Authentisierungsverfahren, gibt es noch weitere Möglichkeiten, sich gegen externe Angreifer zu schützen, zum Beispiel durch Vermeidung oder Verschlüsselung von Daten. Vermeidung bedeutet, dass der Benutzer versucht, möglichst wenige private Daten auf dem Smartphone zu speichern. Dies ist jedoch für die wenigsten Benutzer eine zufriedenstellende Lösung, da sie ihr Smartphone genau aus dem Grund besitzen, um möglichst viel damit zu erledigen. Gerade die vorinstallierten Apps, wie zum Beispiel eine E-Mail- oder Kalender-App, beinhalten bereits private Daten. Die zweite Möglichkeit, Verschlüsselung, dient als zusätzliche Absicherung zu dem bereits verwendeten Authentisierungsverfahren. Verschlüsselung soll dazu beitragen, dass die Daten bei Ausbau des Speichers sicher vor unbefugtem Auslesen sind. Der Nachteil ist, dass bei Android der bei der Verwendung der Verschlüsselung genutzte PIN beziehungsweise das genutzte Passwort dem des Authentisierungsverfahrens entspricht. Der Benutzer muss daher bei jedem Entsperren des Smartphones das Passwort erneut eingeben, was bei einem sicheren Passwort und der häufigen Authentisierung viel Zeit benötigt. Ein sicheres Passwort besteht nach Auffassung des Bundesamts für Sicherheit in der Informationstechnik (BSI) aus einer mindestens zwölfstelligen Buchstaben- und Zahlenkombination[3]. Sollte das Passwort vergessen werden, ist es für den durchschnittlichen Benutzer nicht möglich, die Daten wiederherzustellen, was einige abschrecken dürfte [Sym09]. Dennoch ist auch dieses Verfahren unter Umständen nicht vollkommen sicher gegen den Zugriff durch Unbefugte [MS13].

[3] BSI zum Thema Passwörter: https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html (abgerufen am 26.06.2014)

1.2 Ziel

Das Ziel dieser Arbeit ist die Entwicklung eines Verfahrens, das resistent gegen Shoulder-Surfing bei mobilen Endgeräten ist. Dabei geht es nicht nur um das „Über-die-Schulter-Schauen“ im wörtlichen Sinn sondern auch um vergleichbare kritische Situationen, bei denen der Angreifer versucht die Authentisierung zu beobachten, zum Beispiel wenn Angreifer und Benutzer nebeneinander sitzen oder sich gegenüber stehen. Dieses Verfahren soll sowohl praktikabel sein als auch möglichst große Sicherheit bieten.

Die Zielgruppen sind einerseits Unternehmen, die hohen Wert auf die Sicherheit der gespeicherten Daten legen, andererseits sicherheitsbewusste Privatpersonen, die sich gegen den oben genannten Angriff schützen möchten. Es geht also primär nicht darum, Personen, die bisher kein Interesse an einem solchen Verfahren haben, von einer Verwendung eines solchen zu überzeugen.

Das zu entwickelnde Verfahren soll mit dem klassischen PIN-Verfahren vergleichbar sein, also mindestens genauso sicher. Außerdem soll es dem Benutzer helfen Fehler zu vermeiden und damit seine Zufriedenheit steigern. Schließlich soll es effizient genug sein, um es täglich zu nutzen.

1.3 Aufbau

In Kapitel 2 wird der Angreifer beschrieben. Dabei wird erklärt, welche Fähigkeiten und Möglichkeiten er hat, um das Authentisierungsverfahren herauszufinden. Außerdem werden die Kriterien aufgestellt, die ein entwickeltes Verfahren im Hinblick auf Benutzerfreundlichkeit und Alltagstauglichkeit aufweisen muss. In Kapitel 3 geht es zunächst um Verfahren von Autoren, die eine Methode gegen Shoulder-Surfing entwickelt haben. Diese Verfahren werden anschließend anhand der Kriterien aus Kapitel 2 evaluiert. Im zweiten Teil dieses Kapitels wird das selbst entwickelte Verfahren vorgestellt und ebenso anhand der Kriterien evaluiert. In Kapitel 4 werden zwei Blickschutzfolien analysiert, welche bei dem selbst entwickelten Verfahren eine wichtige Rolle spielen. Gegenstand des Kapitels 5 ist das Studiendesign und die Durchführung einer Online-Studie, bei der das entwickelte Verfahren evaluiert wird. Kapitel 6 betrifft Veröffentlichungen, die sich mit ähnlichen Verfahren beschäftigen, und in Kapitel 7 wird schließlich der Inhalt dieser Arbeit zusammengefasst und ein Ausblick auf Ideen für zukünftige Studien mit ähnlichen Themen gegeben.

2 Kriterien für shoulder-surfing resistente Authentisierung

In diesem Kapitel werden Kriterien ausgewählt, die ein Authentisierungsverfahren, welches vor Shoulder-Surfing schützt, erfüllen sollte. Da, wie in Kapitel 1 beschrieben, Authentisierung durch Biometrie mit zahlreichen Problemen verbunden und Authentisierung durch Besitz noch nicht beim Smartphone noch nicht verfügbar ist, beschränkt sich diese Arbeit auf Authentisierung durch Wissen. Die Kriterien werden in die Kategorien Sicherheit und Praktikabilität gegliedert, welche auf Verfahren, die auf Wissen basieren, anwendbar sind. Sie werden im folgenden Kapitel vorgestellt.

2.1 Sicherheit

Beim Thema Sicherheit werden zwei Akteure unterschieden: Einerseits der Benutzer, der sich an seinem Smartphone authentisiert, andererseits der Angreifer, der versucht, diesen Vorgang zu beobachten. Ziel dieser Beobachtung ist, genügend Informationen zu gewinnen, um sich selbst anstelle des Benutzers erfolgreich authentisieren zu können. Dadurch ist es dem Angreifer möglich, die Vertraulichkeit hinsichtlich der auf dem Smartphone gespeicherten privaten Daten zu brechen.

Vor einigen Jahren besaß ein Angreifer nur die Möglichkeit, den Authentisierungsvorgang mit eigenen Augen zu beobachten. Damit stellte die Fähigkeit des Angreifers, sich etwas zu merken, die Grenzen der Informationsgewinnung dar. Inzwischen besteht durch Wearables, wie beispielsweise Google Glass[4] oder auch Smartwatches wie beispielsweise die Galaxy Gear[5] von Samsung, die Möglichkeit, das Gesehene unbemerkt in HD-Qualität zu filmen. Aus diesem Grund existieren diese Grenzen inzwischen nicht mehr, da der Angreifer das Video beliebig oft anschauen und automatisch auswerten kann. Die Aufgabe des Angreifers besteht heutzutage viel mehr darin, eine geeignete Position zu finden, um den Bildschirminhalt während der gesamten Authentisierung filmen zu können. Im Folgenden wird davon ausgegangen, dass der Angreifer immer die Möglichkeit hat, das Gesehene zu filmen, da dies für den Benutzer den ungünstigsten Fall darstellt. Diese Arbeit beschränkt sich auf die Konstellation, dass der Angreifer nur das filmen kann, was er mit seinen eigenen Augen sehen kann. Situationen in denen er, durch die günstige Platzierung von Kameras oder Wearables, mehr filmen als sehen kann, bleiben unberücksichtigt. Denn ein solches Vorgehen ist äußerst auffällig oder mit ausgiebigen Vorbereitungen verbunden, wodurch es als nicht praktikabel für alltägliche Situationen gilt. Des Weiteren wird davon ausgegangen, dass ein Benutzer in diesem Fall nicht durch Verdecken des Displays versucht, sich vor Shoulder-Surfing zu schützen, weil er beispielsweise von anderen Personen oder der Verwendung des Smartphones abgelenkt wird und nicht auf seine Umgebung achtet. Nach erfolgreichem Shoulder-Surfing des Authentisierungsverfahrens, versucht der Angreifer das Smartphone entweder kurzzeitig und unbemerkt zu verwenden oder es dauerhaft zu entwenden, um auf die privaten Daten zugreifen zu können.

Die Sicherheit eines Authentisierungsverfahrens wird durch das **Sicherheitslevel** beschrieben. Dieses muss anspruchsvoll sein, damit es nicht von einem potentiellen Angreifer erraten werden kann. Als Vergleichswert soll das Sicherheitslevel eines bereits bestehenden Verfahrens dienen. Bei Android ist die Authentisierung mit Hilfe des Musters (*pattern unlock*), der PIN oder eines Passwortes üblich. Da nach Wahrnehmung der Autoren die Authentisierung mit Hilfe der PIN am weitesten verbreitet und das Muster

[4] Google Glass: https://www.google.com/glass/start/ (abgerufen am 26.06.2014)

[5] Galaxy Gear: https://www.samsung.com/at/consumer/mobile-phone/wearables/galaxy-gear/ (abgerufen am 26.06.2014)

anfällig gegen so genannte „Smudge“-Angriffe [Zez+13] ist, wird die PIN als Vergleichswert verwendet. Dabei ist zu beachten, dass die Sicherheit eines Verfahrens welches diesem Kriterium genügt, mindestens genauso hoch sein muss wie das der PIN.

Dabei soll in dieser Arbeit die ursprüngliche Definition der PIN verwendet werden, wonach sie aus mindestens vier Ziffern besteht. Da die PIN von IPhones, Android-Smartphones und auch die des Geldautomaten standardmäßig auf mindestens vier Stellen eingestellt ist, wird dieser Wert als Vergleichswert für das Sicherheitslevel festgelegt. Der theoretische Passwortraum (*theoretical password space*) beträgt damit $10^4 = 10000$. Das bedeutet, dass es bei einer vierstelligen PIN 10000 verschiedene mögliche Passwortkombinationen gibt, das entspricht 13.3 Bits. Es wird davon ausgegangen, dass die verwendete PIN sicher ist und Shoulder-Surfing die einzige Möglichkeit des Angreifers darstellt, an die PIN des Benutzers zu gelangen. Damit werden solche ausgeschlossen, die durch Erraten einer bekannten Kombination, wie zum Beispiel dem Geburtstag, herausgefunden werden können.

2.2 Praktikabilität

Die Praktikabilität eines jeden Authentisierungsverfahrens trägt maßgeblich zur Bereitschaft des Benutzers bei, ein solches Verfahren im alltäglichen Gebrauch zu verwenden. Ein Verfahren, welches einerseits zwar vor vielen Gefahren schützt, andererseits jedoch sehr umständlich und schwer zu erlernen ist, hat bei den wenigsten Benutzern eine aussichtsreiche Zukunft. Um die Praktikabilität eines Verfahrens herauszufinden, spielt der Nutzungskontext eine große Rolle. Aus diesem Kontext können Kriterien abgeleitet werden, anhand derer die Praktikabilität im Sinne von Benutzerfreundlichkeit festgestellt werden kann.

Der Nutzungskontext des Authentisierungsverfahrens am Smartphone ist völlig anders verglichen mit dem eines Geldautomaten. Während der Geldautomat im Extremfall zwei bis drei Mal am Tag verwendet wird, schauen Benutzer eines Smartphones, so der ehemaligen Nokia Manager und Inhaber eines Consulting Unternehmens Tomi Ahonen, durchschnittlich etwa 150 Mal am Tag auf ihr Gerät [Aho13], abzüglich der Anzahl von Funktionen, die ohne Authentisierung verwendbar sind. Aus diesem Verhalten lässt sich das erste Kriterium für die Praktikabilität ableiten, nämlich die **Effizienz**. Effizienz wird, im Kontext einer Authentisierung, allgemein als Zeitdauer definiert, die ein Benutzer benötigt, um sich zu authentisieren. Für die Authentisierungszeit wird die Definition aus der Arbeit von Zezschwitz, Koslow et al. verwendet. Dabei wird zwischen der Zeit für die Orientierung und der Eingabezeit unterschieden [Zez+13]. Die Orientierungszeit ist die Dauer zwischen Beginn der Authentisierung und der ersten Handlung des Benutzers, zum Beispiel das Drücken eines Buttons. Die Eingabezeit ist die Dauer die für die Eingabe des PINs benötigt wird, zwischen der ersten und der letzten Handlung des Benutzers. Da das Sicherheitslevel der PIN als Vergleich gewählt wurde, wird ein Vergleichswert für die Authentisierungszeit benötigt. Ein geübter Benutzer benötigt nach Auffassung von Roth für die Authentisierung mit einer vierstelligen PIN durchschnittlich etwas mehr als eine Sekunde [RR06].

Ein Benutzer, der sich, wie oben beschrieben, täglich sehr oft authentisiert, möchte bei der Anwendung des Verfahrens nur wenig Fehler beim Eingeben machen. Daraus ergibt sich das zweite Kriterium für die Praktikabilität, nämlich die **Effektivität**. Effektivität beschreibt, wie viele Fehler ein Benutzer bei einer bestimmte Aufgabe mit einem bestimmten Verfahren machen darf. Diese wird anhand der Erfolgsquote gemessen, das heißt wie oft sich ein Benutzer korrekt und ohne Fehler authentisiert [Sch+13].

Ein geübter Benutzer macht laut Roth bei der Eingabe einer vierstelligen PIN durchschnittlich keinen Fehler [RR06].

Das dritte Kriterium für die Praktikabilität des Verfahrens ist seine **Eignung für ein Smartphone-display**. Da das Display eines Smartphones, anders als das eines Computers, sehr klein ist, ist nicht jedes Authentisierungsverfahren dafür geeignet. Ein geeignetes Verfahren muss auf diesem Display gut sichtbar, sowie mit Hilfe eines Touchscreens bedienbar sein. Gleichzeitig darf es die Funktionalität des Verfahrens nicht einschränken.

Das vierte und letzte Kriterium für die Praktikabilität ist die **Marktverfügbarkeit**. Darunter ist ein Verfahren zu verstehen, das bislang nur theoretisch beschrieben wurde und daher noch nicht auf dem Markt verfügbar ist. Aus diesem Grund wird dieser Aspekt in dieser Arbeit nicht behandelt. Das Gleiche gilt für Verfahren, die noch sehr teuer sind und wegen ihrer geringen Marktverfügbarkeit im Alltag nicht verwendet werden.

3 Vorschlag für eine shoulder-surfing resistente Lösung

Im Rahmen dieser Arbeit wird eine Kombination einer Blickschutzfolie mit einem positionsunabhängigen Authentisierungsverfahren vorgeschlagen und analysiert. Die Blickschutzfolie soll verhindern, dass ein Angreifer, der sich in der Nähe des Benutzers befindet, den Inhalt des Displays erkennen kann. Außerdem ergibt sich bei Verwendung einer solchen Folie ein weiteres Kriterium, die **Positionsunabhängigkeit**. Damit ist gemeint, dass ein Verfahren nur dann ein Höchstmaß an Sicherheit gewährt, wenn es nicht nur beim direkten Blick auf das Display Schutz bietet, sondern auch dann, wenn der Angreifer beim Shoulder-Surfing nur die Bewegung der Finger des Benutzers beobachten kann. Sofern sich die Authentisierung, beispielsweise durch Veränderung des sichtbaren Inhaltes, bei jeder Verwendung ändert, ist es dem Angreifer nicht möglich, das Verfahren ohne Sicht auf das Display zu erkennen. Vor kurzem wurde bei der Blackhat 2014[6] ein Verfahren mit Google Glass vorgestellt, das dem Entwickler ermöglicht, die Zahlenkombination zu rekonstruieren ohne den Inhalt des Displays zu sehen[7].

Im folgenden Kapitel wird beschrieben, aus welchem Grund zwei bestimmte Folien ausgewählt wurden. Sie werden anschließend im Einzelnen vorgestellt. In Kapitel 3.2 geht es um Authentisierungsverfahren, die in anderen Veröffentlichungen zu diesem Thema entwickelt wurden und ebenfalls das Kriterium der Positionsunabhängigkeit erfüllen. Kapitel 3.3 enthält schließlich einen eigenen Vorschlag welcher hinsichtlich Sicherheit in Kapitel 4 und Praktikabilität in Kapitel 5 getestet wird.

3.1 Auswahl geeigneter Blickschutzfolien

Eine Blickschutzfolie soll die Privatsphäre eines Benutzers schützen, indem sie verhindert, dass ein Angreifer gegen den Willen des Benutzers den Displayinhalt seines Smartphones oder Laptops mitlesen kann. Dieser Schutz wird durch die Beschränkung des Blickwinkels erreicht, in dem der Displayinhalt noch sichtbar ist. Außerhalb dieses Winkels nimmt ein Beobachter das Display als ausgeschaltet wahr, da das Display für ihn dunkel aussieht.

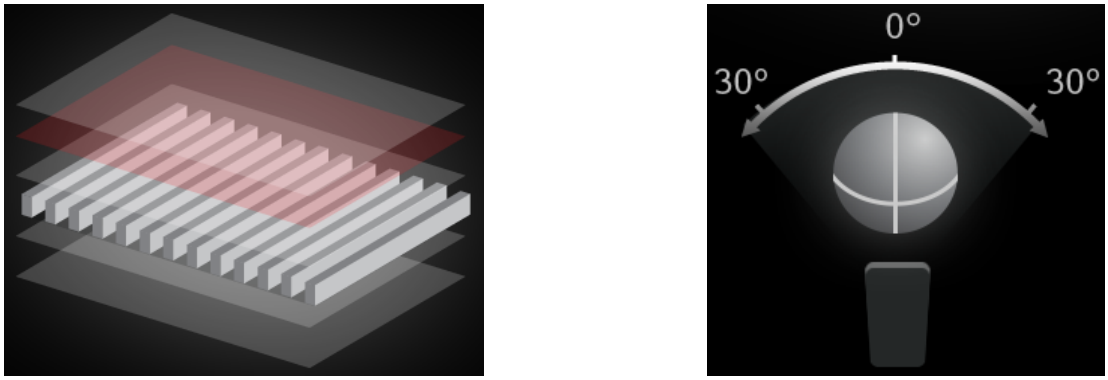
Bei der Auswahl der Folien ist der **Blickschutzwinkel** das wichtigste Kriterium, um eine geeignete Folie zu finden. Je kleiner der Blickwinkel ist, in welchem der Inhalt des Displays sichtbar wird, um so größer ist der Schutz vor Shoulder-Surfing.

Ein weiteres Kriterium ist das der Benutzer durch die Folie nicht beeinträchtigt wird, worunter die **Handhabbarkeit** im Alltag leiden würde. Denn die Folie soll dem Benutzer zwar einen größeren Schutz bieten, aber nicht die gesamte Lösung unpraktikabel machen. Die Handhabbarkeit kann anhand der Qualität der Folien gemessen werden, die sich aus einer optimalen Anbringung, der Veränderung der Sichtbarkeit und der Reaktion des Touchscreens zusammensetzt.

Bei der eigenen Online-Recherche hat sich herausgestellt, dass sehr viele Hersteller wenig oder sogar gar keine Spezifikationen ihrer Blickschutzfolien angeben. Aus diesem Grund wurden bei den Herstellern diese Details angefragt. Hersteller, die weder Informationen auf der entsprechenden Webseite der Folie angeben, noch nach mehreren Wochen auf E-Mails reagiert haben, wurden bei der weiteren Auswahl nicht betrachtet. Zur Auswahl standen: Slabo Blickschutzfolie, Copter Privacy Screen, NEU Privacy Filter LCD Folie, Somikon Privacy-Display-Schutzfolie, Belkin Rundum-Blickschutzfolie und Horny Pro-

[6] Blackhat 2014: https://www.blackhat.com/ (abgerufen am 12.08.2014)

[7] My Google Glass sees your passwords!: https://www.blackhat.com/us-14/briefings.html#my-google-glass-sees-your-passwords (abgerufen am 12.08.2014)



(a) Aufbau **(b)** Blickwinkel

Abbildung 2: Copter-Folie [Quelle: http://copter.com/]

tectors Sichtschutz Privacy. Die Entscheidung fiel schließlich auf eine Folie des Herstellers Belkin und eine des Herstellers Copter. Die Lösung von Belkin wurde aufgrund ihrer besonderen Eigenschaft des 360°-Blickschutzes und der Tru Clear™-Technologie, die trotz Folie für einen gut sichtbaren Displayinhalt sorgen soll, ausgewählt. Außerdem lässt eine Herstellergarantie von 30 Jahren eine gute Qualität erwarten. Die Folie besitzt einen Blickwinkel von 30° - unabhängig von der Ausrichtung des Smartphones. Detaillierte Abbildungen gibt es im Internet allerdings nicht. Der Preis dieser Blickschutzfolie lag bei der Bestellung bei 23,98€ zuzüglich Versand.

Die Folie des Herstellers Copter (Copter™PrivacyFilter), welcher sich auf diese Art von Folien spezialisiert hat, wurde aufgrund der ausführlichen Informationen des Herstellers ausgewählt. Auf seiner Webseite[8] erklärt der Hersteller die Funktionsweise der Folie sehr genau, siehe Abbildung 2a, und gibt auch detailliert die Blickwinkel an. Der Winkel liegt bei dieser Folie bei 30°, wenn das Smartphone im Portrait-Modus (Hochformat) verwendet wird und bei 60° im Landscape-Modus (Querformat), siehe Abbildung 2b. Der Preis dieser Blickschutzfolie lag bei der Bestellung bei 33€ zuzüglich Versand.

3.2 Analyse existierender Authentisierungsverfahren

In diesem Kapitel werden Verfahren vorgestellt, die das beschriebene Kriterium der Positionsunabhängigkeit erfüllen und mit Hilfe der Blickschutzfolie eine potentielle Lösung gegen Shoulder-Surfing darstellen. Die genannten Verfahren werden anhand der Kriterien (Sicherheit, Praktikabilität) aus Kapitel 2 miteinander verglichen und auf Abweichungen überprüft. Sobald eines der Kriterien nicht erfüllt ist, wird dieses Verfahren im weiteren Verlauf der Arbeit nicht weiter betrachtet. Andere Verfahren, die auch potentiell shoulder-surfing resistent sind, aber auch ohne Folie Schutz bieten, werden in Related Work in Kapitel 6 vorgestellt.

Cognitive trapdoor game

Das Verfahren wurde von Roth und Richter [RR06] entwickelt und existiert in *zwei* Varianten, die im Folgenden beschrieben werden. Bei beiden Verfahren werden Eingabefelder mit den Zahlen null bis neun verwendet, die wie bei dem Tastenfeld eines Geldautomaten angeordnet sind.

