

Tippverhaltensbiometrie Psylock

Prof. Dr. Dieter Bartmann,
Psylock GmbH, Regerstrasse 4, 93053 Regensburg
E-Mail: dieter.bartmann@psylock.com

30. Januar 2008

Zusammenfassung

Zeige mir, wie du tippst, und ich sage dir, wer du bist – dies ist das Konzept des Programms Psylock.

Anhand einer kurzen Tipp-Probe auf einer gewöhnlichen Computer-Tastatur authentisiert das System Psylock den Schreiber und gewährt oder verweigert ihm den Zugang zum Computersystem. Das Prinzip macht es sich zunutze, dass jeder Mensch ein charakteristisches Tippverhalten hat. Sogar eineiige Zwillinge lassen sich unterscheiden. Nach 15-jähriger Forschungs- und Entwicklungszeit an der Universität Regensburg ist es jetzt erstmals gelungen, die Tippverhaltensbiometrie auf einen so hohen Qualitätsstand zu bringen, dass sie anderen biometrischen Verfahren mindestens ebenbürtig ist.

Psylock besitzt gegenüber dem Passwortschutz und den biometrischen Verfahren bedeutsame Alleinstellungsmerkmale. Es schützt vor Keyloggern und erkennt Angriffe mit kopierten Merkmalen. Da keine zusätzliche Hardware benötigt wird, ist es die weltweit einzige Authentisierung ohne Passwort, die von Jedermann sofort im Internet genutzt werden kann.

Der Proof of Concept ist erbracht. Psylock ist seit Oktober 2006 an den Hochschulen Regensburg und Landshut erfolgreich im Einsatz. Derzeit wird es von zahlreichen Unternehmen getestet.

Eine interessante Anwendung im Internet ist Login und Fraud Detection. Das Login kommt ohne Passwort aus und bietet darüber hinaus eine zuverlässige Bindung an die Person. Unerlaubte Mehrfachregistrierungen (um z.B. den Preis in einer Auktion hochzutreiben) können entdeckt werden. In Firmennetzen verursachen vergessene Passwörter keine Kosten mehr. Psylock bietet ein webbasiertes Password Reset im Self Service. Für das Login am Computerarbeitsplatz kann man Psylock anstelle eines Passwortes oder in Kombination mit diesem verwenden. Einem getippten Text lässt sich das Tippverhalten mitgeben und so der Nachweis liefern, wer der Autor ist (z.B. sicheres E-Mailing).

Das Marktpotenzial für Psylock ist immens groß. Das Marktfenster ist derzeit offen. Psylock stößt als Biometrie ohne Sensor international auf großes Interesse. Es bietet den Kunden einen wertvollen Beitrag zur Lösung ihrer vielfältigen Authentisierungsprobleme.

1 Stand der Forschung/Technik

1.1 Der Passwortschutz ist für heutige und zukünftige Anforderungen ungenügend

Der Passwortschutz ist das Sorgenkind des IT-Security Managements. Die in der Theorie sichere Authentisierung mit einem geheimen Passwort birgt in der Praxis aus Sicht der Unternehmen ein Sicherheitsrisiko. Der Hauptnachteil besteht darin, dass es keine zuverlässige Bindung des Passworts an die Person gibt. Sie wird nur künstlich erzeugt, indem der kooperationsbereite Benutzer das Geheimnis streng hütet. So ist ein Unternehmen bei der Realisierung von Sicherheitsstandards vollkommen von der äußerst sorgfältigen Mitwirkung des Benutzers abhängig. Verweigert er sie (z.B. aus Leichtfertigkeit, aus Verärgerung oder aus latent krimineller Veranlagung), wird damit der Zugangsschutz zunichte gemacht. Leider besitzt das IT-Security Management keinerlei zuverlässige Handhabe, dieses Risiko zu kontrollieren. Passwortmissbrauch kann nicht verhindert, ja in der Regel nicht einmal entdeckt werden. Sanktionen verlieren deshalb ihre Wirkung. Auch statistische Aussagen über Missbrauchshäufigkeiten sind als unzureichende generelle Schätzungen für das Management der IT-Risiken wertlos.

Besonders gravierend ist die fehlende Bindung an die Person bei der Web-Authentisierung im E-Commerce und E-Business. Dort kann man noch viel weniger als bei der Gruppe der Firmenangehörigen einen kooperativen Benutzer erwarten. Haben Kunden z. B. ein Abonnement für kostenpflichtige Downloads abgeschlossen, kann man dann wirklich ausnahmslos annehmen, dass sie die Passwörter nicht aus Gefälligkeit in der Abteilung oder im Freundeskreis kreisen lassen?

Die Passwort-Authentisierung bietet realistischer Weise nur dort einen Schutz, wo der Benutzer selbst ein ureigenes Interesse daran besitzt. Aber auch dann bleiben erhebliche Restrisiken bestehen. Der Benutzer besitzt in der Regel nicht nur ein Passwort, sondern viele. Um diese Flut bewältigen zu können, notiert er sich die Passwörter. Dadurch entsteht die Gefahr, dass sie in fremde Hände geraten. Oftmals wählt er sie gemäß einer leicht zu durchschauenden Systematik. Derartige Passwörter sind leicht zu knacken.

Eine gewisse Abhilfe schaffen Smartcards. Sie sind ein Besitzmerkmal, welches man mit Methoden der asymmetrischen Kryptografie auf Echtheit überprüfen kann. Die Bindung an die Person geschieht über eine PIN als Wissensmerkmal. Deshalb können auch Smartcards genau so wie Passwörter unentdeckt weiter gegeben werden.

Die einzigen Authentisierungsmerkmale mit einer systemimmanenten Bindung an die Person sind die biometrischen Merkmale. Aber biometrische Systeme besitzen den Nachteil, dass sie sehr teuer und deshalb nicht flächendeckend verbreitet sind. Sie sind nur dort einsetzbar, wo die Computer mit entsprechenden Lesegeräten bzw. Sensoren ausgestattet sind. Als Alternative für die Authentisierung im Web-Markt kommen sie nicht in Frage.

Benötigt wird eine zuverlässige Authentisierung, welche wie ein biometrisches Verfahren eine starke Bindung an die Person besitzt, ohne dabei mit deren Nachteilen (teure Hardware, Wartungsaufwand, Immobilität, Benutzerressentiments,...) behaftet zu sein.

Eine Lösung liefert die Analyse des Tippverhaltens eines Benutzers. Die wissenschaftliche Literatur zeigt, dass dies ein ebenso personentypisches Merkmal ist wie z. B. der Fingerabdruck oder das Gesicht. In der Tat hat jeder Benutzer sein eigenes, spezifisches Tippverhalten, egal, ob er ein geübter Tipper ist oder nicht. Das Tippverhalten trägt seine Handschrift. Deshalb ist es möglich, ihn anhand der Art und Weise zu erkennen, wie er auf einer handelsüblichen Tastatur tippt. Die Analyse des Tippverhaltens ist gewissermaßen die digitale Form der Handschriftenanalyse. Der Benutzer braucht nur einen kurzen Satz zu tippen.

