



E-Interview mit den LAUTMALERN zum Thema Authentifizierungslösungen und Sprachbiometrie



Titel des Interviews: Authentifizierungslösungen und Sprachbiometrie
Name: Manja Baudis, Zeno Wolze
Funktion/Bereich: Gründer
Organisation: Die Lautmalers

Liebe Leserinnen und liebe Leser,

Zugangskontrollen durch biometrische Merkmale wie Fingerabdruck, Gesicht, Iris, Stimme oder Tastenanschlag werden bereits heute erfolgreich in Deutschland eingesetzt. Im Vergleich zu Ausweisen oder Passwörtern, die vergessen, gestohlen, gefälscht oder bewusst weitergegeben werden können, sind sie untrennbar mit der Person verbunden.

Sprachbiometrie ist - insgesamt betrachtet - ein starkes Wachstumsfeld innerhalb der ITK-Märkte: Roland Berger etwa erwartet für die kommenden Jahre ein Wachstum von über 20% per annum. Dies liegt vor allem daran, dass Sprachbiometrie eine hohe Querschnittsrelevanz hat, und branchenübergreifend insbesondere in allen Bereichen der IT-Sicherheit einsetzbar ist, wie bei der Zugangskontrolle zu Netzwerken, Datenbanken und natürlich mobilen Diensten aller Art. Auch auf dem Gebiet der Zugangs- und Anwesenheitskontrolle sind sprachbiometrische Lösungen für viele Branchen relevant.

Sprachbiometrie wird derzeit am intensivsten von Banken und Call Centern eingesetzt. Diese Branchen verfügen über weit ausgebaute Sprachdialogsysteme und eine Kundenbasis, die den Umgang mit Sprachcomputern gewohnt ist. Das erlaubt eine vergleichsweise einfache Integration von Sprachbiometrie, die in diesen Fällen neben Sicherheit auch ein Mehr an Nutzerkomfort bringt und so eher Akzeptanz findet als andere biometrische Systeme.

Im Interview sprechen führende Experten über die Vorteile von Sprachbiometrielösungen gegenüber anderen Authentifizierungsverfahren und nehmen Stellung zu Erfolgsfaktoren und Stolpersteinen. Des Weiteren skizzieren sie aktuelle Projekte und geben Auskunft zu den Kosten von Sprachbiometrielösungen.

Viel Spaß beim Lesen wünscht Ihnen Ihr NetSkill Team



Liebe Lautmaler,

Frageblock 1: Charakteristika Sprachbiometrie

Wie funktioniert die biometrische Erkennung per stimmlichen Fingerabdruck und was ist der Unterschied zwischen Sprecher-Verifikation und Sprecher-Identifikation?

Antwort:

Das Prinzip der Sprachbiometrie ist einfach: Die Struktur eines gegebenen Sprachsignals wird mit der Struktur eines oder mehrerer hinterlegter Sprachsignale verglichen. Ist die Ähnlichkeit zwischen ihnen ausreichend groß, ist die Authentifizierung erfolgreich.

Bei der Sprecher-Identifikation geht es darum, unter mehreren möglichen Sprechern den richtigen zu finden – den nämlich, zu dem ein vorliegendes Sprachsignal gehört. Hierfür wird das gegebene Sprachsignal mit allen in Frage kommenden stimmlichen Fingerabdrücken verglichen. Dieses Verfahren findet vornehmlich in der Kriminalistik Anwendung.

Bei der Sprecher-Verifikation hingegen wird überprüft, ob das Sprachsignal zu einem *bestimmten* Sprecher gehört, ob der Sprecher also derjenige ist, der er zu sein vorgibt. Hierfür wird zunächst eine Kundennummer o.ä. abgefragt und anschließend das Sprachsignal ausschließlich mit dem zu dieser Kundennummer gehörenden, zuvor hinterlegten stimmlichen Fingerabdruck verglichen.

Frageblock 2: Praxiseinsatz Sprachbiometrie-Lösungen

Wie zuverlässig funktioniert Sprachbiometrie? Welche Vorteile bietet die Sprachbiometrie gegenüber anderen Authentifizierungsverfahren?

Antwort:

Eine solide funktionierende Sprachbiometrie steigert die Effizienz von Sprachdialogsystemen erheblich. In der Regel findet die Authentifizierung durch die Abfrage von login (z.B. Kundennummer) und password (z.B. PIN) statt. Derartige Abfragen sensibler Daten aber sind heikel und langwierig: Häufig hat der Anrufer die erforderlichen Daten nicht zur Hand und die meist langen Ketten von Zahlen und Buchstaben, die angesagt werden müssen, bergen das Risiko von Versprechern und Fehlerkennungen. Erfolgt das Login mittels sprachbiometrischer Verfahren, kann der Anrufer sofort mit der Erledigung seiner Aufgabe (beispielsweise einer Überweisung) beginnen. Währenddessen wird - quasi nebenbei - sein stimmlicher Fingerabdruck überprüft.

Die Sprachbiometrie hat jedoch mit dem gleichen Problem zu kämpfen wie die Spracherkennung: Mit der akustischen Variabilität gesprochener Sprache. Einzelne Sprachlaute variieren stark in Abhängigkeit von ihrer lautlichen Umgebung und von der Tagesform des Sprechers. Anders als bei einem echten Fingerabdruck wird es daher so gut wie nie eine exakte Übereinstimmung von Sprachsignal und hinterlegtem stimmlichem Fingerabdruck geben, sondern lediglich eine mehr oder weniger starke Ähnlichkeit.



