Mit Verhaltensbiometrie zur sicheren Authentisierung

Einfache Passwörter sind leicht zu knacken, komplexe Passwörter schwer zu merken und Sicherheitstoken oder Chipkarten können vergessen oder beschädigt werden. Dieser Problematik Abhilfe verschafft die Tippverhaltensbiometrie. Thomas Boll

Die Erkenntnis liegt Jahrzehnte zurück: Geheimdienste erkannten «freundliche» und «feindliche» Funker an der individuellen «Melodie» ihrer Morsezeichen. Was für simple Morsetasten galt, trifft auf Computertastaturen in besonderem Mass zu. Das Tippverhalten eines Nutzers auf einer Tastatur ist ausgesprochen individuell – und nicht kopierbar. In Anbetracht dieser für die Aspekte der IT-Sicherheit relevanten Tatsache begann die gezielte Erforschung und Entwicklung von Verfahren zur Tippverhaltensbiometrie 1993 an der Universität Regensburg (D). Deren Resultate waren derart beeindruckend, dass sich sicherheitsbewusste Branchen für die Technologie zu interessieren begannen und die Weiterentwicklung am Institut für Bankinnovation (IBI Research) vorangetrieben wurde. Heute nun darf die von Psylock kommerzialisierte Tippverhaltensbiometrie als wegweisende neue Form dieser Technologie bezeichnet werden. Sie ergänzt in vielen Applikationen Passwörter und Smartcards oder macht diese gar überflüssig.

Aktive versus passive Biometrie

Der geschützte Zugriff auf Daten und Applikationen wird gemeinhin mithilfe unterschiedlicher Identifikations- und Authentisierungsverfahren bewerkstelligt. Dabei kommen Passwörter und PIN-Codes ebenso zur Anwendung wie Hardware-Tokens und Smartcards. Diesen Komponenten gemeinsam ist jedoch die nicht unproblematische Handhabung. So werden persönliche Zugangsdaten vergessen, fahrlässig weitergegeben, aufgeschrieben oder sie werden gestohlen, ohne dass dies vom Besitzer zwingend bemerkt wird. Bei der Nutzung von Hardwarekomponenten wie Token und Smartcard wiederum fallen Aspekte wie Kosten, Hardwaredefekte oder Diebstahl ins Gewicht. Angesichts dieser sicherheitsrelevanten Unzulänglichkeiten gewannen biometrische Verfahren wie Fingerprint oder Gesichts-, Stimmen- und Iris-Erkennung zunehmend an Bedeutung. Doch auch diese mit «passiv biometrisch» bezeichneten Methoden weisen gewichtige Nachteile auf. Dazu zählen unter anderem die in der Regel hohen Kosten für Hardware und Sensoren, die aufwendige Erfassung der Profile sowie die teils geringe Akzeptanz durch die User. Besonders kritisch sind verfahrensspezifische Schwächen. Bei der Gesichtserkennung sind dies beispielweise Personenveränderungen durch Maskierung oder die Vorlage einer Fotografie. Die Stimmerkennung ihrerseits «schwächelt» bei Heiserkeit und Störgeräuschen. Und auch die Identifikation mittels Fingerprint – das aktuell gängigste biometrische Erkennungsverfahren – kennt zahlreiche Angriffsszenarien.

Thomas Boll ist Geschäftsführer der Boll Engineering AG.

Das Tippen am Computer ist so individuell wie die Handschrift – und ermöglicht folglich eine sichere und komfortable Nutzererkennung.

Verbesserte Verfahren und Technologien sind folglich gefragt, um den zunehmenden Sicherheitsbedürfnissen Rechnung zu tragen. Mit aktiv biometrischen Verfahren – diese basieren auf individuellen Merkmalen wie etwa persönlicher Gang und ganz besonders das persönliche Tippverhalten – stehen heute entsprechende Lösungen zur Verfügung.

Biometrie – ohne Sensor

Als besonders attraktiv erweist sich die Tippverhaltensbiometrie. Diese macht sich die Tatsache zunutze, dass jede Person ein individuelles, einzigartiges Tippverhalten aufweist. Die unverwechselbaren Merkmale sind weder kopierbar, noch können sie weitergegeben werden. Entscheidend ist bei dieser Form der Authentifizierung auch, dass sie immer und überall möglich ist. Spezielle Sensoren oder Hardware sind nicht erforderlich.

Um die Tippverhaltensbiometrie zu nutzen, lernen entsprechende Systeme die individuelle Biometrie der einzelnen User kennen. Dazu werden beim Abtippen eines durch den User frei wählbaren Satzes die individuellen Merkmale des Tippverhaltens analysiert. Berücksichtigt werden dabei Merkmale wie Schreibrhythmus, Tippgeschwindigkeit, Rechts- oder Linkshändigkeit, Beweglichkeit der Finger und Konstanz des Tippens. Dank der Analyse und Auswertung dieser und weiterer Merkmale ergibt sich pro User ein unverwechselbares Tippmuster, das bei jedem Log-in-Versuch als Vergleichsbasis dient.

Meldet sich ein User neu an, tippt er dazu den vordefinierten Satz ein. Dabei wird sein Tippverhalten analysiert, mit der Vorgabe verglichen und mit einer hochgradigen Trennschärfe zur Überprüfung der Identität genutzt. Bemerkenswert ist, dass selbst eine adaptive Anpassung an das sich ändernde Verhalten möglich ist. So werden Veränderungen im Tippverhalten der einzelnen User mit der Zeit erkannt, wodurch das Authentisierungverfahren Verhaltensänderungen laufend berücksichtigt. Somit ist eine erfolgreiche Authentifizierung selbst über Jahre garantiert.

Obwohl es sich bei der Tippverhaltensbiometrie um eine vergleichsweise junge Disziplin handelt, weist das Verfahren eine beachtenswerte Erkennungsleistung auf. Diese durch die Faktoren False Acceptance Rate, False Rejection Rate und Equal Error Rate bestimmte Messgrösse liegt nur unwesentlich tiefer als die der Iris- und Retina-Erkennung, markant jedoch vor der Stimmerkennung. Werden datenschutzrechtliche Anforderungen (z.B. Ausspähbarkeit) in den Vergleich biometrischer Verfahren mit einbezogen, steht die Tippverhaltensbiometrie gänzlich an der Spitze. Vor diesem Hintergrund darf angenommen werden, dass sich das innovative Verfahren in den kommenden Jahren in unterschiedlichsten Bereichen etablieren und das Identity- und Access-Management nachhaltig verändern wird. <