RWTH AACHEN UNIVERSITY

Multitouch Authentifizierung

Diplomarbeit an der
Media Computing Group
Prof. Dr. Jan Borchers
Computer Science Department
RWTH Aachen University

von
Andreas Hüttig

Diplomarbeitsbetreuer:
Prof. Dr. Jan Borchers

Zweitprüfer:
Prof. Dr.-Ing. Ulrike Meyer

Registrierungsdatum: Mar 1st, 2011
Abgabedatum: Sep 12th, 2011

I hereby declare that I have created this work completely on my own and used no other sources or tools than the ones listed, and that I have marked any citations accordingly.

Hiermit versichere ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie Zitate kenntlich gemacht habe.

Aachen, SEPTEMBER2011
Andreas Hüttig

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abstract

Shoulder surfing is a constantly rising threat for IT security with lots of research potential. Few researchers looked into shoulder surfing security and most of them concentrated on new and not widely available hardware. New approaches are needed for a release to the public.
Main goal of this thesis is the development of authentication systems for increasingly popular multitouch systems. Main attributes of these systems shall be usability and security against shoulder surfing attacks.
A taxonomy was made, classifying up-to-date mutlitouch authentication systems to show potential for future research. Based on this, three prototypes were developed.
Utilizing paper prototypes, a study with 11 users was conducted and showed recognition rates of 70%-90% by humans. This study showed a 100% shoulder surfing security.
Subsequently, software prototypes were developed on a MacBookPro. The system was trained by machine learning and a user study with 62 users was conducted. The authentication data was gathered, learned and analyzed.
The software prototype could be improved to a recognition rate of 75% and all three authentication systems were graded "usable" by the users. Possible further research potential is shown in the summary section.

Überblick

Shouldersurfing ist eine von der Forschung wenig beachtete, aber stetig wachsende Bedrohung der IT-Sicherheit.
In den wenigen Fällen der Forschung, die sich mit Shouldersurfing auseinandersetzt, konzentriert sie sich meist auf neuartige und nicht weit verbreitete Hardware. Für eine Nutzung in der breiten Masse sind neue Ansätze sinnvoll.
Ziel dieser Arbeit ist die Entwicklung von Authentifizierungsverfahren, die speziell auf in der Öffentlichkeit immer beliebter werdenden Multitouchsystemen Verwendung finden können. Hauptaspekt dieser Authentifizierungsverfahren soll Sicherheit gegen Shouldersurfattacken bei einer benutzerfreundlichen Bedienung sein.
Hierzu wurde eine Taxonomie erstellt, die aktuelle multitouchfähige Authentifizierungsverfahren klassifiziert und Potential für weitere Forschung aufzeigt. Darauf basierend wurden drei Prototypen erstellt.
Bei einer Analyse der Papierprototypen an 11 Probanden, wurde einer Erkennungsrate von 70%-90% durch Menschen erreicht. Daraufhin wurden die Papierprototypen auf einem MacBookPro als Softwareprototypen entwickelt. Das System erlernte die Eingaben über maschinelles Lernen. Anschließend wurde eine Benutzerstudie mit 62 Testpersonen durchgeführt, deren Authentifizierungsdaten gesammelt, gelernt und analysiert wurden.
Die Papierprototypen erzielten in ersten Testläufen eine 100% Sicherheit gegen Shouldersurfattacken und konnten in der Weiterentwicklung als Softwareprototyp mit begrenzter Optimierung eine Erkennungsrate von 75% erzielen. Alle drei Authentifizierungsverfahren wurden bei einer Umfrage von den Benutzern als benutzerfreundlich eingestuft. Mögliche Forschungsansätze zur Weiterentwicklung werden abschließend aufgezeigt.

Danksagungen

Ich möchte Prof. Dr. Jan Borchers für die Betreuung meiner Diplomarbeit danken. Viel Inspiration für meine Forschung kam aus seinen Vorlesungen *Designing Interactive Systems I + II*.
Des weiteren möchte ich Jonathan Diehl danken. Er weckte mein Interesse für dieses Thema, gab zahlreiches und wertvolles Feedback und hatte viel Geduld mit mir.
Außerdem möchte ich mich bei meinen Studienteilnehmern bedanken, die mir Zeit und zahlreiches Feedback schenkten.
Ich danke meiner Familie, die mich zur richtigen Zeit angeschoben und mich auf meinem bisherigen Weg auf vielfältige Weise unterstützt hat.
Und als letztes und ganz besonders möchte ich meiner Freundin und meiner Tochter danken.

Konventionen

In dieser Arbeit werden die folgenden Konventionen verwendet:

Text Konventionen

Definitionen werden in farbigen Boxen herausgestellt.

EXKURS:
Ein Exkurs ist eine detaillierte Diskussion eines bestimmten Punktes in einem Buch, normalerweise in einem Anhang eines geschriebenen Textes.

Definition:
Exkurs

Die gesamte Arbeit ist in Hochdeutsch verfasst.

"Passwort und PIN Eingabeverfahren" wird am Rand mit "PW/PIN" abgekürzt.

Kapitel 1

Einleitung

IT-Sicherheit wichtig

Computer, Laptops und Smartphones gehören heute zum Alltag. Auf diesen Geräten werden sensible Daten gespeichert. Vor allem im Berufsleben werden Forschungsergebnisse, Firmengeheimnisse oder ähnliches elektronisch gespeichert. Verschaffen sich Dritte unerlaubten Zugang zu diesen Daten, kann der Schaden sehr hoch sein. Deshalb müssen das Gerät oder bestimmte auf ihm gespeicherte Daten besonders geschützt werden. Um auf geschützte Daten zugreifen zu können, muss ein Benutzer sich authentifizieren. Nur ein Benutzer, der beispielsweise die Zugangsdaten kennt und richtig eingibt, erhält Zugang zum Gerät.

Shouldersurfing bietet Forschungspotential

Die Untersuchung und Entwicklung verschiedener Authentifizierungsmöglichkeiten ist schon seit langem Gegenstand der Forschung. Immer noch erweist es sich als problematisch, dass die gängigsten Verfahren Schwächen bei Ausspähen des Authentifizierungsvorgangs durch Beobachten oder Filmen (sogenannte Shouldersurfattacken [1] aufzeigen. Solche Schwachpunkte werden oft von Kriminellen genutzt, um z.B. Zugang zu Kontodaten oder Geschäftsgeheimnissen zu erhalten. Es gibt in der Forschung bereits mehrere Ansätze, dem entgegenzuwirken[2]. Allerdings bedienen die sich komplizierter oder teurer Hardware. Das verhindert zur Zeit noch, solche Programme flächendeckend einzusetzen.

[1] siehe Kapitel 2.2

[2] siehe De Luca et al. [2009] und Sasamoto et al. [2008]

Multitouch zunehmend verbreitet und schützenswert

Multitouchsysteme werden immer beliebter. Vor allem Smartphones finden in der Bevölkerung immer größere Verbreitung. Von 73 im Zuge dieser Arbeit befragten Personen gaben 27 an, ein Multitouchgerät zu besitzen. Auf diesen Geräten werden ebenfalls sensible Daten wie Bankdaten oder PIN-Nummern gespeichert. Daher ist auch hier eine erhöhte Sicherheit bei der Zugangserlaubnis zum Gerät oder nur zu einzelnen dort gespeicherten Inhalten erforderlich.

Nachteile von Passwortverfahren auf Multitouch: kein haptisches Feedback, kleine Tasten, sehr anfällig gegen Shouldersurfing

Aktuell ist eine Zugangsbeschränkung fast ausschließlich auf eine einfache Passwort oder PIN-Eingabe beschränkt. Diese erfolgt durch Eingabe über eine virtuelle Tastatur. Wegen oft sehr kleinen Tasten und dem fehlenden haptischen Feedback ist die Bedienung zum Teil schwierig. Außerdem gibt es bei diesem Verfahren große Sicherheitslücken. Gibt man zum Beispiel über die virtuelle Tastatur des iPhones von Apple ein Passwort ein, wird jeweils das zuletzt eingegebene Zeichen auf dem Display eingeblendet, ehe es verschlüsselt erscheint. Das mag zwar für den legitimen Nutzer zur Orientierung nützlich sein. Ein unbefugter Dritter kann allerdings gegebenenfalls bequem mitlesen. Das System weist noch erhebliche Mängel gegen Shouldersurfattacken auf.

Authentifizierung auf Multitouch bietet auch Forschungspotential

Die Authentifizierung auf Multitouchgeräten ist bereits Gegenstand der Forschung. Sicherheitslücken durch Shouldersurfattacken bieten noch viel Forschungspotential. Hier setzt diese Arbeit an. Durch die Verknüpfung neuartiger Authentifizierungssysteme mit der Eingabe über Multitouch soll diese Lücke geschlossen werden. Ein besonderes Augenmerk wird dabei auf die Benutzerfreundlichkeit gelegt. So soll bei einer eventuellen praktischen Umsetzung ein breiter Einsatz ermöglicht werden.

Hauptziel der Arbeit

Das Hauptziel dieser Arbeit ist die Entwicklung von Authentifizierungsverfahren auf Multitouchsystemen, die einen erhöhten Sicherheitsstandard gegen Shouldersurfattacken bieten und dabei benutzerfreundlich sind.

Forschungsfragen

Forschungsfragen sind:

- Welche Authentifizierungsverfahren können auf weit

verbreiteten Multitouchsystemen eingesetzt werden?

- Wie können diese im Rahmen der Multitouchsysteme verbessert werden?
- Bieten die verbesserten Systeme Sicherheit gegen Shouldersurfing?
- Sind die verbesserten Systeme benutzerfreundlich?[3]

Beitrag zur Forschung

Authentifizierungsforschung, Multitouchsysteme und Shouldersurfing-Untersuchungen werden in dieser Arbeit miteinander verknüpft. Außerdem wird zur besseren Übersicht über bisher bereits erforschte Authentifizierungsverfahren und Multitoucheingabemöglichkeiten eine Taxonomie erstellt.

1.1 Gang der Arbeit

Theorie

Zum besseren Verständnis der IT-Sicherheit, insbesondere bei Brute Force und Shouldersurfattacken, werden im nächsten Kapitel zunächst deren theoretische Grundlagen dargelegt. Auf Aspekte der Benutzerfreundlichkeit und Privatsphäre wird auch eingegangen.

Verwandte Forschungsarbeiten

Das dritte Kapitel stellt Forschungsarbeiten vor, die relevant für diese Arbeit sind. Es wird dargelegt, was die Autoren gemacht haben, was sie erreicht haben und inwiefern sich deren Forschungsarbeit von dieser unterscheidet.

Taxonomie der Multitouchauthentifizierung

Im vierten Kapitel wird eine Taxonomie für Multitouchauthentifizierung erstellt. Es werden Authentifizierungsverfahren, die auf Multitouchsystemen umsetzbar sind, aufgezählt, beschrieben und in die Taxonomie eingeordnet.

Design, Papierprototyp und Studie

Darauf basierend wurden drei neue Authentifizierungsverfahren entwickelt und beschrieben, die über ein Multitouchsystem eingegeben werden können. Im fünften Kapitel werden Messgrößen festgelegt und die grundlegenden Ideen für Weiterentwicklungen beschrieben. Diese wurden

[3] siehe Shneiderman et al. [2009] Seite 32

zuerst als Papier-Prototypen realisiert und getestet. Das Ende dieses Kapitels beschreibt diese Benutzerstudie.

Softwareprototyp auf MacBookPro mit künstlichem neuronalen Netzwerk und Studie

Kapitel sechs behandelt die Implementierung der jeweiligen Authentifizierungssysteme in einen Softwareprototypen. Dieser wurde in Objective C auf einem MacBookPro entwickelt und nutzt das integrierte Multitouchpad mit einem privaten Framework von Apple. Anschließend werden die Daten über Maschinelles Lernen analysiert. Dies wurde über ein künstliches neuronales Netz realisiert. Das Ende des Kapitels bildet die Beschreibung und Auswertung der durchgeführten Benutzerstudie.

Evaluierung

Im siebten Kapitel werden die Messgrößen evaluiert und die Forschungsfragen beantwortet. Die Authentifizierungsverfahren werden abschließend betrachtet und die Ergebnisse interpretiert. Die Zielsetzung dieser Arbeit wird mit mit dem Erreichten verglichen. Aufgezeigt wird, was technisch umsetzbar war.

Zusammenfassung und Ausblick

Nach der Zusammenfassung aller Ergebnisse im letzten Kapitel wird abschließend dargelegt, welche Weiterentwicklungsansätze die in dieser Arbeit entwickelten Authentifizierungsverfahren bieten.

Kapitel 2

Theorie

Herausforderungen

Die großen Herausforderungen der IT-Sicherheit im Bereich der Mensch-Maschine-Interaktion sind Shouldersurfer, Brute-Force-Attacken, Benutzerfreundlichkeit und die informationelle Selbstbestimmung der Benutzer.

Shouldersurfing

Niemand sollte eine Authentifizierung "stehlen" können, indem er beim Authentifizierungsprozess durch Beobachten der Bewegung der Finger oder des Bildschirms den Schlüssel abguckt. Außerdem sollte die Authentifizierung schwer zu nachzuvollziehen oder durch kriminelle Angriffe auf das System zu erhalten sein.

Benutzerfreundlichkeit

Andererseits muss die Authentifizierung an Geräten des täglichen Lebens auch benutzerfreundlich sein. Für einen Nutzer ist es unzumutbar, sich eine lange willkürliche Zeichenkette zu merken und einzugeben. Ein benutzerfreundlicher Schlüssel sollte mit nur einem Versuch einzugeben sein. Handelt es sich zum Beispiel um ein Passwort, sollte es eine angemessene Länge haben. Auch sollte die Authentifizierung nur einige Sekunden in Anspruch nehmen.

informationelle Selbstbestimmung

Des weiteren sollte genau bemessen werden, welche Art der Authentifizierung für welches System sinnvoll ist. Niemand wird beispielsweise bereit sein, seinen Daumenabdruck zu leisten, um sich in einem sozialen Netzwerk anzumelden. Auf einer e-Banking-Seite wird eine solche Au-

thentifizierung besser akzeptiert[1].

2.1 Brute Force

Definition: *Brute Force*

BRUTE FORCE:
Sei d ein Authentifizierungssystem und sei $K = k_1, ..., k_k$ der Schlüsselraum über allen möglichen Schlüsseln k_i. Eine Brute-Force-Attacke prüft für alle $k_i \in K$, ob $d(k_i)$ die Authentifizierung akzeptiert. Wenn das System akzeptiert, wurde möglicherweise ein korrekter Schlüssel gefunden. Wenn nicht, fahre mit dem nächsten Schlüssel fort. (nach Paar and Pelzl [2010])

Brute Force probiert alle Möglichkeiten

Durch eine Brute Force Attacke wird versucht, in ein passwortgeschütztes System einzudringen. Dies geschieht durch Ausprobieren. Das Brute-Force-System durchläuft jeden möglichen Schlüssel, bis der korrekte gefunden wurde. Bisher kann dies kaum verhindert werden.

Abwehr durch großen Schlüsselraum

Beste momentane Abwehrmaßnahme ist der Versuch den Erfolg der Brute-Force-Attacke zu verzögern. Dies geschieht über einen möglichst komplizierten Schlüssel. Je größer der Pool ist, aus dem der richtige Schlüssel zusammengesetzt werden muss, desto länger benötigt das Brute-Force-System, um einzudringen. Handelt es sich bei dem Schlüssel beispielsweise um ein Passwort, sollte dies aus einer möglichst langen und möglichst komplizierten Zeichenkette bestehen. Also z.B. Zahlen, große und kleine Buchstaben in einer willkürlichen Reihenfolge.

Brute Force Beispiel

Eine mögliche Brute-Force-Attacke ist ein Skript, dass nacheinander alle möglichen Kombinationen von Sonderzeichen, Zahlen und Buchstaben kombiniert und ausprobiert. Erst werden alle Einerkombinationen probiert, dann alle Zweier, Dreier, Vierer usw. bis die richtige gefunden wurde. Je länger und komplizierter die Passwortkette, desto mehr Zeit benötigt die Attacke. Es ist daher sinnvoll, wenn das zum Schutz installierte Authentifizierungssystem von vorne herein nur Passwörter mit einer bestimmten

[1] siehe Jones et al. [2007]

Mindestzahl von Zeichen zulässt.

2.2 Shouldersurfing

SHOULDERSURFING:
Unter "Shouldersurfing" versteht man das "Abgucken" oder Ausspionieren der Authentifizierung durch eine neben oder hinter jemandem stehende Person. Das kann auch durch Hilfsmittel, z.B. eine Kamera, geschehen.

Definition: *Shouldersurfing*

Schutzmöglichkeiten

Die Methode ist simpel, Schutz bietet nur erhöhte Aufmerksamkeit anderen Personen gegenüber während der Authentifizierung. Das Gerät, an dem sich eingeloggt wird, sollte Passwörter nur verschlüsselt darstellen. Erhöht werden kann die Sicherheit durch komplexere Eingabemethoden. Gegen in krimineller Absicht installierte Kameras, z.B. an Bankautomaten, kann sich ein Kunde kaum schützen. Hier muss die Bank ihr System verbessern und vor allem regelmäßig überprüfen.

2.3 Benutzerfreundlichkeit

Systeme müssen verständlich und einfach nutzbar sein

Benutzerfreundlichkeit ist besonders wichtig bei der Authentifizierung. Bei allen Sicherheitsmaßnahmen müssen weit verbreitete Systeme, wie sie z.B. in Bankautomaten oder Mobiltelefonen sind, auch für den technischen Laien verständlich und einfach nutzbar sein. Dabei darf nach Grossman et al. [2009] weder die Festlegung der Authentifizierung, wie das Erstellen einer PIN oder das Erlernen einer Geste, noch die eigentliche Authentifizierung zu zeitaufwändig oder kompliziert sein. Das sicherste System ist nutzlos, wenn die Anwendung zu kompliziert oder zeitaufwändig ist.

Beispiel PIN/Passwort

Das am weitesten verbreitete Authentifizierungsverfahren, das Passwort, wird nach einmaliger Eingabe vom System erlernt. Die Authentifizierung selbst dauert auch bei Benutzung einer Standardtastatur für ungeübte Computernutzer

Abbildung 2.1: Shouldersurfing Attacke an einem Bankautomaten

nur wenige Sekunden. Eine vierstellige PIN für den Bankautomaten können sich auch alte Leute merken und die Eingabe über ein Nummernfeld bewältigen auch Computerlaien.