[8] Webseite Copter: http://copter.com/

Immediate oracle choice variant: Bei diesem Verfahren werden die einzelnen Zahlenfelder, siehe Abbildung 3, nach dem Zufallsprinzip entweder schwarz oder weiß eingefärbt, ohne jedoch ihre Position zu verändern. Damit die Zahlen auf den Feldern gut lesbar bleiben, ist der jeweilige Hintergrund in der entsprechenden Komplementärfarbe gehalten. Die PIN eines Benutzers wird mit Hilfe eines schwarzen und eines weißen Buttons unterhalb des Eingabefeldes eingegeben. Wenn sich die erste Ziffer der PIN auf einem weißen Feld befindet, muss der entsprechende Button gedrückt werden und umgekehrt. Sobald der Benutzer einen der beiden Buttons gedrückt hat, werden die Felder erneut zufällig eingefärbt, und der Benutzer drückt wieder einen der beiden Buttons, je nachdem, ob sich die betreffende Zahl auf einem schwarzen oder weißen Feld befindet. Für jede Stelle der PIN müssen die Buttons insgesamt $n = \lceil \log_2 |A| \rceil$ gedrückt werden, wobei A das Alphabet ist. A besteht in diesem Fall, wie oben erwähnt, aus den Zahlen null bis neun, daraus folgt $A = 10$. Das bedeutet wiederum: $n = 4$. Für eine PIN mit $l = 4$ Stellen werden somit $l * n = 16$ Eingaben benötigt. Ein geübter Benutzer benötigt für die Eingabe der PIN mit diesem Verfahren etwa 18 Sekunden.

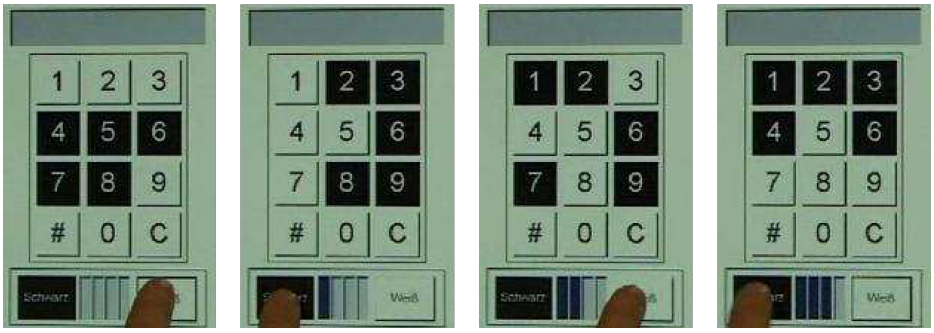


Abbildung 3: Immediate oracle choice variant (Cognitive trapdoor game) [RR06]

Delayed oracle choice variant: Dieses Verfahren unterscheidet sich vom bisherigen Verfahren nur durch die Anzeige des Eingabefeldes. Während es bei der ersten Variante erst nach dem Drücken eines Buttons und damit in der nächsten Runde verändert wurde, werden bei dieser Variante die $n = 4$ Runden nacheinander mit einer Wartezeit von 0.5 Sekunden angezeigt, siehe Abbildung 4. Der Benutzer merkt sich n Mal, ob die Stelle seiner PIN auf einem schwarzen oder weißen Feld lag und gibt dies anschließend, wie oben beschrieben, auf einmal ein. Mit dieser Variante soll verhindert werden, dass sich ein daneben stehender Beobachter die schwarzen und weißen Felder merken und damit auf die PIN schließen kann. Ein geübter Benutzer benötigt für die Eingabe der PIN mit diesem Verfahren etwa 25 Sekunden.

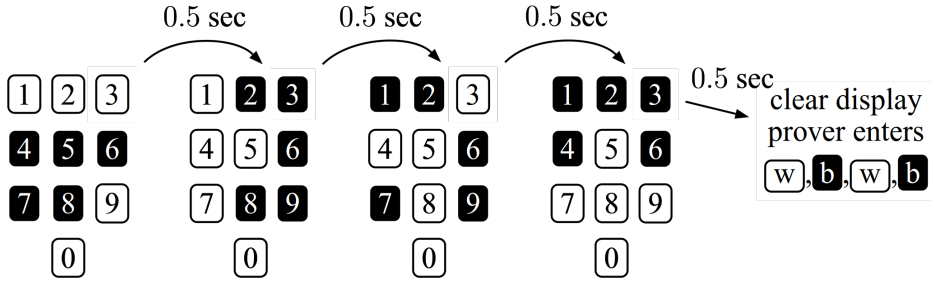


Abbildung 4: Delayed oracle choice variant (Cognitive trapdoor game) [RR06]

Beide vorgestellten Varianten schützen ausreichend gegen Shoulder-Surfing, sofern keine Kamera verwendet wird. Ist dies jedoch der Fall, schlagen die Autoren vor, dass sich in jeder Runde das Tastenfeld durch eine Schwarz- beziehungsweise Weiß-Färbung der Zahlenfelder so verändert, dass zwei PINs denkbar sind. Der Angreifer kann daher kein eindeutiges Ergebnis erzielen. Bei einer PIN mit der Länge $l = 4$ führt das zu $2^l = 16$ möglichen PINs.

Analyse: Beide Verfahren bieten Schutz gegen Shoulder-Surfing, sind aber aufgrund der jeweils benötigten Zeit für die Eingabe am Smartphone nicht effizient genug. Bei den Verfahren ist außerdem das Kriterium des gleichen Sicherheitslevels verletzt, weil in jeder Runde bei der Eingabe der PIN nur zwischen dem Drücken auf einen weißen oder schwarzen Button unterschieden wird (Kapitel 2.1).

Convex Hull Click Scheme

Wiedenbeck, Waters et al. haben das Convex Hull Click Scheme (CHC) entwickelt [Wie+06]. Dieses Verfahren besteht aus mehreren Runden einer Challenge-Response-Authentisierung. Der Benutzer wählt zu Beginn eine festgelegte Anzahl von Symbolen für sein Passwort aus einem Katalog aus. Bei der Passwort-Eingabe sieht er auf dem Bildschirm viele verschiedenen Symbole, siehe Abbildung 5. Die Symbole wurden zufällig aus dem Katalog ausgewählt. Darunter befinden sich auch einige, aber nicht alle Symbole, die der Benutzer ausgewählt hat. Alle Symbole sind zufällig angeordnet und ändern ihre Position nach jeder Eingabe. Außerdem kommen jedes Mal Symbole dazu und andere verschwinden. Der Benutzer muss „seine“ Symbole wiedererkennen. Mindestens drei davon werden angezeigt. In diesem Fall muss er sich auf dem Bildschirm eine Fläche vorstellen, die durch die drei Symbole gebildet wird. Anschließend muss er in diese klicken. Jede Authentisierung besteht aus mehreren Runden (*challenges*), je nachdem, wie viele Stellen das Passwort umfasst. Für jede Runde benötigt ein Benutzer etwa 11 Sekunden.

Analyse: Bei diesem Verfahren ist allerdings das Kriterium der Eignung für ein Smartphonedisplay verletzt, weil es aufgrund der Anzahl Symbole auf einem Smartphonedisplay nicht ausreichend darstellbar ist.

Abbildung 5: Convex Hull Click Scheme [Wie+06]

Spy-resistant keyboard

Tan, Keyani und Czerwinski [TKC05] haben ein Verfahren entwickelt, bei dem Tastaturen auf einem öffentlich einsehbaren Touchscreen ebenfalls resistent gegen Shoulder-Surfing sein sollen. Dabei werden sämtliche mögliche Zeichen (Buchstaben, Zahlen, Sonderzeichen) in drei Gruppen mit je drei Zeilen eingeteilt, siehe Abbildung 6. Dabei besteht eine Zeile aus Kleinbuchstaben, die andere aus Großbuchstaben und die dritte aus Zahlen und Sonderzeichen. Da die Anzahl der Buchstaben im Alphabet geringer ist als die Anzahl der Zahlen und Sonderzeichen, kommen Buchstaben teilweise doppelt vor. Die Zeichen werden in den Zeilen zufällig verteilt. Manche Zeichen sind rot unterstrichen, andere nicht. Unterhalb der drei Gruppen befinden sich zwei Felder mit einem roten Kreis, jeweils mit der Beschriftung „Drag me“. Die Eingabe des gewünschten Zeichens erfolgt in mehreren Stufen:

- Benutzer sucht gewünschtes Zeichen auf der Tastatur.
- Sodann klickt er so lange auf den roten Kreis, bis das gewünschte Zeichen rot unterstrichen ist.
- Anschließend zieht er den roten Kreis zum gewünschten Zeichen. Sobald er damit beginnt, erlischt die Beschriftung der Tastatur.
- Sobald er den Kreis auf die bisherige Position des gewünschten Zeichens gezogen hat, lässt er ihn los und hat das erste Zeichen seines Passworts eingegeben. Auf diese Weise wird nacheinander jedes Zeichen eingegeben.

Analyse: Bei diesem Verfahren ist allerdings das Kriterium der Eignung für ein Smartphonedisplay verletzt, weil es aufgrund der Anzahl Zeichen auf einem Smartphonedisplay nicht ausreichend darstellbar ist.

Abbildung 6: Spy-resistant keyboard [TKC05]

ColorPIN

De Luca, Hertzschuch und Hussmann [DHH10] haben ein Verfahren entwickelt, das die Sicherheit bei der Benutzung von Geldautomaten erhöhen soll. Dabei wird ein Tastenfeld verwendet, das dem eines

herkömmlichen Geldautomaten ähnelt. Unterhalb von jeder Zahl befinden sich drei Kästchen mit unterschiedlichen Buchstaben in verschiedenen Farben (schwarz, rot oder weiß), siehe Abbildung 7. Die PIN besteht aus vier Zahlen, denen jeweils eine bestimmte Farbe zugeordnet ist. Der Benutzer gibt nun nacheinander auf einer gesonderten Tastatur die Buchstaben ein, die der Farb- und Zahlenkombination entsprechen. Da jeder Buchstabe jeweils in allen drei Farben vorkommt, kann ein Angreifer durch Shoulder-Surfing nicht herausfinden, zu welcher Zahl der eingegebene Buchstabe gehört.

Analyse: Bei diesem Verfahren ist allerdings das Kriterium der Eignung für ein Smartphonedisplay verletzt, da nicht nur ein Tastenfeld, sondern zusätzlich noch eine Tastatur angezeigt werden muss und dies auf einem kleinen Display eher schlecht umsetzbar ist.

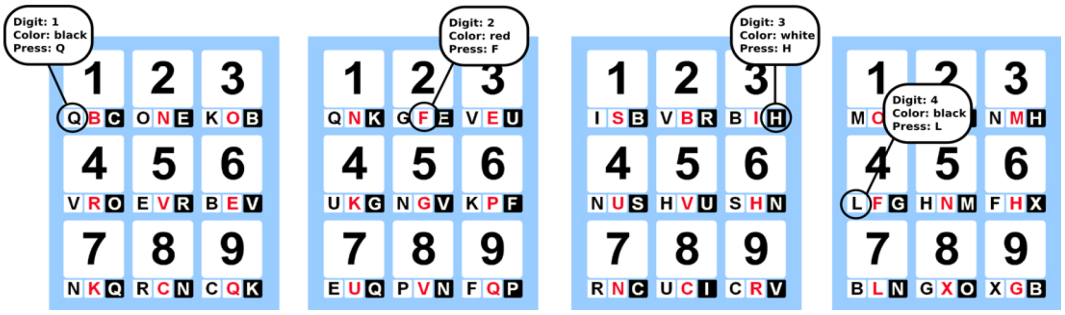


Abbildung 7: ColorPIN [DHH10]

Unclear Images

Harada, Isarida et al. [Har+06] haben ein ähnliches Verfahren entwickelt, bei dem der Benutzer sich anhand von Bildern authentisiert, die als „unclear images“ bezeichnet werden. Zu Beginn wählt der Benutzer einige seiner eigenen Bilder aus, die er für die Authentisierung verwenden möchte. Diese Bilder werden danach durch Bildverarbeitung schwarz-weiß gefärbt und mit Bildrauschen verfremdet, siehe Abbildung 8. Der Benutzer authentisiert sich, in dem er in mehreren Runden (*challenges*) jeweils „sein“ Bild aus einer Anzahl unbekannter, gleich bearbeiteter Bilder auswählt.

Analyse: Bei diesem Verfahren ist allerdings das Kriterium der Effizienz verletzt, da ein Benutzer durchschnittlich 7 Sekunden für jede Runde benötigt.

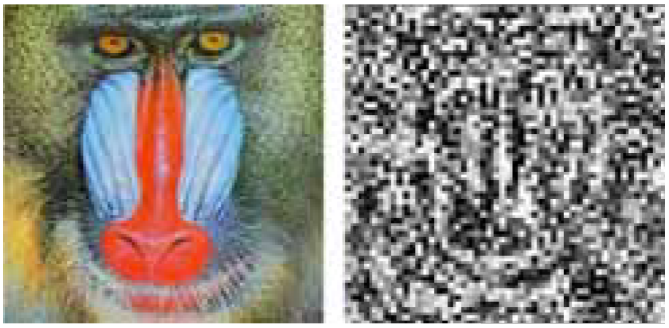


Abbildung 8: Unclear Images [Har+06]

Use Your Illusion

Das Verfahren von Hayashi, Christin et al. [Hay+08] nennt sich „Use Your Illusion“. Dabei wählt der Benutzer eine bestimmte Anzahl eigener Bilder oder Bilder aus einer Datenbank aus. Diese Bilder werden dann mit Hilfe eines Algorithmus verzerrt, so dass keine Details mehr erkennbar sind, sondern nur grobe Strukturen und Farben, siehe Abbildung 9. Bei der Authentisierung sieht der Benutzer neben dem selbst gewählten Bild andere auf die gleiche Weise veränderte Bilder, die zufällig angeordnet sind. Er muss nun das eigene Bild erkennen und auswählen. Um Shoulder-Surfing zu erschweren, erfolgt keine (sichtbare) Reaktion bei der Auswahl des Bildes. Dieses Verfahren basiert auf mehreren Runden (*challenges*), die der Benutzer erfolgreich durchlaufen muss.

Analyse: Bei diesem Verfahren ist allerdings das Kriterium der Effizienz verletzt, da ein Benutzer durchschnittlich mindestens 12 Sekunden für eine Authentisierung mit drei Runden benötigt.

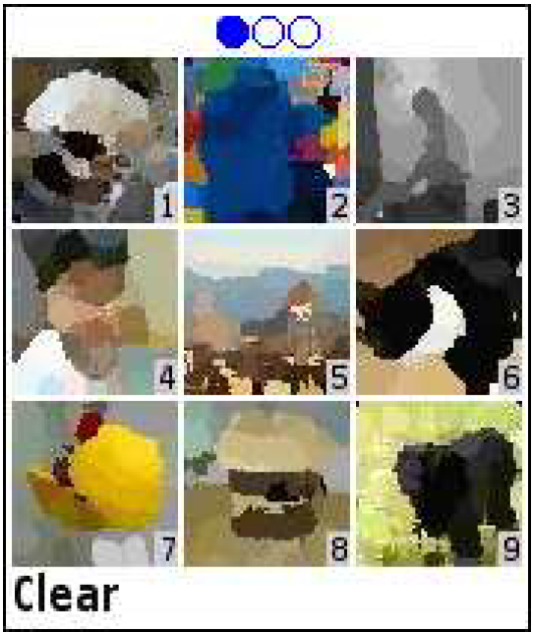


Abbildung 9: Use Your Illusion [Hay+08]

Déjà Vu

Beim Verfahren von Dhamija und Perrig [DP00] authentisiert sich der Benutzer anhand von Bildern. Zu Beginn wählt er eine Anzahl von p Bildern aus einem Katalog aus und erstellt damit sein Portfolio. Bei der Authentisierung werden dem Benutzer n Bilder angezeigt, welche m Bilder aus dem Portfolio des Benutzers enthalten. Die Autoren haben sich entschieden, Andrej Bauer's Random Art [Bau98] zu verwenden, um zufällige abstrakte Bilder zu erstellen, siehe Abbildung 10. Je größer das Portfolio des Benutzers, desto besser ist der Schutz gegen Shoulder-Surfing. Das Verfahren ist so ausgelegt, dass nicht zu sehen ist, was der Benutzer auswählt. Die Bilder können bei jeder Authentisierung leicht verändert werden.

Analyse: Bei diesem Verfahren ist allerdings das Kriterium der Effizienz verletzt, da ein Benutzer durchschnittlich 34 Sekunden für eine Authentisierung mit fünf Runden benötigt.

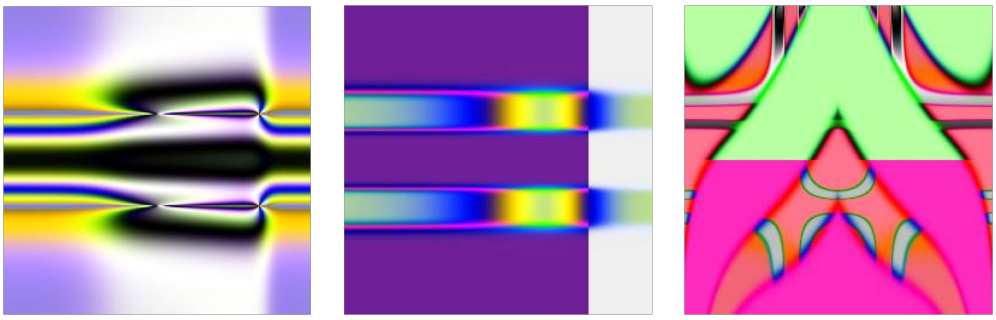


Abbildung 10: Déjà Vu [DP00]

PassFaces

Passfaces [Cor04] ist ein Verfahren, von der Passfaces Corporation, welches kommerziell vermarktet wird. Dabei bekommt ein Benutzer standardmäßig fünf Gesichter in einer bestimmten Reihenfolge als Passwort zugewiesen. Die Gesichter sind Portraits von Männern und Frauen. Wenn der Benutzer sich authentisiert, wird ihm ein Feld aus 3x3 Gesichtern angezeigt, siehe Abbildung 11. Daraus muss er sein zugewiesenes auswählen. Standardmäßig folgen noch vier weitere Runden, in denen er das richtige Gesicht auswählen muss. In jeder Runde werden die gleichen Gesichter angezeigt, nur jedes Mal in einer anderen Mischung. Eine Runde kann, je nach Passwort des Benutzers, aus männlichen oder weiblichen Gesichtern bestehen. Damit dieses System vor Shoulder-Surfing ohne Kamera sicher ist, schlagen die Entwickler vor, das Feld nur 0.5 Sekunden anzuzeigen und danach alle Gesichter in dieser Runde durch das gleiche Gesicht zu ersetzen.

Analyse: Bei diesem Verfahren ist allerdings das Kriterium des gleichen Sicherheitslevels verletzt, weil es nicht mit der Eingabe einer PIN (ausschließliche Verwendung von vier Zahlen) vergleichbar ist, da in jeder Runde nur neun verschiedene Bilder verwendet werden. (Kapitel 2.1).

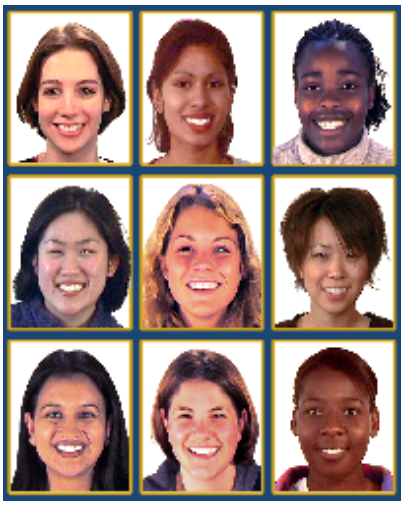


Abbildung 11: PassFaces [Cor04]

GraphNeighbors

Altiok, Uellenbeck und Holz [AUH14] haben drei Verfahren entwickelt, von denen zwei shoulder-surfing resistent sind. Im Folgenden werden daher nur diese beiden Verfahren näher erläutert. Bei beiden besteht

jede Stelle des Passworts aus einer Kombination von Form (Kreis, Quadrat, Dreieck, Raute, Fünfeck oder Stern), Farbe (blau, grün, gelb oder rot) und Position (über, rechts, unter, links oder keine), die der Benutzer vor Verwendung festlegt. Bei der Authentisierung sieht er ein Feld aus 6x4 Formen die unterschiedlich gefärbt und zufällig angeordnet sind, siehe Abbildung 12. Der Benutzer muss nun die selbst gewählte Form in der richtigen Farbe finden und auf diejenige klicken, die sich an der festgelegten Position befindet. Wenn die gewählte Stelle beispielsweise aus den Elementen „Dreieck“, „rot“ und „über“ besteht, muss der Benutzer auf dem Feld das rote Dreieck suchen und daraufhin auf die Form darüber klicken.

Das zweite Verfahren unterscheidet sich von dem ersten darin, dass es insgesamt aus zwölf möglichen Formen besteht, allerdings nur in *einer* Farbe.

Analyse: Beide Verfahren erfordern mehrere Runden. Ein vierstelliges Passwort besteht beispielsweise aus insgesamt 4x3 Eigenschaften, die sich der Benutzer merken muss. Aus diesem Grund gehen die Autoren dieser Arbeit davon aus, dass das Kriterium der Effizienz verletzt ist, da erst die richtige Form mit der richtigen Farbe und danach die richtige Position gefunden werden muss und das insgesamt mindestens vier Mal. In der Veröffentlichung selbst wurden keine Zeiten gemessen.

