

AutoUni – Schriftenreihe

AutoUni 

Matthias Trojahn

Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens

AutoUni – Schriftenreihe

Band 85

Herausgegeben von / Edited by
Volkswagen Aktiengesellschaft
AutoUni

Die Volkswagen AutoUni bietet den Promovierenden des Volkswagen Konzerns die Möglichkeit, ihre Dissertationen im Rahmen der „AutoUni Schriftenreihe“ kostenfrei zu veröffentlichen. Die AutoUni ist eine international tätige wissenschaftliche Einrichtung des Konzerns, die durch Forschung und Lehre aktuelles mobilitätsbezogenes Wissen auf Hochschulniveau erzeugt und vermittelt.

Die neun Institute der AutoUni decken das Fachwissen der unterschiedlichen Geschäftsbereiche ab, welches für den Erfolg des Volkswagen Konzerns unabdingbar ist. Im Fokus steht dabei die Schaffung und Verankerung von neuem Wissen und die Förderung des Wissensaustausches.

Zusätzlich zu der fachlichen Weiterbildung und Vertiefung von Kompetenzen der Konzernangehörigen, fördert und unterstützt die AutoUni als Partner die Doktorandinnen und Doktoranden von Volkswagen auf ihrem Weg zu einer erfolgreichen Promotion durch vielfältige Angebote – die Veröffentlichung der Dissertationen ist eines davon. Über die Veröffentlichung in der AutoUni Schriftenreihe werden die Resultate nicht nur für alle Konzernangehörigen, sondern auch für die Öffentlichkeit zugänglich.

The Volkswagen AutoUni offers PhD students of the Volkswagen Group the opportunity to publish their doctor's theses within the "AutoUni Schriftenreihe" free of cost. The AutoUni is an international scientific educational institution of the Volkswagen Group Academy, which produces and disseminates current mobility-related knowledge through its research and tailor-made further education courses. The AutoUni's nine institutes cover the expertise of the different business units, which is indispensable for the success of the Volkswagen Group. The focus lies on the creation, anchorage and transfer of new knowledge.

In addition to the professional expert training and the development of specialized skills and knowledge of the Volkswagen Group members, the AutoUni supports and accompanies the PhD students on their way to successful graduation through a variety of offerings. The publication of the doctor's theses is one of such offers.

The publication within the AutoUni Schriftenreihe makes the results accessible to all Volkswagen Group members as well as to the public.

Herausgegeben von / Edited by

Volkswagen Aktiengesellschaft

AutoUni

Brieffach 1231

D-38436 Wolfsburg

<http://www.autouni.de>

Matthias Trojahn

Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens

 Springer

Matthias Trojahn
Wolfsburg, Deutschland

Zugl.: Dissertation, Otto-von-Guericke Universität Magdeburg, 2016

Die Ergebnisse, Meinungen und Schlüsse der im Rahmen der AutoUni Schriftenreihe veröffentlichten Doktorarbeiten sind allein die der Doktorandinnen und Doktoranden.

AutoUni – Schriftenreihe
ISBN 978-3-658-14048-9 ISBN 978-3-658-14049-6 (eBook)
DOI 10.1007/978-3-658-14049-6

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer

© Springer Fachmedien Wiesbaden 2016

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH

Danksagung

Die vorliegende Dissertation entstand während der Tätigkeit als Doktorand bei der Volkswagen Aktiengesellschaft im Bereich der mobilen Endgeräte am Standort Wolfsburg in Zusammenarbeit mit dem Institut für Verteilte Systeme (IVS) an der Fakultät für Informatik der Otto-von-Guericke-Universität in Magdeburg.

Zunächst möchte ich Herrn Prof. Dr. Frank Ortmeier für die hervorragende wissenschaftliche Betreuung und zahlreichen Diskussionen danken. Des Weiteren gilt Herrn Prof. Dr. Thomas Leich und Herrn Prof. Dr. Heinrich Hußmann mein Dank für die zahlreichen Gespräche und die Übernahme des Zweit- bzw. Drittgutachtens.

Die vorliegende Arbeit wäre ohne die Unterstützung der vielen Probanden, die sich dazu bereit erklärt haben, an den Studien teilzunehmen, nicht möglich gewesen. Insbesondere möchte ich den zahlreichen Studenten für die Durchführung der Studien und die vielen Anregungen danken.

An dieser Stelle bedanke ich mich bei allen Kollegen der Abteilung „Client & Communication Technologies“ der Volkswagen AG für die vielen Ratschläge, Hinweise und Inspirationen.