Benutzerfreundlichkeit gilt auch für IT-Sicherheit

Benutzerfreundlichkeit ist im Umfeld der IT-Sicherheit besonders wichtig, da ein Benutzer sich immer wieder an einem System authentifizieren muss. Als Beispiel sei das Freischalten eines Handys durch die eigene PIN genannt. Fehlende Benutzerfreundlichkeit erhöht den Zeitaufwand, die Frustration oder den mentalen Arbeitsaufwand bei der Benutzung des Systems. Dadurch kann der Benutzer allgemein unproduktiver werden. Ob er effektiv weniger Arbeitszeit hat, schlechter motiviert ist oder unkonzentrierter ist: schlechte Benutzbarkeit ist nicht nur ein Mangel an Lebensstandard, sondern auch ein wirtschaftlicher Faktor.[2]

[2] siehe Shneiderman et al. [2009] Seite 33ff.

2.4 Informationelle Selbstbestimmung

Privatsphäre des Nutzers achten

Persönliche Vorbehalte können die praktische Anwendung einer Authentifizierungsmethode einschränken. Nutzer sind nicht immer bereit, ihren Fingerabdruck zu hinterlegen. Daher müssen beim Programmieren solcher Authentifizierungsmöglichkeiten auch persönliche Vorlieben und die "Stimmung" in der Zielgruppe beachtet werden. So beschreiben etwa Jones et al. [2007], dass ca. 50% ihrer befragten Nutzer Vorbehalte gegen Gesichtserkennung im Verkaufssektor haben.

Kapitel 3

Verwandte Forschungsarbeiten

In diesem Kapitel werden Forschungsarbeiten vorgestellt, die Grundlage dieser Arbeit sind. Es wird das Thema jedes Aufsatzes dargelegt und deren Relevanz für diese Arbeit.

Hauptsächlich Authentifizierungsverfahren für die Taxonomie

Die meisten der vorgestellten Forschungsarbeiten behandeln verschiedene Authentifizierungsverfahren. Diese Authentifizierungsverfahren werden in Kapitel 4 dieser Arbeit in einer Taxonomie klassifiziert und genauer erläutert. So wird detailliert herausgearbeitet, wo noch Forschungspotential besteht. Im weiteren Verlauf dieser Arbeit werden davon ausgehend drei eigene Authentifizierungsverfahren entwickelt.

"Do Background Images Improve "Draw a Secret" Graphical Passwords?"

Die Forschungsarbeit *"Do Background Images Improve "Draw a Secret" Graphical Passwords?"* stellt "Draw a Secret" als Authentifizierungsverfahren vor. Dunphy and Yan [2007] verbesserte dieses durch ein Hintergrundbild, an dem sich der Nutzer während der Eingabe der Authentifizierung orientieren kann. Dadurch ist es möglich auch kompliziertere Graphiken als Schlüssel zu verwenden.

Inspirierte FreeSwipe

"Draw a Secret" diente in dieser Arbeit als Ausgangspunkt für das hier entwickelte Authentifizierungsverfahren FreeSwipe[1]. Bei FreeSwipe soll die Eingabe mit mehre-

[1] siehe Kapitel 5.5

ren Fingern gleichzeitig erfolgen. Ein möglicher Einsatz eines Hintergrundbildes nach dem Vorbild von Dunphy wird im Kapitel 8 "Zusammenfassung und weitere Forschungsansätze" auf Seite 71 besprochen.

"Empirical Evaluation for Finger Input Properties In Multi-touch Interaction"

In der Forschungsarbeit *"Empirical Evaluation for Finger Input Properties In Multi-touch Interaction"* wird von Wang and Ren [2009] untersucht, welche Parameter von einem Multitouchsystem geliefert werden können. Sie bilden Grundlage zu den hier entwickelten Authentifizierungsverfahren, da diese speziell für Multitouchsysteme erarbeitet wurden.

Fingereigenschaften wichtig für Taxonomie

Desweiteren führt Wang einige Experimente durch, mit der Fragestellung, welche Fingereigenschaften durch ein Multitouchpad erkannt werden können. Neben der allgemein bereits benutzten Koordinate kam er auf Geschwindigkeit, Beschleunigung, Ausmaße, Form, Orientierung und Druck, sowie die beiden Events Tap und Flick. Diese Parameter bilden die Grundlage der in dieser Arbeit erstellten Taxonomie. Neue Kombinationsmöglichkeiten führten zur Entwicklung von den Authentifizierungsverfahren HandScan, TipSlide und FreeSwipe in dieser Arbeit.

"HandsDown: Hand-contour-based User Identification for Interactive Surfaces"

Ein Authentifizierungsverfahren, das den Nutzer über seinen Handumriss erkennt, wird in der Forschungsarbeit *"HandsDown: Hand-contour-based User Identification for Interactive Surfaces"* von Schmidt et al. [2010] vorgestellt. Es wurde für Tabletops entwickelt. Mit "HandsDown" versuchten die Entwickler ein gegen Shouldersurfattacken wirksames Authentifizierungsverfahren zu finden. Die Einfachheit der Authentifizierungsbewegung, das bloße Auflegen der Hand, diente dieser Arbeit als Inspiration für die Entwicklung des Authentifizierungsverfahrens HandScan.

"Identity Authentication Based on Keystroke Latencies Using Neural Networks"

Die Forschungsarbeit *"Identity Authentication Based on Keystroke Latencies Using Neural Networks"* von Lammers and Langenfeld [1991] wird ebenfalls vorgestellt. Der auf Joyce and Gupta [1990] basierende Aufsatz behandelt die Authentifizierung durch Keystroke. Dabei wurde die einfache Eingabe eines Passworts durch die genaue Messung der Zeitabstände zwischen den einzelnen Tastenanschlägen erweitert. Dies geschah mithilfe eines künstlichen neuronalen Netzes anstelle von Bayes-Klassifikatoren. So wurde dem System eine erhöhte Flexibilität ermöglicht und

eine Erfolgsrate von 75% bei nur 3% falsch-positiven Erkennungen erreicht.

Biometrie bei Multitouch?

Die Idee, vorhandene Authentifizierungsverfahren durch biometrische Daten zu erweitern, machte sich auch diese Arbeit zu nutze. Nach dem Vorbild Lammers wurden auch hier die Softwareprototypen mittels eines künstlichen neuronalen Netzwerkes umgesetzt.

"Multi-Touch Authentication on Tabletops"

"Multi-Touch Authentication on Tabletops" von Kim et al. [2010] untersucht Authentifizierungsverfahren in einer bestimmten Arbeitsumgebung: Verschiedene Nutzer arbeiten an nur einem Gerät, hier einem Tabletop. Shouldersurfing ist in dieser Forschungsarbeit von großer Bedeutung, da in der beschriebenen Arbeitsumgebung immer andere Menschen in der Nähe sind. Die Gefahr, dass der eigene Schlüssel abgeschaut wird, ist also erhöht.

Eingeschränkt auf Tabletops

Insgesamt stellt "Multi-Touch Authentication on Tabletops" fünf Authentifizierungsverfahren vor. Diese sind ebenfalls in der Taxonomie[2] dieser Arbeit zu finden. Sie alle basieren auf einer graphischen oder numerischen PIN. Während Kim et al. [2010] sich ausschließlich auf Tabletops konzentriert haben, bezieht diese Arbeit alle Multitouchsysteme mit ein.

"MicroRolls: Expanding Touch-Screen Input Vocabulary by Distinguishing Rolls vs. Slides of the Thumb"

Der Aufsatz *"MicroRolls: Expanding Touch-Screen Input Vocabulary by Distinguishing Rolls vs. Slides of the Thumb"* von Lecolinet et al. [2009] beschäftigt sich mit Eingabegesten auf Singletouch-Handhelds. 16 elementare Gesten wie Ziehen, Wischen, Reiben oder Rollen werden vorgestellt, implementiert und analysiert.

Inspirierte TipSlide

Die Arbeit zeigt, dass diese Gesten vom System ausnahmslos erkannt werden. Auf Geräten mit einem begrenzten Touchdisplay ist die Eingabe mit MicroRolls besser als mit Dropboxen und Scrollleisten. Die hohe Erkennungsrate der MicroRolls diente als Grundlage für die Entwicklung des Authentifizierungsverfahrens TipSlide[3] im Rahmen dieser Arbeit.

[2] siehe Kapitel 4
[3] siehe Kapitel 5.4

"Novel Shoulder-Surfing Resistant Haptic-based Graphical Password"

In der Forschungsarbeit *"Novel Shoulder-Surfing Resistant Haptic-based Graphical Password"* von Malek et al. [2006] wird die Erweiterung graphischer Passwörter durch ein verstecktes Attribut vorgestellt. Das dort entwickelte Authentifizierungsverfahren PassGraph schneidet wegen des zusätzlichen Parameters "Druck" gegen Shouldersurfattacken besser ab als jedes vorher bekannte graphische Passwort.

Druck als zusätzlicher Parameter

PassGraph wurde in die Taxonomie dieser Arbeit eingearbeitet. Außerdem wurde versucht, den Parameter "Druck" auch auf einem Multitouchpad statt auf einem Singletouchpad wie bei Malek et al. [2006] einzusetzen. Allerdings scheiterte der Versuch an der zu geringen Auflösung des Multitouchpads. Eine Verwendung des Parameters Druck wurde daher für die Entwicklung der Authentifizierungsverfahren im Rahmen dieser Arbeit wieder verworfen[4].

"PassShape: Stroke based Shape Passwords"

Um die Entwicklung des Singletouch-Authentifizierungssystems PassShape geht es in der Forschungsarbeit *"PassShape: Stroke based Shape Passwords"* von De Luca et al. [2007]. Die PIN wird hier durch einfache Striche eingegeben. Der Nutzer muss sich kein kompliziertes Passwort aus Buchstaben- und/oder Zahlenketten mehr merken, sondern ein Bild, das er über das Multitouchpad eingibt. Ein Beispiel für ein solches Bild aus Strichen wäre "Das Haus vom Nikolaus".

Gedächtnisbelastung wichtiger Faktor

PassShape findet sich ebenfalls in der Taxonomie dieser Arbeit. Eine Rolle bei der Entwicklung neuer Authentifizierungsverfahren spielte auch hier die Gedächtnisbelastung. Die neuen Verfahren sollten einfacher zu merken sein als herkömmliche Passwörter.

"TapSongs: Tapping Rhythm-Based Passwords on a Single Binary Sensor"

In der Arbeit *"TapSongs: Tapping Rhythm-Based Passwords on a Single Binary Sensor"* beschreibt Wobbrock [2009] ein Authentifizierungsverfahren, das auf nur einem Knopf basiert. Der Authentifizierungsschlüssel ist hierbei eine Abfolge von Clicks, die einem vom Benutzer gewählten Rhythmus folgen. In Versuchen konnten andere Personen den vom Benutzer festgelegten Rhythmus selbst dann nicht kopieren, wenn sie das zugrunde liegende Lied kannten.

[4] siehe Kapitel 6.1

Inspirierte, mit “Draw a Secret”, FreeSwipe

Darauf baut die im Rahmen dieser Arbeit entwickelte Authentifizierungsgeste FreeSwipe auf. Es wird vermutet, dass eine einem zweiten Nutzer ebenfalls bekannte Geste trotzdem nur schwer kopiert werden kann.

Verdeckte Anwendung noch zu erforschen

Mittels TapSong kann sich ein Nutzer an seinem Gerät authentifizieren, ohne dieses zu sehen, was es gegen Shouldersurfangriffe sehr sicher macht. Dies wird für die Authentifizierungsgeste HandScan ebenfalls vermutet.[5]

“Towards Understanding User Perceptions of Authentication Technologies”

In der Arbeit *“Towards Understanding User Perceptions of Authentication Technologies”* untersucht Jones et al. [2007] die Akzeptanz der Benutzer bezüglich Authentifizierungsverfahren im Hinblick auf unterschiedliche Einsatzbereiche.

Die Akzeptanz, Bedenken und gefühlte Sicherheit der Authentifizierungsverfahren Iris/Retina Scan, Fingerabdruckscanner, Handgeometriemessung, Stimmerkennung, Gesichtserkennung, Passwort, Smart Card, RFID Tags, Unterschriftenanalyse und digitale Zertifikate werden im Hinblick auf die Bereiche Finanzwesen, Gesundheitswesen und Einzelhandel abgefragt.

Akzeptanz hängt vom Einsatzgebiet ab

Wichtigstes Ergebnis der Untersuchung ist, dass Benutzer für unterschiedliche Bereiche unterschiedliche Authentifizierungsverfahren akzeptieren. Die Akzeptanz eines bestimmten Authentifizierungssystems hängt nach Jones eher von der Erfahrung eines Nutzers mit diesem System ab. Die tatsächliche Sicherheit oder eventuelle Bedenken über die Abgabe biometrischer Daten spielen untergeordnete Rollen. Dies wurde bei der Entwicklung der Authentifizierungsverfahren im Rahmen dieser Arbeit beachtet.

[5] siehe Kapitel 8 “Zusammenfassung und weitere Forschungsansätze” auf Seite 71

Kapitel 4

Taxonomie der Multitouch-Authentifizierung

TAXONOMIE:
Eine Taxonomie (altgr. táxis "Ordnung" und nómos "Gesetz") oder Klassifikationsschema ist ein einheitliches Verfahren oder Modell, um Objekte eines gewissen Bereichs (ggf. unter Zuhilfenahme eines Klassifikationsinstruments) nach bestimmten Kriterien zu klassifizieren, das heißt, sie in bestimmte Kategorien oder Klassen (auch Taxa genannt) einzuordnen. (nach Wolfgang J. Koschnik [1993])

Definition: *Taxonomie*

Um eine Übersicht über die vorhandenen Authentifizierungsverfahren und Multitouchtechniken zu visualisieren, wurden sie in eine Taxonomie einsortiert. Diese Taxonomie zeigt Abbildung 4.1. Im folgenden Kapitel wird erläutert, wie sie entstand.

Ausmaß nicht verwendet, parallele Eingabe ausbaufähig

Anhand dieser Tabelle lässt sich erkennen, dass der Parameter "Ausmaß" bisher nicht verwendet wird. Auch im Bereich der parallelen bzw. gleichzeitigen Eingabe gibt es viele Entwicklungsmöglichkeiten. So ließe sich das Passwortverfahren um "Form" oder "Ausmaß" erweitern, um analog zum KeyStroke-Verfahren biometrisch festzustellen, ob der zu authentifizierende Finger in Größe und Form der ge-

Taxonomie der Multitouch-Authentifizierung	Singular	Multiple	Timing	Areal/Taste	Position	Ausmaß	Form	Orientierung	Druck
Passwort	●			●					
Keystroke	●		○	●					
TapSongs	●		○	●					
ShieldPIN	●			●	●		●		
SlotPIN	●				●				
CuePIN	●				●				
	●						●		
ColorRings		●			●			●	
PassShape	●		●	●	●				
Draw a Secret	●				●				
PassGraph	●				●				●
HandsDown	●					●	●		
Pinch		●			●				
Rotate		●			●				
Flick	●			●	●				
MicroRolls	●				●				
Multifinger Mouse		●			●				

Abbildung 4.1: Taxonomie der Mulitouch-Authentifizierung. Leere Kreise bedeuten dieser Parameter wird biometrisch analysiert

speicherten Information entspricht. Auch "Draw a Secret" könnte durch den Parameter Ausmaß erweitert werden, so dass nicht nur die Position, sondern auch die Breite der Linien abgeglichen werden kann.

4.1 Dimensionen

Das Wichtigste einer Taxonomie sind ihre Dimensionen. Die Elemente werden anhand bestimmter Eigenschaften oder Kriterien strukturiert. In dieser Arbeit werden die einzelnen Kriterien der verschiedenen Authentifizierungsmethoden in fünf Gruppen unterteilt.

1. Hier analysiert das System die oben beschriebenen Eingabeparameter nahezu ausschließlich biometrisch. Der Benutzer kann sich aufgrund seiner physischen oder psychischen Beschaffenheit authentifizieren. Die psychische Beschaffenheit nutzt charakteristische Eigenschaften wie bei einer ausgeprägten Handschrift. Bei der physischen Beschaffenheit werden zum Beispiel Iris oder Netzhautbeschaffenheit, Fingerabdruck oder ähnliches genutzt. Biometrie

2. Hier ist relevant, ob nur ein einziges Eingabeelement betätigt wird, oder ob mehrere Eingabeelemente gleichzeitig betätigt werden können. Bei der Passworteingabe beispielsweise muss jeder Buchstabe einzeln nacheinander eingegeben werden. Würden zwei Tasten exakt gleichzeitig gedrückt, müsste der Computer die Wahl über die Reihenfolge der Weiterleitung ins System treffen. Denn ein Passwort besteht aus einer singulären Zeichenkette. Parallelität

3. Hier ist zu unterscheiden, ob das Timing bei der Eingabe kritisch ist oder ob zwischendurch beliebig Pausen gemacht werden können. Ein Rhythmus, der eingegeben werden muss, ist zeitkritisch. Bei der Passworteingabe kann nach jedem Symbol eine beliebig lange Pause eingelegt werden. Timing

4. Ein weiteres Kriterium für die Eingliederung in die Areal/Taste

Taxonomie ist die auf einen Teil der Fläche beschränkte Eingabe wie z.B. bei virtuellen Tastaturen. Dabei ist die Position zwar wichtig, aber in einem sehr ungenauen Rahmen, da immer ganze Areale den selben Effekt haben. Soll über eine virtuelle Tastatur der Buchstabe "d" eingegeben werden, ist es unerheblich, wo genau die für den Buchstaben "d" vorgesehene Taste getroffen wird. Dies ist klar zu unterscheiden von der möglichen Varianz bei der Position, um z.B. Ungenauigkeiten der Eingabe durch Hardwarebeschränkungen oder menschliche Ursachen wie minimales Zittern der Finger auszugleichen. In dieser Taxonomie werden Areale und Tasten gleichgesetzt, da physikalische Tastaturen einfach durch virtuelle ersetzt werden können. Dabei kommt es dann auf die areale Eingabe an.