1.2 Historische Entwicklung der Tippverhaltensbiometrie

Bereits im neunzehnten Jahrhundert haben Bryan und Harter [Bryan 1897] festgestellt, dass man Telegraphisten anhand ihres Morse-Verhaltens erkennen kann.

Wie Singh [Singh 2000, S. 135 f.] berichtet, zählte zu den Techniken der französischen Funkaufklärung im ersten Weltkrieg neben der Kryptoanalyse auch die Funkverkehrsanalyse. Letztere beinhaltete die



Verwendung von Peilstationen zur Ortung feindlicher Stellungen sowie die Analyse des Morse-Verhaltens der gegnerischen Funker. So konnten die französischen Horchposten die feindlichen Bataillone anhand der „Handschrift“ ihrer Funker beim Morsen (d. h. anhand der Pausen, der Geschwindigkeit und der relativen Länge von Punkten und Strichen) identifizieren und so deren Bewegungen verfolgen. Diese Information war vor allem dann wertvoll, wenn die Kryptoanalytiker, z. B. auf Grund eines Schlüsselwechsels, gerade nicht in der Lage waren, die gegnerische Kommunikation zu entschlüsseln.

Marks [Marks 1998, S. 601 f.] berichtet, dass die britische SOE (Special Operations Executive) im zweiten Weltkrieg „Fingerabdrücke“ des Morse-Verhaltens ihrer Funker aufzeichnete, bevor diese ihre Missionen antraten. Dadurch wurde eine Möglichkeit geschaffen, die Authentizität ihrer Nachrichten zu überprüfen. Denn trotz Schwankungen (z. B. auf Grund wechselnder Gemütslage) zeigte das Morse-Verhalten der einzelnen Funker unverwechselbare Charakteristika. Geübte Empfänger waren sogar in der Lage, das Tippverhalten eines Funkers allein am Klang zu erkennen.

Die Idee, einen Benutzer anhand seines Tippverhaltens auf einer Computertastatur zu authentisieren, wurde erstmals von Spillane [Spillane 1975] im Jahr 1975 veröffentlicht [Peacock 2005]. Seitdem haben zahlreiche Untersuchungen die Eignung des Tippverhaltens für die Benutzererkennung nachgewiesen. Mateos [Mateos 2000] konnte zeigen, dass sich selbst eineiige Zwillinge in ihrem Tippverhalten unterscheiden. Die Unterschiede zwischen dem Tippverhalten verschiedener Benutzer beruhen nicht nur auf der Tippmethode (d. h. ob jemand z. B. das Zehnfingersystem beherrscht oder nicht), sondern auch auf physischen und mentalen Eigenheiten der einzelnen Personen [Nisenson 2003]. Eine relativ umfassende Übersicht bisher erschienener Arbeiten zur Tippverhaltenserkennung bieten Peacock et al. [Peacock 2005].

1.3 Derzeitiger Stand

Zum praktischen Einsatz hat es nur der Ansatz von Garcia gebracht [Garcia 1986]. Er ist in dem US-amerikanischen Softwareprodukt AdmitOne (ehemals Biopassword) von AdmitOne Security implementiert. Diese Software ist seit den neunziger Jahren auf dem Markt. Das Verfahren arbeitet ausschließlich mit fest vorgegebenem Text. Für das Enrollment muss der Text mehrmals getippt werden. Gemessen werden Anschlagsdauer und Übergangsdauer von einer Taste zur nächsten. Das Tippprofil des Benutzers (Template) wird durch statistische Mittelung berechnet. Bei der Authentisierung muss der besagte Text einmal eingegeben werden. Er wird mit Hilfe eines künstlichen neuronalen Netzes auf Ähnlichkeit mit dem Template des Benutzers verglichen.

Dieses Verfahren ist methodisch so schwach, dass es als alleiniges Authentisierungsverfahren nicht angewendet werden kann. Hiefür sind zwei Gründe zu nennen: erstens die verwendete Mathematik und zweitens die Beschränkung auf rein dynamische Aspekte des Tippverhaltens. Diese sind jedoch nicht besonders trennscharf, da das Tippverhalten großen Schwankungen entsprechend der Tagesform unterliegt. Deshalb ist AdminOne nur als Password Hardener im Einsatz: es prüft, wie das geheime Passwort getippt wurde. Das Produkt AdmitOne schöpft damit die Potenziale der Tippverhaltensbiometrie bei weitem nicht aus.

2 Idee

Eine grundlegende Verbesserung der Tippverhaltensbiometrie gelingt mit vier innovativen Ideen. Sie sind in dem System Psylock (Psychometric Locking) implementiert. Die Psylock-Entwicklung begann 1993. Es gingen daraus zahlreiche Publikationen hervor, darunter drei Dissertationen.

2.1 Vier innovative Ideen

Erste Idee: Verwendung der Testtheorie anstelle des Mustervergleiches

Die erste Idee ist die Abkehr vom Pattern Matching bei der Authentisierung. Dieses ist das Standardverfahren für bildgebende Biometrien und dort auch geeignet. Es basiert auf der Grundannahme, dass die beiden Pattern etwa denselben Informationsgehalt tragen und dieser sehr hoch ist. Für Bilder stimmt das auch. Damit aber



auch Templates von Verhaltensbiometrien einen hohen Informationsgehalt tragen, müssen sehr lange Beobachtungsreihen vorliegen. Für den Praxiseinsatz kann man dies in der Regel nicht verlangen. Ein Login-Vorgang mit einem Tippertext von (mindestens) 400 Zeichen und mehr ist unzumutbar.

Psylock arbeitet nicht mit Methoden der Mustererkennung sondern der Testtheorie. Anstatt des Pattern Matching wird bei Psylock das Tippverhalten als komplexes statistisches Modell beschrieben. Für die Authentisierung wird ein kurzer Tippertext gegen dieses Modell getestet. Das erlaubt Login-Texte mit ca. 40 Anschlägen. Damit wird der Aufwand beim täglichen Gebrauch um 90 % verringert.

Zweite Idee: tiefer liegende personentypische Merkmale

Die zweite Idee besteht darin, zusätzlich zu den dynamischen Merkmalen wie Tippgeschwindigkeit, Rhythmus etc. auch tiefer liegende personentypische Merkmale heranzuziehen, die kaum Schwankungen unterliegen. Zwei dieser Merkmale sind vom Autor patentiert [Bartmann 1997]. Beim ersten Merkmal handelt es sich um die Tastenauswahl, wenn mehrere für denselben Zweck zur Verfügung stehen. Hierzu gehören z.B. die beiden Shift-Tasten. An ihrem Gebrauch kann man z.B. die Rechts-/Linkshändigkeit ablesen und die grundsätzliche Art des Tippens (Zehnfinger-Blindsystem, Tippen mit nur zwei Fingern,...).

