BioMe – Kontinuierliche Authentifikation mittels Smartphone

Marlies Temper · Manfred Kaiser

Fachhochschule St. Pölten – Institut für IT Sicherheitsforschung
vorname.nachname@fhstp.ac.at

Zusammenfassung

Die steigende Verfügbarkeit von Smartphones (über 3,3 Milliarden im Jahr 2016) führt dazu, dass unsere tägliche Kommunikation weitgehend über diese technischen Begleiter stattfindet. Die einzige Möglichkeit Daten vor Unbefugten zu schützen, besteht darin, eine PIN, ein Passwort oder Muster zu verwenden. Dazu wird in diesem Beitrag eine alternative multimodale biometrische Authentifizierungsmethode BioMe vorgestellt, die kontinuierlich Daten von mobilen Endgeräten sammelt und charakteristische Merkmale extrahiert, um das eindeutige Verhalten von autorisierten BenutzerInnen zu erlernen. Ein personenspezifisches dynamisches Verhaltensmuster wird anhand des Bewegungsmusters bei der Bedienung mobiler Endgeräte generiert. Dabei werden typische Bewegungen wie die Geräteführung, Gesten (z.B. „Wischen“) sowie das Tippverhalten berücksichtigt. Mithilfe dieses Systems soll auch eine auf Biometrie basierende Datenauthentifizierung, die z.B. beim Telebanking/Netbanking ein Sicherheitsproblem darstellt, möglich sein. Damit kann z.B. das schon bekannte mTAN-Verfahren durch eine biometrische Komponente sicherheitstechnisch verbessert werden. Das multimodale Verfahren schafft es autorisierte Personen bis zu 100% kontinuierlich zu erkennen, auch 8 von 10 Angreifer werden als solche erkannt und ausgesperrt. Das Verfahren wurde mit Hilfe von 20 ProbandInnen getestet.

1 Einleitung

Mobile Endgeräte begleiten uns mittlerweile auf all unseren Wegen. Sie sind unsere ständigen Begleiter, Informanten, Datenspeicher und unsere tägliche Kommunikation findet über diese statt. Aber nicht nur im privaten Umfeld sind diese technischen Hilfsmittel nicht mehr wegzudenken. Der Begriff ‚Bring Your Own Device‘ (BYOD) kam erstmals 2009 auf und ist die Bezeichnung dafür, private mobile Endgeräte in die Netzwerke von Unternehmen oder Institutionen zu integrieren. BenutzerInnen wollen kaum mehr auf ihre Geräte verzichten und Unternehmen sind gezwungen darauf zu reagieren, besonders da BYOD für Organisationen ein hohes Sicherheitsrisiko darstellt. Firmeninterne, sensible Daten befinden sich auf nicht- oder nur teilweise kontrollierbaren, fremden Geräten. Bei Verlust kann dies zu schwer abschätzbaren Konsequenzen führen. Daher wird eine sichere Authentifizierung immer wichtiger.

Derzeitige Schutzmechanismen wie eine PIN, Passwort oder Mustereingabe stellen dabei keinen adäquaten Schutz dar. Wenn die anfängliche Eingabe dieses Sicherheitsfeatures überhaupt aktiviert ist, zeigt die Arbeit von Aviv et al. [AGMB10], dass es Angreifern problemlos möglich ist, diese zu umgehen. Unter Schmierattacken (Smudge-Attack) versteht man, dass Fettrückstände bei der Eingabe von z.B. PINs zurückbleiben und unter geeigneten Lichtverhältnissen und mittels Kameras detektiert werden können. Nach einer erfolgreichen

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 61-71.

Authentifizierung haben Angreifer uneingeschränkten Zugriff auf alle am mobilen Endgerät befindlichen Daten.

Eine Alternative zu herkömmlichen Authentifizierungsmaßnahmen stellen biometrische Verfahren dar. Zu den wohl bekanntesten biometrischen Merkmalen gehören Fingerabdruck, Gesicht und Iris. Dass biometrische Merkmale wie der Fingerabdruck zur Anmeldung bei Smartphones herangezogen werden können, hat Apple als Pionier gezeigt. Seit dem iPhone 5s [Apple14] ermöglicht der Touch ID Sensor im Home-Button die Aufnahme des Fingerabdrucks, auch wenn dies zu anfänglichen Problemen führte, da es zu einer Überlistung des Sensors kam.

Der in diesem Beitrag vorgestellte Ansatz schlägt einen anderen Weg ein. In der Biometrie unterscheidet man zwischen physiologischen und verhaltensbasierten Merkmalen. [NSTC06] Unter physiologischen Merkmalen versteht man körperliche Charakteristika wie Fingerabdruck, Irismuster, Handvenenmuster oder das Gesicht. Dem gegenüber beschreiben verhaltensbasierte biometrische Merkmale das Verhalten von Personen z.B. Gang oder das Tippverhalten. Zu den sichersten biometrischen Verfahren zählen ohne Zweifel körperliche Besonderheiten.