Fingereigenschaften

5. Mögliche Parameter, die unterschiedliche Multitouchsysteme bieten, sind im Allgemeinen: Position, Ausmaß, Form, Orientierung und Druck. Bei der Position ist es wichtig, wo innerhalb des Eingabefeldes der Touch liegt. Beim Ausmaß werden Höhe und Breite und bei der Form der tatsächliche Umriss des Touches betrachtet. Die Orientierung beschreibt den Winkel des Fingers auf der Eingabeebene während der Eingabe. Der Druck entspricht der physikalischen Größe, die während des Touches auf das Eingabefeld ausgeübt wird.

Fingereigenschaften nur eingeschränkt verfügbar

Allerdings bietet nicht jedes System eine Erkennung für sämtliche Parameter bzw. stellt diese Parameter Entwicklern zur Verfügung. Während die Position bei allen Systemen implementiert ist, verwendet z.B. Apple in seinem Multitouch-Framework nur das Oval als Form. Kompliziertere Formen werden unter anderem in mehrere Ovale zerlegt. Druck wird bisher nur von sehr wenigen Systemen angeboten. Allerdings ändern sich durch Druck im begrenzten Rahmen auch Größe und Form, so dass man bei Systemen, die Druck nicht anbieten, trotzdem in eingeschränktem Rahmen auf eine Druckveränderung schließen kann.

4.2 Ausschlusskriterium

Zusätzliche Hardware ist Ausschlusskriterium

Diese Arbeit beschränkt sich auf Verfahren und Systeme, die auf Multitoucheingabe basieren und ausschließlich die unter "Dimensionen" genannten Eigenschaften nutzen. Auch wenn die Passwortauthentifizierung ursprünglich nicht für Multitouchsysteme entwickelt wurde, ist sie mit virtuellen Tastaturen auch dort umsetzbar. Ein System wie VibraPass (De Luca et al. [2009]) hingegen benötigt weitere Hardware, um dem Benutzer versteckt haptisches Feedback geben zu können.

Auf Geräten mit ausschließlich Multitoucheingabe nutzbar

Dies ist wichtig, da die betrachteten Authentifizierungsverfahren von einer breiten Masse genutzt werden sollen, auch dort, wo eventuelle zusätzliche Hardware nicht verfügbar ist. Wenn beispielsweise auf einem Smartphone nur ein Multitouchscreen als Eingabe vorhanden ist, sollten die Authentifizierungsverfahren dennoch auf diesem Gerät zu verwenden sein.

Es ist möglich, andere Verfahren zu klassifizieren, birgt aber Risiken

Die Taxonomie kann ebenfalls verwendet werden, um Authentifizierungsverfahren zu klassifizieren, die zusätzliche Hardware benötigen. Dann könnten allerdings elementare Merkmale des Authentifizierungsverfahrens außer Acht gelassen werden.

4.3 Authentifizierungsverfahren

In diesem Abschnitt werden Authentifizierungsverfahren vorgestellt, die sich für die einfache Umsetzung in Multitouchsystemen eignen. "Einfache Umsetzung" bedeutet hier, dass außer Multitoucheingabefläche, Bildschirm und verarbeitendem Computer keine zusätzliche Hardware benötigt wird.

Zusätzlich werden die Kriterien erläutert, die zur Einordnung in die Taxonomie dienen.

4.3.1 Passwort

Abbildung 4.2: Password Authentifizierung, wie auf dem iPhone implementiert

Passwort: Singular-Key/Area

Das am meisten genutzte Authentifizierungsverfahren ist die Passworteingabe. Diese ist sehr einfach: Bei der Registrierung wird eine Zeichenkette, das Passwort, festgelegt. Beim Authentifizieren wird dieses Passwort eingegeben, beides wird miteinander verglichen. Bei Deckungsgleich-

heit erfolgt die Authentifizierung. Eine Implementierung auf Single- und Multitouchsystemen hat mit virtuellen Tastaturen schon stattgefunden.

Die Eingabe besteht aus einer singulären Zeichenkette, die über Tasten eingegeben wird. Dementsprechend wird "Passwort" bei Singular-Key/Area einsortiert.

4.3.2 Keystroke

Biometrische Analyse der Tastenanschläge beim Passwort

Keystroke[1] ist als Verfahren der Passworteingabe sehr ähnlich. Die Sicherheit der Authentifizierung über Keystroke ist allerdings etwas höher, da nicht nur die Deckungsgleichheit der Zeichenkette, sondern auch das Timing der einzelnen Tastenanschläge überprüft wird.

Erlernen schwieriger für System und Benutzer

Ein Nachteil der Authentifizierung über Keystroke ist, dass das Erlernen der Authentifizierung komplizierter ist. Der Benutzer muss vor allem den Eingaberhythmus sorgfältig trainieren. Ist der Nutzer zum Beispiel aufgeregt, hat die Erfahrung gezeigt, dass es Probleme machen kann, den festgelegten Rhythmus zu wiederholen. Dann erhält er keinen Zugang zum eigenen System.

Problem: Wechsel von Hardware

Zu Schwierigkeiten kann auch der Austausch von Tastaturen oder Touchpads etc. führen. Veränderte Oberflächenstrukturen, Tastengrößen oder der Abstand zwischen den einzelnen Tasten können ebenfalls zum Problem werden.

Singular-Key/Area

Analog zum Passwort wird es in die Singular-Key/Area eingeordnet. Allerdings ist hier das Timing von entscheidender Bedeutung, denn es wird biometrisch analysiert.

4.3.3 TapSongs

Rhythmus auf einem Knopf

Diese Authentifizierung funktioniert mit nur einem einzigen Knopf. Vorgestellt wurde sie von Wobbrock [2009]. Der

[1] siehe Bergadano et al. [2002] und Joyce and Gupta [1990]

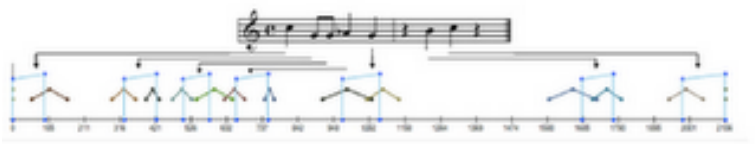

Abbildung 4.3: Lied mit Tap Rhythmus

Nutzer wählt einen bestimmten Song aus, dessen Rhythmus er über den Knopf eingibt.

Von außen kaum nachvollziehbar

Der eingegebene Rhythmus ist von außen kaum nachvollziehbar. Daher ist die Sicherheit dieser Authentifizierungsmethode gegen Shoulder-Surfing-Attacken sehr hoch. Erfahrungen zeigen allerdings, dass die Gefahr, bei erneuter Eingabe vom gewählten Rhythmus zu stark abzuweichen, größer ist als bei der Authentifizierung über Keystroke.

Singular-Key/Area, Timing

Auch hier ist Timing von entscheidender Bedeutung. Es wird allerdings nicht biometrisch analysiert. Zur Eingabe wird nur eine Taste benötigt, die sich über das komplette Multitouch-Feld erstrecken kann. Es wird also bei Singular-Key/Area-With Timing einsortiert.

4.3.4 ShieldPIN

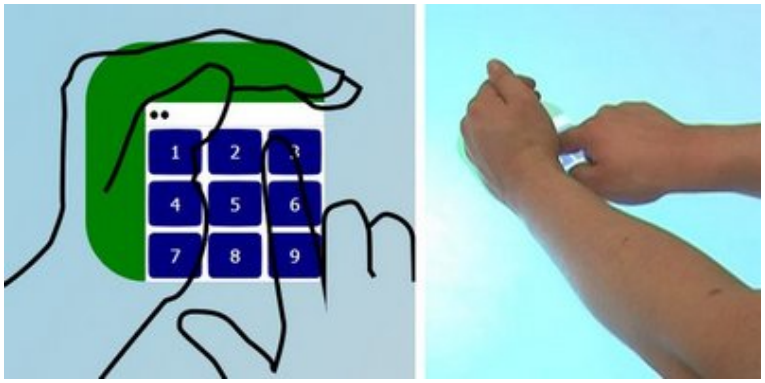

Abbildung 4.4: Links: Während eine Hand gegen Beobachtung abschirmt, wird ein PIN-Pad in den Schild projiziert und von der zweiten Hand bedient. Rechts: Sicht eines nebenstehenden Shouldersurfers

Eine Hand schirmt ab, Nummernblock wird eingeblendet

Diese Authentifizierungsmethode wurde von Kim et al. [2010] speziell für Multitouchtables entwickelt. Der Nutzer bildet auf der Oberfläche des Tisches mit seiner Hand einen Schild, so dass ein kleiner Bereich gegen die Sicht anderer Personen abgeschirmt wird. Innerhalb dieser abgeschirmten Fläche entsteht ein PIN-Eingabefeld, meist eine Tastatur. Über die gibt der Nutzer dann seinen Schlüssel ein.

Singular-Key/Area, Singular-Form, Singular-Position

Auch hier besteht das System aus einer singulären Zeichenkette, diesmal in Kombination mit der Position einer Handform. Daher handelt es sich um eine Verknüpfung zwischen Singular-Key/Area, Singular-Form und Singular-Position.

4.3.5 SlotPIN

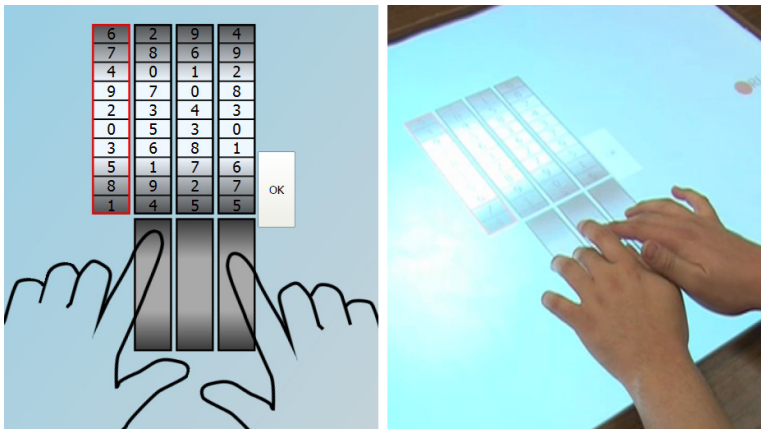

Abbildung 4.5: Links: Eingabe der SlotPIN. Rechts: Sicht eines nebenstehenden Shouldersurfers

Drei Zahlenspalten werden verschoben um vierstellige PIN einzugeben

Diese ebenfalls von Kim et al. [2010] entwickelte Authentifizierungsmethode nutzt eine vierstellige PIN. Eingegeben wird sie über vier Zahlenspalten, die einer Slot-Maschine ähnlich aufgebaut sind. Die erste Zahlenspalte ist festgestellt und kann vom Nutzer nicht verändert werden. Die hinteren drei Zahlenreihen werden vom Nutzer so verschoben, bis seine PIN in der entsprechenden Reihe erscheint.

Singular-Position

Da theoretisch jede Zahlenreihe nacheinander eingegeben werden kann, wird es bei Singular-Position einsortiert.

4.3.6 CuePIN

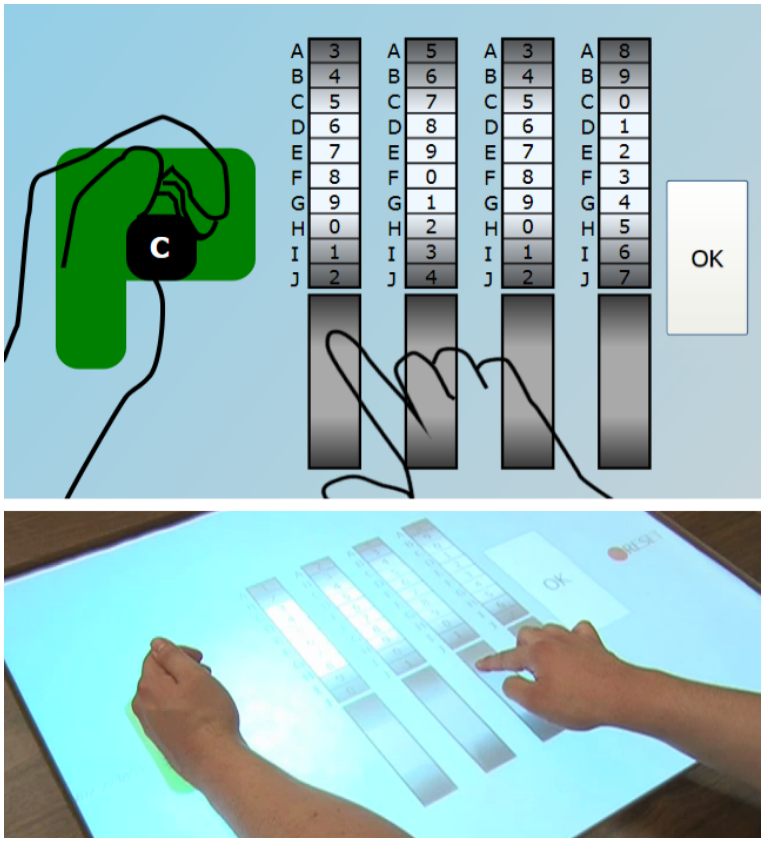

Abbildung 4.6: Oben: Eingabe der CuePIN. Der Hinweis in der Hand links legt die Zeile fest, in der der PIN eingegeben werden muss. Unten: Sicht eines nebenstehenden Shouldersurfers

Kombination von ShieldPIN und SlotPIN

CuePIN ist eine Kombination der zwei ebenfalls von Kim et al. [2010] vorgestellten Verfahren ShieldPIN und SlotPIN. Eine Hand des Benutzers bildet einen Schild, in diesem wird dann ein Buchstabe angezeigt. Zusätzlich werden vier Zahlenspalten angezeigt wie in SlotPIN, nur dass die Zeile durch den Buchstaben festgelegt wird und dass alle vier Zahlenreihen beweglich sind.

Singular-Position, Singular-Form

Wegen der fehlenden Tasteneingabe wird dieses Verfahren, anders als ShieldPIN, bei Singular-Position und Singular-Form einsortiert.

4.3.7 ColorRings

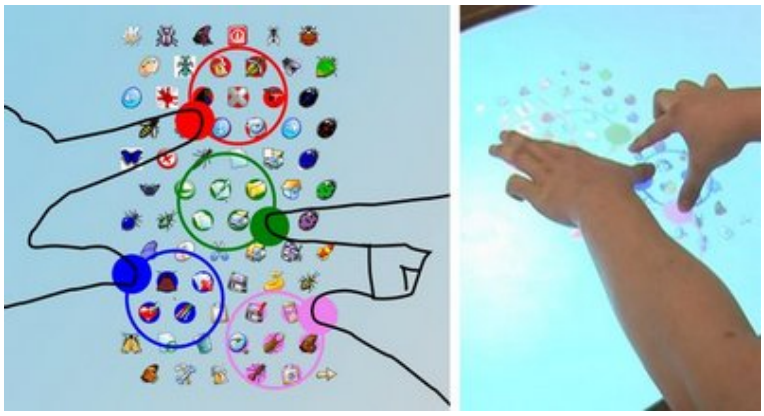

Abbildung 4.7: Links: Icon Gitter und virtuelle Hände, die die Ringe positionieren. Rechts: Hände auf einem Tabletop

Schlüsselicons werden durch farbige Ringe selektiert

Bei diesem ebenfalls von Kim et al. [2010] vorgestellten Authentifizierungsverfahren bildet die Eingabefläche ein großes Gitter mit zahlreichen Icons. Am unteren Bildrand befindet sich eine bestimmte Anzahl farbiger Ringe. Der Nutzer zieht diese Ringe über das Touchpad bis zu festgelegten Icons, die ihm Zugang zum System gewähren. Jeder Ring muss dabei unter anderem ein bestimmtes farblich auf ihn abgestimmte Icon umschließen.

Multiple-Position, Multiple-Orientation

Da nicht nur das Schlüssel-Icon, sondern noch andere von den Farbringen umschlossen werden, erhöht sich die Sicherheit. Falls jemand die Authentifizierung heimlich beobachtet, kann er trotzdem nicht erkennen, welches der umschlossenen Icons das tatsächliche Schlüssel-Icon ist. Dies ist ein System, bei dem mehrere Finger gleichzeitig benutzt werden. Position und Orientierung werden ausgewertet. Daher handelt es sich um eine Verbindung von Multiple-Position und Multiple-Orientation.

4.3.8 PassShape

Eingabe von Strich-PIN

Um Zugang zu seinem System zu bekommen, zieht der Nutzer Linien in einer bestimmten Ausrichtung über den Touchscreen.

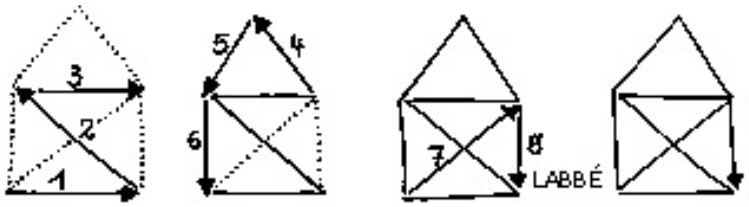

Abbildung 4.8: Die Zusammensetzung einer Zeichnung aus grundlegenden Strichen

Bild leicht zu merken, schwer zu identifizieren

Die Idee hinter diesem von De Luca et al. [2007] vorgestellten Authentifizierungsverfahren ist: Der Nutzer schematisiert in einfachen Strichabfolgen ein Bild wie z.B. einen Stern oder "Das Haus vom Nikolaus". Das zeichnet er immer wieder in der gleichen Reihenfolge nach. Sieht ein heimlicher Beobachter die eingegebene Strichfolge, kann er aber noch nicht das Bild identifizieren.

Singular-Position, Timing, Singular-Key/Area

Mit einem Finger werden verschiedene Linien gezeichnet. Jede Linie muss durchgängig gezogen werden, um die Eingabe korrekt durchzuführen. Die genaue Position der Linien ist hier unwichtig. Daher gehört PassShape zu Singular-Position in Kombination mit Timing und Singular-Key/Area.

4.3.9 "Draw a Secret" und andere grafische Passwörter

Bild als Passwort

Bei dem von Dunphy and Yan [2007] vorgestellten "Draw a secret" und ähnlichen grafischen Passwortsystemen wird mit einem speziellen Stift oder einfach mit dem eigenen Finger auf einem Touchscreen ein Bild gemalt.