Das zweite Merkmal beschreibt die Präzision des Tippens (eine zweite Taste wird gedrückt, noch ehe die erste Taste losgelassen wurde). Dieses ist ebenfalls tief in das Tippverhalten eingeschliffen.

Die Abbildung 1 zeigt, dass man die Erkennungsleistung (ausgedrückt als Equal Error Rate, d.h. Schnittpunkt von Falschrückweisungsrate und Falschakzeptanzrate) durch die Analyse des Shift-Tastengebrauchs in etwa verdoppeln kann (unabhängig von der Textlänge, gerechnet mit Psylock Version V1 2006).

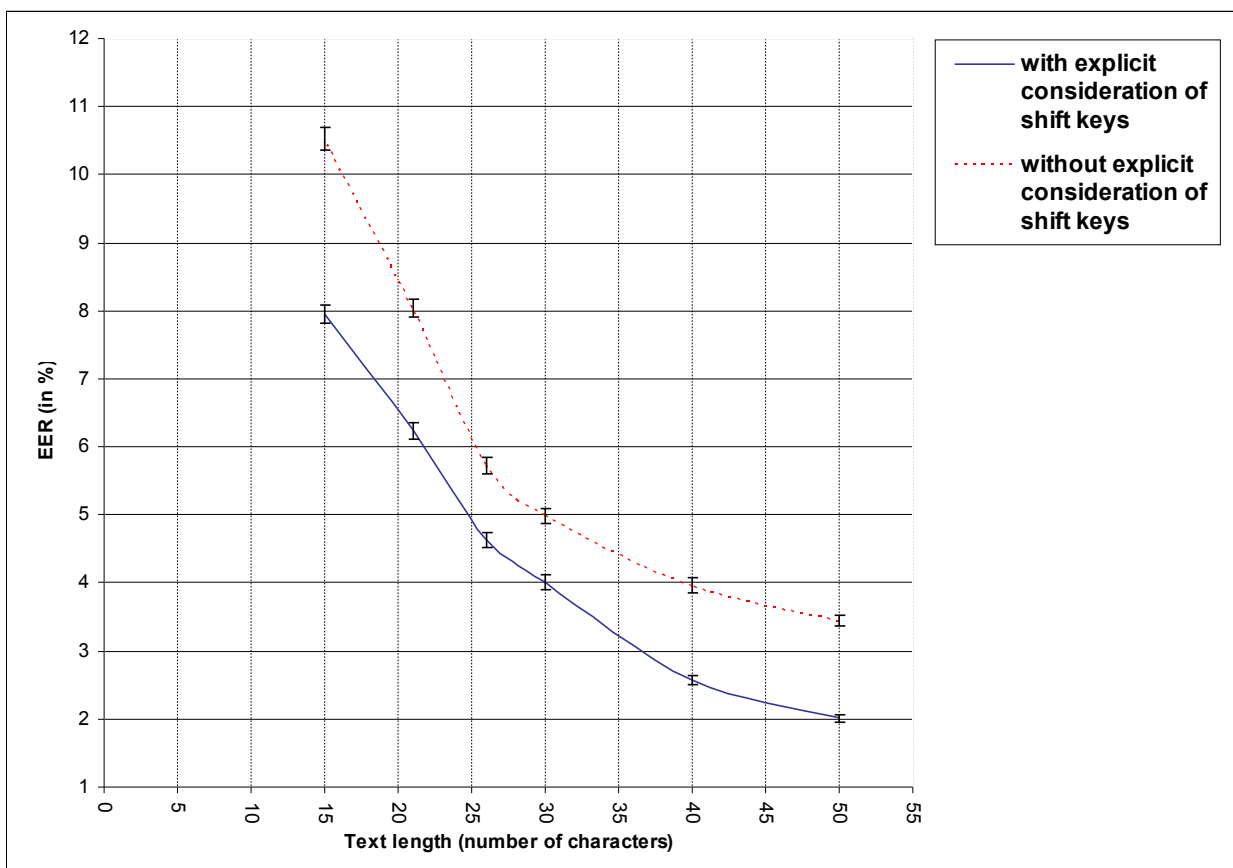


Abbildung 1: Einfluss des Shift-Tastengebrauchs auf die Equal Error Rate bei unterschiedlicher Textlänge

Dritte Idee: Tastendistanz

Um die Erkennungsleistung weiter zu verbessern wird die Distanz der Tasten auf dem Keyboard verwendet. Diese Information lässt sich optimal mit den anderen Merkmalen kombinieren. Auf diese Weise entsteht beispielsweise das Merkmal der Übergangsdauer pro Tasten-Distanz, welches die Trennschärfe maßgeblich verbessert. Weiterhin kann die Distanz-Information eingesetzt werden, um Tippfehler des Benutzers zu korrigieren.

Vierte Idee: verbesserte Vorverarbeitung der Tippprobe

Die Tippproben sind häufig verrauscht. Sie enthalten Tippfehler, die den typischen Tippfluss beeinträchtigt haben oder es treten in den Übergangsdauern Ausreißer auf, wenn z.B. während des Tippens das Telefon klingelt und der Benutzer deshalb beim Tippen inne hält. Die Art und Weise, wie man diese Störungen bereinigt, wirkt sich ebenfalls auf die Qualität des Verfahrens aus. Zum Einsatz kommen Methoden, die der DNA-Analyse entlehnt sind [Needleman 1970]. Dort findet man eine ähnliche Problemstellung beim Vergleich von DNA-Sequenzen.

Alle diese vier Ideen sind in dem System Psylock implementiert. Die Kombination aller Einzelmerkmale fügt sich zu einem benutzerindividuellen Profil. Die Merkmale werden personen-individuell gewichtet. Psylock zieht aus diesem Gesamtprofil mit Hilfe stochastischer Modelle und künstlicher neuronaler Netze Rückschlüsse auf die Identität des Benutzers.