Den wissenschaftlichen Mitarbeitern des Fachgebiets „Software Engineering“ der Otto-von-Guericke-Universität möchte ich für die freundschaftliche Aufnahme und die vielen fachlichen Diskussionen danken.

Nicht zuletzt geht ein großer Dank an meine Familie und meine Freunde, insbesondere an meine Frau Kristina, die mich in der Zeit meines Studiums und meiner Dissertation unterstützt und motiviert haben.

Matthias Trojahn

Inhaltsverzeichnis

Abbildungsverzeichnis	XI
Tabellenverzeichnis	XV
Abkürzungsverzeichnis	XIX
1 Einleitung	1
1.1 Motivation	1
1.2 Zielstellung der Arbeit	4
1.3 Rahmenbedingungen und Einschränkungen	5
1.4 Struktur der Arbeit	6
2 Grundlagen des Aufgabenfeldes	9
2.1 Sicherheit und Sicherheitsaspekte	9
2.2 Identitätsmanagement	10
2.2.1 Zugriff auf Objekte	11
2.2.2 Authentifizierungsfaktoren	12
2.3 Qualitätsanforderungen und -kriterien	14
2.3.1 Anforderungen an die Systemsicherheit	14
2.3.2 Vergleichsraten	18
2.4 Bestandteile der Authentifizierung mittels Biometrie	21
2.4.1 Prozess während der Authentifizierung	21
2.4.2 Authentifizierungsmodalitäten	26
2.5 Multi-biometrische Verfahren	31
2.5.1 Vor- und Nachteile der Fusion	31
2.5.2 Arten multi-biometrischer Verfahren	33
2.5.3 Stufen bei Fusion von multi-biometrischen Verfahren	34

2.6	Herausforderungen der biometrischen Authentifizierung	35
2.7	Zusammenfassung	36
3	Forschungslücken und Lösungskonzept	39
3.1	Stand der Technik für biometrische Authentifizierung .	39
3.1.1	Tippverhalten	39
3.1.2	Gangerkennung und Bewegungserkennung . . .	44
3.2	Abgrenzung und Einordnung der Forschungsarbeiten .	47
3.3	Konzept der Authentifizierung mittels des Tippverhaltens	49
4	Struktur zur Versuchsdurchführung	53
4.1	Aufbau des Hauptteils der Studien	53
4.2	Verwendete Geräte	57
4.3	Implementierung der Prototypen	58
4.3.1	Software-Architektur	58
4.3.2	Aufbau und Ablauf der Authentifizierungsanwendungen	59
4.4	Deskriptive Daten der Probanden	63
4.4.1	Teilnehmer der Studien	63
4.4.2	Erfahrung mit einem Touchscreen	64
4.4.3	Einstellung der Probanden gegenüber der eingesetzten Technik	65
4.5	Zusammenfassung	67
5	Anpassungen am bisherigen Authentifizierungsprozess . .	69
5.1	Zielstellung für die Authentifizierung mittels Smartphone	69
5.2	Konzept für die Anpassungen am Authentifizierungsprozess	71
5.2.1	Datenerhebung mittels Sensoren	72
5.2.2	Vorverarbeitung	77
5.2.3	Extraktion der Merkmale	77
5.2.4	Klassifikatoren und Entscheidung	83
5.3	Evaluierung des Konzeptes	89
5.3.1	Merkmalvergleich für die Klassifikation	89

- 5.3.2 Vergleich von Klassifikatoren 98
- 5.3.3 Vergleich zwischen 12-Tasten- und
QWERT-Layout 103
- 5.3.4 Verwendung von Wischmuster – Swype 105
- 5.3.5 Veränderung des Tippverhaltens durch das
Lernverhalten 108
- 5.4 Ergebnisse und Bewertung des entworfenen Systems . 110

- 6 Gerätespezifische und -übergreifende Authentifizierung . 115**
 - 6.1 Zielstellung für die Authentifizierung mit mehreren
Geräten 115
 - 6.2 Konzept für die Transformation des Merkmalmodells . 119
 - 6.3 Evaluierung des Konzeptes 122
 - 6.3.1 Gerätespezifische Authentifizierung 122
 - 6.3.2 Geräteübergreifende Authentifizierung 129
 - 6.4 Bewertung der Geräteunabhängigkeit 131

