Biometrie vs. Passwort
ADVANTAGE Biometrie

Abstract

Biometrische Verfahren bringen eine Menge Vorteile mit sich und gewinnen zunehmend an Bedeutung gegenüber herkömmlichen Authentifizierungsverfahren. Jedoch wird die Biometrie wie z. B. die Fingerprinterkennung, zunehmend an den Pranger gestellt. Im vorliegenden Artikel werden die Vor- und Nachteile der Biometrie, PINs oder Passwörtern gegenübergestellt, auch im Hinblick auf Erfolgswahrscheinlichkeiten für Angreifer.

Ausgangssituation

Biometrische Verfahren sind in den letzten 3 Jahren mehr und mehr auf dem Vormarsch. Dabei wird die Kritik um diese Verfahren, die körperspezifische Eigenschaften, von statischen (Fingerabdruck) bis hin zu dynamischen (Stimme, Unterschrift), zum Authentifizieren heranzieht, immer lauter. Das häufigste Angriffsziel ist der Fingerprintleser in seinen verbreiteten Varianten kapazitiv[1] und optisch. Wir am FHG SIT haben Arbeitsweisen entwickelt, um Fakefingerformen zu erstellen, die wir dann mit beliebigen Materialien ausgießen konnten. In der Tat stellten wir wie auch der CCC fest, dass mit etwas Geschick fast alle Scannertypen getäuscht werden können. Wir wollen hier keine Anleitung zur Erstellung von Fakefinger abliefern. Vielmehr wollen wir an dieser Stelle die Vorteile und die Sicherheit von Biometrie, insbesondere des Fingerabdrucks, und Passwort gegenüberstellen. Eine zentrale Fragestellung ist dabei die Wahrscheinlichkeit, mit der es einem Angreifer gelingt, einen Fakefinger zu erstellen und sich durch die Überlistung eines Systems einen Vorteil zu verschaffen.

Vorteile der Biometrie

Ein gemeinsamer Vorteil aller biometrischer Verfahren gegenüber dem Passwort besteht darin, dass biometrische Merkmale eng mit der jeweiligen Person verbunden sind und nicht vergessen, verloren oder an andere Personen weitergegeben werden können. Die besonderen Vorteile der Fingerabdruckerkennung liegen in den sehr kompakten Sensoren, die sich leicht in andere Geräte integrieren lassen sowie in ihrer einfachen und schnellen Bedienbarkeit. Somit ist Fingerabdruckerkennung für ein besonders breites Feld von Anwendungen brauchbar, während sich andere Biometrien nur für bestimmte Anwendungen eignen.

	Administ. Aufwand	**weitergeben / vergessen werden**	**ist öffentlich zugänglich**	**begrenzt verfügbar**	**kann erspäht werden**	**kann 1:1 kopiert werden[2]**
Fingerprint	niedrig	nein	ja	ja	nein	nein
Passwort	hoch	ja	nein	nein	ja	ja
Gesichts-erkennung	mittel	nein	ja	ja	nein	nein
dyn. Signatur	mittel	nein	nein	ja	nein	nein
Iriserkennung	mittel	nein	nein	ja	nein	nein

[1] Das Prinzip der kapazitiven Sensoren basiert auf der Messung der elektrischen Kapazität zwischen der Haut und der Sensor-Oberfläche, d.h. beide Oberflächen spielen die Rolle einer Kondensatorplatte.

[2] Bei biometrischen Verfahren ist bei einer 100%igen Übereinstimung der Daten von einer Fälschung auszugehen, da aufgenommene biometrische Daten naturgemäß niemals exakt übereinstimmen, sondern immer einer statistischen Schwankung unterliegen – daher auch die unvermeidlichen Restfehlerraten FAR und FRR!

Bedenken der Bevölkerung

Trotz der technisch guten Eignung als persönliches Wiedererkennungsmerkmal gibt es gerade gegen die Verwendung des Fingerabdrucks (in ähnlicher Form wie bei Gesichtserkennung) noch zahlreiche Kritik in der Bevölkerung:

Zum einen ist der Abdruck ein „öffentliches" Körpermerkmal, das man an vielen Stellen unbemerkt hinterlässt. Zum anderen ist dieses Merkmal – im Gegensatz zu einem Passwort – aufgrund der beschränkten Anzahl von Fingern nicht beliebig gegen ein neues austauschbar.

Diese Eigenschaften bedeuten insbesondere, dass die Sicherheit eines Fingerabdruckerkennungs-Systems nicht alleine von der Geheimhaltung der Merkmalsdaten abhängig gemacht werden kann, auch wenn sie aus Datenschutzgründen selbstverständlich als vertrauliche Daten behandelt werden.