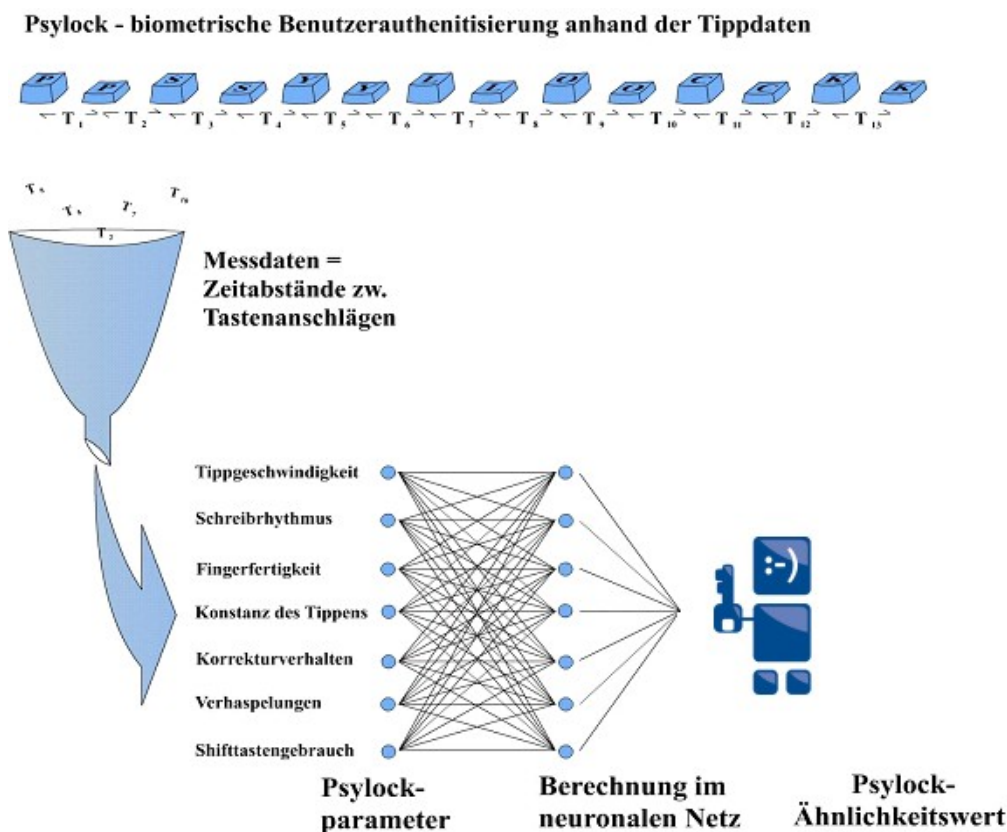


Abbildung 1: Wirkungsweise der Psylock-Methode

2.2 Die Funktionsweise der Methode

Die Psylock-Methode arbeitet in zwei Varianten. Bei der Variante mit beliebigem Text tippt der Benutzer, was immer er will, z.B. eine E-Mail oder den Text in einem Dokument. Psylock beobachtet das Tippverhalten und kann auf diese Weise erkennen, wenn plötzlich eine andere Person vor dem Rechner sitzt (Intrusion

Detection, Bestätigung der Autorenschaft). Bei der Variante mit festem Text tippt der Benutzer einen feststehenden Satz. Diese Variante ist für das Login sehr gut geeignet, weil dieser Satz sehr kurz sein darf.

Das Psylock System besitzt die vier Hauptfunktionen

- Enrollment
- Authentisierung
- Identifizierung
- Adaption.

Enrollment:

Vor dem erstmaligen Gebrauch tippt der Benutzer der Festtextvariante neunmal einen vordefinierten Satz von etwa 40 Anschlägen. Dieses Training dauert ca. 2-5 Minuten. Für die Freitextvariante ist es auch möglich, die Trainingsdaten „nebenbei“ zu sammeln, wenn immer man einen Text tippt. Aus den Trainingsdaten wird das personentypische Tippprofil des Benutzers errechnet. Dazu werden aus den elementaren Beobachtungsdaten key code, hold-key-time und transition-time insgesamt 14 Einzelmerkmale des Tippverhaltens analysiert.

Authentisierung:

Der Benutzer gibt seinen Namen (USER-ID) und eine kurze Tippprobe ein. Das System analysiert das Tippverhalten mit Hilfe des Templates und liefert einen Matchscore zwischen 0 und 100 zurück. Liegt dieser Wert über einer voreingestellten Schwelle (Threshold), so wird der Benutzer als solcher erkannt, andernfalls abgewiesen.

Identifizierung:

Sie funktioniert wie die Authentisierung, nur ist jetzt der Benutzername unbekannt. Das System analysiert die aktuelle Tippprobe mit Hilfe aller infrage kommenden Templates in der Datenbank und liefert die zugehörigen Matchscores.

Adaption:

Wird bei der Authentisierung eine aktuelle Tippprobe als dem Benutzer zugehörig erkannt, dann wird sie den Trainingsdaten angefügt und das Template darauf hin neu berechnet.

2.3 Qualität des Verfahrens

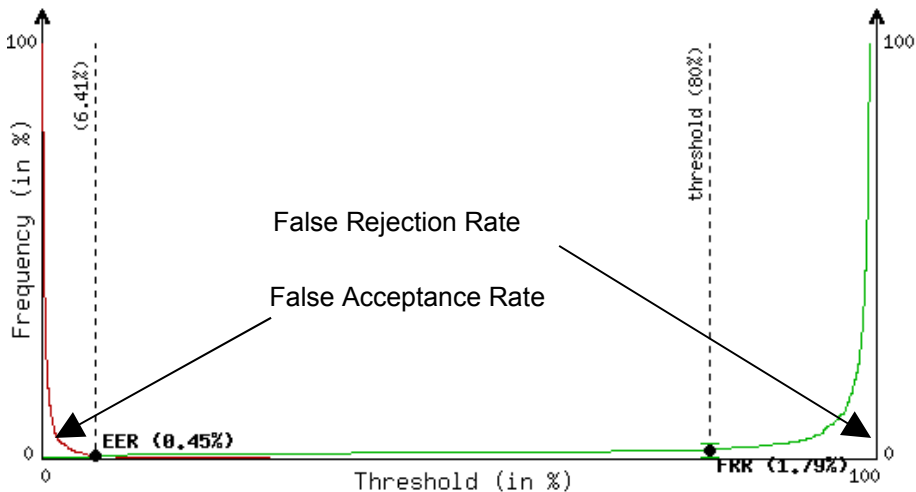
Grundsätzlich ist die Verfahrensqualität von der Textlänge abhängig. Je mehr man tippt, desto mehr Information steht Psylock zur Verfügung und desto besser ist die Erkennungsleistung. Deshalb lässt sich die Qualität von Psylock sehr hoch steigern. Derzeit wird mit etwa 40 Anschlägen ein Sicherheitsniveau erreicht, das für normale Sicherheitsdomänen bei weitem ausreicht. In der Regel liegt der Threshold (Sicherheitsschwelle) bei 80 %. Ein Benutzer erreicht zumeist einen Matchscore von über 95 %. Nur wenn man beim Tippen gestört wird (z.B. durch ein Telefonat), sehr flüchtig oder in einer ungewohnten Körperhaltung tippt oder sich öfters vertippt und der Schreibfluss dadurch wesentlich unterbrochen ist, wird der Matchscore unter 80 % liegen.