Die Stärke des in diesem Beitrages vorgestellten Verfahrens liegt darin unterschiedliche verhaltensbasierte Charakteristika einer Person heranzuziehen und dadurch ein eindeutiges Profil zu erstellen, um dieses am mobilen Endgerät zu hinterlegen. Durch einen kontinuierlichen Abgleich kann ein Smartphone entscheiden, ob es sich um seinen Besitzer/seine Besitzerin handelt oder nicht. Moderne mobile Geräte liefern dafür das notwendige Werkzeug. Sie besitzen neben einen Touchscreen unter anderem einen digitalen Kompass, Beschleunigungssensor, Näherungssensor, Umgebungslichtsensor, Gyroskop, Barometer, GPS oder Magnetometer [LMPC10]. Die Daten, die über diese Sensoren erfasst werden, werden herangezogen, um ein eindeutiges menschliches Profil zu erstellen. Im Rahmen des Beitrages wird ein kontinuierliches Authentifizierungsverfahren vorgestellt, das auf Fuzzy Set Theorie und einem Scoring Modell basiert und Touchbewegungen, Geräteführung und das Tippverhalten der Smartphonebenutzung heranzieht, um zu entscheiden, ob es sich um den/die legitime/n BenutzerIn handelt. Das Verfahren wurde mit einer selbst entwickelten Banking-App getestet, um seine Einsetzbarkeit zu zeigen.

2 Stand der Technik

Der Trend zur kontinuierlichen Authentifizierung steigt. Juni 2015 stellt Google sein zukünftiges Projekt Abacus [Heise15] vor, das Passwörter durch eine kontinuierliche Nutzeranalyse ersetzen will. Dabei soll das Schreibverhalten, sowie eine Analyse zur Verwendung von Apps mit einer Gesichts- und Spracherkennung kombiniert werden.

Aber auch andere wissenschaftliche Projekte befassten sich schon mit dieser Thematik. In [JSGC09] [SNJC11] wird ein Authentifizierungsverfahren vorgestellt, das unsichtbar im Hintergrund läuft. Benutzermodelle werden basierend auf Verhaltensmuster gebildet. Die Autoren verwenden ein Scoring-Modell, um die Wahrscheinlichkeit zu errechnen, dass das Mobiltelefon in den Händen eines berechtigen Benutzers/einer berechtigen Benutzerin ist. Dafür wurden Informationen aus folgenden Interaktionen mit einem Blackberry extrahiert: Email, Telefonate, SMS, Location, Kalender, Batteriestand, usw. Die Autoren testeten ihr Verfahren mit 50 ProbandInnen. Sie schafften es, dass ein autorisierter Benutzer/eine autorisierte Benutzerin das mobile Gerät im Durchschnitt 100 Mal verwenden kann, ohne dass

er/sie versehentlich als Angreifer detektiert und dadurch ausgesperrt wird. Mit dieser Einstellung können aber nur 50% der Angreifer als solche erkannt werden.

SenSec [ZWWZ13] ist ebenfalls ein Framework, das es erlaubt den Beschleunigungssensor, Gyroskop, Orientierungssensor und das Magnetometer heranzuziehen und ein Modell von BenutzerInnen zur Authentifizierung bzw. Anomaliedetektion zu generieren. K-means Clustering wird verwendet, um ein n-gram Language Model zu generieren. SenSec erzielt bei der Benutzerklassifizierung eine Erkennungsrate von 75%, bei der Detektion von Angreifern eine Erkennungsrate von 71,3%. Um das Framework zu evaluieren wurden 20 ProbandInnen eingeladen.

SenGuard [SYJY11] ist ein System, das eine kontinuierliche Identifizierung von mobilen EndgerätebenutzerInnen ermöglicht. Dafür werden biometrische Merkmale wie Stimme, Location, Multitouchgesten und Bewegung aufgezeichnet.

Saevanee et al. [SaBh08] [SaBh09] untersuchten die Machbarkeit das Tippverhalten, Stimme und Interaktionsmuster zur kontinuierlichen Authentifikation zu verwenden. Zur Analyse der Daten wurde ein Feed-Forward Multilayer Perception Neural Network entwickelt und in einer Arbeit von Saevanee eine durchschnittliche EER von 3,3% [Saev14] erreicht.

Giuffrida et al. [GMCB14] stellen ein weiteres multimodales Verfahren vor und verwenden neben dem Tippverhalten auch Informationen, die der integrierte Beschleunigungssensor und das Gyroskop liefern. Daten, die durch die Eingabe von vordefinierten Passwörtern von ProbandInnen eingegeben werden, werden kombiniert, um Merkmalsvektoren für den Vergleich bereitzustellen. One-class SVM, Naive Bayes, k-NN und eine Methode, die in der Publikation 'mean algorithm' genannt wird, werden verwendet, um die Merkmalsvektoren zu klassifizieren. Zur Distanzberechnung werden die Euklidische, normalisierte Euklidische, Manhattan, skalierte Manhattan und die Mahalanobis-Distanz eingesetzt. Sie erreichten eine EER von 0,08% bei der Verwendung von 0,5-Graphs und Bewegungsinformationen. Das beste Ergebnis lieferte k-NN mit k=1.