Beurteilung der Überwindungssicherheit

Zur Beurteilung der Sicherheit von Fingerabdruck-Erkennung muss man der zentralen Frage nachgehen, mit welcher Wahrscheinlichkeit es einem Angreifer gelingt,

- einen geeigneten Fakefinger von einer Person zu erstellen und
- sich mit dessen Hilfe tatsächlich Zugang zu einem entsprechend geschützten Bereich oder einer geschützten Anwendung zu verschaffen.

Ist die Erfolgswahrscheinlichkeit für diesen Angriff nicht höher als die zum Herausfinden und zum anschließenden Missbrauch einer entsprechenden PIN oder eines Passwortes, so kann das Fingerabdruck-Verfahren als sichere Alternative zum Passwort-basierten Verfahren verwendet werden.

Wir wollen die Ausgangssituation betrachten, in der ein Angreifer keinen direkten Zugang zu elektronischen Fingerabdruckdaten (etwa beim Enrollment abgespeicherter Referenzdaten) seines Opfers hat, sondern sie sich an Stellen besorgen muss, wo sie sein Opfer auf natürliche Weise hinterlassen hat.

Die Erfolgswahrscheinlichkeit hängt dann von einer Kette von Faktoren ab:

- Die Person muss mit ihrem Fingerabdruck tatsächlich in einem System registriert sein – Wahrscheinlichkeit $\mathbf{q_1}$.
- Die Person muss denselben Finger registriert haben, den sie auch hinterlassen hat – Wahrscheinlichkeit $\mathbf{q_2}$ (in der Größenordnung von ca. 10%!).
- Der Angreifer muss herausfinden, für welche Systeme die Person ihren Finger zur Erkennung benutzt – Wahrscheinlichkeit $\mathbf{q_3}$.
- Die registrierte Person muss einen latenten Fingerabdruck (z.B. auf einem Glas) hinterlassen haben, der genügend Bildinformationen zum Bau eines Fakefingers beinhaltet – Wahrscheinlichkeit $\mathbf{q_4}$.
- Dem Angreifer muss es gelingen, den hinterlassenen Fingerabdruck so abzunehmen, dass genügend Bildinformationen zum Bau eines Fakefingers erhalten bleiben – Wahrscheinlichkeit $\mathbf{q_5}$.
- Die Bedienung des Fingerabdruck-Erkennungssystems mit dem Fakefinger muss zu einem positiven Identifikations- bzw. Verifikationsergebnis führen (-> mindestens so hohe Fehlerquote wie bei Benutzung des echten Fingers!) – Wahrscheinlichkeit $\mathbf{q_6}$.

Die Gesamtwahrscheinlichkeit für einen Angreifer, mit einem "zufällig aufgegriffenen Finger" einen entsprechenden Erfolg zu erzielen, ist somit gleich dem Produkt der Wahrscheinlichkeiten $\mathbf{q_1}$ bis $\mathbf{q_6}$.

Als Beispiel für einen konkreten Zahlenwert bietet sich die 4-stellige PIN bei EC- oder Kreditkarten an – eines der am häufigsten diskutierten Anwendungsbeispiele für einen möglichen Ersatz von Kennwörtern durch Biometrie: Die Wahrscheinlichkeit, dass ein Bundesbürger eine EC-Karte besitzt und damit unter Verwendung seiner PIN an verschiedenen Stellen Zahlungen tätigt oder Bargeld abhebt, ist sehr hoch – mit Sicherheit wesentlich höher als das Produkt der Wahrscheinlichkeiten $\mathbf{q_1}$ und $\mathbf{q_2}$. Als Zusatzinformation zur PIN braucht der Angreifer jetzt nur noch die Kartennummer seines Opfers. Diese herauszufinden gelingt mit einer wesentlich höheren Erfolgswahrscheinlichkeit als das Ausfindigmachen einer Anwendung, für die eine Person ihren Fingerabdruck nutzt, d.h. die Erfolgswahrscheinlichkeit ist größer als $\mathbf{q_3}$. Ist nun das Produkt der Wahrscheinlichkeiten $\mathbf{q_4} \ldots \mathbf{q_6}$ kleiner als 10^{-4} – der

Wahrscheinlichkeit zum Erraten einer 4-stelligen PIN – so ist die Verwendung des Fingerabdruckes für eine Bezahlfunktion mindestens genau so sicher wie die bisherige Lösung mit EC-Karte und PIN. Aus den vorher genannten Gründen (geringer Wert für das Produkt der Wahrscheinlichkeiten $\mathbf{q_1 \_ q_3}$) wären für das Produkt der Wahrscheinlichkeiten $\mathbf{q_4 \_ q_6}$ aber auch größere Werte akzeptabel.

In anderen Anwendungsbereichen müssen bei der Frage nach der Sicherheit von Fingerabdruck-Erkennung vs. Passwort-Erkennung weitere Erfolgswahrscheinlichkeiten für Angriffe gegenübergestellt werden. Bei PC-Anwendungen können z.B. Befürchtungen auftreten, dass es einem Angreifer gelingt

- von einem "optischen Benutzer-Feedback" einen Screenshot und damit ein digitales Bild des Fingerabdrucks zu erhalten oder
- die übertragenen biometrischen Daten auf dem Weg von der Tastatur mit eingebautem Fingerabdruck-Leser mitzuschneiden.