- 7 Szenarienbasierte Authentifizierung 133**
 - 7.1 Zielstellung für szenarienbasierte Authentifizierung . . 133
 - 7.2 Konzept der szenarienübergreifenden Authentifizierung 136
 - 7.2.1 Prozess des Merkmalmodells 137
 - 7.2.2 Erkennung der Schreibhand 138
 - 7.2.3 Erkennung von Bewegungen 141
 - 7.2.4 Transformationen 143
 - 7.3 Evaluierung des Konzeptes 143
 - 7.3.1 Neues Enrolment für jedes Szenario 144
 - 7.3.2 Enrolment nur im Sitzen 146
 - 7.3.3 Erkennung von Szenarien 149
 - 7.3.4 Nachweis der Verbesserung durch eine
Szenarientransformation 152
 - 7.4 Bewertung der Szenarienabhängigkeit 154

- 8 Authentifizierungsmethoden für die Re-Authentifizierung 157**
 - 8.1 Zielstellung des kontinuierlichen
Authentifizierungssystems 157

8.2	Konzept der kontinuierliche Authentifizierung	158
8.2.1	Textunabhängige Erweiterungen beim klassischen Tippen	158
8.2.2	Generierung der Negativbeispiele	160
8.2.3	Notwendigkeit einer kontinuierlich durchgeführten Authentifizierung	161
8.2.4	Konzept der kontinuierlichen Authentifizierung	163
8.2.5	Vertrauensmodell	164
8.3	Evaluierung des Konzeptes	166
8.3.1	Textunabhängige Authentifizierung	167
8.3.2	Validierung des Frameworks mit zuvor generierten negativen Datensätzen	169
8.3.3	Skalierbarkeit des Tippverhaltens	172
8.3.4	Bewegungserkennung des Smartphones	174
8.3.5	Einflüsse der Fehlerraten auf das Vertrauensmodell	177
8.4	Bewertung des Konzeptes	180
9	Zusammenfassung und Ausblick	183
9.1	Ergebnisse	183
9.2	Limitation	185
9.3	Nutzen	188
9.4	Ausblick	189
A	Anhang	193
A.1	Experiment-Text	193
A.2	Eigene Studien im Überblick	193
A.3	Durchgeführte Bewegungen	195
A.4	Anonyme Identifikator	196
A.5	Deskriptive Daten	197
A.6	Standardkonfigurationen für Weka-Klassifikation	198
A.7	Merkmale für die gerätespezifische Authentifizierung	202
A.8	Geräteübergreifende Authentifizierung ohne Anpassung	204
	Literaturverzeichnis	205

Abbildungsverzeichnis

1.1	Strukturelle Vorgehensweise innerhalb der Arbeit . . .	7
2.1	Prozess: Zugriff auf ein Objekt (nach [Har10, S. 157]) .	11
2.2	Zusammenhang unterschiedlicher Fehlerraten	18
2.3	Die Akzeptanzrate für drei verschiedene Konfigurationen	20
2.4	Ablauf des Authentifizierungsprozesses (nach [KAK11, S. 1566])	21
2.5	Darstellung verschiedener Abstandsfunktionen	24
2.6	Schwellenwertelement bei neuronalen Netzen	24
2.7	Modalitäten für die biometrische Authentifizierung . .	26
2.8	Erkennung des Ganges mithilfe des Gyroskops	30
2.9	ROC-Kurve: (links) Kombination aus Fingerabdruck und Handgeometrie. (rechts) Kombination aus Fingerabdruck, Gesicht und Handgeometrie [RJ03] . .	32
2.10	Ebenen der Fusion	34
3.1	n-Graphen	40
3.2	Grundlegende methodische Erweiterungen	50
4.1	Genereller Aufbau des Authentifizierungsprogrammes .	59
4.2	Genereller Ablauf der Experimente	61
4.3	Verteilung der Personenaltersgruppen	63
4.4	Aussage 1: „Texte wie E-Mails und SMS auf einem Touchscreen zu schreiben dauert mir zu lange und ist zu umständlich.“	66
4.5	Aussage 2: „Ich nutze gerne das Touchscreen meines Smartphones.“	66