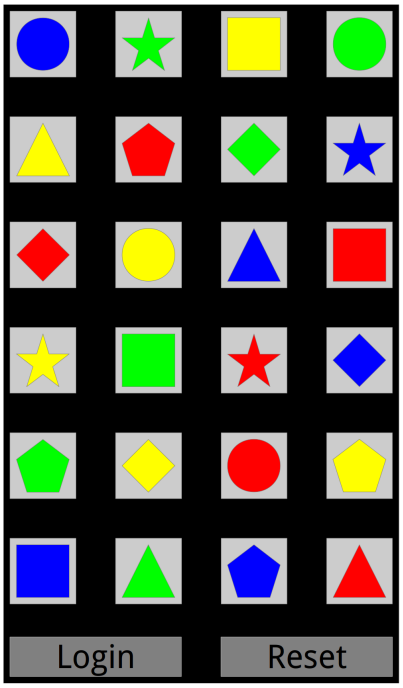
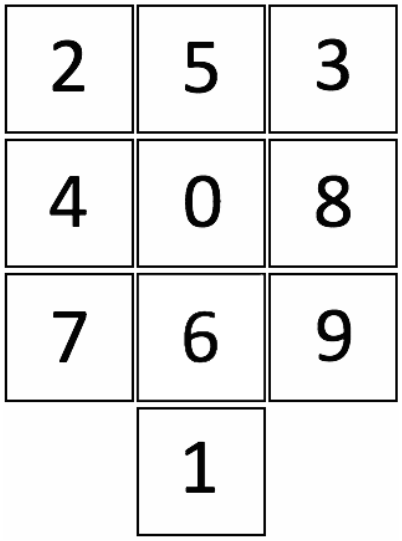


Abbildung 12: GraphNeighbors [AUH14]

3.3 Lösungsansatz

Im Folgenden werden zwei Verfahren vorgestellt, siehe Abbildung 13, die den Kriterien aus Kapitel 2.1 und 3, nämlich mindestens gleiches Sicherheitslevel wie bei dem klassischen PIN-Verfahren und Positionsunabhängigkeit, entsprechen und bei der Verwendung einer Blickschutzfolie resistent gegen Shoulder-Surfing sind.

Das erste, siehe Abbildung 13a, basiert auf dem klassischen PIN-Verfahren. Es gibt insgesamt zehn Tasten im gleichen Layout wie beim Eingabefeld eines Geldautomaten, die mit den Zahlen von null bis



(a) Zufällig angeordnete Zahlen

(b) Zufällig angeordnete Bilder

Abbildung 13: Eigener Lösungsansatz

neun beschriftet sind. Anders als beim PIN-Verfahren sind jedoch die Tasten zufällig angeordnet. Ein Angreifer kann aus diesem Grund von der Position der Finger des Benutzers nicht auf dessen PIN schließen. Bei jeder Authentisierung werden die Tasten erneut zufällig angeordnet. Damit dieses Verfahren dem Kriterium des gleichen Sicherheitslevels genügt, muss die potentielle PIN vierstellig sein.

Das zweite Verfahren, siehe Abbildung 13b, basiert vom Layout her ebenfalls auf dem klassischen PIN-Verfahren. Auch hier gibt es insgesamt zehn Tasten. Der entscheidende Unterschied besteht jedoch darin, dass auf den Tasten keine Zahlen, sondern Bilder angezeigt werden. Diese werden bei jeder Authentisierung zufällig angeordnet. Bei den Bildern handelt es sich um affektbetonte [COP08] Clip-Arts, da diese besser wahrgenommen werden können als Fotos. Auch bei diesem Verfahren besteht eine Authentisierung aus insgesamt vier Bildern. Das traditionelle PassFaces konnte hier nicht verwendet werden, da es auf Grund des Sicherheitslevels mit neun Gesichtern nicht dem des Standard-PIN-Verfahrens entspricht. Da das Hinzufügen eines weiteren Gesichts macht dieses Verfahren sehr ähnlich zu dem eigenen Vorschlag und wurde daher nicht eigenständig getestet.

Diese beiden Verfahren wurden in einer Online-Studie anhand der Kriterien aus Kapitel 2 getestet und die Ergebnisse werden in Kapitel 5 dargestellt.

4 Analyse der Blickschutzfolien

In diesem Kapitel werden die beiden Blickschutzfolien analysiert, die in Kapitel 3.1 ausgewählt wurden. Dazu wird zunächst die Anbringung der Folien beschrieben (4.1). Danach werden die Szenarien vorgestellt, die untersucht werden (4.2). Aus den Szenarien werden Variablen abgeleitet, die bei der späteren Analyse zu beachten sind. Danach wird des Studiendesign (4.3) und die Durchführung (4.4) der Analyse beschrieben. Abschließend werden die Ergebnisse beschrieben (4.5) und es folgen Empfehlungen (4.6), die sich aus den gewonnenen Erkenntnissen ableiten, also was bei der Verwendung solcher Folien beachtet werden sollte.

4.1 Anbringung der Folien

Bei der Belkin-Folie gab es keine Besonderheiten bei der Anbringung. Als Erstes musste das Display des Smartphones mit einem Microfasertuch gereinigt werden, um Staubeinschlüsse zu verhindern. Danach wurde die Schutzfolie von der Blickschutzfolie entfernt, diese auf das Display gelegt und anschließend mit einer Plastik-Karte glatt gestrichen sowie Blasen unter der Folie entfernt. Positiv ist anzumerken, dass Tuch und Karte der Blickschutzfolie beigefügt waren. Die Anbringung war insgesamt zwar einfach. Nach dem Anbringen der Blickschutzfolie war es jedoch sehr schwer, diese zur Korrektur zu verschieben.

Bei der Copter-Folie fiel bereits die sehr hochwertige Verpackung auf. Die mehrsprachige Anleitung war mit zwölf einzelnen Schritten sehr detailliert. Der entscheidende Unterschied gegenüber der Belkin-Folie war bei der Anbringung ein sogenanntes „Copter-Spray“. Mit diesem Spray wurden die Finger und beide Seiten der Folie benetzt. Danach war es problemlos möglich, die Folie akkurat auf dem Display anzubringen, da sie durch die feuchte Oberfläche gut verschoben werden konnte. Anschließend wurden auch bei dieser Folie Blasen - und in diesem Fall auch Feuchtigkeit - mit einem Stück Plastik durch Glattstreichen entfernt. Die restliche Feuchtigkeit wurde mit Hilfe eines beiliegenden Microfasertuchs entfernt. Bei Bedarf soll ein Föhn auf niedrigster Stufe verwendet werden, um den Vorgang zu beschleunigen. Der Hersteller empfiehlt ferner, vor Benutzung die Folie zwölf Stunden trocknen zu lassen. Die Anbringung war insgesamt sehr einfach. Auch nach dem Anbringen konnte die Folie ohne Weiteres verschoben werden, um sie perfekt auszurichten.

In beiden Fällen ist deutlich zu erkennen, dass das Display nach Anbringung der Blickschutzfolie etwas dunkler und unschärfer wirkt. Dieser Effekt sticht bei der ersten Nutzung ins Auge, aber sobald die Folie ein paar Tage verwendet wird, fällt dieser Effekt, außer im direkten Vergleich mit einem Smartphone ohne Blickschutzfolie, kaum noch auf. Bei sehr großer Umgebungshelligkeit, beispielsweise bei direkter Sonneneinstrahlung, ist das Display jedoch insgesamt schlechter lesbar als ohne Folie.

Bei der Reaktion des Touchscreens fällt der etwas höhere Druckpunkt auf. Aber auch dieser Nachteil macht sich später nur noch im direkten Vergleich mit einem Smartphone ohne Folie bemerkbar.

Ein Vorteil beider Folien ist, abgesehen von dem potentiellen Blickschutz, dass das Display vor Kratzern und ähnlichen Schäden besser geschützt ist. Außerdem wird dadurch die Spiegelung des Displays verringert. Sie ist bei direktem Sonnenlicht nicht mehr so stark. Ein weiterer positiver Effekt ist, dass auf den Folien Fingerabdrücke deutlich schlechter sichtbar sind. Dieser Vorteil verbessert zwar nicht den Blickschutz, verhindert aber die oben genannten „smudge attacks“.

4.2 Analysierte Szenarien

Aus alltäglichen Situationen lassen sich folgende drei Gruppen von Szenarien ableiten, die bei der Analyse der Folien getestet werden. Diese stellen Situationen dar, in denen ein Angriff mit Hilfe von Shoulder-Surfing potentiell möglich wäre.

Im Folgenden werden die Begriffe „Benutzer“ und „Angreifer“ verwendet, um einerseits das Opfer, andererseits die Person, die einen Shoulder-Surfing-Angriff durchführt, zu beschreiben. Wie in Kapitel 2.1 erläutert, schützt sich der Benutzer in der Regel nicht aktiv vor Shoulder-Surfing, beispielsweise durch Verdecken des Displays.

Bei der Analyse wurde großer Wert auf konstante Rahmenbedingungen gelegt, um äußere Störeinflüsse zu vermeiden. Diese Rahmenbedingungen, und wie sie konstant gehalten wurden, werden im Folgenden anhand der Variablen bei dieser Analyse erläutert. Die gesamte Analyse wurde mit jedem möglichen Wert einer Variablen durchgeführt. Abbildung 14 zeigt einerseits die direkte Draufsicht 14a, andererseits den Winkel, bei dem der Displayinhalt gerade so nicht mehr sichtbar ist 14b.

(a) Sicht des Benutzers **(b)** Sicht des Angreifers

Abbildung 14: Sichtbarkeit bei verschiedenen Winkeln

Die erste Variable sind die **Lichtverhältnisse**. Sie beinhaltet Tageslicht und Dunkelheit. Um konstante Rahmenbedingungen für Tageslicht zu erreichen, wurde die Analyse an zwei aufeinanderfolgenden Tagen, zur selben Uhrzeit und im selben Raum durchgeführt. Dabei wurde darauf geachtet, dass sich das Wetter innerhalb der zwei Tage nicht verändert hatte. Zusätzlich wurde mit einem Luxmessgerät des Smartphones die Beleuchtungsstärke gemessen. Für die Analyse bei Dunkelheit wurde der selbe Raum mit Hilfe des Rolladens und Vorhängen vollständig verdunkelt. Damit die Displayhelligkeit des Smartphones keinen Einfluss auf das Ergebnis hat, wurde die automatische Helligkeitseinstellung von Android als Grundlage für die Analyse verwendet. Diese passt die Helligkeit des Displays anhand der Umgebungshelligkeit dynamisch an und kommt damit den alltäglichen Bedingungen am nächsten.

Die zweite Variable für die Analyse ist die **Körpergröße**. Hierfür wurden drei verschiedene Werte festgelegt, die das Größenverhältnis zwischen zwei Personen beschreiben sollen. Die Körpergröße des Benutzers wird zunächst auf die durchschnittliche Körpergröße eines Mannes der deutschen Bevölkerung

festgelegt. Diese beträgt laut Angaben des Statistischen Bundesamtes[9] aus dem Jahr 2009 1.78 m. Die Körpergröße des Angreifers ist dagegen variabel. Daraus ergeben sich drei Varianten: Entweder sind Angreifer und Benutzer gleich groß oder der Angreifer ist mit 1.89 m größer als der Benutzer und damit auch größer als der durchschnittliche Deutsche oder er ist mit 1.65 m kleiner als der Benutzer. Je nach Wahl der Körpergröße beim Angreifer ändert sich der konkrete Winkel zwischen Angreifer und Benutzer. Da sich die Tests im sitzen oder stehen nur hinsichtlich der Körpergröße unterscheiden, aber sonst keine weitere Relevanz haben, wurden sie in der Stehend-Variante durchgeführt.

Die dritte und letzte Variable für die Analyse ist die **Ausrichtung** des Angreifers im Verhältnis zum Benutzer. Sie beschreibt einerseits den Abstand zwischen Angreifer und Benutzer und andererseits den Winkel zu einem schräg hinter dem Benutzer positionierten Angreifer. Es wurden zwei Varianten untersucht, nämlich eine mit einem leichten Abstand von 0.3 m und eine andere mit einem weiten Abstand von 1 m. Der Winkel für einen versetzt positionierten Angreifer wurde auf 45° festgelegt.

Beim ersten Szenario befindet sich der Angreifer neben dem Benutzer und zwar direkt oder mit einem leichten Abstand. Beim zweiten Szenario befindet sich der Angreifer versetzt hinter dem Benutzer, aber auf gleicher Höhe beziehungsweise erhöht. Beim dritten Szenario befindet sich der Angreifer entweder direkt oder versetzt gegenüber dem Benutzer. Die Position direkt hinter dem Benutzer wurde nicht betrachtet, da es dem Angreifer in diesem Fall möglich ist, im selben Winkel auf das Display zu schauen wie der Benutzer. Ein Schutz durch eine Blickschutzfolie ist aufgrund der Funktionsweise hier nicht möglich.

Eine Zusammenfassung der Variablen befindet sich in Tabelle 1.

Tabelle 1: Variablen der Analyse

Lichtverhältnisse
Tageslicht
Dunkelheit

Körpergröße Angreifer
kleiner
gleichgroß
größer

Ausrichtung		
gegenüber	frontal	versetzt
dahinter	gleiche Höhe / versetzt	erhöht / versetzt
daneben	direkt	leichter Abstand

Szenario Typ 1: Angreifer gegenüber dem Benutzer

Dieses Szenario könnte auf einer Veranstaltung oder im Bus vorkommen. Der Benutzer befindet sich auf einer festen Position im Raum und zwar entweder stehend oder sitzend. Der Angreifer ist genau gegenüber und zwar sitzend oder stehend. Aus diesem Szenario ergeben sich drei Varianten: Angreifer und Benutzer stehen oder sitzen beide oder der Angreifer steht und der Benutzer sitzt. Dabei ist zu

[9] Destatis: https://www.destatis.de/DE/Publikationen/Thematisch/Gesundheit/Gesundheitszustand/Koerpermasse.html (aberufen am 26.07.14)

beachten, dass die Situation, dass der Benutzer steht und der Angreifer sitzt, ausgespart wird, da der Angreifer in diesem Fall keine Möglichkeit hat, auf das Display des Benutzers zu sehen. Daraus ergeben sich für den Test folgende Varianten: **Gegenüber** und **gegenüber versetzt**.

Szenario Typ 2: Angreifer sitzt neben dem Benutzer

Diese Szenario beschreibt eine Situation in einem Bus oder Wartezimmer. Dabei sitzt der Angreifer in direkter Nähe links oder rechts neben dem Benutzer (siehe Abbildung 15). Das Smartphone befindet sich also sehr nah beim Angreifer. Der Angreifer hat in diesem Szenario auch keine Möglichkeit, den Blickwinkel zu verändern, um einen besseren Blick auf das Display zu erhalten. Dieses Szenario bietet für ihn jedoch gute Möglichkeiten, den Displayinhalt mitzulesen, da sich der Blickwinkel von Angreifer und Benutzer ähneln. Für die Analyse ergeben sich folgende Varianten: **Direkt daneben** und **entfernt daneben**. Entfernt daneben bedeutet, dass zwischen Angreifer und Benutzer ein Platz frei ist.

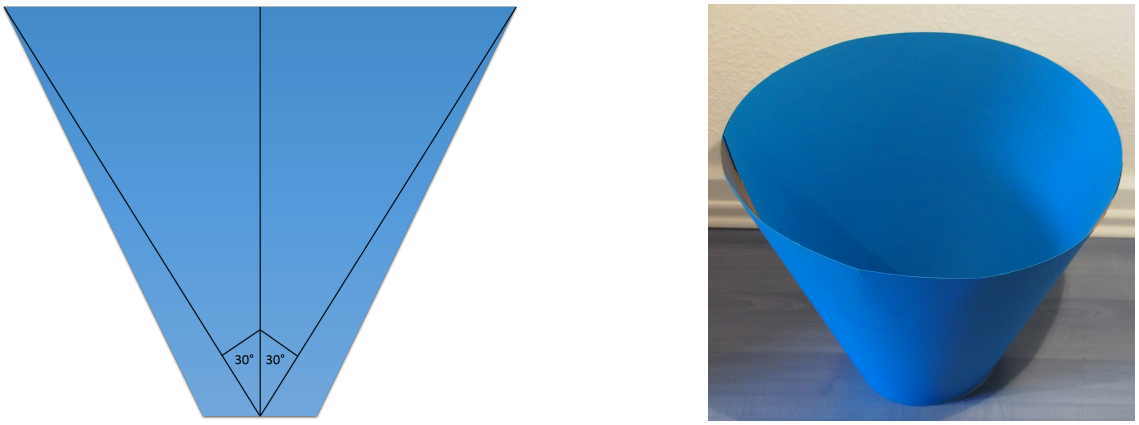
Abbildung 15: Angreifer sitzt neben dem Benutzer

Szenario Typ 3: Stehender Angreifer im unmittelbaren Umfeld des stehenden Benutzers (nicht gegenüber)

Es beschreibt ebenfalls die Situation in einem Bus oder auf einer Veranstaltung. Dabei steht der Benutzer an einem festen Platz im Raum, und der Angreifer befindet sich in dessen unmittelbarem Umkreis. Der Angreifer kann jede Position im Umkreis des Benutzers einnehmen. Die Position gegenüber dem Benutzer wird in diesem Fall jedoch ausgespart, da diese in einem eigenen Szenario behandelt wird. Der Angreifer hat viele Möglichkeiten sich zu positionieren. Aus diesem Grund ist eine Änderung des Blickwinkels problemlos möglich. Sollte sich eine gewählte Position im Nachhinein als schlechte Wahl herausstellen, kann er seine Position erneut verändern. Außerdem kann er sich so positionieren, dass er erhöht zu dem Benutzer steht. Daraus ergeben sich für den Test folgende Varianten: **Dahinter gleiche Höhe** und **dahinter erhöht**.

4.3 Studiendesign

Ziel der Studie ist herauszufinden, ob eine der beiden Folien einen guten Schutz gegen Shoulder-Surfing bietet. Dabei geht es einerseits um den generellen Schutz, andererseits um die Unterschiede zwischen



(a) Schematische Darstellung **(b)** Nachbau aus Hartkarton

Abbildung 16: Aufbau des Spezifikations-Modells

den Folien. Es soll herausgefunden werden, welche Szenarien sich gut für den Einsatz einer solchen Blickschutzfolie eignen und bei welchen Szenarien der Schutz nicht ausreicht. Abschließend sollen anhand der Ergebnisse Empfehlungen erkannt werden, die bei dem Einsatz einer solchen Folie beachtet werden sollten.

Bei der Analyse der Blickschutzfolien wird auf eine hohe Vergleichbarkeit zwischen den Ergebnissen geachtet. Aus diesem Grund wurden die Folien von Belkin beziehungsweise Copter auf zwei Smartphones des gleichen Typs angebracht, einem Galaxy S2 von Samsung aus dem Jahr 2011. Diese Maßnahme soll verhindern, dass eventuelle Helligkeits- oder Blickwinkelunterschiede bei verschiedenen Geräten das Ergebnis beeinflussen. Außerdem wurden beide Geräte auf die neueste verfügbare Android-Version (4.1.2) aktualisiert, um Unterschiede bei der Displayhelligkeit bei verschiedenen Versionen auszuschließen.

Für die Analyse der Blickschutzfolien wurde ein Modell aus Hartkarton erstellt, welches den Blickschutzwinkel der Folien laut Spezifikation des jeweiligen Herstellers nachbildet. Abbildung 16 stellt dieses Modell schematisch und als Karton-Modell dar. Es hat die Form eines Trichters, wobei das Smartphone am unteren Ende in der Mitte positioniert wird. Aufgrund der Form des Modells ergibt sich stets ein Winkel von 30°. Der Bereich, welcher es dem Angreifer ermöglicht, den Displayinhalt zu erkennen, wird im Folgenden als **Spezifikations-Modell** bezeichnet.

Schafft es der Angreifer trotz des Spezifikations-Modells das Display zu sehen, so bietet die Folie keinen Schutz. Bei dem anschließenden Test mit und ohne Folie ergeben sich vier Ergebnisarten:

Fall 1: Weder mit noch ohne Spezifikations-Modell sichtbar

In diesem Fall ist der Displayinhalt des Smartphones nicht sichtbar, unabhängig davon, ob bei dem Test das Spezifikations-Modell verwendet wird oder nicht. Das bedeutet, dass die getestete Blickschutzfolie ausreichend Schutz gegen Shoulder-Surfing bietet und mindestens so gut ist, wie die Spezifikationen es angeben.

Fall 2: Mit und ohne Spezifikations-Modell sichtbar

In diesem Fall ist der Displayinhalt des Smartphones sichtbar, unabhängig davon, ob bei dem Test das Spezifikations-Modell verwendet wird oder nicht. Das bedeutet, dass die getestete Blickschutzfolie hier

überhaupt keinen Schutz gegen Shoulder-Surfing bietet. Auch in diesem Fall sind die Spezifikationen des Herstellers erfüllt.

Fall 3: Mit Spezifikations-Modell nicht sichtbar, ohne schon

In diesem Fall ist der Displayinhalt des Smartphones bei Verwendung des Spezifikations-Modells nicht sichtbar, ohne diese jedoch schon. Das bedeutet, dass die getestete Blickschutzfolie keinen Schutz gegen Shoulder-Surfing bietet und die Spezifikationen der Folie nicht zutreffen.

Fall 4: Mit Spezifikations-Modell sichtbar, ohne nicht

In diesem Fall ist der Displayinhalt des Smartphones bei Verwendung der Spezifikations-Modells sichtbar, ohne diese jedoch nicht. Das bedeutet, dass die getestete Blickschutzfolie ausreichend Schutz gegen Shoulder-Surfing bietet und sogar die Spezifikationen des Herstellers übertrifft.

4.4 Durchführung

Die Analyse wurde mit drei Personen durchgeführt. Die erste Person übernahm die Rolle des Benutzers, die zweite die des Angreifers, und die dritte Person hat die korrekte Einhaltung der Variablen überwacht. Diese übernahm auch die Messung der Körpergrößen und der Abstände zwischen Angreifer und Benutzer. Beide haben sich positioniert und nach Anweisung der dritten Person ihre Größe „angepasst“, zum Beispiel dadurch, dass sie in die Knie gehen. Anschließend wurde getestet, ob es dem Angreifer möglich war, das Display zu erkennen.

Zur Dokumentation der Ergebnisse wurde für alle drei Szenarien ein Versuchsplan mit sämtlichen Ergebnissen angelegt, der sämtliche Kombinationen der Variablen beinhaltet. Die Analyse wurde zusätzlich mit einem Gerät ohne Folie durchgeführt, um zu überprüfen, inwieweit das Gerät auch in diesem Fall in den jeweiligen Szenarien Schutz bietet.

Die Analyse wurde zunächst mit und danach ohne das Spezifikations-Modell durchgeführt. Anschließend wurden beide Ergebnisse dokumentiert. Der Versuch mit Spezifikations-Modell wurde durchgeführt, um herauszufinden, ob sie in dem getesteten Szenario wirklich einen ausreichenden Schutz bietet. Der Versuch ohne Spezifikations-Modell wurde zur Überprüfung der Herstellerangaben durchgeführt und sollte zeigen, ob die Angaben korrekt sind und innerhalb des Winkels der Displayinhalt wirklich nicht sichtbar ist.