In diesem Fall müsste zur Gegenüberstellung, die Erfolgswahrscheinlichkeiten betrachtet werden, eingegebene Passwörter mitzuschneiden, z.B.

- durch Verwendung eines Logging-Programms auf dem PC oder
- durch direktes Mitschneiden der übertragenen Daten von der Tastatur.
- durch Ausspähen mit versteckten Kameras

Ausstehende Untersuchungen

Bislang werden biometrische Systeme im Wesentlichen anhand ihrer erzielbaren Obergrenzen für ihre charakteristischen Fehlerraten – Falschakzeptanzrate (FAR) und Falschrückweisungsrate (FRR) beurteilt. Die Ermittlung dieser Fehlerraten erfolgt in der Regel durch Live-Tests mit berechtigten und unberechtigten Personen oder durch den automatischen Abgleich von Bildern aus Datenbanken. Wie im vorigen Abschnitt ausgeführt, hängt die praktische Erfolgswahrscheinlichkeit eines Angreifers aber von vielen Faktoren ab. Für eine brauchbare Beurteilung der Biometrie im Hinblick auf Sicherheit gegenüber PIN oder Passwort müssen hier eine Reihe von Wahrscheinlichkeiten analysiert und entsprechenden Erfolgswahrscheinlichkeiten zum Herausfinden von Passwörtern und ihrer anschließenden Nutzbarkeit durch den Angreifer gegenübergestellt werden.
Daraus ergibt sich ein unmittelbarer Handlungsbedarf

- die einzelnen Erfolgswahrscheinlichkeiten für die Schritte der Angriffe auf Biometrie- und Passwort-geschützte Anwendungen genau zu identifizieren und
- durch geeignete Untersuchungen mit konkreten Zahlenwerten zu belegen.

Diese Untersuchungen sind zwingend notwendig, um realistische Aussagen über die Sicherheit von Biometrie gegenüber PINs und Passwörtern zu gewinnen. Sollten die Untersuchungen für bestimmte Anwendungsbereiche zu dem Ergebnis kommen, dass die Gesamt-Erfolgswahrscheinlichkeit für einen Angriff auf das biometrische System mit Hilfe von Fakefingern nicht höher ist als für einen Angriff auf ein PIN- oder Passwort-geschütztes System, so ist der Nachweis erbracht, dass die Biometrie für diesen Anwendungsbereich einsetzbar ist und mindestens ein gleich hohes Sicherheitsniveau bieten kann wie bisherige PIN- oder Passwort-basierte Lösungen.

Fazit

Biometrie ist definitv eine Alternative zum PIN oder Passwort zur Benutzerauthentisierung, d.h. zum Beweis einer vorgegebenen Identität mit bestimmten Rechten. Durch Biometrie lassen sich zahlreiche Probleme lösen, die bei Passwortverfahren durch unsachgemäßen Umgang (z.B. Vergessen oder nach außen sichtbares Aufschreiben) entstehen.

In vielen Anwendungsbereichen bietet Biometrie einen höhere Sicherheits- und Benutzer-Komfort, z.B. bei Bezahlvorgängen, wo das Leisten einer Unterschrift unter Aufsicht der Verkäufer durch das Auflegen des Fingers auf einen Sensor ersetzt werden könnte.

Für einen reinen Identifikationsbetrieb (Ermittlung der Identität ohne Abfrage weiterer Daten) ist die Biometrie, speziell der Fingerprint, nur bedingt geeignet. Empfehlenswert aus unserer Sicht ist hier eine Kombination von Biometrie und PIN, bei der die Biometrie die Identifikation und die PIN die anschließende Authentifizierung übernimmt. Dadurch kann auf Benutzernamen oder Karten verzichtet werden, und es wird eine deutliche Anhebung des Sicherheitsniveaus und des Bedienkomforts erreicht. Zusätzlich sinken die administrativen Kosten.

Wichtige noch ausstehende Untersuchungen betreffen die genauere Spezifikation der o. g. Wahrscheinlichkeiten q1-q6, um noch genauere quantitative Aussagen über die Erfolgschancen potentieller Angreifer zu gewinnen.

Ansprechpartner:
Fraunhofer Institut für Sichere Informationstechnologie
Rheinstraße 75
64295 Darmstadt
Internet: www.sit.fraunhofer.de

Dr. Dirk Scheuermann
E-Mail: dirk.scheuermann@sit.fraunhofer.de
Tel.: 06151 869 290

Thomas T. Kniess
E-Mail: thomas.kniess@sit.fraunhofer.de
Tel.: 06151 869 60051