Da man das mehrmalige Tippen hintereinander als stochastisch nur schwach abhängig betrachten kann, sind Rückweisungswahrscheinlichkeiten multiplikativ verknüpft. Für jede erneute Falschrückweisung reduziert sich die Wahrscheinlichkeit um etwa 50 %. Beim zweiten Versuch ist eine Rückweisung schon sehr unwahrscheinlich und nach dem dritten Versuch nur noch bei sehr groß angelegten Feldversuchen beobachtbar.

Die Wahrscheinlichkeit, dass ein Angreifer bei einem Threshold von 80 % erfolgreich ist, kann ebenfalls nur in groß angelegten Feldversuchen gemessen werden, so verschwindend gering ist sie. In vielen Praxistests lag sie bei Null. Bei dem jüngsten Feldversuch vom März 2008 lag die Falschrückweisung bei unter zwei Prozent und die Falschakzeptanz bei unter einem Promille. Siehe hierzu die Abb. 2. Dies belegt die hohe Qualität.

False Acceptance Rate (FAR), False Rejection Rate (FRR)

25 Mar 2008 14:21:45 - Psylock internal Test



Number of attacks: 1189 Number of user logins: 837

Abbildung 2: Bei einem Threshold von 80% liegt die Falschakzeptanz bei unter einem Promille und die Falschrückweisung bei 1,79%.

Eine Zertifizierung der Psylock-Software vom Bundesamt für Sicherheit in der Informationstechnik ist beantragt. Außerdem wird derzeit an dem Nachweis gearbeitet, dass Psylock SOX-compliant ist.

2.4 Proof of Concept

Der Proof of Concept ist erbracht. An der Universität und der Fachhochschule Regensburg mit insgesamt 32.000 Benutzern wurde Psylock in der Produktvariante Password Reset im Oktober 2006 installiert. Bei vergessenem Passwort kann man sich ein neues Passwort im Self Service als Web-Applikation vergeben. Im Mai 2008 wurde sie durch die Version V2 abgelöst. Das Programm läuft fehlerfrei.

Die Fachhochschule Landshut mit etwa 3.000 Benutzern verwendet Psylock seit März 2007. Nach einem Anfangstest von Password Reset, der ähnlich verlief wie bei der Universität Regensburg, wurde an der Fachhochschule Psylock in die eigenen Lösungen integriert, z.B. in das SB-Portal für Studenten.

Versionierung

Version V1: Release im Oktober 2006

Version V2: Release im Mai 2008; neuer Methodenkernel, Enrollment um über 70 % gekürzt

Version V3: Ende 2008; jeder kann sich seinen eigenen Satz wählen, Lebenderkennung.

3 Nutzen

3.1 Alleinstellungsmerkmale von Psylock

Biometrie ohne Sensor

Psylock benötigt keine speziellen Sensoren oder andere Hardware – als reine Softwarelösung funktioniert es mit handelsüblichen Tastaturen und an jedem PC. Das ermöglicht einen mobilen und flächendeckenden Einsatz zu günstigen Kosten.

Skalierbare Sicherheit ohne Technologiewechsel

Die Qualität des Verfahrens lässt sich über die Länge des Tippertextes einstellen. Je mehr man tippt, desto mehr Information über das Tippverhalten kann Psylock auswerten und desto besser wird in der Konsequenz die Trennschärfe (Unterscheidung zwischen berechtigtem Benutzer und Angreifer). Man kann deshalb das Sicherheitsniveau je nach Kundenbedarf beliebig erhöhen. Für Anwendungen im Hochsicherheitsbereich braucht man nur etwas mehr zu tippen. Bildgebende Biometrien können dies nicht leisten.

Das Authentisierungsmerkmal ist verborgen

Bildgebende biometrische Merkmale wie Fingerabdruck, Iris, Handgeometrie etc. liegen offen zutage und bergen deshalb die Gefahr, ohne großen Aufwand gestohlen zu werden. Im Internet existiert bereits eine Plattform für den Handel mit derartigen Personendaten. Das Tippverhalten einer Person auszuspähen, ist wesentlich aufwändiger. Aber selbst wenn es gelingt, einen Keylogger als Trojaner einzuschleusen, ist Psylock dagegen gefeit, wie das Folgende zeigt.

Wirksame Abwehr von Angriffen

Kann man einen Angriff mit erspähten Passwörtern oder mit kopierten biometrischen Merkmalen erkennen? Beim Passwort ist dies unmöglich. Ihm sieht man nicht an, ob es gestohlen wurde oder nicht. Kennt ein Angreifer das Passwort, kann man gegen sein unberechtigtes Eindringen in das System nichts unternehmen. Bei bildgebenden Biometrien hängt es davon ab, wie gut die Kopie des Fingerprints, Iris-Scans etc. ist. Ein billiger Sensor lässt sich durchaus überlisten, wie zahlreiche Presseberichte dokumentieren.

Wie ist das beim Tippverhalten? Eine Angriffsmöglichkeit sind Keylogger. Das sind Trojaner, welche alle Tasteneingaben, also auch die Passworteingabe, mitschneiden und an den Angreifer senden. Psylock schützt sich vor derartigen Attacken. Es erkennt alte Mitschnitte als Kopien, auch wenn sie an manchen Stellen abgeändert wurden. In der Version V3 arbeitet es zusätzlich nach dem Challenge-Response-Verfahren. Das bedeutet: Der kurze Satz, der auf dem Bildschirm zum Abtippen erscheint, beinhaltet jedes Mal als Überraschung an unterschiedlichen Stellen ein oder mehrere neue Wörter, die auf den mitgeschnittenen Tippversuchen fehlen. Jede Login-Tippvorlage besitzt den Charakter der Einmalverwendung.

Lebenderkennung ohne Sensor

In der Version V3 bietet Psylock eine Lebenderkennung auf reiner Software-Basis. Die Textvorlage erscheint als Captcha, also in einer Form, die nur der Mensch lesen kann, aber kein Computerprogramm. Deshalb muss es auch ein Mensch sein, der diese Vorlage eintippt und insbesondere die richtige Response auf die Challenge gibt.

Einzigste uneingeschränkte Web-Authentisierung ohne Passwort

Psylock ist die einzige Authentisierungstechnologie ohne Passwort, die uneingeschränkt im Internet anwendbar ist. Sie funktioniert in den verschiedensten Sprachen und mit den unterschiedlichsten Tastatur-Layouts. Damit kann ein Mitarbeiter von überall in der Welt über das Internet auf seine Daten in der Firma zugreifen. Auch jeder Kunde, der eine Online-Überweisung tätigt, im Webshop einkauft oder sich anderswo im Web authentisieren muss, kann dies ohne Einschränkung tun, wenn immer er eine handelsübliche Tastatur zur Verfügung hat.