Im Gegensatz zu den hier vorgestellten Arbeiten, haben wir uns einem bestimmten Szenario, dem Telebanking gewidmet. Durch Beobachtung konnte festgestellt werden, dass sich verhaltensbasierte Merkmale wie das Tippverhalten, die Gerätehaltung und die Eingabe von Touchbewegungen für unser Szenario als günstig erweisen, um Personen zu authentifizieren. Weiters sehen wir unser Verfahren als zusätzlichen Sicherheitsmechanismus zur Eingabe von Benutzerdaten oder TANs an, um eine höhere Sicherheit zu bieten und nicht als alleinigen Schutz vor Missbrauch. Unser multimodales Verfahren analysiert die Banking-App kontinuierlich und überprüft ununterbrochen, ob es sich um den berechtigten Benutzer/die berechtigte Benutzerin handelt oder nicht.

3 Architektur

BioMe agiert unbemerkt im Hintergrund einer Smartphone Applikation. Zu Testzwecken wurde eine Applikation entwickelt, die dem Layout einer Banking-App angelehnt ist, siehe Abbildung 1. Nach dem erfolgreichen Login mittels Verfügernummer und PIN, können Buchungen kontrolliert oder Überweisungen getätigt werden. Diese Applikation ermöglicht eine kontrollierte Umgebung, um ProbandInnen in mehreren Sessions unterschiedliche Aktionen durchführen zu lassen.

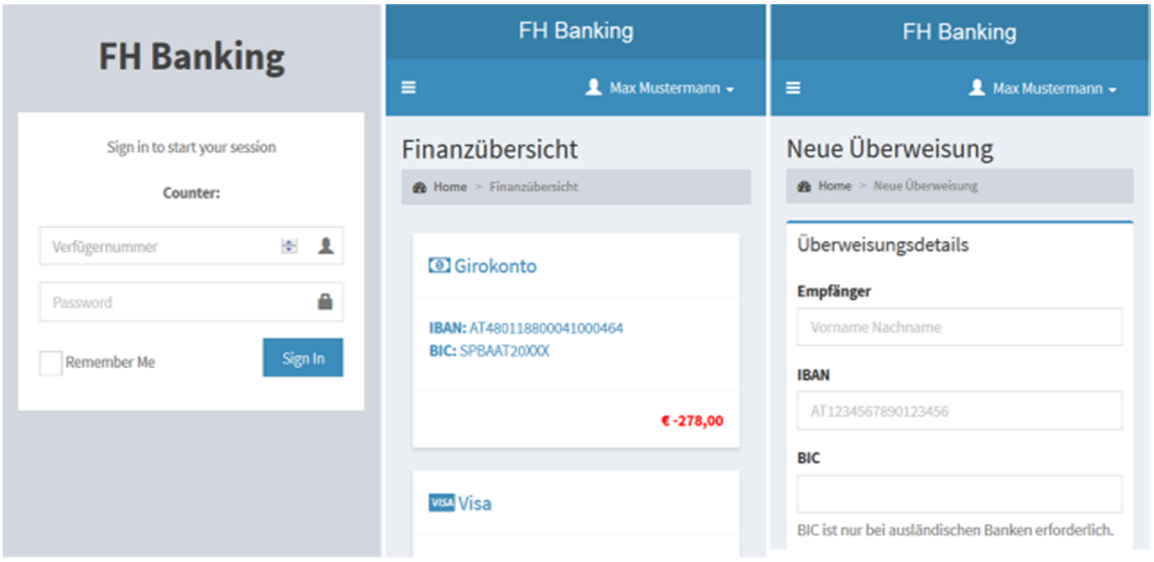

Abb. 1: Banking App

Die Stärke dieses Beitrages liegt im experimentellen Setup. Verwandte Arbeiten verzichten teilweise auf einen längeren Zeitraum der Datenaufnahme [AnWä13] [LHB12] [TrOr12]. Bei der in diesem Beitrag vorgestellten Datenerhebung wurde darauf geachtet ProbandInnen über einen längeren Zeitraum aufzunehmen, um unterschiedliche Gemütszustände oder Veränderungen im Verhalten durch Anpassung an das Szenario bzw. das Erlernen des Umgangs mit dem Smartphone und der App zu berücksichtigen. Insgesamt wurden 20 Freiwillige für insgesamt 30 Sessions gewonnen. Diese 30 Sessions fanden innerhalb von 2 Wochen statt. Ihre Aufgabe bestand darin, sich mit einer 6-stelligen Verfügernummer und einem 7-stelligen alphanumerischen Passwort anzumelden. Es besteht eine weitere Anmeldemöglichkeit in Form eines Musters, das ebenfalls eingegeben werden musste. Weiters wurden die ProbandInnen gebeten, sowohl die Kontostände des Giro- als auch des Kreditkartenkontos zu überprüfen. Die Beträge der Ausgaben ändern sich laufend, um das Szenario interaktiver zu gestalten und eine Gewöhnung zu umgehen. Zusätzlich mussten Überweisungen getätigt werden. Benutzerinteraktionen variieren, sei es durch Müdigkeit, Freude oder Zorn. Fühlten sich die ProbandInnen am Morgen noch frisch, sah man in den aufgenommen Daten gegen Spätnachmittag oder Abend eine Veränderung der Verhaltensmuster. Daher war es besonders wichtig die Sessions an unterschiedlichen Tagen und Zeitpunkten durchzuführen und ein Verfahren zu entwickeln, das flexibel genug ist, mit Variationen umzugehen.