4.6	Aussage 3: „Es fällt mir schwer, mich ohne physikalische Tastatur beim Tippen zu orientieren.“ . . .	67
5.1	Tastaturenlayout mit den x- und y-Koordinaten	73
5.2	Verschiedene Kennzeichnungen für Aktionen	75
5.3	Das Koordinatensystem des Gerätes	76
5.4	Baumstruktur des Merkmalmodells	78
5.5	Extraktion verschiedener Merkmale.	79
5.6	Die drei Neigungsachsen eines Gerätes (Vgl. [Bee10, S. 222])	81
5.7	Swypen des Wortes „hello“ [Swy12]	82
5.8	Inter-Klassen-Unterschiede	88
5.9	Prozentualer Unterschied der Werte der einzelnen Merkmale von den letzten zu den ersten Versuchen . . .	109
6.1	Unterschiedliche Verhältnisse zwischen der Anzahl an Werten der Druckstärke und der Auflagefläche	116
6.2	Darstellung unterschiedlicher Verhältnisse zwischen Druckstärke und Auflagefläche	117
6.3	Unterschiedliche Normierungen der Auflagefläche für verschiedene Geräte, die schon in der Veröffentlichung [TSO13] vorgestellt wurden	118
6.4	Unterscheidung zwischen gerätespezifischer und geräteübergreifender Verarbeitung	119
7.1	Unterscheidung zwischen szenarienspezifischer und szenarienübergreifender Extraktion der Merkmale . . .	137
7.2	Darstellung der Bestimmung der Händigkeit	139
7.3	Links: Verlauf der Druckstärke für Rechtshänder (Maximum oben links), rechts: Verlauf der Auflagefläche (Maximum unten links)	140
7.4	Zustände des Gerätes und Aktivitäten	142
8.1	Ablauf der Sperrzustände eines Smartphones	162
8.2	Skala für das Vertrauensmodell (in %)	166

8.3	Beeinflussung des Vertrauens bezüglich der Ungenauigkeit der biometrischen Methoden	179
9.1	Übersicht der analysierten Gebiets beim Tippverhalten	186
A.1	Fragebogen	197

Tabellenverzeichnis

3.1	Übersicht über tragbare Sensoren (angelehnt an Gafurov [Gaf08, S. 13]	45
3.2	Erkannter Forschungsbedarf bei der Authentifizierung mittels des Tippverhaltens	48
4.1	Vergleich der verwendeten Geräte	57
4.2	Verteilung der Personen mit Erfahrung mit Smartphones und deren Nutzungsdauer pro Tag.	64
4.3	Unterschiedliche Betriebssysteme, die von den Testpersonen genutzt werden (Mehrfachantworten sind möglich)	65
5.1	Unterschiede in den Fehlerraten bei den verschiedenen Merkmalen (in %)	90
5.2	Unterscheidungen der Intra-Personen- und Inter-Personen-Unterschiede (in %)	93
5.3	Fehlerraten für fusionierte Merkmale (in %)	95
5.4	Ungewichtete Fusion aller Merkmale (in %)	96
5.5	Fehlerraten für einzelne Gewichtungsmodelle (in %)	97
5.6	Fehlerraten (Durchschnitt und Standardabweichung) für verschiedene Testpersonen (in %)	100
5.7	Bearbeitungszeit und durchschnittliche Fehlerraten der einzelnen Klassifikatoren im Test pro Benutzer	102
5.8	FAR und FRR für beide Tastaturenlayouts (in %) bei der numerischen Eingabe	103
5.9	FAR und FRR für beide Tastaturenlayouts (in %) bei der alphabetischen Eingabe	104
5.10	Resultierende Fehlerraten pro Passwort (in %)	106

5.11	Vergleich der Fehlerraten zwischen dem ersten und letzten Tag (in %)	108
5.12	Korrelationsanalyse mittels PSPP	112
6.1	Vergleich der Anzahl unterschiedlicher Merkmale . . .	123
6.2	Unterschiedliche FAR und FRR (in %) ausgewählter Merkmale (EER maximal 20 %) in Relation zu dem verwendeten Passwort und Gerät (Auszug, komplette Liste in Abschnitt A.7)	124
6.3	Merkmale mit den geringsten Fehlerraten (basierend auf der durchschnittlichen Fehlerrate), aufsteigend sortiert	126
6.4	Fehlerraten für die einzelnen Passwörter und Geräte (in %)	127
6.5	Fehlerraten, bei nur einem Enrolment für unterschiedliche Geräte (in %)	129
7.1	Auszug an existierenden Szenarien, die das Tippverhalten verändern	134
7.2	Fehlerraten für die verwendeten Passwörter bei der Extraktion der Daten für Enrolment und Verifizierung des gleichen Szenarios (in %)	144
7.3	Vergleich der Fehlerraten für ein Enrolment nur im Sitzen (in %).	147
7.4	Erkennungsraten Einhändigkeit vs. Beidhändigkeit (in %)	150
7.5	Erkennungsrate von Links- und Rechtshändern (in %)	150
7.6	Gesamterkennungsrate mit welcher Hand bzw. ob mit beiden Händen getippt wurde (in %)	151
7.7	Fehlerraten bei einer Transformation zum Szenario Sitzen (in %)	152
8.1	Fehlerraten für eine unterschiedliche Blocklänge (in %)	167
8.2	Fehlerraten, je nach Konfiguration (in %)	170