Hintergrundbild fördert Komplexität und entlastet Gedächtnis

Auf dem Touchscreen wird oft ein Hintergrundbild vorgegeben, an dem der Nutzer sich orientiert, um den Schlüssel korrekt einzugeben. Dies verhindert zwar, dass bei der Eingabe zu große Abweichungen entstehen. Außenstehende können sich aber an markanten Punkten des Hintergrundbildes orientieren und den Schlüssel so leichter knacken.

Singular-Position

Im Gegensatz zu PassShape ist hier die genaue Position der

Abbildung 4.9: Beispielzeichnung mit Hintergrundbild

Linien wichtig, das Timing kann aber außer Acht gelassen werden. Das System wird bei Singular-Position eingeordnet.

4.3.10 PassGraph

Graph mit wechselndem Druck

Dieses Verfahren von Malek et al. [2006] zeigt dem Nutzer ein Gitter an. Innerhalb dieses Gitters muss ein bestimmter Graph eingegeben werden. An einigen Punkten auf diesem Graphen muss der Druck des Fingers/Eingabestiftes auf den Touchscreen erhöht werden. Ein heimlicher Beobachter kann zwar die Form des Graphen erkennen, nicht aber die Stellen mit erhöhtem Druck.

Gute Sicherheit gegen Shouldersurfing und Brute Force

So ist die Sicherheit gegenüber Shouldersurfattacken sehr hoch. Auch gegen Brute Force bietet diese Methode einen guten Schutz. Die Form des Graphen kann aus einer nahezu unendlichen Menge an möglichen Formen gewählt werden. Außerdem erhöhen Anzahl und Stellen der erhöhten Druckpunkte die Variabilität nochmals.

Singular-Position, Singular-Pressure

Während der Eingabe wird ab und an Druck auf das Touchpad ausgeübt, das Timing ist nicht von Bedeutung. Deshalb muss es bei Singular-Position und Singular-Pressure einge-

ordnet werden.

4.3.11 HandsDown

Biometrische Analyse der Handkontur

Bei diesem Verfahren von Schmidt et al. [2010] für Multitouch-Tische legt der Benutzer seine Hand mit ausgespreizten Fingern auf den Tisch. Anhand der Handsilhouette[2] wird er authentifiziert. Da die Silhouette aufgrund der Biometrie relativ einzigartig ist, sind Brute Force und Shouldersurfattacken nahezu ausgeschlossen.

Singular-Form, Singular-Ausmaß

Beim Einlesen der Handform kommt es auf Singular Form und Singular Ausmaß an.

4.4 Multitouch Techniken

In diesem Abschnitt werden Multitouch Techniken vorgestellt, die sich für Authentifizierungsverfahren eignen könnten.

4.4.1 Pinch, Rotate and Flick

Diese Eingabemöglichkeiten sind als "Gesten" weit verbreitet.

Kneif-/Greifbewegung

Pinch wird eine Zweifinger-Geste genannt, die aus zwei sich nähernden oder entfernenden Touches besteht, bei dem die Finger eine kneifende oder sich öffnende Bewegung machen. Ein Beispiel für die bisherige Verwendung ist Hinein- oder Herauszoomen aus Webseiten, Karten o.ä..

Drehbewegung

Rotate ist ebenfalls eine Zweifinger-Geste. Allerdings bleiben hier die Finger in gleich bleibendem Abstand und die Hand dreht sich um die Vertikalachse. Dabei wird die

[2] Bis jetzt bieten die meisten Multitouchsysteme diese Möglichkeit nicht. Weitere Ausführungen zu den Möglichkeiten von Multitouchsystemen siehe Kapitel 5 Seite 20.

Touchfläche als Horizontale betrachtet. Dies wird z.B. bei Navigationssoftware zum Drehen der Karten verwendet.

Schnippen

Flick ist eine Einfingerbewegung, bei der der Finger in eine Richtung beschleunigt und dann hoch gehoben wird, ohne vorher abzubremsen. Dies wird im Allgemeinen für Bewegungen genutzt, die fortlaufen oder zumindest über den Eingabeplatz hinausreichen.

Singular-Position, Timing bzw. Multiple-Position

Die beiden Eingabegesten "Pinch" und "Rotate" werden von jeweils zwei Fingern benutzt und sind deshalb unter Multiple-Position einzuordnen. Die Geste "Flick" wird bei Singular-Position in Kombination mit Timing eingeordnet.

4.4.2 Micro Rolls

Abbildung 4.10: MicroRoll Gesten und ihre Interpretation

Neigen eines Fingers

MicroRolls sind Gesten, die durch Neigen eines Fingers

durchgeführt werden. In dem Paper haben die Entwickler Lecolinet et al. [2009] dem Daumen sechs Bewegungsausrichtungen zugeordnet: Zum Einen das Aufrichten des Daumens nach oben, unten, links und rechts, sowie eine Kreisbewegung mit und gegen den Uhrzeigersinn. Der Daumen umkreist dabei einen gedachten Spitzkegel.

Singular-Position

Die Eingabe erfolgt über einen einzelnen Finger. Das System fragt dabei die Position ab. Einzuordnen ist es unter Singular-Position.

4.4.3 Multifinger Mouse

Abbildung 4.11: Links: Maus Emulation durch Position (roter Kreis). Rechts: Linksclick durch Positionsfinger und eine Berührung links davon.

Emulation einer Dreitastenmaus

Im Paper von Matejka et al. [2009] stellen die Autoren Techniken zur Emulation einer Drei-Tasten-Maus in einer Multitouch-Umgebung vor. Dabei wird z.B. einem Finger die Cursorfunktion der Maus zugeordnet. Die anderen Finger übernehmen die Funktionen von mittlerer, rechter und linker Maustaste.

Wenn z.B. der Zeigefinger die Position der Maus vor-

gibt, wäre ein Tap mit dem Daumen, also links vom Positionstouch, bei einer relationalen Position gleichbedeutend mit einem Linksklick. Ein Tap mit dem Mittelfinger sehr nah rechts vom Positionstouch, ein Drücken der mittleren Maustaste. Und ein Tap mit dem kleinen Finger rechts vom Positionstouch mit größerem Abstand wäre ein Rechtsklick.

Multiple-Position

Die Eingabe erfolgt über mehrere Finger. Das System fragt wie bei MicroRolls die Position ab. Es wird daher unter Multiple-Position eingeordnet.

Kapitel 5

Designansätze für Multitouch-Authentifizierung

Drei Ansätze: HandScan, TipSlide und FreeSwipe

Mit den im Rahmen dieser Arbeit entwickelten Prototypen soll versucht werden, Multitouch-Authentifizierungs-Mechanismen zu entwickeln, die sowohl die Parameter Ausmaß als auch multiple Position stärker berücksichtigen. Es wurden drei neue Authentifizierungsverfahren entwickelt. Im folgenden Abschnitt werden diese genauer erläutert. Sie sind aus der in Kapitel 4 beschriebenen Taxonomie entstanden. Der Nutzer soll sich beim ersten Authentifizierungssystem mittels seines Handabdrucks legitimieren. Beim zweiten erfolgt der Zugang zum System über das Abrollen seiner Finger. Das dritte Authentifizierungssystem benötigt zum Einloggen eine selbst gewählte Geste. Abbildung 5.1 zeigt die Einordnung der drei im Rahmen dieser Arbeit entwickelten Authentifizierungsverfahren in die in Kapitel 4 erstellte Taxonomie. Es wird deutlich, dass die Parameter Ausmaß und multiple Position nun besser abgedeckt sind.

Ausmaß und Multiple-Position besser abgedeckt

Taxonomie der Multitouch-Authentifizierung	Singular	Multiple	Timing	Areal/Taste	Position	Ausmaß	Form	Orientierung	Druck
Passwort	●			●					
Keystroke	●		○	●					
TapSongs	●		○	●					
ShieldPIN	●			●	●		●		
SlotPIN	●				●				
CuePIN	●				●				
	●						●		
ColorRings		●			●			●	
PassShape	●		●	●	●				
Draw a Secret	●				●				
PassGraph	●				●				●
HandsDown	●					●	●		
HandScan		●			○	○			
TipSlide		●	○		○				
FreeSwipe		●	○		○	○		○	
Pinch		●			●				
Rotate		●			●				
Flick	●			●	●				
MicroRolls	●				●				
Multifinger Mouse		●			●				

Abbildung 5.1: Taxonomie der Mulitouch-Authentifizierung mit HandScan, TipSlide und FreeSwipe. Leere Kreise bedeuten dieser Parameter wird biometrisch analysiert

5.1 Iteratives Design

Mehrere Iterationen bei der Entwicklung

Iteratives Design ist ein Vorgehensmodell nach Nielsen [1993], bei dem wiederholend über mehrere Versionen entwickelt wird. Bei jeder Iteration wird ein Benutzertest durchgeführt. Hierbei werden jeweils die Bedürfnisse des Benutzers und die Benutzerfreundlichkeit überprüft und das System entsprechend angepasst.

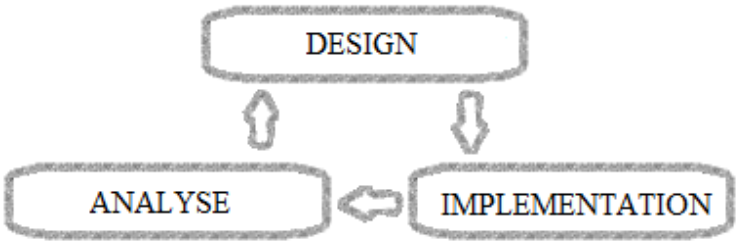

Abbildung 5.2: Schematische Darstellung des DIA Kreises

Design, Implementierung, Analyse

Bei der Entwicklung neuer Möglichkeiten der Authentifizierung wurde dem DIA-Kreis folgend vorgegangen. Gemäß des iterativen Designs wird nach einer ersten Design-Phase ein Prototyp entwickelt und getestet. Dieser Test wird analysiert und eventuelle Probleme werden in ein neues Design eingearbeitet. Darauf basierend erfolgen Entwicklung und Test des Prototypen.

5.2 Messgrößen

Benutzerfreundlichkeit:

Nach Shneiderman et al. [2009] sollen für ein benutzerfreundliches System folgende Punkte evaluiert werden:

- Wie lange dauert es für einen typischen Benutzer, die für ein Aufgabenset relevanten Aktionen zu erlernen?

  Zeitaufwand zum Erlernen

- Wie lange dauert es, eine Benchmark-Aufgabe zu erledigen?

  Eingabegeschwindigkeit

Fehlerrate durch den Benutzer

- Wie viele Fehler machen Benutzer bei der Lösung der Benchmark-Aufgabe? Wie lassen sich diese Fehler klassifizieren?

Erinnerung über Zeit

- Wie gut erinnern die Benutzer das Wissen nach einer Stunde, einem Tag oder einer Woche?

Subjektive Zufriedenheit

- Wie sehr mochten die Benutzer die unterschiedlichen Aspekte des Systems?

Sicherheit:

Um die Sicherheit der Systeme zu testen, müssen weitere Messgrößen geprüft werden:

Korrekte Erkennung

- Wie viele Authentifizierungsversuche wurden korrekt erkannt?

Erfolgreiche Shouldersurfattacken

- Wie viele Authentifizierungsversuche einer anderen Person, die die Authentifizierung gesehen hat, sind erfolgreich?

Verarbeitungsgeschwindigkeit

- Wie lange braucht das System nach einer Eingabe, um den Benutzer zu authentifizieren?

5.3 Erstes Authentifizierungssystem: HandScan

Authentifizierung über Handabdruck

Das erste Authentifizierungsverfahren soll über den Handabdruck erfolgen. Es basiert auf dem in Schmidt et al. [2010] vorgestellten System HandsDown[1] und versucht dies für eine breitere Masse an Multitouchsystemen zu verwirklichen.

Biometrische Analyse der Touches der flachen Hand

Der Idee nach soll das System die durch das Auflegen der flachen Hand entstehenden Touches als charakteristisch für einen Benutzer identifizieren. Das Touchpad soll den Handabdruck also biometrisch erfassen und analysieren.

Keine Handkontur, benötigt nur kleinere Eingabefläche

Unterschiede zu HandsDown sind, dass die Handkontur

[1] siehe Kapitel 4.3.11

nicht eingelesen wird, sondern nur die resultierenden Touches. So kann es auf einem wesentlich kleineren Element, wie einem Smartphone oder dem Touchpad eines Laptops, realisiert werden.

Das System muss erkennen, ob der Handabdruck zu einem vorher eingegebenen Benutzernamen gehört oder nicht. In der Taxonomie gehört dieses Authentifizierungsverfahren zu Multiple-Position und Ausmaß.

Multiple-Position, Ausmaß

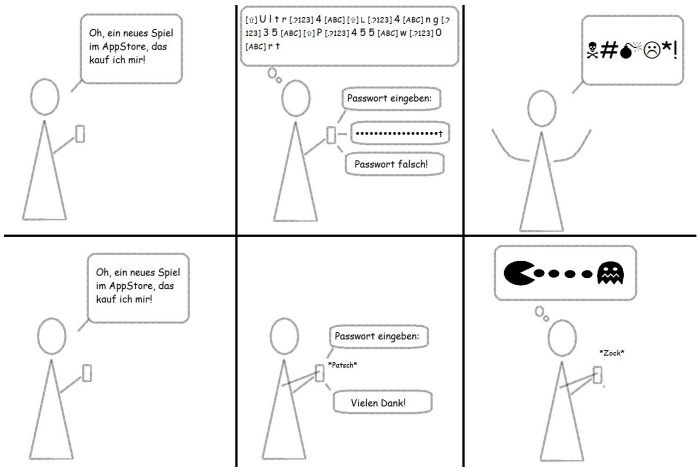

Abbildung 5.3: Oben: Ein Benutzer soll sich auf dem iPhone per Passwort anmelden. Unten: Ein Benutzer meldet sich mit HandScan an.

5.4 Zweites Authentifizierungssystem: TipSlide

Hier soll sich der Nutzer durch Abrollen der Finger auf dem Touchpad identifizieren. Da der Mittelfinger jeder Person unterschiedlich lang ist, entstehen beim Abrollen charakteristische Bewegungsabläufe.

Abrollen über die Fingerspitzen

Der Nutzer soll seine Fingerspitzen in gerader Linie auf das Touchpad aufsetzen und sie dann über den Mittelfinger abrollen und dabei die Hand strecken. Diese Idee basiert auf

MicroRolls mit der ganzen Hand

MicroRolls[2] aus Lecolinet et al. [2009].

Multiple-Position, Timing

Konkret soll das System versuchen, verschiedene Nutzer anhand der zeitlichen Bewegungsabläufe zu unterscheiden. Es muss dann abgleichen, ob das Muster der Touches zu einem vorher eingegebenen Benutzernamen passt oder nicht. In der Taxonomie gehört TipSlide zu Multiple Position in Kombination mit Timing.

5.5 Drittes Authentifizierungssystem: FreeSwipe

Freie Geste

Hier soll ein auf freien Mehrfingergesten basiertes Authentifizierungsverfahren realisiert werden. Der Benutzer muss, um sich zu authentifizieren, eine selbst gewählte Geste auf einem Multitouchsystem eingeben.

"Draw a Secret" mit mehreren Fingern

Die Geste ist vollkommen frei wählbar. Grundlegende Idee hierzu kam von "Draw a Secret" aus Dunphy and Yan [2007].

Multiple-Position, Orientierung, Ausmaß, Timing

Nach Möglichkeit sollte die Geste mit mehreren Fingern gleichzeitig eingegeben werden. Das System vergleicht dann Multiple Position, Orientierung, Ausmaß und Timing mit den gespeicherten Informationen des zugehörigen Benutzernamens.

[2] siehe Kapitel 4.4.2

5.6 Erste Studie an einem Papierprototypen

Papierprototyp mit Fingerfarbe auf Klarsichtfolie

Nach der Ausarbeitung dieser drei Ideen wurde ein Papierprototyp entwickelt. Daran wurden alle drei Authentifizierungsverfahren einem ersten Test unterzogen. Das Touchpad wurde durch ein Stück Klarsichtfolie in Größe des Touchpads simuliert. Die Touches sollten durch Fingerfarbe darauf gekennzeichnet werden. Den Testpersonen wurde die Handfläche mit Fingerfarbe bestrichen, womit sie die oben beschriebenen Bewegungsabläufe, HandScan, TipsSlide und FreeSwipe auf die Klarsichtfolie übertrugen. Die einzelnen Klarsichtfolien wurden dann durch Übereinander legen miteinander verglichen.

Testlauf:

Ein Testdurchlauf bestand aus sieben Phasen:

HandScan

- Simulation des HandScan durch Auflegen der flachen und mit Fingerfarbe bestrichenen Hand auf die Klarsichtfolie.

TipSlide

- Simulation des TipSlide durch Abrollen der mit Fingerfarbe bestrichenen Fingerspitzen über den Mittelfinger auf die Klarsichtfolie.

FreeSwipe

- Simulation des FreeSwipe durch Übertragung eines frei gewählten Musters mittels Fingerfarbe auf die Klarsichtfolie.

Nachmachen durch zusehen

- Simulation einer Shouldersurfattacke durch Nachahmung einer durch den Versuchsleiter vorgegebenen Geste.

Nachmachen nach Video

- Simulation einer wiederholten Shoulder-Surfing-Attacke durch Nachahmung derselben Geste, nachdem ein entsprechendes Video beliebig oft angesehen werden konnte.

Zuordnung der Folien

- Hier wurden alle bisher erstellten Klarsichtfolien vermischt. Die Testpersonen sollten dann alle Klarsichtfolien einer Testperson und Phase zueinander sortieren.

  Pro Person und Phase entstanden je drei Sets aus jeweils fünf Klarsichtfolien. Im Idealfall sollten von den

Testpersonen dann auch wieder Sets aus je fünf Folien sortiert werden.

Fragebogen

- Ausfüllen eines Fragebogens[3] über den Versuch.

Ein Testdurchlauf dauerte ungefähr 30 Minuten. Die Testpersonen mussten der Teilnahme an dem Versuch durch eine Einverständniserklärung[4] zustimmen.

Elf Personen

Der Papierprototyp wurde von elf Testpersonen im Alter von 24 bis 62 getestet. Das Durchschnittsalter betrug 34,8 Jahre.