Neben diesen technischen Risiken lauern noch Gefahren des Missbrauchs. Zum Beispiel könnte sich ein Betrüger einfach durch das Abspielen einer zuvor aufgenommenen Äußerung Zugang zum System verschaffen. Um dem entgegenzuwirken, wird sich häufig folgendes Verfahrens bedient: Pro Anruf wird eine zufällige Kette von z.B. Zahlen erzeugt, die der Anrufer zwecks Überprüfung seines stimmlichen Fingerabdrucks wiederholen soll. Durch dieses zufällige Element wird ein zusätzlicher Sicherheitsfaktor eingeführt. Denn wenn anstatt der vorgegebenen Zahlenfolge eine andere Zahlenfolge eingegeben wird, gilt die Authentifizierung als nicht erfolgreich – auch wenn der stimmliche Fingerabdruck passt.

Frageblock 3: Anwendungsfälle

Was sind die wichtigsten Anwendungsfälle und Einsatzgebiete von Sprachbiometrie-Lösungen und für welche Art von Geschäftsvorfällen sind Sprachbiometrie-Lösungen besonders geeignet?

Antwort:

Trotz der genannten Unsicherheitsfaktoren findet die Sprachbiometrie Anwendung in der Praxis. Sie wird zum Beispiel zusätzlich zu einem gängigen Login-Vorgang eingesetzt, was den Dialog zwar nicht verkürzt, aber zusätzlich Sicherheit schafft.

Ein weiterer, sehr häufiger Anwendungsfall ist die Passwort-Rücksetzung: Ein Nutzer, der sein Passwort (z.B. für eine Web-Anwendung) vergessen hat, authentifiziert sich via Sprachdialogsystem anhand seiner Rufnummer und seines stimmlichen Fingerabdrucks und bekommt anschließend ein neues Passwort zugewiesen. Dieses Verfahren findet vor allem innerhalb großer Unternehmen Anwendung: Bei einer großen Anzahl von Mitarbeitern ist Passwort-Rücksetzung eine der häufigsten Anfragen an das interne Help-Desk. Durch eine Automatisierung kann hier viel Potential eingespart werden. Gleichzeitig sind Risiko und möglicher Schaden durch Missbrauch im Vergleich beispielsweise zum Telefonbanking relativ unwahrscheinlich und gering.

Frageblock 4: Erfolgsfaktoren und Stolpersteine

Wie ist die generelle Nutzerakzeptanz der Sprachbiometrie, wurden bereits Studien durchgeführt, was sind die Ergebnisse?

Antwort:

Sprachdialogsysteme haben nicht den besten Ruf und sie gelten als wenig transparent und unzuverlässig. Dementsprechend herrscht auch gegenüber sprachbiometrischen Verfahren Misstrauen vor. Man traut einer Maschine nicht zu, richtig zu urteilen, vor allem dann nicht, wenn es um so sensible Dinge wie den Zugang zu einem Bankkonto geht.

Darüber hinaus vermitteln die Verfahren der Sprachbiometrie dem Anrufer kaum Sicherheit: Wenn der Anrufer aufgefordert wird, eine zufällige Abfolge von Zahlen zu wiederholen, trägt dies zwar faktisch zur Sicherheit bei, der Anrufer aber empfindet diese Zufälligkeit als Ratespiel und daher alles andere als sicher. Sicherheit wird immer noch am besten durch das Abfragen „harter Fakten“ - der PIN oder von zuvor vereinbarten Geheimfragen (Wie lautet der Mädchenname Ihrer Mutter?) – vermittelt. Durch ein ausgefeiltes Voice User Interface Design und ent-



sprechendes Texting jedoch lässt sich nicht nur die Akzeptanz von Sprachdialogsystem im allgemeinen, sondern auch das Vertrauen in sprachbiometrische Verfahren erheblich steigern.

Frageblock 5: Zukunft der Sprachbiometrie

Wird die Sprachbiometrie in Zukunft häufiger zum Einsatz kommen? Welche Anwendungsgebiete werden noch erschlossen werden?

Antwort:

Sprachbiometrie steigert die Effizienz von Sprachanwendungen zum Teil erheblich. Damit sie aber weit reichend zum Einsatz kommen kann, muss der stimmliche Fingerabdruck einen hohen Grad an Sicherheit erreichen. Ähnlich wie bei der Spracherkennung wird es aber auch in der Sprachbiometrie keine hundertprozentige Sicherheit geben.

Der bestehende Grad an Sicherheit erlaubt gegenwärtig den Einsatz von Sprachbiometrie in denjenigen Fällen, in denen ein Missbrauch weniger wahrscheinlich und weniger kritisch ist bzw. die Sprachbiometrie durch andere sicherheitsrelevante Verfahren ergänzt werden kann.

Dennoch werden die sprachbiometrischen Verfahren in Zukunft nicht hauptsächlich nur unternehmensintern, sondern auch vermehrt bei Sprachportalen beispielsweise der Versicherungs- und Finanzbranche zum Einsatz kommen. Auch um dem Identitätsdiebstahl im Telefoniebereich entgegenzuwirken wird momentan die sprachbiometrische Authentifizierung von Anrufern im Callcenter diskutiert. Ein weiteres Anwendungsfeld wird sich darüber hinaus durch die Verknüpfung von Sprachtechnologien mit Web-Anwendungen ergeben.

Vielen Dank für das Interview!