Jedes Szenario wurde zuerst mit beiden Folien getestet, bevor mit dem nächsten Szenario begonnen wurde. Die Analyse bei Tageslicht wurde bei 700 Lux durchgeführt. Anschließend wurden alle Tests bei Dunkelheit wiederholt. Da nur zwei gleiche Smartphones verfügbar waren, wurde die Analyse ohne Folie erst nach Beendigung aller anderen Tests durchgeführt. Dazu wurde bei einem Gerät die Blickschutzfolie entfernt und es erneut in allen Szenarien getestet. Im Verlauf jedes dieser Tests innerhalb eines Szenarios wurde, wie oben detailliert beschrieben, nur die Körpergröße des Angreifers variiert.

4.5 Ergebnis

Bei der Auswertung der Ergebnisse werden die Folien anhand der einzelnen Szenarien miteinander verglichen. Dabei ist zu beachten, dass die Folie von Copter nur seitlich einen Blickschutz von 30° und

die Folie von Belkin dagegen einen 360° Schutz bieten soll. Aus diesem Grund sind die Folien zwar vergleichbar, aber schützen aufgrund der Konzeption nicht in allen Szenarien im gleichem Maß.

Gegenüber (Typ 1)

Bei diesem Szenario stehen sich Benutzer und Angreifer frontal gegenüber. Die Belkin-Blickschutzfolie entspricht vollständig den Spezifikationen des Herstellers. Dem Angreifer ist es nicht möglich, das Display zu sehen, wenn das Spezifikations-Modells verwendet wird. Wird diese entfernt, ändert sich am Ergebnis nichts. Auch dann ist es nicht möglich, den Displayinhalt zu erkennen. Beide Ergebnisse sind unabhängig von den jeweiligen Lichtverhältnissen.

Bei der Copter-Folie wird auf den Test mit dem Spezifikations-Modell verzichtet, da diese keinen 360°-Schutz bietet. Beim Test ohne Spezifikations-Modell ist es dem Angreifer nicht möglich, den Displayinhalt zu erkennen, sofern er kleiner als der Benutzer ist.

Nichts anderes gilt in dem Fall, wenn überhaupt keine Folie verwendet wird. Aus diesem Grund gibt es bei diesem Test zwischen der Folie von Copter und einem Smartphone ohne Folie keinen Unterschied.

Gegenüber versetzt (Typ 1)

Bei diesem Szenario stehen sich Benutzer und Angreifer auch gegenüber, allerdings - im Unterschied zu dem vorherigen - versetzt. Die Blickschutzfolie von Belkin bietet erneut den besseren Schutz. Unabhängig von den Lichtverhältnissen und der Körpergröße des Angreifers ist es ihm nicht möglich, den Displayinhalt zu sehen.

Die Folie von Copter bietet weiterhin keinen ausreichend Schutz und verhindert nur, dass ein kleinere Angreifer den Displayinhalt sehen kann. Bei Dunkelheit ergibt sich das gleiche Resultat.

Ohne Folie entspricht das Ergebnis dem der Verwendung der Folie von Copter. Allerdings bietet die Verwendung keiner Folie bei direkter Sonneneinstrahlung sogar einen größeren Schutz, da das Display seitlich gesehen spiegelt und die seitliche Sicht auf das Display behindert.

Direkt daneben (Typ 2)

Bei diesem Szenario stehen Benutzer und Angreifer direkt nebeneinander. Die Blickschutzfolie von Belkin entspricht bei Tageslicht weitestgehend den Angaben des Herstellers. Sofern jedoch der Angreifer größer ist als der Benutzer, ist es für jenen sowohl möglich, das Display bei Verwendung des Spezifikations-Modells als auch ohne zu sehen. Bei Dunkelheit trat zum ersten Mal ein kritischer Effekt auf: Sofern die Umgebungshelligkeit zu gering ist, kann sie nicht ausreichend gebrochen werden, und das Display wirkt noch heller als bei Tageslicht. Aus diesem Grund bietet die Blickschutzfolie ohne Verwendung des Spezifikations-Modells keinen ausreichenden Schutz. Die Verwendung des Spezifikations-Modells ist in diesem Fall nicht sinnvoll, da die Displayhelligkeit von der Pappe blockiert wird. Erwartungsgemäß ist der Inhalt des Displays bei Verwendung der Folie nur für einen größeren Angreifer sichtbar.

Bei der Folie von Copter ergibt sich ein gemischtes Bild. Während sie bei Tageslicht und einem kleineren Angreifer ausreichend schützt, sind die Spezifikationen bei einem gleich großen Angreifer bei beliebigen Lichtverhältnissen sowie bei einem kleineren Angreifer bei Dunkelheit nicht erfüllt. Das bedeutet, dass die Blickschutzfolie in diesem Fall die Spezifikation des Herstellers nicht erfüllt. (Fall 3). Bei

einem größeren Angreifer ist das Display unabhängig von den Lichtverhältnissen sichtbar, die Spezifikationen des Herstellers sind erfüllt (Fall 2).

Beim Test ohne Folie ist der Displayinhalt bei jeder Körpergröße und allen Lichtverhältnissen sichtbar.

Entfernt daneben (Typ 2)

Bei diesem Szenario befindet sich der Angreifer auch neben dem Benutzer, jedoch – im Unterschied zu dem vorigen Szenario - nicht direkt daneben. Beide Blickschutzfolien bieten unabhängig von den Lichtverhältnissen, der Größe des Angreifers und der Verwendung des Spezifikations-Modells vollständigen Schutz gegen Shoulder-Surfing.

Ohne Folie ist in diesem Szenario der Displayinhalt jedoch jederzeit erkennbar.

Dahinter versetzt, gleiche Höhe (Typ 3)

Bei diesem Szenario befindet sich der Angreifer versetzt hinter dem Benutzer. Die Position direkt dahinter wird, wie in der Beschreibung der Szenarien angegeben, ausgeschlossen, da der Angreifer in diesem Fall einen nahezu identischen Blickwinkel wie der Benutzer besäße. Die Blickschutzfolie von Belkin bietet in zwei der drei Fälle Schutz gegen Shoulder-Surfing. Ein größerer Angreifer hat bei allen Lichtverhältnissen die Möglichkeit, den Displayinhalt zu sehen. Dies ist allerdings nur deshalb möglich, da ein Benutzer das Smartphone nie vollständig horizontal hält. Der Schutz bei einem Winkel von 60° ist zwar gegeben,- durch die zusätzliche Neigung des Gerätes wird aber der sichtbare Bereich erweitert. In diesem Fall werden die Spezifikationen des Herstellers verletzt (Fall 3).

Ähnlich wie beim ersten Szenario bietet die Blickschutzfolie von Copter aufgrund ihrer Konzeption keinerlei Schutz gegen diesen Angriff und wird deshalb nur ohne Spezifikations-Modell analysiert.

Sie unterscheidet sich im Ergebnis nicht von der Lösung ohne Folie.

Dahinter versetzt, erhöht (Typ 3)

Bei diesem Szenario befindet sich der Angreifer ebenfalls versetzt hinter dem Benutzer, allerdings erhöht. Dies stellt aufgrund des Winkels eine besonders günstige Situation für ihn dar. Die Blickschutzfolie von Belkin bietet hier einen sehr geringen Schutz, und zwar nur gegen einen Angreifer, der kleiner als der Benutzer ist. Sofern der Angreifer genauso groß wie der Benutzer ist, sieht er bei Verwendung der Folie nichts, ohne Folie jedoch schon. Aus diesem Grund sind die Spezifikationen der Folie unzutreffend (Fall 3). Bei einem größeren Angreifer ist der Displayinhalt mit und ohne Spezifikations-Modell sichtbar, entspricht daher den Spezifikationen, ist aber nicht shoulder-surfing resistent. Die Ergebnisse gelten sowohl für Tageslicht als auch für Dunkelheit.

Ähnlich wie beim ersten Szenario bietet die Blickschutzfolie von Copter aufgrund ihrer Konzeption keinerlei Schutz gegen diesen Angriff und wird deshalb nur ohne Spezifikations-Modell analysiert. Der Displayinhalt ist bei jeder Größe des Angreifers sichtbar, ob mit oder ohne Folie.

Zusammenfassung

Während die Folie von Copter nur in einem von sechs Szenarien ausreichenden Schutz bietet, sind es bei der Folie von Belkin immerhin drei von sechs, also die Hälfte. Bei dem einzigen Szenario, gegen das die Folie von Copter auch schützt, nämlich „direkt daneben“, ist die Schutzleistung nur unzureichend.

Tabelle 2: Ergebnis der Analyse (T: Tageslicht, D: Dunkelheit)

Ausrichtung	Körpergröße	Belkin (T)	Belkin (D)	Copter (T)	Copter (D)
Gegenüber (frontal)	kleiner	nein	nein	nein	nein
	gleich	nein	nein	ja	ja
	größer	nein	nein	ja	ja
Gegenüber (versetzt)	kleiner	nein	nein	nein	nein
	gleich	nein	nein	ja	ja
	größer	nein	nein	ja	ja
Daneben (direkt)	kleiner	nein	**ja**	nein	ja
	gleich	nein	**ja**	**ja**	ja
	größer	ja	ja	ja	ja
Daneben (entfernt)	kleiner	nein	nein	nein	nein
	gleich	nein	nein	nein	nein
	größer	nein	nein	nein	nein
Dahinter (normal)	kleiner	nein	nein	ja	ja
	gleich	nein	nein	ja	ja
	größer	**ja**	**ja**	ja	ja
Dahinter (erhöht)	kleiner	nein	nein	ja	ja
	gleich	**ja**	**ja**	ja	ja
	größer	ja	ja	ja	ja

Die Folie von Belkin erzielt im Gegensatz dazu bei fast allen Szenarien mindestens ausreichende Schutzwirkung, insbesondere in den Szenarien „dahinter, gleiche Höhe“, „dahinter, erhöht“, „gegenüber“ und „gegenüber versetzt“.

Aus diesem Grund können mit der Blickschutzfolie von Belkin eindeutig bessere Ergebnisse erzielt werden, da diese in vielen Szenarien gut schützt und weniger Fehler auftreten. Aber auch bei dieser Folie ist der Schutz nicht immer vollständig.

Zusammenfassend lässt sich sagen, dass es beim Schutz vor Shoulder-Surfing mit Hilfe einer Blickschutzfolie ganz entscheidend auf die verwendete Folie und das Szenario ankommt, siehe Tabelle 2. Die Szenarien in denen die jeweilige Folie nicht den Spezifikationen des Herstellers entspricht sind fett markiert.

4.6 Empfehlung für die Verwendung von Blickschutzfolien

In diesem Kapitel werden Empfehlungen, abgeleitet aus den Ergebnissen der Analyse, gegeben, die bei der Verwendung einer solchen Folie beachtet werden sollten. Sie dienen dazu, den Benutzer bei der Verwendung zu unterstützen und ihm gleichzeitig Grenzen der Folien aufzuzeigen.

Die Tests haben ergeben, dass die Folien bei Dunkelheit aus oben genannten Gründen teilweise weniger Schutz bieten als bei Tageslicht. Eine manuelle Änderung der Helligkeitseinstellung ist für den täglichen Gebrauch unrealistisch und dem Benutzer auch kaum zumutbar, da dieser die Displayhelligkeit für jede Situation manuell anpassen müsste. Daher müsste die automatische Helligkeitseinstellung von Android überarbeitet werden, um die Funktionalität der Blickschutzfolien zu verbessern. In der Zwischenzeit sollte der Benutzer bei der Verwendung des Smartphones generell davon ausgehen, dass es einem potentiellen Angreifer bei Dunkelheit leichter fällt, den Displayinhalt mitzulesen. Daraus ergibt

sich die Empfehlung, dass der Benutzer darauf achten sollte, dass bei Verwendung des Smartphones bei Dunkelheit sich niemand hinter ihm befindet und dass es möglichst parallel zum Körper gehalten wird.

Die Ausrichtung des Smartphones ist maßgebend für den Winkel, in dem der Sichtschutz gewährt wird. Hält ein Benutzer sein Smartphone also nahezu vertikal, so bietet die Folie keinen Schutz gegen Angreifer, die sich hinter ihm befinden. Der Benutzer könnte und sollte diese Tatsache allerdings auch zu seinem Vorteil nutzen. In Situationen, bei denen sich der Angreifer dahinter versetzt zum Benutzer befindet und trotz Folie einen Einblick in das Display hat, ist aufgefallen, dass eine leichte Neigung den Blickschutz erheblich verbessert. Bemerkt ein Benutzer daher einen potentiellen Angreifer, der sich durch die Gegebenheiten in einem Bereich befindet, in dem der Displayninhalt sichtbar ist, so kann er diese Erkenntnis nutzen und durch leichte Anpassung des Neigungswinkels seines Smartphones ein erfolgreiches Shoulder-Surfing verhindern.

Natürlich ist es möglich sich dadurch gegen potentielle Angreifer zu schützen, dass das Smartphone sehr nah am Körper gehalten wird. Dies gilt allerdings nur für den Fall, dass sich der Angreifer versetzt hinter dem Benutzer befindet. Auf diese Weise ist es dem Angreifer nicht einmal möglich, das Gerät zu sehen, geschweige denn den Displayinhalt. Solches Verhalten entspricht allerdings nicht den Gepflogenheiten und wäre darüber hinaus in aller Regel umständlich und wenig benutzerfreundlich. In den anderen Fällen wäre der Schutz bei einem solchen Verhalten ohnehin reduziert.

Die Empfehlungen lassen sich wie folgt zusammenfassen:

- Verwendung der Folie von Belkin
- Bei Dunkelheit besonders auf potentielle Angreifer achten
- Insbesondere auf Personen hinter und neben einem achten
- Durch Neigung des Smartphones Blickwinkel verändern
- Smartphone nah am Körper halten

5 Analyse der vorgeschlagenen Authentisierungsverfahren

Die in Kapitel 3.3 vorgeschlagenen Verfahren, zufällig angeordnete Zahlen beziehungsweise Bilder, sollen im Folgenden bezüglich der Kriterien analysiert werden. Mit Hilfe einer Studie sollte herausgefunden werden, wie die ausgewählten Verfahren im Vergleich zum Standard PIN-Verfahren abschneiden. Ziel der Studie war herauszufinden, ob eines dieser Verfahren besser ist und damit das PIN-Verfahren ersetzen kann.

Zu Beginn dieser Arbeit sollte die Studie als eine Feldstudie durchgeführt werden. Dabei sollten die beiden Authentisierungsverfahren als App realisiert werden, die der Teilnehmer als Ersatz für sein bisheriges Verfahren verwendet. Da es bei Android jedoch nicht möglich ist eine App vollständig als Ersatz für die Authentisierung zu verwenden, wurde dieser Gedanke wieder verworfen. Die andere Möglichkeit war, dass jeder Teilnehmer die App jeden Tag manuell starten muss um sich zu authentisieren. Auch diese Idee wurde nicht verwendet, da sich vollkommen auf die Teilnehmer verlassen werden müsste, dass sie täglich teilnehmen. Eine Android-App hatte auch noch andere Nachteile, einerseits die Rekrutierung von genügend Android-Nutzern und andererseits die Verteilung und Installation der App. Eine Veröffentlichung im GooglePlay Store sollte vermieden werden, damit ansonsten niemand die App installieren würde, der nicht an der Studie teilnimmt und damit die Ergebnisse verfälschen könnte.

Aus diesem Grund wurde entschieden, die Studie online durchzuführen. Dabei wurde unter anderem auch die Effizienz und die Effektivität dieser Verfahren genauer untersucht.

Dieses Kapitel teilt sich in vier Unterkapitel auf. Zuerst werden die Hypothesen vorgestellt und näher erläutert. Danach wird das Studiendesign erklärt, das heißt wie die Online-Studie aufgebaut ist. Anschließend wird die Durchführung beschrieben und insbesondere auf die die während der Durchführung auftretenden Probleme eingegangen. Abschließend wird das Ergebnis vorgestellt und interpretiert.

5.1 Fragestellung

In diesem Unterkapitel werden die Hypothesen beschrieben, die mit Hilfe der Online-Studie überprüft werden sollten. Die ersten sechs beschreiben den Zusammenhang zwischen dem Standard PIN-Verfahren und den Verfahren mit zufällig angeordneten Feldern (Zahlen beziehungsweise Bilder).

- **H1**: Das Verfahren mit zufällig angeordneten Bildern ist nicht signifikant weniger effizient als das Standard PIN-Verfahren.
- **H2**: Das Verfahren mit zufällig angeordneten Zahlen ist nicht signifikant weniger effizient als das Standard PIN-Verfahren.
- **H3**: Das Verfahren mit zufällig angeordneten Bildern ist nicht signifikant weniger effektiv als das Standard PIN-Verfahren.
- **H4**: Das Verfahren mit zufällig angeordneten Zahlen ist nicht signifikant weniger effektiv als das Standard PIN-Verfahren.

Weitere drei Hypothesen beschreiben den Vergleich von grafischen Verfahren mit solchen, die auf zufällig angeordneten Zahlen basieren. In der Literatur wird im allgemeinen die Auffassung vertreten, dass grafische Verfahren besser einprägsam seien als solche, die auf Zahlen beruhen.

Laut des „Picture superiority“-Effekts [Sta73] können Menschen sich Bilder besser merken als Wörter, beziehungsweise Zahlen. Die Wirkung dieses Effekts wird von der „Dual-Coding“-Theorie [Pai91] unterstützt, die besagt, dass Bilder in mehreren Darstellung im Gehirn gespeichert werden, einmal visuell und einmal verbal. Studien haben belegt, dass Benutzer sich Bilder über einen langen Zeitraum merken können [BS00]. Außerdem kann die Einprägsamkeit durch bereits existierendes Wissen eines Benutzers unterstützt werden, anstatt sich neue oder zufällige Informationen zu merken [BCV12] [Sch+13].

Wird nun angenommen, dass die Faktoren Effizienz, Effektivität und Zufriedenheit aufgrund ihrer Definitionen nicht vollkommen unabhängig von der Einprägsamkeit sind, kann davon ausgegangen werden, dass die Einprägsamkeit ebenfalls einen positiven Einfluss auf diese Kriterien hat. Daraus ergeben sich nun die drei folgenden Hypothesen:

- **H5**: Das Verfahren mit zufällig angeordneten Bildern ist signifikant effizienter als das Verfahren mit zufällig angeordneten Zahlen.
- **H6**: Das Verfahren mit zufällig angeordneten Bildern ist signifikant effektiver als das Verfahren mit zufällig angeordneten Zahlen.
- **H7**: Die Zufriedenheit der Benutzer bei dem Verfahren mit zufällig angeordneten Bildern ist signifikant größer als bei dem Verfahren mit zufällig angeordneten Zahlen.

In dieser Studie werden die drei Kriterien, Effizienz, Effektivität und Zufriedenheit der Teilnehmer gemessen. Die **Effizienz** bemisst sich anhand der Zeitdauer, die ein Benutzer für die Authentisierung benötigt. Dabei werden, wie in Kapitel 2.2 beschrieben, Orientierungszeit und Eingabezeit unterschieden. Die **Effektivität** wird anhand der Erfolgsquote gemessen, das heißt, wie oft sich ein Benutzer korrekt und ohne Fehler authentisiert. Die **Zufriedenheit** der Teilnehmer wird anhand des Fragebogens ermittelt, in dem sie unter anderem beantworten mussten, ob sie das Verfahren in Zukunft gerne einsetzen würden.

5.2 Studiendesign

Die Online-Studie wurde in eine umfangreiche Studie mit insgesamt acht Verfahren eingebettet, die in Zusammenarbeit mit Frau Dr. Karen Renaud von der Universität Glasgow durchgeführt wurde. Sie besteht aus fünf verschiedenen Teilen, die in dieser Arbeit als **Sessions** bezeichnet, werden. Lediglich die ersten beiden Sessions werden hier ausgewertet und im Folgenden näher erläutert.

Bei den anderen, nicht analysierten Verfahren, handelt es sich um die Code-Eingabe, bei welcher der Code zu Beginn dreimal animiert dargestellt wird und um die Eingabe, bei welcher der Teilnehmer den Code einmalig dreimal hintereinander eingeben muss.

5.2.1 Session Anmeldung

In der ersten Session registriert sich ein Teilnehmer mit seiner E-Mail-Adresse auf der Startseite der Online-Studie. Die Startseite besteht aus einer Webseite mit einer Beschreibung des Ablaufs der Studie und allgemeinen Informationen. Nach Eingabe der E-Mail-Adresse wird er auf die nächste Seite weitergeleitet. Dort befindet sich ein Fragebogen zur Demografie und allgemeinen Fragen zum Thema PIN, siehe Anhang Abbildung 30. Danach wird jeder Teilnehmer zufällig einer von acht verschiedenen Gruppen zugeordnet, wobei jede Gruppe mit einem bestimmten Verfahren verknüpft ist. Zufällig heißt in

diesem Fall, dass die einzelnen Teilnehmer nacheinander den Gruppen eins bis acht zugeteilt werden, damit jede Gruppe die gleiche Anzahl an Personen umfasst.

Um ein aussagekräftiges Ergebnis zu erhalten, wurde eine Gruppengröße von mindestens 20 Personen pro Verfahren bestimmt. Der für das Thema Benutzerfreundlichkeit bekannte Wissenschaftler Jakob Nielsen[10] gibt an, dass diese Anzahl normalerweise ausreicht um Benutzerfreundlichkeit zu testen. Da es insgesamt acht verschiedene Verfahren gibt, wurden mindestens 160 Teilnehmer für diese Studie benötigt. Die Gleichverteilung auf die Gruppen wird, wie oben beschrieben, durch entsprechende Zuteilung gewährleistet.