5.6.1 Auswertung Versuch und Fragebogen

Fünf Antwortmöglichkeiten

Über den Fragebogen sollten verschiedene Aspekte herausgefunden werden. Geantwortet wurde durch Ankreuzen der Felder "Starke Zustimmung", "Zustimmung", "Neutral", "Ablehnung" und "starke Ablehnung". Pro Authentifizierungsverfahren gab es einen sich wiederholenden Fragenblock:

- Wurde der Versuchsablauf verstanden?
- Fielen die für die drei Authentifizierungsverfahren auszuführenden Bewegungen leicht?
- Sind die Verfahren zur Authentifizierung geeignet?
- Sind sie sogar geeignet, um sie an einem eigenen Gerät zu benutzen?
- Sind die Verfahren einfacher als die momentan geläufige Passworteingabe?

Zu der Simulation der Shoulder-Surfing-Attacken sollten die Versuchspersonen angeben, ob Ihnen das Erkennen der Geste leicht fiel.

[3] siehe Anhang A
[4] siehe Anhang A

5.6.2 HandScan

Abbildung 5.4: Vier Handabdrücke mit Fingerfarbe auf Klarsichtfolie. Links oben und links unten von der selben Person, rechts oben und rechts unten von zwei weiteren Personen

Leichte Ausführung, schneller als PW/PIN

Sich über den Handabdruck zu authentifizieren fiel acht von elf Testpersonen leicht. Ebenfalls wurde dieses Authentifizierungsverfahren von den Testpersonen als “schneller als eine Passwort- oder PIN-Eingabe” eingeschätzt.

75% Erfolgsrate

Insgesamt sortierten die Versuchspersonen 75% der Sets fehlerfrei. 67% der von Testpersonen sortierten Sets enthielten mehr als zwei Folien. Die Wahrscheinlichkeit, dass eine Testperson nur zufällig zueinander gehörende Sets bildet, liegt aufgrund der Menge der Testfolien bei unter einem Prozent. Das Erkennen der zueinander gehörenden Sets ist also möglich. Auch wurde der HandScan grundsätzlich positiv bewertet. Daher war eine Umsetzung dieses Authentifizierungsverfahrens als Software sinnvoll.

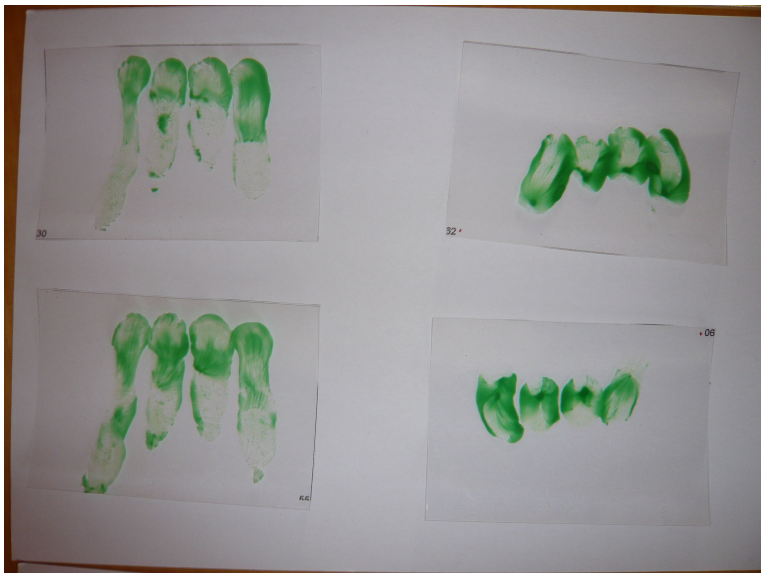

Abbildung 5.5: Vier vorgegebene Bewegungen mit Fingerfarbe auf Klarsichtfolie. Links oben und links unten von der selben Person, rechts oben und rechts unten von zwei weiteren Personen

5.6.3 TipSlide

Weniger positiv als HandScan, Bewegung umständlich

Das Authentifizierungsverfahren TipSlide wurde weniger positiv aufgenommen als HandScan. Viele Testpersonen konnten die notwendige Abrollbewegung der Finger nach dem Durchlesen der Instruktionen nicht sofort umsetzen. Der Versuchsleiter musste sie zeigen und erst durch Nachahmung wurde die Bewegung verstanden. Dennoch beschwerten sich während des Versuchs viele Testpersonen, dass die Bewegung zu umständlich, schwierig oder unbequem sei. Auch auf dem Fragebogen tauchten solche Beschwerden auf, wenn auch oft mit einem Hinweis, dass die Umstände aber in Kauf genommen würden.

83% Erfolgsrate, Anpassung der Bewegung

Das Sortieren der zueinander gehörenden Sets war ähnlich gut wie bei HandScan. 83% der Gruppen wurden fehlerfrei sortiert, 73% der Sets enthielten mehr als zwei Bilder. Dieses Ergebnis macht eine Umsetzung des Verfahrens als Software sinnvoll. Aufgrund der oben beschriebenen Beschwerden wurde die Bewegung für den Softwareprototy-

pen aber überarbeitet. Um das Abrollen der Finger zu erleichtern dürfen die Fingerspitzen während des Abrollens nach vorne geschoben werden.

5.6.4 FreeSwipe

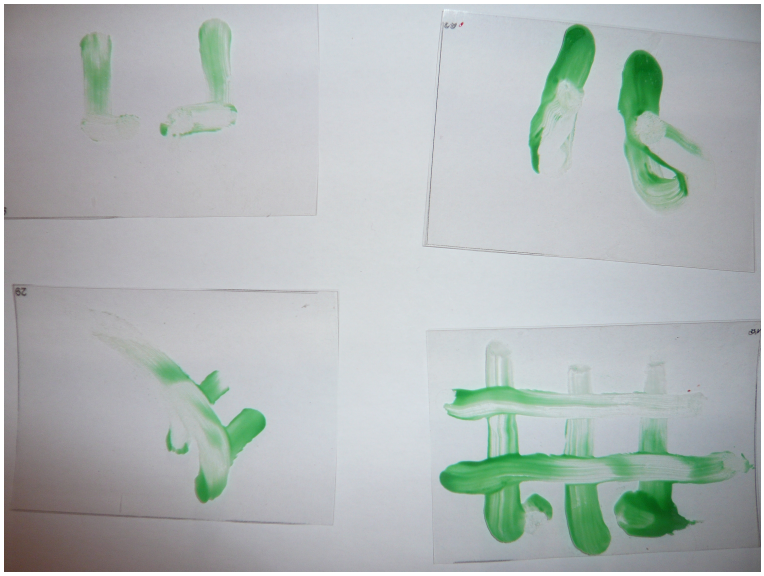

Abbildung 5.6: Vier frei gewählte Bewegungen mit Fingerfarben auf Klarsichtfolie. Jeweils unterschiedliche Personen

Ausschließlich positiv bewertet, 80% gefiel dies am besten

FreeSwipe wurde von den Testpersonen ausschließlich positiv bewertet. Da die Geste frei gewählt werden konnte, war nicht mit Schwierigkeiten bei der Ausführung zu rechnen. Keine Testperson schloss aus, ein solches Authentifizierungsverfahren am eigenen Computer oder Smartphone zu verwenden. 80% der Probanden gefiel diese Version am besten.

90% Erfolgsrate

Insgesamt 90% der Folien konnten von den Testpersonen wieder richtig sortiert werden. 86% der Sets enthielten zwei oder mehr Folien, 82% sogar drei oder mehr.

Vielversprechendster Ansatz

Damit scheint FreeSwipe bisher das am meisten versprechende Authentifizierungsverfahren der drei im Rahmen dieser Arbeit entwickelten zu sein. Es schneidet nach dem ersten Testlauf sowohl bei der Benutzerfreundlichkeit als

auch bei der Sicherheit am besten ab. Auch hier folgt im nächsten Schritt die Umsetzung des Verfahrens als Softwareprototyp und ein entsprechender Testlauf.

5.6.5 Hacking

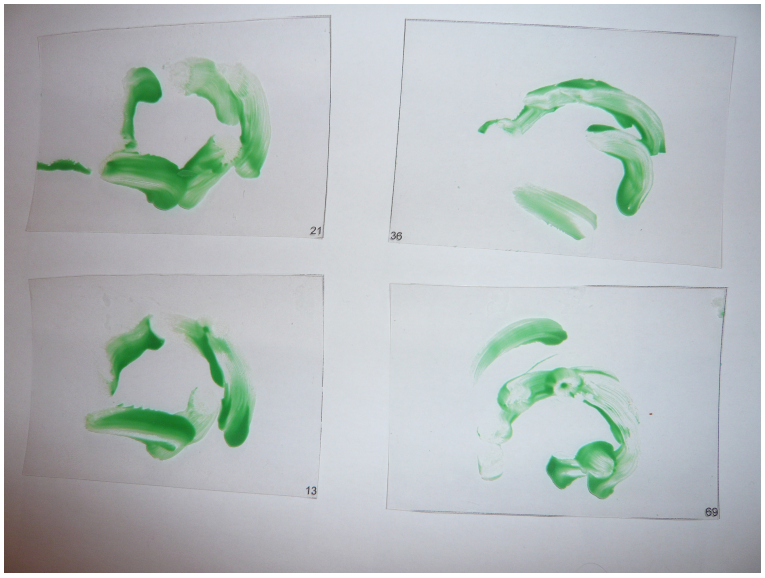

Abbildung 5.7: Links: Zwei Zeichnungen der Originalbewegung vom Versuchsleiter. Rechts: Zwei Zeichnungen Bewegung von Testpersonen, die versuchten die Bewegung nachzumachen

Simulation von Shouldersurfing durch vormachen und nachmachen

Um eine Shouldersurfattacke zu simulieren, sollten die Versuchspersonen eine vom Versuchsleiter vorgegebene Geste kopieren. Zunächst nach einmaliger Beobachtung, dann nachdem ein entsprechendes Video beliebig oft angesehen werden konnte. So sollte herausgefunden werden, ob das Authentifizierungsverfahren auch nach mehreren Shouldersurfattacken noch Sicherheit bietet.

Geste: Kreis mit Strich

Die vom Versuchsleiter vorgegebene Geste war ein mit allen Fingerspitzen gleichzeitig auf dem Touchpad gezogener enger Kreis, dem zum Schluss ein mit dem Daumen gezogener waagerechter Strich hinzugefügt wurde.

Nachahmungen klar erkennbar

Die Versuchspersonen gaben an, dass die Nachahmung ih-

nen nach der ersten Vorführung möglich, aber schwierig erschien. Dies spiegelt sich auch in den Ergebnissen auf Klarsichtfolie wieder. Beim Versuch Sets zu bilden, scheiterten alle Versuchspersonen. Kein Nachahmungsversuch wurde mit dem Original in eine Gruppe sortiert.

Nachahmung nach Video auch klar erkennbar

Auch nachdem das Video mehrmals geschaut wurde, entstand keine einzige Fälschung, die beim Sortieren in ein Set mit der Originalvorlage gemischt wurde. Die Versuchspersonen gaben zwar an, die Bewegung gut erkannt zu haben und konnten sie vom Prinzip her auch richtig ausführen. Eine korrekte Kopie auf der Klarsichtfolie entstand aber nicht.

100% Sicherheit gegen Shouldersurfing bei entsprechender Geste

Dies entspricht einer Sicherheit von 100% gegen Shouldersurfattacken. Die Sicherheit hängt allerdings auch von der gewählten Geste ab. Wie bei Dunphy and Yan [2007] angeführt, hat auch "Draw a Secret" einen Unsicherheitsfaktor durch zu einfach gewählte Benutzergesten.

Vorgegeben Geste nur mittelmäßig kompliziert

Wenn man die Anzahlen der einzelnen Elemente, wie Strich, Kreis oder Kurve, und die Anzahl der benutzen Finger vergleicht, war die vom Versuchsleiter gewählte Geste im Vergleich zu den anderen 72 Gesten der Benutzer der zwei Studien[5] nur mittelmäßig kompliziert.

Die vorgegebene Geste bestand aus zwei Elementen und nutzte alle fünf Finger. Nur sehr wenige Gesten bestanden nur aus einem Element, manche sogar aus vier oder fünf. Nur sehr wenige Benutzer nutzten dafür alle fünf Finger, die meisten nutzten nur zwei oder drei.

Geringe Gestenkomplexität möglicherweise Problem

Es gab nur sehr wenige Benutzer, die wenige Elemente mit wenigen Fingern ausführten. Dies müsste vom System eventuell genauer überprüft werden, so dass bei zu geringer Komplexität der Geste das Passwort von vorne herein abgelehnt wird. Bei Passwortsystemen werden heutzutage ebenfalls Passwörter mit zu geringer Komplexität zum Schutz des Benutzers abgelehnt.

[5] zweite Studie siehe Kapitel 6.5

5.7 Erinnerung

Erinnerung gut möglich

Nach zwei Wochen wurden fünf der elf Versuchspersonen nach den Gesten zu den drei Ansätzen befragt. Alle fünf konnten sich an sämtliche Gesten erinnern, sogar an die Vorgabe bei der simulierten Shouldersurfattacke.

Kapitel 6

Implementierung

Alle drei Ansätze weiterentwickelt

Wie bereits beschrieben, sind bei allen drei Authentifizierungsmethoden eine genauere Betrachtung als Softwareversion und weitere Tests vielversprechend.

Vorraussetzungen: Multitouchsystem mit erforderlichen Parametern, Verifikation in Echtzeit, maschinelles Lernen, Benutzerstudie

Für die Implementierung von Softwareprototypen mussten noch weitere Vorraussetzungen erfüllt werden. Es sollte ein bereits auf dem Markt erhältliches Multitouchsystem gefunden werden, das die erforderlichen Daten liefert. Es war ebenfalls zu testen, ob das System nach einer längeren Lernphase in der Lage ist, die Testdaten in Echtzeit zu verifizieren. Die Suche nach einem entsprechendem Multitouchsystem, das Entwickeln eines entsprechenden Programms zur Datensammlung und eines maschinellen Lernalgorithmuses zur Datenanalyse werden in dem folgenden Kapitel dargelegt. Anschließend folgen die Beschreibung und Analyse der Benutzerstudie.

6.1 Multitouch System

Multitouch zunehmend verbreitet, für Entwickler oft nur Koordinate

Zunächst musste ein Multitouchsystem gefunden werden, welches alle Ansprüche der drei im Rahmen dieser Arbeit entwickelten Authentifizierungsverfahren erfüllen kann. Es sind viele verschiedene Multitouchsysteme frei auf dem Markt erhältlich. Die meisten werten die Touches allerdings nur intern aus. Sie liefern dem Benutzer oder System le-

diglich die fertige Verarbeitung der Eingabe, beispielsweise in Gestalt eines Mauszeigers an der jeweiligen Position. Nur wenige Multitouchsysteme bieten Entwicklern die Möglichkeit intern auf Fingerpositionen oder andere Eigenschaften wie Ausmaß, Ausrichtung, Form oder ähnliche zuzugreifen.

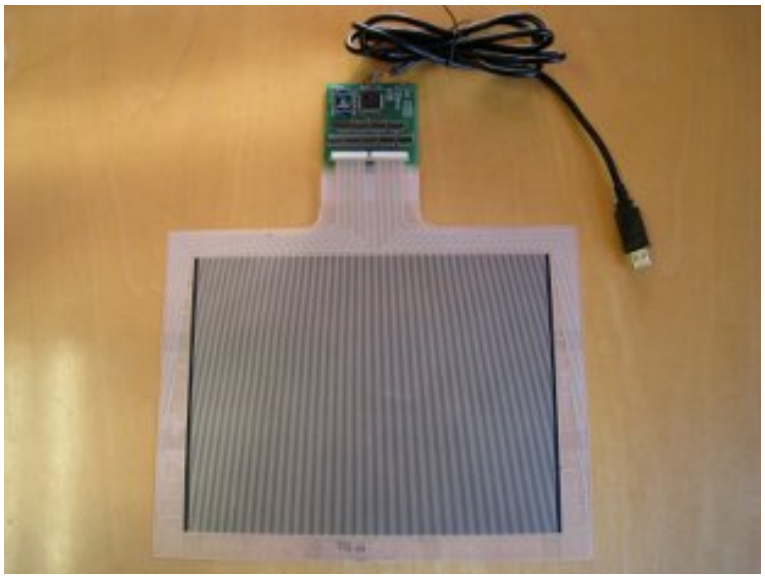

Abbildung 6.1: Multitouchpad der Firma TouchCo

TouchCo Touchpad mit Druck, aber zu geringer Auflösung

Der erste Versuch der Umsetzung als Software mit einem Multitouchpad[1] der Firma TouchCo[2] scheiterte, da die Auflösung zu gering war. Das System konnte eine kleine Veränderungen der Position des Fingers auf dem Touchpad nicht als Veränderung des Touches erkennen. Eine Authentifizierung über die hier entwickelten Methoden schien daher nicht Erfolg versprechend und eine Implementierung auf diesem System wurde verworfen. Dieses System hätte den Vorteil gehabt, dass es neben den benötigten Parametern auch Druckinformationen geliefert hätte und beliebig viele Touches verarbeiten kann.

MacBookPro liefert die benötigten Parameter

Mittels einer undokumentierten Schnittstelle ist es möglich,

[1] `http://news.softpedia.com/news/I-F-S-R-Multitouch-Allows-for-Unlimited-Touch-Inputs-130953.shtml` Stand: 02.08.2011

[2] Betrieb eingestellt im Jan. 2010, siehe `http://www.touchco.com/` Stand: 02.08.2011

Abbildung 6.2: Multitouchpad des MacBookPro von Apple

auf die Daten des Multitouchpads des MacBookPro zuzugreifen. Nach ersten Versuchen mit diesem Modell erschienen die Auflösung und Schnittstelle vielversprechend. Mittels einer wesentlich höheren Auflösung konnten auch kleinste Veränderungen der Fingerposition korrekt vom System erkannt und verarbeitet werden. Die Schnittstelle bot alle der in Kapitel 4 vorgestellten Parameter außer Druck und Form. Diese werden allerdings für die hier vorgestellten Verfahren nicht benötigt. Das Touchpad liefert die Daten mit einer Aktualisierungsrate von 125Hz.