Während der Benutzung der BioMe Banking-App, werden das Tippverhalten, Touchbewegungen, sowie die Geräteführung zu bestimmten Zeitpunkten (z.B. Drücken des Speichern-Buttons) erfasst. Aus den Rohdaten werden anschließend charakteristische Merkmale extrahiert und mit bereits gespeicherten biometrischen Templates des Benutzers/der Benutzerin verglichen. Der Matchingoutput wird für jede Aktion (Anschlag einer Taste, eine Wischbewegung, Winkel des Mobiltelefons beim Drücken des OK-Buttons) errechnet und nimmt einen Wert zwischen 0 und 1 an. Je näher der Wert bei 1 ist, desto wahrscheinlicher handelt es sich um den berechtigten Benutzer/die berechtigte Benutzerin. Um nun eine kontinuierliche Verifikation zu gewährleisten, werden die Matchingoutputs herangezogen, um einen Trust Score zu bilden. Die Berechnung des Trust Scores orientiert sich an der Arbeit von Deutschmann et al. [DNN13]. Der Prozess wird in Abbildung 2 visualisiert.

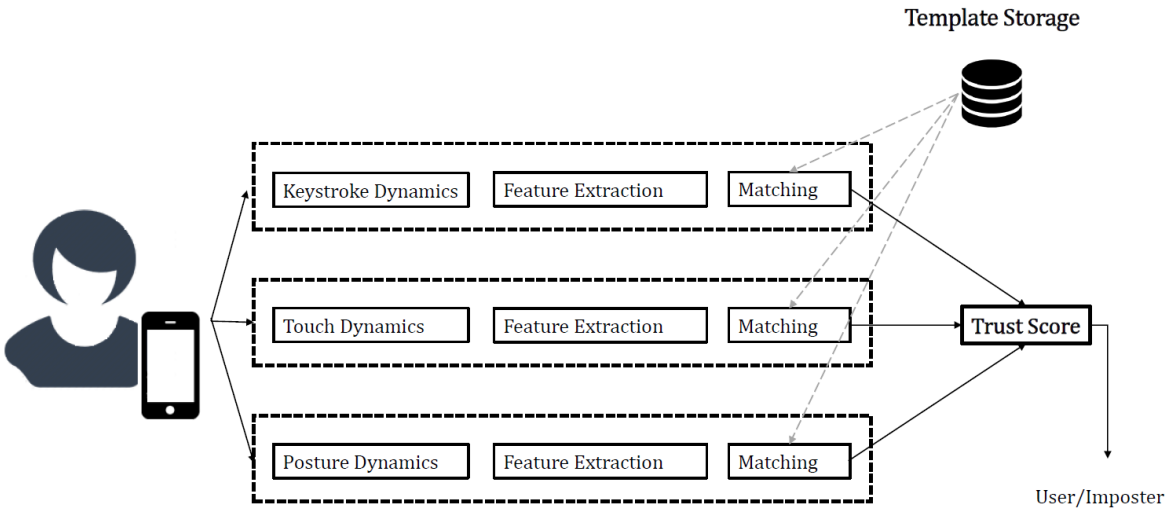

Abb. 2: Übersicht des Authentifizierungsprozess

Die beschreibenden Charakteristika, die beim Tippen, bei Touchbewegungen und der Geräteführung extrahiert werden, unterscheiden sich wesentlich. Eine Wisch- oder Zoomgeste besitzt andere Eigenschaften als das Schreiben eines Textes.

Während beim Tippen der Benutzer/die Benutzerin schnell hintereinander und kurz auf das Display tippt, wird zum Beispiel bei einer Wischgeste der Finger über einen längeren Zeitraum über das Display geführt. Bei den meisten mobilen Geräten erfolgt die Eingabe von Texten über eine virtuelle Tastatur. Alternative Eingabeformen können mit Hilfe eines Stiftes und entsprechender Handschrifterkennung erfolgen. Jedoch hat sich in der Praxis gezeigt, dass die Eingabe von Texten auf Geräten, die keinen Digitizer besitzen, zu einem unnatürlichen Schreibverhalten führt und dadurch von BenutzerInnen nicht gut angenommen wird. Aus diesem Grund ist die primäre Eingabeform auf mobilen Endgeräten immer noch die virtuelle Tastatur, die auch in unserer Applikation neben dem Touchscreen und dem Beschleunigungssensor als Aufnahmesensor dient.

Um die Eingabe von Texten zu erleichtern besitzen virtuelle Tastaturen eine Autokorrektur, um falsch geschriebene Wörter zu ersetzen. Dadurch ist es nicht mehr notwendig ein Wort richtig zu schreiben und die entsprechenden Buchstaben zu treffen, weil kleine Fehler automatisch korrigiert werden. In unserer Implementierung wurde aber auf dieses Feature verzichtet.

Während des Tippens generiert die virtuelle Tastatur einen Event, der von der BioMe-Applikation verwendet wird, um charakteristische Merkmale über das Tippverhalten zu berechnen. Die Tastatur liefert unter anderem die Koordinaten eines Touchevents, den KeyCode (Angabe welcher Buchstabe gedrückt wurde) und den Fingerdruck. Um keine sensiblen Eingaben rekonstruieren zu können, wird in der BioMe-App darauf verzichtet den KeyCode und die Koordinaten mitzuprotokollieren oder zu speichern. Generische Charakteristika werden berechnet und als biometrische Templates hinterlegt. Diese bieten keinen Rückschluss auf den vorher geschriebenen Text.