8.3	Fehlerraten für unterschiedliche Personenzahlen im Versuch (in %)	172
8.4	Fehlerraten Standardaktivitäten und Angriffsszenarien (in %)	175
8.5	Erkennungsfehler unter Berücksichtigung des Zustandes vor der Aktivität (in %)	176
8.6	Vergleich der kalkulierten EER (in %)	178
8.7	Auswirkungen auf die Fehlerraten bei mehreren Versuchen (in %)	181
A.1	Überblick über die verschiedenen Studien	194
A.2	Liste der aufgenommenen Aktivitäten	195
A.3	Unterschiedliche FAR und FRR (in %) der einzelnen Merkmale in Relation zu dem verwendeten Passwort und Geräte	202
A.4	Fehlerraten, bei nur einem Enrolment für die unterschiedlichen Geräte, wenn keine Transformation verwendet wird (in %)	204

Abkürzungsverzeichnis

API	Application Programming Interface (dt. Schnittstelle bei der Programmierung)
App	Applikation
BSI	Bundesamt für Sicherheit in der Informationstechnik
DPI	Dots Per Inch (dt. Auflösung u. a. beim Drucken)
DTW	Dynamic Time Warping (dt. Klassifikator für unterschiedlich lange Sequenzen)
EER	Equal Error Rate (dt. Punkt bei dem FAR und FRR gleich sind)
FAR	False Acceptance Rate (dt. prozentualer Anteil an falsch akzeptierten Personen)
FFT	Fast Fourier-Transformation (dt. schnelle Fourier-Transformation)
FRR	False Rejection Rate (dt. prozentualer Anteil an falsch zurückgewiesenen Personen)
GAR	Genuine Accept Rate (dt. prozentualer Anteil an korrekt zurückgewiesenen Personen)
GPS	Global Positioning System (dt. Globales Positionsbestimmungssystem)
HD	High Definition (hochauflösendes Display)

IBAN	International Bank Account Number
IBk	Instance-Based learner for k (dt. Instanz-basierter Klassifikator)
IEC	International Electrotechnical Commission (dt. Normungsgremium für Elektrotechnik)
ISO	International Organization for Standardization (dt. Internationale Organisation für Normung)
IT	Information Technology (dt. Informationstechnologie)
kNN	k-Nearest-Neighbor (dt. k nächsten Nachbarn - Algorithmus)
LED	Light Emitting Diode (dt. Leuchtdiode)
NLP	Natural Language Processing (dt. Computerlinguistik)
NIST	National Institute of Standards and Technology (dt. Nationales Institut für Standards und Technologie)
OHA	Open Handset Alliance (Konsortium zur Entwicklung offener Standards für mobile Endgeräte)
OLED	Organic Light Emitting Diode (dt. organische Leuchtdiode)
OTP	One Time Password (dt. Einmalpasswort)
PC	Personal Computer (dt. persönlicher Computer)
PIN	Personal Identification Number (dt. (persönliche) Geheimnummer)
PKI	Public Key Infrastructure (dt. Public-Key-Infrastruktur)
PSPP	Open-Source Version von SPSS (Statistical Package for the Social Sciences)

RBFN	Radial Basis Function Network (dt. radiale Basisfunktionsnetzwerk – Klassifikator)
QWERT	Standard Tastaturenlayout
ROC	Receiver Operator Characteristic (dt. Kurve zur Grenzwertoptimierung)
SPSS	Statistical Package for Social Scientists (Statistik- und Analyse-Software)
SVM	Support Vector Machines (dt. Klassifikation basierend auf Stützvektoren)
TAN	Transaction Number (dt. Transaktionsnummer)
Weka	Waikato Environment for Knowledge Analysis (dt. Klassifikationsumgebung)

1 Einleitung

Der Fokus dieser Arbeit liegt auf der biometrischen Authentifizierung anhand des Tippverhaltens mithilfe der in Smartphones verbauten Sensoren. In der Motivation wird dargestellt, weshalb dieses Themenfeld von entscheidender Bedeutung ist. Im Anschluss daran wird das Thema von bisherigen Untersuchungsbereichen abgegrenzt und aufgezeigt, in welches Gebiet diese Forschungsarbeit einzugliedern ist. Die Zielstellung dieser Arbeit und der daraus resultierende Aufbau werden im letzten Abschnitt vorgestellt.