6.2 Objective C Multitouch Framework

Privates Multitouch Framework von Apple

Die Implementierung der Softwareprototypen erfolgte in Objective C. Es wurde ein privates Multitouch Framework von Apple verwendet[3]. Der enthaltene Listener feuert einen Event, sobald mindestens ein Touch registriert wird. Das Framework stellt dann dem Programmierer ein Array zur Verfügung. Darin können ein bis elf Touches enthalten sein. Sollten mehr als elf Touches registriert werden, enthält das Array scheinbar eine zufällige Auswahl dieser. Da im hier angestrebten Versuch mit hoher Wahrscheinlichkeit nie mehr als zehn Touches genutzt werden würden,

[3] Mac OS X 10.6.8

konnte dieses Problem außer Acht gelassen werden.

Frameworkeigenschaften

Das verwendete Framework stellt dem Entwickler für jeden Touch folgende Eigenschaften zur Verfügung:

- Zeitpunkt
- Geschwindigkeit (in X und Y-Achsen Richtung)
- Größe (in Hauptachse und Nebenachse)
- Koordinate (in X und Y-Achsen Richtung)
- Winkel (des Fingers, sowie der Haupt- und Nebenachse)
- Identifier
- Frame
- Status

Dabei bildet der Identifier eine Zahl. Jedem Finger wird während der Eingabe eines Touches eine solche Zahl zugeordnet. Während einer Bewegung auf dem Touchpad bleibt diese Zuordnung bestehen.

Der Status gibt an, ob der Finger gerade aufgesetzt, abgesetzt oder bewegt wurde.

Gespeichert in CoreData

Gespeichert werden die gesammelten Daten in der Objective C eigenen Datenverwaltungslösung CoreData. Bei einer zeitnahen Speicherung hat dies allerdings Performanceeinbußen zur Folge. Um dies zu umgehen, werden die Daten zuerst im Arbeitsspeicher zwischengelagert. Nachdem eine Testperson alle Touches eingegeben hat, werden sie gesammelt gespeichert.

6.3 Maschinelles Lernen

Maschinelles Lernen zur automatischen Mustererkennung

Die Auswertung der Daten sollte über maschinelles Lernen erfolgen. Mittels maschinellen Lernens versucht der

Computer, innerhalb eines Lernprozesses eingegebene Daten nach einem oder mehreren Mustern einzuordnen. Dieser Lernprozess kann uninformiert oder informiert sein.

Uninformiertes Lernen

Beim uninformierten Lernen werden die Daten dem Computer ohne weitere Informationen zur Verfügung gestellt. Er sucht nach Gemeinsamkeiten und fasst diese in Gruppen zusammen.

Informiertes Lernen

Beim informierten Lernen werden in den Computer Daten bereits mit vorgegebenen Klassifikationen eingespeist. Dem Computer wird schon während der Lernphase gesagt, welche Daten in eine Gruppe gehören. Mit diesen Informationen kann der Computer den Daten dann Gruppen zuordnen.

Dieser Untersuchung wurde das informierte Lernen zu Grunde gelegt, da die Benutzernamen und die zugehörigen Eingaben eindeutig bekannt sind.

Algorithmus: Künstliches neuronales Netz

Im vorliegenden Fall wurde das maschinelle Lernen über ein neuronales Netz realisiert. Dieses ist zwar komplizierter zu implementieren und zu bedienen als andere Ansätze maschinellen Lernens, bietet aber Lösungsansätze für große Bandbreiten von eventuell auftretenden Problemen. Die Eingabeparameter werden in sogenannten Neuronen abhängig von ihrer Gewichtung kombiniert. Tauchen Fehler auf, wird die Gewichtung der Kombinationen entsprechend verändert[4].

Lernphase problematisch bezüglich Benutzerfreundlichkeit

Die Dauer der Lernphase des neuronalen Netzwerks kann problematisch werden. Im Sinne der Benutzerfreundlichkeit ist es nicht zumutbar, wenn der Benutzer seinem System die Authentifizierung zu oft beibringen muss. Beispielsweise wurde von mehreren Testpersonen der Studien gesagt, dass sie nicht bereit wären, mehr als zehnmal die selbe Bewegung einzugeben. Eine einfache Passworteingabe lernen gängige Systeme schon nach einem einmaligen Vorgang.

Training zeitintensiv

Während des Trainings muss das System erst die Gewichtung der Eingabeparameter anpassen. Dies kann bezüglich

[4] siehe Han [2005] Seite 398ff.

der Benutzerfreundlichkeit gegebenenfalls zu viel Zeit in Anspruch nehmen. Sollte ein solches Authentifizierungsverfahren auf einem Smartphone implementiert werden, kann es zu weiteren Problemen kommen, weil nur eine sehr eingeschränkte Rechen- und Speicherkapazität zur Verfügung steht.

Die Implementierung erfolgte über ein neuronales Netzwerk in Objective C von Matt Brewer[5]. Als problematisch erwies sich die Beschränkung des vorliegenden neuronalen Netzwerks auf maximal drei Eingabedimensionen. Daher wurde es auf beliebig viele Eingabedimensionen erweitert. Dazu musste das die Eingabe enthaltene Array von einer festen Größe auf eine variable Größe umgestellt werden. Außerdem wurde die Beschränkung aufgehoben. Eventuell fehlende Werte wurden mit einem Standardwert, hier 0, aufgefüllt.

6.4 Datenreduktion

Datenreduktion wichtig

Bei der Authentifizierung des Softwareprototypen wird eine sehr große Datenmenge gesammelt. Jeder Touch hat 13 Parameter, jedes Touchset hat bis zu 10 Touches. Bei 125Hz ergibt das bis zu 16.250 Daten pro Sekunde. Unbearbeitet sind diese kaum zu bewältigen. Unwichtige Dimensionen können bei neuronalen Netzen das Finden eines Musters stark stören. Durch die Kombination der Eingabeparameter mit allen anderen Eingabeparametern wächst zudem die Komplexität auch mit dem Quadrat der Dimensionen.

Realisiert über SQL-Skripte

Daher musste die Datenmenge zunächst reduziert werden. Dazu wurden die in der Taxonomie herausgearbeiteten Parameter der drei Prototypen aus der Datenmenge gefiltert. Hierzu werden die Daten in eine Oracle Express Edition Datenbank eingespielt und über SQL-Skripte die unwichtigen Daten herausgefiltert. Anschließend wird die Anzahl der Touchsets pro Eingabe ebenfalls über SQL-Skripte re-

[5] Bei beiden Stand: 02.08.2011 `http://www.macfanatic.net/blog/2008/12/01/back-propagation-neural-network/` Download: `http://www.macfanatic.net/downloads/bio_series/neural-net-source.dmg`

duziert.

HandScan

Die Parameter Position und Ausmaß sind hier wichtig. Pro Touch wurden daher die x- und y-Koordinate auf dem Touchpad sowie die Touchhöhe und Touchbreite betrachtet. Touchsets mit mehr als 10 Touches wurden aussortiert. Pro Touchset wurden 10 Touches gewählt. Die Touchsets wurden ebenfalls gleichmäßig ausgedünnt, indem nur jedes zehnte Touchset betrachtet wurde. Außerdem wurde eine Eingabe auf insgesamt 25 Touchsets limitiert.

TipSlide

Hier kommt es auf die Parameter Multiple Position in Kombination mit Timing an. Pro Touch wurde die x- und y-Koordinate festgelegt, sowie der Zeitpunkt jedes Touchsets berücksichtigt. Touchsets mit mehr als 10 Touches wurden aussortiert. Pro Touchset wurden 10 Touches gewählt und diese auf insgesamt 40 Touchsets pro Eingabe limitiert. Die Touchsets wurden ebenfalls gleichmäßig ausgedünnt, indem nur jedes zehnte Touchset betrachtet wurde.

FreeSwipe

Die entscheidenden Parameter für dieses Verfahren sind Multiple Position, Ausmaß und Timing. Daher wurde zur Datenreduzierung die x- und y-Koordinate, die Touchhöhe und Touchbreite und der Winkel des Touches betrachtet. Ebenfalls wurde der Zeitstempel des Touches ausgewertet. Die Touchsets wurden auf fünf Touches reduziert und auf 40 ausgedünnt. So wurde verhindert, dass die Anzahl der Eingabedimensionen weit über 1000 lagen.

Ergebnis: 1000 dimensionale Eingabe

Die unterschiedlichen Reduktionen auf 25 bzw. 40 Touchsets sind sinnvoll, da die Eingaben der Gesten FreeSwipe und TipSlide durchschnittlich länger dauern als bei HandScan. Daher entstehen pro Eingabe auch mehr Touchsets. Der Reduktionsfaktor bleibt trotzdem gleich. So wurde für alle drei Authentifizierungsverfahren eine circa 1000-dimensionale Eingabe bei einer eindimensionalen Ausgabe, dem Benutzer, erreicht.

6.5 Zweite Studie an einem Softwareprototypen

Benutzerstudie sammelt Authentifizierungsdaten zur Analyse

Für das Programm zur Datensammlung wurde um das Multitouch Framework eine einfache Benutzeroberfläche programmiert. Nach Eingabe einer zugewiesenen Benutzer-ID sollte jede Testperson die drei Authentifizierungsmethoden HandScan, TipSlide und FreeSwipe am Softwareprototypen ausprobieren. Jede Geste sollte zehn Mal wiederholt werden, um dem Lernalgorithmus später genug Daten zur Auswertung zur Verfügung zu stellen.

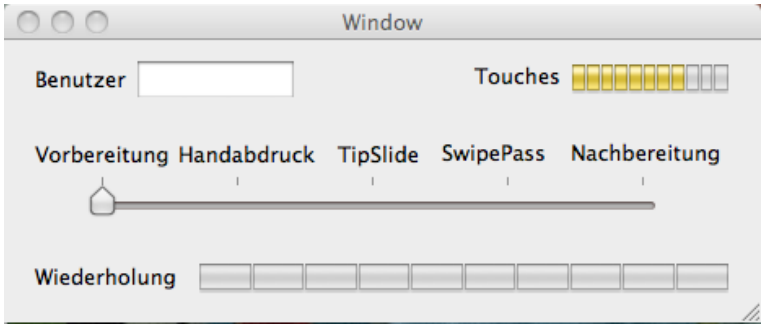

Abbildung 6.3: Das Tool zur Datensammlung. Oben links wird die Benutzer-ID eingegeben. Oben rechts wird angezeigt, wie viele Touches das System gerade erkennt. In der Mitte wird die Phase angezeigt. Unten füllt sich nach jeder Wiederholung der aktuellen Geste ein Kästchen.

Visualisierung der aufgenommenen Daten

Zum besseren Verständnis des Zusammenhanges zwischen dem abgegebenen Handabdruck und der Touch-Sammlung für die Testpersonen wurde ein Visualisierungsprogramm benutzt. So sollte gezeigt werden, dass das Multitouchpad nicht den Handumriss oder etwa den tatsächlichen Handabdruck mit allen Linien und Falten speichert. Eventuelle Bedenken der Testpersonen ihre biometrischen Daten abzugeben, sollten so beseitigt werden. Letztendlich hat auch nur eine Person aus diesem Grund ihre Teilnahme verweigert. Dieser Teilnehmer wird im weiteren Verlauf dieser Arbeit nicht weiter beachtet. Das Visualisierungsprogramm wurde vom Autor Jonathan Dhiel zur Verfügung gestellt.

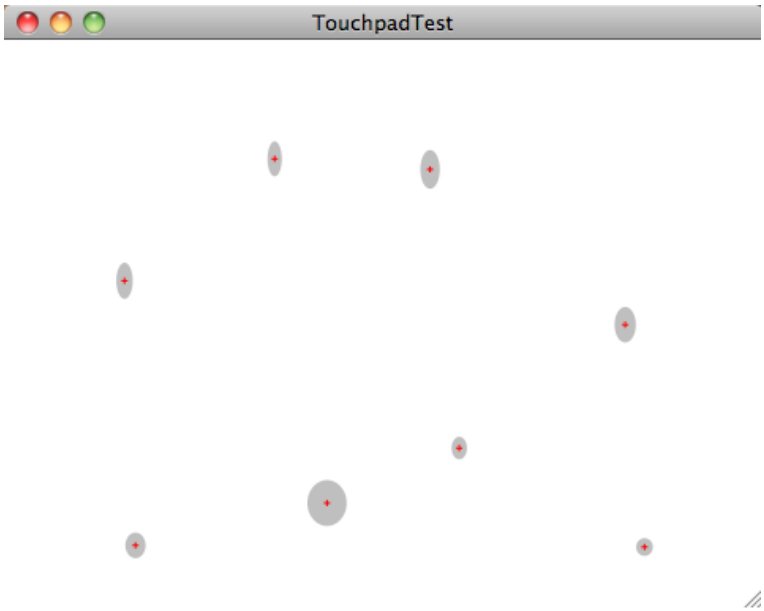

Abbildung 6.4: Das Visualisierungstool bei Auflage der Finger der geschlossenen Hand. Es wird deutlich, dass Mittel- und Ringfinger länger sind als kleiner Finger und Zeigefinger, allerdings werden weder der komplette Handumriss, noch die Hautstruktur gezeigt.

Die Versuchsreihe bestand aus fünf Phasen: Ablauf:

- Der Testperson wurden die einzelnen Gesten erklärt. Des Weiteren wurde ihr die Möglichkeit gegeben, sich mit dem Gerät vertraut zu machen, und die Gesten zu üben. Erklärung
- Zehnmalige Eingabe des HandScan HandScan
- Zehnmalige Eingabe des TipSlide TipSlide
- Zehnmalige Eingabe des FreeSwipe FreeSwipe
- Ausfüllen eines Fragebogens[6] über den Versuch. Fragebogen

Aufgrund der extrem hohen Sicherheit der ersten Studie gegen Shouldersurfattacken, auch bei einer Kameraunterstützung, wurde dieser Aspekt nicht weiter untersucht. Shouldersurfing nicht weiter untersucht

[6] siehe Anhang B

Fragebogen ähnlich zur ersten Studie

Ein Testdurchlauf dauerte ungefähr 15 Minuten. Die Testpersonen mussten der Teilnahme an dem Versuch wieder mittels einer Einverständniserklärung[7] zustimmen. Der Fragebogen ist dem aus der ersten Versuchsreihe sehr ähnlich. Die Fragen zu den Authentifizierungsverfahren HandScan, TipSlide und FreeSwipe waren identisch, Fragen zum Sortieren der einzelnen Sets wurden weggelassen.

Studie mit 62 Teilnehmern

62 Personen im Alter von 15 bis 69 nahmen an der Versuchsreihe teil. Das Durchschnittsalter betrug 42,7 Jahre. Ein Großteil der Studie wurde im Heimatdorf des Autors durchgeführt. Studienteilnehmer wurden gewonnen, indem von Tür zu Tür gegangen und gefragt wurde, ob die Person sich zur Teilnahme bereit erklärt.

Über eine Million Touches gesammelt

Insgesamt wurden im Rahmen des Versuchs über eine Million Touches gesammelt. Bei 62 Teilnehmern mit je drei Eingabephasen mit je 3x10 Eingaben ergibt das durchschnittlich 500 Touches pro Eingabe. Pro Benutzer wurden aufgrund des Speicherverfahrens von CoreData jeweils 15-30 MB Daten generiert. Wegen dieser großen Datenmenge entwickelten sich nach ca. 24 Testpersonen starke Performanceprobleme auf dem MacBookPro. Um dies zu umgehen, wurden die gespeicherten Daten jeweils nach ca. 15 Testläufen ausgelagert.

[7] siehe Anhang B

6.5.1 Fragebogen

Fragen

Wie oben beschrieben, füllten die Testpersonen auch nach dem Testlauf der Softwareprototypen einen Fragebogen aus. Überprüft wurden folgende Punkte:

- Waren die Instruktionen verständlich?
- Fiel es den Testpersonen leicht, die erforderlichen Gesten in das System einzugeben?
- Kann die Testperson sich vorstellen, eine oder mehrere der Gesten am eigenen Multitouchgerät zur Authentifizierung zu benutzen?
- Schätzt die Testperson die jeweilige Geste als einfacher, sicherer und schneller ein als die bekannte Passworteingabe?

Auch hier wurden die Fragen nach einer zufälligen Verteilung positiv oder negativ formuliert. Geantwortet wurde wieder durch Ankreuzen eines von fünf Feldern: “Starke Zustimmung”, “Zustimmung”, “Neutral”, “Ablehnung” und “Starke Ablehnung”.

HandScan sehr positiv bewertet

Die Authentifizierungsmethode HandScan erhielt die meisten positiven Bewertungen. 89% der Testpersonen fiel diese Geste sehr leicht und 94% konnten sich sogar vorstellen, sich darüber am eigenen System anzumelden. Die Methode wurde auch als sehr sicher eingestuft.

TipSlide neutral bewertet

Die Geste TipSlide erhielt auf den Fragebögen zwar keine negativen Bewertungen, schnitt aber schlechter ab als die beiden anderen Optionen. Während HandScan und FreeSwipe bezüglich der Leichtigkeit der Bewegung positiv beurteilt wurden, erhielt TipSlide nur neutrale Bewertungen. Diese Einschätzung kündigte sich bereits im ersten Testdurchlauf an. Sie konnte auch durch eine Anpassung der Bewegung nicht verbessert werden. Diese Bewegung kann daher nicht als benutzerfreundlich bewertet werden.

FreeSwipe Favorit

Die Geste FreeSwipe wurde von den Testpersonen mit 32 zu 27 Stimmen vor HandScan favorisiert. Dies verwundert,

weil HandScan von ihnen als schneller und einfacher eingeschätzt wurde als FreeSwipe. Dementsprechend können Schnelligkeit und Einfachheit der Eingabe nicht die ausschlaggebenden Kriterien der Testpersonen gewesen sein. Als die sicherste Authentifizierungsmethode schätzten sie TipSlide ein. Favorisiert wurde diese aber nur von zwei der 62 Befragten[8]. Die Testpersonen scheinen daher die Aspekte Sicherheit, Einfachheit oder Schnelligkeit der Eingabe nicht als besonders wichtig anzusehen. Das ausschlaggebende Kriterium könnte für sie die freie Wahlmöglichkeit einer Geste wie bei FreeSwipe sein. Zum einen bietet dieses Verfahren eine große Freiheit, zum anderen könnte der nahezu unendliche Pool an verfügbaren Gesten ein erhöhtes Sicherheitsgefühl erzeugen. Auch die Leichtigkeit der Bewegung scheint eine große Rolle zu spielen. Darauf deutet auch die bereits erwähnte niedrige Präferenz von TipSlide hin.