Zu den von BioMe berechneten Charakteristika des Tippverhaltens zählen die Dwell-Time und Flight Time. Darunter versteht man einerseits wie lange eine Taste gedrückt wurde sowie die Dauer zwischen dem Drücken der ersten und einer zweiten Taste. Zusätzlich wird der durchschnittliche Druck pro Taste ermittelt, die durchschnittliche Auflagefläche des Fingers beim Drücken einer Taste sowie die Geschwindigkeit von Texteingaben. Eine Herausforderung

bei der Analyse des Tippverhaltens stellt die Eingabe von Sonderzeichen bzw. Zahlen dar, da diese meist einen längerer Druck auf einen Buchstaben verlangen, um anschließend das gewünschte Zeichen zu verwenden. Da diese Tasten den normalen Tipprhythmus beeinflussen, werden diese zur Authentifizierung nicht herangezogen. Evaluierungen haben zusätzlich gezeigt, dass die Erkennungsrate steigt, wenn mehrere Buchstaben zusammengefasst und als Template hinterlegt werden, als wenn jeder Tastenanschlag separat betrachtet wird. Ein weiterer Vorteil mehrere Tastenanschläge zu verwenden und damit Durchschnittscharakteristika zu bilden ist, dass sich wirklich keine Informationen mehr über bestimmte Texteingaben in biometrischen Templates befinden.

Um die Erkennungsrate bei der Klassifikation von Gesten zu steigern, hat sich eine Vorklassifikation dieser anhand ihrer Bewegungsrichtung als günstig erwiesen. Dafür wird eine Toucheingabe in eine von acht Sektoren je nach Bewegungsrichtung eingeteilt, siehe Abbildung 3. Die Einteilung in insgesamt acht Sektoren wurde bewusst gewählt. Die Touchgeste in der Abbildung würde als Nord-Ost Sektor vorklassifiziert werden Bei einer Unterteilung in weniger Sektoren, können diagonale Bewegungen nicht von horizontalen bzw. vertikalen Bewegungen unterschieden werden, bei mehr als acht Klassen wären wesentlich mehr Templates pro Klasse notwendig, damit eine Klassifikation aussagekräftig bleibt.

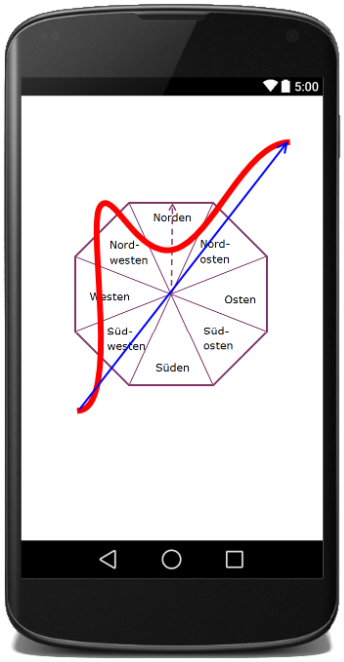

Abb. 3: Sektoreneinteilung von Touchbewegungen

Nach einer Vorklassifizierung werden folgende Charakteristika zur Beschreibung von Touchgesten extrahiert: Distanz zwischen Anfang und Ende einer Bewegung, (minimaler, maximaler und durchschnittlicher) Fingerdruck, (minimale, maximale und durchschnittliche) Auflagegröße des Fingers, Zeit, Geschwindigkeit und Startwinkel der Touchbewegung.

Die Länge bzw. Distanz der Touchbewegung kann auf zwei Arten bestimmt werden. Die erste Möglichkeit ist die tatsächlich zurückgelegte Distanz, die Zweite ist die kürzeste Distanz. Als Merkmal für die Erstellung eines Templates ist die zurückgelegte Distanz interessanter, da in Verbindung mit der vergangenen Zeit die Geschwindigkeit der Fingerführung berechnet werden kann.

Zusätzlich wird aus den Daten, die der Beschleunigungssensor liefert der Haltungswinkel des mobilen Gerätes zu bestimmten Zeitpunkten wie beim Drücken von Tasten berechnet.

All diese Informationen werden als biometrische Templates hinterlegt und bei jeder neuen Eingabe ein Merkmalsvektor generiert. Dieser wird einem Fuzzy Rough Klassifizierer übergeben. Um genau zu sein, verwendet BioMe den Vaguely Quantified Nearest Neighbours (VQNN) Klassifizierer [JeCo08] [JeCo11a] [JeCo11b]. Dieser stellt eine Kombination aus bekannten k-Nearest Neighbour (k-NN) Klassifizierern dar und der Fuzzy Rough Set Theorie. Das Konzept der nächsten Nachbar-Klassifikation wird dabei herangezogen, um Entscheidungsklassen zu bilden, die von Fuzzy-Grenzen umgeben sind. Neue Daten werden anhand einer Zugehörigkeitsfunktion $R_a(x, y)$ einer Klasse zugeordnet. Die Zugehörigkeitsfunktion gibt den Grad der Ähnlichkeit von Attributen a des Merkmalsvektors x und eines neu zu klassifizierenden Merkmalsvektor y an.