3.2 Genereller Kundennutzen des Systems Psylock

Psylock erhöht der Sicherheit

Beim Passwort ist man nie sicher, wer es tippt. Schätzungen gehen davon aus, dass in Betrieben etwa ein Viertel aller Passwörter im Kollegenkreis verbreitet sind. Selbst wenn alle Mitarbeiter sorgfältig mit ihren Passwörtern umgehen, so bleibt dennoch die Gefahr, dass diese mit Hilfe von Trojanern ausgespäht werden. Psylock schließt die Lücken des Passwortschutzes zuverlässig. Es schafft die notwendige strenge Bindung des Merkmals an den Merkmalsträger und erkennt Angriffe mit gefälschten bzw. erspähten oder gestohlenen Merkmalen. Das Tippverhalten kann nicht weiter gegeben werden. Die personentypischen Eigenheiten des Tippens spielen sich im Millisekundenbereich ab.

Das Tippverhalten unterliegt nicht der Gefahr, geraubt zu werden

Die Abgabe eines Fingerabdrucks oder Passwortes kann von Kriminellen unter Gewaltanwendung geraubt oder abgepresst werden. Beim Tippverhalten ist dies nicht möglich.

Psylock bietet eine hohe Benutzerfreundlichkeit

Psylock zeigt den Weg aus der Passwortflut. Der Benutzer braucht sich keine Passwörter mehr zu merken. Den Tipptext muss man sich nicht merken, er wird am Bildschirm angezeigt. Wenn sich das Tippverhalten einer Person ändert, dann lernt Psylock automatisch mit. Der erstmalige Trainingsaufwand beträgt nur 2-5 Minuten.

3.3 Nutzen von Psylock Password Reset

Psylock Password Reset bietet eine webbasierte Self-Service-Lösung für das Problem vergessener Passwörter im Unternehmen an. Benutzer können sich über eine Webschnittstelle nach erfolgreicher Authentisierung selbstständig ein neues Passwort zuweisen.

Psylock Password Reset bietet hohe Einsparungspotenziale. Das Helpdesk wird um durchschnittlich 30 % entlastet und der Mitarbeiter verliert wenig Zeit. Die selbstständige Passwortneuvergabe ist innerhalb einer Minute geschehen. Ohne Psylock muss er zwischen 10 Minuten und zwei Stunden auf sein neues Passwort warten. Oftmals ist auch der Vorgesetzte in den Password Reset Prozess eingebunden. Eine Untersuchung bei einem Unternehmen mit 30.000 Benutzern hat ergeben, dass im Jahresdurchschnitt jeder Benutzer das Passwort 4,2-mal vergisst. Pro Vorfall kostet dies laut einer Internetrecherche ca. 25-45 €. Somit lassen sich in großen Unternehmen mit Password Reset jährlich 110-190 € pro Benutzer sparen. In kleinen und mittelständischen Unternehmen können zusätzliche Probleme entstehen, wenn im Zweischichtbetrieb oder auch am Samstag am Computer gearbeitet wird, die DV-Administration aber nur im Einschichtbetrieb besetzt ist. Hier bietet Password Reset den Vorteil, dass es rund um die Uhr sieben Tage die Woche verfügbar ist.

3.4 Nutzen von Psylock Web Login

Psylock Web Login bietet eine stark personengebundene Authentisierung im Web als Alternative zum Passwort. Genutzt werden kann sie bei allen Web-Authentisierungen, die bisher mit Passwort arbeiten (e-Bay, PayPal, Amazon, Online Banking, etc.). Auch eine Absicherung des Remote Access auf das Firmennetz über das Internet, z.B. für Wartungszwecke, von überall in der Welt ist möglich.

Der Kundennutzen liegt gegenüber der Passwort-Authentisierung in der höheren Sicherheit und Bequemlichkeit. Bei kostenpflichtigen Abonnementdiensten im Internet kann sichergestellt werden, dass sie ausschließlich von Personen genutzt werden, die tatsächlich Abonnenten sind. Dies wirkt Ertrag steigernd.

3.5 Nutzen der Psylock API

Die Psylock API kann vom Kunden in dessen Produkte und Anwendungen integriert werden. Für die Login-Funktion kommen Betriebssysteme (Netzwerk, PC, Notebook, Smartcard), Single Sign On-Systeme und Kundensoftware (SAP-Systeme, Lotus Notes, Finanzbuchhaltungssoftware, Workflow Management Systeme,...) in Frage.

Neben der reinen Login-Funktion sind weitere Anwendungen für Web-Applikationen Web möglich:

- *Fraud Protection:* bei der Registrierung eines Kunden wird das Tippverhalten aufgezeichnet. Es kann überprüft werden, ob sich eine Mehrfachregistrierung vorliegt, um z.B. bei Auktionen den Preis künstlich hoch zu treiben oder um ein kostenloses Schnupperangebot mehrmals hintereinander zu nutzen.
- *Online Banking:* Das Tippverhalten beim Ausfüllen des Überweisungsauftrages wird aufgezeichnet und der Überweisung fälschungssicher beigefügt. Das macht die TAN überflüssig. Auch können Transaktionen mit höheren Beträgen zusätzlich durch eine Psylock-Authentisierung abgesichert werden.
- *Marktforschung:* Bei Online-Befragungen beweist der Panelist durch sein Tippverhalten, dass auch er es ist – z.B. der Arzt und nicht die Sprechstundenhilfe – der den Fragebogen ausfüllt.



- *eLearning*: Für viele Online-Weiterbildungskurse verweigern die Berufskammern die Anerkennung, weil die Identität des Teilnehmers nicht zuverlässig überprüft werden kann. Sie müssen deshalb zum Veranstaltungsort reisen. Eine Psylock-Authentisierung akzeptieren die Berufskammern wegen der zuverlässigen Personenbindung.

Der Nutzen besteht im Sicherheits- und der Komfortgewinn.

3.6 Nutzen der Intrusion Detection

Lässt man Psylock im Hintergrund laufen, so wird online das Tippverhalten darauf hin kontrolliert, ob noch immer der gleiche Benutzer vor dem Rechner sitzt (Intrusion Detection). Falls nicht, gibt es eine Meldung aus oder initiiert eine Sperrung des Nutzers. Mit Psylock Intrusion Detection können natürlich nicht nur Arbeitsplatzrechner, sondern auch Server und andere Systeme überwacht werden.

Der Nutzen liegt in der höheren Sicherheit. Hier wird eine Lösung geboten, die es so noch nicht gibt.