Generell unterscheiden sich die Verfahren dadurch, dass die einzelnen Tasten des Eingabefeldes entweder aus zehn Zahlen oder zehn Bildern bestehen. Im Folgenden wird die Kombination aus Zahlen beziehungsweise Bildern als **Code** bezeichnet. Zu Beginn bekam jeder Teilnehmer einen vierstelligen Code zugewiesen. Die Zuweisung sollte verhindern, dass der Teilnehmer sich einen Code wählt, der aufgrund seiner Eigenschaften unsicher oder besonders leicht zu merken ist. Als unsicher gilt eine Code dann, wenn die selbe Zahl mehrfach vorkommt, beispielsweise „1, 1, 1, 1“ oder wenn er aus einer Zahlenfolge besteht der natürlichen Ordnung der Zahlen entspricht, beispielsweise „1, 2, 3, 4, ...“. Entsprechendes gilt bei der mehrfachen Verwendung des selben Bildes. Vier für diese Arbeit relevante Verfahren werden genauer analysiert: Eines mit fest platzierten Zahlen, ein anderes mit zufällig angeordneten Zahlen und zwei weitere analog mit Bildern. Sie werden im Folgenden näher erläutert.

Die Eingabe des vierstelligen Codes erfolgt durch Klicken auf die einzelnen Zahlen/Bilder-Buttons, siehe Abbildung 17. Sobald vier Stellen eingegeben wurden, erscheint auf der rechten unteren Seite ein grüner „OK“-Button. Es ist nicht möglich, mehr als vier Stellen einzugeben. Weitere Klicks auf den Button werden ignoriert. Jede eingegebene Stelle wird oberhalb der Zahlen-/Bilder-Buttons als schwarzer Kreis dargestellt, wie auch bei vielen Smartphones. Durch das Klicken auf ein Symbol, bekannt aus Android und IOS, neben den schwarzen Kreisen ist es möglich, Ziffern zu löschen. Sobald Zahlen/Bilder mit Hilfe des „Löschen“-Buttons gelöscht werden, verschwindet auch der „OK“-Button wieder. Damit wird verhindert, dass ein Code mit einer ungültigen Länge eingegeben wird. Durch einen Klick auf den „OK“-Button ist die Eingabe abgeschlossen.

In jeder Session wird nach Abschluss der Code-Eingabe geprüft, ob der eingegebene Code dem zu Beginn zugewiesenen entspricht. Bei Eingabe des korrekten Codes wird der Teilnehmer auf eine neue Seite weitergeleitet und ihm für die Teilnahme gedankt. Damit hat der Teilnehmer die erste Session erfolgreich abgeschlossen.

Sollte der eingegebene Code nicht korrekt sein, hat der Teilnehmer zwei weitere Versuche, wie bei Eingabe der PIN beim Smartphone. Gibt er bei einem dieser Versuche den Code korrekt ein, wird er - wie oben beschrieben - weitergeleitet. Im anderen Fall wird er auf eine andere Seite weitergeleitet, bei der er die Möglichkeit hat, die Studie erneut mit ersten Session zu beginnen. Sollte er sich entschließen, die Studie erneut zu starten, wird er auf die Startseite der Studie weitergeleitet. Durch die Eingabe seiner E-Mail-Adresse wird ihm abermals zufällig ein Verfahren zugeteilt. Sollte er sich stattdessen dafür entscheiden, das Browser-Fenster zu schließen, wird seine Eingabe gespeichert, und die Studie ist für ihn beendet.

[10] Nielsen Norman Group: http://www.nngroup.com/articles/quantitative-studies-how-many-users/ (abgerufen am 23.07.2014)

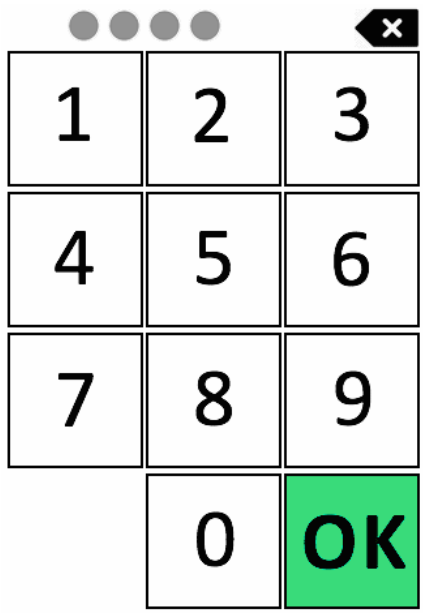


Abbildung 17: Eingabe des Codes

5.2.2 Session Code Eingabe

Nach erfolgreichem Durchlaufen der ersten Session bekommt jeder Teilnehmer einen Tag später eine E-Mail. Darin wird er aufgefordert, sich mit dem in der ersten Session festgelegten Code zu authentisieren. Nach Eingabe des korrekten Codes befindet er sich in der nächsten Session. Bei einer Falscheingabe verhält sich das System wie in der ersten Session. Bei beiden Verfahren mit den zufällig angeordneten Feldern werden diese in jeder Session und auch bei jedem weiteren Versuch wiederum zufällig angeordnet.

Nach der zweiten Session erhält der Teilnehmer einen Fragebogen mit Fragen, wie er sich den Code merken konnte, siehe Anhang Abbildung 31 und Abbildung 32. Zusätzlich bekommen die Teilnehmer mit zufällig angeordneten Feldern weitere Fragen, zum Beispiel wie sie zufällige Anordnung beeinflusst hat, siehe Kapitel 5.2.4.

5.2.3 Folgende Sessions

Nach Abschluss der zweiten Session erhält ein Teilnehmer zwei Tage später eine E-Mail, nach sechs Tagen und nach weiteren 31 Tagen jeweils noch eine. Anders gesagt erhält der Teilnehmer eine E-Mail an Tag 1, Tag 3, Tag 10 und Tag 41. In jeder Session hat er drei Versuche, den Code korrekt einzugeben, gelingt ihm das nicht, hat er die Möglichkeit, von vorne zu beginnen.

Nach der fünften und letzten Session wird der Teilnehmer gefragt, ob er Anmerkungen zu der Studie hat, beim Gewinnspiel teilnehmen und über das Ergebnis der Studie informiert werden möchte.

5.2.4 Gruppierung des Fragebogens anhand des Kriteriums Zufriedenheit

In diesem Abschnitt wird der zweite Fragebogen vorgestellt, welchen die Teilnehmer während der Studie ausfüllen mussten.

Da bei dieser Studie noch weitere Verfahren evaluiert werden, sind für diese Arbeit nicht alle Fragen relevant. Aus diesem Grund werden nicht alle Fragen genauer erläutert. Der vollständige Fragebogen ist im Anhang zu finden.

Hinter jeder Frage stehen in Klammern die Antwort-Möglichkeiten. Beispielsweise bedeutet (TEXT), dass bei dieser Frage eine freie Antwort in ein Textfeld geschrieben werden sollte.

Zufriedenheit

Bei der folgende Frage hatte der Teilnehmer die Möglichkeit, die Eingabe auf den zufällig angeordneten Eingabefeldern zu bewerten. Es sollte herausgefunden werden, ob er die zufällige Anordnung der Eingabefelder als störend empfand.

> *Inwieweit hat Sie das Mischen des Eingabefeldes (zufällige Reihenfolge) bei Eingabe der PIN beeinflusst? (TEXT)*

Anschließend wird in einem kurzen Absatz der Mehrwert eines solchen Verfahrens erläutert. Der Teilnehmer sollte angeben, ob er dieses Verfahren im Alltag verwenden würde. Zusätzlich wurde er gebeten einige Situationen zu nennen, in denen er das Verfahren als störend empfinden würde.

> *Bei diesem Verfahren werden die Zahlen/Bilder auf dem PINPad bei jeder Eingabe in einer zufälligen Reihenfolge angezeigt. Dadurch ist Ihr Code besser geschützt, da Leute, die Ihnen über die Schulter schauen (sogenanntes Schulter-Surfen), sich Ihren Code nur sehr schwer merken können.*
>
> *Ich würde mich in Zukunft gerne gegen Schulter-Surfen schützen und daher dieses Verfahren auf meinem Smartphone einsetzen. (JA/NEIN)*
>
> *Wenn Sie sich die Verwendung prinzipiell vorstellen können, können Sie sich Situationen vorstellen, bei denen dieser Ansatz störend ist? (TEXT)*

5.3 Durchführung

In diesem Kapitel wird die Durchführung der Studie genauer beschrieben. Dabei geht es besonders um die technischen Details, um Pretests, die vor dem offiziellen Start der Studie durchgeführt wurden, um Fehler zu finden, um technische Probleme die während der Durchführung aufgetreten sind und um die Rekrutierung von Teilnehmern.

5.3.1 Technische Durchführung

Das Konzept der Studie wurde in Zusammenarbeit mit Frau Professor Dr. Volkamer und Frau Dr. Renaud erarbeitet. Die grundlegende Programmierung wurde von Dr. Renaud erstellt, während spätere Verbesserungen gemeinsam vorgenommen wurden. Die Übersetzung in die deutsche Sprache sowie diverse Tests bezüglich Fehlern erfolgte durch die Autoren.

Der Server, auf dem die Studie ausgeführt wurde gehört der Universität Glasgow. Bei der Programmierung wurde Cold Fusion von Adobe Systems, ein Apache Web Server und eine MySql Datenbank verwendet. Teilweise wurde für die Darstellung Javascript und jquery eingesetzt.

Die E-Mails wurden mit Hilfe eines Python-Skripts, siehe Anhang 1 auf einem Server mit Ubuntu versandt. Dieses Skript wurde täglich um 10 Uhr durch einen Eintrag in der Cron-Tabelle gestartet. Es sandte einen Request an eine vorher eingerichtete Webseite, die sämtliche E-Mail-Adressen mit passenden Links und der aktuellen Session von den Teilnehmern enthielt, welche an diesem Tag in eine neue Session gekommen waren. Das Skript sandte selbstständig eine E-Mail mit dem passenden Text und Link an die entsprechende E-Mail-Adresse und speicherte, sofern erfolgreich, die Informationen zu Debug-Zwecken in einer Log-Datei. Falls ein Teilnehmer versuchte, während er auf die nächste E-Mail wartete, sich mit der selben E-Mail-Adresse zu registrieren, wurde ihm nur die Webseite mit dem Dank für seine Teilnahme angezeigt.

5.3.2 Pretest

Vor dem Start der Studie wurden diverse Testdurchläufe durchgeführt, um abschließend potentielle Probleme zu identifizieren und Formulierungen zu verbessern. Dabei wurden geringfügige Designänderungen vorgenommen und Fehler behoben. Danach erfolgten erneut mehrere Tests.

Im Anschluss daran wurde mit Teilnehmern aus dem Familien- und Freundeskreis ein weiterer Test durchgeführt. Sie sollten ein paar Tage vor dem offiziellen Start der Studie beginnen, um den anderen Teilnehmern immer mindestens eine Session voraus zu sein. Da bei diesem Durchlauf keine weiteren Fehler auftraten, konnten die Personen auch in die Studie einbezogen werden.

5.3.3 Technische Probleme

Während der Durchführung der Studie traten einige Probleme auf, die im Folgenden näher erläutert werden:

Zu Beginn der Studie konnten beispielsweise die Fragebögen bei der zweiten Session teilweise nicht gespeichert werden und wurden deswegen in den nächsten Sessions erneut angezeigt. Dieser Fehler beruhte darauf, dass Anführungszeichen in einem Textfeld den Fragebogenteil abstürzen ließ und deswegen nicht gespeichert werden konnte. Zu Beginn der darauf folgenden Session wurde vom System eine Überprüfung durchgeführt, ob für den Teilnehmer bereits ein Fragebogen gespeichert wurde. Anderenfalls wurde dieser erneut angezeigt. Als der Fragebogen erneut beantwortet werden sollte, wurden von manchen Teilnehmern die Freitextfelder teilweise nicht ausgefüllt. Sofern ein Teilnehmer erneut Anführungszeichen verwendete, trat der Fehler wieder auf. Die Fragebögen dieser Teilnehmer wurden nach der Studie aussortiert und nicht für die Auswertung verwendet, da sie in einer anderen Session und damit zu einem anderen Zeitpunkt als vorgesehen, beantwortet wurden.

Ein weiteres Problem war der festgelegte „Timeout“ bei jeder Session. Zu Beginn der Studie hatte jeder Teilnehmer lediglich 60 Minuten Zeit, um seinen Code einzugeben. Sofern er erst nach Ablauf dieser Zeit auf den Link geklickt hatte, wurde er auf die Seite mit dem Dank für seine Teilnahme weitergeleitet. Nachdem dieses Problem erkannt war, wurde die Zeitspanne auf zehn Stunden erweitert und die E-Mail um den Hinweis ergänzt, dass es zu einem Timeout kommen kann, wenn zwischen dem Klicken auf den Link und der Eingabe des Codes mehr als zehn Stunden verstreichen. Die Teilnehmer, bei denen dieser Fall auftrat, konnten identifiziert werden und haben eine neue Mail mit einem anderen Link erhalten. Die Ergebnisse dieser Teilnehmer wurden dennoch aussortiert, da bei ihnen der Abstand der einzelnen Sessions nicht konstant war.

Aus dem vorigen Problem hat sich ein weiteres ergeben. Sobald ein Teilnehmer auf den Link in der E-Mail geklickt hat, wurde die nächste Session gestartet. Dieser Vorgang kann aufgrund der Implementierung in Cold Fusion nicht rückgängig gemacht werden. Jeder Teilnehmer, der auf den Link in der E-Mail geklickt und die Webseite daraufhin geschlossen hat ohne seinen Code einzugeben, beendete die Session damit vorzeitig. Aus diesem Grund war es ihm nicht möglich, den Link in der E-Mail erneut anzuklicken, da er so behandelt wurde wie Teilnehmer, der die Session ordnungsgemäß abgeschlossen hat. Um dieses Problem zu vermeiden, wurde die Mail um einen Absatz ergänzt, in dem empfohlen wurde, sich bei diesem Problem an die Autoren der Online-Studie zu wenden. Sie konnten dann einen neuen Link bekommen, um die Session erfolgreich zu beenden. Das Problem trat nur im Zusammenhang mit dem „Timeout“ auf. Nach dessen und der Ergänzung der Mail ist das Problem nicht mehr aufgetreten. Die betroffenen Personen, wurden dennoch in die Auswertung nicht einbezogen.

Ein weiteres Problem war das Cache-Management der angezeigten Grafiken. Damit bei den Verfahren bei denen die Eingabefelder zufällig angeordnet sind, keine falschen Grafiken angezeigt werden, wurde der Cache für diese deaktiviert und ein Nachladen erzwungen. Das hatte zur Folge, dass die Grafiken bei jedem Aufruf neu geladen werden mussten und es bei der Anzeige einer kurzen Verzögerung kam. Aus diesem Grund wurden für die Eingabefelder mit Zahlen auch Grafiken verwendet, um die Ladezeiten bei allen Verfahren zu vereinheitlichen.

Zwei Teilnehmer haben berichtet, dass sich, nachdem sie auf den Link in der Mail geklickt hatten, eine Webseite mit der Fehlermeldung „Die Verbindung zum Server wurde zurückgesetzt, während die Seite geladen wurde.“ erschien. Dieser Fehler konnte, auch nach verschiedenen Tests, nicht nachvollzogen werden. Beide Teilnehmer haben umgehend einen neuen Link bekommen und sich daraufhin erfolgreich gemeldet. Aus diesem Grund wurden keine weiteren Maßnahmen ergriffen.

Insgesamt sind bei der Studie einige technische Probleme aufgetreten, die jedoch durch verschiedene Maßnahmen gelöst werden konnte. Die jeweils betroffenen Personen wurden vor der Auswertung der Studie aussortiert und beeinflussen daher das Ergebnis nicht.

5.3.4 Rekrutierung von Teilnehmern

Um ausreichend Teilnehmer für die Online-Studie zu finden wurde ein DIN-A5 Plakat erstellt, siehe Anhang Abbildung 29 und an Pinnwänden innerhalb der Universität und an öffentlichen „Schwarzen Brettern“, wie beispielsweise in Supermärkten, angebracht.

Außerdem wurde die Studie in diversen Foren vorgestellt und per E-Mail an Freunde, Bekannte und Verwandte geschickt.

Zusätzlich hatten Psychologiestudierende der Technischen Universität Darmstadt die Möglichkeit, für ihre Teilnahme eine halbe Versuchspersonenstunde zu bekommen. Dazu mussten sie nach der letzten Session ein Kästchen ankreuzen, um damit zu dokumentieren, dass sie Psychologiestudierende sind. Innerhalb von zwei Wochen erhielten Sie eine E-Mail mit einem Code, den sie gegen Anrechnung der halben Versuchspersonenstunde einlösen konnten.

Außerdem bestand die Möglichkeit einen 40€ Amazon-Gutschein zu gewinnen.

5.4 Ergebnis

In diesem Kapitel werden die Ergebnisse der Online-Studie vorgestellt. Für die Auswertung der offenen Fragen wurden jeweils Kategorien festgelegt und die Antworten entsprechend eingeordnet. Die passenden Kategorien haben beide Autoren unabhängig voneinander entwickelt. Anschließend wurde die Schnittmenge der Kategorien ermittelt und für die Auswertung der Studie zugrunde gelegt, um eine hohe Interrater-Reliabilität zu gewährleisten.

Insgesamt konnten von den 214 Teilnehmern 172 Datensätze für die Auswertung genutzt werden. Acht Teilnehmer haben angegeben, dass sie sich ihren Code aufgeschrieben haben, daher wurden diese Datensätze entfernt. Des Weiteren wurden Datensätze aufgrund der in Kapitel 5.3.3 beschriebenen Probleme aussortiert.

5.4.1 Auswertung der Fragebögen

Im Folgenden werden die Auswertungen der beiden Fragebögen ausführlich dargestellt.

Daten des ersten Fragebogens

Bei der Auswertung der demografischen Daten ergab sich das von den 172 Teilnehmern 119 männlich und 53 weiblich waren. Der Anteil Männer war damit doppelt so hoch wie derjenige der Frauen. Mit 133 Teilnehmern jünger als 29 Jahre liegt der Altersdurchschnitt bei weniger als 30 Jahren, siehe im Einzelnen Abbildung 18.

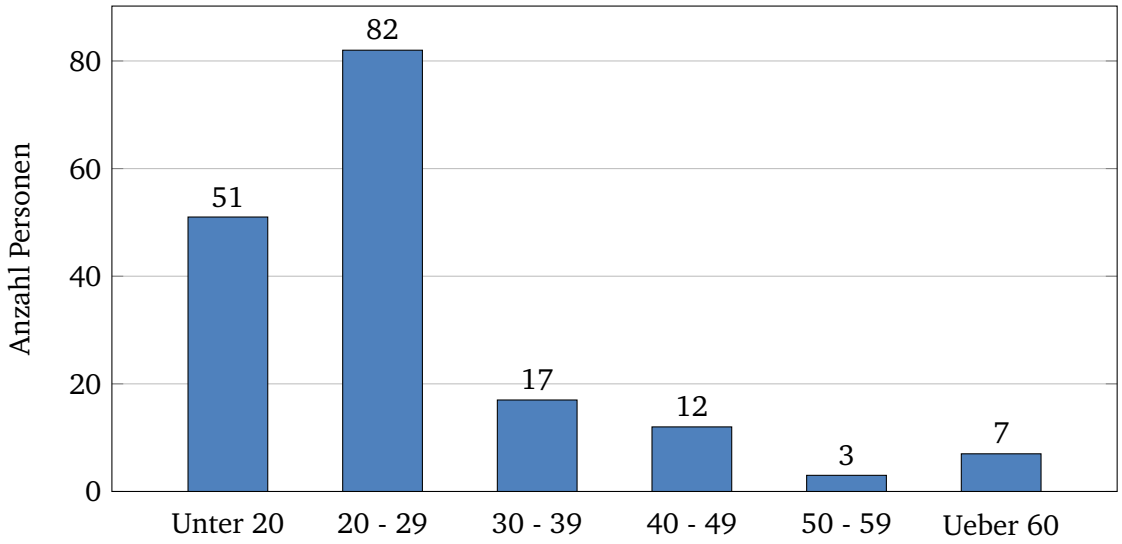


Abbildung 18: Verteilung der Altersgruppen

Alle Teilnehmer besitzen ein Smartphone, benutzen allerdings sehr unterschiedlich Authentisierungsverfahren. Immerhin 13% der Teilnehmer verzichten auf jegliche Authentisierung. Das am häufigsten verwendete Verfahren ist die klassische PIN (40%) gefolgt vom Android-Muster (23%), siehe im Einzelnen Abbildung 19.

40% der Teilnehmer vergessen häufig ihre PIN. Allerdings empfinden es nur 36% der Teilnehmer als schwer, sich eine PIN zu merken.

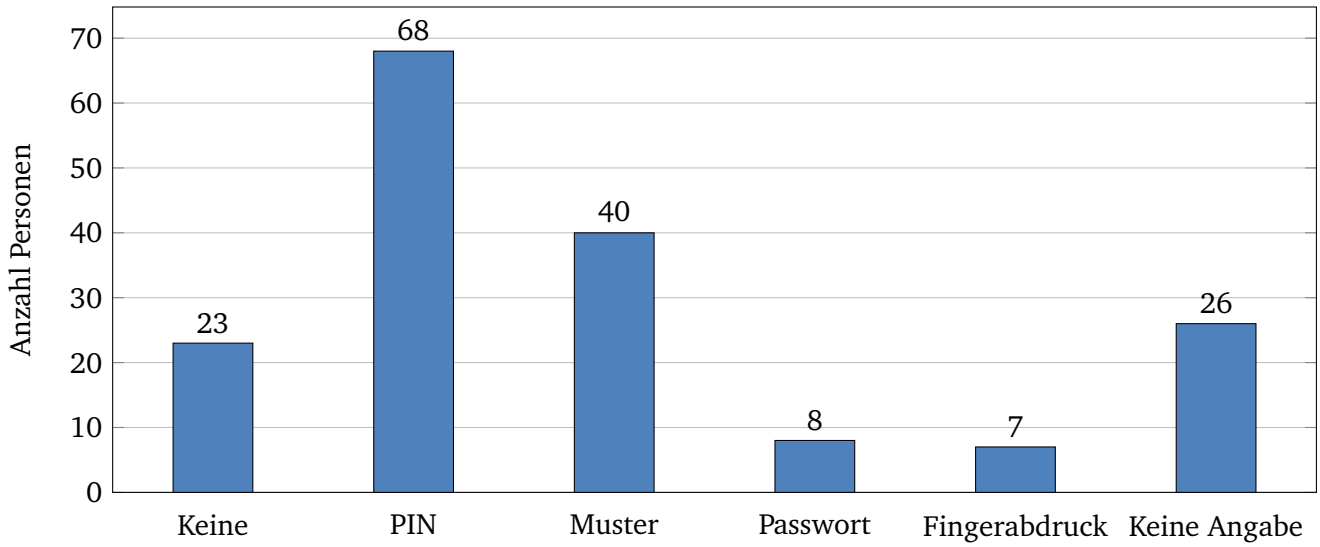


Abbildung 19: Verteilung der Authentisierungsverfahren

Daten des zweiten Fragebogens

Bei der Auswertung des zweiten Fragebogens wurden nicht alle acht verschiedenen Gruppen untersucht, sondern nur die Gruppen 1 (Zahlen mit festgelegter Position), 4 (Zahlen mit zufälliger Anordnung), 5 (Bilder mit festgelegter Position) und 8 (Bilder mit zufälliger Anordnung).

