AutoUni – Schriftenreihe

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 knew 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

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

Tabellenverzeichnis

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,

M. Trojahn, *Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens*, AutoUni – Schriftenreihe 85,
DOI 10.1007/978-3-658-14049-6_1

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 Sicherheitsschutz 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 entsperrtes 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