3.7 Nutzen eines Psylock Authentication Services

Eine weitere spezielle Lösung ist der Psylock Authentication Service. Dieses Produkt ermöglicht die Benutzeranmeldung in privaten und semi-professionellen Internetanwendungen (Vereinsseiten, Blogs, Fotoalben usw.). Die Psylock-Authentisierung steht als Webservice nach dem OpenID-Konzept für Jedermanns Benutzung zur Verfügung.

Nur eine festgelegte Benutzergruppe erhält Zugriff auf bestimmte Webseiten. Die Kunden erhalten eine einfache Quellcode-Vorlage, mit der sie die Psylock-Authentisierung als Webservice in die eigene Homepage einbauen. Über eine Verwaltungsseite legt der Kunde fest, welche Benutzer (auf Basis der E-Mail-Adresse) Zugriff erhalten. Der Benutzer enrollt sich beim Psylock Authentication Service. Als User-ID wird die E-Mail-Adresse verwendet.

Beim aktuellen Zugriff auf eine geschützte Seite gibt der Benutzer seine E-Mail-Adresse und sein Tippverhalten ein. Es wird ein Re-Direct zum Psylock Authentication Service aufgebaut. Bei erfolgreicher Authentisierung sendet der Server ein Zertifikat (Ticket) zurück.

Einsatzgebiete sind:

- Private Homepages, Blogs usw. im Web 2.0
- Freigabe von bestimmten Seiten nur für Vereinsmitglieder
- Quellcode-Verwaltung bei Open Source Entwicklungen
- Zugang zu Online-Kooperationsprojekten.

4 Marktchancen

4.1 Vergleich mit Wettbewerbern

Das Psylock-System ist derzeit einmalig auf dem Markt. Es gibt keine direkten Konkurrenzprodukte mit vergleichbaren Eigenschaften. Vor Imitaten schützen die Patente bis ins Jahr 2017. Der einzige Wettbewerber mit einer Tippverhaltensbiometrie BioPassword (jetzt AdminOne) bietet sein Produkt nur als Passwort Hardener an, also keine echte Alternative zur Passwort-Authentisierung. Die Stimmerkennungssoftware Voice.Trust von der gleichnamigen Firma bedient nur den Nischenmarkt Password Reset. Konkurrenten für den Login-Markt sind Sensor-Biometrien und Smartcards. Sie haben gegenüber Psylock einen Preisnachteil.

Die Wincor Nixdorf AG hat 2006 einen Vergleich von Psylock Version V1 mit dem unternehmenseigenen Produkt Identity Manager Pro Tect/Work Enterprise (Fingerprint) und mit der Stimmerkennungssoftware Voice.Trust vorgenommen. Hierin zeigt Psylock die größte Anwendungsbreite.

Tabelle 1

Gegenüberstellung biometrischer Verfahren

Merkmale	ProTect/Work Enterprise	Voice Trust	Psylock
Beschreibung	Authentifizierung mittels Fingerabdruck	Authentifizierung mittels Stimme	Authentifizierung mittels Tastatur
Notwendige Medien	Fingerprint Sensor	Telefon	PC Tastatur
Authentifizierungsvarianten	Identifikation / Verifikation	Verifikation	Identifikation
Enrollment			
Vorgehensweise	1-10 Finger 3 mal aufzeichnen und jeweils 1 mal verifizieren	3-10 vorgeschene Vornamenspaare 3-7 mal nachsprechen	Vorgegebenes Textmuster 20 mal nachtippen
Zeitlicher Aufwand	3 - 5 Minuten je Anwender	5 - 10 Minuten je Anwender	5 - 10 Minuten je Anwender
Abhängigkeiten	Qualität des Sensors	Sprachkanal (Festnetz, Handy, VOIP)	keine (Funk Tastaturen noch problematisch)
Authentifizierung			
Vorgehensweise	Einen zugelassenen Finger nach Anforderung auf den Sensor legen.	Vorgegesprochene Vornamenpaare nachsprechen	Vorgegebenes Textmuster nachtippen
Zeitlicher Aufwand	1-2 Sekunden	2-3 Minuten	Je nach Länge des Textmusters zwischen 10 und 30 Sekunden
Anwendungsgebiete			
Anmeldung am PC	Ja	Wenn überhaupt, dann nur eingeschränkt	Ja
Freischaltungen / Kennwortrücksetzungen	nicht notwendig	Ja	Ja
Legitimationsprozesse	Auf Grund der notwendigen Spezialhardware eher nein	Ja	Ja

Tabelle 2

Mögliche Anwendungsfälle

Integration	ProTect/Work Enterprise	Voice Trust	Psylock
Individuelle Anwendungen	Ja	Ja	Ja
Berechtigungs-systeme	Ja	Ja	Ja
E-Mail / Dokumenten-signatur	Eingeschränkt	Eingeschränkt	Ja
Legitimierungen wie Online Banking	Eingeschränkt	Ja	Ja
Authentifizierungs-dienst im WEB	Nein	Eingeschränkt	Ja

Im hinsichtlich wichtiger Vermarktungskriterien schneidet Psylock sehr gut ab.

Tabelle 3

Leistungsvergleich					
	Biometrie	Token	Voice Trust	Biopasswort	Psylock
Verfügbarkeit (immer dabei)	++	+	++	++	++
Komfort	++	++	o	++	o
Sicherheit	+	+	+	o	++
Ubiquität	o	o	+	++	++
Einführungsaufwand	o	o	+	++	++
Betriebskosten	o	o	++	++	++
Vertriebsaufwand	o	o	o	++	++
Mögliche Anwendungsfälle	o	o	o	o	++

4.2 Benutzerakzeptanz der Psylock Software

Hierzu liegen zwei Ergebnisse vor. Die Benutzerakzeptanz wurde erstmals in einem ausgedehnten Feldversuch in den beiden Standorten München und Schweinfurt der HVB Direkt erhoben. Obwohl man Biometrien gegenüber eher ablehnend gegenüber stand, war man dem Tippverhalten gegenüber aufgeschlossen.

Das deutsche Marktforschungsinstitut Psyma führte Anfang 2007 eine Befragung von 3000 Panelisten durch. Die Akzeptanz war bei über 98 Prozent der Befragten sehr hoch, obwohl man zu diesem Zeitpunkt für das Enrollment einen Satz mit 45 Anschlägen dreißig Mal tippen musste (Version V1). Jetzt ist es nur noch neun Mal.