$$R_a(x, y) = 1 - \frac{|a(x) - a(y)|}{|a_{max} - a_{min}|}$$

VQNN verwendet Fuzzy-Quantifizierer, um Unschärfe zu modellieren und dadurch obere und untere Klassengrenzen zu berechnen:

$$(R \downarrow A)(y) = Q_u\left(\frac{|R_y \cap A|}{|R_y|}\right) = Q_u\left(\frac{\sum \min(R(x, y), A(x))}{\sum R(x, y)}\right)$$

$$(R \uparrow A)(y) = Q_l\left(\frac{|R_y \cap A|}{|R_y|}\right) = Q_l\left(\frac{\sum \min(R(x, y), A(x))}{\sum R(x, y)}\right)$$

Wie bereits oben erwähnt, erhält man nach Übergabe eines Merkmalsvektors an den VQNN einen Wert zwischen 0 und 1, der die Zugehörigkeit des Merkmals zu einer Klasse beschreibt. Dieser Wert wird danach einem Trust Score [DNN13] übergeben, der eine kontinuierliche Authentifikation ermöglicht.

4 Ergebnisse

Um die BioMe App zu evaluieren wurden insgesamt 20 ProbandInnen unterschiedlichen Alters (zwischen 15 und 60 Jahren) und unterschiedlicher demographischer Herkunft zu unterschiedlichen Sessions eingeladen. Diese wurden gebeten vordefinierte Szenarien auszuführen, z.B. eine Überweisung an ein Schlosshotel inkl. Ausfüllen eines IBANs, BICs, Betrags und Verwendungszweckes. In jeder Session wurden anderen EmpfängerInnen Geldbeträge überwiesen. Zusätzlich mussten sie ihren Kontostand überprüfen und Muster zur Entsperrung eines Bildschirmes eingeben. Die ersten zehn Sessions eines jeden Benutzers / einer jeden Benutzerin wurden als biometrisches Template hinterlegt. Anschließend konnte der Trust Score jeder weiteren Session kontinuierlich in Echtzeit berechnet werden. Zusätzlich wurden ProbandInnen gebeten als Angreifer zu fungieren. Sobald ein fremder Benutzer / eine fremde Benutzerin das Handy verwendete, fiel der Trust Score rapide ab. Der Trust Score kann individuell durch das Setzen von Parameter verändert werden. Das bedeutet, dass in unserer derzeitigen Implementierung dieser einen Wert zwischen 0 und 100 einnimmt. Bei jeder Eingabe sei es durch Tippen oder durch eine Touchbewegung kann der Trust Score maximal um den Wert 1 sinken oder steigen. Dies kann durch das Ändern einer Konstanten verschärft werden. Das bedeutet, dass ein stärkeres Steigen oder Sinken möglich ist, um Falschklassifikationen noch mehr zu bestrafen. Derzeit wurde der Schwellwert auf 55 gesetzt.

Sobald der Schwellwert diesen Wert unterschreitet, wird der Benutzer / die Benutzerin gesperrt. Beim Öffnen der App, ist der Wert des Trust Scores standardmäßig auf 60 gesetzt. In Abbildung 4 wird exemplarisch ein Trust Score von zwei autorisierten BenutzerInnen dargestellt.

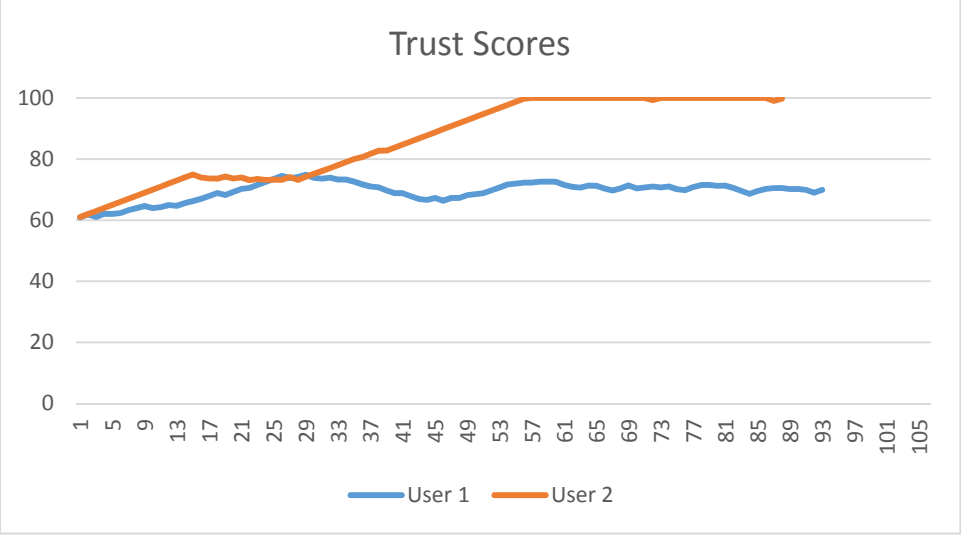

Abb. 4: Trust Scores von zwei autorisierten BenutzerInnen

In Abbildung 5 sieht man wie der Trust Score bei Angriffen während einer Session sinkt. Es muss erwähnt werden, dass sich die Eingabedaten während des Telebankings ständig ändern und nie gleich sind. Das bedeutet, dass es BioMe schafft, Personen auch anhand von vorher unbekannten Textpassagen zu authentifizieren.