Bei der ersten Frage, ob der Teilnehmer es bei der Anmeldung als schwer empfand, sich den Code zu merken, ergaben sich bereits einige Unterschiede. Während es bei den Gruppen mit Zahlen 16% beziehungsweise 19% schwer einschätzten, beschränkte sich dies bei den beiden Gruppen mit den Bildern auf 10% beziehungsweise 6%, siehe im Einzelnen Tabelle 3.

Tabelle 3: Fiel es Ihnen schwer, sich an den Code zu erinnern, als Sie sich angemeldet haben und sich den Code versucht haben zu merken?

	Gruppe 1	**Gruppe 4**	**Gruppe 5**	**Gruppe 8**
Ja	3	2	3	1
Nein	15	17	11	16
Enthaltung	-	1	2	-

Den Teilnehmern aus den Gruppen mit Zahlen fiel es bei der erneuten Rückkehr mit 22% beziehungsweise 35% noch einmal deutlich schwerer bei den beiden anderen Gruppen mit jeweils 6%, siehe Tabelle 4.

Tabelle 4: Fiel es Ihnen schwer, sich an den Code zu erinnern, als Sie Ihren Code heute eingegeben haben?

	Gruppe 1	**Gruppe 4**	**Gruppe 5**	**Gruppe 8**
Ja	4	7	1	1
Nein	14	12	13	16
Enthaltung	-	1	2	-

Mit einem Schnitt von 2.2, 2.5, 2.3 und 1.6 auf einer Skala von 0 - 5, wobei 0 einer Enthaltung entspricht, waren die Teilnehmer generell nicht über ihre Leistung überrascht, siehe Tabelle 5.

Tabelle 5: Falls Sie sich an den Code erinnern konnten, waren Sie überrascht, dass Sie sich den Code merken konnten?

	0 (Nicht überrascht)	1	2	3	4	5 (Sehr überrascht)
Gruppe 1	1	7	4	2	2	2
Gruppe 4	3	2	5	5	3	2
Gruppe 5	2	2	6	2	4	0
Gruppe 8	2	7	5	1	2	0

Die nächsten Fragen beziehen sich auf die Art und Weise, wie ein Teilnehmer sich seine PIN beziehungsweise seinen Code merkt, ob für Bank, Smartphone oder diese Online-Studie. Dafür wurden folgende Kategorien erstellt: Leer/ungeeignet, Lerneffekt (Muster), bekannte Kombination, Auswendig lernen, eigene Brücke, aufschreiben, kein Code. Die Kategorie *Lerneffekt* meint einen motorischen Lerneffekt, den der Teilnehmer durch häufige Eingabe eines gewissen Musters auf dem Eingabefeld erfährt. *Bekannte Kombination* bedeutet, dass der Teilnehmer sich den Code anhand einer bereits bekannten Kombination merkt, bei einer PIN zum Beispiel ein Geburtsdatum. Unter *Auswendig lernen* ist zu verstehen, dass der Benutzer ohne jegliches Muster oder Gedächtnisbrücke versucht, den Code zu behalten. Die Kategorie *Eigene Brücke* bedeutet, dass sich der Benutzer durch eine eigene Technik versucht, den Code zu merken.

Um eine bessere Übersicht zu gewähren, werden hier nur die am häufigsten genannten Kategorien hervorgehoben, angefangen mit der Bankkarte. Mit 31 beziehungsweise 26 Nennungen wurden hierbei *Auswendig lernen* beziehungsweise der *Lerneffekt* (Muster auf dem Eingabefeld) genannt. Beim Smartphone ist der Lerneffekt mit 24 Nennungen dominierend, gefolgt von der *bekannten Kombination* mit 18 Nennungen, siehe im Einzelnen Tabelle 6.

Tabelle 6: Wie versuchen Sie, sich den Code für Ihre Bankkarte zu merken?

	Gruppe 1	Gruppe 4	Gruppe 5	Gruppe 8
Keine Angabe / ungeeignet	4	2	2	-
Lerneffekt (Muster)	5	9	2	10
Bekannte Kombination	1	3	1	1
Auswendig Lernen	10	4	10	7
Kein Code	-	-	-	-
Aufschreiben	1	2	2	-
Eigene Brücke	1	1	2	1

Für den Code für dieses Experiment wurden die Ergebnisse wiederum nach Gruppen aufgeteilt. Gruppe 1 merkt sich diesen hauptsächlich durch den *Lerneffekt* oder eine *eigene Brücke*. Alle anderen Gruppen hingegen *lernen* diesen *auswendig* oder nutzen vor allem wieder eine *eigene Brücke*, siehe Tabelle 7. Für das Smartphone vergleiche Tabelle 8.

Einige der Teilnehmer sind der Meinung, dass sie sich Bilder besser merken können als Zahlen und zwar mit 33%, 40%, 38% und 53%. Das bedeutet im Schnitt bei 41%, siehe Tabelle 9.

Für die Frage, ob die zufällige Anordnung (Mischen) die Teilnehmer beeinflusst, hat wurden die fünf folgenden Kategorien aufgestellt: gar nicht, Zeit/Aufwand, Lernfaktor, besser merkbar, weiß nicht.

Tabelle 7: Wie versuchen Sie, sich den Code für Ihr Smartphone zu merken?

	Gruppe 1	Gruppe 4	Gruppe 5	Gruppe 8
Keine Angaben / ungeeignet	5	6	2	3
Lerneffekt (Muster)	6	7	3	8
Bekannte Kombination	4	4	6	4
Auswendig Lernen	2	1	4	3
Kein Code	2	1	1	-
Aufschreiben	-	1	-	-
Eigene Brücke	1	-	1	-

Tabelle 8: Wie versuchen Sie, sich den Code für dieses Experiment zu merken?

	Gruppe 1	Gruppe 4	Gruppe 5	Gruppe 8
Keine Angabe / ungeeignet	3	4	3	2
Lerneffekt (Muster)	6	-	2	-
Bekannte Kombination	1	1	-	-
Auswendig Lernen	3	7	6	4
Kein Code	-	-	-	-
Aufschreiben	-	-	-	-
Eigene Brücke	5	8	6	9

Tabelle 9: Haben Sie das Gefühl, Sie können sich generell Bilder besser merken als Zahlen?

	Gruppe 1	Gruppe 4	Gruppe 5	Gruppe 8
Ja	6	8	6	9
Nein	4	4	4	4
Enthaltung	-	1	-	-

Die Kategorie *Zeit/Aufwand* beinhaltet Aussagen, die sich zum Beispiel auf stressige Situationen beziehen in denen sie allgemeinen mehr Zeit benötigen, um sich zu authentisieren. In beiden Gruppen mit zufälliger Reihenfolge beklagten sich die Teilnehmer über den fehlenden Lerneffekt wegen des fehlenden Musters auf dem Eingabefeld. Drei Teilnehmer meinten, sie könnten sich ihren Code auf diese Weise besser merken, da sie sich durch den fehlenden Automatismus mehr auf den Code selbst konzentrieren müssten. Siehe im Einzelnen Tabelle 10.

Tabelle 10: Inwieweit hat Sie das Mischen des Eingabefeldes (zufällige Reihenfolge) bei Eingabe der PIN beeinflusst?

	Gruppe 4	**Gruppe 8**
Gar nicht	3	4
Zeit / Aufwand	2	1
Lernfaktor (Merken nach Position)	9	6
Besser merkbar	1	2
Weiß nicht	1	1
Keine Angabe	5	3

Die nächste Frage soll herausstellen ob die Teilnehmer ein Verfahren nutzen würden, bei denen die Eingabefelder zufällig angeordnet sind wird, um sich gegen Shoulder-Surfing zu schützen. 45% der Gruppe 4 kann sich vorstellen, ein solches Verfahren zu nutzen, sogar 59% der Gruppe 8. Siehe Tabelle 11.

Tabelle 11: Ich würde mich in Zukunft gerne gegen Schulter-Surfen schützen und daher dieses Verfahren auf meinem Smartphone einsetzen.

	Gruppe 4	**Gruppe 8**
Ja	9	10
Nein	10	7
Enthaltung	1	-

Bei der nächsten Frage wird davon ausgegangen, dass sich die Teilnehmer die Verwendung prinzipiell vorstellen können, aber sie im Einzelfall möglicherweise als störend empfinden. Dafür wurden folgende Kategorien erstellt: Nein, Immer, Zeit/Aufwand, Sichtverhältnisse und Unterkategorie. In Gruppe 8 waren neun Teilnehmer entweder der Meinung, die zufällige Anordnung der Bilder störe sie nicht oder haben keine Situation genannt. Vier Teilnehmer sind der Meinung, dass die zufällige Anordnung der Zahlen immer bei der Benutzung stört und unter anderem den bekannten Lerneffekt verhindert. Insgesamt acht Teilnehmer aus beiden Gruppen haben angemerkt, dass die Authentisierung mit zu viel Aufwand verbunden sei. Die Kategorie *Sichtverhältnisse* beinhaltet Situationen, wie eine verdeckte Eingabe oder auch die Eingabe des Codes, ohne auf das Display zu schauen. Ein Großteil der Benutzer beider Gruppen hat keine Antwort abgegeben oder ist der Kategorie *Nein* zuzuordnen. Siehe im Einzelnen Tabelle 12.

Im Folgenden wird genauer auf die für die Authentisierung benötigten Zeiten eingegangen. Diese werden in die bereits erwähnte Orientierungszeit und die tatsächliche Eingabezeit aufgeteilt.

Mitglieder der Gruppe 1 haben im Durchschnitt rund 26 Sekunden für die Orientierung und rund 29 Sekunden für die Eingabe benötigt. Die entsprechenden Daten für die Gruppe 4 betragen durchschnittlich 41 und 32 Sekunden, 31 und 43 Sekunden für die Gruppe 5. In Gruppe 8 finden sich die höchsten Zeiten mit 56 und 46 Sekunden. Siehe im Einzelnen Tabelle 13.

Tabelle 12: Wenn Sie sich die Verwendung prinzipiell vorstellen können, können Sie sich Situationen vorstellen, bei denen dieser Ansatz störend ist?

	Gruppe 4	Gruppe 8
Nein	1	4
Immer	4	1
Zeit/Aufwand	3	5
Sichtverhältnisse	2	2
Sonstiges	1	1
Keine Angabe	10	5

Tabelle 13: Authentifizierungszeit in Sekunden

	Gruppe 1	Gruppe 4	Gruppe 5	Gruppe 8
Orientierungszeit (O)	2.63	4.15	3.1	5.64
Eingabezeit (E)	2.94	3.19	4.26	4.56
Gesamt (O + E)	5.57	7.34	7.36	10.2

Ein weiteres Maß für die Benutzerfreundlichkeit einer Authentisierungsmethode ist die Erfolgsquote. Diese unterscheidet sich bei den einzelnen Gruppen nur marginal und liegt bei den vier Gruppen bei 82.7%, 82.5%, 80% und 88%. Siehe im Einzelnen Tabelle 14.

Tabelle 14: Erfolgsquote

	Gruppe 1	Gruppe 4	Gruppe 5	Gruppe 8
Korrekt	67	66	52	65
Falsch	14	14	13	9
Durchschnitt	82.72 %	82.5 %	80 %	87.84 %

5.4.2 Interpretation der Ergebnisse

Die Auswertung der demografischen Daten zeigt, dass die Teilnehmer zum Großteil junge Smartphonebenutzer sind. Die Mehrheit nutzt eine PIN als Authentisierungsverfahren.

Verfahren mit zufällig angeordneten Feldern vs. Standard PIN-Verfahren

Im ersten Schritt werden Verfahren mit zufällig angeordneten Feldern gegenüber dem Standard PIN-Verfahren im Hinblick auf Effizienz und Effektivität getestet.

Effizienz:

H1: Das Verfahren mit zufällig angeordneten Bildern ist nicht signifikant weniger effizient als das Standard PIN-Verfahren.

H2: Das Verfahren mit zufällig angeordneten Zahlen ist nicht signifikant weniger effizient als das Standard PIN-Verfahren.

Aufgrund der Ergebnisse müssen beide Hypothesen verworfen werden. Das Standard PIN-Verfahren ist in beiden Fällen signifikant effizienter.

Effektivität:

H3: Das Verfahren mit zufällig angeordneten Bildern ist nicht signifikant weniger effektiv als das Standard PIN-Verfahren.

H4: Das Verfahren mit zufällig angeordneten Zahlen ist nicht signifikant weniger effektiv als das Standard PIN-Verfahren.

Interessant ist auch die Tatsache, dass etwa 40% der Teilnehmer nach eigener Aussage Probleme mit dem Merken einer PIN haben und die Erfolgsraten bei diesem Experiment dennoch bei ca. 80% liegen. Verfahren, bei denen die Felder zufällig angeordnet werden, scheinen also die Erfolgsrate nicht negativ zu beeinflussen.

Grafische Verfahren vs. zahlenbasierte Verfahren

Im zweiten Schritt werden grafische Verfahren gegenüber zahlenbasierten Verfahren getestet. Aus der Literatur geht hervor, dass grafische Verfahren einprägsamer sind als zahlenbasierte Verfahren. Daher wird in diesem Abschnitt getestet, ob sich dies auf Effizienz, Effektivität und Zufriedenheit der Verfahren auswirkt.

Effizienz:

H5: Das Verfahren mit zufällig angeordneten Bildern ist signifikant effizienter als das Verfahren mit zufällig angeordneten Zahlen.

Diese Hypothese konnte aufgrund der erhobenen Daten nicht bestätigt werden. Dieses Ergebnis ist deshalb verwunderlich, weil Zahlen eine natürliche Ordnung haben (1, 2, 3, ...), Bilder dagegen nicht.

Effektivität:

H6: Das Verfahren mit zufällig angeordneten Bildern ist signifikant effektiver als das Verfahren mit zufällig angeordneten Zahlen.

Diese Hypothese konnte aufgrund der erhobenen Daten ebenfalls nicht bestätigt werden. Zufällig angeordnete Bilder zeigten zwar eine höhere Effektivität als entsprechend angeordnete Zahlen, der Unterschied war allerdings nicht signifikant.

Die meisten Benutzer wurden nach eigener Aussage nicht durch die zufällige Anordnung beeinflusst. Vor allem die Gruppe mit den zufällig angeordneten Zahlen vermisste aber den Lerneffekt des Standard PIN-Verfahrens. Mit der gleichen Begründung erklärten 13% der Teilnehmer aus Gruppe 4, sich die Nutzung eines solchen Systems nicht vorstellen zu können. Hinzu kommt, dass Gruppe 8 mit den zufällig angeordneten Bildern die höchste Erfolgsrate hat, obwohl die Teilnehmer den Lerneffekt über das Muster auf dem Eingabefeld als häufigste Methode genannt haben, was es bei zufällig angeordneten Bildern gar nicht gibt.

Zufriedenheit:

H7: Die Zufriedenheit der Benutzer bei dem Verfahren mit zufällig angeordneten Bildern ist signifikant größer als bei dem Verfahren mit zufällig angeordneten Zahlen.

Diese Hypothese konnte aufgrund der erhobenen Daten nicht bestätigt werden, da sich die Zufriedenheit zwischen den beiden Gruppen nicht signifikant unterscheidet. Aufgrund der deutlich abweichenden Orientierungszeiten und der höheren Eingabezeiten bei Verfahren mit zufällig angeordneten Feldern wird davon ausgegangen, dass ein Benutzer ein solches Verfahren künftig nicht verwenden würde. Nachdem jedoch den Teilnehmern der Zugewinn an Sicherheit verdeutlicht wurde, erklärten sich bis zu 59% bereit, ein solches Verfahren zu benutzen.

Allerdings muss dabei beachtet werden, dass ein solches Ergebnis von mehreren sachfremden Faktoren beeinflusst sein kann. So ist ein Teilnehmer einer Studie beispielsweise häufig geneigt, nett zu sein. Daher ist es wahrscheinlich, dass der Prozentsatz tatsächlich geringer ist. Andererseits muss ein solches Verfahren langfristig getestet werden, um belastbare Ergebnisse zu dessen Akzeptanz zu erhalten.

5.5 Empfehlung für die Verwendung der vorgeschlagenen Authentisierungsverfahren

Die Analyse der beiden Authentisierungsverfahren hat ergeben, dass sie zwar nicht weniger effektiv als herkömmliche Verfahren sind, sich aber deutlich in der Effizienz unterscheiden. Für den durchschnittlichen Benutzer ist ein solches Verfahren allerdings für den alltäglichen Gebrauch nicht geeignet, da der Zugewinn an Sicherheit den zusätzlichen Aufwand nicht aufwiegt. Anwendung findet eine solche Lösung also eher im betrieblichen Kontext, bei welchem typischerweise auf dem Smartphone sehr sensible Daten gespeichert sind. Insofern stehen die Authentisierungsverfahren hier in einem ganz anderen Kosten-/Nutzenverhältnis.

Abschließend noch eine Empfehlung für einen Benutzer, dessen Smartphone keine hoch sensiblen Daten enthält. Die Autoren schlagen für diesen Fall ein Verfahren vor, bei dem der Benutzer die Möglichkeit hat, zwischen dem Standard PIN-Verfahren und dem shoulder-surfing resistenten Verfahren auszuwählen. Fühlt er sich etwa beobachtet oder ist sich nicht sicher, ob er den Code ungesehen eingeben kann, so wischt er beispielsweise nach rechts und nutzt das Verfahren mit den zufällig angeordneten Feldern. Wischt er dagegen nach links, so erscheint das herkömmliche Eingabefeld. Der Benutzer kann sich daher wie gewohnt authentisieren und nutzt weiterhin den bekannten Lerneffekt über das Muster. Der Benutzer muss sich also entscheiden, ob er sich lieber schnell oder sicher authentisiert.

6 Related Work

Es gibt in der Literatur verschiedene Alternative zu dem klassischen PIN-Verfahren, die behaupten auch ohne Verwendung einer Blickschutzfolie shoulder-surfing resistent zu sein. Im Folgenden werden einige davon näher erläutert. Die Verfahren werden danach aufgeteilt, ob für die Funktionalität biometrische Daten erforderlich sind oder nicht.

6.1 Verfahren ohne Verwendung von Biometrie

In diesem Kapitel werden Verfahren erläutert, die für ihre Funktion keine biometrischen Daten benötigen.

PIN 3D

Lee und Nam [LN13] haben ein Verfahren entwickelt, welches den 3D-Effekt ausnutzt. Sie verwenden ein Smartphone mit einem 3D-Display mit dem Autostereoskopie-Verfahren. Dabei wird kein zusätzliches Hilfsmittel, zum Beispiel Brille, vor den Augen benötigt. Auf einem Feld mit 10x10 Zeichen werden die Buchstaben A bis K jeweils zehn Mal dargestellt, links daneben in einer Spalte die Ziffern von 1 bis 0, siehe Abbildung 20. Sobald der Benutzer auf den rechts angebrachten Button klickt, wird einer der Buchstaben mit dem 3D-Effekt hervorgehoben. In der (vertikalen) Spalte mit diesem Buchstaben sucht der Benutzer die Zeilen, die der Stelle der PIN entsprechen und merkt sich diese. Diese so ermittelten Buchstaben werden dann im nächsten Schritt als PIN eingegeben. Die durchschnittliche Eingabezeit liegt laut ihrer Studie bei 8.4 Sekunden.

Analyse: Dieses Authentisierungsverfahren basiert auf Wissen und verhält sich ohne die Verwendung einer Blickschutzfolie, wie die vorgeschlagene Kombination aus Kapitel 3.3. Wenn sich der Angreifer neben oder gegenüber des Benutzers befindet, kann er auf dem Display nichts besonderes erkennen. Befindet er sich jedoch hinter dem Benutzer und hat damit einen ähnlichen Blickwinkel wie dieser, ist zu vermuten, dass der Angreifer den 3D-Effekt auch wahrnehmen kann. Außerdem ist bei diesem Verfahren das Kriterium der Marktverfügbarkeit verletzt. Während im Jahr 2011 ein paar wenige Modelle vorgestellt wurde, ließ dieser Trend schon im Jahr 2012 nach. Schließlich sind im Jahr 2013 auch diese Modelle vom Markt verschwunden.

Abbildung 20: PIN entry with 3D-Display [LN13]

XSide

Das Verfahren von de Luca, Harbach et al. [De +14] setzt voraus, dass auch die Rückseite des Smartphones ein Display besitzt, welches halb so groß wie das der Vorderseite ist. Beide Seiten des Smartphones können für die Authentisierung verwendet werden, siehe Abbildung 21. Der Benutzer legt von vornherein verschiedene Formen als Passwort fest. Er hat nun die Möglichkeit, entweder horizontal oder vertikal über einen der beiden Bildschirme zu streichen und aus der Kombination dieser Bewegungen die gewünschte Form zu erzeugen. Zwei Mal in die gleiche Richtung zu streichen, wird vom System ignoriert. Sobald der Benutzer den Touchscreen nicht mehr mit seinem Finger berührt, gilt die Form als beendet. Mehrere dieser Formen werden von vornherein als Passwort festgelegt. Wenn der Benutzer sich authentisieren möchte, kann er situationsabhängig die Vorder- oder Rückseite des Smartphones verwenden, um sich gegen Shoulder-Surfing zu schützen.

Analyse: Dieses Verfahren basiert auf Wissen und würde bei Verwendung einer Folie keinen Mehrwert bieten. Alleine der Benutzer entscheidet welches der beiden Displays er für die Authentisierung benutzen möchte und sich so vor Shoulder-Surfing schützen. Die Gefahr besteht darin, dass der Angreifer anhand der Fingerbewegung die Authentisierung erkennen kann, da der Displayinhalt nicht wichtig ist. Da es nur sehr wenige Smartphones mit zwei Displays gibt und gar keine bei denen die Displays so wie in der Veröffentlichung angebracht sind, ist das Kriterium der Marktverfügbarkeit verletzt.