1.1 Motivation

Die Authentifizierung gegenüber digitalen Systemen ist heutzutage ein alltäglicher Prozess. Für eine elektronische Banküberweisung werden Kontonummer (ab 2014: International Bank Account Number (IBAN)), ein geheimes Passwort und eine einmalig verwendbare Transaction Number (TAN) benötigt; Spieler des Online-Rollenspiels „World of WarCraft“ nutzen One Time Password (OTP)-Generatoren, um ihre virtuelle Identität vor Hackern zu schützen; Anmeldungen am E-Mail-Postfach oder an einem Computer benötigen Benutzernamen und Passwort, in einigen Firmen ist darüber hinaus ein Mitarbeiterausweis notwendig. Diese Passwörter sollten einer Richtlinie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) [Bun11a] folgen, die besagt, dass ein Passwort folgende Merkmale aufweisen sollte: eine ausreichende Länge (mindestens acht Zeichen), alpha-numerisch mit Sonderzeichen und nicht im Wörterbuch stehend. Insbesondere bei der Eingabe von Passwörtern in Smartphones sollte diese Richtlinie befolgt werden, da Eingaben selten unbeobachtet durchgeführt werden können [Bun11b, S. 9]. Wenn Wörter als Passwort verwendet werden,

können sich diese schneller gemerkt werden als eine kryptische Zeichenabfolge mit Sonderzeichen. Somit muss ein Angreifer die Eingabe des Passworts mehrfach beobachten, falls ein komplexes Passwort verwendet wird.

Diese Richtlinien für Passwörter werden jedoch aufgrund von zu kurzer Personal Identification Number (PIN)/Passwort oder Standardpasswörtern (wie z. B. die Zeichenfolge 1 bis 6 oder das Wort „Passwort“) oft nicht eingehalten. Besonders durch Techniken, wie der Brute-Force-Methode, bei der alle möglichen Passwörter getestet werden, kann so in kurzer Zeit das richtige Passwort ermittelt werden. Gleichzeitig existieren Verfahren, wie z. B. Shoulder Surfing (über die Schulter schauen bei der Eingabe) oder Social Engineering (Passwort von der Person durch eine geschickte Fragetechnik erfahren [HKNT09]), mit welchen das Passwort herausgefunden werden kann.

Passwörter allein stellen somit keinen ausreichenden Sicherheitschutz dar. Daher werden diese in vielen Firmen mit einem Mitarbeiterausweis mit integriertem Public Key Infrastructure (PKI)-Chip oder einem OTP-Generator kombiniert. Hiermit wird die Sicherheit zwar erhöht, aber das zusätzliche Gerät muss immer mitgeführt werden, wenn die Authentifizierung erfolgen soll. Wird das Gerät vergessen, ist entweder keine Authentifizierung möglich oder nur mit eingeschränktem Zugriff. Jedes zusätzliche Gerät/Karte stellt zugleich ein Platzproblem dar, wodurch die Akzeptanz der Anwender sinken kann.

Für Smartphones werden die dazu genannten Authentifizierungsmethoden nur beschränkt genutzt und meist in Form von: kurzer PIN/Passwort, ein Entsperrmuster oder gar kein Mechanismus. Doch besonders für diese Geräte sollte ein höheres Sicherheitsniveau erreicht werden, das gleichzeitig benutzerfreundlich ist. Dies zeigt z. B., dass 2009 in einem halben Jahr in Londoner Taxis 55.000 Mobiltelefone liegen gelassen wurden [Twe09]. Außerdem hat laut einer Studie des Bundesverbandes Informationswirtschaft, Telekommunikation und Neue Medien (BITKOM) bereits jeder zehnte Deutsche ab 14 Jahren sein Handy schon einmal verloren [BI12]. Zudem können sie sehr schnell und einfach gestohlen werden. Mit der zunehmenden Anzahl an Geräten (bis 2012 wurden insgesamt über eine Milliarde Smartphones

auf der Welt verkauft [Bic12]) wird diese Technologie für Kriminelle immer interessanter und kann, nachdem das Passwort einmal herausgefunden wurde, beliebig oft verwendet werden. Auf Smartphones kann bei Fettrückständen des Fingers auf dem Display durch Betrachtung der spiegelnden Oberfläche auf das Passwort geschlossen werden. Insbesondere durch die gespeicherten Daten (sensible, berufliche Informationen oder intime, private Daten [BI12]) und Zugriffe der Geräte auf entsprechende Systeme, kann ein entsperartes Gerät in falschen Händen erheblichen Schaden anrichten.

