Stimmbiometrie in der Finanzdindustrie

Von Heiner Kruessmann

Beim Thema biometrische Authentifizierung dominiert bislang der Fingerabdruck. Ebenso einzigartig ist jedoch der Stimmabdruck, sagt Heiner Kruessmann. Die Stimmbiometrie eignet sich zum Beispiel für telefonischen Kundenservice. Denn dann entfällt die bisherige Abfrage von Passwörtern. Identifiziert werden kann der Nutzer per Passphrase oder auch im Freitext. Weil beim Abgleich auch Sprechgeschwindigkeit, Wortschatz und Satzbau berücksichtigt werden können, gilt das System als sehr sicher. Red.

Die Entwicklungen im Bereich der Cyber-Kriminalität legen nahe, dass wissensbasierte Sicherheitsmethoden in der Zukunft nicht mehr für den Schutz der Nutzer garantieren können. Gerade im Finanzsektor ist dieser jedoch oberste Priorität. Eine Umfrage in diesem Jahr ergab, dass in den letzten zwölf Monaten eine von vier Personen Geld aufgrund ineffizienter Passwörter verloren hat – 1 500 Euro im Durchschnitt.

Angesichts zunehmender Komplexität des Datenschutzes und der damit verbundenen Gefährdung von Benutzernamen und Passwörtern ist es für Betrüger heute einfach, Zugang zu nahezu allen persönlichen Daten zu erhalten. Hierbei sind nicht nur Anmeldedaten für soziale Netzwerke betroffen, sondern auch sensible Daten mit denen Nutzer ihre Finanzen verwalten. Auch Hacker halten Schritt mit der fortschreitenden Technik und führen immer komplexere Angriffe durch. Anfang 2019 wurden Passwortsammlungen von Cyberkriminellen veröffentlicht und es waren 2,2 Milliarden Accounts betroffen. Normale, wissensbasierte Sicherheitsmethoden wie Passwörter können keinen umfassenden Schutz gewährleisten. Eine Lösung bietet die Authentifizierung über Stimmbiometrie.

Bereits erfolgreich im Einsatz

Die Technologie blickt bereits auf einige Erfolgsgeschichten zurück.

– In Großbritannien konnte die HSBC-Bank durch die KI-basierte Stimmbiometrie betrügerische Dateneingriffe frühzeitig aufdecken und somit den Diebstahl von rund 300 Millionen britischen Pfund verhindern.

– Auch in Schottland zeigte sich der Einsatz von Stimmbiometrie effektiv: die Royal Bank of Scotland konnte bei einer Stimmuntersuchung von 17 Millionen eingehenden Anrufen einen von 3 500 als Betrug identifizieren. Zusätzlich kann die Spracherfassung nun Beweise liefern, um eine Strafverfolgung der Betrüger zu ermöglichen.

– Stimmbiometrie findet auch bereits in Deutschland Einsatz: Die Deutsche Telekom greift auf die Technologie in ihrem Kundendienst zurück.

„Meine Stimme ist mein Passwort"

Die Funktionsweise ist nicht sonderlich kompliziert. Die Stimmbiometrie ist eine Technologie zur Sprecherauthentifizierung. Hierbei wird zunächst ein Stimmabdruck von einer Person erstellt, in dem diese eine festgelegte Phrase, wie beispielsweise „Meine Stimme ist mein Passwort", sagt und sich dabei aufzeichnen lässt. Der daraus generierte Stimmabdruck setzt sich aus über 1 000 einzigartigen Merkmalen zusammen. Diese werden durch physische Faktoren wie etwa die Länge des Stimmtraktes, der Größe und Form des Kehlkopfes oder der Nasenhöhle sowie durch verhaltensabhängige Merkmale wie Tonhöhe, Rhythmus oder den Akzent bestimmt.

Unabhängige Untersuchungen haben gezeigt, dass ein Stimmabdruck dadurch ebenso einzigartig ist wie ein Fingerabdruck. Zudem gibt es neben der Möglichkeit, sich per Passphrase zu authentifizieren, nun auch die Option, sich mit Lightning Engine per Freitext

Heiner Kruessmann,
Nuance Communications, München

identifizieren zu lassen – da erfolgt die Validierung innerhalb von nur wenigen Sekunden.

Anbieter der Stimmbiometrie-Lösungen speichern die dadurch gewonnenen einzigartigen Sprachcharakteristiken dann wie andere sensible Kundendaten in einer sicheren Datenbank hinter einer Firewall. Durch mathematische Algorithmen werden die Klardaten umgewandelt und verschlüsselt. Wenn Kunden dann auf ihre Daten zugreifen möchten, wird eine digitale Sprachprobe erfasst und mit den vorhandenen Referenzdaten in Echtzeit verglichen sowie deren Übereinstimmung ermittelt. Hacker können solche Referenzdateien zwar bei einem Hacker-Angriff stehlen, aber die Stimme der Person ist daraus nicht ableitbar und somit ist die Datei wertlos.

Imitatoren, Erkältung und Roboterstimmen

Um die Stimmbiometrie-Systeme vor möglichen Cyberangriffen schützen zu können, gibt es verschiedene Technologien. Playback Detection und Liveness Detection erkennen den Unterschied zwischen einer aufgezeichneten und einer aktuellen Stimmprobe, die live aufgenommen wird. So können weder Imitatoren noch Hacker die Authentifizierung überwinden.

Auch bei einer Erkältung versagt das System nicht. Leichte Schwankungen in der Stimme können aufgrund der verschiedenen Merkmale, die bei der Erstellung des Stimmabdrucks berücksichtigt werden, das System nicht beeinflussen. Bei größeren Einschränkungen durch eine starke Kehlkopfentzündung beispielsweise stellt dies eine Herausforderung für die Technologie dar. Hier können die Kunden dann auf andere Authentifizierungsarten zurückgreifen, je nachdem, welches System im Einsatz ist.

Satzbau, Grammatik und Wortschatz erkennen

Keine Stimme gleicht der anderen – so können die sensiblen Daten optimal geschützt werden. Auch andere biometrische Faktoren spielen eine Rolle wie zum Beispiel die persönlichen Tipp- und Sprachgewohnheiten sowie einzigartige Verhaltensmuster einer Person. Mittels neuer KI-Techniken kann ein möglicher Betrug erkannt werden, wenn Satzbau, Grammatik und Wortschatz oder das Verhalten nicht mit dem Kundenmodell übereinstimmten.

Zudem kann das biometrische Verhalten an der Art und Weise gemessen werden, wie eine Person eine Tastatur nutzt, eine Maus bewegt oder Apps auf einem Touchscreen bedient. Basierend auf dem ausführlichen Kundenprofil ist es möglich, anhand neuer Technologien verdächtige Aktivitäten zu markieren und im Anschluss an Betrugsspezialisten weiterzuleiten.

Stimmbiometrie bietet Nutzern dadurch nicht nur durch den individuellen Stimmabdruck umfassende Sicherheit, sondern berücksichtigt weitere wichtige Merkmale einer Person. Das steigert den Nutzerkomfort und erleichtert gleichzeitig den Authentifizierungsprozess.

Neben der einfachen Handhabung der Stimmbiometrie verringert sich die Gefahr durch Betrug und Servicemitarbeiter können direkt in das jeweilige Kundenanliegen einsteigen, statt wie bisher Sicherheitsfragen abzuarbeiten. Die Eingabe von PINs, Passwörtern oder Sicherheitsfragen ist nicht mehr länger erforderlich. So profitieren die Nutzer doppelt – und auch die Anbieter, da sie ihren Kunden den bestmöglichen Schutz und Service ermöglichen. ■