4.4 Business Model

Das Business Model sieht vor, die Psylock-Technologie für zwei hoch standardisierte Einsatzfelder Password Reset und Web Login als fertige Produkte anzubieten. Daneben gibt es eine große Zahl von individuellen Lösungen, in welche Psylock eingebunden werden kann. Um einen raschen Markteintritt zu erreichen, sollen diese Lösungen nicht von der Psylock GmbH eigens entwickelt werden. Vielmehr werden die Softwarehersteller bzw. Endkunden in die Lage versetzt, über eine Auslizenzierung Psylock selbst in ihre Lösungen zu integrieren. Dazu wird ihnen die Psylock API als Entwicklerpaket zur Verfügung gestellt. Speziell ausgebildete Software-Partnerhäuser bieten einen Wartungsservice in den verschiedenen Vertriebsregionen.

4.5 Derzeitiger Vertriebsstand

Ende 2007 wurde die Psylock GmbH gegründet und von Investoren mit dem benötigten Kapital ausgestattet. Der Unternehmenszweck ist die Weiterentwicklung und der Vertrieb der Psylock Software. Die Ausstellung auf der diesjährigen CeBIT in Hannover stieß auf außergewöhnlich großes Interesse bei Besuchern und Medien. Im Augenblick befindet sich die Psylock-Software bei zahlreichen in- und ausländischen Unternehmen im Test, darunter auch bei sehr großen Unternehmen. Derzeit werden die Vertriebskanäle in Deutschland und Westeuropa ausgebaut.

4.6 Marktpotenziale

Password Reset zielt in einen weltweiten sehr großen Markt, der noch kaum ausgeschöpft wird. Zielkunden sind alle Unternehmen mit mehr als 250 Computerarbeitsplätzen. In Deutschland gibt es 23,9 Mio sozialversicherungspflichtig Beschäftigte (Quelle: Unternehmensregister - System 95 (Stand 31.12.2006)). Davon arbeiten 10,1 Mio in Unternehmen mit mehr als 250 Beschäftigten. Der Anteil an Computerarbeitsplätzen beträgt 58 %. Also beträgt das Marktpotenzial in Deutschland 5,858 Mio Beschäftigte. Der Anteil Deutschlands am Weltmarktpotenzial beträgt 5,63% (Quelle: <http://www.c-i-a.com/pr0305.htm> Computer Industry Almanac). Daraus errechnet sich ein weltweites Marktpotenzial von fast 110 Mio Beschäftigten am Computerarbeitsplatz.

Das Marktpotenzial für Psylock Web und für die Psylock API ist weltweit sehr groß. Für das Login in Betriebssysteme kann man mit 370 Mio Benutzern weltweit rechnen, für welche die Psylock Login infrage kommt. Bei Web Login sind die wichtigsten Zielkunden Unternehmen mit vielen Millionen Kunden

(Webmailer, Auktionshäuser, Webshops,...). Die Zahl der Internet-Benutzer beträgt derzeit ca. 1,1 Mrd. Personen.

Auch die Zielmärkte für Intrusion Detection und für den Authentication Service sind sehr groß. Die Psylock Intrusion Detection kann z.B. von Herstellern von Anti-Viren-Software mit vertrieben werden. Die drei größten Anbieter (Symantec, Trend Micro, McAfee) besitzen 86 % Marktanteil. Das Marktvolumen liegt bei jährlich 5 Mrd. Euro.

4.7 Fazit

Das Marktpotenzial für Psylock ist immens groß. Dessen Ausschöpfung wird im Wesentlichen von den Möglichkeiten und Fähigkeiten des Vertriebs bestimmt. Das Marktfenster ist derzeit offen. Psylock stößt als Biometrie ohne Sensor international auf großes Interesse. Es bietet den Kunden einen wertvollen Beitrag zur Lösung ihrer vielfältigen Authentisierungsprobleme.

Literaturverzeichnis

- [Bartmann 1997] Bartmann, D., Bartmann, D. jun.: Verfahren zur Verifizierung der Identität eines Benutzers einer mit einer Tastatur zur Erzeugung alphanumerischer Zeichen zu bedienenden Datenverarbeitungsanlage, Deutsches Patent Nummer: 196 31 484, 1997.
- [Bartmann 2001] Bartmann, , Dieter: Verfahren zur Verifizierung der Identität eines Benutzers einer mit einer Tastatur zur Erzeugung alphanumerischer Zeichen zu bedienenden Datenverarbeitungsanlage. Europäische Patentschrift, Nummer EP 0 917678 B1, August 2001.
- [Bartmann 2007] Bartmann, D., Bakdi, I., Achatz, M.: On the design of an authentication system based on keystroke dynamics using a predefined input text. Int. Journal of Information Security and Privacy. 2 (1) 2007, 1-12.
- [Bleha 1991] Bleha, S. A. und Obaidat, M. S.: Dimensionality reduction and feature extraction applications in identifying computer users. IEEE transactions on systems, man, and cybernetics, Bd. 2, 1991, Nr. 2, S. 452 - 456.
- [Brown 1996] Brown, Marcus E.; Rogers, Samuel J.: Method and apparatus for verification of a computer user's identification, based on keystroke characteristics. US Patent, Nummer 5,557,686, September 1996.
- [Brayn 1897] Brayn, William L.; Harter, Noble: Studies in the Physiology and Psychology of the Telegraphic Language. In: Psychological Review 4 (1897), Nr. 1, S. 27-53.
- [de Ru 1997] de Ru, W. G. und Elo, J. H. P.: Enhanced password authentication through fuzzy logic. IEEE expert intelligent systems & their applications, Bd. 12, 1997, S. 38-45.
- [Foot 1999] Foot, Michael R. D.: SOE – An Outline History of the Special Operations Executive 1940-1946. London : Pimlico, 1999. – ISBN 0-7126-6585-4.
- [Gaines 1980] Gaines, R. S.; Lisowski, William; Press, S. J.; Shapiro, Norman: Authentication by Keystroke Timing: Some Preliminary Results. Rand Report R-256-NSF / Rand Corporation. 1980. – Forschungsbericht.
- [Garcia 1986] Garcia, J. D: Personal identification apparatus, United States Patent Number: 4 621 334, 1986.
- [Grundner 2008] Grundner, Thomas; Wöfl, Thomas: Verfahren und Vorrichtung zur Identifizierung einer Person mittels ihres Tippverhaltens unter Berücksichtigung der örtlichen Verteilung der Tasten einer Tastatur. Deutsches Patentamt 102008002544.5, Juni 2008.
- [Legget 1988] Legget, J. und Williams, G.: Verifying identity via keystroke characteristics. International journal of man-machine studies, Bd. 28, 1988, S. 67 - 76.
- [Monrose 2002] Monrose, F., Reiter, M., Wetzel, S.: Password hardening based on keystroke dynamics. IJIS, 4, 2002, 69-83.

[Needleman 1970] Needleman, Saul B.; Wunsch, Christian: A general method applicable to the search for similarities in the amino acid sequence of two proteins. *Journal of molecular biology* Bd. 48, S. 443-453, 1970.