Eine Alternative zu den Authentifizierungsgeräten bietet die Nutzung von Biometrie. Die Biometrie beschreibt das Erkennen einer Person anhand von individuellen physischen, chemischen oder verhaltensbasierten Eigenschaften [JFR08b, S. 1]. Dazu gehören u. a. die Erkennung des Benutzers auf Basis des Fingerabdrucks, aber auch die Schrift und Sprache. Vorteil der Biometrie ist, dass sie sich mit dem Benutzer bewegt und somit nicht vergessen werden oder verloren gehen kann. Nachteil ist die nicht hundertprozentige Erkennungsgenauigkeit, daher sollte zudem ein Passwort/PIN eingegeben werden. Ob PIN oder Passwort, bei beiden Authentifizierungsmethoden erfolgt die Eingabe über die Tastatur. Während der Eingabe kann eine Erkennung der Person anhand ihres Tippmusters erfolgen, was als ein biometrisches Charakteristikum definiert werden kann. Jedoch wurde dieses Verfahren bisher nur auf Computertastaturen oder Tastaturen auf einem Handy mit 12-Hardwaretasten analysiert. Für Smartphones mit kapazitivem Display (Displayart, die auf Kapazitätsänderungen reagiert – genauere Beschreibung vgl. Abschnitt 5.2.1) wurden bisher keine Studien durchgeführt. Gleichzeitig beschränkten sich die Auswertungen auf einen Klassifikator, ein Gerät und ein Szenario. Wie benutzerfreundlich und sicher dieses Verfahren ist, wurde hingegen nicht untersucht. Eine Authentifizierung mittels des Tippverhaltens und eines Passwortes kann als 2-Faktor-Authentifizierung gesehen werden und ist somit sicherer als eine 1-Faktor-Authentifizierung mittels Passwort, da nicht automatisch jeder Authentifizierungsversuch erfolgreich ist, selbst bei bekanntem Passwort.

Doch nicht nur die Authentifizierung zum Entsperren eines Gerätes muss berücksichtigt werden. Wird ein Gerät direkt nach der Authentifizierung gestohlen, dann kann diese Person ohne Authentifizierung auf das Gerät zugreifen. Für diesen Fall muss eine Lösung gefunden werden, wie in diesem Szenario eine Identifizierung der Person erfolgen kann.

1.2 Zielstellung der Arbeit

Für das Tippverhalten ergeben sich, wie für alle biometrischen Systeme, eine Reihe von Anforderungen, die das System erfüllen muss. Diese Anforderungen sind *Allgemeingültigkeit*, *Einzigartigkeit*, *Dauerhaftigkeit*, *Messbarkeit*, *Effizienz*, *Akzeptanz* und *Umgehen des Verfahrens* [PPJ03, JBP02, Cla94, IEE10].

Darüber hinaus existieren im Bereich der Smartphones weitere Anforderungen, z. B. dass die Authentifizierung geräteunabhängig, geräteübergreifend, unabhängig und universell anwendbar sein muss. Diese werden in Abschnitt 2.3.1 beschrieben.

Zusätzlich zu diesen Anforderungen muss eine Verringerung der Fehlerraten erfolgen, damit das Authentifizierungsverfahren in Bezug zur Sicherheit und Benutzerfreundlichkeit verbessert wird.

Das Hauptziel dieser Arbeit ist die Prüfung der Authentifizierung mittels des Tippverhaltens auf Smartphones. Damit diese Erkennung durchgeführt werden kann, müssen durch die vorliegende Arbeit die folgenden vier Ziele, die sich aus den Anforderungen ergeben, erreicht werden:

- Es muss eine hohe Sicherheit durch das Verfahren gewährleistet werden, sodass nicht mehr als 3,9 % der Angriffe bei bekanntem Passwort erfolgreich sind. Gleichzeitig darf einem echten Benutzer nur in weniger als 3,9 % der Versuche der Zugriff verweigert werden. Der Wert 3,9 % basiert auf einer in einer skandinavischen Bank eingesetzten Methode [Beh13a], welche im Vergleich zu anderen durchgeführten Untersuchungen (siehe Abschnitt 3.1.1) eine geringe Fehlerrate aufweist und gleichzeitig in der Praxis eingesetzt wird.