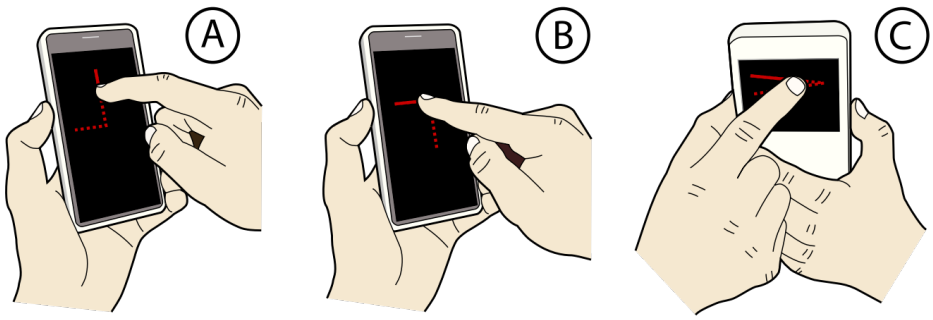


Abbildung 21: XSide [De +14]

Tetrad

Renaud und Maguire [RM09] haben ein Verfahren entwickelt, bei dem ein Benutzer aus einer Menge von Bildern einige auswählt, die „sein“ Geheimnis (*secret*) darstellen. Anschließend bekommt er ein Raster angezeigt, auf dem alle Bilder, also auch die von ihm ausgewählten, angezeigt werden, siehe Abbildung 22. Seine Aufgabe besteht nun darin, durch Verschieben von Zeilen oder Spalten des Rasters seine ausgewählten Bilder entweder horizontal oder vertikal in einer Linie anzuordnen. Dies geschieht mit Hilfe einer so genannten Remote Fernbedienung von Apple.

Analyse: Das Verfahren basiert auf Wissen. Die Verwendung einer Blickschutzfolie würde nur einen geringen Vorteil bieten. Es ist davon auszugehen, dass das Kriterium der Effizienz verletzt ist, da jedes Bild einzeln angeordnet werden muss. Außerdem ist fraglich, ob bei Verwendung auf einem Smartphone, die Anzahl der möglichen Bildern - wegen der geringen Größe des Displays - ausreicht, um shoulder-surfing resistent zu sein.

Abbildung 22: Tetrad [RM09]

6.2 Biometrische Verfahren

Bei der Authentisierung durch biometrische Merkmale authentisiert sich der Benutzer durch eigene Merkmale, zum Beispiel den Fingerabdruck. Während diese Verfahren vollkommen sicher gegenüber Shoulder-Surfing sind, gibt es, wie in Kapitel 1.1 genannt, einige andere Probleme, wie zum Beispiel false-positive Erkennung und Probleme mit dem Datenschutz.

Fingerabdruck- und Gesichtserkennung

Biometrische Verfahren wie beispielsweise die Fingerabdruckerkennung, siehe Abbildung 23 oder die Gesichtserkennung (bei Android) sind ebenfalls ohne Blickschutzfolie shoulder-surfing resistent.

Analyse: Die Fingerabdruckerkennung ist zur Zeit nur bei Geräten im hohen Preissegment verfügbar. Außerdem haben beide genannten Verfahren das Problem, dass sie durch genommene Fingerabdrücke oder Fotos überlistet werden können.

Abbildung 23: IPhone Fingerabdruckerkennung [Quelle: www.apple.de]

Authentisierung mit Hilfe des Blicks

Kumar, Garfinkel et al. [Kum+07] haben ein Verfahren entwickelt, bei dem der Benutzer das Passwort mit seinen Augen eingibt. Auf dem Bildschirm sieht er beispielsweise eine QWERTY-Tastatur, siehe Abbildung 24. Um das Passwort einzugeben, muss er nacheinander die Buchstaben fokussieren, aus denen sein Passwort besteht. Groß- und Kleinschreibung wird durch Fokussieren der Umschalttaste erreicht. Um das Verfahren shoulder-surfing resistent zu gestalten, soll der Benutzer nach Angabe der Autoren kein Feedback darüber bekommen, welchen Button er gerade „gedrückt“ hat.

Analyse: Bei diesem Verfahren ist insbesondere die Eignung für ein Smartphonedisplay verletzt. Eine Tastatur müsste auf dem Display so groß dargestellt werden, dass man die einzelnen Buchstaben mühelos fokussieren kann und die Kamera die Unterschiede zwischen den einzelnen Buchstaben auch erkennen kann.

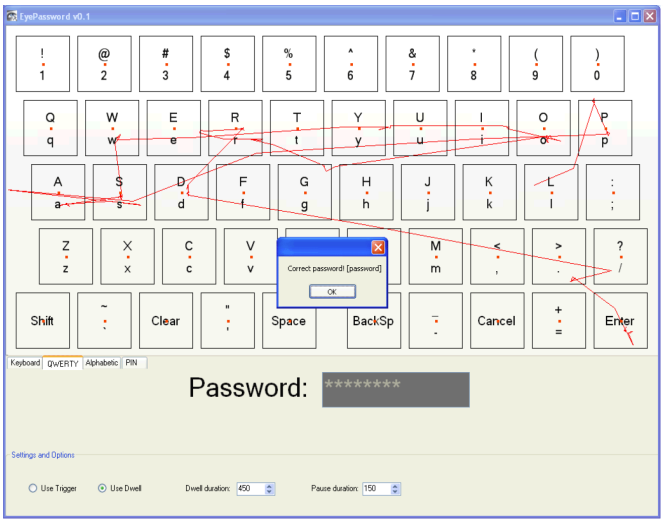
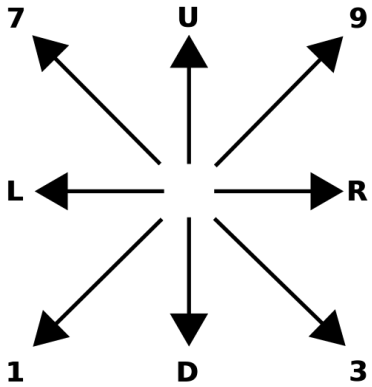


Abbildung 24: Authentisierung mit Hilfe des Blicks [Kum+07]

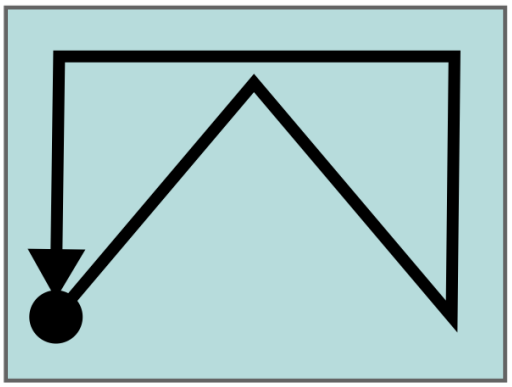
EyePassShapes

Bei diesem Verfahren, das von De Luca, Denzel und Hussmann [DDH09] entwickelt worden ist, authentisiert sich ein Benutzer anhand seiner Augenbewegungen. Der Benutzer sieht zum Beispiel ein Feld, auf dem Punkte wie bei einem Gitter angeordnet sind. Mit der Bewegung seiner Augen kann er dadurch ein Muster eingeben, dass er von einem Punkt zum nächsten schaut. Es gibt acht verschiedene Richtungen, die anhand von Zahlen und Buchstaben kodiert sind: links (L), rechts (R), oben (U), unten (D), unten links (1), unten rechts (3), oben links (7) und oben rechts (9), siehe Abbildung 25a. Als erstes legt der Benutzer die Form fest, mit der er sich authentisieren möchte, indem er diese mit seinen Augen erstellt, siehe Abbildung 25b. Dabei drückt er auf einen Button, und so lange er diesen gedrückt hält, wird seine Augenbewegung gefilmt. Sobald er den Button loslässt, wird die Augenbewegung fixiert und analysiert und mit der gespeicherten Form verglichen. Stimmen beide Formen überein, ist die Authentisierung erfolgreich.

Analyse: Bei diesem Verfahren könnte die Eignung für ein Smartphonedisplay verletzt sein, da die Kamera eventuell nicht zwischen den einzelnen Teilen der Form unterscheiden kann. Außerdem besteht die Möglichkeit die Authentisierung anhand der Augenbewegung herauszufinden.



(a) Richtungsmöglichkeiten



(b) Beispiel für Form

Abbildung 25: EyePassShapes [DDH09]

Authentisierung durch Analyse des Eingabeverhaltens

Bei dem von Gascon, Uellenbeck et al. [Gas+14] entwickelten Verfahren authentisiert sich der Benutzer anhand des Eingabeverhaltens seiner PIN (*typing motion behavior*). Zu Beginn muss er einen kurzen Text zehn Mal eingeben, damit genügend Informationen über die Eingabe gesammelt werden können. Bei der Eingabe des Textes werden die Daten der verschiedenen Sensoren des Smartphones (Beschleunigungsmesser, Gyroskop und Lagesensor) gesammelt und daraus ein Profil erstellt. Wenn der Benutzer sich authentisieren möchte, wird überprüft, ob die Art der Eingabe mit dem tatsächlichen Eingabeprofil übereinstimmt. Während diese Methode bei einigen Benutzern sehr gut funktioniert, können andere Benutzer deshalb kaum auseinandergehalten werden, weil sich die Eingabeverhalten zu sehr ähneln.

Analyse: Dieses Verfahren funktioniert, laut Autoren der Arbeit, gut bei vielen Personen, andererseits gab es auch einige Fälle in Benutzer kaum von ihrem Eingabeverhalten unterschieden werden konnten. Dieses Problem mit false-positives ist insbesondere bei der Unterscheidung zwischen Benutzer und Angreifer ein Problem.

Authentisierung mit Hilfe von Gangerkennung

Das Verfahren von Derawi, Nickel et al. [Der+10] zeichnet sich dadurch aus, dass sich der Benutzer anhand von Gangerkennung authentisiert. Dabei gibt es drei mögliche Ansätze: Maschinelles Sehen [Nix+96], Fußbodensensoren [JE07] und Gangarterkennung mit Hilfe von Wearables. Da Gegenstand der Thesis die Authentisierung mit Hilfe des eigenen Smartphones ist, ist hier nur der dritte Ansatz relevant. Bei einem Test wurde ein Smartphone an eine Tasche am Gürtel der Versuchsperson horizontal befestigt, siehe Abbildung 26a, und zwar mit dem oberen Teil des Smartphones in Laufrichtung. Anschließend mussten die Versuchspersonen einen Gang entlang gehen, und zwar möglichst so, wie sie auch im Alltag gehen würden. Abbildung 26b zeigt die drei Achsen, mit welchen die Beschleunigung gemessen wird. Anhand der Daten wurde für jede Versuchsperson ein Profil erstellt, mit dem sie später wiedererkannt werden soll. Die durchschnittliche Fehlerrate lag bei 20.1%. Bei einer ähnlichen Analyse von Holien [Hol08] betrug die Fehlerquote 12,9%. Im zuletzt genannten Beispiel wurde jedoch ein (externer) Beschleunigungsmesser verwendet und nicht der eines Smartphones. Dieses Verfahren kann nur angewandt werden, wenn sich der Benutzer bewegt. Alternativ hat er die Möglichkeit, sich mit seiner PIN zu authentisieren.

(a) Ausrichtung des Smartphones

(b) Achsen

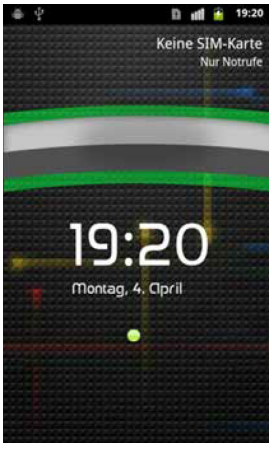
Abbildung 26: Gangerkennung [Der+10]

Analyse: Dieses Verfahren schützt einerseits gut gegen Shoulder-Surfing, hat aber mit etwa 20% eine viel zu hohe Fehlerrate.

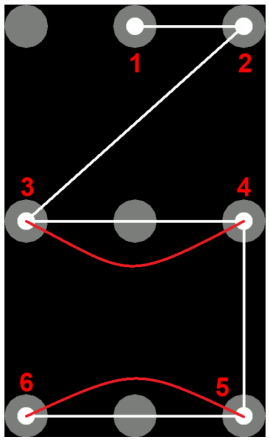
Touch me once

De Luca, Hang et al. [De +12] haben einige Authentisierungsverfahren auf Basis von biometrischen Daten entwickelt. Der Benutzer verwendet bekannte Verfahren, wie zum Beispiel das Wischen bei Android, siehe Abbildung 27a. Mittels eines Algorithmus (dynamic time warping) werden verschiedene Datenpunkte verglichen und dadurch bestimmt, ob es sich um denselben Benutzer handelt. Dieses Verfahren wurde auf vier verschiedene Arten variiert, um an mehr biometrische Daten des Benutzers zu gelangen. Das diagonale Wischen beispielsweise liefert mehr Daten als das horizontale. Im Anschluss daran wurde diese Technik auf das Muster von Android übertragen. Es war den Autoren möglich, eine Genauigkeit von bis zu 96% zu erreichen. Die false-positive Rate lag dabei jedoch bei 21%. Bei diesem Verfahren ist allerdings das Kriterium des gleichen Sicherheitslevels verletzt, weil es nicht mit der Eingabe einer PIN (ausschließliche Verwendung von vier Zahlen) vergleichbar ist (Kapitel 2.1).

Analyse: Ähnlich wie bei den vorhergehenden Verfahren hat auch dieses Verfahren ein großes Problem mit der false-positive Erkennung.



(a) Aufbau



(b) Blickwinkel

Abbildung 27: TouchMeOnce [De +12]

7 Fazit und Ausblick

Shoulder-Surfing ist in der heutigen Zeit ein ernstzunehmendes Problem. Um ihm zu begegnen, haben die Autoren eine Lösung entwickelt, die auf der Kombination einer Blickschutzfolie mit einem positionsunabhängigen Authentisierungsverfahren basiert und mit anderen Verfahren verglichen, die in der Literatur vorgeschlagen werden. Dabei hat sich gezeigt, dass meisten die zugrunde gelegten Kriterien, wie etwa Effizienz oder Eignung für Smartphonedisplay, nicht erfüllen.

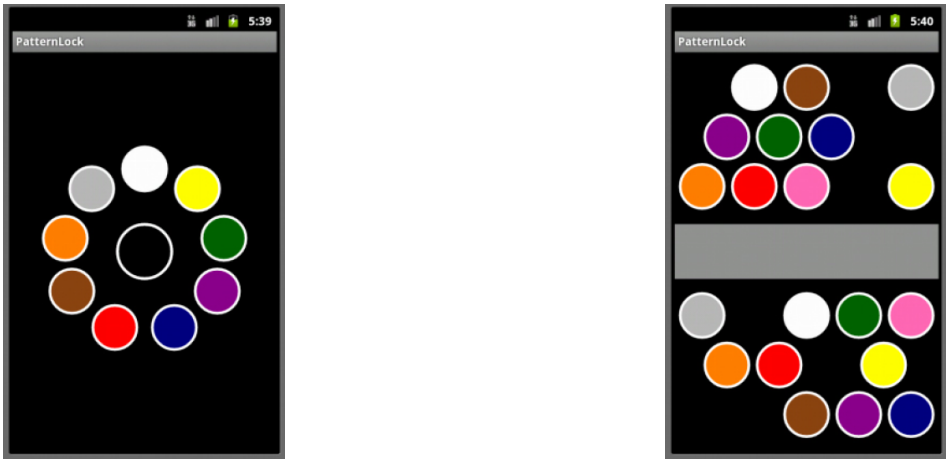
Bei der Analyse von verschiedenen Blickschutzfolien hat sich ergeben, dass keine der beiden Folien in jeder Situation ausreichend vor Shoulder-Surfing schützt. Aus diesem Grund wurden einige Empfehlungen für den potentiellen Benutzer gegeben, wie er die Gefahr des Shoulder-Surfings in bestimmten Situationen verringern kann.

Bei der Analyse der Authentisierungsverfahren hat sich gezeigt, dass die vorgeschlagene Lösung für den privaten Benutzer im alltäglichen Gebrauch zu aufwändig wäre. Im Hinblick auf das Kriterium der Effizienz erzielten die Verfahren mit zufällig angeordneten Eingabefeldern signifikant schlechtere Ergebnisse, wohingegen bei der Effektivität keine signifikanten Unterschiede zu erkennen waren. Daher wurde eine hybride Lösung empfohlen. Hierbei authentisiert sich der Benutzer je nach Situation entweder wie gewohnt über ein Standard- oder - falls er beobachtet wird - über ein zufällig angeordnetes Eingabefeld. Dadurch können die Einbußen bezüglich Effizienz minimiert und dennoch eine sichere Authentisierung erreicht werden.

Die Evaluation eines solchen Verfahrens könnte Gegenstand zukünftiger Forschung sein. Dabei sollte bedacht werden, dass die Frage, ob eine Situation sicher ist oder nicht, der subjektiven Entscheidung des Benutzers unterliegt. Aus diesem Grund bietet sich eine Laborstudie an. Dabei kann überprüft werden, ob die Entscheidung des Benutzers der jeweilige Situation angemessen ist oder nicht. Bei einer solchen Studie ist außerdem darauf zu achten, dass er den Code in für Smartphones typischeren Zeitabständen eingibt. Zudem sind realistischere Zeitmessungen möglich, da der Benutzer statt einer Computermaus die Smartphone-Tastatur verwendet. Ein weiteres Problem könnte sein, dass Benutzer, die ihren Code sehr häufig auf dem Standard-Eingabefeld eingeben und sich nur das Muster der Authentisierung merken, sich nicht mehr auf dem anderen Eingabefeld authentisieren können.

Nach Beginn der Online-Studie haben die Autoren bei der Literaturrecherche eine weitere Veröffentlichung gefunden, die mit Blickschutzfolie vor Shoulder-Surfing schützen könnte. Es handelt sich um ein Verfahren, das von Zezschwitz, Koslow et al. [Zez+13] gegen so genannte „smudge attacks“ entwickelt wurde. Eines davon nennt sich „Marbles“, siehe Abbildung 28a. Hier sind neun bunte Kugeln (*marbles*) um einen mittleren Kreis angeordnet. Der Benutzer zieht diese Kugeln in einer bestimmten Reihenfolge in dass Zentrum, um sich zu authentisieren. Jede farbige Kugel kann beliebig oft verwendet werden. Bei jeder Authentisierung ändert sich die Position der einzelnen Kugeln.

Ein anderes Verfahren nennt sich „Marble Gap“, siehe Abbildung 28b. Ähnlich wie Marbles müssen die bunten Kugeln ins Zentrum gezogen werden. Allerdings ist das Feld nun durch eine horizontale Spalte in zwei Bereiche aufgeteilt. In beiden Bereichen befindet sich die gleichen farbigen Kugeln. Eine Kugel mit einer bestimmten Farbe im oberen Bereich unterscheidet sich nicht von der Kugel der selben Farbe im unteren Bereich. Zum Authentisieren werden die Kugeln in die Spalte gezogen. Jede Kugel kann, im Unterschied zu dem anderen Verfahren, nur einmal verwendet werden.



(a) Marbles **(b)** Marble Gap

Abbildung 28: Marbles und Marble Gap [Zez+13]

Analyse: Beide Verfahren sind positionsunabhängig. Mit 7 beziehungsweise 7.5 Sekunden für eine Authentisierung ist das Kriterium der Effizienz ebenfalls erfüllt. Das Sicherheitslevel kann durch eine Modifizierung der Verfahren an das einer PIN angeglichen werden, bei Marbles beispielsweise durch Hinzufügen einer weiteren Kugel. Außerdem ist es für den Einsatz auf einem Smartphone konzipiert, wodurch es auch diese Kriterium erfüllt. Daher bietet es sich durchaus in Kombination mit einer Blickschutzfolie als Lösung gegen Shoulder-Surfing an.