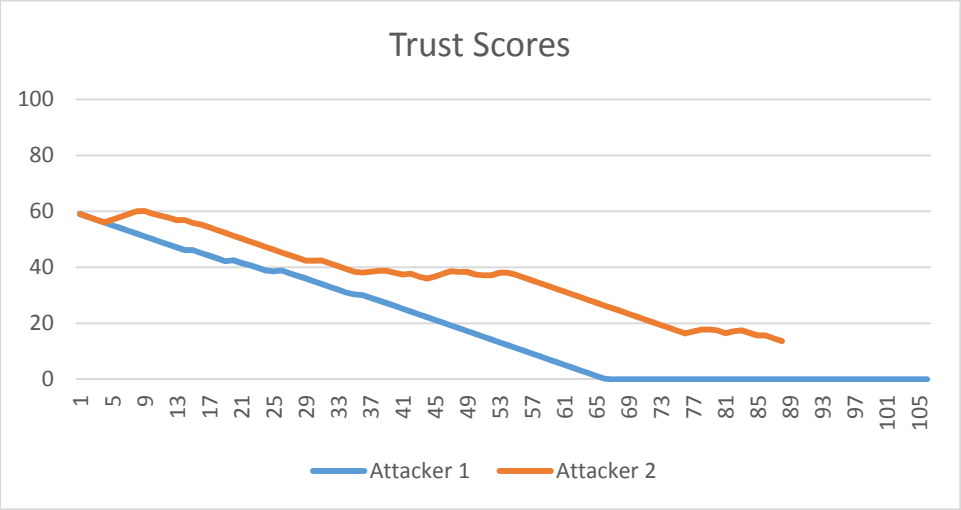

Abb. 5: Trust Scores bei Angriffen

Zur kontinuierlichen biometrischen Benutzerauthentifizierung mittels BioMe-App müssen insgesamt Templates zweier Klassen erstellt werden. Klasse 1 beinhaltet das Benutzertemplate, Klasse 2 das generische Profil von möglichen Angreifern. In der derzeitigen BioMe Version müssen die beiden Klassen manuell angelegt werden. Eine automatische Generierung ist aber zukünftig geplant. BioMe erreicht eine Erkennungsrate von 100%, alle 20 Personen konnten kontinuierlich nach dem Training mit den ersten 10 Sessions erkannt werden. Hier muss aber

zusätzlich gesagt werden, dass BioMe die Templates in regelmäßigen Abständen aktualisiert, um die Erkennungsrate zu gewährleisten.

Jeder Benutzer / Jede Benutzerin fungierte zusätzlich bei anderen Personen als Angreifer. Im Durchschnitt konnten 8 von 10 BenutzerInnen erfolgreich als Angreifer vom System identifiziert werden. Die Ergebnisse zeigen, dass unsere Methode einen vielversprechenden Sicherheitsmechanismus darstellt. Es ist festzuhalten, dass eine kontinuierliche Authentifikation nicht als alleiniger Sicherheitsmechanismus eingesetzt werden kann, da 20% aller Angriffe nicht erkannt werden. In Kombination mit Verfügernummer und Passwort oder mTANs kann es aber zu zusätzlicher Sicherheit verhelfen. Weiters gewöhnten sich die ProbandInnen an die Eingabe ihrer Verfügernummer und ihres Passwortes. Kommt ein Angreifer in den Besitz fremder Zugangsdaten, ist der Eingaberhythmus anfänglich ein komplett anderer, da eine Gewöhnung noch nicht erfolgte. Ein erfolgreich erkannter Angreifer konnte im Durchschnitt nach 9 Text- bzw. Toucheingaben ausgeschlossen werden.

5 Lessons Learned

In diesem Beitrag wird gezeigt, dass kontinuierliche Authentifizierung auf mobilen Endgeräten möglich ist. Probleme, die sich speziell bei einer Implementierung von multimodaler verhaltensbasierter Biometrie in einer Banking-App ergeben haben, sind, dass das Verhalten beim Online-Banking von ProbandInnen sehr variabel ist. Gerade die Eingabe von IBANs und BICs beeinflusst das natürliche Tippverhalten von Personen enorm. Durch das Abtippen von langen Zahlenreihen, wird deren natürlicher Rhythmus gestört. ProbandInnen halten gerade bei der Eingabe von IBANs überdurchschnittlich oft inne und kontrollieren diese nach. Ein Auslassen der Überprüfung besonders bei diesen Fällen kann die Erkennungsrate steigern. In unserer Implementierung haben wir es durch das Eliminieren besonders langer Pausen geschafft, diese Einflüsse zu verhindern. Zusätzlich hat sich gezeigt, dass biometrische Templates regelmäßig erneuert werden sollten. Dadurch kann auf Anpassungen und Erlernen des Umganges mit dem mobilen Endgerät reagiert werden. Die Implementierung von zusätzlichen Klassifikationsregeln wie der Vorkategorisierung von Touchbewegungen hat ebenfalls dazu beigetragen die Erkennungsrate zu erhöhen.