6.5.2 Ergebnisse

60% zum Lernen, 20% zur Lernkontrolle, 20% zum Testen

Während des Softwaretests hat jede Testperson jede Geste zehn Mal eingegeben. Aus dem entstandenen Datenpool verwendete das System 60% für das Erlernen der Eingabemethode. Anhand weiterer 20% kontrollierte es sich schon während des Lernvorgangs immer wieder selbst. Mit Hilfe der letzten 20% der Eingaben überprüfte es abschließend das Gelernte.

Fehlerquote konnte von 40% auf 23% gesenkt werden

Bei HandScan ergab sich beim ersten Durchlauf der Datenauswertung eine Fehlerquote von 40%. Durch verschiedene Anpassungen der Anzahl der Synapsen und der versteckten Ebenen des neuronalen Netzes konnte diese schließlich auf 23% gesenkt werden. Bei TipSlide und FreeSwipe lag die minimale Fehlerquote bei 24%. Von einer Implementierung als abgeschlossener Prototyp wurde aufgrund der schlechten initialen Ergebnisse zugunsten von mehr Variation im neuronalen Netzwerk und der Datenreduktion Abstand genommen.

Alle drei im Rahmen dieser Arbeit entwickelten Authentifi-

[8] Eine Testperson gab keinen Favoriten an

Ergebnisse aus menschlicher Erkennung konnten umgesetzt werden

zierungsverfahren erschienen nach dem ersten Testlauf als Papierprototyp vielversprechend. In der Implementierung als Software konnte dies entsprechend umgesetzt werden. Die korrekte Erkennungsrate lag bei 75%. Eine zufällige Zuordnung passender Authentifizierungen zum Benutzernamen hätte nur eine Erkennungsrate unter 10% hervorgebracht. Eine zuverlässige Methode, die Vorteile der beiden Systeme zu nutzen, konnte im Rahmen dieser Arbeit nicht gefunden werden.

Erkennungsrate noch zu verbessern

75% sind für eine sichere Authentifizierung noch zu niedrig. Eine mehrfache Authentifizierung des selben Nutzers würde die Erkennungsrate exponentiell erhöhen. Dies geht aber zu Lasten der Benutzerfreundlichkeit. Das ist nicht akzeptabel. Grundidee der hier entwickelten Authentifizierungsverfahren ist die breite Anwendbarkeit. Das kann nur durch entsprechende Benutzerfreundlichkeit erreicht werden.

Höherer Grunddatenbestand sinnvoll

Um eine sichere Wiedererkennungsrate zu erreichen, war möglicherweise der Grunddatenbestand bei einer 1000-dimensionalen Funktion zu niedrig. Eine größer angelegte Studie ginge aber weit über den zeitlichen Rahmen dieser Diplomarbeit hinaus[9].

Authentifizierungsverfahren positiv angenommen

Grundsätzlich fanden die Testpersonen die entwickelten Authentifizierungsverfahren sehr benutzerfreundlich. Einzige Ausnahme: TipSlide[10]. Auch der Sicherheitsaspekt wurde höher als bei einer einfachen Passworteingabe eingeschätzt. Eine Weiterverfolgung der Methoden HandScan und FreeSwipe erscheint demnach lohnenswert.

Eingabegeschwindigkeit 0-4s

Die Eingabegeschwindigkeit war bei allen drei Authentifizierungsmethoden akzeptabel. Keine Eingabe dauerte länger als vier Sekunden. Die Eingabe eines tatsächlichen Passworts, das aufgrund seiner Länge und Varianz der Zeichen den aktuellen Sicherheitsbestimmungen entspricht, dauert vermutlich länger. Das wurde im Rahmen dieser Arbeit allerdings nicht untersucht.

[9] siehe Kapitel 8 auf Seite 70
[10] siehe Seite 59

Kapitel 7

Evaluierung

Ziel der Arbeit zu großen Teilen erreicht

Ziel dieser Arbeit ist die Entwicklung eines Authentifizierungsverfahrens auf Multitouchsystemen, die einen erhöhten Sicherheitsstandard gegen Shouldersurfattacken bietet. Dieses wurde zu großen Teilen erreicht. Die Benutzerfreundlichkeit der entwickelten Systeme wurde als gut bis sehr gut eingestuft. Die Authentifizierungsvorgänge HandScan, TipSlide und FreeSwipe konnten in Echtzeit verarbeitet werden. Der erhöhte Sicherheitsstandard gegen Shouldersurfattacken wurde ebenfalls erreicht. Allein die nur mäßige Erkennungsrate lässt noch Forschungsspielraum.

Einsatz nur eingeschränkt möglich

Ein tatsächlicher Einsatz der im Rahmen dieser Arbeit entwickelten Systeme kann zum momentanen Zeitpunkt zwar nur in einem sehr eingeschränkten Umfeld empfohlen werden, aber insbesondere HandScan und FreeSwipe zeigen vielversprechende Tendenzen. Es wurde nachgewiesen, dass ein Handabdruck bzw. eine frei wählbare Geste auf einem Multitouchpad einem Benutzer zugeordnet werden können.

Messgrößen waren

In Kapitel 5.2 wurden folgende Messgrößen festgelegt:

1. Zeitaufwand zum Erlernen
2. Eingabegeschwindigkeit
3. Fehlerrate durch den Benutzer

4. Erinnerung über Zeit
5. Subjektive Zufriedenheit
6. Korrekte Erkennung
7. Erfolgreiche Shouldersurfattacken
8. Verarbeitungsgeschwindigkeit

Anhand der ersten fünf Punkte wird die Benutzerfreundlichkeit gemessen. Die Punkte sechs und sieben messen die Sicherheit und über die Verarbeitungsgeschwindigkeit wird die tatsächliche Anwendbarkeit geprüft.

Im folgenden Abschnitt werden die Ergebnisse der Studien anhand dieser Punkte beurteilt.

7.1 Benutzerfreundlichkeit

Benutzerfreundlichkeit: Erreicht

Der sehr geringe Zeitaufwand zum Erlernen der notwendigen Authentifizierungsgesten, die sehr schnelle Eingabegeschwindigkeit und die gute bis sehr gute subjektive Zufriedenheit machen alle drei Authentifizierungsverfahren benutzerfreundlich. HandScan und FreeSwipe erhielten hier sogar sehr gute Bewertungen. Das Ziel der Benutzerfreundlichkeit wurde erreicht. Die Auswertung der einzelnen Messgrößen folgt.

7.1.1 Zeitaufwand zum Erlernen

Sehr geringer Lernaufwand

Nach kürzester Zeit beherrschten alle Testpersonen die für HandScan, TipSlide und FreeSwipe erforderlichen Gesten. Bei beiden Studien wurden die Instruktionen sofort verstanden. Nach einer einmaligen Erklärung und Vorführung waren die Testpersonen in der Lage, die Gesten korrekt zu wiederholen. Der zum Erlernen nötige Zeitaufwand ist dementsprechend als sehr gering zu bewerten.

7.1.2 Eingabegeschwindigkeit

Die Eingabegeschwindigkeit für das Durchführen einer Authentifizierungsgeste schwankt je nach Authentifizierungsverfahren zwischen "unter einer Sekunde" und "eine bis fünf Sekunden". Bei der ersten Studie wurde das Auftragen der Fingerfarbe auf die Finger nicht mitgemessen.

Grundsätzlich erfolgten die Eingaben am Softwareprototypen schneller als am Papierprototypen. Dies ist wahrscheinlich auf die Fingerfarbe zurückzuführen. Die Zeitunterschiede waren aber sehr gering.

HandScan am schnellsten, FreeSwipe am langsamsten

HandScan konnte am schnellsten eingegeben werden. Nur sehr wenige Studienteilnehmer benötigten länger als eine Sekunde für die Eingabe der Geste. Ein Drittel der Testpersonen benötigten zwischen einer und drei Sekunden für die Eingabe von *TipSlide*. Die anderen Probanden benötigten weniger als eine Sekunde. Bei *FreeSwipe* war die Eingabegeschwindigkeit von der Komplexität der gewählten Geste abhängig. Die tatsächlich benötigte Zeit variierte zwischen unter zwei Sekunden und drei bis vier Sekunden. Länger brauchte niemand.

Eingabegeschwindigkeit sehr gut

Auf den Fragebögen wurden die getesteten Authentifizierungsverfahren schneller als die bekannte Passworteingabe eingeschätzt. Die Eingabegeschwindigkeit ist demnach sehr gut.

7.1.3 Fehlerrate durch den Benutzer

Eine von 1947 Eingaben falsch

Von den insgesamt 187 Eingaben der ersten Benutzerstudie und 1860 Eingaben der zweiten Benutzerstudie wurde ein einziges Mal eine Geste falsch eingegeben. Dem Benutzer fiel es sofort auf und er wiederholte die Eingabe korrekt. Dies entspricht einer Fehlerquote von 0,05%.

Gesten grundsätzlich einfach

Auf den Fragebögen wurden die drei Gesten grundsätzlich als einfach bewertet. Einzig TipSlide betrachteten einige aufgrund der ungewohnten Bewegung kritisch.

Fehlerrate sehr gering

Die Fehlerrate der Benutzer ist dementsprechend sehr gering.

7.1.4 Erinnerung über die Zeit

Erinnerung sehr gut

Keiner der überprüften Versuchsteilnehmer hatte Schwierigkeiten, sich nach einem Zeitraum von 14 Tagen an die getesteten Eingabegesten zu erinnern[1]. Die Erinnerung über die Zeit kann mit sehr gut bewertet werden.

7.1.5 Subjektive Zufriedenheit

Subjektive Zufriedenheit durch Befragung analysiert

Zur Analyse der subjektiven Zufriedenheit wurden die Studienteilnehmer befragt, ob sie sich vorstellen können, sich selbst mit diesen Ansätzen an ihrem eigenen Computer oder Smartphone anzumelden. Eine positive oder sehr positive Antwort wurde als Zufriedenheit gewertet.

HandScan und FreeSwipe sehr gut bewertet, TipSlide "noch ok"

HandScan schnitt hier mit 85% zufriedenen Studienteilnehmern am besten ab. Mit 82% zufriedenen Studienteilnehmern schneidet auch *FreeSwipe* bei der subjektiven Zufriedenheit der Benutzer sehr gut ab. Die Geste *TipSlide* erhält zwar mit 66% ebenfalls ein zufriedenstellendes Ergebnis. Allerdings fällt es deutlich hinter HandScan und FreeSwipe zurück.

7.2 Sicherheit

Sicherheit verbesserbar

Mit einer Erkennungsrate von 75% bzw. 76% schneiden alle drei Authentifizierungsverfahren zwar wesentlich schlechter ab als z.B. eine PIN Eingabe[2]. Dennoch bieten sie einen deutlich höheren Schutz gegen kameraunterstütztes Shouldersurfing. Sie bieten eine maximale Einbruchsrate von 25%, die einer PIN liegt deutlich höher[3].

[1] siehe Kapitel 5.7
[2] Erkennungsrate 100%
[3] Einbruchsrate 100% laut Almaula [2008]

7.2.1 Korrekte Erkennung

Grundsätzlich korrekt

Mit einer Erkennungsrate von 75% bzw. 76% sind die Systeme grundsätzlich in der Lage, Benutzer und ihre Eingabe einander korrekt zuzuordnen. Unter dem Aspekt der Sicherheit schneiden alle drei Authentifizierungsverfahren allerdings in ihrer jetzigen Form zu schlecht ab.

7.2.2 Erfolgreiche Shouldersurfattacken

Hohe Sicherheit gegen Shouldersurfattacken

FreeSwipe hielt im Papierprototypen allen Shouldersurfattacken ausnahmslos stand. Auch beim Softwareprototypen wurde trotz der schlechten Erkennungsrate maximal eine Einbruchsrate von 25% erreicht. Dies ist wesentlich besser als z.B. die Einbruchsrate einer kameraunterstützten Shouldersurfattacke auf eine vierstellige PIN an einem Bankautomaten.

7.3 Verarbeitungsgeschwindigkeit

Authentifizierung sehr schnell

Die Lernphase der Authentifizierungsgeste durch das System ist zwar wesentlich länger als das Erlernen eines Passwortes, die eigentliche Authentifizierung ist aber innerhalb einer Sekunde abgeschlossen. Da dieser Lernvorgang pro Benutzer nur einmal durchgeführt werden muss, ist dieser Mehraufwand zu vernachlässigen. Bei Umgebungen mit vielen Nutzern kann es hier allerdings zu Problemen kommen. Hier sind z.B. bei Webseiten mit vielen Neuanmeldungen, bei denen die Auswertung serverseitig realisiert wird, zu nennen.

Kapitel 8

Zusammenfassung und weitere Forschungsansätze

Theorie

Ziel dieser Arbeit ist, Authentifizierungsverfahren im Hinblick auf Multitouchsysteme zu verbessern. Zunächst wurden bereits entwickelte Authentifizierungsverfahren für Multitoucheingaben vorgestellt. Mögliche Sicherheitslücken, die durch Brute-Force- und Shouldersurf-Attacken ausgenutzt werden können, wurden aufgezeigt.

Verwandte Forschungsarbeiten, Taxonomie und Design

Nach der Einordnung der bereits existierenden Authentifizierungsverfahren in eine Taxonomie, wurden drei neue Authentifizierungsverfahren entwickelt. Um sich über eines dieser Systeme einloggen zu können, wurden bisher weniger gebräuchliche Parameter wie Timing oder Form genutzt. Damit sollte eine erhöhte Sicherheit gegen die oben erwähnten Angriffsmöglichkeiten gewährleistet werden. Dem Autor war außerdem die hohe Benutzerfreundlichkeit der Authentifizierungsverfahren wichtig.

Sicherheitsaspekt ausbaubar

Die im Rahmen dieser Arbeit entwickelten Systeme erwiesen sich zwar als benutzerfreundlich, der Sicherheitsaspekt konnte mit einer Erkennungsrate von nur 74% aber nicht zufriedenstellend gelöst werden.

Shouldersurfingsicherheit gut

Die Sicherheit gegenüber Shouldersurfing konnte im

Vergleich zur PIN-Eingabe deutlich verbessert werden, während zweitere bei Einsatz einer Kamera eine Einbruchsrate von 100% hat, kommen die hier vorgestellten Ansätze auf eine maximale Einbruchsrate von 25%.

Grundprinzip funktioniert

Die drei im Rahmen dieser Arbeit entwickelten Authentifizierungsverfahren sind vielversprechend. Die bisher erzielten Ergebnisse zeigen, dass die Systeme grundsätzlich in der Lage sind, verschiedene Benutzer voneinander zu unterscheiden. Die Sicherheit gegen Shouldersurfattacken ist deutlich höher als bei bisher bekannten Authentifizierungsverfahren. Auch erhielten sie von Testpersonen durchweg positive Bewertungen.

HandScan und FreeSwipe vielversprechend

Wie bereits erläutert, erscheint eine Weiterentwicklung der Authentifizierungsverfahren HandScan und FreeSwipe lohnenswert. Sie wurden von den Testpersonen positiv bewertet und die Erkennungsrate des Systems lag etwa gleich hoch.

Future Work:

Die Weiterentwicklung kann im Rahmen dieser Arbeit nicht erfolgen. Dennoch sollen hier mögliche Ansatzpunkte aufgezeigt werden:

Größere Benutzerstudie

Um genauere Ergebnisse erzielen zu können, sollte eine größer angelegte Studie durchgeführt werden. Für das neuronale Netz ist ein größerer Grunddatenbestand sinnvoll. Bei einer hohen Netzkomplexität, also bei vielen Neuronen und vielen versteckten Ebenen in Kombination mit nur wenigen Daten, sucht es nicht nach einem Muster, sondern lernt stattdessen die Daten einzeln auswendig.

Verbesserung der Datenreduktion

Die durchgeführte Datenreduktion[1] sollte genauer untersucht werden. Eventuell können die Daten noch weiter reduziert werden, um die Eingabedimension weiter zu verringern. Möglicherweise war die vorgenommene Datenreduzierung aber auch bereits zu stark. Ungewollt könnten signifikante Daten, die dem neuronalen Netz die Suche nach Mustern vereinfacht hätten, herausgefiltert worden sein.

Direkter Vergleich zu PW/PIN

Aufgrund der im Rahmen dieser Arbeit gezogenen For-

[1] siehe Kapitel 6.4

schungsergebnisse kann nicht erschlossen werden, ob die Testpersonen die einfache Passworteingabe einem der neu entwickelten Authentifizierungsverfahren vorziehen würden. Es bleibt ebenfalls unklar, warum genau ein System vorgezogen wird. Es gab keine eindeutige Tendenz zu Faktoren wie Schnelligkeit oder Einfachheit der Eingabe.

Akzeptanz von biometrischer Authentifizierung weiter untersuchen

Bei der Ablehnung eines Systems spielt sicherlich der persönliche Hintergrund jedes Benutzers eine Rolle. Bedenken bei der Abgabe biometrischer Daten sollten nicht unterschätzt werden. Hier könnten zusätzliche Untersuchungen durchgeführt werden, die aufzeigen, ob ein auf biometrischen Daten basierendes Passwort auf einem eigenen/privaten System eher akzeptiert wird als auf einem öffentlichen, wie beispielsweise an einem Bankautomaten.

Hintergrundbild bei FreeSwipe

FreeSwipe könnte analog zur Verbesserung von "Draw a Secret" um ein Hintergrundbild erweitert werden. Dies führt in Dunphy and Yan [2007] zu einer Wahl von komplexeren und somit sichereren Gesten. Ob diese Verbesserung auch für einfache Touchpads zu realisieren ist, müsste auch untersucht werden.

Versteckter Einsatz von HandScan

Der versteckte Einsatz von HandScan und eventuell auch FreeSwipe, z.B. auf einem Handy in der Hosentasche, könnte auch ein interessantes Forschungsthema sein.

Weiterer Prototyp und Untersuchung in der Praxis

Die weiterentwickelten Authentifizierungsverfahren sollten in einen abgeschlossenen Prototypen implementiert werden. Abschließend müssten Untersuchungen beim Einsatz in einem realen System praxisnah beobachtet werden.