Anhang

A Quellcode für das automatische Versenden der Mails

Listing 1: Quellcode Mailversand

```
1  # coding: utf8
2
3  import urllib.request
4  import re
5  import smtplib
6  import codecs
7  import sys
8  from email.mime.text import MIMEText
9  from email.mime.multipart import MIMEMultipart
10 import datetime
11
12 mail_server = 'MAIL_SERVER'
13 mail_accountName = 'ACCOUNT_NAME'
14 mail_password = 'PASSWORT'
15 mail_sender = "SENDER_ADRESSE"
16
17 counter = 1
18
19 email_contact = "Bitte antworten Sie nicht auf diese E-Mail. Die Adresse dient
       nur dem Versenden der E-Mails. Falls Sie Fragen haben sollten, wenden Sie
       sich bitte an uns - Kristoffer Braun (kristoffer.braun@cased.de) oder
       Philipp Rack (philipp.rack@cased.de). \nNachdem Sie auf den Link geklickt
       haben, Ihre PIN jedoch nicht eingegeben haben, kommt es nach etwa zehn
       Stunden zu einem timeout. Sollte es daraufhin nicht mehr möglich sein die
       PIN einzugeben, schreiben Sie uns bitte eine Mail, um einen neuen Link zu
       erhalten."
20
21 websiteContent = str(urllib.request.urlopen("http://khios.dcs.gla.ac.uk/pins/
       PinService.cfm?password=XXXXXXX").read())
22
23 cleanContent = websiteContent.replace("\\n", "")
24 cleanContent = cleanContent.replace("\\r", "")
25 cleanContent = cleanContent.replace("\\t", "")
26
27 splitToList = cleanContent.split("<br>")
28
29 if len(splitToList) == 1:
30     sys.exit()
31
```

```
32 for item in range(len(splitToList) - 1):
33     mail_receiver = re.search("Email:(.*) URL:", splitToList[item]).group(1)
34     link = re.search("URL:(.*) Session:", splitToList[item]).group(1)
35     sessionNumber = re.search("Session:([\d])", splitToList[item]).group(1)
36     if int(sessionNumber) == 1:
37         emailText = "Sehr geehrte Teilnehmerin, sehr geehrter Teilnehmer,\n\
               nvielen Dank, dass Sie an unserem Experiment teilnehmen. Sie haben
               im Rahmen der Registrierung einen Code erhalten. In dieser Phase
               geht es darum, diesen erneut einzugeben und danach ein paar Fragen
               zu beantworten.\n\nEs folgen noch drei weitere E-Mails. In den
               weiteren Phasen besteht Ihre Aufgabe nur noch darin, den Code
               richtig einzugeben.\n\nBitte beachten Sie, dass Sie sobald Sie auf
               den Link geklickt haben, die PIN auch direkt eingeben müssen,
               ansonsten kann diese Runde ungültig werden.\n\nLink: " + link + "\n\
               nWir möchten uns nochmals für Ihre Teilnahme und damit für die
               Unterstützung bei unserer Bachelorarbeit bedanken.\n\nMit
               freundlichen Grüßen,\nKristoffer Braun und Philipp Rack\n\n" +
               email_contact
38     elif int(sessionNumber) == 2:
39         emailText = "Sehr geehrte Teilnehmerin, sehr geehrter Teilnehmer,\n\
               ndas Experiment ist in die zweite Phase gestartet. Wir freuen uns,
               dass Sie weiterhin dabei sind. Um die Phase abzuschließen, klicken
               Sie bitte auf den Link und geben Sie Ihren Code ein.\n\nBitte
               beachten Sie, dass Sie sobald Sie auf den Link geklickt haben, die
               PIN auch direkt eingeben müssen, ansonsten kann diese Runde ungültig
                werden.\n\nLink: " + link + "\n\nEs folgen noch zwei weitere E-
               Mails. Vielen Dank, dass Sie uns weiterhin unterstützen.\n\nMit
               freundlichen Grüßen,\nKristoffer Braun und Philipp Rack\n\n" +
               email_contact
40     elif int(sessionNumber) == 3:
41         emailText = "Sehr geehrte Teilnehmerin, sehr geehrter Teilnehmer,\n\
               ndas Experiment ist in die dritte Phase gestartet. Wir freuen uns,
               dass Sie weiterhin dabei sind. Um die Phase abzuschließen, klicken
               Sie bitte auf den Link und geben Sie Ihren Code ein.\n\nBitte
               beachten Sie, dass Sie sobald Sie auf den Link geklickt haben, die
               PIN auch direkt eingeben müssen, ansonsten kann diese Runde ungültig
                werden.\n\nLink: " + link + "\n\nEs folgt noch eine weitere E-Mail
               in etwa 30 Tagen. Vielen Dank, dass Sie uns weiterhin unterstützen.\
               n\nMit freundlichen Grüßen,\nKristoffer Braun und Philipp Rack\n\n"
                + email_contact
42     elif int(sessionNumber) == 4:
43         emailText = "Sehr geehrte Teilnehmerin, sehr geehrter Teilnehmer,\n\
               ndas Experiment ist in die vierte und letzte Phase gestartet. Wir
               freuen uns, dass Sie bis zum Schluss dabei geblieben sind. Um die
               Phase abzuschließen, klicken Sie bitte auf den Link und geben Sie
               Ihren Code ein. Danach erhalten Sie drei weitere Fragen (u.a. ob Sie
```

```
                an der Verlosung des Amazon Gutscheins teilnehmen möchten) und das
                Experiment ist für Sie abgeschlossen.\n\nBitte beachten Sie, dass
                Sie sobald Sie auf den Link geklickt haben, die PIN auch direkt
                eingeben müssen, ansonsten kann diese Runde ungültig werden.\n\nLink
                : " + link + "\n\nVielen herzlichen Dank!\n\nMit freundlichen Grüß
                en,\nKristoffer Braun und Philipp Rack\n\n" + email_contact
44
45      msg = MIMEMultipart('alternative')
46      msg['Subject'] = "Rückmeldung PINPad Experiment"
47      msg['From'] = mail_sender
48      msg['To'] = mail_receiver
49      message_body_plain = MIMEText(emailText, 'plain', _charset="UTF-8")  #
            Plain text mail
50      msg.attach(message_body_plain)
51
52      smtp = smtplib.SMTP(mail_server)
53      smtp.starttls()
54      smtp.ehlo()
55      smtp.login(mail_accountName, mail_password)
56      smtp.sendmail(mail_sender, mail_receiver, msg.as_string())
57      smtp.quit()
58      with codecs.open(str(datetime.date.today()) + ".xml", "a", "utf-8") as file
            :
59          if counter == len(splitToList) - 1:
60              file.write(str(counter) + ". Receiver: " + mail_receiver + " - Link
                    : " + link + " - Session: " + sessionNumber + " - done")
61          else:
62              file.write(str(counter) + ". Receiver: " + mail_receiver + " - Link
                    : " + link + " - Session: " + sessionNumber + " - done\n\n")
63          counter += 1
```

B Werbung

Abbildung 29: Aushang

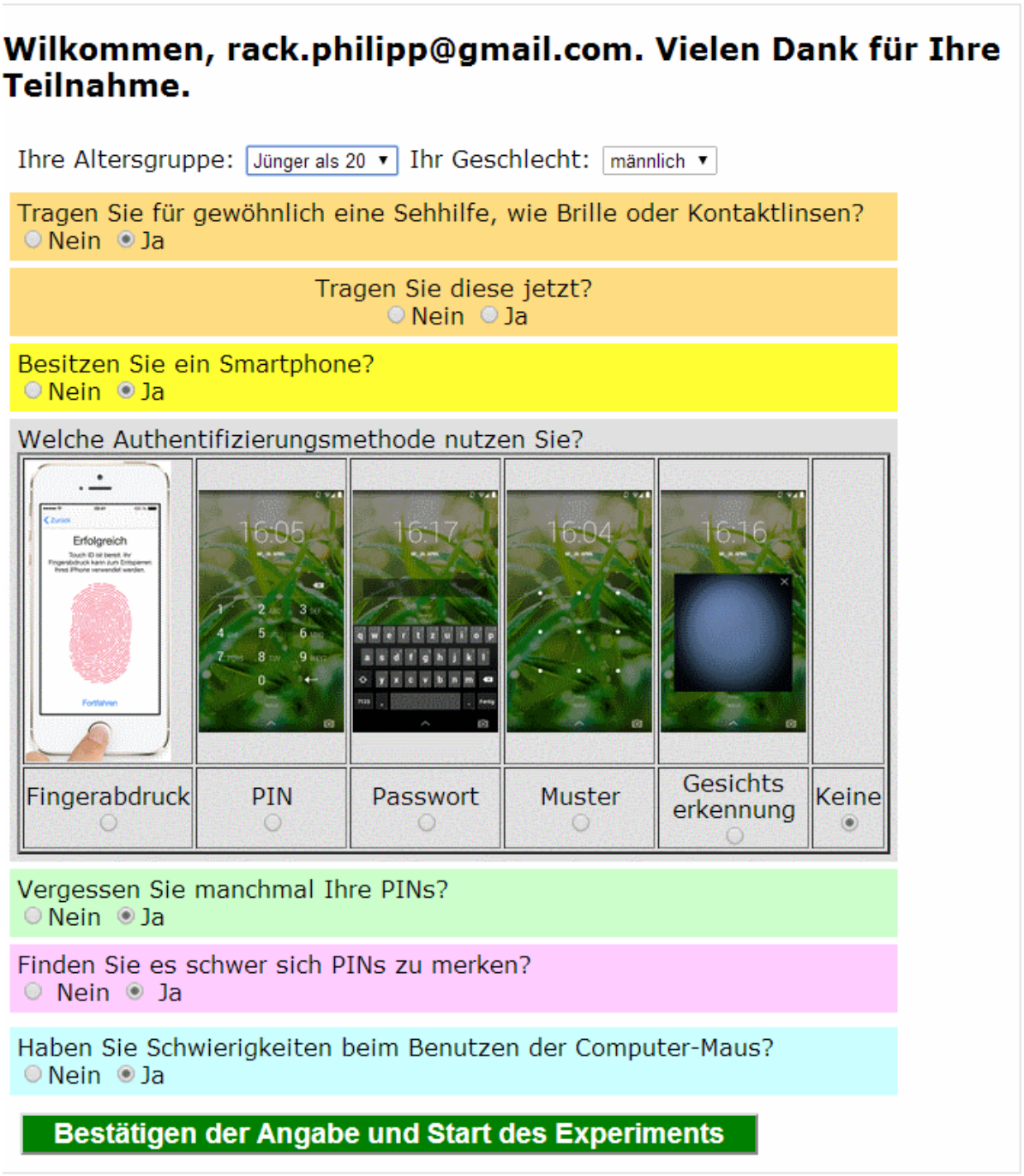


Abbildung 30: Fragebogen zu Beginn des Expriments

Zunächst interessiert uns, ob Sie Ihren geheimen Code (oder Hinweise darauf) aufgeschrieben haben, um sich daran zu erinnern.
Für uns ist es wichtig, dass Sie eine ehrliche Antwort geben. Wenn Sie das Gefühl hatten, dass Sie sich den Code sonst nicht merken können, dann ist das für uns auch eine wichtige Information.

Haben Sie Ihren geheimen Code (oder Hinweise darauf) aufgeschrieben? ○ Ja ○ Nein

Fiel es Ihnen während der folgenden Situationen schwer, sich an den Code zu erinnern:

1. Als Sie sich angemeldet haben und sich den Code versucht haben zu merken?

○ Nein ○ Ja

2. Als Sie Ihren Code heute eingegeben haben?

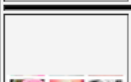
○ Nein ○ Ja

Falls Sie sich an den Code erinnern konnten, waren Sie überrascht, dass Sie sich den Code merken konnten?

Nicht überrascht	○ 1	○ 2	○ 3	○ 4	○ 5	Sehr überrascht

Wie versuchen Sie, sich die PIN für Ihre Bankkarten zu merken?

Wie haben Sie sich den Code für dieses Experiment gemerkt?



Haben Sie das Gefühl, Sie können sich generell Bilder besser merken als Zahlen?
○ Nein ○ Ja ○ Weiß Nicht

Bitte begründen Sie Ihre Antwort kurz.

Abbildung 31: Fragebogen nach der ersten Rückkehr (Teil 1)

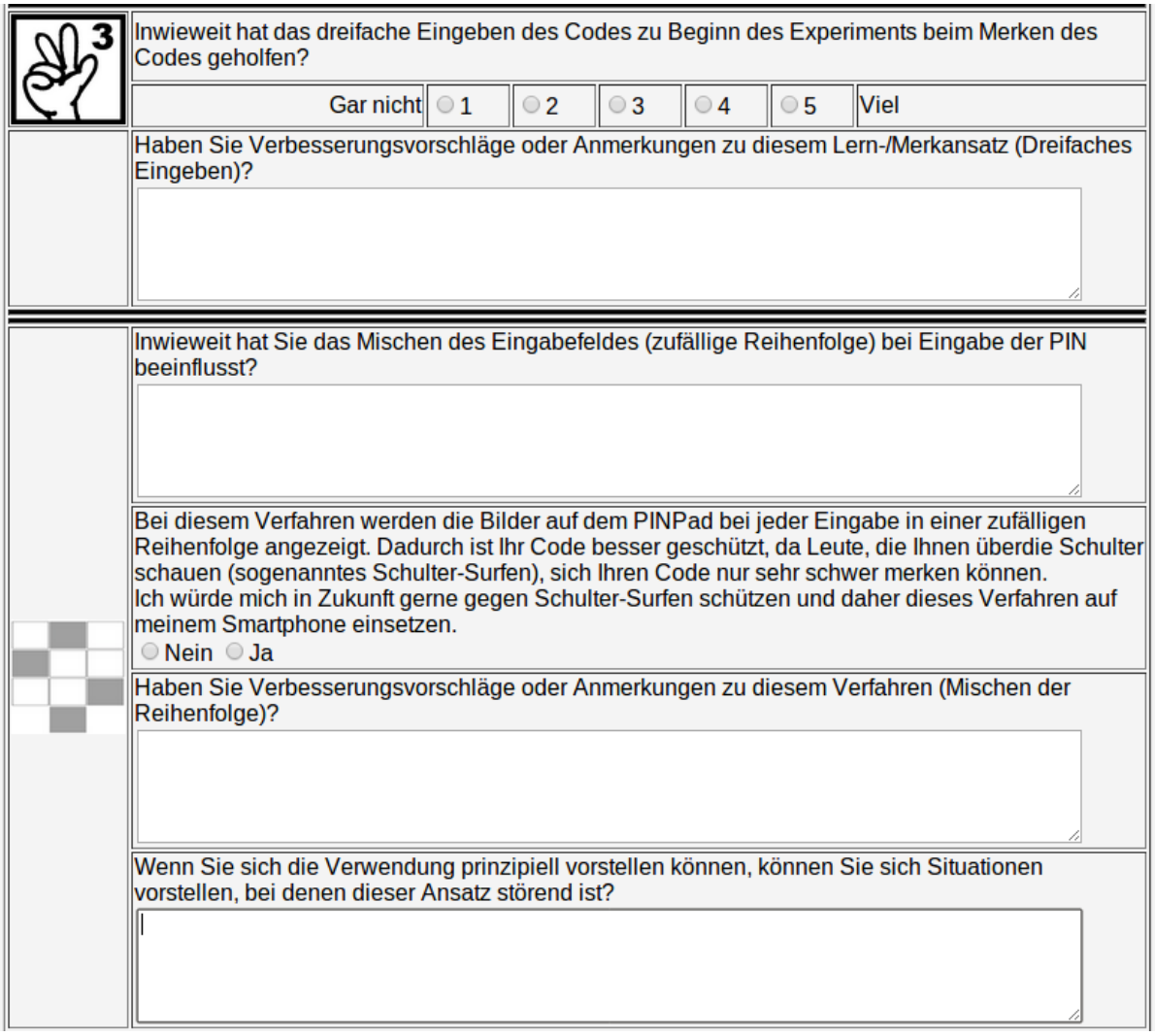


Abbildung 32: Fragebogen nach der ersten Rückkehr (Teil 2)

Abbildungsverzeichnis

Tabellenverzeichnis

Literatur

[Aho13] Tomi T. Ahonen. *The Annual Mobile Industry Numbers and Stats Blog - Yep, this year we will hit the Mobile Moment.*. März 2013. URL: http://communities-dominate.blogs.com/brands/2013/03/the-annual-mobile-industry-numbers-and-stats-blog-yep-this-year-we-will-hit-the-mobile-moment.html (besucht am 10. 07. 2014).

[AUH14] Irfan Altiok, Sebastian Uellenbeck und Thorsten Holz. „GraphNeighbors: Hampering Shoulder-Surfing Attacks on Smartphones." In: *Sicherheit*. 2014, S. 25–35.

[Bau98] Andrej Bauer. *Gallery of random art*. 1998. URL: http://www.random-art.org/ (besucht am 15. 07. 2014).

[BCV12] Robert Biddle, Sonia Chiasson und P.C. Van Oorschot. „Graphical Passwords: Learning from the First Twelve Years". In: *ACM Comput. Surv.* 44.4 (Sep. 2012), 19:1–19:41.

[BS00] Sacha Brostoff und Angela M. Sasse. „Are Passfaces More Usable Than Passwords? A Field Trial Investigation". English. In: *People and Computers XIV — Usability or Else!* Hrsg. von Sharon McDonald, Yvonne Waern und Gilbert Cockton. Springer London, 2000, S. 405–424.

[COP08] Rafi MMI Chowdhury, G Douglas Olsen und John W Pracejus. „Affective responses to images in print advertising: Affect integration in a simultaneous presentation context". In: *Journal of Advertising* 37.3 (2008), S. 7–18.

[Cis14] Inc. Cisco Systems. *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018*. Feb. 2014. URL: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html (besucht am 02. 07. 2014).

[Clu13] Chaos Computer Club. *Chaos Computer Club breaks Apple TouchID*. 2013. URL: http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid (besucht am 07. 07. 2014).

[Cor04] Real User Corporation. *The Science Behind Passfaces*. Juni 2004.

[DDH09] Alexander De Luca, Martin Denzel und Heinrich Hussmann. „Look into My Eyes!: Can You Guess My Password?" In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. SOUPS '09. Mountain View, California: ACM, 2009, 7:1–7:12.

[DHH10] Alexander De Luca, Katja Hertzschuch und Heinrich Hussmann. „ColorPIN: Securing PIN Entry Through Indirect Input". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '10. Atlanta, Georgia, USA: ACM, 2010, S. 1103–1106.

[De +14] Alexander De Luca u. a. „Now You See Me, Now You Don'T: Protecting Smartphone Authentication from Shoulder Surfers". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '14. Toronto, Ontario, Canada: ACM, 2014, S. 2937–2946.

[De +12] Alexander De Luca u. a. „Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '12. Austin, Texas, USA: ACM, 2012, S. 987–996.

[Der+10] Mohammad Omar Derawi u. a. „Unobtrusive user-authentication on mobile phones using biometric gait recognition“. In: *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on*. IEEE. 2010, S. 306–311.

[DP00] Rachna Dhamija und Adrian Perrig. „Déjà Vu: A User Study Using Images for Authentication“. In: *Proceedings of the 9th Conference on USENIX Security Symposium - Volume 9*. SSYM'00. Denver, Colorado: USENIX Association, 2000, S. 4–4.

[Gas+14] Hugo Gascon u. a. „Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior.“ In: *Sicherheit*. 2014, S. 1–12.

[GMM13] Google, Ipsos MediaCT und Interactive Advertising Bureau Mobile Marketing Association. *Our mobile planet - Smartphone Penetration*. 2013. URL: http://think.withgoogle.com/mobileplanet/en/graph/?country=cn&country=de&country=us&category=DETAILS&topic=Q00&stat=Q00_1&wave=2011&wave=2012&wave=2013&age=all&gender=all&chart_type=bar&active=country (besucht am 02. 07. 2014).

[Har+06] Atsushi Harada u. a. „A User Authentication System Using Schema of Visual Memory“. In: *Proceedings of the Second International Conference on Biologically Inspired Approaches to Advanced Information Technology*. BioADIT'06. Osaka, Japan: Springer-Verlag, 2006, S. 338–345.

[Hay+08] Eiji Hayashi u. a. „Use Your Illusion: Secure Authentication Usable Anywhere“. In: *Proceedings of the 4th Symposium on Usable Privacy and Security*. SOUPS '08. Pittsburgh, Pennsylvania: ACM, 2008, S. 35–45.

[Hol08] Kjetil Holien. „Gait recognition under non-standard circumstances“. Magisterarb. Gjøvik University College, 2008.

[JE07] Jam Jenkins und Carla Ellis. „Using Ground Reaction Forces from Gait Analysis: Body Mass As a Weak Biometric“. In: *Proceedings of the 5th International Conference on Pervasive Computing*. PERVASIVE'07. Toronto, Canada: Springer-Verlag, 2007, S. 251–267.

[Kum+07] Manu Kumar u. a. „Reducing Shoulder-surfing by Using Gaze-based Password Entry“. In: *Proceedings of the 3rd Symposium on Usable Privacy and Security*. SOUPS '07. Pittsburgh, Pennsylvania: ACM, 2007, S. 13–19.

[LN13] Mun-Kyu Lee und Hyeonjin Nam. „Secure and Fast PIN-entry Method for 3D Display“. In: *SECURWARE 2013, The Seventh International Conference on Emerging Security Information, Systems and Technologies*. 2013, S. 26–29.

[MS13] Tilo Müller und Michael Spreitzenbarth. „FROST“. English. In: *Applied Cryptography and Network Security*. Hrsg. von Michael Jacobson u. a. Bd. 7954. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, S. 373–388.

[Mus12] Ildar Muslukhov. *How to bypass Android liveness check*. 2012. URL: https://www.youtube.com/watch?v=zYxphDK6s3I (besucht am 07. 07. 2014).

[Nix+96] Mark S Nixon u. a. „Automatic gait recognition“. In: *Biometrics*. Springer, 1996, S. 231–249.

[Pai91] Allan Paivio. „Dual coding theory: Retrospect and current status.“ In: *Canadian Journal of Psychology/Revue canadienne de psychologie* 45.3 (1991), S. 255–287.

[RM09] Karen Renaud und Joseph Maguire. „Armchair Authentication“. In: *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*. BCS-HCI '09. Cambridge, United Kingdom: British Computer Society, 2009, S. 388–397.

[RR06] Volker Roth und Kai Richter. „How to fend off shoulder surfing“. In: *Journal of Banking & Finance* 30.6 (2006), S. 1727–1751.

[Sch+13] Florian Schaub u. a. „Exploring the Design Space of Graphical Passwords on Smartphones“. In: *Proceedings of the Ninth Symposium on Usable Privacy and Security*. SOUPS '13. Newcastle, United Kingdom: ACM, 2013, 11:1–11:14.

[Sec12] European Association For Visual Data Security - Secure. *Visual Data Security White Paper*. 2012.

[Sta73] Lionel Standing. „Learning 10,000 pictures.“ In: *The Quarterly Journal of Experimental Psychology* 25 (1973), S. 207–222.

[Sym09] Symantec. *Datenverlust für Deutsche ein Drama*. 2009. URL: http://www.symantec.com/de/de/about/news/release/article.jsp?prid=20090527_02 (besucht am 07. 08. 2014).

[TKC05] Desney S. Tan, Pedram Keyani und Mary Czerwinski. „Spy-resistant Keyboard: More Secure Password Entry on Public Touch Screen Displays“. In: *Proceedings of the 17th Australia Conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future*. OZCHI '05. Canberra, Australia: Computer-Human Interaction Special Interest Group (CHISIG) of Australia, 2005.

[TOH06] Furkan Tari, A. Ant Ozok und Stephen H. Holden. „A Comparison of Perceived and Real Shoulder-surfing Risks Between Alphanumeric and Graphical Passwords“. In: *Proceedings of the Second Symposium on Usable Privacy and Security*. SOUPS '06. Pittsburgh, Pennsylvania: ACM, 2006, S. 56–66.

[Wie+06] Susan Wiedenbeck u. a. „Design and Evaluation of a Shoulder-surfing Resistant Graphical Password Scheme“. In: *Proceedings of the Working Conference on Advanced Visual Interfaces*. AVI '06. Venezia, Italy: ACM, 2006, S. 177–184.

[Zez+13] Emanuel von Zezschwitz u. a. „Making Graphic-based Authentication Secure Against Smudge Attacks“. In: *Proceedings of the 2013 International Conference on Intelligent User Interfaces*. IUI '13. Santa Monica, California, USA: ACM, 2013, S. 277–286.