- Verschiedene Geräte besitzen Sensoren, die Daten in unterschiedlicher Qualität aufnehmen. Diese Qualitätsunterschiede dürfen die Fehlerraten nicht negativ beeinflussen, sodass keine Authentifizierung mehr möglich ist. Falls doch eine Authentifizierung auf unterschiedlichen Geräten durchführbar sein soll, stellt sich die Frage (die beantwortet werden muss), ob die Merkmalseigenschaften auf ein anderes Gerät übertragen werden können (geräteübergreifende Authentifizierung), ohne dass ein Einfluss auf die Fehlerraten erkennbar ist.
- Das Authentifizierungsverfahren soll nicht nur in klinischen Szenarien (die keine Praxisrelevanz besitzen), z. B. nur im Sitzen, verwendbar sein, sondern auch in verschiedenen Alltagssituationen (u. a. im Gehen oder Stehen), ohne dass sich die Fehlerraten über den Wert 3,9 % vergrößern.
- Es muss ein System für die kontinuierliche Überprüfung des Benutzers des Smartphones generiert werden, welches implizit und transparent agiert. Es soll gezeigt werden, ob biometrische Authentifizierungsverfahren genutzt werden können, die Personen auch während der Nutzung überprüfen. Dabei soll die Fehlerrate unter 7,0 % liegen, die durch ein textunabhängiges Verfahren bereits an Telefonen mit einer Hardwaretastatur erreicht wurde (siehe Abschnitt 3.1.1). Ohne ein solches Verfahren ist die Sicherheit nach der initialen Authentifizierung nicht mehr gegeben. Zusätzlich muss das Lernverhalten betrachtet werden, welches im Laufe der Zeit das Tippverhalten verändert. Es muss geprüft werden, ob das Modell mit den Merkmalen einer Person dauerhaft angepasst werden muss.

1.3 Rahmenbedingungen und Einschränkungen

Neben den Zielen gibt es für die reale Nutzung weitere zu analysierende Punkte, die jedoch in dieser Arbeit nicht betrachtet werden:

Rechtliche Grundlagen: Die Dissertation soll die wissenschaftliche und technische Durchführbarkeit eines solchen Verfahrens darstellen.

Daher wird auf die rechtlichen Grundlagen, insbesondere das Speichern von personenbezogenen Daten, nicht eingegangen. Dies stellt ein allgemeines Problem aller biometrischer Verfahren dar und muss an anderer Stelle verallgemeinert betrachtet werden.

Akzeptanz des Verfahrens: Die Akzeptanz gegenüber dem Verfahren wird nicht betrachtet. Es wird vom Einverständnis der betreffenden Personen ausgegangen, ihr Tippverhalten aufzunehmen. Zudem kann z. B. die Nutzung von der Leitung eines Unternehmens vorgeschrieben werden (Corporate Environment), eine persönliche Akzeptanz ist dann für die Nutzung nicht Voraussetzung.

Angriffsmodalitäten: Angriffsmodalitäten, die auf Schnittstellen zu anderen Bereichen (z. B. Benutzeroberfläche oder Datenbank) basieren, wurden bereits bei mehreren biometrischen Authentifizierungsverfahren analysiert [JNN08]. Daher werden die Schnittstellen in dieser Arbeit nicht weiter adressiert.

Lauffähiges Design auf dem Smartphone: Die Arbeit stellt ein Konzept mit teil-automatisierten Prozessen dar. Es sollen lediglich Funktionsweisen verglichen und bewertet werden. Die Entwicklung eines lauffähigen Prototyps ist nicht angedacht.

Weitere Sicherheitsmechanismen: Antivirus-Software bzw. gehärtete Betriebssysteme sind neben der Authentifizierung essentiell für die Sicherheit von Smartphones wichtig, stehen aber nicht im Fokus dieser Arbeit.

1.4 Struktur der Arbeit

Die nachfolgende Abbildung 1.1 stellt den strukturellen Aufbau der vorliegenden Arbeit dar.

Die Heranführung an das Thema ist im Rahmen der Motivation und der Abgrenzung des Untersuchungsbereiches sowie der Einordnung der Forschungsarbeit in Kapitel 1 gegeben. Um die dort präsentierten