Anhang A

Einverständniserklärung und Fragebogen zur “Evaluierung der Papierprototypen zur Multitouch Authentifizierung”

Einverständniserklärung

Evaluierung der Papierprototypen zur Multitouch Authentifizierung

STUDIENLEITER Andreas Hüttig
Media Computing Group
RWTH Aachen University
Telefon: 0221/16812912
Email: andreas.huettig@gmx.de

Ziel der Studie: Das Ziel der Studie ist es, die Papierprototypen auf Wiedererkennbarkeit der Muster und Shoulder Surfing Sicherheit bei der Authentifizierung zu testen. Die Teilnehmer werden gebeten, mit Fingerfarbe Muster nach vorgegebenen und frei gewählten Bewegungen auf Klarsichtfolie zu malen und Fingerfarbenbilder zu sortieren. Es wird untersucht, ob die Sortierung die zusammengehörigen Muster vereint hat.

Ablauf: Die Teilnahme an der Studie besteht aus neun Phasen. In der ersten Phase wird die Handinnenseite der Finger mit Fingerfarbe bestrichen und der Teilabdruck auf Klarsichtfolie genommen. In den Phasen zwei bis vier werden jeweils nur die Fingerspitzen mit Fingerfarbe bestrichen und das Bewegungsmuster auf Klarsichtfolie gegeben. In der zweiten Phase wird eine Bewegung vorgegeben und erklärt. In der dritten Phase kann das Muster frei gewählt werden. In der vierten Phase wird einmal eine Bewegung gezeigt, diese soll dann nachgemacht werden. In der fünften Phase wird ein Video von einer Bewegung gezeigt, die nachgemacht werden soll, dieses Video kann beliebig oft angesehen werden. In der Phase sechs werden die Ergebnisse der vorherigen Phasen mit den Ergebnissen anderer Testpersonen vermischt und sollen zusammengehörig sortiert werden. Diese Studie sollte etwa eine halbe Stunde dauern.

Nach der Studie werden wir Sie bitten, den Fragebogen über das getestete System auszufüllen. In diesem Fragebogen werden wir Ihnen einige Fragen zur Benutzung des Systems und zur Wiedererkennbarkeit der Muster stellen.

Risiken/Beschwerden: Es könnte sein, dass Sie die Teilnahme an der Studie ermüdet. Sie werden mehrere Gelegenheiten haben, sich zu erholen; zusätzliche Pausen sind ebenfalls möglich. Es sind keine weiteren Risiken im Zusammenhang mit der Studie bekannt. Sollte die Aufgabe oder der Fragebogen zu anstrengend für Sie sein, können Sie die Bearbeitung sofort abbrechen.

Nutzen: Die Resultate der Studie werden für die Entwicklung eines Systems genutzt, das eine schnellere und shouldersurfing resistentere Authentifizierung auf Multitouchgeräten ermöglichen soll.

Alternativen zur Teilnahme: Die Teilnahme an der Studie ist freiwillig. Es steht Ihnen frei, Ihre Teilnahme zurückzuziehen oder abzubrechen.

Kosten und Entschädigung: Die Teilnahme an der Studie wird Ihnen keinerlei Kosten verursachen. Während und nach ihrer Teilnahme werden für Sie Getränke und Snacks bereitstehen.

Vertraulichkeit: Alle Informationen, die während der Studienphase gesammelt werden, werden streng vertraulich behandelt. Ihre Daten werden nur durch Identifikationsnummern identifiziert. Keine Publikationen oder Berichte aus diesem Projekt werden personenbezogene Informationen über die Teilnehmer beinhalten, abgesehen von Teilen des Handabdrucks, die aber nur anonymisiert veröffentlicht werden. Wenn Sie sich bereit erklären, an dieser Studie teilzunehmen, unterschreiben Sie bitte unten.

_____ Ich habe die Hinweise auf diesem Formular gelesen und verstanden.
_____ Man hat mir die Hinweise auf dem Formular erklärt.

Name des Teilnehmers	Unterschrift des Teilnehmers	Datum
	Studienleiter	Datum

Wenn Sie Fragen zu dieser Studie haben, wenden Sie sich bitte an den Testleiter.

Fragebogen zur Studie „Evaluierung der Papierprototypen zur Multitouch Authentifizierung“

Benutzer-ID: Alter: Geschlecht:

1 = Starke Zustimmung, 2 = Zustimmung, 3 = Neutral, 4 = Ablehnung, 5 = Starke Ablehnung

	1	2	3	4	5
Phase 1					
Die Instruktionen waren missverständlich					
Die Bewegung fiel mir leicht					
Dieses System ist nicht geeignet um sich an einem Computer oder Smartphone anzumelden					
Diese System ist einfacher zu bedienen als eine Passworteingabe					
Dieses System ist unsicherer als eine Passworteingabe					
Dieses System ist langsamer als eine Passworteingabe (das Bemalen der Finger bitte nicht mit einberechnen)					
Ich kann mir vorstellen mich mit diesem System an meinem eigenen Computer oder Smartphone anzumelden					
Phase 2					
Die Instruktionen waren missverständlich					
Die Bewegung fiel mir schwer					
Dieses System ist geeignet um sich an einem Computer oder Smartphone anzumelden					
Diese System ist einfacher zu bedienen als eine Passworteingabe					
Dieses System ist unsicherer als eine Passworteingabe					
Dieses System ist schneller als eine Passworteingabe (das Bemalen der Finger bitte nicht mit einberechnen)					
Ich kann mir vorstellen mich mit diesem System an meinem eigenen Computer oder Smartphone anzumelden					
Phase 3					
Die Instruktionen waren verständlich					
Die Bewegung fiel mir schwer					
Dieses System ist geeignet um sich an einem Computer oder Smartphone anzumelden					
Diese System ist schwieriger zu bedienen als eine Passworteingabe					

Diese System ist schwieriger zu bedienen als eine Passworteingabe					
Dieses System ist sicherer als eine Passworteingabe					
Dieses System ist langsamer als eine Passworteingabe (das Bemalen der Finger bitte nicht mit einberechnen)					
Ich kann mir nicht vorstellen mich mit diesem System an meinem eigenen Computer oder Smartphone anzumelden					
Phase 4					
Die Instruktionen waren missverständlich					
Das Erkennen der Bewegung war einfach					
Die Bewegung fiel mir leicht					
Phase 5					
Die Instruktionen waren missverständlich					
Das Erkennen der Bewegung war schwer					
Die Bewegung fiel mir leicht					
Phase 6					
Die Instruktionen waren verständlich					
Die Sortierung fiel mir leicht					

Zutreffendes bitte ankreuzen oder einkreisen:

Welches System hat ihnen am besten gefallen? 1 2 3

Besitzen Sie ein Multitouchgerät (Smartphone, MacBook, iPad, etc.)? Ja Nein

Haben Sie Anmerkungen?

Vielen Dank für Ihre Teilnahme

Anhang B

Einverständniserklärung und Fragebogen zur “Benutzerdatenanalyse zur Multitouch Authentifizierung”

Einverständniserklärung

Benutzerdatenanalyse zur Multitouch Authentifizierung

STUDIENLEITER Andreas Hüttig
Media Computing Group
RWTH Aachen University
Telefon: 0221/16812912
Email: andreas.huettig@gmx.de

Ziel der Studie: Das Ziel der Studie ist es, Muster bei der Multitoucheingabe zu erkennen, die für eine Authorisierung geeignet sind. Die Teilnehmer werden gebeten, vorgegebene und frei gewählte Multitouchgesten wiederholt einzugeben. Es wird untersucht, ob es erkennbare Gemeinsamkeiten bei den Wiederholungen und Unterschiede zu anderen Benutzereingaben gibt.

Ablauf: Die Teilnahme an der Studie besteht aus 4 Phasen. In der ersten Phase wird der Ablauf erklärt, der Benutzer mit dem Gerät vertraut gemacht und kann die Bewegungen der Phasen 2-4 schonmal üben. In den Phasen zwei bis vier werden Gesten auf einem Multitouchpad zehnmal wiederholt eingegeben. In der zweiten Phase besteht die Geste aus dem flachen auflegen eines Teils der Hand. In der dritten Phase werden Zeige- bis kleiner Finger zuerst bei gekrümmter Hand in gerader Linie senkrecht auf das Touchpad gestellt und dann die Hand gestreckt und abgeflacht. In der vierten Phase wird eine beliebige Geste gewählt. Diese Studie sollte etwa eine Viertelstunde dauern.

Nach der Studie werden wir Sie bitten, den Fragebogen über das getestete System auszufüllen. In diesem Fragebogen werden wir Ihnen einige Fragen zur Benutzung des Systems stellen.

Risiken/Beschwerden: Es sind keine Risiken im Zusammenhang mit der Studie bekannt. Sollte die Aufgabe oder der Fragebogen zu anstrengend für Sie sein, können Sie die Bearbeitung sofort abbrechen. Es kann aber auch jederzeit eine Pause eingelegt werden.

Nutzen: Die Resultate der Studie werden für die Entwicklung eines Systems genutzt, das eine schnellere und shouldersurfing resistentere Authentifizierung auf Multitouchgeräten ermöglichen soll.

Alternativen zur Teilnahme: Die Teilnahme an der Studie ist freiwillig. Es steht Ihnen frei, Ihre Teilnahme zurückzuziehen oder abzubrechen.

Kosten und Entschädigung: Die Teilnahme an der Studie wird Ihnen keinerlei Kosten verursachen. Eine Entschädigung ist nicht vorgesehen.

Vertraulichkeit: Alle Informationen, die während der Studienphase gesammelt werden, werden streng vertraulich behandelt. Ihre Daten werden nur durch Identifikationsnummern identifiziert. Keine Publikationen oder Berichte aus diesem Projekt werden personenbezogene Informationen über die Teilnehmer beinhalten, abgesehen von Teilen des Handabdrucks, die aber nur anonymisiert veröffentlicht werden.

Wenn Sie sich bereit erklären, an dieser Studie teilzunehmen, unterschreiben Sie bitte unten.

_____ Ich habe die Hinweise auf diesem Formular gelesen und verstanden.
_____ Man hat mir die Hinweise auf dem Formular, wo nötig, erklärt.

Name des Teilnehmers	Unterschrift des Teilnehmers	Datum
	Studienleiter	Datum

Wenn Sie Fragen zu dieser Studie haben, wenden Sie sich bitte an den Testleiter.

Fragebogen zur Studie
„Benutzerdatenanalyse zur Multitouch Authentifizierung“

Benutzer-ID: Alter: Geschlecht:

1 = Starke Zustimmung, 2 = Zustimmung, 3 = Neutral, 4 = Ablehnung, 5 = Starke Ablehnung

	1	2	3	4	5
Phase 1					
Die Instruktionen waren missverständlich					
Die Bewegung fiel mir leicht					
Dieses System ist nicht geeignet um sich an einem Computer oder Smartphone anzumelden					
Dieses System ist einfacher zu bedienen als eine Passworteingabe					
Dieses System ist unsicherer als eine Passworteingabe					
Dieses System ist langsamer als eine Passworteingabe					
Ich kann mir vorstellen mich mit diesem System an meinem eigenen Computer oder Smartphone anzumelden					
Phase 2					
Die Instruktionen waren missverständlich					
Die Bewegung fiel mir schwer					
Dieses System ist geeignet um sich an einem Computer oder Smartphone anzumelden					
Dieses System ist einfacher zu bedienen als eine Passworteingabe					
Dieses System ist unsicherer als eine Passworteingabe					
Dieses System ist schneller als eine Passworteingabe					
Ich kann mir vorstellen mich mit diesem System an meinem eigenen Computer oder Smartphone anzumelden					
Phase 3					
Die Instruktionen waren verständlich					
Die Bewegung fiel mir schwer					
Dieses System ist geeignet um sich an einem Computer oder Smartphone anzumelden					
Dieses System ist schwieriger zu bedienen als eine Passworteingabe					
Dieses System ist sicherer als eine Passworteingabe					

Dieses System ist langsamer als eine Passworteingabe					
Ich kann mir nicht vorstellen mich mit diesem System an meinem eigenen Computer oder Smartphone anzumelden					

Zutreffendes bitte ankreuzen oder einkreisen:

Welches System hat ihnen am besten gefallen? 1 2 3

Besitzen Sie ein Multitouchgerät (Smartphone, MacBook, iPad, etc.)? Ja Nein

Haben Sie Anmerkungen?

Vielen Dank für Ihre Teilnahme

Literaturverzeichnis

Varun Kartik Almaula. Protecting the login session from camera based shoulder surfing attacks. January 2008. URL http://escholarship.org/uc/item/5d91n0jn;jsessionid=1DF23652203BEEAD00EF8B4B2BC4BDF6#page-4.

Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. User authentication through keystroke dynamics. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):367–397, 2002. URL http://portal.acm.org/citation.cfm?id=581272.

A. De Luca, Roman Weiss, and Heinrich Hussmann. PassShape: stroke based shape passwords. In *Proceedings of the 19th Australasian conference on Computer-Human Interaction: Entertaining User Interfaces*, page 240, Adelaide, Australia, 2007. ACM. ISBN 978-1-59593-872-5. URL http://portal.acm.org/citation.cfm?id=1324943.

A. De Luca, E. von Zezschwitz, and H. Huß mann. Vibrapass: secure authentication based on shared lies. In *Proceedings of the 27th international conference on Human factors in computing systems*, pages 913–916, Boston, MA, USA, 2009. ACM. ISBN 978-1-60558-246-7. URL http://portal.acm.org/citation.cfm?id=1518840.

Paul Dunphy and Jeff Yan. Do background images improve"draw a secret"graphical passwords? In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 36–47, Alexandria, Virginia, USA, 2007. ACM New York, NY, USA. ISBN 978-1-59593-703-2. URL http://portal.acm.org/citation.cfm?id=1315245.1315252.

Tovi Grossman, George Fitzmaurice, and Ramtin Attar. A survey of software learnability: metrics, methodologies and guidelines. In *Proceedings of the 27th international conference on Human factors in computing systems*, pages 649–658, Boston, MA, USA, 2009. ACM New York, NY, USA. ISBN 978-1-60558-246-7. URL http://portal.acm.org/citation.cfm?id=1518701.1518803.

Jiawei Han. Data Mining: Concepts and Techniques. November 2005. URL http://dl.acm.org/citation.cfm?id=1076797.

L.A. Jones, A.I. Antón, and J.B. Earp. Towards understanding user perceptions of authentication technologies. In *Proceedings of the 2007 ACM workshop on Privacy in electronic society*, page 98, Alexandria, Virginia, USA, 2007. ACM. ISBN 978-1-59593-883-1. URL http://portal.acm.org/citation.cfm?id=1314352.

Rick Joyce and Gopal Gupta. Identity authentication based on keystroke latencies. *Communications of the ACM*, 33(2):168–176, 1990. URL http://portal.acm.org/citation.cfm?id=75582.

David Kim, Paul Dunphy, Pam Briggs, Jonathan Hook, John Nicholson, James Nicholson, and Patrick Olivier. *Multi-touch authentication on tabletops*. CHI '10. ACM Press, New York, New York, USA, 2010. ISBN 9781605589299. doi: 10.1145/1753326.1753489. URL http://doi.acm.org/10.1145/1753326.1753489.

Angela Lammers and Sharon Langenfeld. Identity Authentication Based on Keystroke Latencies Using Neural Networks. *Journal of Computing Sciences in Colleges*, 6(5):48–51, April 1991. ISSN 1937-4771. URL http://dl.acm.org/citation.cfm?id=128000.903999.

Eric Lecolinet, Yves Guiard, and Anne Roudaut. MicroRolls: expanding touch-screen input vocabulary by distinguishing rolls vs. slides of the thumb. pages 927–936, Boston, MA, USA, 2009. ACM. ISBN 978-1-60558-246-7. URL http://portal.acm.org/ft_gateway.cfm?id=1518843&type=pdf&coll=Portal&dl=ACM&CFID=75469084&CFTOKEN=89753563.

B. Malek, M. Orozco, and A. El Saddik. Novel shoulder-surfing resistant haptic-based graphical password. In *Proc. EuroHaptics*, volume 6. Citeseer, 2006. URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.2083&rep=rep1&type=pdf.

Justin Matejka, Tovi Grossman, Jessica Lo, and George Fitzmaurice. The design and evaluation of multi-finger mouse emulation techniques. In *Proceedings of the 27th international conference on Human factors in computing systems*, pages 1073–1082, Boston, MA, USA, 2009. ACM. ISBN 978-1-60558-246-7. URL http://portal.acm.org/citation.cfm?id=1518865.

J. Nielsen. Iterative user-interface design. *Computer*, 26(11):32–41, 1993. ISSN 00189162. doi: 10.1109/2.241424. URL http://dl.acm.org/citation.cfm?id=618985.619982.

Christof Paar and Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010. ISBN 3642041000.

Hirokazu Sasamoto, Nicolas Christin, and Eiji Hayashi. Undercover: authentication usable in front of prying eyes. In *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, pages 183–192, Florence, Italy, 2008. ACM. ISBN 978-1-60558-011-1. URL http://portal.acm.org/citation.cfm?id=1357054.1357085.

Dominik Schmidt, Ming Ki Chong, and Hans Gellersen. *HandsDown*. NordiCHI '10. ACM Press, New York, New York, USA, 2010. ISBN 9781605589343. doi: 10.1145/1868914.1868964. URL http://doi.acm.org/10.1145/1868914.1868964.

Ben Shneiderman, Catherine Plaisant, Maxine Cohen, and Steven Jacobs. Designing the User Interface: Strategies for Effective Human-Computer Interaction. March 2009. URL http://dl.acm.org/citation.cfm?id=1593001.

Feng Wang and Xiangshi Ren. Empirical evaluation for finger input properties in multi-touch interaction. In *Proceedings of the 27th international conference on Human factors*

in computing systems, pages 1063–1072, Boston, MA, USA, 2009. ACM New York, NY, USA. ISBN 978-1-60558-246-7. URL http://portal.acm.org/citation.cfm?id=1518864.

J.O. Wobbrock. TapSongs: tapping rhythm-based passwords on a single binary sensor. In *Proceedings of the 22nd annual ACM symposium on User interface software and technology*, pages 93–96, Victoria, BC, Canada, 2009. ACM. ISBN 978-1-60558-745-5. URL http://portal.acm.org/citation.cfm?id=1622194.

Wolfgang J. Koschnik. *Standardwörterbuch für die Sozialwissenschaften*. K. G. Saur Verlag, München, London, New York, Paris, 1993. ISBN ISBN 3-598-11080-4.

Index

Typeset 7. September 2011