Zusätzlich muss man sich mit den sozialen Kosten und Nebenwirkungen dieser Technologie mit möglicherweise anfallenden ökonomischen, sozialen und Opportunitätskosten beschäftigen, um datenschutzrechtliche Aspekte zu berücksichtigen. Verhaltensbasierte Biometrie auf mobilen Endgeräten ist eine kostengünstige Variante zur Implementierung eines zusätzlichen Sicherheitsmechanismus, da bereits alle Sensoren mit dem Gerät mitgeliefert werden. Weiters sind keine wissentlichen Interaktionen von BenutzerInnen notwendig im Gegensatz zu anderen biometrischen Merkmalen wie der Gesichts- oder der Fingerabdruckerkennung. Es wurde auf folgende datenschutzrechtliche Aspekte bei der Entwicklung der BioMe-App geachtet. Es wurde auf die zusätzliche Erhebung von verhaltensbasierten Charakteristika durch Sensoren wie GPS oder WLAN verzichtet, um BenutzerInnen zu erkennen. Ein Trackingprofil von Personen wird somit nicht angelegt. BioMe läuft nur im Hintergrund einer Applikation ab und schützt damit nur diese. Ein Zugriff auf andere Apps oder Telefondaten findet nicht statt. Bei der Erhebung der Daten zur Authentifizierung wird darauf geachtet, nicht auf einzelne Eingaben zurückschließen zu können. Bei Texteingaben werden weder KeyCode einer Tasteneingabe noch die Koordinaten mitgespeichert, auch bei Touchgesten werden nur generische Charakteristika gespeichert, da

detailliertere Informationen für den weiteren Verlauf nicht relevant sind. Damit wurde versucht, anfallende ökonomische, soziale und Opportunitätskosten so gering wie möglich zu halten.

Literatur

[AGMB10] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, J. M. Smith, „Smudge Attacks on Smartphone Touch Screens“, in Proceedings of the 4th USENIX Conference on Offensive Technologies, 2010.

[AnWä13] J. Angulo, E. Wästlund, „Exploring touch-screen biometrics for user identification on smart phones“, in Privacy and Identity Management for Life, Springer, pp. 130-143, 2013.

[Apple14] Apple Inc., iPhone 5s: About Touch ID security, 2014.

[DNN13] I. Deutschmann, P. Nordstrom, L. Nilsson, „Continuous Authentication Using Behavioral Biometrics“, IT Professional, Bd. 15, Nr. 4, pp. 12,15, 2013.

[GMCB14] C. Giuffrida, K. Majdanik, M. Conti, H. Bos, „I Sensed It Was You: Authenticating Mobile Users with Sensor-Enhanced Keystroke Dynamics“, Lecture Notes in Computer Science on Detection of Intrusions and Malware, and Vulnerability Assessment, Bd. 8550, pp. 92-111, 2014.

[Heise15] heise Security, „Google Project Abacus: Nutzeranalyse statt Passwort“, 2015.

[JeCo08] R. Jensen, C. Cornelis, „A New Approach to Fuzzy-Rough Nearest Neighbour“, Lecture Notes in Computer Science, Bd. 5306, p. 310–319, 2008.

[JeCo11a] R. Jensen, C. Cornelis, „Fuzzy-rough nearest neighbour classification and“, Theoretical Computer Science, Bd. 412, Nr. 42, p. 5871–5884, 2011.

[JeCo11b] R. Jensen, C. Cornelis, „Fuzzy-rough nearest neighbour classification“, Transactions on rough sets XIII, p. 56–72, 2011.

[JSGC09] M. Jakobsson, E. Shi, P. Golle, R. Chow, „Implicit Authentication for Mobile Devices“, in Proceedings of the 4th USENIX Conference on Hot Topics in Security, 2009.

[LHB12] A. De Luca, A. Hang, F. Brudy, „Touch me once and i know it's you!: implicit authentication based on touch screen patterns“, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2012.

[LMPC10] N. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury und A. Campbell, „A survey of mobile phone sensing“, IEEE Communications Magazine, Bd. 48, Nr. 9, pp. 140-150, 2010.

[NSTC06] NSTC Subcommittee on Biometric, „Biometrics Glossar“, 2006.

[SaBh08] H. Saevanee, P. Bhatarakosol, „User Authentication Using Combination of Behavioral Biometrics over the Touchpad Acting Like Touch Screen of Mobile Device“, in International Conference on Computer and Electrical Engineering (ICCEE'08), 2008.

[SaBh09] H. Saevanee, P. Bhattarakosol, „Authenticating User Using Keystroke Dynamics and Finger Pressure“, in 6th IEEE Consumer Communications and Networking Conference (CCNC'09), 2009.

[Saev14] H. Saevanee, Continuous User Authentication using muli-modal Biometrics, Plymouth University, 2014.

[SNJC11] E. Shi, Y. Niu, M. Jakobsson und R. Chow, „Implicit Authentication Through Learning User Behavior“, in Proceedings of the 13th International Conference on Information Security, 2011.

[SYJY11] W. Shi, J. Yang, Y. Jiang, F. Yang, Y. Xiong, „Senguard: Passive user identification on smartphones using multiple sensors“, in 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2011.

[TrOr12] M. Trojahn, F. Ortmeier, „Biometric authentication through a virtual keyboard for smartphones“, International Journal of Computer Science & Information Technology (IJCSIT), Bd. 4, Nr. 5, 2012.

[ZWWZ13] J. Zhu, P. Wu, X. Wang, J. Zhang, „SenSec: Mobile security through passive sensing“, in 2013 International Conference on Computing, Networking and Communications (ICNC), 2013.